NATIONAL DEFENCE UNIVERSITY “CAROL I”

REGIONAL DEPARTMENT OF DEFENSE RESOURCES
MANAGEMENT STUDIES

INFORMATION SECURITY MANAGEMENT – TRENDS AND OPPORTUNITIES

Workshop unfolded during the postgraduate course in Information Security Management

- 11.01 - 05.02.2010, Brasov -

Coordinator:

LTC Lect. eng. Daniel Sora

National Defense University „Carol I” Publishing House
BUCHAREST 2010

ISBN: 978-973-663-831-2

The content of the papers is in the entire responsibility of the author(s), and does not necessarily reflect the opinion of the Scientific Board.

CONTENT

ACKNOWLEDGEMENT

This volume is the first from what will hopefully be a long series of such undertakings. In fact, it is intended to be the materialization of my and my students' studies, research, and discussion sessions in the field of Information Security Management. The first course in Information Security Management unfolded between 11.01 - 05.02.2010, and the papers presented in this volume are the outcome of the course-related workshop.

I initiated this course for I am convinced that information is vital for any organization's success, whereas information security is vital for any organization's survival in today's over-competitive environment. Economic, social, military, cultural, political challenges are ever growing, and companies must learn how to face these challenges in an effective and efficient manner. Therefore, this course attempts to address such issues both proactively and interactively.

I would like to emphasize that the entire course is designed as a constructive exchange of ideas and information in a student-centered format, while I act as a facilitator rather than an answer provider. Case studies and real-life examples play a pivotal role in this educational process, which is seen more as an orientation opportunity and less as a solution collection. In my opinion, it is more important to know *how* and *where* to look for answers than to rely on pre-established – and, therefore, hazardous – recipes for success.

To conclude this brief introductory note, I would like to reiterate our intention to make such endeavors into a long lasting and fruitful tradition, based on which to build our future successes. In this respect, I believe that our future collaboration and alumni's common projects can be beneficial to all parties participating in the processes.

Also, I would like to thank every course participant individually and all of them as a group for their honest and active involvement in our analyses and discussions, which contributed to creating a friendly classroom atmosphere that fostered my teaching activity and enhanced our mutual learning.

LTC Lecturer eng. Daniel Sora

ENHANCED SYSTEM SECURITY WITH THE LABVIEW DATALOGGING AND SUPERVISORY CONTROL MODULE

LTC lect. eng. Daniel SORA

The Regional Department of Defense Resources Management Studies - Brasov

Abstract

Handling sensitive data often brings up security questions. Who should have access to the data and to which parts? Should everyone be able to modify the file or database? By defining the system needs up front, engineers can choose tools to help them to do this. LabVIEW with the DSC Module enables engineers to define user profiles that limit access to different specific user interface controls on the application, as well as to different and sensitive sections of the data. This article describes the functionality provided by the LabVIEW Datalogging and Supervisory Control (DSC) Module to facilitate the implementation of security for LabVIEW project libraries, shared variables and front panel objects. This article also discusses how the security architecture separates user management and authentication from resource permissions.

Introduction

The LabVIEW DSC Module provides a set of powerful tools to facilitate security for LabVIEW project libraries, shared variables and front panel objects located on local and network systems. Security functionality is divided into two categories: user management and authentication, and resource permissions. User management and authentication is provided by the Domain Account Manager, so the developer can store all user information in a centralized location. With this architecture, distributed systems can access a single location for user information instead of storing the accounts on each computer. The Domain Account Manager also manages user authentication so distributed or networked systems do not need to implement the functionality themselves. The user information provided by the Domain Account Manager is used by LabVIEW project libraries, shared variables and front panel objects to assign permissions.

Distributed data logging systems have the most extensive lists of best practices:

- Reliable, efficient data storage
- Efficient tools for managing system-wide data
- Real-time and historical viewing of the entire system
- The ability to configure and log alarms and events
- Easy networking for different types of devices
- User interface security

Early LabVIEW DSC Module Security Model

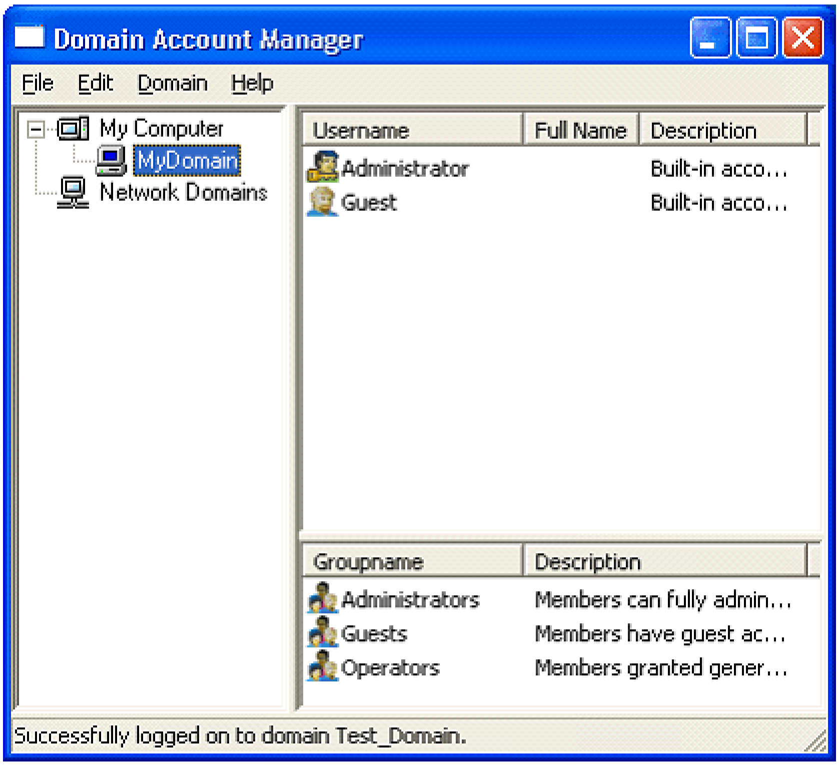
In LabVIEW 7.x and earlier, the LabVIEW DSC Module uses a user account database on each computer to authenticate users and provide security for different resources. Having a single user account database creates a problem because the authenticating computer has knowledge of only users on the computer where the database resides. The authenticating computer is not aware of users on other computers. Furthermore, attaching a user account database to each computer might not be feasible for embedded or real-time targets because of their limited computing power.

Domain Account Manager

The LabVIEW 8 DSC Module introduces the Domain Account Manager, which provides a more flexible, mature, and robust security solution than earlier versions of the LabVIEW DSC Module. The Domain Account Manager serves as a central repository for managing local and remote user authentication and account management. You use the Domain Account Manager to create users and user groups, each with different privilege levels. Users can be added to any number of groups. This arrangement simplifies the process of assigning permissions to local and networked LabVIEW resources. Instead of having a single computer implement user authentication and store user or group information, individual computers communicate with a Domain Account Manager located on a remote computer. This remote computer then determines which users are trying to access a resource and to which group each user belongs.

Implementing Security with the LabVIEW DSC Module

To launch the Domain Account Manager, select **Tools»Security»Domain Account Manager** from the pull-down menu in the project manager. In the Domain Account Manager, shown in Figure 1, right-click the **My Computer** icon and select **New Local Domain** from the shortcut menu. Then, enter a domain name and create an Administrator password. The Administrator is the default user that can add or remove users and user groups, change user permissions, modify user passwords, and so on. This functionality is limited to the Administrator and any users in the Administrators group. The other default groups include Operators and Guests.



Username	Full Name	Description
Administrator		Built-in acco...
Guest		Built-in acco...

Groupname	Description
Administrators	Members can fully admin...
Guests	Members have guest ac...
Operators	Members granted gener...

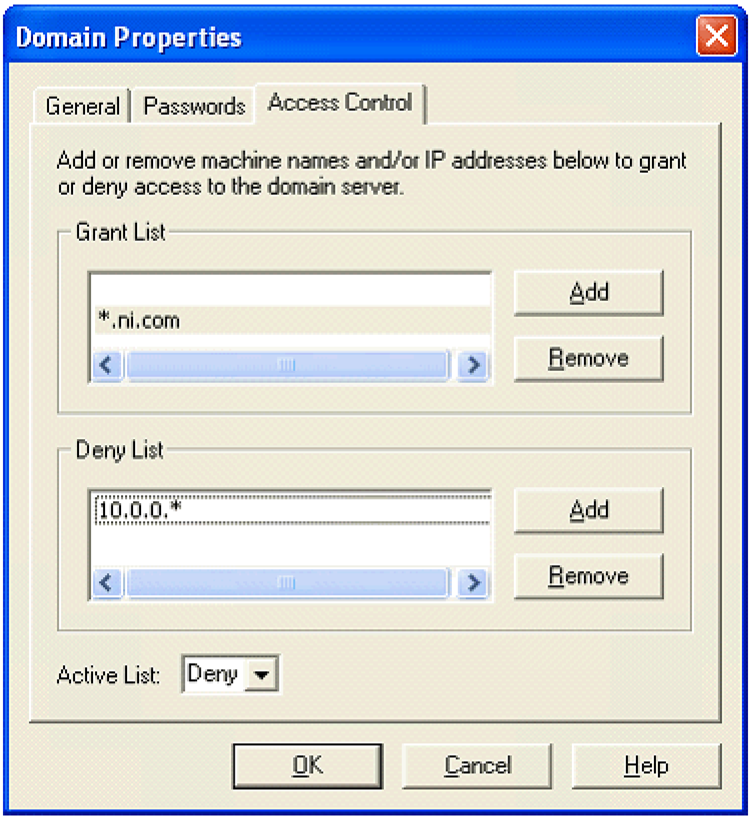
Successfully logged on to domain Test_Domain.

Figure 1. Main Window of the Domain Account Manager

The Domain Account Manager has many security features, such as encryption, that increase the security of the computer on which it is deployed. The Domain Account Manager uses a challenge and response protocol to transmit passwords over the network. Because no clear text password is transmitted through the network, malicious eavesdropping techniques do not reveal the user’s password. The Domain Account Manager also uses a one-way hash function to store passwords. Using this type of storage, applications can validate passwords with the Domain Account Manager, but these applications cannot determine the actual password.

To increase security, you can control access to the Domain Account Manager by assigning permissions to both individual computers and subnets. By denying access to the Domain Account Manager you are effectively denying access to any of the resources that use the Domain for user authentication. If a computer or subnet cannot access the Domain Account Manager, the requested resource cannot determine the necessary permissions.

You can use both individual computer names and IP addresses to control access to the Domain Account Manager. You also can use the "*" wildcard to control access by a range of computers or IP addresses. For example, granting access by "*.ni.com" specifies that all computers whose name ends with "ni.com" can access to the Domain Account Manager. Conversely, denying access by "10.0.0.*" specifies that no computer on the 10.0.0 subnet can access the Domain Account Manager. Figure 2 shows these settings of the **Domain Properties** window. You access this window by launching the Domain Account Manager, selecting **Edit»Properties** from the pull-down menu, and clicking the **Access Control** tab.



Add or remove machine names and/or IP addresses below to grant or deny access to the domain server.

Grant List

*.ni.com

Deny List

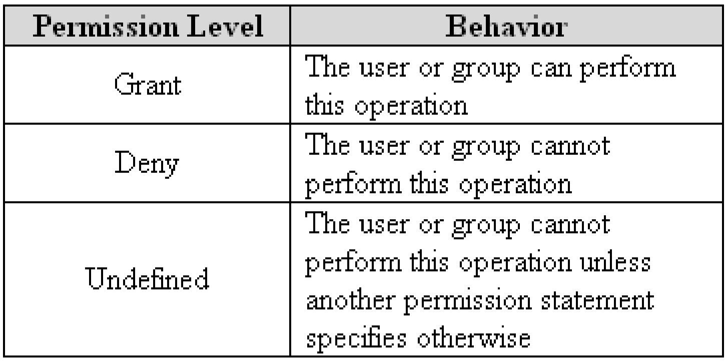
10.0.0.*

Active List: Deny

Figure 2. Domain Properties Windows/Access Control Tab

Project Library and Shared Variable Operations and Permissions

Project libraries and shared variables are two types of resources that use the security features provided by the LabVIEW DSC Module. You can use permission levels to control read/write access to both of these resource types. The three permission levels are Grant, Deny, and Undefined. Table 1 describes these permission levels.



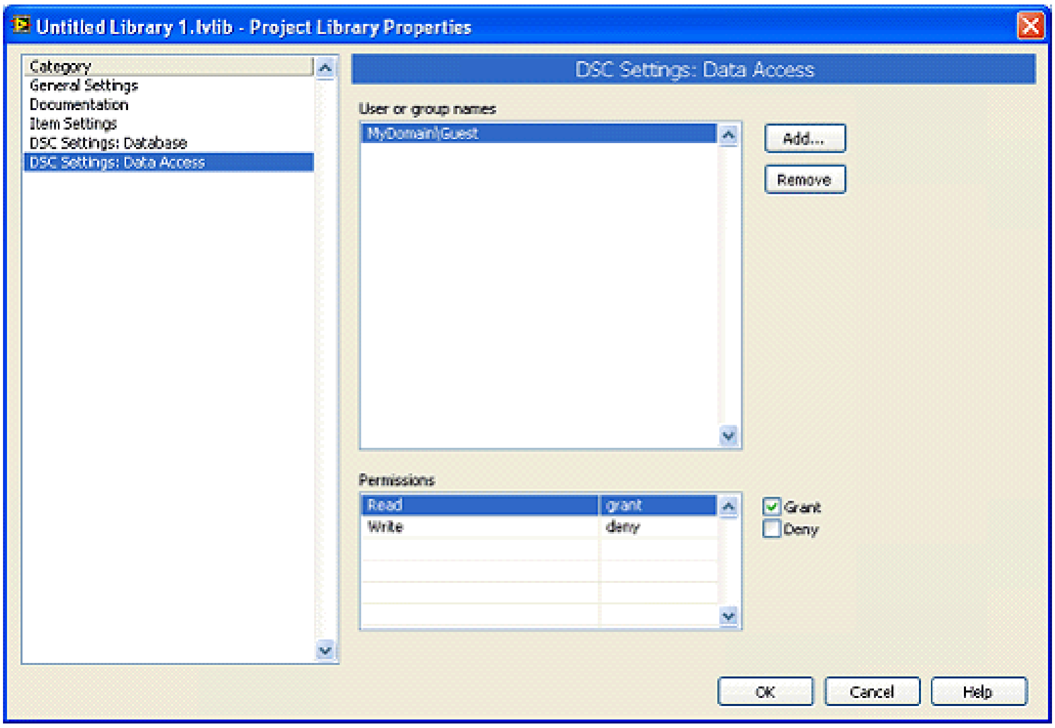
Permission Level	Behavior
Grant	The user or group can perform this operation
Deny	The user or group cannot perform this operation
Undefined	The user or group cannot perform this operation unless another permission statement specifies otherwise

Table 1. Permission Levels for Project Libraries and Shared Variables

Permissions are assigned hierarchically. The highest level of permissions is that which is defined at the project library level. By assigning permission to a library, you are assigning permissions to all project libraries and shared variables contained in that project library. The undefined permission can be overridden at the same hierarchical level or at a higher one.

Project Library Security

Once users and user groups have been defined in the Domain Account Manager, this user information can be used to determine the read/write permissions to perform operations on different resources. To set user and group permissions for a project library, right-click the project library and select **Properties** from the shortcut menu. Then select **DSC Settings: Data Access** from the **Category** list. Figure 3 shows the Data Access category of the **Properties** window for a project library. Notice the user has only read access to the project library.



Untitled Library 1.lvlib - Project Library Properties

DSC Settings: Data Access

User or group names: MyDomain\Guest

Permissions

Read	grant
Write	deny

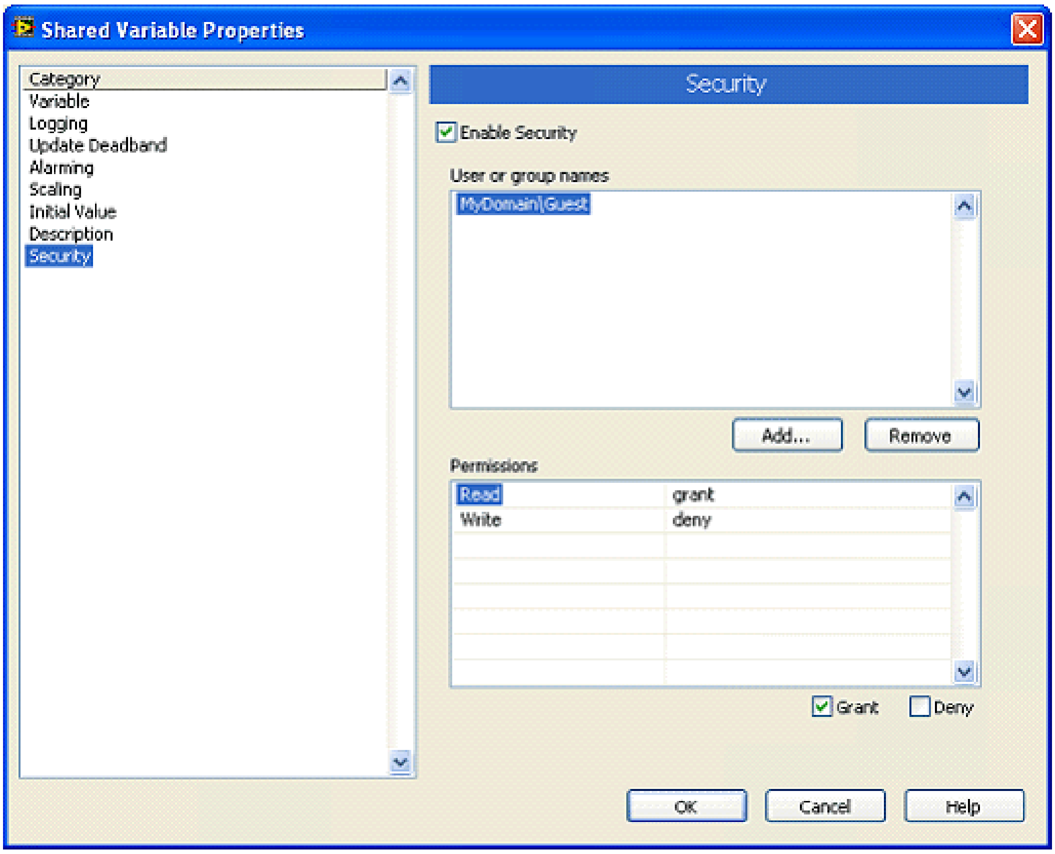
☑ Grant
☐ Deny

Figure 3. Setting Permissions for a Project Library

Shared Variable Security

Shared variables use the Domain Account Manager user information and authentication functionality to set permissions much in the same way that the project libraries do. However, because shared variables reside inside a project library, there might be discrepancies between the permissions assigned to the project library and permissions assigned to the shared variable. In this situation, the most restrictive permission always is enforced.

To assign permissions for a shared variable, right-click the variable and select **Properties** from the shortcut menu. Then select **Security** from the **Category** list. Figure 4 shows the shared variable properties window providing the user read access and denying write access.



☑ Enable Security

User or group names

MyDomain\Guest

Permissions

Read	grant
Write	deny

☑ Grant ☐ Deny

Figure 4. Setting Permissions for a Shared Variable

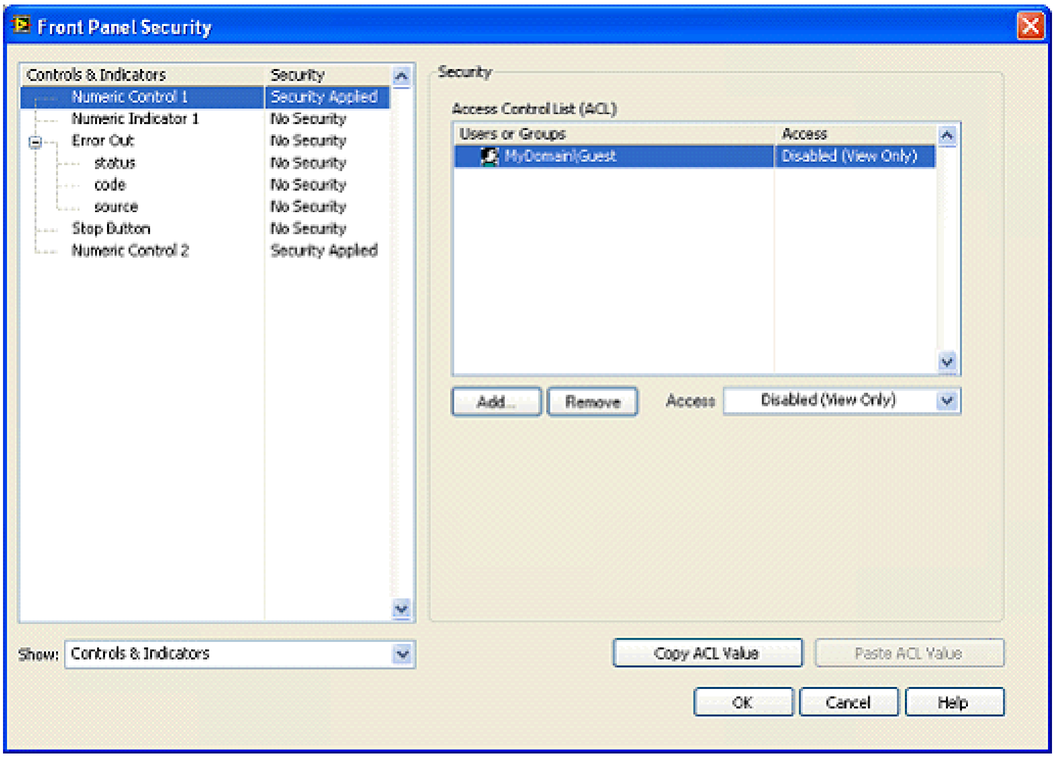
Front Panel Security

The LabVIEW DSC Module also uses the Domain Account Manager to assign permission levels to controls and indicators on the front panel. You can assign the following four permission levels to front panel objects.

- **Full Access** – The user has unrestricted access to the front panel object.
- **Disabled (View Only)** – The user only can view the front panel object.
- **Disabled & Grayed Out** – Similar to **Disabled (View Only)**, but the front panel object appears dimmed.
- **No Access (Hidden)** – The user cannot see the front panel object at all.

You can use the following two procedures to assign permissions to front panel objects.

- Right-click the object and select **Properties** from the shortcut menu to launch the **Properties** dialog box. Then click the **Security** tab. Use this tab to assign permissions to that object.
- Select **Tools»Security»Front Panel Security** to launch the **Front Panel Security** dialog box. This dialog box, shown in Figure 5, lists all the font panel objects. Use this dialog box to assign permissions to more than one front panel object at a time.



Controls & Indicators	Security
Numeric Control 1	Security Applied
Numeric Indicator 1	No Security
Error Out	No Security
status	No Security
code	No Security
source	No Security
Stop Button	No Security
Numeric Control 2	Security Applied

Users or Groups	Access
MyDomain\Guest	Disabled (View Only)

Access: Disabled (View Only)

Show: Controls & Indicators

Figure 5. Front Panel Security Dialog Box

Using the **Front Panel Security** dialog box to assign object permissions is different from changing the object state using the Properties menu. Using the properties of that object changes the security of the object based on the user that is logged in to the front panel. Conversely, using the **Front Panel Security** dialog box keeps the security at the same level no matter which user is logged in. Also, permissions set by front panel security override the state defined for a front panel object by its properties. Therefore, no matter what the state of the object is set to, its behavior will be controlled by front panel security.

Conclusion

The LabVIEW DSC Module provides a set of tools to facilitate the implementation of security for local or network resources such as LabVIEW project libraries, shared variables, and front panel objects. The security architecture of the DSC Module separates user management and authentication from resource permissions. User management and authentication is provided by the Domain Account Manager while the permissions assigned for users to access a resource are defined by the resource itself. The three resources that take advantage of the security functionality of the LabVIEW DSC Module assign permissions in different ways. Project libraries can be used as containers to assign permissions to multiple shared variables or other project libraries contained in that project library. Although shared variables inherit permissions from the project library where they reside, shared variables can assign individual permissions as well. Front panel objects can also assign permission levels based on the user or group.

References

1. http://www.ni.com
2. http://zone.ni.com/devzone/cda/tut/p/id/3322

WIRELESS SECURITY FOR DATA ACQUISITION

LTC lect. eng. Daniel SORA

The Regional Department of Defense Resources Management Studies - Brasov

Abstract

The flexibility of wireless remote monitoring systems can translate into large cost savings. Wireless monitoring systems require less installation and maintenance cost. The financial benefits of using wireless for remote monitoring are compelling; yet, industry has been slow to adopt the technology. Security, reliability, integration, and power are all challenges that must be overcome before there is widespread adoption of wireless measurement systems. NI Wi-Fi DAQ supports the highest commercially available security, IEEE 802.11i (commonly known as WPA2 Enterprise). This article provides an overview of the industry-standard security practices associated with IEEE 802.11i and steps for protecting data with NI Wi-Fi DAQ devices.

IEEE 802.11 Security Background

NI Wi-Fi data acquisition (DAQ) devices use IEEE 802.11 to stream continuous waveform data over a wireless network. Because IEEE 802.11 uses over-the-air RF signals as its physical transmission medium, it offers unique security challenges beyond those of a wired system. Previously, many companies have been reluctant to deploy wireless applications over fears of security breaches. Today, however, IEEE 802.11 network security is a viable solution for wireless data acquisition applications, having matured significantly in the IT space for more than 10 years.

A proper understanding of wireless security requires some background on the history of wireless networking and the lessons learned from early wireless deployments. Since the original IEEE 802.11 standard was introduced in 1997, the IEEE 802.11 task group has iterated on several security protocols, finally arriving at one (IEEE 802.11i) that is universally accepted by IT departments worldwide.

Wireless Security History

Fears over the security of wireless networks have their roots in the history of early networks. The original IEEE 802.11 standard introduced Wired Equivalent Privacy (WEP) as a means of protecting against unwanted wireless network access. In this type of network, each client computer has a password to an access point on the network. That password is used to gain access to the network and to encrypt all messages between the access point and the client.

Internet
Encrypted Traffic

Figure 1. Wireless security standards define how data is encrypted across a wireless network link.

Most home and small office networks use WEP because of its easy setup. However, WEP can be vulnerable to attack, especially if used improperly. WEP uses an RC4 cipher to encrypt data and a 40-bit key to encode and decode messages.

WEP Vulnerabilities

Attackers have found weaknesses in the WEP protocol and have developed methods for breaching a WEP network that is not properly protected:

Dictionary Attack – Many users leave their wireless access points and network interface cards at the factory default settings. Others choose a "weak" WEP key that can be found in a dictionary. Potential attackers can take advantage of these networks by "guessing" at security settings. Some may use a brute force method, but more sophisticated algorithms are also available. Dictionary attacks are easily prevented by choosing a strong password.

Man-in-the-Middle Attack – Most Wi-Fi network access points broadcast their service set identifiers (SSIDs) so that clients can easily find and connect to them. A rogue access point broadcasting the same SSID can trick a client into sending its security information, thereby giving an attacker access to the real network. A common best practice is to turn off SSID broadcasts from your router.

Replay Attack – A replay attack occurs when an attacker eavesdrops on wireless communication packets and records the transmitted data. The attacker then uses that data to replay messages with false or erroneous data to "trick" an access point into transmitting additional Address Resolution Protocol (ARP) packets. With enough packets (50,000 to 100,000), an attacker can decrypt the WEP key.

NI Wi-Fi DAQ supports WEP security. However, many wireless data acquisition applications require stronger security protocols.

NI Wi-Fi DAQ Network Security Components

NI Wi-Fi DAQ supports several wireless security protocols, including WEP, Wi-Fi Protected Access (WPA), and IEEE 802.11i (commonly known as WPA2 Enterprise). WPA offers better security than WEP by preventing replay attacks. WPA2 and WPA2 Enterprise offer the best wireless network security, providing both stronger data protection (encryption) and access control (authentication).

Encryption

For effective protection of wireless data transmissions, a Wi-Fi network must have a strong encryption algorithm (cipher) and some form of key management. Two encryption standards are widely used today with Wi-Fi networks: TKIP and AES.

The IEEE 802.11i task group introduced the Temporal Key Integrity Protocol (TKIP) with WPA as a stop gap for existing WEP networks. Access points and clients can upgrade from WEP to WPA/TKIP with a simple firmware or software change. One advantage of TKIP over WEP is that it uses a 128-bit key versus a 40-bit key, though the encryption algorithm (RC4) is still the same. The more significant difference is that TKIP uses a different key for every message packet, hence the name "temporal." This key is created dynamically by mixing a known pairwise transient key (PTK) with the MAC address of the client and a serial number for each packet. The PTK is created when a client connects to an access point using a preshared key (a passphrase that is known to all network members) and a random number generator. The serial number is incremented each time a new packet is sent. This means that replay attacks are impossible because the same key is never used from one packet to the next. An access point can detect when an attacker attempts to replay old packets.

As a final security solution, the IEEE 802.11i task group chose the Advanced Encryption Standard (AES) as the preferred encryption algorithm for Wi-Fi networks. Unlike TKIP, AES requires hardware upgrades for most older WEP installations because the cryptographic algorithm is more processor-intensive. AES uses a 128-bit cipher that is significantly more difficult to crack than the RC4 algorithm used by TKIP and WEP. In fact, the National Institute of Standards and Technology (NIST) chose AES as the encryption standard recommended for all U.S. government agencies. (FIPS publication 197 describes these requirements in detail.) Any wireless data acquisition application for the government or military likely has to use AES to transmit data.

Table 1 shows that even with massively parallel computing systems, it takes 10^{18} years to crack a 128-bit AES cipher.

Key Size (bits)	Number of Alternative Keys	Time required at 1 Decryption/µs	Time Required at 10^6 Decryptions/µs
32	$2^{32} = 4.3 \times 10^9$	35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	1,142 years	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{24} years	5.4×10^{18} years

Table 1. Time Required for Exhaustive Key Search or Brute Force Attack

Authentication

Authentication is the second key component of wireless security. Network authentication is essentially client access control. Before a client can communicate with a wireless access point, it must authenticate with the network. There are two basic forms of authentication: server-based and preshared key (PSK)-based.

Most enterprise networks have at least one authentication server, usually running a Remote Authentication Dial-In User Service (RADIUS). WPA2 Enterprise network security makes use of the IEEE 802.1X port-based authentication standard and consists of the following components:

Supplicant – the client wireless devices accessing the network

Authenticator – the wireless access point that controls what a supplicant can access

Authentication server – the server that provides an authentication service (usually RADIUS) to the authenticator

When a supplicant requests access to a network, the authenticator provides access to uncontrolled ports for authentication. The authenticator forwards the access request to the authentication server, which either accepts or denies access to the supplicant. The authenticator forwards the response from the authentication server to the supplicant and either grants access to controlled ports or continues to block a denied supplicant.

A successful authentication process results in a pairwise master key (PMK) used to encrypt wireless traffic. The details of this exchange depend on which Extensible Authentication Protocol (EAP) method the network supports. The following are the most common EAP methods (all supported by NI Wi-Fi DAQ devices):

LEAP (Lightweight EAP) – an older, propriety EAP method developed by Cisco Systems. There is no native support for LEAP in any Microsoft Windows operating system, though most wireless network interface card (NIC) software supports it.

EAP-TLS (EAP-Transport Layer Security) – an open standard supported by most wireless vendors. EAP-TLS requires both server- and client-side certificates, which can make installations more difficult.

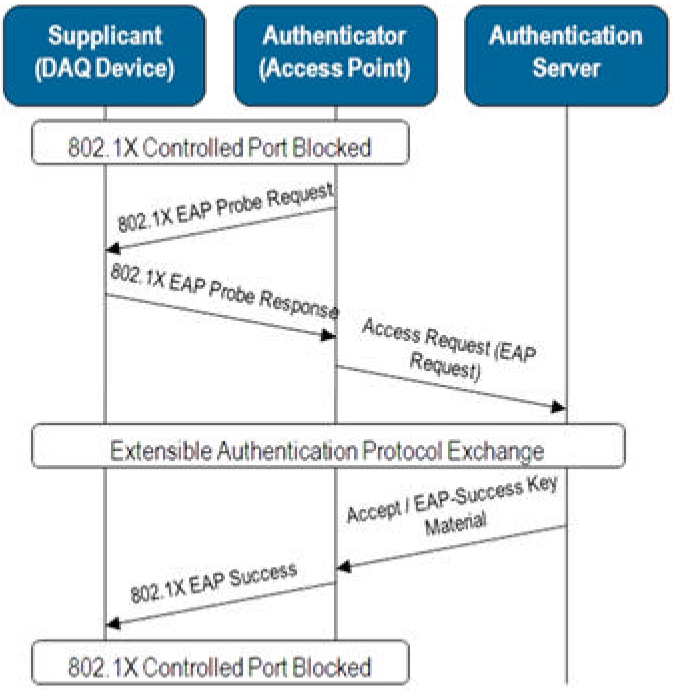

Supplicant (DAQ Device)
Authenticator (Access Point)
Authentication Server
802.1X Controlled Port Blocked
802.1X EAP Probe Request
802.1X EAP Probe Response
Access Request (EAP Request)
Extensible Authentication Protocol Exchange
Accept / EAP-Success Key Material
802.1X EAP Success
802.1X Controlled Port Blocked

Figure 2. The IEEE 802.1X authentication process involves a layered exchange between the supplicant, authenticator, and authentication server.

EAP-TTLS (EAP-Tunneled Transport Layer Security) – a protocol that removes the client-side certificate requirement from the EAP-TLS method for a more scalable network.

PEAP (Protected EAP) – an open standard developed by Cisco Systems, Microsoft, and RSA security. This is a popular EAP method that requires only server-side certificates. PEAPv0/MS-CHAPv2 is the most common variant of this method.

All the EAP methods listed above support mutual authentication, which prevents man-in-the-middle attacks because the client has to authenticate the server and vice versa. A rogue wireless access point cannot fake the server-side security certificate.

Not all networks have an authentication server, which makes the previous authentication methods impossible. Small office or home office (SOHO) networks can use a PSK instead between the client (wireless data acquisition device) and access point. This is essentially a passphrase that the user provides to initiate authentication with the network.

Implementing a Secure Network with NI Wi-Fi Data Acquisition

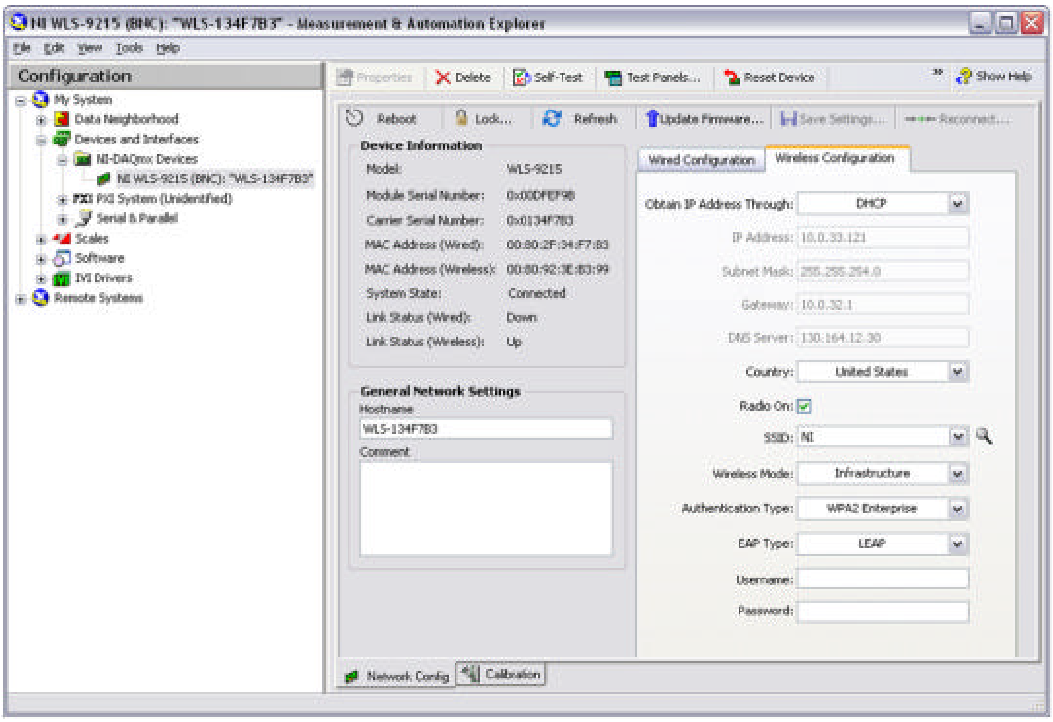
NI Wi-Fi DAQ devices support the full IEEE 802.11i security standard, including AES encryption and IEEE 802.1X authentication. This is the highest commercially available wireless network security, meaning your sensitive data is protected from unwanted access.

Figure 3. NI Wi-Fi DAQ streams continuous waveform data over a secure IEEE 802.11 network.

If you are connecting to an enterprise network, you should work with your IT group to determine which security protocols and EAP methods your server(s) accept. Because NI Wi-Fi DAQ devices support the most common IEEE 802.1X EAP methods (LEAP, PEAP, EAP-TLS, and EAP-TTLS), you are free to choose which works best for your application and network infrastructure.

Security settings for NI Wi-Fi DAQ devices are easy to use. In Measurement & Automation Explorer (MAX), select your NI Wi-Fi DAQ device under "NI-DAQmx Devices" and click on the "Network" tab at the bottom of the screen. Select the "Wireless" tab to configure your network security options with a series of drop-down menus.

If your EAP method requires a client-side certificate, be sure to obtain it before attempting to set up your data acquisition device. And if you are setting up your own network without an authentication server, be sure to use a strong PSK passphrase (with both WPA and WPA2 networks).



Device Information

Model: WLS-9215
Module Serial Number: 0x00DFEF98
Carrier Serial Number: 0x0134F7B3
MAC Address (Wired): 00:80:2F:34:F7:B3
MAC Address (Wireless): 00:80:92:3E:83:99
System State: Connected
Link Status (Wired): Down
Link Status (Wireless): Up

General Network Settings

Hostname: WLS-134F7B3
Comment:

Obtain IP Address Through: DHCP
IP Address: 10.0.33.121
Subnet Mask: 255.255.254.0
Gateway: 10.0.32.1
DNS Server: 130.164.12.30
Country: United States
Radio On: ☑
SSID: NI
Wireless Mode: Infrastructure
Authentication Type: WPA2 Enterprise
EAP Type: LEAP
Username:
Password:

Figure 4. Configure your NI Wi-Fi DAQ encryption and authentication settings using MAX.

MAX uses an encrypted, write-only process based on transport layer security (TLS) to send all this configuration and setup data, including usernames, passwords, and client-side certificates, to a wireless data acquisition device, which further protects your network.

Summary

NI Wi-Fi DAQ devices implement the highest commercially available wireless network security standard, IEEE 802.11i (WPA2 Enterprise), including network authentication and data encryption. Authentication ensures that only authorized devices have network access, and encryption prevents data packets from being intercepted. IEEE 802.11 security standards build on more than 10 years of use in the IT sector, and are widely adopted worldwide. By using standard security protocols, NI Wi-Fi DAQ devices make it easy to add wireless measurements to your IT networks safely.

References

1. http://www.ni.com
2. http://zone.ni.com/devzone/cda/tut/p/id/7376

CYBER TERORISM

CAPT. Codrut TINTA

UM 01021 Targu Mures

Abstract

Vandalizing websites, disrupting services, sabotaging data and systems, launching computer viruses, harassing individuals and companies, and fraudulent transactions. These are just a few examples of what cyber terrorists can do. All that is needed is a computer and a connection to the internet. Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Overview

As the Internet becomes more pervasive in all areas of human endeavor, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups (i.e. with embership based on ethnicity or belief), communities and entire countries, without the inherent threat of capture, injury, or death to the attacker that being physically present would bring.

As the Internet continues to expand, and computer systems continue to be assigned more responsibility while becoming more and more complex and interdependent, sabotage or terrorism via cyberspace may become a more serious threat.

Cyberterrorism can also be defined much more generally, for example, as “The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives.”

It is the use of computers to intimidate or destroy a population; armed with nothing more deadly than a hard drive and a keyboard, terrorists may be able to take control of the stock market, alter government security codes — even hacking into a hospital computer system and changing someone's medicine prescription to a lethal dosage as an act of revenge. And what makes cyber terrorism so attractive to groups like al-Qaeda is the fact that the Internet has no boundaries. There are not any icy, mountainous borders to cross, no paperwork to present to suspicious customs officers. Instead, terrorists can use cyber space to access extremely sensitive information and spread their doctrine further than ever.

1. The new terrorism

The job of a terrorist is to spread terror. How does one spread terror through the Internet?

The goal of cyber terrorism is not necessarily to spread terror as much as it is to spread fear and uncertainty by causing people to lose faith in the government's ability to protect and serve them or, for example, significantly hinder the financial industry's ability to function properly and protect private assets. One of the problems with the post-9/11 security environment is that the tremendous loss of human life on that day has caused us to a certain extent to ignore the political and economic warfare aspects of international terrorismNew terrorist organizations are highly funded, technologically articulate groups capable of inflicting devastating damage to a wide range of targets. While most published work in the computer industry has focused on the impact of the computer as target (pure cyberterrorism) it is our belief that the real danger posed by the synthesis of computers and terrorism is not only the insertion of computer as target in the terrorism matrix, but in many of the other areas, too.

The current narrowness of focus poses a significant risk to US infrastructure. By being too concerned about one particular part of the matrix, we are apt to let our guard down in areas which may be more critical. A forward-looking approach to terrorism that involves computers is highly contextual in its basis. Traditional antiterrorism defenses must be deployed, but these countermeasures must fully take into account many of the virtual factors that we have outlined in this paper.

If the events of September 11th teach us one thing, it is that we should always consider the ‘big picture’ of the overall terrorist threat, rather than view one aspect in isolation. The ‘cyber’ aspects of the puzzle must be woven throughout the picture, not simply confined to one cell. To view a problem with too narrow a perspective is to invite anarchy into our lives.

Most Attacked Countries Since September 2002	
USA	71,868
Germany	17,529
Brazil	14,785
UK	13,417

1.1. Computers — the weapons of the cyberterrorist

Following on from the discussions above, it becomes obvious that the most likely ‘weapon’ of the cyberterrorist is the computer. Thus, one might ask, are we arguing that one should restrict access to computers, just as access to explosives is restricted? Not quite, but close. I believe that the stockpile of connected computers needs to be protected. There are many laws that define how one should protect a firearm from illegal/dangerous use. The mandatory use of trigger locks, though controversial, has been put forward to prevent danger should the gun end up in the wrong hands.

Similarly, powerful explosives like C4 are not simply sold over the counter at the corner store.

Explosives and guns are certainly not entirely analogous to computers. A better analogy might stem from the concept of an ‘attractive nuisance’. For example, a homeowner shares some responsibility for injury caused by a pool on his property — it is deemed an attractive nuisance, and as such, the innocent should be prevented from simply being attracted and harmed.

1.2. Current threats

The Internet has brought considerable change to economic transactions, social interactions and military operations. Although it provides huge benefits, it has also significant personal, organizational, and infrastructural dependencies that are not confined by national borders. However, physical borders complicate international efforts to secure networks. Governments are limited by the multitude of physical borders because they are more constrained and face higher costs in regards to pursuing cyber attackers outside their jurisdictions.

Most sovereign states view the intrusion of another state into their territory as an illicit or outrageous act. A resident of one country does not need to obey the laws or police of another. In this situation, the Internet and cyber space are no diferent than any other national activity. Cooperation in cyber security becomes crucial because there are no national solutions to transnational problems. National governments will need to take the lead in building cooperative relationships.

Our public and private organizations continue to grow dependent on common systems, networks, and commercial off-the-shelf (COTS) hardware and software. This situation makes it very difficult to draw lines of accountability and responsibility for the increasing tactical and strategic vulnerabilities.

Globalization and the explotion of information have empowered nation-states, opposition groups, ideological radicals, terrorist organizations, and individuals. In addition, small interest groups or non-governmental organizations (NGOs) can meet and plan online to disrupt or derail policies and negotiations. Ownership and responsbility for maintenance and protection of national infrastructure are more widely diversified. Lines of defense and accountability lie in the hands of individuals and smaller organizations.

National security goes beyond economic infrastructure, military and political domains. It has come to include human security, personal privacy, financial security, healthcare concerns, systemic educational concerns, and social ethics. A large percentage of military traffic moves over civilian telecommunications and computer systems. Security exists not only in the physical world but in cyber space.

Threats that Emerge From the New Environment

There are four threats that emerge from the new environment: the threat of disruption, the threat of exploitation, the threat of manipulation, and the threat of destruction.

The Threat of Disruption

The effect of disruption in communication flow, economic transactions, public information campaigns, electric power grids, and political negotiations will be felt in economic terms, and therefore will be of greatest concern to private sector entities. The disruption of military communication in times of conflict presents the potential for loss of life or aborted offensive missions. The probability of this type of threat materializing is considerable, as the tools required to create disruptive viruses and denial-of-service attacks are simple and all-encompassing.

The Threat of Exploitation

The threat of exploitation affects sensitive, proprietary, or classified information. Information theft, fraud, and cyber crime can have extremely serious effects, at personal levels (e.g., identity theft), institutional levels (e.g., online credit card fraud or theft of thousands of credit card numbers), and national security levels (e.g., systematic probing of classified or unclassified but sensitive government systems). This threat is made all the more menacing by the difficulty in detecting these types of intrusions and compromised systems. As with the threat of disruption, the probability of occurrence is high.

The Threat of Manipulation

The threat of manipulation of information takes places for political, economic, military, or inflammatory purposes. Several incidents of defaced Web sites in the former Yugoslavia and the Middle East, and of altered personal financial information on e-commerce sites, point to the clear potential for using the Internet as a powerful tool for manipulating information. While many instances of manipulation simply serve the cause of making a statement, and can be remedied rapidly, the more dangerous instances are those that go undetected: manipulation of financial data, military information, or functional infrastructure data (e.g., the timing of dam releases).

The Threat of Destruction

The threat of destruction of information or, potentially, of critical infrastructure components can have harmful economic and national security consequences. Destruction of information, like disruption, can be carried out through relatively simple hacker techniques. Examples of such viruses and Trojan Horses are well-documented.

1.3. Trends in cyber attacks

Cyber attacks designed to disrupt major web networks present a serious weakness in security. It exposes how vulnerabilities on the Internet can create risks for all. Cyber attacks demonstrate the need for all nations to work together to develop strategies to strengthen cyber security. Cyber attacks affect millions of Internet users and result in revenue losses. While this damage is relatively minimal in proportion to the traffic volume of the Internet, cyber attacks are a wake-up call as to the extent of cyber crime, and the degree to which we are all vulnerable.

The overall sophistication of cyber attacks has been steadily increasing. There are several types of cyber vulnerabilities and attacks: worms, distributed denial of service (DDoS), unauthorized instrusions, Web defacements and semantic attacks, Domain Name Service (DNS) attacks, and routing vulnerabilities.

Worms

Worms and viruses are malicious, autonomous computer programs. Most modern viruses are in fact worms. The worm epidemic is enabled by buffer overflows in which more data is put into the buffer (computer data holding area) than the buffer has allocated. This results in a mistmatch between the producing and consuming processes. Therefore, resulting in system crashes or the creation of back doors leading to unauthorized access. Examples of worms include Code Red, Code Red II and Nimda.

A computer virus dubbed the "Love Bug" forced email servers to shut down in Europe and the US. The new virus originates in an email entitled "I love you." Once the attachment is launched, the virus sends copies of the same email to everybody listed in the user's address book. The Melissa virus operated similarly, infecting about a million computers, clogging whole networks in the Western Hemisphere, and causing $80 million in damage. Anti-virus firm Symantec released an update to its software to combat the virus, but warned computer users not to open any "I love you" messages. The email said the company had reports from over 20 countries. The “Love Bug” epidemic exceeded Melissa in both speed and destructiveness. The virus originated in the Philippines and has been nicknamed the "Killer from Manila". The culript, Onel de Guzman, was found but could not be prosecuted because the Philippines did not have laws against cyber crime. This incident prompted the Philippines to change its laws. Most prolific worms are suspected of being created in response to political events. If maximum destruction is a hostile adversary’s goal, worms are a cost effective way to disrupt information infrastructures.

On the morning of September 18, 2001, only seven days after 9/11, the world woke up to the Nimda Internet worm. This malicious code destroyed data and had the ability to self-replicate and find its way through the Internet to other vulnerable computers. Nimda, which contained five different malicious payloads, infected all 32-bit Windows systems it encountered, including Windows 98, 2000, Millennium Edition, XP and NT. It scanned systems for as many as 100 different vulnerabilities and automatically exploited them when found. Within 30 minutes of being discovered, Nimda had become a global problem.

Distributed Denial of Service (DDoS) Attacks

DDoS attacks employ armies of unsecure servers compromised by a hacker who places software on it. When triggered, an overwhelming number of requests towards an attacked web site will be launched, generally in coordination with other unsecure servers.

On February 2000, some of the Internet's most reliable sites were rendered nearly unreachable by DDoS attacks. Yahoo took the first hit on February 7, 2000. In the next few days, Buy.com, eBay, CNN, Amazon.com, ZDNet.com, E*Trade, and Excite were taken down by DDoS attacks. Though damage estimates vary widely, the FBI estimates that the companies suffered $1.7 billion in lost business and other damages.

In a denial-of-service attack, the target system is rendered inoperable. Some attacks aim to crash the system while other DDoS attacks make the targeted system so busy that it cannot handle its normal workload. The attacks on Yahoo and the other companies were DDoS attacks, where one attacker can control tens or even hundreds of servers. After installing the DDoS script on several computers, a coordinated attack can be orchestrated from a remote location.

On April 18, 2000, a juvenile in Canada, known online as "MafiaBoy," was arrested and charged in connection with the February DDoS attacks. Prosecutors alleged he broke into several computers, mostly at US universities, and used them to launch the attack against the web sites. MafiaBoy gained illegal access to 75 computers in 52 different networks and planted a DDoS tool on them which he then activated and used to attack 11 Internet sites by sending up to 10,700 phony information requests in 10 seconds.

According to police, “MafiaBoy” boasted in Internet chat rooms about the attacks and was tracked through traces he left of his computer activity. On January 18, 2001, the 16-year-old computer hacker pled guilty to 56 charges, including mischief and illegal use of a computer service.

DDoS attacks on high value political and economic targets are also likely to increase during the war on terrorism since defending against these attacks is a formidable task. DDoS could be very harmful during periods of crises. Potential targets are mail servers, government web sites, e-commerce sites, and communications.

Unauthorized Intrusions

These intrusions are of great concern to businesses and government. The theft of money, credit card numbers, proprietary information, or sensitive government information can have devastating consequences. In 2001, a series of actions originating in Russia, collectively known as Moonlight Maze, intruded into US government systems over a period of several years. The first attacks were detected in March 1998 and hundreds of unclassified networks in the Pentagon, Department of Energy, National Aeronautic and Space Administration (NASA) and other defense contractors were compromised. Cyber attackers can employ sophisticated attack tools and techniques to disrupt or compromise critical infrastructure systems in response to a US and allied military strike during the war on terrorism.

Web Defacements and Semantic Attacks

Politically motivated web defacements will likely continue to escalate as the war on terrorism is fought. Minor intrusions result in defacements and anti-Western or pro-terrorist propaganda. Major attacks involve changing the content of a web page thus disseminating false information. Potential targets include government and military sites as well as high volume sites such as search engines, e-commerce sites, and news services.

In late April and early May 2001 pro-Chinese hacktivists and cyber protesters began a cyber assault on US web sites. This resulted from an incident in early April where a Chinese fighter jet was lost at sea after colliding with a US naval reconnaissance airplane. It also coincided with the two-year anniversary of the Chinese embassy bombing by the US in Belgrade and the traditionally celebrated May Day and Youth Day in China. Led by the Honkers Union of China (HUC), pro-Chinese hackers defaced or crashed over 100 seemingly random web sites, mainly .gov, .org and .com. Although some of the tools used were sophisticated, they were readily available to both sides on the Internet.

This year, hackers based in Brazil attacked a series of online banking Web sites, leaving behind written criticisms about each bank's faulty security precautions. Although the banks suffering the attacks are not among the first tier in Internet banking, the hacking comes at a bad time for the rising online personal financial services industry in Latin America. It also suggests that smaller banks struggling to make their own way onto the Internet may have to alter their course.

Domain Name Service (DNS) Attacks

Computers connected to the Internet use numerical Internet Protocol (IP) addresses to communicate with one another. Domain Name Service (DNS) are the information pages that computers consult in order to obtain the mapping between the name of a system (or website) and the IP address of that system. If the DNS server provides an incorrect IP address for a website, the user would connect to the incorrect server. The result will be that the user thinks he is connected to the correct server when in reality he is connected to the attacker’s server. An attacker can disseminate false information or deprive the original web site of its righteous traffic. The system of DNS is hierarchical. Therefore, the cascading effect on remote servers would result in traffic to selected sites to be redirected or lost. The potential for an attack on the root DNS servers increases during the war on terrorism.

Routing Vulnerabilities

Routers are the air traffic controllers of the Internet. They ensure that the information, in the form of packets, gets from the source to the destination. Although routing operations have not been the main cause of deliberate disruption, the lack of diversity in router operating systems leaves open the possibility of a massive routing attack. Currently, most sold routers are Cisco routers. If an attacker can find a common vulnerability in the Cisco hardware, an attack on routing operations would bring the Internet to a halt. It is very important for Internet backbone operators to follow standards or regulation for maintaining security on routers.

2. Cyberterrorists

We can clearly see that the infrastructure is weak and can be manipulated by various mean…but what of the people who have the ability to do this…is there motive. This is why Cyber Terrorism is so dangerous, most hackers do posses the knowledge, but lack the motivation to create such violence and severe disruption. However many terrorist pride themselves on his ability.

Despite the many actions of the few, there are few indications that this is going to become a widespread tactic of terrorists.

2.1. Sources of attacks

Potential cyber attackers are grouped in four categories: terrorist groups, targeted nation-states, anti-capitalism/anti-globalizations movements and terrorist sympathizers, and thrill seekers.

Terrorist Groups

Today’s terrorists, characterized by religious and social motivations, stand at the threshold of netwar. Terrorists are known to have used information technology and the Internet to communicate securely, formulate plans, spread propaganda, and raise funds. Trends seem to point to the possibility of terrorists using information technology as a weapon against critical infrastructure targets.

Targeted Nation-States

Many nations have identified the utility of developing cyber attack techniques for purposes of engaging in covert espionage against governments and industries as well as employing information warfare. Among the nations developing cyber warfare capabilities are Lybia, China, North Korea, Cuba and Russia.

Anti-Capitalism/Anti-Globalization Movements and Terrorist Sympathizers

Anti-capitalism and anti-globalization movements have employed violent tactics in recent years to demonstrate their opposition to the values that define the global status quo. These extremists and some moderate supporters could become involved in a cyber campaign against the Western nations.

Thrill Seekers

This category of attackers may not be motivated by political or ideological reasons but simply by the desire to brag about their exploits. The likelihood of attacks from thrill seekers is high because of the intense media coverage.

2.2. Infrastructure attacks

The possibility of unexpected and massive attacks on critical infrastructures that disable telecommunications, electrical power systems, government services, and emergency services has been raised in numerous security reports. Information systems associated with critical infrastructures should be considered likely targets for terrorists, nation-states, and hackers in the age of asymmetrical warfare. Some examples:

- Banking and financial institutions utilize infrastructures that are vulnerable to cyber attacks due to their dependence on networks. However, this sector still operates largely private networks and intranets with very limited external access, thus affording it some protection from external cyber attacks.
- Voice communication systems are vulnerable to proprietary software attacks from insiders familiar with the technical details of the system. This includes 911 and emergency services telephone exchanges.
- Electrical infrastructures have sensors that assist engineers in shutting down components of the electrical grids in times of natural disaster, which could become vulnerable to cyber manipulation, potentially resulting in power outages.
- Water resources and the management of water levels are often controlled by sensors and remote means. Physical security, in addition to heightened cyber security awareness, must be followed during the impending conflict.
- Oil and gas infrastructures widely rely on the use of computerized Supervisory Control and Data Acquisition (SCADA) and Energy Management Systems (EMS). These systems could be vulnerable to cyber attack with the potential of affecting numerous economic sectors, such as manufacturing and transportation.

Malicious insiders are the greatest threat to critical national infrastructures. Insiders armed with specialized knowledge of systems and privileged access are capable of doing great harm. The tragedy of 9/11 illustrates that terrorists live and operate within their targeted countries, obtaining specialized skills with deadly intentions.

Any one of the scenarios discussed here could have serious consequences. However, a multi-faceted attack employing some or all of the attack scenarios in compound fashion could be devastating if nations are unprepared. A compound cyber attack by terrorists or nation-states could have disastrous effects on infrastructure systems, potentially resulting in human casualties. Such an attack could also be coordinated to coincide with physical terrorist attacks, in order to maximize the impact of both.

2.3. Effects and costs of cyber crime

Cyberterrorism can have a serious large-scale influence on significant numbers of people. It can weaken countries economy greatly, thereby stripping it of its resources and making it more vulnerable to military attack.

Cyberterror can also affect internet-based businesses. Like brick and mortar retailers and service providers, most websites that produce income (whether by advertising, monetary exchange for goods or paid services) could stand to lose money in the event of downtime created by cyber criminals.

As internet-businesses have increasing economic importance to countries, what is normally cybercrime becomes more political and therefore "terror" related.

Costs

Attacks are becoming more destructive, widespread and more difficult to contain. Post 9/11, there seems to be a greater appreciation for how much information security means not only to each individual enterprise but also to the economy itself and to society as a whole.

- $17 billion dollars will be spent worldwide on security products and services
- $200 - $300 is spent by US companies for every host that needs patching
- $221.2 billion dollars will be lost worldwide due to identity theft by year-end 2003 (up from $73.8 billion in 2002) with $73.8 billion (up from $24.6 billion) of those losses in the US
- By 2005 financially or politically motivated attacks will represent 30% of total security-breach incidents and 60% of related costs incurred by US enterprises

3. Counter and anti cyberterrorism

3.1. Defending against the new terrorism

Defending against terrorism where a computer or the Internet plays an important part in the terrorism matrix is very similar to defending against terrorism that does not. The regular practices (deterrence, law, defense, negotiations, diplomacy, etc.) are still effective, except that the scope of certain elements is expanded. For example, traditional strikes against military bases, targeting of key leaders, and collective punishment have been effective in traditional terrorism (Whitelaw, 1998) and certainly have potential for dealing with some aspects of cyberterrorism. These techniques are often presented, and can be to be updated to include their ‘virtual’ counterparts. It should be noted, however, that differences in international law and culture could make this process a complex task.

Crenshaw (Crenshaw, 1999) presented here at length, examines a summary of traditional counterterrorist techniques:

Deterrence

Governments can use their coercive capacity to make terrorism too costly for those who seek to use it. They can do this by military strikes against terrorist bases, assassinations of key leaders, collective punishment, or other methods. There are several drawbacks to this approach, however. On the one hand, it can lead to unacceptable human rights violations. In addition, groups may not come to government attention until movements are so well developed that efforts to contain them through deterrent methods are insufficient.

Criminal justice

Governments can treat terrorism primarily as a crime and therefore pursue the extradition, prosecution, and incarceration of suspects. One drawback to this approach is that the prosecution of terrorists in a court of law can compromise government efforts to gather intelligence on terrorist organizations. In addition, criminal justice efforts (like deterrent efforts) are deployed mostly after terrorists have struck, meaning that significant damage and loss of life may have already occurred.

Governments can make targets harder to attack, and they can use intelligence capabilities to gain advance knowledge of when attacks may take place. As targets are hardened, however, some terrorist groups may shift their sights to softer targets. An example is the targeting of US embassies in Kenya and Tanzania in August 1998 by truck bombs. Although the attacks are believed to have been coordinated by individuals with Middle Eastern ties, targets in Africa were chosen because of their relatively lax security compared with targets in the Middle East.

Negotiations

Governments can elect to enter into negotiations with terrorist groups and make concessions in exchange for the groups' renunciation of violence. While governments are often reluctant to do so at the beginning of terror campaigns, negotiations may be the only way to resolve some long-standing disputes.

For example, data gathering and monitoring operations of terrorist communications has typically applied to signal intelligence and fieldwork. In a virtual environment, the ability to gather information from various sources is eminently achievable in a somewhat automated manner. Specific groups can be watched easily, and computers are comparatively simple to 'bug'. All contacts that a particular user interacts with could then be tracked, and the network of communication mapped. Furthermore, much of this surveillance can be carried out over the very same network that the terrorists intend to use to facilitate their plot.

This extension, however, must be carried out with care. Consider, for example, the original US export regulations on the export of 'strong encryption' (ITAR). Under such regulations, certain encryption products were classified as munitions. While ITAR has since been replaced, the revamped 'Export Administration Regulations' (DOC, 2002), while somewhat more relaxed, continue to blacklist several countries from receiving encryption products, despite the fact that strong encryption technology is freely available via the Internet. While this law seems to be aimed at preventing the use of strong encryption by other potentially hostile governments and terrorist entities, strong encryption algorithms and implementations remain trivially available to pretty much anyone.

This classification of knowledge as munitions seems to be the ultimate (and flawed) extension of traditional anti-terrorist tactics into the virtual realm. Clearly, it is not sufficient to quickly draw analogies that are not, in fact, correct. A far better approach is to carefully consider the impact of the computer in the different cells of the terrorism matrix. For example, banning the export of encryption from just America is akin to banning the sale of C4 only on weekdays — the asset would be hardly even an inconvenience to the would be terrorist. A far better solution is to consider the safeguard in the context of the virtual world. When examined in this aspect, for example, it is reasonably clear that the original classification of encryption products as munitions is not likely to be effective. Similarly, while the use of export grade encryption can (and has) resulted in the ability of officials to read some terrorist communiqués, a restrictive "export to here, not here" ban is unlikely to succeed in any meaningful way.

A forward-looking approach to terrorism that involves computers is therefore highly contextual in its basis. Traditional antiterrorism defenses must be deployed, but these countermeasures must fully take into account the virtual factors that we have outlined in this paper.

3.2. Future research

Certainly there are many unanswered questions. Most people, governments included, consider cyberterrorism primarily as the premeditated, politically motivated attack against information, computer systems, computer programs, and data by sub national groups or clandestine agents.

However, as we have seen, the real impact of the computer on the terrorism matrix is considerably wider. By limiting our understanding of cyberterrorism to the traditional 'computer as target' viewpoint, we leave our nation open to attacks that rely on the computer for other aspects of the operation.

Conclusion

"A computer keyboard can be a very useful tool for the progress of humanity, but it can also become a dangerous weapon capable of producing enormous economic damages to the infrastructure of a state or company, and even against the integrity and the life of human beings" – Cesar Gaviria Secretary General of The Organization of American States

The Internet was developed primarily as an unregulated, open architecture. Not only are we observing a predictable backlash to the 'corporatization' of the network, where the tools of destruction can easily be placed in the hands of the dissatisfied or malevolent people, we must also deal with the fact that the infrastructure is ideally suited to criminal activities. Some of these activities are being promoted as cyberterrorism; however, the loose use of the term is actually undermining the defense capabilities of the very corporations and governments who are at risk.

Events can be analyzed in terms of their critical factors, and only if these factors all exist can the event legitimately be called terrorism. However, that does not mean if all these factors do not exist that a corporation is 'safe'. Unfortunately, corporations are built around the premise that people will do the right thing. The fact, as we have seen, is that this is not necessarily the case.

This brings us to the final point of this study: turning the tables on terrorism. As we have shown, computers can play an enormous role in terrorism. At the same time they can provide perhaps our biggest defense against terrorism if used to our advantage. However, just like as we need to understand the integration of computers with terrorism, we must examine how computers can assist in defense broadly.

This begins with the re-examination of basic beliefs about 'cyberterrorism' which must take place within academia, industry, government and defense sectors. This re-examination is, however, only the first step in combating terrorism.

Information at each level of analysis must be shared, collated and redistributed across federal, state and local government boundaries, as well as amongst industry and academia, and in some cases, the private citizenry.

Aside from the role of computers in defense, we must attempt to re-educate policy makers, defusing the latent danger of vertical 'cyberterrorism' defenses and replacing them with a well-rounded, integrated approach to a problem that is extremely broad. From a corporate and governmental perspective this requires a careful examination of the 'messaging' that is broadcast. How do we portray the fusion of computers with terrorism? Can the messaging be made more productive so that we can shape the mindset of our audience to one that is synergistic with a broad view of cyberterrorism?

Finally, it is impossible to neglect to mention the fact that the rapid increase in connectivity and the ultimate frailty of our national IT infrastructure coupled with the astonishing homogeneity of our computing base is a matter of grave concern. Continued focus must be put on increasing the public demand for computer security as well as the corporate awareness of the issue: whereas security flaws in widely used applications were once perceived as personal risks, we must begin to recognize the potentially global consequences of such issues in balance with the more general problems posed by the integration of computing with terrorism.

The lack of understanding of cyberterrorism, and the overall insecurity of America's networks have allowed a situation to develop which is not in the best interests of the country or computer users. The need to protect computing resources, making the job of a cyberterrorist more difficult is obvious.

Only by combining the strengths of both the private and public sectors on issues such as early warning detection and information dispersal, promotion of best practices, agreement over sound information security policies will we be able to turn the tide on the cyber security threat facing our world.

However, this can only be accomplished by re-examining commonly held beliefs about the very nature of computer systems and of cyberterrorism itself.

In conclusion at the present cyber terrorism to the extreme is not as much of a burden, however general cyber crime is very much a part of today's cyberspace; and cyber terrorism is very likely to be a few years in the future but nevertheless coming.

References

- Cyber Terrorism Post 9/11 In The Western Hemisphere - Lieutenant Colonel Wanda I. Cortes Inter American Defense College-2004
- Verton, Dan, Black Ice: The Invisible Threat of Cyber Terrorism, 2003
- Spencer, Vikky, Cyber Terrorism: Mass Destruction or Mass Disruption?, Februrary 2002, Computer Crime Research Center, http://www.crime-research.org/eng/library/mi2g.htm
- "What is Hacktivism?" – http://thehacktivist.com/hacktivism.php
- "Cyberterrorism" – http://en.wikipedia.org/wiki/Cyberterrorism
- Cyber Terrorism By Kevin Coleman, Technolytics October 10, 2003 – http://www.directionsmag.com/article.php?article_id=432
- Serge Krasavin Ph.D. MBAv "What is Cyber-terrorism?" http://www.crime-research.org/library/Cyber-terrorism.htm
- Dr. Ian Brown "Cyberterrorism" – http://www.slideshare.net/blogzilla/cyberterrorism

SECURITY ASPECTS OF NETWORK-CENTRIC ENVIRONMENT

MAJ. Adrian CROITORU

UM 02499 Bucuresti

Introduction

Military transformation and the Revolution in Military Affairs is not as forthright a process as it was perceived only several years ago. The globalization and the boom of information, computing, networking, satellite and precision technologies all have tremendous implications for the defense and security sector. The extensive use of modern technologies in the offensive campaigns in Kosovo, Afghanistan and Iraq enabled the military to achieve an unprecedented operational tempo and precision, and to win wars in the course of several weeks, instead of years, as was the case in the not too distant past. The high-tech side of military transformation proved to be enormously promising, prompting a number of states to assign a significant part of their military budget to programs such as Network Centric Warfare (NCW).

The network centric approach to warfare is the military embodiment of information age concepts. Studies have shown that networking enables forces to undertake a different range of missions than non-networked forces, by improving both efficiency and effectiveness of operations.

Network Centric Warfare applies the vast potential of the Information Age to warfare, envisioning a networked battle force executing high-speed, synchronized operations with precise effect.

Battlefield operations in the foreseeable future will depend heavily on network-centric computing systems that link a diverse multitude of geographically dispersed resources, operating on widely varied platforms, into a cohesive fighting force. The warfighter at all levels will depend on these unified systems to conduct successful multi-force operations in the 4-dimensional battle space. Such complex and widely dispersed operations expose network-based systems to unprecedented levels of reliability and security risks.

While USA uses the term Network Centric Warfare or Operation (NCW/NCO), NATO uses the British term of Network Enabled Capability (NEC). However, any of the two mentioned term used, it refers the use of a communication network to fight a war.

1. Network centric warfare – what is it?

1.1 History

"The concept of network-centric warfare (NCW) emerged in 1997 and has become the Navy's central concept for organizing its efforts to change and transform itself for 21st Century military operations. NCW focuses on using advanced information technology (IT) – computers, high-speed data links, and networking software – to link together Navy ships, aircraft, and shore installations into highly integrated computer/telecommunications networks".[1]

The term network-centric warfare broadly describes the combination of emerging tactics, techniques and procedures that a networked force can employ to create a decisive warfighting advantage. According to John Keegan, author of A History of Warfare, it is similar to the significant warfighting developments of the industrial age and agrarian age in that network-centric warfare seeks to exploit an order of magnitude change in an underlying source of power to increase warfighting advantage dramatically. In the industrial age, power was primarily derived from mass and the sources of power for moving mass. In the information age, power is increasingly derived from information sharing, information access and speed.

In their book, Network Centric Warfare, Alberts et al, describe NCW as “an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision-makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.

In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battle space”.[2]

NCW relies on computer processing power and networked communications technology to provide a shared awareness of the battle space for military forces. Proponents say that a shared awareness increases synergy for command and control, resulting in superior decision-making, and the ability to coordinate complex military operations over long distances for an overwhelming war-fighting advantage.

1.2 Definition of Network Centric Warfare

Net-centricity, the military expression of the Information Age, is a relatively new concept, coined and introduced by US Navy Vice Admiral Arthur K. Cebrowski and John J. Garstka, Assistant Director of the US Office of Force Transformation, in their article "Network-Centric Warfare: Its Origins and Future" in 1998. Net-centricity is not merely about sharing information between different branches of the armed forces using modern technology. The virtue of network-centricity is that it creates an added value by providing all battlespace entities with real- or near-to-real time access to the information exchange system and thus dramatically reduces the 'fog of war'.

The three most prominent experts of NEC, David S. Alberts, John J. Garstka and Frederick P. Stein defined net-centricity as:

"An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision-makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, [network-centric warfare] translates information superiority into combat power".

In my opinion, network-centric warfare/network enabled capabilities, means that every fighting entity, soldier, armored vehicle, or something else is unique addressable in order to receive information from sensors or to give direction. This can be done through a convergent network that permits the transfer of voice, video and data. As we can see nowadays, the most powerful convergent network is that based on Internet Protocol (IP), even if we use IPv4 or IPv6. Also, the use of IP rise many security issues to be faced.

In 2009, the ACT launched an awareness campaign within NATO, as well as in NATO Nations and beyond, to promote the NNEC concept and have it adopted NATO-wide.

[1] http://www.globalsecurity.org/military/library/report/crs/RS20557.pdf

[2] Network centric warfare and command and control: rethinking organizational architecture - Julius Calvin Washington – 2001

Achieving full collaboration and full coherence between the various NATO and NATO Nations projects is the long term goal.

2. Tenets of network-centric warfare

The basic tenets of Network-Centric Warfare are:

- A robustly networked force improves information sharing;
- Information sharing enhances the quality of information and shared situational awareness;
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command;
- Dramatically increased mission effectiveness.[3]

2.1. Networks

The focus on networks is highlighted in the first tenet, pointing to the need for a 'robustly networked force' to enable improved information sharing. The size, scope and reach of the network(s) required are determined by the missions, force structures and concepts of operations involved.

2.2. Information

The focus on information and its use is highlighted in the second and in parts of the third tenet. These tenets point to the need to exploit robust networking capabilities to improve information sharing; to enhance the quality of information shared, collaboration, and shared situational awareness.

The type of information which needs to be shared, the people with whom it needs to be shared, and the speed with which the information needs to be gathered and made available, is determined by force structures, concepts of operations, and the way the information is utilized to support a mission.

2.3. People

The focus on people and the benefits of working together in a networked environment is highlighted in portions of the third and fourth tenets. These highlight the role of improved information sharing and shared situational awareness in allowing people to work together in new more effective ways and thereby to improve speed of command, leading to dramatic increases in mission effectiveness. The tenets make it clear that implementing NCW involves adapting the way people think and work together The network centricity addresses the dimension of 'people' from the perspective of achieving "Decision Superiority". Decision Superiority is defined as *"the state in which betterinformed decisions are made and implemented faster than an adversary can react"*. Decision superiority is critically dependent on achieving and maintaining a position of information dominance and shared situational awareness during all phases of an operation, to enable a better understanding of the operational situation than the adversary. It means that the pace, coherence and effectiveness of operations can be dramatically improved, resulting in dramatic reductions in the length of decision cycles.

3. Infrastructure

Basically, the infrastructure needed by network-centricity concept is a broad network that supports voice, video and data. The information shared through this convergent network should travel from sensors to decision makers in order to enable them to make a right and quick decision, then, back from decision makers to the fighting entity as orders to be fulfilled.

[3] http://www.globalsecurity.org/military/library/report/crs/RS20557.pdf

The most important thing is that the information has to rich to the right person based on the principle "need-to-know".

Network-centricity concept is highly dependent on the interoperability of communications equipment, data, and software to enable networking of people, sensors, and manned and unmanned platforms. There is a large amount of data to be transferred so communications bandwidth should be adequate to allow the accurately, timely and trustworthy exchange of information. Parts of the technology rely on line-of-sight radio transmission for microwave or infrared signals, or laser beams. Other parts of the technology aggregate information for transmission through larger network trunks for global distribution via fiber optic cables, microwave towers, or both low-altitude and high-altitude satellites. The designs for this technology must enable rapid communications between individuals in all services, and rapid sharing of data and information between mobile platforms and sensors used by all military services. The architectures must also have the ability to dynamically adapt the network when one or more communications nodes are interrupted[4].

There are different terms used to describe the infrastructure that enables network-centricity concept. USA uses Global Information Grid (GIG), while NATO uses Networking and Information Infrastructure (NII). There are a lot of similarities and some minimum differences between the two mentioned concepts.

3.1. Global Information Grid (GIG)

The GIG is the communications infrastructure that supports Department of Defense (DOD) and related intelligence community missions and functions, and enables sharing of information between all military bases, mobile platforms, and deployed sites. The GIG also provides communications interfaces to coalition, allied, and non-DOD users and systems. Older messaging systems will all be made accessible via the GIG.

DOD planned that military communications equipment use the new Internet Protocol version 6 (IPv6) as the standard for all transmission through the Global Information Grid (GIG) by 2008. The new IPv6 protocol will reportedly offer greater message security and better tracking of equipment, supplies, personnel through use of digital tags, and enough IP addresses to be used.

3.2. Networking and Information Infrastructure (NII)

The strategy for developing the networking and information sharing aspects of NATO NEC (NNEC) focuses on the 'joining together' of networking systems and core information systems from NATO and NATO nations, to form a Federation-of-Systems (FoS) capability that implements the NII. The FoS concept is used here to refer to a set of different systems, which are not centrally managed, but are so connected or related so as to produce results beyond those achievable by the individual systems alone. In effect, the NII is to be made up of a combination of national Networking and Information Infrastructures segments and a NATO Networking and Information Infrastructure (NNII), which together will provide capabilities that no one system can provide by itself.

In order to build the NNII, NATO needs that every network from so called Federation-of-Systems to be interoperable, not only technically, but human and procedural.

4. Security in network-centric environment

Since the convergent network is agreed to be the base of network-centric environment, the issues of network security applies.

Talking about network security we have to answer three questions to meet the key elements for a secure network: **confidentiality**, **integrity** and **availability** (as they are stated in NATO document C-M (2002) 49 - 2002). The questions are:

[4] http://www.au.af.mil/au/awc/awcgate/crs/rl32411.pdf

- What to protect?
- What are the threats?
- How to protect?

To give a simple answer to the first question, the valuable information is to be protected.

During the NATO IA Symposium 2009, John Stewart from Cisco identified the following answers to the first question:

- Current operations information and activities;
- Past sensitive information or activities;
- Intelligence and sensitive communications;
- New or planned operations or capabilities.

Regarding the second question, there are a lot of known and unknown threats that can interfere with a convergent network based on IP. Some active threats identified by the Director of NATO CIS Service Agency (NCSA), Lieutenant General Kurt Herrmann, during the NATO IA Symposium 2009 are:

- Spam;
- Malware (viruses, worms, Trojans…);
- Web defacements;
- Denial of Service;
- Classified information leakage;
- Vulnerability exposed by poor maintenance;
- User indiscretion.

Also, he identified the attackers that can use the threats mentioned above:

- Script kiddie;
- Recreational hacker;
- Cyber activist;
- Organized crime;
- Terrorist organizations;
- Nations;
- Insider.

When talking about how to protect, everything starts with a coherent security policy and doctrine, applied to the network; some possible answers can be:

- Permanently monitoring the network;
- Use of enterprise security technologies;
- Security trained people.

4.1. Key Communication Elements

The communications component of the GIG/NII is characterized by the intended use of the Internet Protocol (IP) to provide a common, secure transport mechanism for all types of information moving across all types of transmission media. The process of adoption IP as the common transport mechanism will take time. It requires that IPv6 be adopted for any new systems and that IPv4 continues to be support for some time to come.[5] Key to this process will be the standardization of interfaces between deployable SATCOM terminals, and static networks and the optimization of these deployable networks to support IP traffic. This standardization process will help support the development of a SATCOM pooling concepts, which will be particularly important in supporting Expeditionary Operations.

Development of flexible IP encryption devices and supporting key management systems is a key pacing technology for all GIG/NII services. The rapid fielding of interoperable IP encryption devices is important to the development of a so called "black"

[5] http://www.globalsecurity.org/military/library/report/crs/RS20557.pdf

core network, operating at the UNCLASSIFIED level, that can handle voice, video and data traffic for multiple security domains and classification levels.

Along with development in IP encryption devices, rapid progress is needed in the area of passing of information between IP and non-IP networks. “Edge Proxy” is one of the names given to those devices that sit on the edge of IP networks, acting as an interface to non-IP networks and providing information proxy services as well as communications layer services. The use of edge proxies to support the interfacing of Tactical Data Links to IP networks is particularly important in the near and mid term.

4.2. Key Information Assurance Elements

Information assurance (IA) is the practice of managing information-related risks. More specifically, IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity and avilability[6].

Information Assurance mechanism are embedded into every aspect of the overall architecture of network-centric environment and work together to achieve the overall aim of protecting information whether at rest or in motion. These mechanisms help ensure that the right information, can be delivered to the right people at the right time, and that the information that they receive can be trusted. The emerging approach of “Duty to Share Balanced with the Need to Know” captures this intent. Duty to Share helps ensure that policies, procedures, and systems are developed and implemented with an inherent capability to share information, but have the necessary security measures in place to ensure only authorized users can access the information.

In the near-term IP encryption and key management infrastructures are keys to meeting the needs for secure communications. Work also needs to begin now with PKIs and XML technologies to enable the fielding of dynamic, role-based, policy-based, information access schemes in the mid-term. One of the major challenges is the deployment of large and interoperable PKI infrastructure and identifying the management scheme to support information access schemes.

4.3. Flexible security mechanisms

The “need to share” concept requires changes not only related to technical solutions, but maybe even more at the organizational level. The concept of sharing information with others in such a flexible manner may be perceived as loosing control compared to the preplanned and preconfigured solutions. The willingness to share information requires that the provider can be sure that the information is protected all the way during transport and also when received by the consumer.

The increased information sharing may lead to increased vulnerability if security is not properly integrated. The situation of today is that separate networks protect information of different classification using physical, cryptographic and administrative separation. Introduction of security mechanisms which allow for dynamic and seamless exchange of information between units will be a challenge in network-centric environment. IP level security will give confidentiality between systems, but will not prevent unauthorized access within the systems or LANs. Computer Network Attacks (CNA) will focus on attacks behind the firewalls (crypto devices) within the LANs/Systems. Therefore, end-to-end security services are required in order to secure the information inside the network systems, and to make sure the security is not broken in proxies or servers.

Security is a challenge with respect to network-centric environment, making seamless sharing of information a bit more difficult. The use of end-to-end security solutions does not exclude additional use of traditional network and transport level security. To obtain end-to-

[6] http://en.wikipedia.org/wiki/Information_assurance

end security there have been experimented XML and Web Services security solutions with the addition of XML Security Labels and a Public Key Infrastructure.

Conclusions

In the not too distant future, warfighters and their commanders will share unprecedented visual awareness of every pertinent aspect of the battlespace. These elements will be able to see what each other see in real time and share the composite picture, allowing increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.

As we gradually build a working concept of network-centric operations, we need to bear in mind some commonsense caveats. Networking is not a universal solution to warfare problems, nor will it change the nature of war. Speed will be critical to our success, but numbers and endurance will still count. Situational awareness will multiply our power, but knowing the enemy will be more important than ever. Above all, intelligent adversaries will respond, and the more successful our concept of network-centric operations becomes, the more asymmetrical their responses are likely to be.

Network enabled capabilities without Information Assurance would not work!

"Even if possible technologically, people will not share their information within the network-centric framework unless Information Assurance is guaranteed and networks are successfully defended against Cyber Attacks".[7] The attackers range from hackers who want to earn the "I hacked …" sticker, to organized criminals, and even nation-sponsored attacks. As in conventional warfare, the attackers have the advantage. They just need to find a single vulnerability to exploit while we need to always strike the balance between securing the network and enabling effective use of the network. This defender's imbalance becomes even more critical for us in the future, for the more we proceed on our path to network-centricity environment, the more attractive it becomes for adversaries to intrude, steal information or deny access. In fact, a strong focus on Information Assurance is essential if we are to continue on our path to NEC with the plug and play options in the Service Oriented Architecture.

Finally, Information Assurance in network-centric environment is not only about politics, management and technology. It is also about the security awareness of the personnel. The personnel remain a significant threat for the security of the networks; and the staff needs to be constantly educated.

References

1. http://www.cisco.com/web/strategy/docs/gov/defense_Network-Centric.pdf -26.01 2010
2. Security within the North Atlantic Treaty Organization (NATO), document C-M(2002)49 – 2002
3. http://www.nato.int/cps/en/natolive/topics_54644.htm - 21.01 2010
4. http://en.wikipedia.org/wiki/Information_assurance - 28.01 2010
5. Network centric warfare and command and control: rethinking organizational architecture - Julius Calvin Washington – 2001
6. http://www.au.af.mil/au/awc/awcgate/crs/rl32411.pdf - 21.01 2010
7. http://www.globalsecurity.org/military/library/report/crs/RS20557.pdf - 21.01 2010
8. http://www.stormingmedia.us/71/7180/A718015.html - 25.01 2010
9. http://accsco.be/wp-content/download/3NATO SAS Maturity Levels for NNEC Command.pdf – 25.01 2010
10. Director of NCSA speech on NNEC on 10 Dec 2008

[7] Director of NCSA speech on NNEC on 10 Dec 2008

CYBER WARFARE

CMDR Adrian NITU

UM 02418 Bucuresti

Introduction

Every country has it's right to defend itself by all appropriate means. Defense industries arose to satisfy demand for armies and doesn't seem to stop growing. This industry is driven by daily progress in advanced defense or offence technologies that make all the previous advancements obsolete. There are very few countries whose wealth allows to keep up with this speed. Even the best economic countries can't afford to develop technologies too advanced due to high expenses required for such programs.

Any conventional army needs to be well equipped and well organized. Equipment is not the only expense because organization of the army is much more important. Organization is distribution of correct information in exact scale and timing. Every army needs information and telecommunication network, every army is based on logistics and every army needs to know the enemy. Information age doesn't show only in business but also on the battlefield.

The information distribution needs to be done much faster; enemy movement must be communicated more precisely; troops need to be deployed more exactly and decisions have to be based on more accurate information. This shows that armies rely more and more on information, but they don't realize that information is an asset with great value that needs to be protected. All the effort to protect the information was targeted on physical security (eg. Limiting access to the information), but today with internetworking and tele-working there are other risks that need to be taken into account. Weaknesses in logical security enable attackers do all what is possible with conventional weapons (destruction of infrastructure) as well as weapons of mass destruction (nuclear reactor meltdown).

1. Cyber warfare

Cyber warfare is a relatively new type of weaponry with various effects on the target. It doesn't have any limitations of use and can achieve most of the goals set.

1.1 Weapons

Cyber weapons are usually basic programs that have the objective to defend or attack a target. Most of them are freely available on the internet but some more sophisticated or newer ones are kept privately or are commercial.

1.1.1. Detection

Systems in this category have the goal to detect possible attackers and identify what are they trying to do and possible where they are.

Detection can be based on expert knowledge (if I hear bullets flying then somebody is attacking us) or based on standard behavior (if a patrol doesn’t come back from recon mission on time there might be an attack imminent).

Tools in this category are

- Intrusion detection systems

- Security monitoring
- Log analysis

1.1.2. Prevention

Stopping the attacker is the primary concern even if the attack has not been identified (locking the entrance door is always a good idea). Most of the attacks are very simple and straightforward just like testing each door if it is open and a good prevention is to simply lock it, unless somebody expects an army trying to enter (but then other preventive measures apply).

Main tools in this category are:

- Firewalls
- Authentication systems
- Authorization systems

1.1.3. Target Identification

- Network scanners
- System scanners
- Vulnerability scanners

1.1.4. Attack

Here come all the tools that use the vulnerability of the system or application and achieve the objective an attacker wants. There are too many tools here to mention them as for every vulnerability there is more than one tool available.

It is also important to mention internet worms, that are automated tools misusing certain vulnerabilities and self-replicating themselves from one system to the other.

Another group are Trojan horses that can be deployed on the system to gain access to it later or to create a covert channel to obtain important information.

1.1.5. Deception tools

Deceiving the enemy is also important in case a distraction is needed to perform an attack or to slow the detection time of it. Here belong these subcategories:

- Log modifiers
- Distributed attack systems
- Root-kits
- Stealth tools

1.2 Strategy and Tactics

The acclaimed British strategic thinker B.H. Liddell-Hart approached strategy from two different perspectives. He differentiated between a grand strategy and military strategy. Liddell- Hart s grand strategy focused on a nation s ability to coordinate and direct all resources of a nation toward the attainment of a political objective.

Military strategy was more narrow, related to the execution of a battle plan or the projection of military force.

In Cyber-security there is no difference between military and civilian infrastructure as many targets are non- military but indirectly are involved in military infrastructure.

Disrupting economy or damaging image of a public infrastructure can wield much larger effect as weapons of mass destruction and therefore it is necessary not to limit the tactics or a strategy with any boundaries in order to get a global understanding of what attackers can gain or loose.

Strategies are based on certain behavior that defines the acting party. In cyber-security there are 3 major types (if not counting chaotic behavior)

1.2.1. Reactive behavior

Here strategy is based on action that can be seen or reported in any way. It reacts upon it with the appropriate response by increasing the awareness on that weakness.

As an example US security started to concentrate on airport security after September 11th incident. Or increasing awareness on information security after extensive cyber-attacks from china and other not “pro-american” countries.

This behavior strengthens those points in defense where attacks already happened, which means that there will be always several successful penetrations at the beginning.

Although it seems as in long-term infrastructure may reach a point where the systems would be secured sufficiently, but the fact is that with introduction of new software or new updates (and this happens very often) there are new security holes introduced which may be misused in time.

Infrastructures with limited security resources are very often using this behaviour to manage security. This means that security team in charge is either not very experienced or there is not enough people devoted to maintain IT systems. Depending on the response on a system breach there might be conclusions drawn upon their cyber-security strategy (especially incident handling and security monitoring).

By analyzing the security vulnerabilities of their systems it is possible to see the history of attacks upon their infrastructure.

There is also another alternative to this behavior, which is learning from mistakes of others, but not always can solutions of others be used to increase security of a bit different infrastructure.

1.2.2. Planned behavior

Importance of planning is already well known to project managers, but due to the nature of IT infrastructure it is not always applicable. IT infrastructure can't be kept strictly static and no t change to fit the work needs of its owner. To keep up with the progress in IT field as well as match the requirements for functionality in a very short time it is not possible to keep everything planned and well documented.

It is similar in national security planning where detailed plans won't work as expected as they cover huge economic; military and other systems that are changing very often and are not well documented.

In a best case with appropriate security planning well thought of and implemented appropriately can achieve decent level of security defense.

In former communist countries planning was done in almost every part of the state, but although many scenarios were thought of one aspect wasn't so much covered and that was human resources. Due to unexpected deviations in human behavior the whole system collapsed.

Cyber-security can be very well planned but the plan can't cover all scenarios and by not employing capable and experienced security people who can adopt the response there would always be a risk of a break-in.

If companies lack skilled people to operate defensive security measures or keep the systems secured (this is very often the case) appropriate response would follow after a long period of investigation and escalation. By knowing the procedures used by external companies an attacker can predict specific behaviors that would follow and adjust the cyber-attack to prevent any response.

A risk may be to underestimate the possibility of having outsourced managed security system that might be difficult to overcome. This trend gains importance in middle-sized or progressively thinking companies and if implemented nation-wide can be a very effective measure.

1.2.3. Proactive behavior

Previous behaviors were trying to cover known risks and vulnerabilities, but what if there is something new that wasn't reported or documented? In such case this attacks would remain undetected and would be identified as anomalies. For detecting and preventing also unknown new attacks it is necessary to be highly flexible and "be the first to know" your weakness.

A security strategy that concentrates on identifying its own potential weaknesses and covering its own holes is based on proactive behavior.

There are many functions that fall under proactive behavior category:

- source code review
- formal functionality proving
- traffic analysis
- self penetration testing
- self-adaptable security measures

There are already some security solutions and products on the market but are not very capable due to lack of skilled people to operate it. Formal functionality testing and source code review is not done in necessary scope to insure the safety of such system.

Several countries already started investigating this field and started adapting some parts of their systems. China already invested a lot into building large and well trained cyber-security force or USA has built national cyber-security research center to concentrate security experts and skilled engineers to improve bits and pieces of national cyber-security.

Proactive behavior needs highly skilled people and very tight security system in place and therefore it is important to keep highly skilled people in the country to either ensure its own security or to develop security systems that do it.

National security strategy

This is more an utopist approach as it is not possible to integrate and synchronize all the parts of one nation into one cyber-defense initiative, but it should be the goal of any cyber-security initiative.

The main goal here is to secure the nation from the network provider side up to the end-user. There is one general security standard and security policy which is being implemented and audited by authorized experts. Central electronic warfare centres is responsible of handling incidents that are reported by any entity in the country.

Educational system is capable of providing sufficient number of security experts and research capabilities to ensure implementation of national security strategy in every important infrastructure.

Attacking such system is extremely hard and may be only done from inside near by the target in order to minimize the possibility of detection or prevention. Such attacks require cooperation with conventional special forces that help the cyber-attack team to get to the target as close as possible and gain access to its data or functionality.

2. People

Security is based on 3 aspects: people; systems and procedures. As systems and procedures are developed by people, human resources are the key to cyber-security defense initiative.

2.1 Experts

The core of a cyber-security defense force is the people with security knowledge.

These are not administrators who are able to install a firewall, but these are people who design and develop firewalls and other security measures.

Without these people a country or a company needs to rely upon external help that may or may not be successful.

Position of a security expert is similar to a nuclear scientist, who can invent and develop deadly weapon for any state that is willing to pay for his research.

2.2 Intelligence

Information about the enemy is according to Sun Tzu the key to success in the battle or warfare. Gathering information about enemy tools and cyber-security systems is as valuable as knowing what kind of weapons and soldiers enemy has. Even on a company level it is important to know what kind of new security tools are on the market and what kind of security problems were discovered recently. Also information about security experts may be valuable in case of recruiting needs.

2.3 Hackers

Defense force is one side of cyber-security but it is also necessary to have offense capabilities. For the training scenarios as well as for identification of existing and new security holes in systems hackers are important.

Very often ex-hackers tend to do security consulting but the major difference between a hacker and security expert is that a hacker needs to identify one hole while the security expert has to cover them all.

2.4 System programmers

With all the knowledge of security requirements and new security holes, there needs to be somebody who integrates and modifies the software/hardware or a solution.

Knowledge of a system and skills in programming are necessary for progress of the IT industry as well as cyber-security.

3. DEFENSE

Information systems have many potential weaknesses, but whatever they are if they don't operate there is a problem.

It is the scale of this problem that determines the importance of such system and necessary security measures to protect it.

Minimizing the risk of such problem or the scale of it requires security measures that cover all the potential initiators of the problem. Here security experts tend to differentiate 3 main categories, although some security measures are in more than one and there is no clear definition which security measure belongs where.

3.1 Physical security

For thousands of years people, goods, towns or states were protected by physical security measures starting with stone walls up to nuclear bunkers. But no matter how smart or good the defense was there were always ways to get through. Therefore combination of each category is necessary to prevent the accident.

A good example of physical security is detecting and preventing EMP weapons getting in contact with logical security measures and switching them off. A EMP blast can disable C3 (command and communication center) communication system and herewith stop the attack or prevent defensive force from operating efficiently. A good physical countermeasure may be anti air defense or air patrols in the area.

A company level physical security countermeasure may be storing information system in a shielded data center with UPS.

3.2 Logical security

This is the main cyber-security battlefield where digital information is being exchanged or stored. Every security measure that is performed by a non-human device in the digital world is a member of this group.

There are many sub-fields here:

- Encryption
- Network security
- System security
- Application security
- Security monitoring/auditing

3.3 Organizational security

Even if information is sealed behind the blast doors there might be a risk that somebody would open the door and let the attacker take it.

That is why security procedures are in place to ensure that in case other security measures fail people would know what to do and by following procedures ensure the safety of the information. Very often in stressful situations with lack of expertise people tend to do more mistakes than ever. Procedures are there to help people do the right thing even if they don’t know what to do these guidelines would show them how to prevent the worst.

4. Offence

4.1 Strike scenario

The cyber-attack requires detailed structure and a plan in order to achieve the expected objective. Such plan should have this structure:

- General Target analysis
- Choosing specific objectives
- Selection of team members with sufficient qualification
- Detailed target analysis
- Attack planning
- Training the attack
- Execution of the attack
- Observing the target to ensure the objectives were met

At first point analysts collect as much information about the target as possible by standard means (eg. Newspapers, web-sites; newsgroups;..). This information should help identify:

- Target's mission (what is the goal of system's existence)
- Content and structure of the target's systems (network structure; geographical location; external systems connected; customers ;..)
- Technologies used (systems used; software and hardware implemented; defensive measures)
- History of system implementation (system integration times; upgrade dates; vendors)
- Human resources (how many people are employed; how well trained are they; what kind of information they collect; what are their interests;..)

All the information above should help to pick up the best (or the weakest) target and possible source of attack as well as time plan of action.

Second point should identify all the weakest spots or interesting spots that should be looked into more deeply. These targets do not have to be specific systems they also can be information sources or people.

In third point the team should be assembled containing specialists for every type of system used at the target. As it is not always possible to collect all the information necessary to choose the team all the starting members in the team should be able to call in any specialists they need for target analysis or strike.

Point four should gather all the necessary information about the target to create a specific plan of action to achieve the objectives specified in point two. This point identifies specific target structure and validates the information collected at point one. This is done by scanning the target systems and identifying operation systems, network elements as well as services and daemons running on them.

At point five the above information is processed and specific weaknesses identified for possible break-in. It is not always possible to identify them up to the detail necessary, but with correlation of other information collected it may be possible to make the attack plan more specific. The plan can contain further testing and scanning as there may be other systems that are not identifiable from outside.

Training the attack at point six is a preparation for the attack that optimizes and tests the cyber-weapons as well as the plan for the attack on a group of similar systems.

This also helps to develop a certain level of automation that speeds up the attack and minimizes the probability of human intervention.

Attack plan is usually very simple:

- use a system vulnerability detected
- gain the authorization level required
- achieve the objectives
- remove all the clues (if the objective was other than destroying the target)

Verification of achieving the objectives is dependant on their contents, but can be proved by analyzing the information collected or checking the target's services that should have been disrupted or analyzing the local information sources (eg. Newspapers).

4.2 Training

Building cyber army from volunteers can't be a solution for national security even if they are the elite of computer security experts. It is the same as if best sportsmen or hunters were to build an army. They may run fast or excel in precision shooting, but they will not succeed in logistics and tactics.

In order to train a cyber army there needs to be a structure created that will use them efficiently. There have to be procedures created to help handle the situations effectively. All this needs to be built first before any training can begin.

It is already clear that standard army field manuals can't be used to help build the cyber troops as here quality matters not quantity. Also tactics has to be built from scratch in order to achieve objectives necessary. Separation of offensive and defensive training is clearer and distinctive than in real combat training.

4.3 Defensive training

Infrastructure protection requires training in security technologies.

Field	*Technologies*	*Roles*
Network Security	•Firewalls •NIDS •Network design	•Firewalls specialist •NIDS specialist •Network designer
System Security	•System installation and configuration •HIDS (system monitoring, integrity checking) •Authentication •Auditing and logging •System programming	•System administrator •HIDS specialist •Authentication specialist •System auditor •System coder
Application Security	•Application installation and configuration •Application design and development •Data encryption	•Application administrator •Application developer •Encryption specialist
Organization Security	•Security policies •Disaster recovery planning •Incident handling •Forensics •Auditing	•Policy writer •Disaster recovery planner •Incident manager •Forensics officer •Auditor
Other	•Security monitoring	•Surveillance crew

All the roles described above are already existent in many companies and government agencies. There are many trainings for technologies specified above, but in order to use them in cyber warfare they need to be integrated together.

For example there is a potential target detected and commanding officer decides it is important to protect the target. Here is a general plan that needs to be executed:

- Auditors are sent onsite to investigate current status of security
- Every area specified above is assessed and commanding officer decides what area needs improvement and what experts would join the taskforce.
- Experts start improvements in organizational security (priority nr.1)
- After improving security policy other areas start improving systems and networks accordingly.
- Incident reporting (if possible also security monitoring) is linked to a defense center with security surveillance crew.
- General advisory is given to the target's security crew.
- After de-escalation of security alert monitoring and incident reporting is given back to target's security team.

This all needs to happen in a very short time as cyber attacks may start immediately after warning. Also cooperation with target's security team is vital due to the fact that they know their systems better.

Defense teams need to be trained in various technologies on the market and practice their skills on most of the common systems on the market.

Trainings on specific technologies need to be done by external companies who have resources and skills for it, but trainings in tactics should be done locally with cooperation of offensive warfare teams.

There are 3 types of training:

- Proactive securing of a target
- Immediate reaction on a attack and security of the target
- Security forensics after attack and securing of target's infrastructure to prevent more attacks

Type 1 training start with deployment of a system with application and a function defined for it. It continues with performing security checklists in order to bring the system and network components to a securely configured level. Next there are active security measures deployed in order to prevent majority of standard attacks. After that there are passive security measures deployed to monitor the system as well as provide sufficient auditing data to identify what happened.

Type 2 trainings are very similar to security drills on a military base. After an alert is issued team members have to gain control over the system and remove all the attackers from the system. This can be done with cooperation with offensive warfare teams. After allert is issued there needs to be an escalation procedure executed which informs global security control center (GSC2) of an ongoing attack. After gaining back complete control of the system team has to investigate how attackers got into the system and report it to GSC2. With this information system needs to be secured and security holes need to be patched. Also this process needs to be reported to GSC2 in order to secure other similar system that may be possible targets.

Type 3 trainings take place in systems that have already been hacked. Their main objective is to analyze system state and logs and reconstruct the actions that attackers did. This can help to secure the system as well as give some information to offensive warfare teams how to perform similar attacks. Another objective is to detect what has been changed in the system to prevent further damage or fraud.

4.4 Offensive training

It is difficult to train something not very specific that varies every moment. Offensive cyber-warfare is a set of tools and technologies based on security holes in various software.

These holes get fixed very quickly and training how to misuse would become obsolete after several days. Offensive training should be therefore based on general technologies rather than on specific tools.

Training objectives:

- psychological fitness (working under time pressure)
- technological understanding (general concepts of systems and networks)
- operational procedures and policies understanding
- State/government/army functionality understanding (information flow, command structure)

In order to meet these objectives there should be a training plan set to meet the army needs.

4.4.1. Psychological fitness

To succeed in cyber battlefield soldier needs to be able to work under pressure and make correct decisions very fast. Just like in conventional warfare a hole or a window in enemy's defense is opened for limited amount of time. Strike team needs to use this window and every second counts that they can gain with good preparation and training. Stress is not only a side-effect when working under pressure but also a key factor for success. Training should be done just in a same way as conventional trainings by learning procedures in order to minimize the reaction time in between.

4.4.2. Technological understanding

In conventional warfare it is necessary to know how weapons work in order to use them properly. This same concept is necessary for cyber-warfare. The level of detail must be sufficient to guarantee understanding of what happened, is happening or is expected to happen. By knowing the technologies a cyber warrior is able to make decisions and predict the enemy move as human interactions are very rare to happen.

Understanding of networking and operation systems technology should not be underestimated and should be the main objective of cyber warrior’s training.

4.4.3. Operational procedures and policies

Technological protection is very limited thanks to openness of every system. Protective measures don't affect required functionality of a system and therefore can't be expected to be the only defense of a target. By logical security there is also organizational security that comprises of procedures and policies. These are usually deployed in order to strengthen the defenses up to a maximum. Due to the human nature they are not as quick and precise as technological means, but they are not very visible and can't be easily predicted.

As an example if the target follows government cyber-security standard and has already detected a breach it needs around 10 minutes to report an incident and ask for help.

This external help requires at least 30 minutes to analyze the environment and assess the indicators of the breach. All this time can be used for achieving the objectives and covering tracks by cyber-attack team.

By knowing standard procedures employ end in specific industry a cyber warrior is able to predict the human response and assess the actions necessary to take or the remaining time he has to achieve his objectives.

4.4.4. General target's functionality

Learning about counterforce functionality and structure helps to choose the correct targets as well as make quick decisions about tactics to be used in specific attack. By hitting correct targets it is possible to achieve expected effect as well as create sufficient confusion and distraction to enlarge the attack window or leave the attacked system unnoticed. Although it is not very useful for execution cyber force but it is surely valuable for target choosing or tactics planning,

As an example US government initiated cyber-defense strategy which requires central emergency center. Information about the incident should be sent to the experts there but if the path is disabled and cyber attack team takes over the communication target may be gained *easier under control. Or by estimating time of response from the target knowing of existence of such center can increase the time delay of such response as target is expected to wait until the decision from such center.*

Conclusion

Gaining importance of information systems in today's warfare shows that information security is being a key to success of a conflict or even a war. Cyber warfare is becoming more and more powerful on today's battlefield and affects development of armies in many countries as well as development of weapon technologies. It's use should not be underestimated as it is highly flexible and hard to detect. Its costs allow any country to train or hire a team capable of doing more than a complete army.

Effective use of such teams can gain dominance on battlefield or force the enemy to retreat by shutting down its command infrastructure or communication network.

Value of cyber warfare is growing and with digitization of conventional warfare technologies as well as using more complex devices creates risks and weaknesses that allow cyber warfare units to do more damage than they could in past.

Information age is taking over conventional industries and with growing needs for automation and digitization nations realize la ck of skilled people able to control them.

Governments realize that this problem is slowing economy but they don't realize that it also creates risks and holes in national security strategy. Shutting down nuclear power-plants may destroy the whole economy in a matter of minutes; opening water dams may kill thousands of people or releasing poisonous chemicals destroy country's nature.

Cyber warfare units have a important mission to ensure country's survivability, prosperity and stability. They need to ensure national security and in worst case he lp with disaster recovery. In past countries relied on strength of conventional military units but now future of a country may depend on how well trained cyber warfare units are and how much practice they have.

Enemy is already there and getting stronger every moment. We must make sure we can keep him from destroying our values we've been creating so hardly.

References

1. www.cyberwarfare-event.com
2. *staff.washington.edu/.../cyberwarfare.html*
3. *news.softpedia.com/.../U-S-Military-Developing-Hacking-for-Dummies-Cyber-Warfare-Device-112483.shtml*

TEMPEST - INFORMATION LEAKAGE FROM ELECTROMAGNETIC EMANATIONS

1st LT Ionut CURELARIU

UM 02180 Bucuresti

Introduction

It has been known to military organizations since at least the early 1960s that computers generate electromagnetic radiation which not only interferes with radio reception, but also leaks information about the data being processed. Known as *compromising emanations* or *Tempest* radiation, a code word for a U.S. government programme aimed at attacking the problem, the electromagnetic broadcast of data has been a significant concern in sensitive computer applications.

TEMPEST is the name of a technology involving the monitoring (and shielding) of devices that emit electromagnetic radiation (EMR) in a manner that can be used to reconstruct intelligible data. The term's origin is believed to simply be a code word used by the U.S. government in the late 1960s, but at a later stage it apparently became an acronym for *Telecommunications Electronics Material Protected from Emanating Spurious Transmissions*. Some sources insist that it is an acronym for *Transient Electromagnetic Pulse Emanation Standard*.

1. Introduction to TEMPEST

1.1 Introduction to TEMPEST Attacks

TEMPEST attacks work on the principle that electronic devices such as monitors and fax machines emit electromagnetic radiation during normal use. With correct equipment such as antennas, receivers and display units an attacker could in theory intercept those emissions from a remote location (from across the street perhaps) and then replay the information that was captured. Imagine if this were possible how it could be misused to violate your privacy. Closing doors and blinds wouldn't do anything to stop a TEMPEST attack. If your monitor was displaying sensitive material then it would be exposed. However don't become paranoid for it's extremely difficult to execute an attack to "capture", but it's certainly possible.

Emsec is commonly understood as consisting of Tempest (the interception of stray information bearing RF emissions from equipment), Hijack (the interception of sensitive information that has somehow contaminated an electrical signal accessible to an attacker, e.g. a power line or ciphertext feed) and Nonstop (the interception of sensitive information that has accidentally modulated secondary emissions of an RF carrier such as a mobile phone or radar signal). Each of these three terms is also used to refer to the relevant defensive techniques.

These definitions do not exhaust the space of emsec threats; it is possible, for example, to extract information from some equipment by illuminating it with a microwave beam and studying the return signal. Other equipment can be caused to fail and leak information by an attacker who inserts transients in the power supply. Such active attacks tend to be given less attention by military equipment suppliers but are likely to become more important with the increasing use of COTS products; they can interact in nasty ways with protocol and algorithm design.

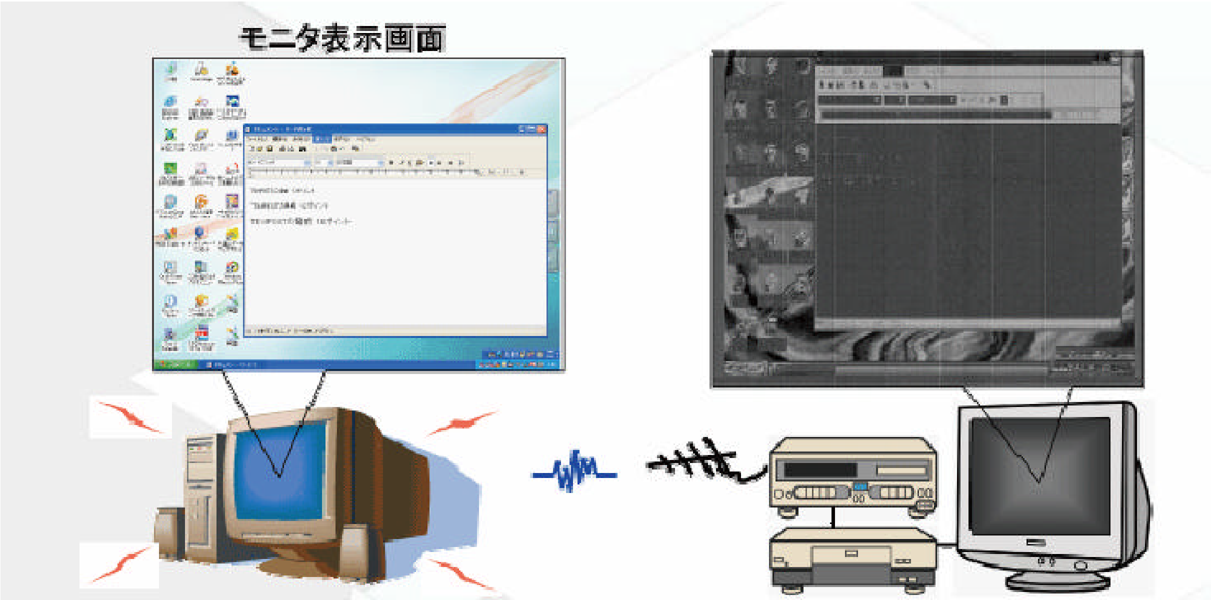
Nor is emsec an exclusively military problem. Banks are worried about Tempest attacks on automatic teller machines; the ease with which the stray RF from an RS-232 line can be monitored has been documented in the open literature, and such lines are used to connect the ATM CPU with the magnetic card reader and PIN pad. A number of sources report the capture of both PIN and card stripe contents at a distances of up to 8 m .

A growing concern is that many security processors sold to the commercial market are vulnerable to emsec exploits.

Passive TEMPEST Attacks: Such an attack is passive in that it cannot be detected. A device emits compromising radiation which could be reconstructed from a remote location. This means that you cannot detect it as the device is not in any way connected/installed on your system. To simply put it your computer can't detect a guy down the street with equipment trying picking up radio emissions from your monitor.

How it works: All electronic devices big or small may emit low-level electromagnetic radiation. In fact your CPU chip is probably doing it right now. This happens whenever an electric current changes in voltage and thus generates electromagnetic pulses that radiate as invisible radio waves. These electromagnetic radio waves can carry a great distance in ideal situations.

Monitors that contain a CRT system contain an electron gun in the back of the picture tube which transmits a beam of electrons. When the electrons strike the screen they cause the pixels to light up (fluoresce). This beam scans across the screen from top to bottom very rapidly in a repetitive manner, line by line, flashing on and off, making the screen light and dark thus creating the viewed image. These changes in the high voltage system of the monitor generate the signal that TEMPEST monitoring equipment receive, process (reconstruct) and finally view. Here is an example from a Japanese site:



Unshielded cables such as those from your computer to your monitor can act like an antena which instantly increases the signal thus increasing the distance which a TEMPEST device may be located. A telephone line connection to your computer may also act as an antenna and that could also increase the distance to some lengths.

1.2. TEMPEST risks.

1.2.1 TEMPEST objectives

Communication security (COMSEC) the term used to denote steps taken to prevent disclosure of national security information to unauthorized recipients during the communication process. The information to be guarded includes plain text of classified messages, as well as cryptographic technology and materials. Cryptographic information is especially sensitive, not as an end in itself, but because it is used to protect other classified data. If the integrity of an encryption system is breached at any point, all classified information protected by that coding may be compromised.

COMSEC consists of four main parts:

- physical security - all physical measures to safeguard materials from unauthorized access;
- emissions security - control of emanations from equipments processing classified data;
- transmission security - protection of transmissions from traffic analysis, imitative deception, and disruption;
- cryptographic security - the use of technically sound cryptosystems.

Only the emissions security discipline or TEMPEST is specifically addressed in this study.

Details of TEMPEST issues. Because the details of many TEMPEST issues are classified and controlled under strict conditions of need-to-know, the following discussions must be somewhat general. Nevertheless, it provides the reader with a needed appreciation of TEMPEST fundamentals.

Theory of electromagnetic signal emanation. Any electrical/electronic circuit that carries a time-varying current will emanate electromagnetic signals with the strength of the emission proportional to the current amplitude and its time rate of change. These signals propagate outward from the source as free space waves and as guided waves along conductors connected to or close to the radiator. If time variations of the source currents are related in any way to the information content of the signals, then the emanation will also bear some relationship to the data. It may, therefore, be possible to reconstruct the original intelligence by analysis of these unintentional emissions.

Aim of TEMPEST discipline. If the source information is classified, interception and analysis of the emanations by unauthorized personnel will compromise national security. The aim of the TEMPEST discipline is to control stray emissions in a manner that prevents such disclosures.

1.2.2. Equipment emission characteristics

RED and BLACK terminology. Before addressing the emission characteristics issue, the RED and BLACK terminology will first be introduced. A RED equipment or circuit is one that handles plain text information with national security value. Equipment processing signals that are unclassified, either because of content of the text or because the intelligence is obscured by encryption, is denoted in BLACK.

Strength and nature of emanations. The unintentional emission characteristics of RED systems and equipments are categorized according to strength and nature of their emanations. The reason for the strength element is clear: high-level signals can be intercepted at magnitudes that permit analysis with greater physical separations between the source and the eavesdropper. The second factor relates to the correlation between waveform of the emitted signal and the information to be protected.

Classes of equipment. For purposes of facility engineering and construction within the limitations of this study, it is only necessary to define two classes:

- Equipments that are TEMPEST-approved according to the criteria established in the military system;
- All equipments that have not been TEMPEST-tested or are nonapproved.

1.2.3 TEMPEST isolation requirements

Isolation approaches Encryption is the method used to guard against disclosure of classified information when long-distance telecommunications are monitored. However, it does not prevent possible compromise through interceptions and analyses of unintentional emanations from RED equipments.

Many approaches are available to equipment and facility designers to avoid disclosures through potentially compromising emanations. All of these techniques reduce the stray signal strength at locations where access is uncontrolled, so that the intelligence content is lost in the background electrical noise.

Examples of preventive measures include the following:

- Physical separation - excluding unauthorized individuals from areas near the source where the emanations are larger in amplitude than the ambient noise.
- Electromagnetic separation - the use of shielding, filtering, and other methods of EM isolation to attenuate the unintentional emissions.
- Signal level minimization - design and operation of circuits at lowest feasible power levels to minimize the strength of unintentional emissions.

The first requirement, a physical security measure, is the establishment of a controlled space (CS) containing the equipment to be TEMPEST-protected and within which access is not available to those not authorized to receive the information being processed at the site.

Shielding effectiveness requirements for specific TEMPEST applications, parameters of the problem include measured emission characteristics of the equipments and distance to the perimeter of the controlled space. The calculation determines the attenuation needed to reduce emanation levels below detectable limits in the ambient noise environment. If reasonable worst-case assumptions are made regarding the variables, however, then 50 decibels (nominal) attenuation is adequate for an installation within CONUS. This requirement can be met by a shield and penetration treatments.

TEMPEST design criteria. Since electromagnetic performance requirements of a 50-decibel (nominal) TEMPEST design are quite consistent with performance necessary for HEMP considerations and only a few additional features are prescribed for the shielding and penetration protection subsystem, the reasonable worst-case TEMPEST assumptions have been incorporated into the recommended HEMP/TEMPEST approach.

The following paragraphs summarize the TEMPEST-unique requirements for facility design:

(a) **Shielding effectiveness**. Minimum attenuation levels of the shielded enclosure.

(b) **Shield doors**. TEMPEST shield design includes a shielded vestibule entrance arrangement with two doors oriented at 90 degrees to each other. The purpose of double doors is to preserve the shielding effectiveness during actual entries and exits. Effectiveness requirements for the doors are the same as those for the main shield.

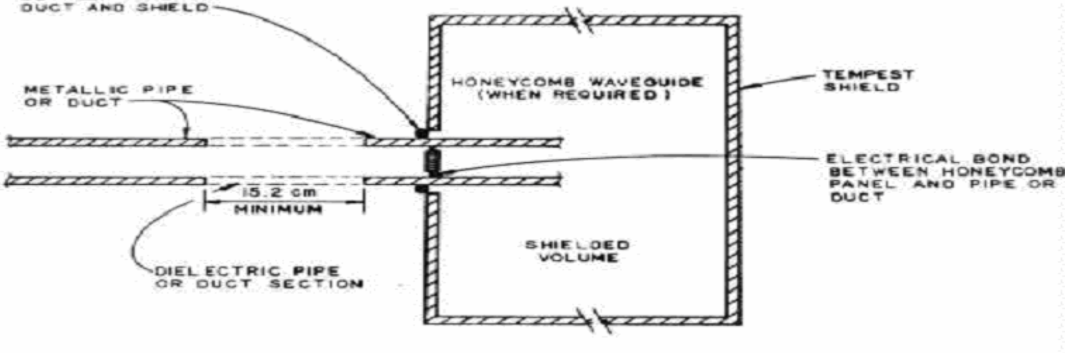

ELECTRICAL BOND BETWEEN PIPE OR DUCT AND SHIELD
METALLIC PIPE OR DUCT
HONEYCOMB WAVEGUIDE (WHEN REQUIRED)
TEMPEST SHIELD
ELECTRICAL BOND BETWEEN HONEYCOMB PANEL AND PIPE OR DUCT
15.2 cm MINIMUM
SHIELDED VOLUME
DIELECTRIC PIPE OR DUCT SECTION

Figure 1: Fifty - decidel (nominal) TEMPEST pipe or air duct penetration design

(c) **Piping and ventilation penetration**. Mechanical penetrations, piping, and air ducts are to be bonded to the shield at the point of penetration. The design must be configured as a waveguide-beyond-cutoff to attenuate all frequencies within the specified band, as shown in figure 1.

(d) **Electrical penetration**. The specification requires that a filter providing at least 50 decibels of insertion loss from 14 kilohertz to the upper design protection frequency, typically 1 to 10-gigahertz upper frequency, be installed on each power, telephone, and signal line that penetrates the enclosure shield wall.

1.2.4. Installation within the shielded volume

Precluding unintentional coupling. It is virtually certain that the volume enclosed by the TEMPEST shield will contain some BLACK equipment and wiring, as well as RED circuits that handle national security information. Therefore, the facility design and hardware/wiring layouts must preclude unintentional coupling of RED emanations into BLACK conductors.

Limited exclusion area. The room or area within which RED equipment is located and to which controls are applied for protection of national security information is known as a limited exclusion area (LEA). The TEMPEST shield may enclose part or all of the LEA and might also envelope other spaces.

Spacing of equipment. RED equipment must be physically separated from the facility walls and ceiling, from BLACK equipment and wiring, and from utility conductors such as ventilation ducts and piping. Minimum required spacings depend on whether the RED equipment is low-level signaling, TEMPEST- approved hardware or not, and on the nature of possible propagation paths between the BLACK element and an area of uncontrolled access.

Penetrations. Physical separation practices, as well as special shielding and distribution (for example, using conduits, ducts, and trays) instructions, also apply between RED and BLACK wiring in the LEA. Markings with paint or tape are prescribed to distinguish RED wiring runs from BLACK cables, and RED conduits must be accessible for inspection.

Separating RED and BLACK. Also, depending on characteristics of the RED equipment, separate filter-isolated RED and BLACK power distribution subsystems or individual equipment power filters may be required. Further, it may be necessary to provide separate and distinctively identified RED and BLACK convenience outlets.

Telephones and intercoms. Administrative telephone and facility intercommunication subsystems require particular attention. The most effective protection is to eliminate or, at least, minimize the number of instruments in the LEA. If exclusion is not practical, separation, shielding, and filter isolation devices and positive disconnect capabilities are to be provided.

2. Soft Tempest - an opportunity for security

Soft Tempest consists of the use of software techniques to filter, mask or render incomprehensible the information bearing electromagnetic emanations from a computer system. This may give complete protection to some system components, and while the level of protection available for others is only of the order of 10-20 dB, this translates to a difference of about one zone, which can still give a very significant cost saving.

It has been known for some time that the information bearing RF emanations from a computer can be modified by its software. For example, IBM machine which had a 1.5 MHz clock; a radio tuned to this frequency in the machine room would emit a loud whistle. With a set of subroutines of different lengths such that by calling them in sequence, the computer could be made to play a tune.

A modern re-implementation of this is : a PC monitor with a pixel frequency of 70 MHz can be fed video signals which implement a 10 MHz radio signal, amplitude modulated with different tones. This can be used to attack computers that are not connected to networks and have good physical security: the computer is infected with a virus which searches the disk for keys or other interesting material and then transmits it to a nearby receiver. (A more sophisticated implementation could use spread spectrum rather than simple AM.) Indeed, there has been speculation that such a 'Tempest virus' has been used in at least one actual incident of espionage.

Such phenomena led us to consider whether software techniques could be used for defense as well.

2.1 Filtered fonts

The technique which has attracted most publicity, and which is already fielded in two commercial security packages, is font filtering. Most of the information bearing RF energy from a VDU was concentrated in the top of the spectrum, so filtering out this component is a logical first step. We removed the top 30% of the Fourier transform of a standard font by convolving it with a suitable sin(x)/x low-pass filter.

Figure 1 shows standard black on white text; figure 2 shows the same text after low pass filtering; figure 3 shows a section through the original text; figure 4 a section through the filtered text, whose background is set at 85% white; figure 5 a section as received by the monitor if a cheap low-pass filter is installed in the VDU cable; figures 6 and 7 show the same text (normal and filtered) as it appears to the authorized user on the PC monitor; and finally figures 8 and 9 show the normal and filtered text as it appears to the unauthorized viewer using an ESL model 400 Tempest monitor.

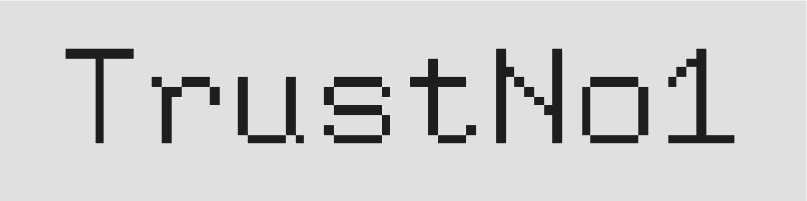


Figure 1: Standard black on white text image.

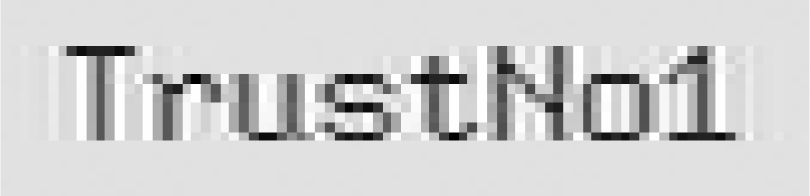


Figure 2: The same text after horizontal low-pass filtering.

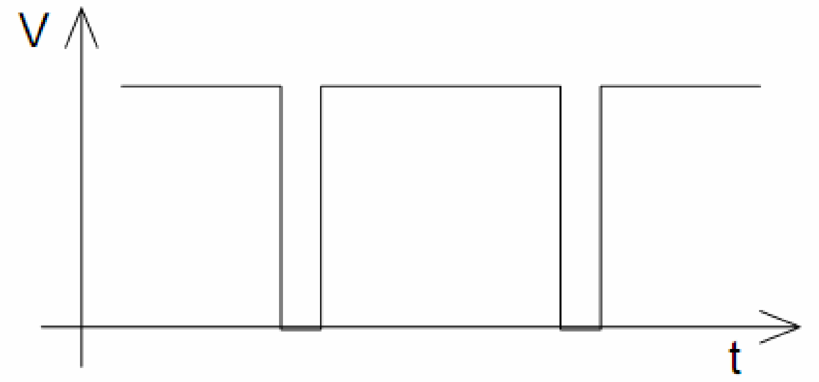


Figure 3: Video signal of a normal font

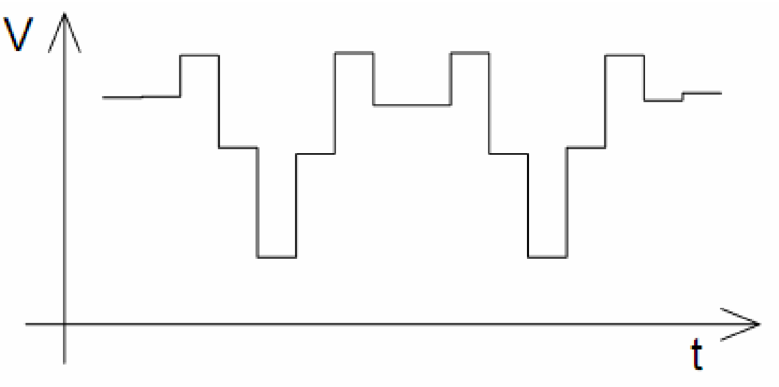


Figure 4: Video signal of a filtered font

The filtered text looks rather blurred and unpleasant in the magnified representation of figure 2, but surprisingly, the loss in text quality is almost unnoticeable for the user at the computer screen, as can be seen from the magnified photos figures 6 and 7. The signal is in any case filtered by the video and monitor electronics and the impedance of the VDU cable. When one adds in the limited focus of the electron beam and the limited resolution of the eye, the net effect of filtering is small. Indeed, some observers think that the image quality is slightly improved.

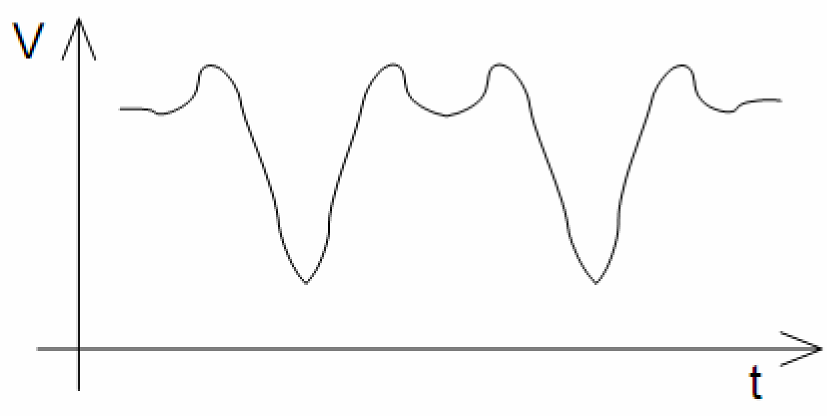


Figure 5: Video signal of altered font after analog HF suppression

While there is little visible change for the user, such filtering causes a text which could previously be received easily to vanish from the Tempest monitor, even when the antenna is right next to the VDU. The Tempest receiver screen shots in figures 8 and 9 show that not only has the information bearing signal disappeared, but the receiver's automatic gain control has turned up, displaying the synch pulses as vertical lines (the text appears four-up here as the line frequency of the monitor in use is 70 kHz while our elderly Tempest receiver was designed in the era of the PC-AT and only goes up to 20 kHz).

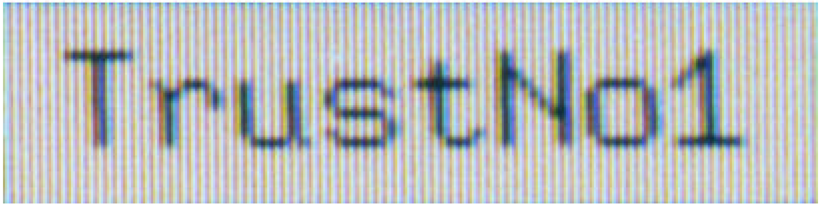


Figure 6: Screen appearance of a normal font

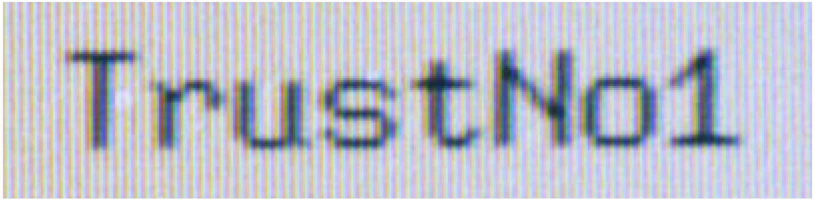


Figure 7: Screen appearance of a filtered font

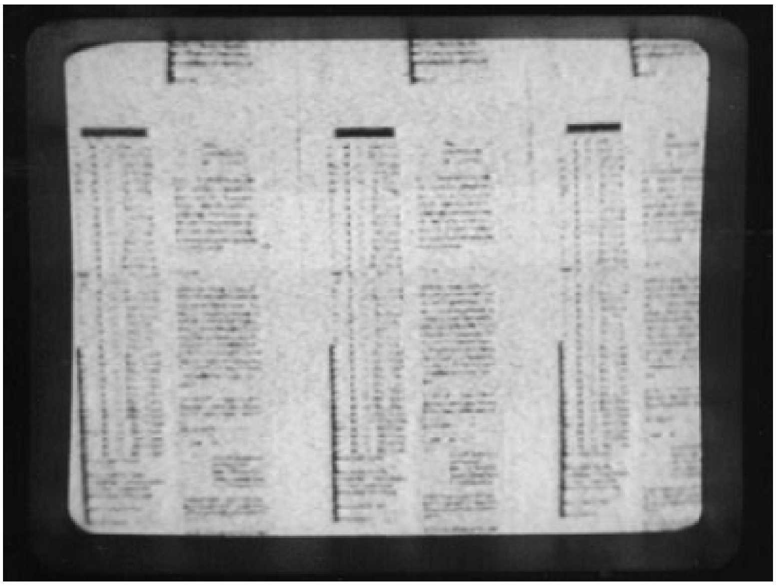


Figure 8: Eavesdropper's view of normal fonts

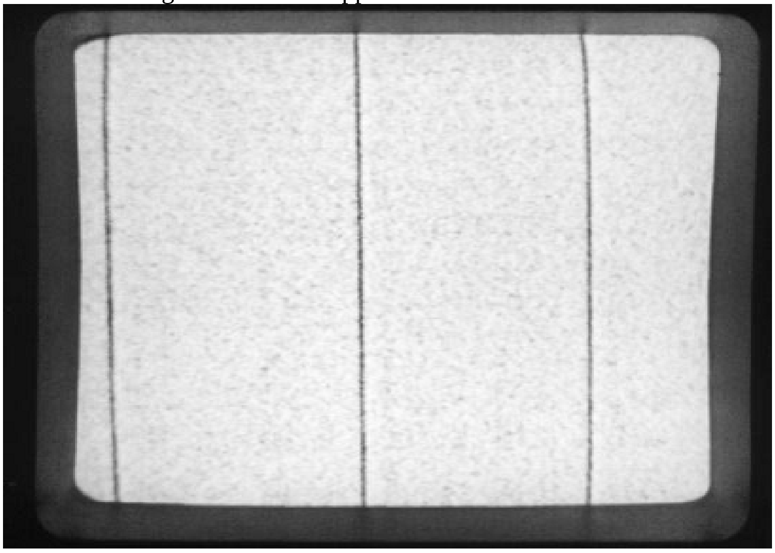


Figure 9: Eavesdropper's view of filtered screen content

Filtered text display requires greyscale representation of glyphs, but this technology is already available in many display drivers in order to support antialiasing fonts. The next generation of anti-Tempest display routines may also apply the opposite of the techniques used in OCR fonts: signal differences between glyphs of different characters can be minimized and there can be multiple representations of some glyphs with quite different signal characteristics. This should make automatic character recognition by the eavesdropper more challenging.

Eavesdropping text from a monitor is only one of the Tempest risks associated with personal computers. Nevertheless, I still consider it the most significant one, as the video display unit is usually the strongest source of information bearing radiation.

2.2 Securing a keyboard

Another possible application of Soft Tempest techniques lies in securing computer keyboards. Here there are two main threats: the passive observation of RF emanations at harmonics of the keyboard scan cycle, and active attacks in which the keyboard cable is irradiated at a harmonic of its resonant frequency and the scan codes are detected in the return signal which is modulated by the nonlinear junction effect.

Here our defensive technique involves reprogramming the keyboard microcontroller so that the scan cycle is randomized, and then encrypting the scan codes before they are sent to the PC. Thus for a given key press, the number of keys scanned in a cycle will be a random and changing value rather than a known constant, and even although the value can be measured by an attacker, it should give him no information on the value of the key press, on the user's typing pattern, or even on whether the keyboard is in use at all. The necessary system modifications affect only the PC's device driver and the firmware in the keyboard microcontroller.

Three features of this keyboard protection technique should be noted. The first is that, whereas font filtering may give only 10-20 dB of protection and thus be inadequate on its own in the most demanding applications, the keyboard technique may be sufficient even there (the exception is where complete shielding is needed for tactical reasons to prevent radio direction finding). The second is that the keyboard protection can be independent of other protection options. The third is that suitably modified keyboards can be supplied through existing trusted distribution chains (and can reinforce these controls as they will not work with an unmodified PC).

Conclusions

Soft Tempest techniques have the potential to save NATO governments a very large amount of money. They are already fielded in COTS products, some of which are already used by government agencies. More generally, it is time that governments started looking seriously at a more systematic exploitation of Soft Tempest technology.

All applications should use Soft Tempest. Where a high level of protection is needed, as in a diplomatic or intelligence system, 100 dB of shielding may be prudent - but this can always fail, shield failure can leave critical data unprotected.

In less critical applications, where zoning techniques are used at present, Soft Tempest has the potential to make a difference of about one zone. NATO governments should consider whether the cost savings from this will justify adopting the technology. It should also be borne in mind that once adopted it can be extended to large numbers of systems at little marginal cost; this will provide some potential for extending protection against future attackers using low-cost software radios.

References

[1] *'Electromagnetic Pulse (EMP) and Tempest Protection for Facilities', Engineer Pamphlet EP 1110-3-2, 469 pages, U.S. Army Corps of Engineers, Publications Depot, Hyattsville, December 31, 1990;* ***http: //www.jya.com/emp.htm***

[2] *'Emission Security Countermeasures Reviews', Air Force Systems Security Memorandum 7011 (1 May 1998),* ***http://jya.com/afssm-7011.htm****.*

[3] MG Kuhn, RJ Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", in David Aucsmith (Ed.), *Information Hiding, Second International Workshop,* Portland, Oregon, USA, 15-17 April, 1998; Springer LNCS v 1525 pp 124-142; **http://www.cl.cam.ac.uk/Research/ Security/tamper/**

[4] ER Koch, J Sperber, *'Die Da,ten,m,afia,: Computerspionage und neue Informationskartelle',* Rowohlt, ISBN 3-498-06304-9, 1995.

[5] MG Kuhn, RJ Anderson, *'Low Cost Counter- measures Against Compromising Electromagnetic Computer Emanations',* UK patent application no 9801745.2, January 28, 1998; also filed as US patent

[6] STEGANOS II Security Suite, from DEMCOM, Germany; **http://www.demcom.com**

[7] Pretty Good Privacy v 6.0.2, from NAI Inc, USA; **http://www.pgpi.com**

[8] *'Operating Manual for DataSafe/ESL Model 400B/400B1 Emission Monitors', DataSafe Limited, 33 King Street, Cheltenham, Goucestershire GL50 4AU, United Kingdom, June 1991*

[9] *NACSIM (National COMSEC Information Memorandums) 5000, 5203.*

VIRTUAL PRIVATE NETWORKS

CAPT Flavius BLAJAN

UM 01607 Someseni

INTRODUCTION

Why VPN?

The rapid growth of the INTERNET and widespread deployment of networks are creating a demand for new capabilities in IP networking. Some companies have set up their own WAN (wide area network) using a dedicated leased line. But such networks are expensive and there is no scope in such a system to share under-utilized bandwidth across several customers.

VPN is one method for interconnecting multiple sites belonging to customers using an Internet Service Provider (ISP) backbone network in place of a dedicated line.

What is VPN?

A virtual private network, VPN, is the extension of a private network that encompasses links across shared or public networks like the Internet. Another definition for VPN states that is a computer network that is implemented in an additional logical layer (overlay) on top of an existing larger network.

A VPN enables you to send data between two computers across a shared or public inter-network in a manner that emulates the properties of a point-to-point private link. The act of configuring and creating a virtual private network is known as virtual private networking. It is called "virtual" because it depends on the use of virtual connections - that is temporary connections, but consists of packets routed over various machines on an ad-hoc basis. It is an implementation of a private network on top of the Internet technology infrastructure using modern switching or routing hardware, encryption, authentication, packet tunnelling and firewalls.

To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The portion of the connection in which the private data is encapsulated is known as the tunnel. The portion of the connection in which the private data is encrypted is known as the virtual private network (VPN) connection.

1. Common uses of virtual private networks

1.1 Remote Access over the Internet

VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. Figure 1 shows a VPN connection used to connect a remote user to a corporate intranet.

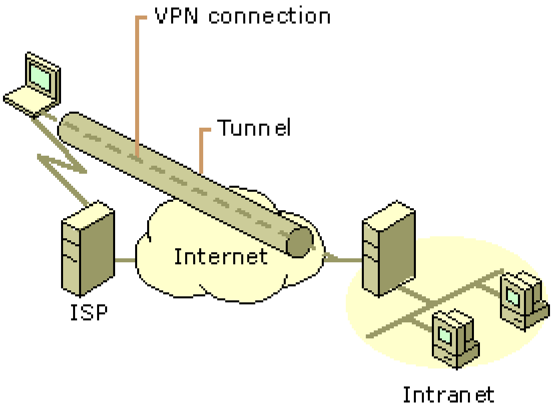


Figure 1: Using a VPN connection to connect a remote client to a private intranet

Rather than making a long distance call to a corporate or outsourced network access server (NAS), the user calls a local ISP. Using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

1.2 Connecting Networks over the Internet

There are two methods for using VPNs to connect local area networks at remote sites:

- **Using dedicated lines to connect a branch office to a corporate LAN**. Rather than using an expensive long-haul dedicated circuit between the branch office and the corporate hub, both the branch office and the corporate hub routers can use a local dedicated circuit and local ISP to connect to the Internet. The VPN software uses the local ISP connections and the Internet to create a virtual private network between the branch office router and corporate hub router.
- **Using a dial-up line to connect a branch office to a corporate LAN**. Rather than having a router at the branch office make a long distance call to a corporate or outsourced NAS, the router at the branch office can call the local ISP. The VPN software uses the connection to the local ISP to create a VPN between the branch office router and the corporate hub router across the Internet.

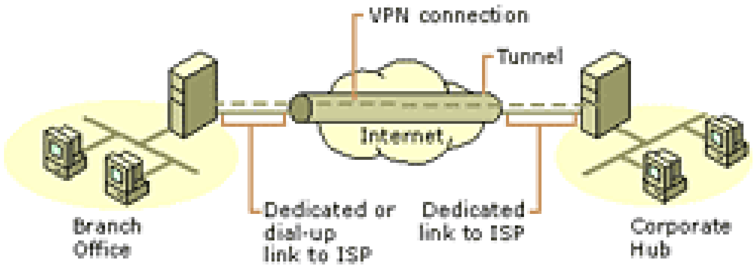


Figure 2: Using a VPN connection to connect two remote sites

In both cases, the facilities that connect the branch office and corporate offices to the Internet are local. The corporate hub router that acts as a VPN server must be connected to a local ISP with a dedicated line. This VPN server must be listening 24 hours a day for incoming VPN traffic.

1.3 Connecting Computers over an Intranet

In some corporate inter-networks, the departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the corporate inter-network. Although this protects the department's confidential information, it creates information accessibility problems for those users not physically connected to the separate LAN.

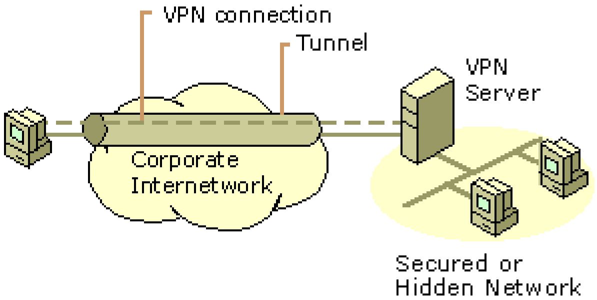


Figure 3: Using a VPN connection to connect to a secured or hidden network

VPNs allow the department's LAN to be physically connected to the corporate inter-network but separated by a VPN server. The VPN server is not acting as a router between the corporate inter-network and the department LAN. A router wo uld connect the two networks, allowing everyone access to the sensitive LAN. By using a VPN, the network administrator can ensure that only those users on the corporate inter-network who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.

2. Virtual private networks – tunnelling

2.1 Tunneling Basics

The act of configuring and creating a virtual private network is known as virtual private networking.

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public transit inter-network to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The portion of the connection in which the private data is encapsulated is known as the tunnel. The portion of the connection in which the private data is encrypted is known as the virtual private network (VPN) connection.

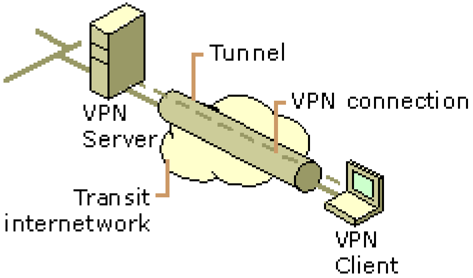


Figure 4: Virtual private network connection

Tunneling is a method of using an inter-network infrastructure to transfer data for one network over another network. The data to be transferred (or payload) can be the frames (or packets) of another protocol. Instead of sending a frame as it is produced by the originating node, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate inter-network.

The encapsulated packets are then routed between tunnel endpoints over the inter-network. The logical path through which the encapsulated packets travel through the inter-network is called a tunnel. Once the encapsulated frames reach their destination on the inter-network, the frame is decapsulated and forwarded to its final destination. Tunneling includes this entire process (encapsulation, transmission, and decapsulation of packets).

The transit inter-network can be any inter-network - the Internet is a public inter-network and is the most widely known real world example. While the Internet provides one of the most pervasive and cost-effective inter-networks, references to the Internet in this paper can be replaced by any other public or private inter-network that acts as a transit inter-network.

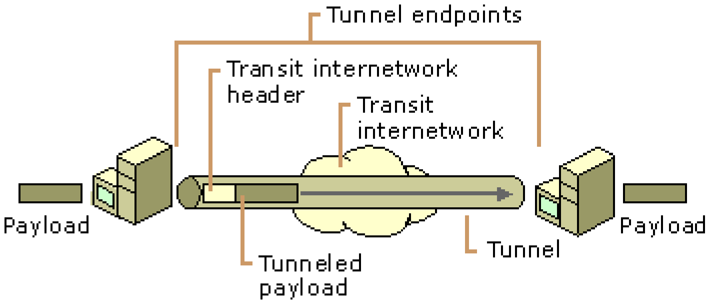


Figure 5: Tunneling

2.2 Tunneling Protocols and Technologies

Over the years, several protocols are developed for encrypting network packets for VPN purpose. Each protocol has its own advantages and disadvantages and are incompatible with each other. The four major protocols, which are widely accepted in the industry, are listed below:

- **Point-to-Point Tunneling Protocol (PPTP)**. PPTP allows IP, IPX, or NetBEUI traffic to be encrypted, and then encapsulated in an IP header to be sent across a corporate IP inter-network or a public IP inter-network such as the Internet;
- **Layer Two Tunneling Protocol (L2TP)**. L2TP allows IP, IPX, or NetBEUI traffic to be encrypted, and then sent over any medium that supports point-to-point datagram delivery, such as IP, X.25, Frame Relay, or ATM;
- **IPSec tunnel mode**. IPSec tunnel mode allows IP packets to be encrypted, and then encapsulated in an IP header to be sent across a corporate IP inter-network or a public IP inter-network such as the Internet.
- **Secure Sockets Layer** (**SSL**), is a cryptographic protocol that provide security for communications over networks such as the Internet. SSL encrypts the segments of network connections at the Transport Layer end-to-end.

For a tunnel to be established, both the tunnel client and the tunnel server must be using the same tunneling protocol.

Tunneling technology can be based on either a Layer 2 or a Layer 3 tunneling protocol. These layers correspond to the Open Systems Interconnection (OSI) Reference Model. Layer 2 protocols correspond to the data-link layer and use frames as their unit of exchange. PPTP and L2TP are Layer 2 tunneling protocols; both encapsulate the payload in a PPP frame to be sent across an inter-network. Layer 3 protocols correspond to the Network layer, and use packets. IPSec tunnel modes is an example of a Layer 3 tunneling protocol and encapsulate IP packets in an additional IP header before sending them across an IP inter-network.

For Layer 2 tunneling technologies, such as PPTP and L2TP, a tunnel is similar to a session; both of the tunnel endpoints must agree to the tunnel and must negotiate configuration variables, such as address assignment or encryption or compression parameters. In most cases, data transferred across the tunnel is sent using a datagram-based protocol. A tunnel maintenance protocol is used as the mechanism to manage the tunnel.

Layer 3 tunneling technologies generally assume that all of the configuration issues are preconfigured, often by manual processes. For these protocols, there may be no tunnel maintenance phase. For Layer 2 protocols (PPTP and L2TP), however, a tunnel must be created, maintained, and then terminated.

Once the tunnel is established, tunneled data can be sent. The tunnel client or server uses a tunnel data transfer protocol to prepare the data for transfer. For example, when the tunnel client sends a payload to the tunnel server, the tunnel client first appends a tunnel data transfer protocol header to the payload. The client then sends the resulting encapsulated payload across the inter-network, which routes it to the tunnel server. The tunnel server accepts the packets, removes the tunnel data transfer protocol header, and forwards the payload to the target network. Information sent between the tunnel server and the tunnel client behaves similarly.

2.3 Basic Tunneling Requirements

Because they are based on the well-defined PPP protocol, Layer 2 protocols (such as PPTP and L2TP) inherit a suite of useful features. These features and their Layer 3 counterparts address the basic VPN requirements, as outlined below:

- **User Authentication**. Layer 2 tunneling protocols inherit the user authentication schemes of PPP, including the EAP methods discussed below. Many Layer 3 tunneling schemes assume that the endpoints were well known (and authenticated) before the tunnel was established. An exception to this is IPSec Internet Key Exchange (IKE) negotiation, which provides mutual authentication of the tunnel endpoints. Most IPSec implementations including Windows 2000 support computer-based certificates only, rather than user certificates. As a result, any user with access to one of the endpoint computers can use the tunnel. This potential security weakness can be eliminated when IPSec is paired with a Layer 2 protocol such as L2TP.
- **Token card support**. Using the Extensible Authentication Protocol (EAP), Layer 2 tunneling protocols can support a wide variety of authentication methods, including one-time passwords, cryptographic calculators, and smart cards. Layer 3 tunneling protocols can use similar methods; for example, IPSec defines public key certificate authentication in its IKE negotiation.
- **Dynamic address assignment**. Layer 2 tunneling supports dynamic assignment of client addresses based on the Network Control Protocol (NCP) negotiation mechanism. Generally, Layer 3 tunneling schemes assume that an address has already been assigned prior to initiation of the tunnel. Schemes for assignment of addresses in IPSec tunnel mode are currently under development and are not yet available.
- **Data compression**. Layer 2 tunneling protocols support PPP-based compression schemes. For example, the Microsoft implementations of both PPTP and L2TP use Microsoft Point-to-Point Compression (MPPC). The IETF is investigating similar mechanisms (such as IP Compression) for the Layer 3 tunneling protocols.
- **Data encryption**. Layer 2 tunneling protocols support PPP-based data encryption mechanisms. The Microsoft implementation of PPTP supports optional use of Microsoft Point-to-Point Encryption (MPPE), based on the RSA/RC4 algorithm. Layer 3 tunneling protocols can use similar methods; for example, IPSec defines several optional data encryption methods, which are negotiated during the IKE exchange. The Microsoft implementation of the L2TP protocol uses IPSec encryption to protect the data stream from the VPN client to the VPN server.
- **Key Management**. MPPE, a Layer 2 encryption mechanism, relies on the initial key generated during user authentication, and then refreshes it periodically. IPSec explicitly negotiates a common key during the IKE exchange, and also refreshes it periodically.
- **Multi-protocol support**. Layer 2 tunneling supports multiple payload protocols, which makes it easy for tunneling clients to access their corporate networks using IP, IPX, NetBEUI, and so on. In contrast, Layer 3 tunneling protocols, such as IPSec tunnel mode, typically support only target networks that use the IP protocol.

3. Virtual private network – characteristics

3.1 Types of VPN

a. Hardware based VPN Systems

Hardware-based VPN systems are encrypting routers. They are secure and easy to use. They provide the nearest thing to "plug and play" encryption equipment available. They provide the highest network throughput of all VPN systems. They don't waste processor overhead in running an operating system or other applications. However, they may not be as flexible as software-based systems. The best hardware VPN packages offer software-only clients for remote installation, and incorporate some of the access control features more traditionally managed by firewalls or other perimeter security devices.

b. Firewall based VPN Systems

Firewall-based VPNs take advantage of the firewall's security mechanisms, including restricting access to the internal network. They also perform address translation, satisfy requirements for strong authentication; and serve up real-time alarms and extensive logging. Most commercial firewalls also "harden" the host operating system kernel by stripping out dangerous, unnecessary services, providing additional security for the VPN server. OS protection is a major plus, since very few VPN application vendors supply guidance on OS security. Performance may be a concern, especially if the firewall is already loaded. However, some firewall vendors offer hardware-based encryption processors to minimize the impact of VPN management on the system.

c. Software based VPN Systems

Software-based VPNs are ideal in situations where both endpoints of the VPN are not controlled by the same organization (typical for client support requirements or business partnerships), or when different firewalls and routers are implemented within the same organization. At the moment, software VPNs offers the most flexibility in how network traffic is managed. Many software-based products allow traffic to be tunneled based on address or protocol, unlike hardware-based products, which generally tunnel all traffic they handle. In situations where performance requirements are modest (such as users connecting over dial-up links),software-based VPNs may be the best choice. But software-based systems are generally harder to manage than encrypting routers. They require familiarity with the host operating system, the application itself, and appropriate security mechanisms. And some software VPN packages require changes to routing tables and network addressing schemes.

3.2 VPN Benefits

a. Cost Savings with a VPN

A VPN can save organization money in several situations:

1. VPNs vs. leased lines

Organizations historically needed to rent network capacity such as T1, E1 lines to achieve full, secured connectivity between their office locations. With a VPN, you use public network infrastructure including the Internet to make these connections and tap into that virtual network through much cheaper local leased lines or even just broadband connections to a nearby Internet Service Provider (ISP).

2. Long distance phone charges

A VPN also can replace remote access servers and long-distance dialup network connections commonly used in the past by business travellers needing to access to their company intranet. For example, with an Internet VPN, clients need only connect to the nearest service provider's access point that is usually local.

3. Support costs

With VPNs, the cost of maintaining servers tends to be less than other approaches because organizations can outsource the needed support from professional third-party service providers. This provides a much lower cost structure through economy of scale by servicing many business clients.

b. VPN Network Scalability

The cost to an organization of building a dedicated private network may be reasonable at first but increases exponentially as the organization grows. A company with two branch offices, for example, can deploy just one dedicated line to connect the two locations, but 4 branch offices require 6 lines to directly connect them to each other, 6 branch offices need 15 lines, and so on.

Internet based VPNs avoid this scalability problem by simply tapping into the public lines and network capability readily available. Particularly for remote and international locations, an Internet VPN offers superior reach and quality of service.

3.3 VPN Limitations

a. VPNs require detailed understanding of network security issues and careful installation / configuration to ensure sufficient protection on a public network like the Internet.

b. The reliability and performance of an Internet-based VPN is not under an organization's direct control. Instead, the solution relies on an ISP and their quality of service.

c. VPN technologies from different vendors may not work well together due to immature standards. Attempting to mix and match equipment may cause technical problems, and using equipment from one provider may not give as great a cost savings.

d. VPNs need to accommodate protocols other than IP and existing ("legacy") internal network technology.

Conclusion

VPNs are increasingly becoming an everyday part of life on the Internet. Many people use them to gain access to many of the systems in their offices, such as e-mail and intranets. This trend is certain to become more popular as many companies are finding it cheaper for their employees to work from home, relieving them of the need to lease additional office space.

Site-to-site VPNs will also continue to be deployed as companies, both small and large find it increasingly necessary to share access to their business systems. One notable area is in the realm of IP telephony, where VPNs enable all remote offices to use a single IP switchboard at the center of a VPN hub and spoke network. Intra-office communication is therefore encrypted and the use of a single switchboard saves costs. Knowledge of VPNs is now indispensable for systems administrators.

Because this topic encompasses aspects of protocols, encryption, methods of communication, synchronization and security, VPN technology it is already a field of study in itself.

References

1. http://ro.wikipedia.org/wiki/Virtual_private_network
2. http://technet.microsoft.com/en-us/library/bb742566.aspx
3. http://www.clavister.com/manuals/ver8x/manual/vpn/vpn_overview.htm
4. http://compnetworking.about.com/od/vpn/a/vpn_tutorial.htm
5. http://www.vpnc.org/vpn-technologies.html
6. http://en.wikipedia.org/wiki/OpenVPN
7. http://en.wikipedia.org/wiki/IPSEC
8. http://en.wikipedia.org/wiki/Transport_Layer_Security
9. http://en.wikipedia.org/wiki/PPTP
10. http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol

WIRELESS NETWORK SECURITY

1st LT Ana Maria TAMAS

UM 01495 Cincu

Introduction

In today's business environment, controlling access to data is critical to long-term business survivability. Wireless is widely used because of the benefits it offers in its improved productivity, efficiency and cost effectiveness. The broad range of wireless technologies is no exception - such technologies allow for access to information outside an organization's normal perimeter.

Wireless signals are broadcast in an open and easily detected manner and will often travel well beyond the organization's physical security perimeter. As these technologies gain wider acceptance in the marketplace and increased adoption in the organization, these security risks require attention by the right people and at the right levels within your organization.

The widespread reliance on networking in business as well as the growth of the Internet and online services are strong testimonies to the benefits of shared data and resources. Wireless solutions advance these benefits by allowing users to access shared information, e-mail, and applications without the constraints of a wired connection. Further, wireless technology allows network managers to set up or augment networks without installing or moving wires. Almost all computing devices, including desktops, workstations, monitors, keyboards, notebooks, tablets, handhelds, and printers can be equipped to communicate wirelessly.

The availability of simple-to-use, more secure, wireless solutions have created the opportunity to reduce costs and improve performance. Business problems once thought of as "business as usual" are now being solved with wireless.

Wireless networks extend core networks, provides greater utilization of existing assets. Up-front expenses of the wireless network can be recovered in several cost saving areas; for example, dynamic environments requiring frequent moves and changes, adding network service to a new or temporary office, and adding connectivity to meeting rooms.

Wireless systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

1. Wireless networks technologies

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

Wireless Networks. Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range:

- Wireless Wide Area Networks (WWAN)
- Wireless Local Area Networks (WLAN)
- Wireless Personal Area Networks (WPAN)

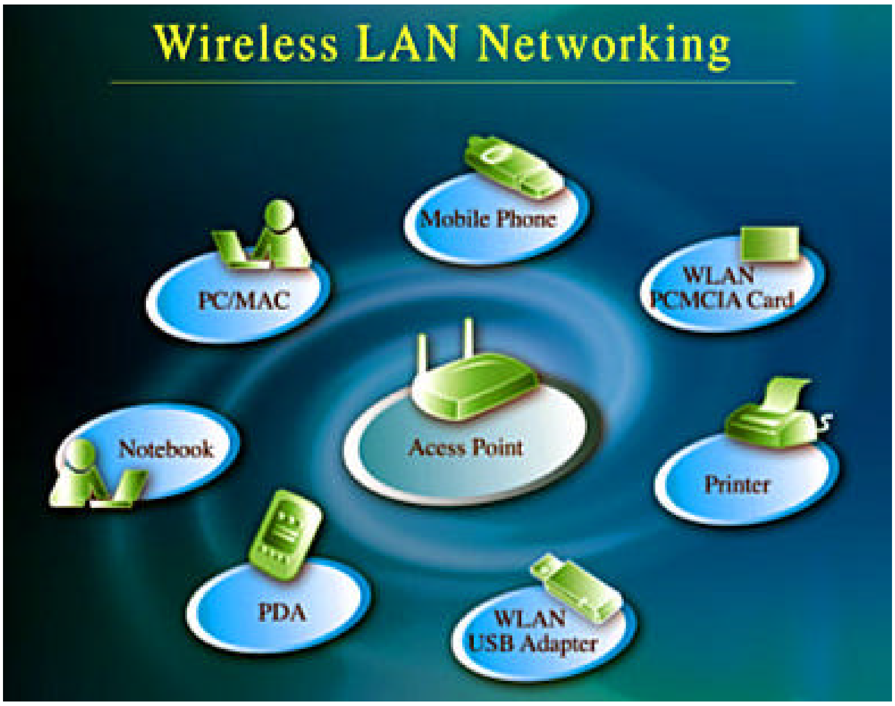
WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), and Global System for Mobile Communications (GSM). WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN represents wireless personal area network technologies such as Bluetooth and IR. All of these technologies are "tether-less" - they receive and transmit information using electromagnetic (EM) waves.

Although wireless LANs and wireless WANs may appear to be competing technologies, they are far more useful as complementary technologies. Used together, a user would have the best of both technologies, offering high-speed wireless access in a campus area, and access to all their data and applications with high-speed cellular access from anywhere with wireless WAN network coverage.

1.1. Wireless Local Area Network – WLAN

A wireless local area network (Wireless LAN) is a computer network that allows a user to connect without the need for a network cable. A laptop or PDA equipped with a wireless LAN card lets a user move around a building with their computer and stay connected to their network without needing to "plug in" with a cable. The most popular wireless LAN today is called an 802.11b network.

A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter. The coverage of a wireless access point can be up to 100 m (330 feet) indoors.



Wireless LANs are used in office buildings, on college campuses, or in houses, allowing multiple users shared access to one Internet connection. Some airports also plan to, or already offer wireless LAN access. Coffee shops, for example, are beginning to equip their shops with wireless LANs, which will allow laptop users to connect to the Internet.

WLANs provide wireless network communication over short distances using radio or infrared signals instead of traditional network cabling.

Network security remains an important issue for WLANs. Random wireless clients must usually be prohibited from joining the WLAN. Technologies like WEP raise the level of security on wireless networks to rival that of traditional wired networks.

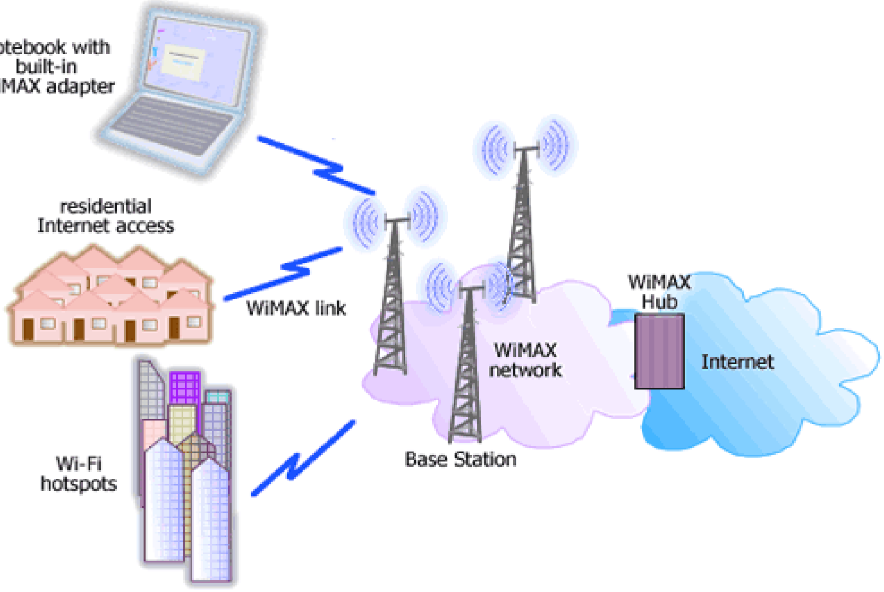
1.2. Wireless Metropolitan Area Network - WMAN

Wireless Metropolitan Area Network (WMAN) is a computer network usually spanning a campus or a city, which typically connect a few local area networks using high speed backbone technologies. A MAN often provides efficient connections to a wide area network (WAN). There are three important features which discriminate MANs from LANs or WANs:

- The network size falls intermediate between LANs and WANs. A MAN typically covers an area of between 5 and 50 km range. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings.
- A MAN (like a WAN) is not generally owned by a single organization. The MAN, its communications links and equipment are generally owned by either a consortium of users or by a network service provider who sells the service to the users.
- A MAN often acts as a high speed network to allow sharing of regional resources. It is also frequently used to provide a shared connection to other networks using a link to a WAN.

This network enables you to access the Internet via a wireless wide area network (WWAN) access card and a PDA or laptop.

These networks provide a very fast data speed compared with the data rates of mobile telecommunications technology, and their range is also extensive. Cellular and mobile networks based on CDMA and GSM are good examples of WWAN. The WMAN technology uses the 802.16a standard that will provide broadband wireless connectivity to Fixed, Portable and Nomadic devices.



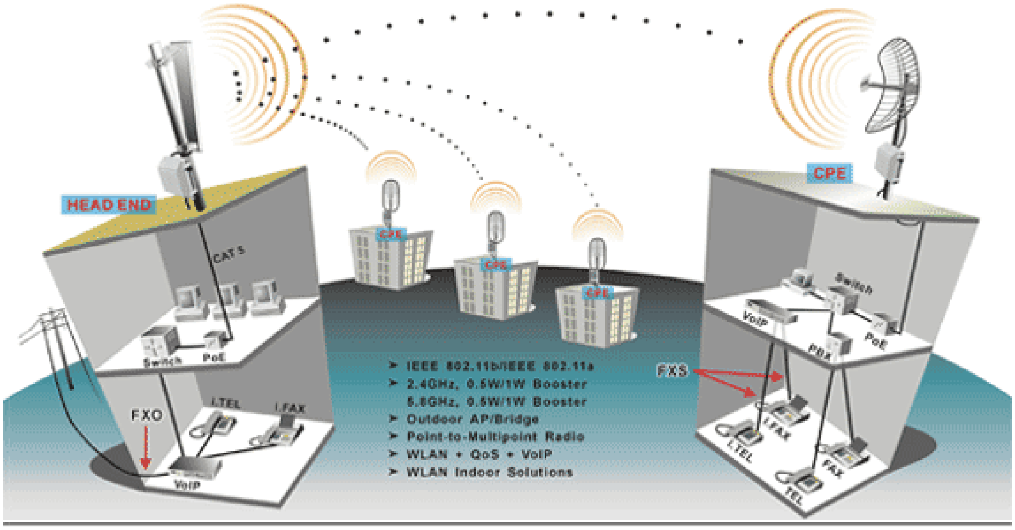
1.3. Wireless Wide Area Network – WWAN

A wireless wide area network (Wireless WAN) covers a much more extensive area than wireless LANs. Coverage is generally offered on a nationwide level with wireless network infrastructure provided by a wireless service carrier (for a monthly usage fee, similar to a cellular phone subscription).

While wireless LANs are used to allow network users to be mobile within a small fixed area, wireless WANs are used to give Internet connectivity over a much broader coverage area, for mobile users such as business travelers or field service technicians. Wireless WANs allow users to have access to the Internet, e-mail, and corporate applications and information even while away from their office.

Wireless WANs use cellular networks for data transmission and examples of the cellular systems that are used are: CDMA, GSM, GPRS and CDPD. A portable computer with a wireless WAN modem connects to a base station on the wireless networks via radio waves. The radio tower then carries the signal to a mobile switching center, where the data is passed on to the appropriate network. Using the wireless service provider's connection to the Internet, data communications are established to an organization's existing network.

Wireless WANs use existing cellular telephone networks, so there is also the option of making voice calls over a wireless WAN. Both cellular telephones and wireless WAN PC Cards have the ability to make voice calls as well as pass data traffic on wireless WAN networks.

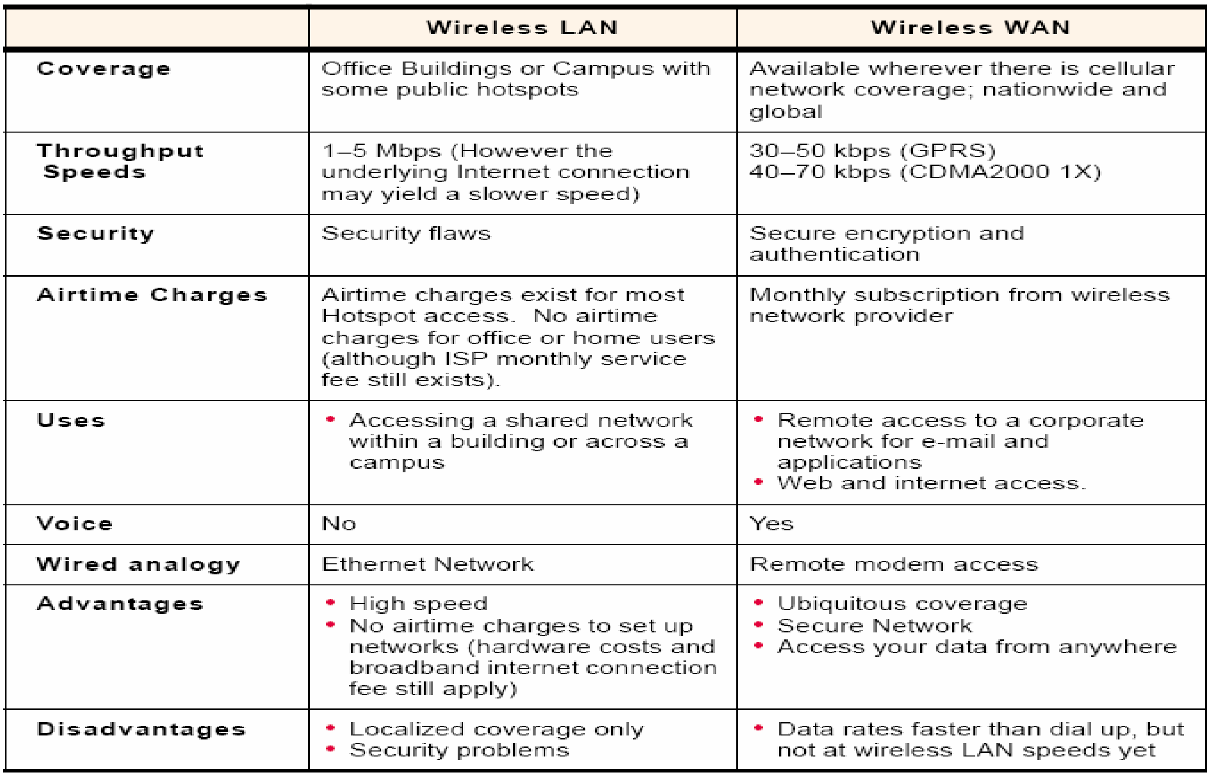


A wired analogy of these complimentary technologies would be as follows: A user would plug their laptop (with built in network adapter) into a wired LAN connection while they are in the office. This gives them high-speed access to their e-mail, applications, data and the web. When they leave the office and work from home, or on the road at their hotel, they would use their dial up modem to have remote access to their e-mail, applications, and the web.

In the wireless example, the same user has a laptop with built-in wireless LAN access. This wireless LAN access is used for high-speed access to applications while in the office. Once out of the office, traveling to a local customer site, completing a work order in the field, or accessing e-mail from a hotel or airport, there is no longer any access to an 802.11 network. The wireless WAN card is now used to access a cellular provider's network and obtain secure, remote access to e-mail, applications and the web.

Since many computers are now coming with wireless LAN devices built in, having a wireless WAN PC Card inserted into the computer would ensure that users can have high-speed wireless access where it is available, but still be able to access their important data with their wireless WAN card wherever there is cellular network coverage.

The following table summarizes the main differences between wireless LAN and Wireless WAN.



	Wireless LAN	Wireless WAN
Coverage	Office Buildings or Campus with some public hotspots	Available wherever there is cellular network coverage; nationwide and global
Throughput Speeds	1–5 Mbps (However the underlying Internet connection may yield a slower speed)	30–50 kbps (GPRS) 40–70 kbps (CDMA2000 1X)
Security	Security flaws	Secure encryption and authentication
Airtime Charges	Airtime charges exist for most Hotspot access. No airtime charges for office or home users (although ISP monthly service fee still exists).	Monthly subscription from wireless network provider
Uses	• Accessing a shared network within a building or across a campus	• Remote access to a corporate network for e-mail and applications • Web and internet access.
Voice	No	Yes
Wired analogy	Ethernet Network	Remote modem access
Advantages	• High speed • No airtime charges to set up networks (hardware costs and broadband internet connection fee still apply)	• Ubiquitous coverage • Secure Network • Access your data from anywhere
Disadvantages	• Localized coverage only • Security problems	• Data rates faster than dial up, but not at wireless LAN speeds yet

2. Wireless standards used in wireless networks

Wireless LANs based on the IEEE 802.11 or Wi-Fi standards have been a resounding success, and now the focus in wireless is shifting to the wide area. While Wi-Fi has virtually obliterated all other contenders in the local area, the wide area market is still up for grabs.

The cellular carriers got into the market first with their 2.5G/3G data services, but their offerings are positioned as an add-on to what is essentially a voice service. Sales have been lackluster to say the least. The real challenge to the cellular data services will come from the two emerging data-oriented technologies, WiMax and Mobile-Fi. With chip-level components due for shipment in the last quarter of 2004, WiMax will be the next to debut.

WiMax, short for Worldwide Interoperability for Microwave Access, is defined in IEEE 802.16 standards, and is being promoted by the WiMax Forum. The Forum looks to develop interoperability test suites to insure a multi-vendor solution that will result in lower cost products based on open standards. Internationally, a European Telecommunications Standards Institute (ETSI) initiative called HIPERMAN addresses the same area as WiMax/802.16 and shares some of the same technology.

With increased market recognition for WiMax, it is now regularly compared with Wi-Fi. While the two do indeed share some fundamental technical characteristics, they are approaching the wireless space from completely different perspectives. Further, different design approaches will make it unlikely that the two will actually compete except by coincidence. The purpose of this paper is to provide a technical and market comparison of the Wi-Fi and WiMax technologies highlighting their similarities and fundamental differences, and to identify the applications each will address in the coming years.

2.1. 802.11 – Wi-Fi (Wireless Fidelity)

Wi-Fi is a trademark of the Wi-Fi Alliance that may be used with certified products that belong to a class of wireless local area network (WLAN) devices based on the IEEE 802.11 standards. Because of the close relationship with its underlying standard, the term Wi-Fi is often used as a synonym for IEEE 802.11 technology.

A Wi-Fi enabled device such as a personal computer, video game console, mobile phone, MP3 player or personal digital assistant can connect to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more interconnected access points — called a hotspot — can comprise an area as small as a few rooms or as large as many square miles covered by a group of access points with overlapping coverage.

IEEE 802.11 is a set of standards carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802).

The 802.11 family includes over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. Security was originally purposefully weak due to export requirements of some governments, and was later enhanced via the 802.11i amendment after governmental and legislative changes. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and equipment may occasionally suffer interference from microwave ovens, cordless telephones and Bluetooth devices. Both 802.11 and Bluetooth control their interference and susceptibility to interference by using spread spectrum modulation. Bluetooth uses a frequency hopping spread spectrum signaling method (FHSS), while 802.11b and 802.11g use the direct sequence spread spectrum signaling (DSSS) and orthogonal frequency division multiplexing (OFDM) methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 19 non-overlapping channels rather than the 3 offered in the 2.4 GHz ISM frequency band. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.

The used segment of the radio frequency spectrum varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six (802.11b) fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.

2.2. 802.16 – WiMAX (Worldwide Interoperability for Microwave Access)

WiMAX (Worldwide Interoperability for Microwave Access) is designed to deliver next-generation, high-speed mobile voice and data services and wireless “last-mile” backhaul connections that could potentially displace a great deal of existing radio air network (RAN) infrastructure. For network providers, this will enable an expansive array of multimedia and real-time subscriber services that go well beyond current 2.5/3G applications, including mobile streaming media services, mobile TV, Unified Communications, and Voice over IP (VoIP), which, for the first time, becomes practical and viable on a metro-wide scale through WiMAX.

Network service providers can’t take full advantage of mobile voice and multimedia over IP unless there is the potential to manage Quality of Service (QoS). With this in mind, five distinct classes of service quality have been built into WiMAX, allowing a more robust and resilient connection for users who require time-sensitive applications and service level agreements (SLAs).

WiMAX can offer a large wireless access network footprint to subscribers (similar to data-enabled cellular services such as UMTS/CDMA), while at the same time providing higher throughputs that are similar to WLAN networks. With its large footprint, high access speeds, built-in QoS and SLA capabilities, WiMAX is an ideal access network for next-generation converged voice and data services and streaming wireless multimedia.

The technology provides up to 10 Mbps broadband speed without the need for cables. The technology is based on the IEEE 802.16 standard (also called Broadband Wireless Access).

The terms "WiMAX", "mobile WiMAX", "802.16d" and "802.16e" are frequently used incorrectly. Correct definitions are the following:

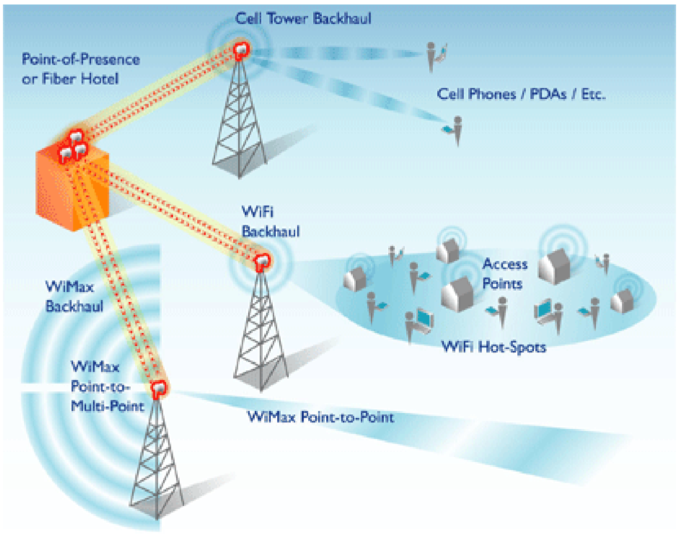
- 802.16-2004 is often called 802.16d, since that was the working party that developed the standard. It is also frequently referred to as "fixed WiMAX" since it has no support for mobility.
- 802.16e-2005 is an amendment to 802.16-2004 and is often referred to in shortened form as 802.16e. It introduced support for mobility, among other things and is therefore also known as "mobile WiMAX".

WiMAX is a possible replacement candidate for cellular phone technologies such as GSM and CDMA, or can be used as an overlay to increase capacity. It has also been considered as a wireless backhaul technology for 2G, 3G and 4G networks in both developed and poor nations.

As a standard intended to satisfy needs of next-generation data networks (4G), 802.16e is distinguished by its dynamic burst algorithm modulation adaptive to the physical environment the RF signal travels through. Modulation is chosen to be spectroscopically more efficient (more bits per OFDM/SOFDMA symbol). That is, when the bursts have a high signal strength and a carrier to noise plus interference ratio (CINR), they can be more easily decoded using digital signal processing (DSP). In contrast, operating in less favorable environments for RF communication, the system automatically steps down to a more robust mode (burst profile) which means fewer bits per OFDM/SOFDMA symbol; with the advantage that power per bit is higher and therefore simpler accurate signal processing can be performed.

A commonly-held misconception is that WiMAX will deliver 70 Mbps over 50 kilometers (30 miles). In reality, WiMAX can either operate at higher bitrates or over longer distances but not both: operating at the maximum range of 50 km increases bit error rate and thus results in a much lower bitrate. Conversely, reducing the range (to under 1 km) allows a device to operate at higher bitrates. There are no known examples of WiMAX services being delivered at bit rates over around 40 Mbps.

Like most wireless systems, available bandwidth is shared between users in a given radio sector, so performance could deteriorate in the case of many active users in a single sector. In practice, most users will have a range of 2-3 Mbps services and additional radio cards will be added to the base station to increase the number of users that may be served as required.



Future development. The IEEE 802.16m standard is the core technology for the proposed Mobile WiMAX Release 2, which enables more efficient, faster, and more converged data communications. The IEEE 802.16m standard has been submitted to the ITU for IMT-Advanced standardization. IEEE 802.16m is one of the major candidates for IMT-Advanced technologies by ITU. Among many enhancements, IEEE 802.16m systems can provide four times faster data speed than the current Mobile WiMAX Release 1 based on IEEE 802.16e technology.

Mobile WiMAX Release 2 will provide strong backward compatibility with Release 1 solutions. It will allow current Mobile WiMAX operators to migrate their Release 1 solutions to Release 2 by upgrading channel cards or software of their systems. Also, the subscribers who use currently available Mobile WiMAX devices can communicate with new Mobile WiMAX Release 2 systems without difficulty.

It is anticipated that in a practical deployment, using 4X2 MIMO in the urban microcell scenario with only a single 20-MHz TDD channel available system wide, the 802.16m system can support both 120 Mbps downlink and 60 Mbps uplink per site simultaneously. It is expected that the WiMAX Release 2 will be available commercially in the 2011-2012 timeframe.

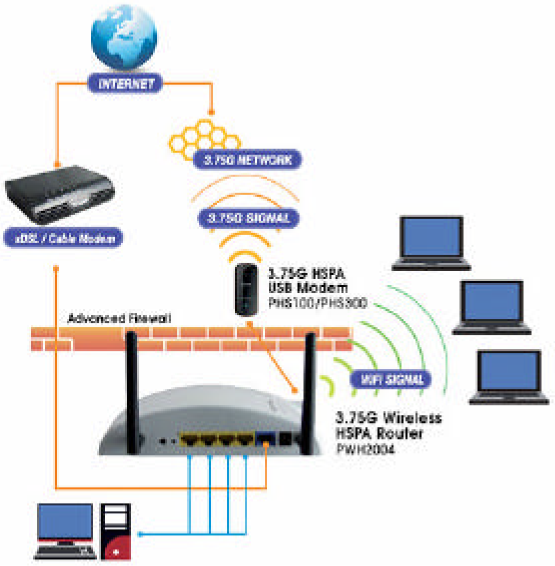
The goal for the long-term evolution of WiMAX is to achieve 100 Mbps mobile and 1 Gbps fixed-nomadic bandwidth as set by ITU for 4G NGMN (Next Generation Mobile Network).

Comparison with Wi-Fi. Comparisons and confusion between WiMAX and Wi-Fi are frequent because both are related to wireless connectivity and Internet access:

- WiMAX is a long range system, covering many kilometers, that uses licensed or unlicensed spectrum to deliver a point-to-point connection to the Internet;
- Different 802.16 standards provide different types of access, from portable (similar to a cordless phone) to fixed (an alternative to wired access, where the end user's wireless termination point is fixed in location);
- Wi-Fi uses unlicensed spectrum to provide access to a network;
- Wi-Fi is more popular in end user devices;
- WiMAX and Wi-Fi have quite different quality of service (QoS) mechanisms:
    - WiMAX uses a QoS mechanism based on connections between the base station and the user device. Each connection is based on specific scheduling algorithms.
    - Wi-Fi has a QoS mechanism similar to fixed Ethernet, where packets can receive different priorities based on their tags. For example VoIP traffic may be given priority over web browsing.
- Wi-Fi runs on the Media Access Control's CSMA/CA protocol, which is connectionless and contention based, whereas WiMAX runs a connection-oriented MAC;
- Both 802.11 and 802.16 define Peer-to-Peer (P2P) and ad hoc networks, where an end user communicates to users or servers on another Local Area Network (LAN) using its access point or base station.

2.3. 3G and 4G

International Mobile Telecommunications - 2000 (IMT-2000), better known as **3G** or **3rd Generation**, is a family of standards for mobile telecommunications defined by the International Telecommunication Union, which includes GSM EDGE, UMTS, and CDMA2000 as well as DECT and WiMAX. Services include wide-area wireless voice telephone, video calls, and wireless data, all in a mobile environment. Compared to 2G and 2.5G services, 3G allows simultaneous use of speech and data services and higher data rates (up to 14.0 Mbps on the downlink and 5.8



Mbps on the uplink with HSPA+). Thus, 3G networks enable network operators to offer users a wider range of more advanced services while achieving greater network capacity through improved spectral efficiency.

Security. 3G networks offer a greater degree of security than 2G predecessors. By allowing the UE (User Equipment) to authenticate the network it is attaching to, the user can be sure the network is the intended one and not an impersonator. 3G networks use the KASUMI block crypto instead of the older A5/1 stream cipher. However, a number of serious weaknesses in the KASUMI cipher have been identified.

In addition to the 3G network infrastructure security, end-to-end security is offered when application frameworks such as IMS are accessed, although this is not strictly a 3G property.

Applications. The bandwidth and location information available to 3G devices gives rise to applications not previously available to mobile phone users. Some of the applications are:

- Mobile TV - a provider redirects a TV channel directly to the subscriber's phone where it can be watched.
- Video on demand - a provider sends a movie to the subscriber's phone.
- Video conferencing - subscribers can see as well as talk to each other.
- Tele-medicine - a medical provider monitors or provides advice to the potentially isolated subscriber.
- Location-based services - a provider sends localized weather or traffic conditions to the phone, or the phone allows the subscriber to find nearby businesses or friends.

2G networks were built mainly for voice services and slow data transmission.

From 2G to 2.5G. The first major step in the evolution to 3G occurred with the introduction of General Packet Radio Service (GPRS). So the cellular services combined with GPRS became *"2.5G"*.

GPRS could provide data rates from 56 kbps up to 114 kbps. It can be used for services such as Wireless Application Protocol (WAP) access, Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access. GPRS data transfer is typically charged per megabyte of traffic transferred, while data communication via traditional circuit switching is billed per minute of connection time, independent of whether the user actually is utilizing the capacity or is in an idle state.

From 2.5G to 2.75G (EDGE). GPRS networks evolved to EDGE networks with the introduction of 8PSK encoding. Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC) is a backward-compatible digital mobile phone technology that allows improved data transmission rates, as an extension on top of standard GSM. EDGE was deployed on GSM networks beginning in 2003 - initially by Cingular (now AT&T) in the United States.

EDGE is standardized by 3GPP as part of the GSM family, and it is an upgrade that provides a potential three-fold increase in capacity of GSM/GPRS networks. The specification achieves higher data-rates by switching to more sophisticated methods of coding (8PSK), within existing GSM timeslots.

Evolution towards 4G. Both 3GPP and 3GPP2 are currently working on further extensions to 3G standards, named Long Term Evolution and Ultra Mobile Broadband, respectively. Being based on an all-IP network infrastructure and using advanced wireless technologies such as MIMO, these specifications already display features characteristic for IMT-Advanced (4G), the successor of 3G. However, falling short of the bandwidth requirements for 4G (which is 1 Gbps for stationary and 100 Mbps for mobile operation), these standards are classified as 3.9G or Pre-4G.

3GPP plans to meet the 4G goals with LTE Advanced, whereas Qualcomm has halted development of UMB in favour of the LTE family.

4G refers to the fourth generation of cellular wireless standards. It is a successor to 3G and 2G standards, with the aim to provide a wide range of data rates up to ultra-broadband (gigabit-speed) Internet access to mobile as well as stationary users. Although 4G is a broad term that has had several different and more vague definitions, this article uses 4G to refer to IMT Advanced (International Mobile Telecommunications Advanced), as defined by ITU-R.

A 4G cellular system must have target peak data rates of up to approximately 100 Mbps for high mobility such as mobile access and up to approximately 1 Gbps for low mobility such as nomadic/local wireless access, according to the ITU requirements. Scalable bandwidths up to at least 40 MHz should be provided. A 4G system is expected to provide a comprehensive and secure all-IP based solution where facilities such as IP telephony, ultra-broadband Internet access, gaming services and HDTV streamed multimedia may be provided to users.

4G is being developed to accommodate the QoS and rate requirements set by further development of existing 3G applications like wireless broadband access, Multimedia Messaging Service (MMS), video chat, mobile TV, but also new services like HDTV content, minimal services like voice and data, and other services that utilize bandwidth. It may be allowed roaming with wireless local area networks, and be combined with digital video broadcasting systems.

The 4G working group has defined the following as objectives of the 4G wireless communication standard:

- Flexible channel bandwidth, between 5 and 20 MHz, optionally up to 40 MHz.
- A nominal data rate of 100 Mbps while the client physically moves at high speeds relative to the station, and 1 Gbps while client and station are in relatively fixed positions as defined by the ITU-R.
- A data rate of at least 100 Mbps between any two points in the world.
- Peak link spectral efficiency of 15 bps/Hz in the downlink, and 6.75 bps/Hz in the uplink (meaning that 1000 Mbps in the downlink should be possible over less than 67 MHz bandwidth).
- System spectral efficiency of up to 3 bps/Hz/cell in the downlink and 2.25 bps/Hz/cell for indoor usage.
- Smooth handoff across heterogeneous networks.
- Seamless connectivity and global roaming across multiple networks.
- High quality of service for next generation multimedia support (real time audio, high speed data, HDTV video content, mobile TV, etc.).
- Interoperability with existing wireless standards.
- An all IP, packet switched network.

2.4. Comparison of Mobile Internet Access methods

Comparison of Mobile Internet Access methods

Standard	Family	Primary Use	Radio Tech	Downlink (Mbps)	Uplink (Mbps)	Notes
LTE	UMTS/ 4GSM	General 4G	OFDMA/ MIMO/SC -FDMA	360	80	LTE-Advanced update expected to offer peak rates of at least 1 Gbps fixed speeds and 100 Mbps to mobile users.
WiMAX	802.16e	Mobile Internet	MIMO-SOFDMA	144	35	WiMAX update IEEE 802.16m expected offer up to 1 Gbps fixed speeds.
Flash-OFDM	Flash-	Mobile	Flash-	5.3	1.8	Mobile range

	OFDM	Internet mobility up to 200mph (350km/h)	OFDM	10.6 15.9	3.6 5.4	18miles (30km) extended range 34 miles (55km)
HIPERMAN	HIPERMAN	Mobile Internet	OFDM	56.9	56.9	
Wi-Fi	802.11 (11n)	Mobile Internet	OFDM/MIMO	288.9 (Supports 600Mbps @ 40MHz channel width)		Antenna, RF front end enhancements and minor protocol timer tweaks have helped deploy long range P2P networks compromising on radial coverage, throughput and/or spectra efficiency (310km & 382km).
iBurst	802.20	Mobile Internet	HC-SDMA/TDD/MIMO	95	36	Cell Radius: 3–12 km Speed: 250kmph Spectral Efficiency: 13 bits/s/Hz/cell Spectrum Reuse Factor: "1"
EDGE Evolution	GSM	Mobile Internet	TDMA/FDD	1.9	0.9	3GPP Release 7
UMTS **W-CDMA** **HSDPA+** **HSUPA** **HSPA+**	UMTS/ 3GSM	General 3G	CDMA/FDD CDMA/FDD/MIMO	0.384 14.4 42	0.384 5.76 11.5	HSDPA widely deployed. Typical downlink rates today 2 Mbps, ~200 kbps uplink; HSPA+ downlink up to 42 Mbps.
UMTS-TDD	UMTS/ 3GSM	Mobile Internet	CDMA/TDD	16	16	Reported speeds according to IPWireless using 16QAM modulation similar to HSDPA+HSUPA
1xRTT	CDMA 2000	Mobile phone	CDMA	0.144	0.144	Succeeded by EV-DO
EV-DO 1x Rev. 0 **EV-DO 1x Rev.A** **EV-DO Rev.B**	CDMA 2000	Mobile Internet	CDMA/FDD	2.45 3.1 4.9xN	0.15 1.8 1.8xN	Rev B note: N is the number of 1.25 MHz chunks of spectrum used. Not yet deployed.

3. Wireless security: risks and defenses

Security is one of the most important features when using a wireless network. Security is one of the biggest strengths for cellular wireless networks (WWANs) and one of the biggest weaknesses in 802.11 networks (WLANs). 802.11b networks have several layers of security; however there are weaknesses in all of these security features. The first level of security is to have wireless LAN authentication done using the wireless adapter’s hardware (MAC) address.

Security can be increased on wireless LANs by using shared key authentication. This shared key must be delivered through a secure method other than the 802.11 connection. In practice, this key is manually configured on the access point and client, which is not efficient on a large network with many users. This shared key authentication is not considered secure and is not recommended to ensure security.

Another weakness in an 802.11 network is the difficulty in restricting physical access to the network, because anyone within range of a wireless access point can send, receive, or intercept frames. WEP (Wired Equivalency Protocol) was designed to provide security equivalent to a wired network by encrypting the data sent between a wireless client and an access point.

However, key management is a significant problem with WEP. WEP keys must be distributed via a secure channel other than 802.11. The key is normally a text string that needs to be manually configured on the wireless access point and wireless clients, which is not practical to a large network. There is also no mechanism to change the WEP key regularly or periodically, so all wireless access points and clients use the same manually configured WEP. With several wireless clients sending large amounts of data, without changing the WEP key, it is possible to intercept data traffic and determine the WEP key. This would allow a hacker to intercept and decrypt the data traffic.

Another problem that has been reported with wireless LANs is that when the security features are turned on, there are problems with interoperability between wireless LAN modules from one vendor and wireless LAN access points from another vendor.

Wireless LANs were designed specifically to operate in the 2.4 GHz band, which is a globally allocated frequency for unlicensed operation. This means that there is no requirement to be a licensed operator to run a wireless LAN in this frequency. A wireless WAN however operates in tightly regulated frequency spectrums and all operators must be licensed to operate in this frequency. This implies much better data security and protection, since licensed operators have to follow government regulations for wireless access.

In contrast to the security weaknesses in 802.11 networks, cellular wireless WAN networks are extremely secure. These networks incorporate military technology and sophisticated encryption and authentication methods.

3.1. Types of Security

WEP (Wired Equivalent Privacy). Developed in the late 1990s, WEP is a basic protocol that is sometimes overlooked by wireless administrators because of its numerous vulnerabilities. The original implementations of WEP used 64-bit. By means of a Brute Force attack, 64-bit WEP can be broken in a matter of minutes, whereas the stronger 128-bit version will take hours. It’s not the best line of defense against unauthorized intruders but better than nothing and mainly used by the average home user. One of the drawbacks of WEP is that since it uses a shared key, if someone leaves the company then the key will have to be changed on the access point and all client machines.

WEP2 (Wired Equivalent Privacy version 2). In 2004, the IEEE proposed an updated version of WEP; WEP2 to address its predecessor’s shortcomings. Like WEP it relies on the RC4 algorithm but instead uses a 128-bit initialization vector making it stronger than the original version of WEP, but may still be susceptible to the same kind of attacks.

WPA (Wi-Fi Protected Access). WPA provides encryption via the Temporary Key Integrity Protocol (TKIP) using the RC4 algorithm. It is based on the 802.1X protocol and addresses the weaknesses of WEP by providing enhancements such as Per-Packet key construction and distribution, a message integrity code feature and a stronger IV (Initialization Vector). The downside of WPA is that unless the current hardware supports WPA by means of a firmware upgrade, you will most likely have to purchase new hardware to enjoy the benefits of this security method. The length of a WPA key is between 8 and 63 characters – the longer it is the more secure it is.

WPA2 (Wi-Fi Protected Access version 2). Based on the 802.11i standard, WPA2 was released in 2004 and uses a stronger method of encryption – AES (Advanced Encryption Standard). AES supports key sizes of 128 bits, 192 bits, and 256 bits. It is backward compatible with WPA and uses a fresh set of keys for every session, so essentially every packet that sent over the air is encrypted with a unique key. As did WPA, WPA2 offers two versions – Personal and Enterprise. Personal mode requires only an access point and uses a pre-shared key for authentication and Enterprise mode requires a RADIUS authentication server and uses EAP.

MAC Address Filtering. MAC Address Filtering is a means of controlling which network adapters have access to the access point. A list of MAC Addresses is entered into the access point and anyone whose MAC address on the wireless network adapter does not match an entry in the list will not be permitted entry. This is a pretty good means of security when also used with a packet encryption method. However, keep in mind that MAC addresses can be spoofed. This type of security is usually used as a means of authentication, in conjunction with something like WEP for encryption.

SSID (Service Set Identifier). An SSID, or Network Name, is a "secret" name given to a wireless network. By default, the SSID is a part of every packet that travels over the WLAN. Unless you know the SSID of a wireless network you cannot join it. Every network node must be configured with the same SSID of the access point that it wishes to connect, which becomes a bit of a headache for the network administrator.

VPN (Virtual Private Network) Link. Perhaps the most reliable form of security would be to setup a VPN connection over the wireless network. VPNs have for long been a trusted method of accessing the corporate network over the internet by forming a secure tunnel from the client to the server. Setting up a VPN may affect performance due to the amount of data encryption involved. The VPN option is preferred by many enterprise administrators because VPNs offer the best commercially available encryption. VPN software uses advanced encryption mechanisms (AES for example), which makes decrypting the traffic a very hard, if not impossible, task.

3.2. Risks/Vulnerabilities

In addition to all the vulnerabilities common to wired networks, wireless LANs introduce a new series of risks. The critical vulnerabilities are eavesdropping, illicit entry into the network and denial of service. Some users may perceive they are at risk from being exposed to radio wave energy, but there is no credible research supporting this thesis, and US FCC Part 15 certification requires that devices meet the government standard for exposure.

Eavesdropping. By their nature, wireless LANs radiate network traffic into space. Once that is done, it is impossible to control who can receive the signals. So, it must be assumed in any wireless LAN installation that the network traffic is subject to interception and eavesdropping by third parties. The obvious solution to this problem is to encrypt the data stream. The 802.11 standards provide for doing precisely that. Unfortunately, the implementation of this solution is less than perfect.

To provide security on wireless LANs, the 802.11b standard provides for wired equivalent privacy (WEP). There are several problems with the implementation of this approach. First, WEP is an option. It is not activated by default in shipped products, and it reduces raw throughput by as much as 50 percent. In such a situation, the network is broadcasting all network traffic in the clear for the benefit of all who can intercept it. That is hardly a secure mode of operation.

The WEP approach to cryptography sounds secure: WEP encrypts every packet with a different key. It uses a straightforward and predictable way of incrementing the vector from one packet to the next. Coupled with weak key management and a restricted key space, WEP is demonstrably insecure. The WEP password scheme also has been found to be flawed with the result that an intruder can gain access to some WEP-protected networks in as little as 30 seconds.

There are technologies that can be employed to provide cryptographic level confidentiality beyond what is offered by WEP. The researchers who "broke" WEP recommend treating all wireless networks as being outside the firewall and using higher-level protocols, such as SSH or IPSec, to provide security.

The goal of WEP was to provide a level of security commensurate with that found on wired LANs. Wired networks are not generally very secure unless protected by measures beyond those provided by the network protocols. Many have experienced connecting a computer to a wired LAN and being able suddenly to access resources to which they had no right. This is a common problem, usually controlled by limiting which computers may physically connect to the LAN. However, in the wireless domain, it is more difficult to limit who can connect to the LAN, so WEP - despite its shortcomings - is an important tool in the overall management of network security.

Illicit Entry. The very nature of the wireless protocols is to make the network user friendly by facilitating connection to an access point - and thus the entire network - as the user moves about. That is to say, the system has weak authentication.

Wireless network equipment is generally set so the network name is a default name for public access and all network interface cards that conform to the standard of the network (e.g., 802.11b) can readily connect to the system. Few network administrators bother to change the level of access to something more restrictive than the default. The wireless access point advertises its presence and its network name, and when a wireless client senses the access point, the client attempts to connect to the network. Unless the ability to connect is somehow restricted, the connection attempt will succeed, and another user will have been added to those already supported. As wireless LANs primarily serve to extend wired networks, the view this newcomer has of the network may be quite extensive, and the resources available may include many not intended for casual visitors. With a wireless LAN, one only has to be in the vicinity. As it happens, the vicinity may be rather large.

Depending on the structural elements in the path, a wireless LAN signal may be usable for distances of approximately 500 meters. While this is helpful from a coverage standpoint, it is not helpful from a security standpoint. Using directional antennae, one can detect wireless network signals at distances up to eight miles (12.8 kilometers) from the network node. In such a situation, someone can connect to a network from outside the perimeter of a place of business and probably without the organization's knowledge.

Large networks that cater to itinerant users are more or less forced to accept the poor authentication provided by WEP. It would not do if one had to register in advance to use a network in a public airport space, for instance. However, smaller networks have an option that can help. It is possible to restrict access to the network to those network nodes whose media access control (MAC) addresses are known in advance by the access point. For small wireless networks with a stable user population, this is an attractive option.

Denial of Service. A denial-of-service (DoS) attack is one wherein the attacker attempts to render the target network unable to serve its legitimate users. In the wired domain, many have become accustomed to protocol-based attacks, such as the "Ping of Death," which seek to overwhelm the target network with traffic forcing the network servers to crash. This type of attack also is effective against wireless networks.

In addition to protocol-based DoS attacks, wireless networks are vulnerable to a denial-of-service attack that is not viable against their wired brethren. Because their signals must travel through the public airwaves rather than in protected cables, wireless networks are extremely vulnerable to radio interference, either deliberate or accidental. Accidental interference occurs all too often owing to the shared nature of the bands in which these networks operate. It is very common for a wireless network, or a portion of it, to become unusable when a cordless telephone is operating in the same band and in physical proximity to the wireless node. It also is common for one wireless network to interfere with another nearby network, often making both useless.

3.3. Defense in Depth

In deploying a wireless LAN, the same importance must be stressed in terms of security as when deploying a wired LAN. Security must be looked at several aspects like in the policy and the three A's of Security - Access control, Authentication and Auditing. Defense in depth, in particular, defines several layers with each layer having its own security mechanisms and controls. The layers are the perimeter defense, network, host, application and information.

Authentication will look at the perimeter defense and the network layer. This is basically looking at how users get authenticated and what defense strategies are applied at the perimeter. Access control meanwhile will define who can have access to the wireless network and how to control and monitor them. It will also look at the access control at the host level and application by implementing host based firewall for example. As to protect the information, security policies and procedures need to be defined and enforced while auditing the wireless network with relevant tools will strengthen all the layers defined earlier.

Security Policy and Procedure. As we know, all technologies will have their own advantages, disadvantages and limitations that will make the technologies useful to the users. Nonetheless, technology alone will not be able to be utilized to its most potential without the intervention of human factor, like the policies and procedures. Policies and procedures will become the guidelines for technology to be properly used and to get the most out of it. Hence, it is vital that any deployment of wireless LAN is preceded by a wireless security policy. Having a security policy that defines the right procedures for implementing wireless networks will help reduce the risk of wireless network being breached. Policy and procedures can help enforced standard rules sets required in a deployment of wireless network.

Hence, it is recommended to implement the following security controls in order to maximize the 802.11b network by following certain best practices:

- Disable broadcast of the 32-bit plain text Service Set Identifier (SSID). This way, only clients with the known correct SSID can associate with the access point.
- More sophisticated attackers will counter a lack of broadcast SSID by analyzing the authentication frames with an 802.11 scanner to obtain the plain text SSID. To limit the effect of passive attacks, if possible, only broadcast beacon packets at higher bandwidth and reduce the frequency of beacon packets to inhibit such methods.
- Set non-standard SSIDs. Do not use the company name, address or any other easy to guess information about the organization.
- Do not choose SSIDs that could be attractive to attackers. Follow strong password generation methods to create SSIDs that are difficult to guess.
- Always enable 40-bit or 128-bit WEP encryption. Although there are numbers of WEP shortcomings, it will be a barrier to casual attack.
- Choose strong encryption keys on all wireless devices and change shared keys regularly. Encryption key changes make it harder for attackers to obtain and maintain a foothold on the network.
- Change all default vendor passwords.
- Administer the wireless devices using secure protocols like SSH or HTTPS, instead of telnet and HTTP.

Authentication. Authentication is always the best possible security measures in any systems. In 802.11, it specifies two major approaches which are open system authentication and shared key authentication.

Open system authentication is the default authentication method for 802.11. In open system authentication, the access point accepts anyone who requests authentication without verifying its identity. It works by exchanging only two management frames between the mobile station and access points.

Shared key authentication makes use of Wired Equivalent Privacy (WEP) and requires a shared key to be distributed to stations before attempting authentication. As with open system authentication, it works by exchanging management frames except with shared key authentication, it uses four frames instead of two.

There is another mechanism used by vendors to provide security with the use of access control lists based on the Ethernet MAC address of the client. Each access points can limit the clients of the network to those using a listed MAC he addresses. If a client's MAC address is listed, then they are permitted access to the network or else they will be rejected. Moreover, it is important to note one security problem with the MAC access control list. This mechanism only authenticates the machine with the right MAC address but not the users.

Access Control. The nature of wireless networks can be treated as an external network to the enterprise LAN. As such, any security measure taken to secure the network from Internet access, for example, can also be applied to the wireless network, as well.

One of the measures that can be applied to secure wireless LAN is by implementing a wireless firewall gateway. Wireless firewall is actually a wired firewall that bridges the wireless network and the wired network.

Packet filtering can also be applied at the firewall to allow only selected lied protocols or hosts into the network.

In addition to having a firewall, an intrusion detection system must also be installed between the wireless network and the wired network. Intrusion detection system or IDS should be able to add more security to the network by sniffing, the wireless traffics and alerting the administrators on suspected malicious traffics through defined signatures. This vigilance monitoring will provide administrators preventive and also response security measure as certain malicious traffics could be blocked before doing some damage to the network.

Furthermore, we can also deploy DHCP for issuing and maintaining IP addresses of wireless networks' clients. DHCP also allows to group users into IP address range that is based on the requirement and defined in the firewall. This kind of arrangement will allow legitimate users to get access to the network and restrict other unnecessary access.

At the host level, it is recommended to have some kind of filtering mechanism like the personal firewall. This is to provide security access control and measure at the application and host layer.

Auditing. Auditing the network is supposed to be the top priority for all network administrators. By auditing the network, we are actually looking at the vulnerabilities that are available inside the wireless networks. By finding and knowing what type of vulnerabilities existed in the network, it will prepare the administrators to put necessary measures to overcome or prevent any kind of threats that resulted from the vulnerabilities.

4. Hacking tools in wireless networks

As the information age continues to mature, more and more individuals have access to sophisticated computer and Internet technology. Today's personal computer has more power than it once took to put a man on the moon. Improved technology and lower prices allow many more people to access superior technology in their homes.

Today, the power at an individual's fingertips is enough to disable a medium-sized Web hosting company. This accessibility to computer power, in part, explains the sharp rise in attacks every year. Other contributors are the increased Internet population and the availability of hacking tools.

More attacks mean increased risk. A risk is defined as a possibility of harm or loss. It is important to assess the risk your company faces as you plan and implement network security measures.

Companies with more assets and intellectual capital, as well as companies with a high profile, have more to lose than others; and therefore have a much higher risk of attack. A hacker relies on a variety of tools as well as his or her own creativity in order to attack your network. Because every network is different, hackers employ a variety of means to breach your security. However, most hackers follow the same basic steps to perpetrate an attack:

1. Profiling
2. Scanning
3. Enumerating
4. Exploiting

Profiling. Profiling, or footprinting, is the process of gathering information about targets. The result is a profile of an organization's security posture, also known as the infrastructure. Profiling may also include gathering information about the physical site. Insiders (people who already work for the company) may have a significant advantage during the profiling process due to preknowledge of the network and physical environment.

*Scanning***.** After profiling a network, a hacker will then scan the network for additional information. This will allow him to create a list of network devices active on the network. There are several ways to complete the scanning phase. Hackers often use PING sweeps to identify what systems are active and responding on the network

*Enumeration***.** Enumeration is the intrusive process of determining valid user accounts and accessible resources such as shares. Having identified these accounts, the hacker can then guess passwords to gain access to a system. Identifying and accessing resources might allow a way into confidential documents or even a database.

*Exploiting***.** Exploiting is the process by which the attacker gains unlawful entry to a system. At this point, the attacker would have identified vulnerabilities during the scanning and enumeration phases.The attacker can now attempt to exploit one or more of these vulnerabilities with the ultimate goal of gaining complete control of the machine.

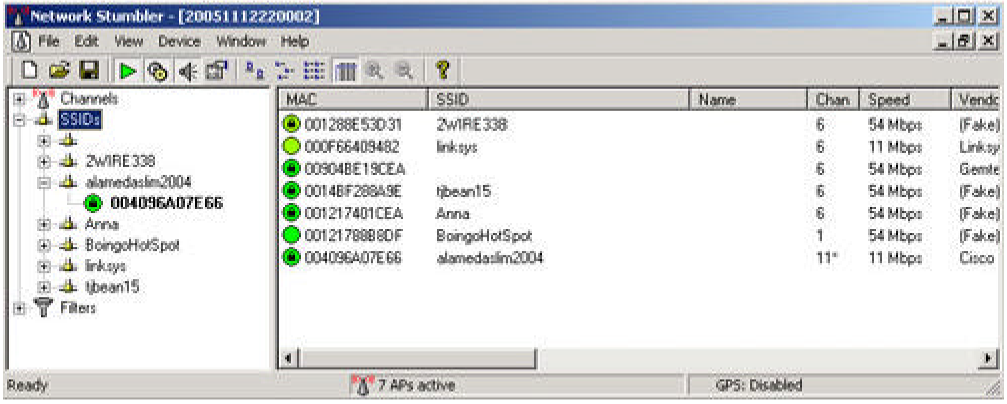
Below are commonplace wireless hacking tools:

- Airsnort – a common tool to break WEP encryption.
- Netstumbler – Windows wireless network scanner.
- Kismet – a wireless network sniffer that separates and identifies different wireless networks in an area
- Ethereal – a free network protocol analyzer.
- AirDefense IDS – Wireless IDS that provides 24x7 monitoring.

4.1. Finding Wireless Networks

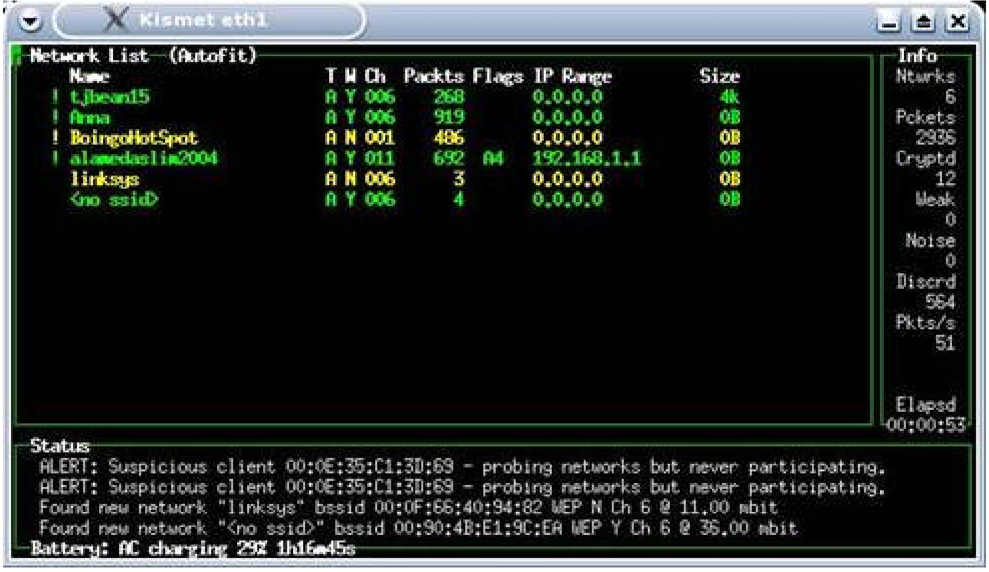
Locating a wireless network is the first step in trying to exploit it. There are two tools that are commonly used in this regard:

Network Stumbler (NetStumbler) – This Windows based tool easily finds wireless signals being broadcast within range – a must have. It also has ability to determine Signal/Noise info that can be used for site surveys. I actually know of one highly known public wireless hotspot provider that uses this utility for their site surveys.



MAC	SSID	Name	Chan	Speed	Vendc
001288E53D31	2WIRE338		6	54 Mbps	(Fake)
000F66409482	linksys		6	11 Mbps	Linksy
00904BE19CEA			6	54 Mbps	Gemte
0014BF288A9E	tjbean15		6	54 Mbps	(Fake)
001217401CEA	Anna		6	54 Mbps	(Fake)
00121788B8DF	BoingoHotSpot		1	54 Mbps	(Fake)
004096A07E66	alamedaslim2004		11*	11 Mbps	Cisco

Kismet – One of the key functional elements missing from NetStumbler is the ability to display Wireless Networks that are not broadcasting their SSID. As a potential wireless security expert, you should realize that Access Points are routinely broadcasting this info; it just isn't being read/deciphered. Kismet will detect and display SSIDs that are not being broadcast which is very critical in finding wireless networks.



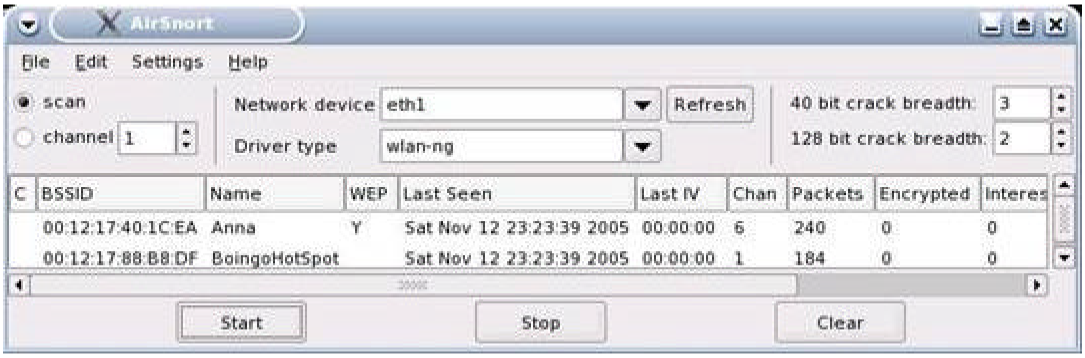
```
Network List (Autofit)                                                   Info
    Name                     T W Ch  Packts Flags IP Range        Size   Ntwrks
  ! tjbean15                 A Y 006   268        0.0.0.0          4k        6
  ! Anna                     A Y 006   919        0.0.0.0          0B    Pckets
  ! BoingoHotSpot            A N 001   486        0.0.0.0          0B      2936
  ! alamedaslim2004          A Y 011   692  A4    192.168.1.1      0B    Cryptd
    linksys                  A N 006     3        0.0.0.0          0B        12
    <no ssid>                A Y 006     4        0.0.0.0          0B      Weak
                                                                              0
                                                                          Noise
                                                                              0
                                                                         Discrd
                                                                            564
                                                                         Pkts/s
                                                                             51

                                                                         Elapsd
                                                                       00:00:53
Status
 ALERT: Suspicious client 00:0E:35:C1:3D:69 - probing networks but never participating.
 ALERT: Suspicious client 00:0E:35:C1:3D:69 - probing networks but never participating.
 Found new network "linksys" bssid 00:0F:66:40:94:82 WEP N Ch 6 @ 11.00 mbit
 Found new network "<no ssid>" bssid 00:90:4B:E1:9C:EA WEP Y Ch 6 @ 36.00 mbit
Battery: AC charging 29% 1h16m45s
```

4.2. Attacking the Found Wireless Network

Once you've found a wireless network, the next step is to try to connect to it. If the network isn't using any type of authentication or encryption security, you can simply connect to the SSID. If the SSID isn't being broadcast, you can create a profile with the name of the SSID that is not being broadcast. Of course you found the non-broadcast SSID with Kismet, right? If the wireless network is using authentication and/or encryption, you may need one of the following tools.

Airsnort – This is a very easy to use tool that can be used to sniff and crack WEP keys. While many people bash the use of WEP, it is certainly better than using nothing at all. Something you'll find in using this tool is that it takes a lot of sniffed packets to crack the WEP key. There are additional tools and strategies that can be used to force the generation of traffic on the wireless network to shorten the amount of time needed to crack the key, but this feature is not included in Airsnort.



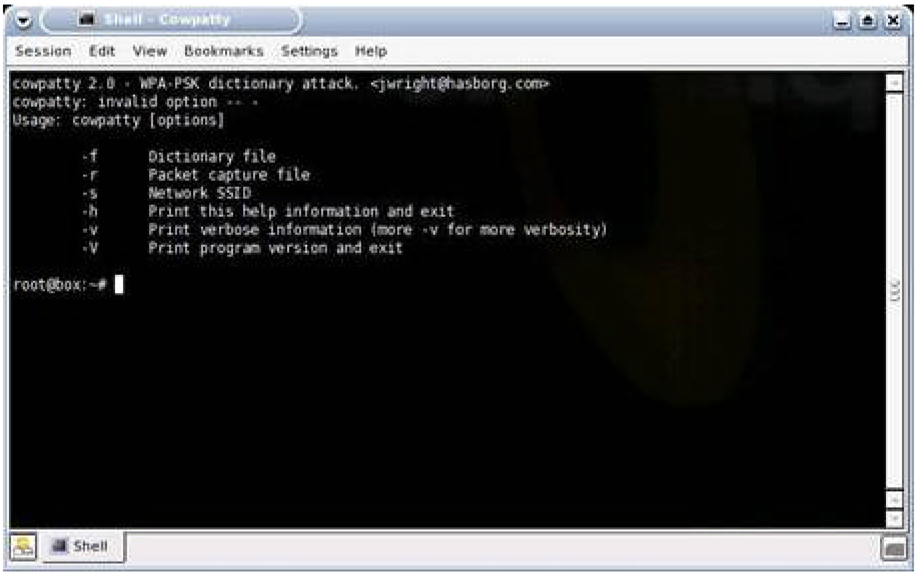
● scan
○ channel 1

Network device: eth1
Driver type: wlan-ng

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interes
	00:12:17:40:1C:EA	Anna	Y	Sat Nov 12 23:23:39 2005	00:00:00	6	240	0	0
	00:12:17:88:B8:DF	BoingoHotSpot		Sat Nov 12 23:23:39 2005	00:00:00	1	184	0	0

CowPatty – This tool is used as a brute force tool for cracking WPA-PSK, considered the "New WEP" for home Wireless Security. This program simply tries a bunch of different options from a dictionary file to see if one ends up matching what is defined as the Pre-Shared Key.

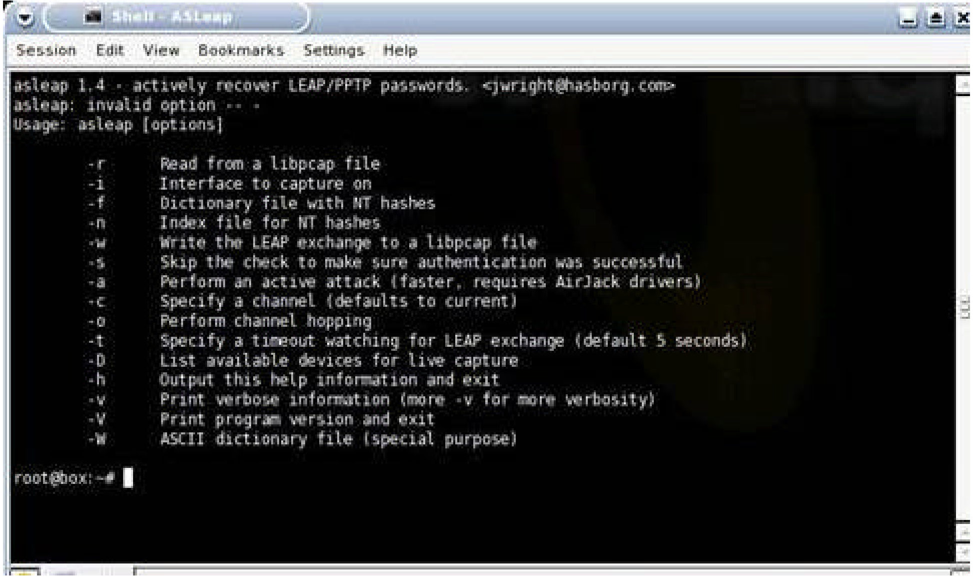


```
cowpatty 2.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>
cowpatty: invalid option -- -
Usage: cowpatty [options]

        -f      Dictionary file
        -r      Packet capture file
        -s      Network SSID
        -h      Print this help information and exit
        -v      Print verbose information (more -v for more verbosity)
        -V      Print program version and exit

root@box:~#
```

ASLeap – If a network is using LEAP, this tool can be used to gather the authentication data that is being passed across the network, and these sniffed credentials can be cracked. LEAP doesn’t protect the authentication like other “real” EAP types, which is the main reason why LEAP can be broken.



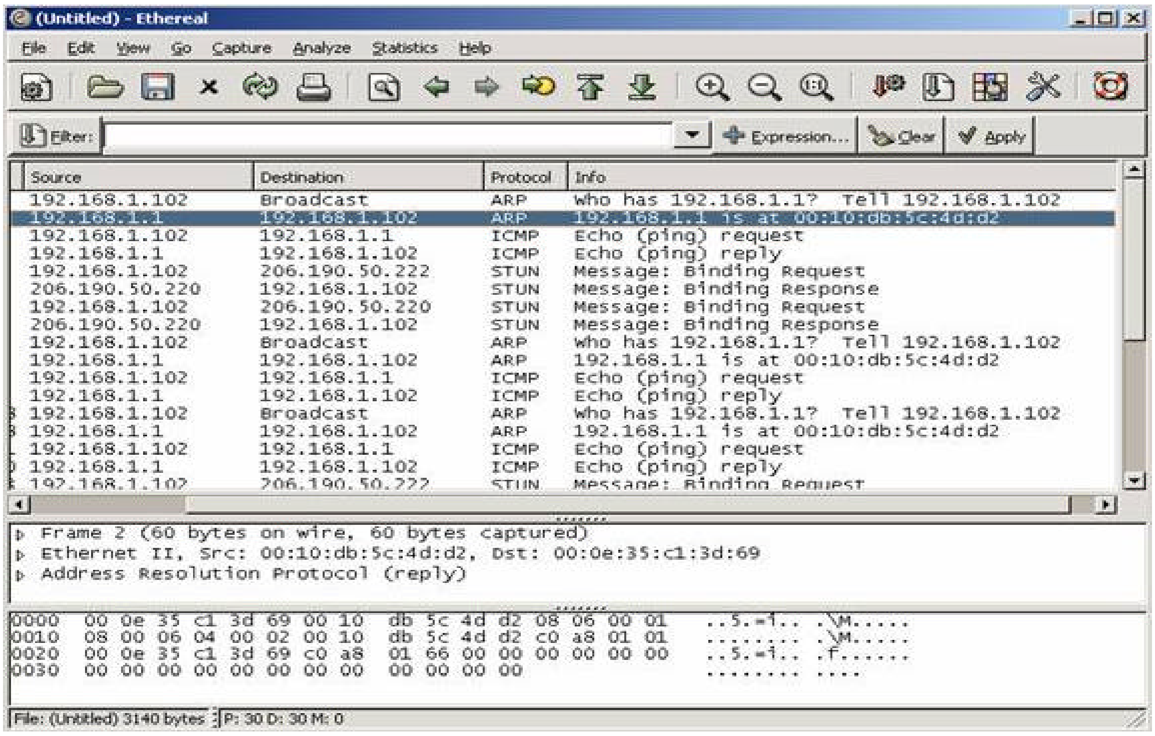
```
asleap 1.4 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
asleap: invalid option -- -
Usage: asleap [options]

        -r      Read from a libpcap file
        -i      Interface to capture on
        -f      Dictionary file with NT hashes
        -n      Index file for NT hashes
        -w      Write the LEAP exchange to a libpcap file
        -s      Skip the check to make sure authentication was successful
        -a      Perform an active attack (faster, requires AirJack drivers)
        -c      Specify a channel (defaults to current)
        -o      Perform channel hopping
        -t      Specify a timeout watching for LEAP exchange (default 5 seconds)
        -D      List available devices for live capture
        -h      Output this help information and exit
        -v      Print verbose information (more -v for more verbosity)
        -V      Print program version and exit
        -W      ASCII dictionary file (special purpose)

root@box:~#
```

4.3. Sniffing Wireless Data

Whether you are directly connected to a wireless network or not, if there is wireless network in range, there is data flying through the air at any given moment. You will need a tool to be able to see this data.


(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

Source	Destination	Protocol	Info
192.168.1.102	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.102
192.168.1.1	192.168.1.102	ARP	192.168.1.1 is at 00:10:db:5c:4d:d2
192.168.1.102	192.168.1.1	ICMP	Echo (ping) request
192.168.1.1	192.168.1.102	ICMP	Echo (ping) reply
192.168.1.102	206.190.50.222	STUN	Message: Binding Request
206.190.50.220	192.168.1.102	STUN	Message: Binding Response
192.168.1.102	206.190.50.220	STUN	Message: Binding Request
206.190.50.220	192.168.1.102	STUN	Message: Binding Response
192.168.1.102	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.102
192.168.1.1	192.168.1.102	ARP	192.168.1.1 is at 00:10:db:5c:4d:d2
192.168.1.102	192.168.1.1	ICMP	Echo (ping) request
192.168.1.1	192.168.1.102	ICMP	Echo (ping) reply
192.168.1.102	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.102
192.168.1.1	192.168.1.102	ARP	192.168.1.1 is at 00:10:db:5c:4d:d2
192.168.1.102	192.168.1.1	ICMP	Echo (ping) request
192.168.1.1	192.168.1.102	ICMP	Echo (ping) reply
192.168.1.102	206.190.50.222	STUN	Message: Binding Request

```
▷ Frame 2 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: 00:10:db:5c:4d:d2, Dst: 00:0e:35:c1:3d:69
▷ Address Resolution Protocol (reply)
```

```
0000   00 0e 35 c1 3d 69 00 10   db 5c 4d d2 08 06 00 01    ..5.=i.. .\M.....
0010   08 00 06 04 00 02 00 10   db 5c 4d d2 c0 a8 01 01    ........ .\M.....
0020   00 0e 35 c1 3d 69 c0 a8   01 66 00 00 00 00 00 00    ..5.=i.. .f......
0030   00 00 00 00 00 00 00 00   00 00 00 00                ........ ....
```

File: (Untitled) 3140 bytes | P: 30 D: 30 M: 0

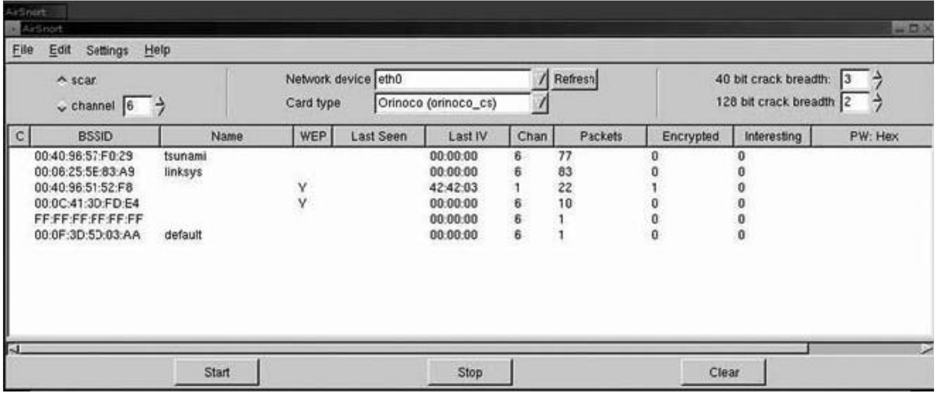
Wireshark (formerly Ethereal) – While there has been much debate on the proper way to pronounce this utility, there is no question that it is an extremely valuable tool. Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff-out 802.11 management beacons and probes and subsequently could be used as a tool to sniff-out non-broadcast SSIDs.

*WEPCrack***.** The WEPCrack tool was the first tool to crack WEP (Wired Equivalent Privacy). It was created before the more famous AirSnort tool. WEPCrack is a couple of Perl scripts that validate the workings of Fluhrer, Matin, and Shamir's (FMS) theoretical attack. It took their paper and created an automated tool to perform and prove their research.

These Perl scripts are as follows:

- WEPCrack.pl
- WeakIVGen.pl
- Prism-getIV.pl
- Prismdecod.pl

The tool works by collecting weak IVs and sending them to the IVfile.log. Once they are in the log file, the WEPCrack.pl can run the FMS attack against them. The WEPCrack tool uses pcap files and Perl. This allows the program to be very versatile; it can be loaded on a PDA or another device that supports Perl. This tool does not have a front end or a pretty GUI. This helps with battery life and processing power, although it affects the ability to run the program by novice users. This is one of the main reasons that the next tool (AirSnort) has become the more popular choice for WEP cracking.



channel: 6
Network device: eth0
Card type: Orinoco (orinoco_cs)
40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex
	00:40:96:57:F0:29	tsunami			00:00:00	6	77	0	0	
	00:06:25:5E:83:A9	linksys			00:00:00	6	83	0	0	
	00:40:96:51:52:F8		Y		42:42:03	1	22	1	0	
	00:0C:41:3D:FD:E4		Y		00:00:00	6	10	0	0	
	FF:FF:FF:FF:FF:FF				00:00:00	6	1	0	0	
	00:0F:3D:5D:03:AA	default			00:00:00	6	1	0	0	

Conclusions

Wireless LANs are very valuable in today's mobile society. They have proliferated over the past few years, and although the market has not quite reached its maturity level due to refinements to some of the hardware and software, it is no longer a secret to the public at large. Anyone who does not personally have a wireless LAN knows someone who does, uses one at work, has heard of the technology or is unknowingly affected by the technology each day of their lives. Although wireless LANs for both small office/home office and the enterprise have some security vulnerabilities, if care is taken to implement the following safeguards the vulnerabilities will be greatly minimized or removed allowing the LAN to be used safely:

- inform and train users
- configure the access points
- monitor the LANs
- use strong encryption
- implement 802.1X with authentication, authorization and accounting (AAA)
- deploy an EAP method

To compliment the measures above, there should also be:

- a system of checks and balances in place, for example, have a second IT staff member double checked the access point configuration.
- a plan to consistently demand better products from manufacturers
- an effort to stay abreast of the latest in developing technology

With newer technology that promises greater built-in or add-on security measures, wireless LANs will attract greater, more sophisticated hacker attacks - another chapter in the continuing saga of security versus hacker. We know that hackers will never go away, so we bear the burden to provide the best "locks" we can to protect our LANs. Finally, whatever the outcome, wireless LANs will survive and are here to stay even if the technology has a new look and, or feel in coming years.

References

1. Earle A. - *Wireless Security Handbook*, Auerbach Publications, New York, 2006
2. Finneran M. - *WiMax versus Wi-Fi, a Comparison of Technologies,* 2005
3. PhD. Zota R., - *New Broadband Wireless Technologies – WiMax*, in *Economic Informatics* Magazine, Bucharest, 2006
4. John J. Laskar, - *Concept of Secure Wireless Metropolitan Area Network (SWMAN) in a Mobile Computing Environment*, Mitretek Systems
5. Vladimirov A., Gavrilenko K. V. - *Wi-Foo*, Addison Wesley, 2004
6. *MOTOROLA WI4 WiMAX, Solutions Guide*

Weblinks

1. http://en.wikipedia.org/wiki/WLAN, http://en.wikipedia.org/wiki/WWAN
2. http://en.wikipedia.org/wiki/WWAN
3. www.about.com
4. "*Top 5 Wireless Tools*", http://sectools.org/wireless.html, 2006
5. "*The Top 10 Hacker Attack Tools*", http://www.thenetworkadministrator.com
6. "*AirSnor*t", http://airsnort.shmoo.com/, The Schmoo Group
7. "*AirCrack*", http://www.wirelessdefence.org/Contents/AircrackMain.htm
8. http://en.wikipedia.org/wiki/Wi-Fi
9. http://en.wikipedia.org/wiki/WiMAX
10. http://en.wikipedia.org/wiki/3G, http://en.wikipedia.org/wiki/4G
11. http://en.wikipedia.org/wiki/4G

12. www.securityoverview.com
13. http://www.army-technology.com/features/feature41023/
14. http://www.radio-electronics.com/info/wireless/index.php
15. http://www.wirelessoverview.net/wireless-security?start=9
16. http://www.wifinotes.com/
17. http://www.javvin.com/wirelessmap.html
18. http://defense-update.com/features/du-1-05/c4-data.htm
19. http://www.wimaxxed.com/wimax_reports/20041116/a_wireless_mili.html
20. www.wi-foo.com
21. http://netsecurity.about.com/cs/hackertools/a/aafreewifi.htm
22. http://docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless

FIREWALLS AND INTRUSION DETECTION SYSTEMS

LTCDR eng Razvan STOLERU

UM 02039 Constanta

Introduction

Internet Information Services (IIS) web servers – which host web pages and serve them to users – are highly popular among business organizations, with over 6 million such servers installed worldwide. Unfortunately, IIS web servers are also popular among hackers and malicious fame-seekers – as a prime target for attacks. As a result, every so often, new exploits emerge which endanger your IIS web server's integrity and stability. Many administrators have a hard time keeping up with the various security patches released for IIS to cope with each new exploit, making it easy for malicious users to find a vulnerable web server on the Internet. Immediate Intrusion Detection suggests that all of these vulnerabilities the same system files, careful monitoring of these files could provide you with an inexpensive form of real-time intrusion detection. The market is currently filled mostly by rule-based IDS solutions aiming at detecting already known attacks by analysing traffic flow and looking for known signatures. This fact requires such IDS to be under constant construction updating and modifying attack signatures and requiring to pay considerable financial amount for support. On the other hand it is possible to use anomaly based IDS solutions detecting not just known attacks but also unknown attacks and informing network engineers about possible network problems or helping them to troubleshoot them. The market is currently filled mostly by rule-based IDS solutions aiming at detecting already known attacks by analysing traffic flow and looking for known signatures. This fact requires such IDS to be under constant construction updating and modifying attack signatures and requiring to pay considerable financial amount for support. On the other hand it is possible to use anomaly based IDS solutions detecting not just known attacks but also unknown attacks and informing network engineers about possible network problems or helping them to troubleshoot them.

A correct firewall policy can minimize the exposure of many networks however they are quite useless against attacks launched from within. Hackers are also evolving their attacks and network subversion methods. These techniques include email based Trojan, stealth scanning techniques, malicious code and actual attacks, which bypass firewall policies by tunneling access over allowed protocols such as ICMP, HTTP, DNS, etc. Hackers are also very good at creating and releasing malware for the ever-growing list of application vulnerabilities to compromise the few services that are being let through by a firewall.

IDS arms your business against attacks by continuously monitoring network activity, ensuring all activity is normal. If IDS detects malicious activity it responds immediately by destroying the attacker's access and shutting down the attack. IDS reads network traffic and looks for patterns of attacks or signatures, if a signature is identified, IDS sends an alert to the Management Console and a response is immediately deployed.

1. Against what we protect

1.1. The Effect of Hackers

There is a community, a shared culture, of expert programmers and networking wizards that traces its history back through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments. The members of this culture originated the term ‘hacker’. Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work.

In the context of computer systems, there is a similar dichotomy. There are some career criminals who steal by electronic means. This small group poses a large problem for society, but it's not a new one. Thieves are thieves. Just as banks use special armored cars, they must also develop special armored computer systems. But the rest of us don't use armored cars for routine transportation, and we don't need armored computer systems for routine communication either.

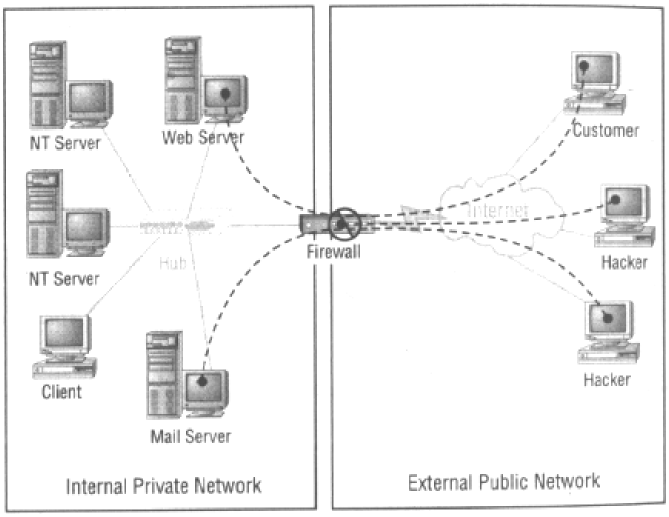
What we lose if we do not protect:

- System down time
- Network down time
- Loss of productivity
- Loss of confidence
- Data Loss
- Information disclosure

2. How we protect

Firewalls are devices or software packages that monitor traffic passing through them and accept or block it depending on their rules. They operate at the network layer of security which is one of the oldest and most common types of protection used within security solutions.

Network Firewalls are located as a gateway between the private network and the Internet as shown in the diagram below:



There are three main types of Firewall:

- Packet Filtering – Rejects TCP/IP packets from unauthorised hosts and rejects connection attempts to unauthorised services. Packet Filters compare network protocols and transport protocol packets to a database of rules and forward only those packets that conform to the criteria specified in the database of rules. Filters can either be implemented in routers or in the IP stacks of servers.
- Network Address Translation (NAT) – Provides security benefits by hiding the actual IP address of a host computer when that host makes a request from servers on the internet. A firewall that uses NAT does this by using its own IP address instead of the hosts when it sends requests to servers out on the internet. When replies come back in the NAT component, the firewall places the hosts real IP address in the packet and forwards it to the host. NAT also has the advantage that only one IP address is needed for a LAN to be connected to the internet.

- Proxy Services – Makes high level application connections on behalf of internal hosts to completely break the network layer connection between internal and external hosts. Proxies are application specific and have to be written to support a particular service such as HTTP.

Most firewalls on the market today are a combination of the above to increase their effectiveness.

Because of the firewalls location as the gateway between the Internet and the local network, if the firewall were to fail it could mean the local network losing Internet access. Unfortunately this is very hard to protect against without special clustering software because firewalls have to know about connections. If these connections are shared amongst firewalls they need a way of sharing the information between them about the connections.

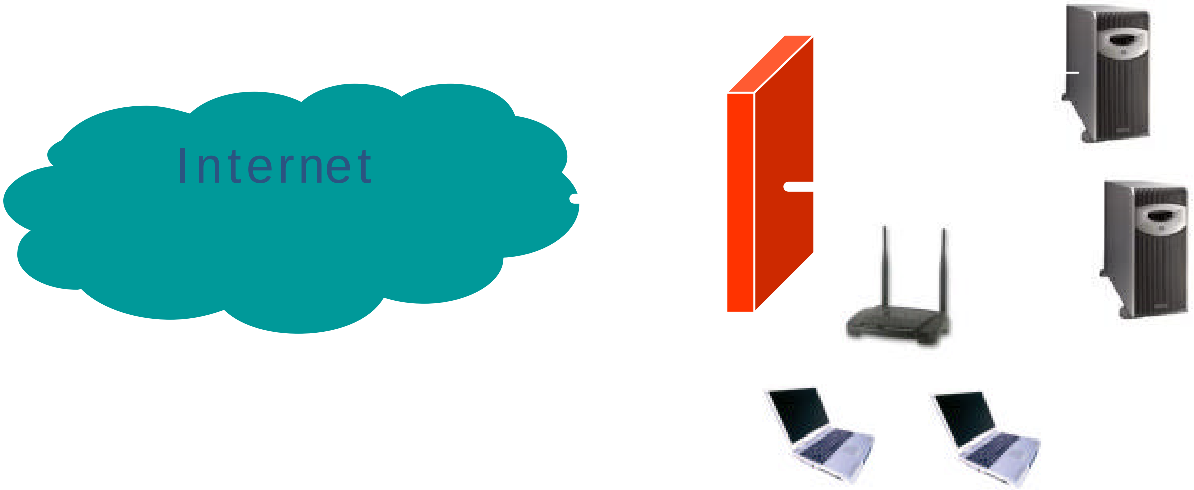
Preventing Hackers

a. Firewall & Security Zones
b. System Updates
c. Account Policies
    i. One user per account
    ii. Strong passwords
    iii. Deactivate on departure
d. IDS/IPS
e. Application Firewall
f. Data Encryption

3. What is Firewall?

3.1. Introduction

Firewall/VPN is a perimeter-defense device, typically deployed where the enterprise's internal network meets the open Internet. The main purpose of the firewall is to stop unwanted traffic from entering or leaving the internal enterprise network. The purpose of the IPSec VPN is to provide secure communication between two sites through the open Internet.



Network firewalls are great for implementing a security policy between different networks, but are often expensive, complicated, inflexible, or do not progress quickly enough to keep up with new attacks. They may also be rendered useless by dialup access weaknesses, encryption, VPNs, teleworkers connecting directly to the Internet from home, etc.

An interesting new breed of "personal firewalls" have surfaced that are installed on Windows and allow both beginner and expert users to protect their PCs. The risk faced by the home user on the Internet is analyzed in Summary and Conclusion. Basically, there is a significant risk of information being stolen or destroyed; of your PC being misused to attack others, or used to access sensitive (e.g., banking) software; or simply of PC/network resources wasted; and it needs to be addressed.

3.2. Precautionary Measures

There are a few measures that Windows users should take, whether they install a firewall or not:

- Never run any executable file or script received by email unless you are very sure of its original and are convinced the originator has excellent virus/Trojan protection in place.
- Disable file and printer sharing.
- Disable the SMB/Microsoft protocols on the interface used to access the Internet. For example, on NT with a dialup connection, select Control Panel -> Network -> Bindings -> NetBIOS Interface, select the Remote Access WAN Wrapper entries, right-click and select "disable."
  If you use dialup for both Internet and intranet access, though, disabling SMB/Microsoft protocols might disrupt your intranet access.
- Install Windows, Explorer and Office security fixes/service packs: This is a tricky one as it can be very time-consuming and cause major headaches. For instance, one Outlook2003 security patch was so restrictive as to make it unusable on intranets (in my opinion).
- Antivirus/worm/Trojan measures
  - Install a good antivirus scanner and keep it up to date. Scan email attachments before opening them.
  - MS Office: Switch on Word/Excel 2003 Macro virus protection (Tools/Options/General/Macro virus protection) or run Word/Excel 2003 with at least medium security settings. This will ensure the user is presented with a dialog box when documents containing macros are opened. If suspect Word documents are received by email, open them in Wordpad rather than Word, since macros won't be understood by Wordpad. Set the file-permissions of "normal.dot" to read only, to prevent viruses or Trojans from infecting your Word setup.
  - If possible, configure your browser to ignore ActiveX and prompt when Java or Jscript or VBscript is run.
- Scan your system remotely to see what ports are open to the Internet .
- Don't stay connected to the network unless you need to.
- Don't connect to the network before tools like personal firewalls are active.
- Back up your system regularly.

3.3. Key Criteria in Choosing a Personal Firewall

a. Effectiveness of security protection: penetration, Trojans, controlling leaks, denial of service.
b. Effectiveness of intrusion detection: few false positives, alerting of dangerous attacks.
c. Effectiveness of reaction: discovering identity of attacker, blocking attacks, ease of use.
d. User interface: ease of use, instructiveness, simplicity, quality of online help. Can rules be easily added/removed/checked? Does the interface suit the way you use your PC? Do you understand the questions the software asks and what it is doing?
e. Price: how much are you willing to pay initially, and each year for support/updates?

3.4. How Did we Test Effectiveness?

a. Ping and accessing shares to and from the test host.
b. A powerful, well-known "remote-control" Trojan (Netbus Pro v2.1) was installed on the system on a nonstandard port (to make detection more difficult), he Netbus server started and attempts made to connect from a remote system.

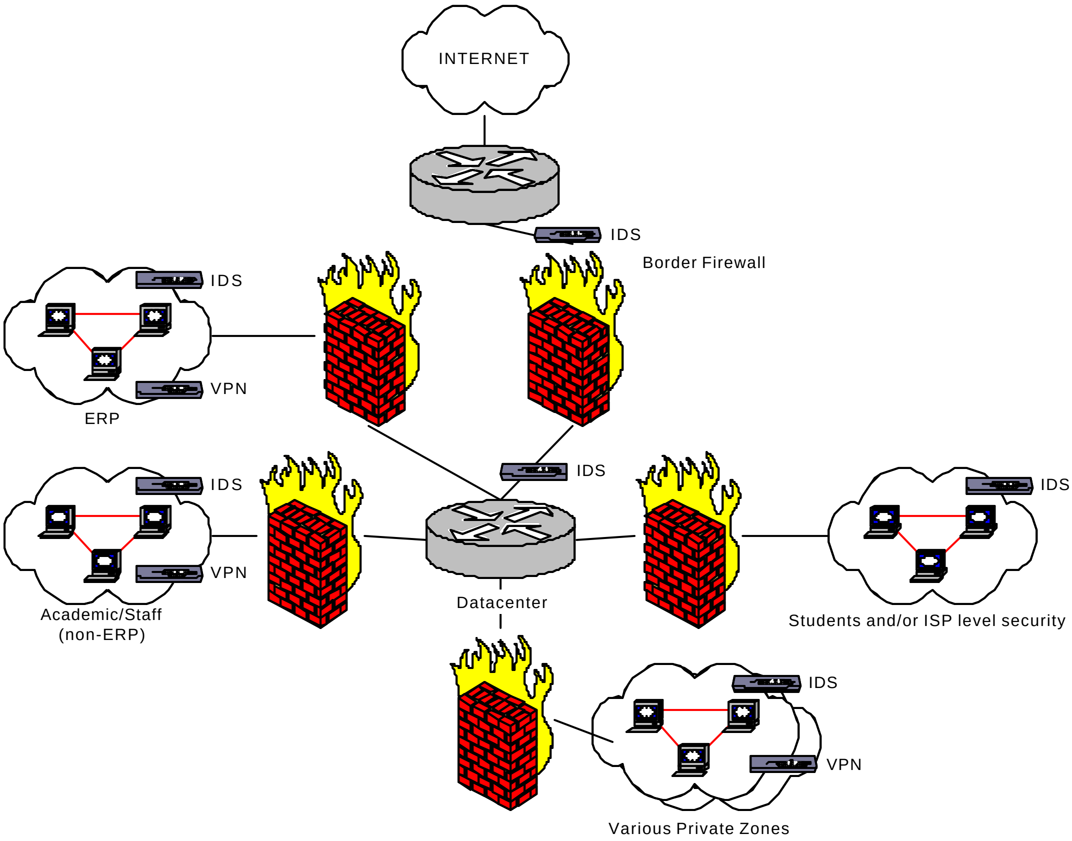
c. The telnet server was enabled on the Win2K test PC. It was then attempted to connect to this service remotely. It is not recommended that you enable telnet; we do this purely for testing purposes.

d. An nmap scan was run against each product (see below), to check that incoming ports were effectively blocked.

3.5. Note on Trojans

- One reader pointed out that the SubSeven 2.1 Trojan has a "wait until reboot" feature that allows the program to be downloaded to a system, installed, but not activated until the next time the system is started. This allows the Trojan to start before the personal firewall, so the firewall might view the Trojan as a "regular Windows application" and not issue an alert, leaving the system vulnerable. ZoneLabs released an updated version of ZA to correct this problem, but this may be an exploitable vulnerability in other firewalls.
- We haven't tested these products with SubSeven. You should be aware of this risk; if you are a vendor, make sure your product covers this issue!
- In the same vein, some firewalls start as services (on NT), others from the Startup folder. Beware! If the firewall does not start as a service, it is not active until logon.
- Trojans can also "leak" information by sending it out via standard ports that the firewall probably allows by default (e.g., port 80). Defense: detecting and controlling accurately which application (for example by the use of one-way hashes such as SHA-1) connects out on what port. In the Norton report, detailed "leakage tests" were carried out — a procedure is documented that can be used on any product.
- Vendors: Ensure that the firewall is started as a service, rather than in the Startup folder. Verify existing network connections when the firewall is started. Control network connections even prior to logon. Use strong hashing algorithms to identify applications and allow the user to easily see/change which application is allowed on what port.

4. How it functions?



Working of IDS

Anomaly detection

The most common way people approach network intrusion detection is to detect statistical anomalies. The idea behind this approach is to measure a "baseline" of such stats as CPU utilization, disk activity, user logins, file activity, and so forth. Then, the system can trigger when there is a deviation from this baseline.

The benefit of this approach is that it can detect the anomalies without having to understand the underlying cause behind the anomalies.

For example, let's say that you monitor the traffic from individual workstations. Then, the system notes that at 2am, a lot of these workstations start bgging into the servers and carrying out tasks. This is something interesting to note and possibly take action on.

Signature recognition

The majority of commercial products are based upon examining the traffic looking for well-known patterns of attack. This means that for every hacker technique, the engineers code something into the system for that technique.

This can be as simple as a pattern match. The classic example is to example every packet on the wire for the pattern "/cgi-bin/phf?", which might indicate somebody attempting to access this vulnerable CGI script on a web-server. Some IDS systems are built from large databases that contain hundreds (or thousands) of such strings. They just plug into the wire and trigger on every packet they see that contains one of these strings.

Traffic consists of IP datagrams flowing across a network. A NIDS is able to capture those packets as they flow by on the wire. A NIDS consists of a special TCP/IP stack that reassembles IP datagrams and TCP streams. It then applies some of the following techniques:

- *Protocol stack verification*: A number of intrusions, such as "Ping-O-Death" and "TCP Stealth Scanning" use violations of the underlying IP, TCP, UDP, and ICMP protocols in order to attack the machine. A simple verification system can flag invalid packets. This can include valid, by suspicious, behavior such as severally fragmented IP packets.
- *Application protocol verification*: A number of intrusions use invalid protocol behavior, such as "WinNuke", which uses invalid NetBIOS protocol (adding OOB data) or DNS cache poisoning, which has a valid, but unusually signature. In order to effectively detect these intrusions, a NIDS must re-implement a wide variety of application-layer protocols in order to detect suspicious or invalid behavior.
- *Creating new loggable events*: A NIDS can be used to extend the auditing capabilities of your network management software. For example, a NIDS can simply log all the application layer protocols used on a machine. Downstream event log systems (WinNT Event, UNIX syslog, SNMP TRAPS, etc.) can then correlate these extended events with other events on the network.

NIDS fights back

Once intrusion has been detected NIDS reacts by performing the following tasks:

- **Reconfigure firewall -** Configure the firewall to filter out the IP address of the intruder. However, this still allows the intruder to attack from other addresses. Checkpoint firewall's support a "Suspicious Activity Monitoring Protocol (SAMP)" for configuring firewalls. Checkpoint has their "OPSEC" standard for re-configuring firewalls to block the offending IP address.
- **Chime -** Beep or play a .WAV file. For example, you might hear a recording "You are under attack".
- **SNMP Trap -** Send an SNMP Trap datagram to a management console like HP OpenView, Tivoli, Cabletron Spectrum, etc.
- **NT Event -** Send an event to the WinNT event log.
- **Syslog -** Send an event to the UNIX syslog event system.
- **Send e-mail -** Send e-mail to an administrator to notify of the attack.
- **Page -** Page (using normal pagers) the system administrator.

- **Log the attack -** Save the attack information (timestamp, intruder IP address, victim IP address/port, protocol information).
- **Save evidence -** Save a tracefile of the raw packets for later analysis.
- **Launch program -** Launch a separate program to handle the event.
- **Terminate the TCP session -** Forge a TCP FIN packet to force a connection to terminate.

5. Benefit & Limitation

Protect Windows from network attacks when connected to hostile networks (like the Internet), especially those connected for hours or even days at a time (DSL or cable users). The longer you're on the Net, the more likely you'll be attacked.

If an infected email should install a back door (like BackOrifice), the personal firewall will still prevent network access to the backdoor.

When trying out new applications, you can see exactly what communications are needed, when.

Teleworkers who connect to the corporate LAN via Internet VPNs may be exposing the corporate intranet. If their PC is penetrated, it could be used as a bridge by attackers to penetrate the intranet. With a personal firewall installed, VPNs on the Internet do not pose as much of a risk.

Education: Become aware of just how hostile your network environment is.

Ensure that your PC is not used to attack others.

In a corporate environment, laptop users/Internet VPN users/home workers, etc. could be mandated to use a preconfigured personal firewall that prevents their PCs from posing additional risks to the corporate intranet.

In today’s corporate market, the majority of businesses consider the Internet as a major tool for communication with their customers, business partners and the corporate community. This mentality is here to stay; as a result businesses need to consider the risks associated with using the Internet as communication tool, and the methods available to them to mitigate these risks. Many businesses are already aware of the types of risks that they are facing, and have implemented measures such as Firewalls, Virus detection software, access control mechanisms etc. However it is all too apparent that although these measures may deter the “hobby hacker”, the real danger and threat comes from the “determined hacker”. The determined hacker is just that “determined” and they will find a way of penetrating your system, sometimes for malicious intent but mostly because they can and it is a test of skills. Whilst the above mentioned tools are preventative measures, IDS is more of an analysis tool, which will give you the following information:

- Instance of attack
- Method of attack
- Source of attack
- Signature of attack

This type of information is becoming increasingly important when trying to design and implement the right security program for an organization. Although some of this information can be found in devices such as Firewalls and access control systems as they all contain log information on system activity In these instances the onus is on the administrator to check the logs to determine if an attempted attack has occurred or after the event find out when the attack occurred and the source of the attack. Usually information pertaining to the method of the attack and the signature of the attack cannot be found in the logs. This is because devices such as Firewalls are designed to check the IP packet header information and not the payload portion of the IP packet.

IDS will check the payload of the packet to determine if the pattern of data held within, matches that of a known attack signature. The benefits of the above information are as follows:

Instance of attack: IDS will alert when an attack is in progress, this gives you the benefit of counteracting the attack as it happens, without having to go through lengthy logs to find out when this particular attack occurred.

Method of attack: IDS will let you know what area of your network or system on your network is under attack and how it is being attacked. This enables you to react accordingly and hopefully limit the damage of the attack by i.e. disabling communications to these systems.

Source of attack: IDS will let you know the source of an attack, it is then down to the administrator to determine if it is a legitimate source. By determining the legitimacy of the source the administrator is able to determine if he/she can disable communications from this source.

Signature of attack: IDS will identify the nature of the attack and the pattern of the attack and alert accordingly. This information alerts the organization to the types of vulnerabilities that they are susceptible to and permits them to take precautions accordingly.

The above information allows an organization to:

- Build a vulnerability profile of their network and the required precautions.
- Plan its corporate defense strategy
- Budget for security expenditure
- IDS and Firewalls

A common misunderstanding is that firewalls recognize attacks and block them. This is not true.

Firewalls are simply a device that shuts off everything, then turns back on only a few well-chosen items. In a perfect world, systems would already be "locked down" and secure, and firewalls would be unneeded. The reason we have firewalls is precisely because security holes are left open accidentally. Thus, when installing a firewall, the first thing it does is stops ALL communication. The firewall administrator then carefully adds "rules" that allow specific types of traffic to go through the firewall. For example, a typical corporate firewall allowing access to the Internet would stop all UDP and ICMP datagram traffic, stops incoming TCP connections, but allows outgoing TCP connections. This stops all incoming connections from Internet hackers, but still allows internal users to connect in the outgoing direction.

A firewall is simply a fence around you network, with a couple of well chosen gates. A fence has no capability of detecting somebody trying to break in (such as digging a hole underneath it), nor does a fence know if somebody coming through the gate is allowed in. It simply restricts access to the designated points.

In summary, a firewall is not the dynamic defensive system that users imagine it to be. In contrast, IDS is much more of that dynamic system. IDS do recognize attacks against the network that firewalls are unable to see.

For example, in April of 1999, many sites were hacked via a bug in ColdFusion. These sites all had firewalls that restricted access only to the web server at port 80. However, it was the web server that was hacked. Thus, the firewall provided no defense. On the other hand, an intrusion detection system would have discovered the attack, because it matched the signature configured in the system.

Another problem with firewalls is that they are only at the boundary to your network. Roughly 80% of all financial losses due to hacking come from inside the network. A firewall a the perimeter of the network sees nothing going on inside; it only sees that traffic which passes between the internal network and the Internet.

Some reasons for adding IDS to you firewall are:

- Double-checks misconfigured firewalls.
- Catches attacks that firewalls legitimate allow through (such as attacks against web servers).
- Catches attempts that fail.

- Catches insider hacking.

LIMITATIONS OF IDS

Network intrusion detection systems are unreliable enough that they should be considered only as secondary systems designed to backup the primary security systems.

Primary systems such as firewalls, encryption, and authentication are rock solid. Bugs or misconfiguration often lead to problems in these systems, but the underlying concepts are "provably" accurate. The underlying concepts behind NIDS are not absolutely accurate. Intrusion detection systems suffer from the two problems whereby normal traffic causes many false positives (cry wolf), and careful hackers can evade or disable the intrusion detection systems. Indeed, there are many proofs that show how network intrusion detection systems will never be accurate.

This doesn't mean intrusion detection systems are invalid. Hacking is so pervasive on today's networks that people are regularly astounded when they first install such systems (both inside and outside the firewall). Good intrusion detection systems can dramatically improve the security of a site. It just needs to be remembered that intrusion detection systems are backup.

Switched network (inherent limitation)

Switched networks pose dramatic problems to network intrusion detection systems. There is no easy place to "plug in" a sensor in order to see all the traffic. For example, somebody on the same switched fabric as the CEO has free reign to attack the CEO's machine all day long, such as with a password grinder targeting the File and Print sharing. There are some solutions to this problem, but not all of them are satisfactory.

Resource limitations

Network intrusion detection systems sit at centralized locations on the network. They must be able to keep up with, analyze, and store information generated by potentially thousands of machines. It must emulate the combined entity of all the machines sending traffic through its segment. Obviously, it cannot do this fully, and must take short cuts.

Network traffic loads

Current NIDS have trouble keeping up with fully loaded segments. The average website has a frame size of around 180-bytes, which translates to about 50,000 packets/second on a 100-mbps Ethernet. Most IDS units cannot keep up with this speed. Most customers have less than this, but it can still occasionally be a concern.

TCP connections

IDS must maintain connection state for a large number of TCP connections. This requires extensive amount of memory. The problem is exacerbated by evasion techniques, often requiring the IDS to maintain connection information even after the client / server have closed it.

Long term state

A classic problem is "slow scans", where the attacker scans the system very slowly. The IDS is unable to store that much information over that long a time, so is unable to match the data together.

Attacks against the NIDS

The intrusion detection system itself can be attacked in the following ways:

Blind the sensor

Network intrusion detection systems are generally built as "passive monitors" from COTS (commercial-off-the-shelf) computers. The monitors are placed alongside the networking stream, not in the middle. This means that if they cannot keep up with the high rates of traffic, they have no way to throttle it back. They must start dropping packets. Not only will the sensor start dropping packets, high traffic rates can completely shut down the sensor. Therefore, an intruder can attack the sensor by saturating the link.

Blind the event storage (snow blind)

The 'nmap' port scanning tool contains a feature known as "decoy" scans. It scans using hundreds of spoofed source addresses as well as the real IP address of the attacker. It therefore becomes an improbable task for the administrator to find discover which of the IP addresses was real, and which was one of the decoy addresses. Any attack can be built from the same components. A massive attack with spoofed addresses can always hide a real attack inserted somewhere inside. Administrators would be hard pressed to discover the real attack inside of all that noise.

These two scenarios still retain forensics data, though. If the attacker is suspected, the data is still there to find. Another attack is to fill up event storage. When the database fills up, no more attacks will be discovered, or older attacks will be deleted. Either way, no evidence exists anywhere that will point to the intruder.

Simple evasion

This section describes simple evasion tactics that fool basic intrusion detection systems.

Fragmentation

Fragmentation is the ability to break up a single IP packet into multiple smaller packets. The receiving TCP/IP stack then reassembles the data back again before forwarding the data back up to the application. Most intrusion detection systems do not have the ability to reassemble IP packets. Therefore, there exist simple tools that can auto-fragment attacks in order to evade IDS.

Slow scans

Because of the volume of traffic on the wire, NIDS have difficulty maintaining long-term traffic logs. It is therefore difficult to detect "slow scans" (ping sweeps or port-scans) where intruders scan one port/address every hour.

Coordinated, low-bandwidth attacks

Sometimes hackers get together and run a slow scan from multiple IP addresses. This make it difficult for an intrusion detection system to correlate the information.

Address spoofing/proxying

One goal of intrusion detection is to point fingers at who is attacking you. This can be difficult for a number of reasons. In 'Smurf' attack, for example, you receive thousands of replies from a packet that you never sent. The NIDS can detect those replies, but cannot discover who sent the forged packet.

6. Intrusion Detection Definition

The Intrusion System (IDS) is traditionally deployed to monitor traffic in vital segments in the network, generating alerts when an intrusion is detected. The importance of the IDS has grown significantly as the industry recognizes that 90 percent of attacks in recent years have exploited application vulnerabilities. The traditional stateful inspection firewall, based largely on matching packet header information against Access Control Lists (ACLs), is ineffective to fend off such attacks. Good IDS, on the other hand, can expose these application layer attacks.

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat. We’ll cover each of these briefly.

What is intrusion?

An intrusion is somebody attempting to break into or misuse your system. The word "misuse" is broad, and can reflect something severe as stealing confidential data to something minor such as misusing your email system for Spam.

What is IDS?

IDS are the real-time monitoring of network/system activity and the analyzing of data for potential vulnerabilities and attacks in progress.

Intrusion Detection Systems is a topic that has recently garnered much interest in the computer security community. In the last few years, this interest level has spurred the development of a variety of approaches to providing IDS capabilities that are both reliable and low-impact in terms of management or cost. When presented with different types of IDS one might be tempted to assume that one approach or another was inherently superior. In fact, the mixture of approaches used for IDS offers the security analyst a unique opportunity in terms of the synergies inherent in combined techniques. Intrusion Detection Systems are like a burglar alarm for your computer network. They detect unauthorized access attempts. They are the first line of defense for your computer systems.

NEED FOR IDS

Who are attacked?

Internet Information Services (IIS) web servers – which host web pages and serve them to users – are highly popular among business organizations, with over 6 million such servers installed worldwide. Unfortunately, IIS web servers are also popular among hackers and malicious fame-seekers – as a prime target for attacks! As a result, every so often, new exploits emerge which endanger your IIS web server's integrity and stability. Many administrators have a hard time keeping up with the various security patches released for IIS to cope with each new exploit, making it easy for malicious users to find a vulnerable web server on the Internet. There are multiple issues which can completely endanger your Web server – and possibly your entire corporate network and reputation.

People fell there is nothing on their system that anybody would want. But what they are unaware of is that, there is the issue of legal liability. You are potentially liable for damages caused by a hacker using your machine. You must be able to prove to a court that you took "reasonable" measures to defend yourself from hackers. For example, consider if you put a machine on a fast link (cable modem or DSL) and left administrator/root accounts open with no password. Then if a hacker breaks into that machine, then uses that machine to break into a bank, you may be held liable because you did not take the most obvious measures in securing the machine.

NIDS

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.

HIDS

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

Signature Based

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat.

Anomaly Based

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is “normal” for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

Passive IDS

A passive IDS simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to take action to block the activity or respond in some way.

Reactive IDS

Reactive IDS will not only detect suspicious or malicious traffic and alert the administrator, but will take pre-defined proactive actions to respond to the threat. Typically this means blocking any further network traffic from the source IP address or user.

One of the most well known and widely used intrusion detection systems is the open source, freely available Snort. It is available for a number of platforms and operating systems including both Linux and Windows. Snort has a large and loyal following and there are many resources available on the Internet where you can acquire signatures to implement to detect the latest threats. There is a fine line between a firewall and IDS. There is also technology called IPS – Intrusion Prevention System. An IPS is essentially a firewall which combines network-level and application-level filtering with reactive IDS to proactively protect the network. It seems that as time goes on firewalls, IDS and IPS take on more attributes from each other and blur the line even more.

Essentially, your firewall is your first line of perimeter defense. Best practices recommend that your firewall be explicitly configured to DENY all incoming traffic and then you open up holes where necessary. You may need to open up port 80 to host web sites or port 21 to host an FTP file server. Each of these holes may be necessary from one standpoint, but they also represent possible vectors for malicious traffic to enter your network rather than being blocked by the firewall.

That is where your IDS would come in. Whether you implement a NIDS across the entire network or a HIDS on your specific device, the IDS will monitor the inbound and outbound traffic and identify suspicious or malicious traffic which may have somehow bypassed your firewall or it could possibly be originating from inside your network as well.

IDS can be a great tool for proactively monitoring and protecting your network from malicious activity, however they are also prone to false alarms. With just about any IDS solution you implement you will need to “tune it” once it is first installed. You need the IDS to be properly configured to recognize what is normal traffic on your network vs. what might be malicious traffic and you, or the administrators responsible for responding to IDS alerts, need to understand what the alerts mean and how to effectively respond.

7. Why do I need IDS?

An intruder normally hacks into your system only after he has carefully accessed you and your security and he attacks you in a systematic way to cause maximum damage. The normal steps towards intrusion are:

Outside reconnaissance: The intruder will find out as much as possible without actually giving himself away. They will do this by finding public information or appearing as a normal user. In this stage, you really can't detect them. The intruder will do a 'whois' lookup to find as much information as possible about your network as registered along with your Domain Name (such as foobar.com. The intruder might walk through your DNS tables (using 'nslookup', 'dig', or other utilities to do domain transfers) to find the names of your machines. The intruder will browse other public information, such as your public web sites and anonymous FTP sites. The intruder might search news articles and press releases about your company.

Inside reconnaissance: The intruder uses more invasive techniques to scan for information, but still doesn't do anything harmful. They might walk through all your web pages and look for CGI scripts (CGI scripts are often easily hacked). They might do a 'ping' sweep in order to see which machines are alive. They might do a UDP/TCP scan/strobe on target machines in order to see what services are available. They'll run utilities like 'rcpinfo', 'showmount', 'snmpwalk', etc. in order to see what's available. At this point, the intruder has done 'normal' activity on the network and has not done anything that can be classified as an intrusion. At this point, a NIDS will be able to tell you that "somebody is checking door handles", but nobody has actually tried to open a door yet.

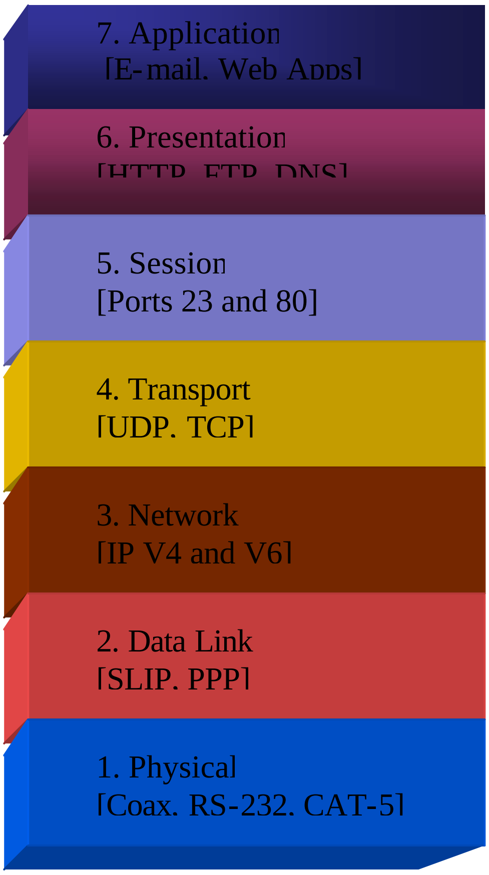
Exploit: The intruder crosses the line and starts exploiting possible holes in the target machines. The intruder may attempt to compromise a CGI script by sending shell commands in input fields. The intruder might attempt to exploit well-known buffer-overrun holes by sending large amounts of data. The intruder may start checking for login accounts with easily guessable (or empty) passwords. The hacker may go through several stages of exploits. For example, if the hacker was able to access a user account, they will now attempt further exploits in order to get root/admin access.

Foot hold: At this stage, the hacker has successfully gained a foot hold in your network by hacking into a machine. The intruder's main goal is to hide evidence of the attacks (doctoring the audit trail and log files) and make sure they can get back in again. They may install 'toolkits' that give them access, replace existing services with their own Trojan horses that have backdoor passwords, or create their own user accounts. System Integrity Verifiers (SIVs) can often detect an intruder at this point by noting the changed system files. The hacker will then use the system as a stepping stone to other systems, since most networks have fewer defenses from inside attacks.

Profit: The intruder takes advantage of their status to steal confidential data, misuse system resources (i.e. stage attacks at other sites from your site), or deface web pages.

8. Structure of IDS

An Intrusion Detection System (IDS) monitors all traffic passing by it looking for network data which matches pre defined rules within the IDS rules database. The rules database is searched for all network traffic and as soon as a match occurs, the appropriate defined action is taken, such as to log to the screen. An IDS is different from a firewall in that it doesn't actually block the data, it merely monitors it. An IDS also works differently from a Firewall in that the data doesn't have to be passing through it, it just has to be able to view it (the network adaptor is running in promiscuous mode). IDS can be configured to monitor for any network traffic you want by creating the appropriate rule. These rules are far more comprehensive than firewall rules. For example a typical firewall rule maybe to let Telnet traffic through. IDS may expand on this to log if Telnet traffic is received which contains the string 'root' in the data – this could indicate someone trying to login the Telnet server with the super user account root. Although the IDS would not block the data it would alert you to the fact that there could be a problem. A typical alert from a open source IDS called Snort (www.snort.org) is:



```
07-01-2002 06:33:07 Auth.Alert 192.168.1.10 snort[786]: [1:0:0]  CodeRed Defacement: 211.57.12.69:2491 -> 192.168.1.11:80
```

This alerts us to the fact that an attempted CodeRed Defacement took place. Of course it didn't succeed because the server was patched to prevent it.

The rules within IDS can be very detailed, and can even be set to detect particular versions of software transmitting data. Below is an example of an alert a ping has taken place using the Nmap software, recorded again by Snort:

```
10-02-2002 01:01:19 Auth.Alert snort[1156]: IDS162 - PING Nmap2.36BETA: 202.37.133.114 (nkvd.sli.net.nz) (nkvd.sli.net.nz) -> 192.168.1.10
```

It's possible to use the output from IDS to update rules within the firewall. This allows greater levels of control of exactly what traffic to block than could be expected by using a firewall alone. For example IDS might instruct the firewall to block all access to all services from a particular host because it's detected suspicious activity from the host.

9. Development

Detection alone is insufficient - it is also important to terminate the attack upon detection. Hence, the trend is to evolve the IDS into an Intrusion Prevention System (IPS), which takes detection to the next level and stops the detected attacks, including application attacks.

Summary and Conclusions

Personal firewalls are useful and should be considered by any Windows user who directly connects to hostile networks, such as the Internet. They have a role to play in both the corporate and SOHO (Small Office/Home Office) markets. Although many products are immature, there have been major advances over recent months. All these products need to be subjected to more scrutiny and given time to prove their security effectiveness. None of these products is provided with source code.

- There is a tendency for antivirus and personal firewalls to be integrated into the one product, which is not necessarily a good thing. It may make sense for the home user, but the corporate user may find his antivirus already mandated by a central IT organization, or may want the choice of separate tools.
- Personal firewalls can't just be installed and forgotten about. The user has to learn how to use them and understand their interface/consequences, for them to be effective.
- The main difficulties are making such products easy to use, being flexible enough for power users, and reducing false positives (a common ailment among intrusion detection systems).
- Personal Firewalls cannot offer 100% protection. For instance, they can be badly configured, or switched off; can start too late (e.g., after Trojans are running or long after the TCP/IP stack is active); they might not recognize all hostile traffic; they may have bugs; may crash, etc. It's a good strategy to have several barriers to attackers, e.g., antivirus tools, file encryption, good passwords, a well-configured OS. The underlying operating system also plays a role: security-conscious Windows users are advised to use NT or Win2K and configure them restrictively.

As IDS technologies continue to evolve, they will more closely resemble their real-world counterparts. Instead of isolated sensor units, the IDS of the future will consist of sensor units that report to master visualization consoles which are responsible for checking whether alerts from the sensors agree or correlate to likely event-chains. In the future, IDS, firewalls, VPNs, and related security technologies will all come to interoperate to a much higher degree. As IDS data becomes more trustworthy because of better coverage, firewalls and VPN administrators will be more comfortable with reacting based on the input from the IDS. The current generations of IDS (HIDS and NIDS) are quite effective already; as they continue to improve they will become the backbone of the more flexible security systems we expect to see in the not-too-distant future.

References

1. **Nmap**
   http://www.insecure.org/nmap
2. **Netbus Pro: Remote-control program often used as an attack tool to control remote PCs.**
   http://netbus.nu/
3. **Toy Box** (a collection of tools that may help clean a system possessed by Trojans)
   http://home.earthlink.net/~rmbox/Reticulated/Toys.html
4. **Best Comparative Personal Firewall Review**
   http://www.firewallguide.com/freeware.htm
5. **ADSL: Security Risks and Countermeasures** - *Sean Boran*
   pf_adsl20010614.html
   ADSL Firewalls: Product Reviews - *Sean Boran*
   pf_adsl_tests_20010627.html
6. **Free remote testing of your open ports**:
   Neoworx port probe: http://www.hackerwatch.org/probe/

CHANGE MANAGEMENT

1stLT Ovidiu OLARIU

UM 01714 Pitesti

> *"It must be considered that there is nothing more difficult to carry out nor more doubtful of success nor more dangerous to handle than to initiate a new order of things."*
> Machiavelli (1446-1507)

Introduction

Motivation

There is nothing more constant than change.
Take care of change, or it will take care of you.
Information security cannot be static.
Technologies do not last too much.

Be proactive!

Premises

Explicit part = what is written
Implicit part = what is not written, what is behind the text and is part of the same truth.
A thing discovered by YOU is a better understood one.

In this paper, starting from the explicit text and using the reading keys you will be able to build an implicit part of it that matches your organization and your personality.

It is difficult to have good answers without good questions.

We do not provide answers here. Combining the text and reading keys you will produce the answers you need.

1. The reading keys

The epistemology went beyond the systemic level of explanations, but at that level things can not be understand without a proper formation in the procesuality domain. To simplify the presentation we propose the "change" instead of "evolution, becoming, procesuality".

For accessibility reasons, we kept the management terminology.

Because we want to provoke the reader and not just to provide some text, please pay attention to the implicit aspects starting from the explicit ones.

For that, we suggest to put yourself during the reading at least the following question-keys:

- How is information security affected by changes within organization?
- How is organization affected by changes within information security?
- What implies an individual change?
- What can be use in your military organization?

2. Definition

Change management[8] is a systematic approach to dealing with change, both from the perspective of an organization and on the individual level. A somewhat ambiguous term, change management has at least three different aspects, including: adapting to change, controlling change, and effecting change. A proactive approach to dealing with change is at the core of all three aspects. For an organization, change management means defining and implementing procedures and/or technologies to deal with changes in the business environment and to profit from changing opportunities.

Successful adaptation to change is as crucial within an organization as it is in the natural world. Just like plants and animals, organizations and the individuals in them inevitably encounter changing conditions that they are powerless to control. The more effectively you deal with change, the more likely you are to thrive. Adaptation might involve establishing a structured methodology for responding to changes in the business environment (such as a fluctuation in the economy, or a threat from a competitor) or establishing coping mechanisms for responding to changes in the workplace (such as new policies, or technologies).

In a computer system environment, change management refers to a systematic approach to keeping track of the details of the system (for example, what operating system release is running on each computer and which fixes have been applied).

3. Different principles

3.1. Basic principles 1

Change management is a basic skill in which most leaders and managers need to be competent.

When leaders or managers are planning to manage change, there are five key **principles** that need to be kept in mind[9]:

1. Different people react differently to change
2. Everyone has fundamental needs that have to be met
3. Change often involves a loss, and people go through the "loss curve"
4. Expectations need to be managed realistically
5. Fears have to be dealt with

<u>Different people react differently to change</u>

The following diagram represents a spectrum of change:

Stability - - - - - - - - - - - - - - - Change

Different people have different preferences for where they like to be on this spectrum. Some people like to be at the STABILITY end of the spectrum - they like things to be the way they have always been. Other people like to be at the CHANGE end of the spectrum - they are always looking for something different and new.

Problems arise when the individual's preferences differ from the situation they find themselves in. That is, if:

- a stability-oriented person finds that circumstances are changing quite rapidly, or
- a change-oriented person finds that everything is the same and there is nothing new.

In these situations, the individuals involved can experience:

- strong dissatisfaction
- stress
- negative attitudes towards individuals with preferences at the other end of the spectrum (eg: distrust, dislike)
- resistance (to change, or to the status quo)

[8] http://searchciomidmarket.techtarget.com/sDefinition/0,,sid183_gci799426,00.html
[9] http://www.teamtechnology.co.uk/changemanagement1.html

- intense emotions
- loss of rational judgment

People tend to resist, therefore, approaches on other parts of the spectrum than where they themselves prefer to be.

Everyone has fundamental needs that have to be met

A famous psychologist called Will Schutz identified three basic needs that people have in interpersonal relations. These basic needs are also of fundamental importance in people's reaction to change:

- The need for control,
- The need for inclusion,
- The need for openness.

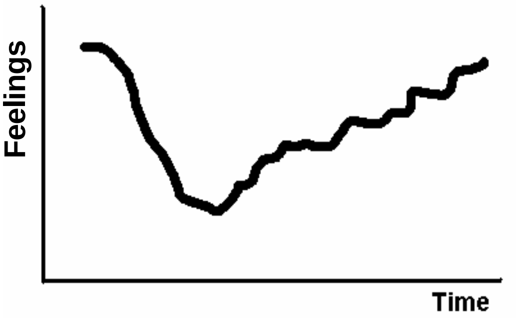
Whilst the need for these can vary between people, in any change process there is always some degree of need for control over one's environment/destiny, some degree of need to be included in the process of forming the change that is taking place, and some degree of need for managers/leaders to be open with their information.

If a change program fails to meet the control, inclusion and openness needs of the individuals affected by it then that program is likely to encounter a range of negative reactions, ranging from ambivalence through resistance to outright opposition.

Change often involves a loss, and people go through the "loss curve"

The relevance of the "loss curve" to a change management program depends on the nature and extent of the loss. If someone is promoted to a more senior position, the 'loss' of the former position is rarely an issue because it has been replaced by something better. But if someone is made redundant with little prospect of getting a new job, there are many losses (income, security, working relationships) that can have a devastating effect.

There are many variations of the "loss curve". One is known as "Sarah" - that is, the individual experiences (in this order):



1. S-hock
2. A-nger
3. R-ejection
4. A-cceptance
5. H-ealing

The common factors amongst all "loss curves" are:

- there can be an initial period where the change does not sink in. For example, feelings may be kept high by the individual convincing themselves that the change is not going to happen.
- when the loss is realized, the individual hits a deep low. The depth of this 'low' is deepened if the loss is sudden/unexpected.
- the period of adjustment to the new situation can be very uncomfortable and take a long time. In the case of bereavement, the period of adjustment can be as long as two years.

Expectations need to be managed realistically

The relationship between expectations and reality is very important. You can see this in customer relations - if a supplier fails to meet expectations then the customer is unhappy; if the supplier exceeds expectations then the customer is happy.

To some extent the same principle applies to staff and change. If their expectations are not met, they are unhappy. If their expectations are exceeded, they are happy.

Sometimes, enforced change (eg: redundancies) inevitably involve the failure to meet expectations: there had been an expectation of job security, which has now been taken away.

What leaders/managers have to do, however, is make sure they don't pour petrol on the fire by making promises that can not or will not be kept. Expectations have to be set at a realistic level, and then exceeded (eg: in terms of the degree of outplacement support that will be provided).

Fears have to be dealt with

In times of significant change rational thought goes out of the window. This means that people often fear the worst - in fact, they fear far more than the worst, because their subconscious minds suddenly become illogical and see irrational consequences. Eg:

- Our company is reducing staff, which means...
- They will make people redundant, and...
- I'll be the first to be kicked out, and...
- I'll have no hope of getting another job, and...
- I won't be able to pay the mortgage, so...
- I'll lose the house, so...
- My family won't have anywhere to live, and...
- My wife won't be able to cope, so...
- She'll leave me, and...
- I'll be so disgraced the children won't speak to me ever again.

Such fears need to be addressed, eg by helping people to recognize that most people who are made redundant find a better job with better pay and have a huge lump sum in their pocket! Or, where appropriate, by explaining how the reductions in staff numbers are going to be achieved (by natural wastage or voluntary redundancy).

3.2 Basic principles 2

1. At all times involve and agree support from people within system (system = environment, processes, culture, relationships, behaviors, etc., whether personal or organizational).
2. Understand where you/the organization is at the moment.
3. Understand where you want to be, when, why, and what the measures will be for having got there.
4. Plan development towards above No.3 in appropriate achievable measurable stages.
5. Communicate, involve, enable and facilitate involvement from people, as early and openly and as fully as is possible.

As you see it is difficult to know what “basic” is. The 2 sets of principles are not equivalent. After the enumeration of the first set the reader may start to build the implicit part for every principle. Comparing them with the explicit explanation offered by the author, the reader may find the last ones poor or inadequate.

Two sets may be generated by two points of view. What implication may have *changing the point of view?*

4. Different techniques

4.1. Tips to apply

Here are some tips to apply the above principles when managing change:

- Give people information - be open and honest about the facts, but don't give overoptimistic speculation. Meet their OPENNESS needs, but in a way that does not set UNREALISTIC EXPECTATIONS.
- For large groups, produce a communication strategy that ensures information is disseminated efficiently and comprehensively to everyone Eg: tell everyone at the same time. However, follow this up with individual interviews to produce a personal strategy for dealing with the change. This helps to recognize and deal appropriately with the INDIVIDUAL REACTION to change.

- Give people choices to make, and be honest about the possible consequences of those choices. Meet their CONTROL and INCLUSION needs.
- Give people time, to express their views, and support their decision making, providing coaching, counseling or information as appropriate, to help them through the LOSS CURVE.
- Where the changes involves a loss, identify what will or might replace that loss - loss is easier to cope with if there is something to replace it. This will help assuage potential FEARS.
- Where it is possible to do so, give individuals opportunity to express their concerns and provide reassurances - also to help assuage potential FEARS.
- Keep observing good management practice, such as making time for informal discussion and feedback (even though the pressure might seem that it is reasonable to let such things slip - during difficult change such practices are even more important).

Where you are embarking on a large change programmes, you should treat it as a project. That means you apply all the rigors of project management to the change process - producing plans, allocating resources, appointing a steering board and/or project sponsor etc.. The five principles above should form part of the project objectives.

4.2 Steps to successful change

John P. Kotter in "The Heart Of Change" (2002) describe a helpful model for understanding and managing change. Each stage acknowledges a key principle identified by Kotter relating to people's response and approach to change, in which people **see**, **feel** and then **change** the eight step change model can be summarized as[10]:

1. **Increase urgency** - inspire people to move, make objectives real and relevant.
2. **Build the guiding team** - get the right people in place with the right emotional commitment, and the right mix of skills and levels.
3. **Get the vision right** - get the team to establish a simple vision and strategy, focus on emotional and creative aspects necessary to drive service and efficiency.
4. **Communicate for buy-in** - Involve as many people as possible, communicate the essentials, simply, and to appeal and respond to people's needs. De-clutter communications - make technology work for you rather than against.
5. **Empower action** - Remove obstacles, enable constructive feedback and lots of support from leaders - reward and recognize progress and achievements.
6. **Create short-term wins** - Set aims that are easy to achieve - in bite-size chunks. Manageable numbers of initiatives. Finish current stages before starting new ones.
7. **Don't let up** – Build and encourage determination and persistence - ongoing change - encourage ongoing progress reporting - highlight achieved and future milestones.
8. **Create a new culture** - reinforce the value of successful change via recruitment, promotion, new change leaders. Weave change into culture.

Different "basic principles" sets always conduct to different techniques that will be use. Different results and consequences are guaranteed. Information Security Policies can not be the same in two distinct units and they can not remain unchanged during a long period of time.

5. The change management process

Habits are a normal part of every person's lives, but it is often counterproductive when dealing with change.

As humans we are not very good at changing. We see changes as a negative thing, something that creates instability and insecurity. A normal change management process often evolves trough number of mental phases:

[10] John P. Kotter, "The Heart Of Change", 2002

1. **Denial -** Where we fight the change and protect status quo.
2. **Frustration and anger -** When we realize that we cannot avoid the change and we become insecure because of lack of awareness.
3. **Negotiation and bargaining -** Where we try to save what we can.
4. **Depression -** When we realize that none of the old ways can be incorporated into the new.
5. **Acceptance -** When we accept the change, and start to mentally prepare ourselves.
6. **Experimentation -** Where we try to find new ways, and gradually remove the old barriers.
7. **Discovery and Delight -** When we realize that the change will improve our future possibilities.
8. **Integration -** Where we implement the change.

Notice: These phases are usually referred to as the Change Curve. It is described and visualized in many varieties.

The first four phases are very negative and counterproductive. To solve this quickly focus on understanding (what's and why's) and the potential possibilities the change will bring with it. Try to create energy from start to finish and ensure that everyone is committed.

6. A complex change management model

The complex model[11] can be used for very large and complicated change management projects. It usually involved a large group of people from many different departments. It also covers change of more than one thing. The project duration is usually between 6-36 months. The project is very complex and covers the majority of the company. The project contains a significant amount of unknown factors and tasks.

The time needed for **analysis is sizeable and takes more than 60% of the total project time**. A senior group of people (a top-level analysis team) is gathering and evaluating what each project team should do.

The project itself will be handled by a number of "Power Teams" – dedicated project team, which covers parts of the total project.

An open information policy is vital, as many employees will have doubts about themselves and the project ("what does this mean to me?", "Will I be fired?" etc.) It is very important to inform **why we need to change**, and **what we expect the future to be like**.

Marking the end is often a critical action in complex change management projects.

Unfreeze
01 What is going on – and why
Analysis
02 "Need-for-Change" Cost/Benefit
Analysis
03 Establish analysis team
Action
04 Explain the situation
Action
05 Discuss the change
Action
06 Listen
Action
07 Invalidate present rules and policies
Action
08 Mark the end

[11] Thomas Baekdal, Change Management Handbook**,** http://www.baekdal.com/reports/change/change-management/

Notice: from this day, all existing rules and attitudes no longer applies
Action
09 Define your vision
Action
10 Define your goals
Action
11 Know you target group
Analysis
12 Identify problems
Analysis
13 Create your "Power Teams" - Project teams
Action
14 Create a plan
Notice: With short term goals and changes
Analysis / Action

Move
01 Explain your vision, goals and plan – in relation to the future outcome
Action
02 Ensure a sense of security
Action
03 Get everyone onboard
Action
04 Act!
Action
05 Evaluate, notice and present improvements/results – create energy
Analysis / Action
06 Encourage great work – coach bad
performers
Action
07 Listen
Get the pulse of your team
Action
08 Adjust your plan
Slow down is necessary
Action
09 Ensure accept for the next step
Action
10 Close the current task - create energy for the next
Action
11 Repeat
Action

Freeze
01 Define new rules and policies
Action
02 Present the new "way of life"
Action
03 Celebrate - create energy
Action
04 Evaluate the result
Analysis

05 (Unfreeze - and start the next project)
Action

At Postgraduate level, the best way to analyze a phenomenon is from general to particular. We propose this model as reference, having the advantage of being adaptable to particular situation. What percentage and what critical areas are covered for a user, an administrator or a manager (commander)?

Conclusions

For a better sustain of change subject, we had to change the way we usually speak about changes.

This could be an exercise for information security administrators and an inspirational source for their work.

Changes may trigger threats and vulnerabilities.

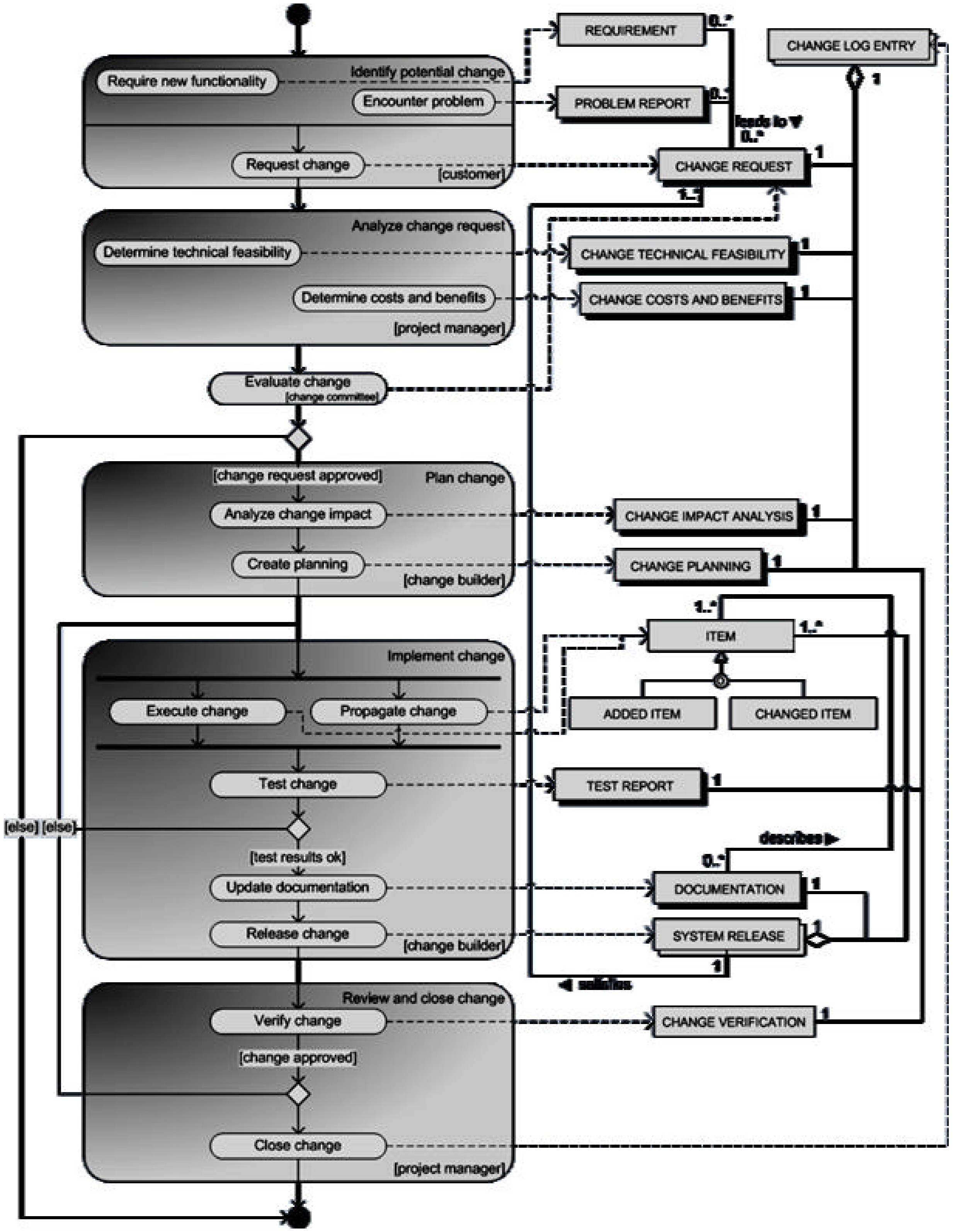
Change-based security covers all classical aspects for managers (and not only, sensors are triggered by a change too) and underlines better the importance of proactivity.

The authorities could improve the structure of documents for accreditation.

References

1. http://searchciomidmarket.techtarget.com/sDefinition/0,,sid183_gci799426,00.html
2. http://www.teamtechnology.co.uk/changemanagement1.html
3. John P. Kotter, “The Heart Of Change”, 2002
4. Thomas Baekdal, Change Management Handbook,
   http://www.baekdal.com/reports/change/change-management/

Appendix A



The process-data diagram

Appendix B

The Top 10 Principles For Leading Change

1. **Keep performance results the primary objective of behavior and skill change.**
2. **Continually increase the number of individuals taking responsibility for their own change.**
3. **Make sure that each person always knows why his or her performance and change matters to the purpose and results of the whole organization.**
4. **Put people in a position to learn by doing and provide them with the information and support they need just in time to perform.**
5. **Embrace improvisation as the best path to both performance and change.**
6. **Use team performance to drive change whenever demanded.**
7. **Concentrate organizational designs on the work that people do, not on the decision-making authority they have.**
8. **Create and focus energy and meaningful language because these are the scarcest resources during periods of change.**
9. **Stimulate and sustain behavior-driven change by harmonizing initiatives throughout the organization.**
10. **Practice leadership based on the courage to live the change you wish to bring about.**

About the Submitter:

Submitted by Coach Charles Powell, MCC, who can be reached at coach@coach-charles.com, or visited on the web at http://coachingatitsbest.homestead.com. The original source is: Douglas K. Smith in Leader to Leader, ed. F. Hesselbein & P.M. Cohen.

Appendix C

The Top 10 Questions To Ask Before Implementing Organizational Change

1. **Have we got the right leadership and "buy-in" support for the proposed change?**
2. **Is the proposed change aligned with the strategic plan?**
3. **What current/future issues/concerns will performance measurement/management address?**
4. **What are the implications and barriers to successful implementation?**
5. **What are the inherent risks/costs of not embracing the change?**
6. **Who should we target as the key drivers for the "new way we are going to do things round here?"**
7. **What processes will we need to change/introduce?**
8. **How will success be measured and what value will success have for the business and individual?**
9. **How do we change people's behavior**
10. **Who will feel threatened by the change?**

About the Submitter:

Submitted by Cam Sorenson, who can be reached at cams@corp-strategies.com, or visited on the web at http://www.corp-strategies.com

Appendix D

The Top 10 Reasons Employees Resist Change

1. **The individual's personal predisposition to change.**
2. **Surprise and fear of the unknown.**
3. **Climate of mistrust.**
4. **Fear of failure.**
5. **Loss of status and/or job security**
6. **Peer pressure.**
7. **Disruption of cultural traditions and/or group relationships.**
8. **Personality conflicts.**
9. **Lack of tact and/or poor timing.**
10. **Not seeing the benefits.**

http://topten.org/public/AC/AC224.html

Appendix E

The Top 10 Steps to Making Major Life Changes

1. **Identify the payoffs and price of staying where you are.**
2. **Begin developing a reserve of everything.**
3. **Develop a vision of what's possible to pull you through the transition.**
4. **Uncover your self-judgments.**
5. **Give up playing the victim.**
6. **Give up analysis that breeds paralysis.**
7. **Risk failure.**
8. **Access your inner warrior.**
9. **Don't go to your deathbed wondering what would have happened if...**
10. **Get support to prepare and walk with you through the transition.**

About the Submitter:

This piece was originally submitted by Steve Davis, MS, MA, CCUG, Life Coach and Infopreneur, steve@livingmastery.com,

Appendix F

The Top 10 Things To Consider When Planning Or Making Big Changes

1. **What is the worst that could happen?**
2. **Whom will my making this change impact?**
3. **What do I need to have in place to feel OK about this change?**
4. **What do I need to do before making the change?**
5. **Who can help me, and how?**
6. **What will it cost me not to do it?**
7. **How will I make this work**
8. **How long will the journey take?**
9. **What will I do when I feel scared?**
10. **How can I celebrate my successes?**

About the Submitter:

Submitted by Aboodi Shaby, Coach U Graduate., aboodi@wonderful-life.com, http://www.makebigchanges.com

Appendix G

The Top 10 Things to Know About Transitions

1. **The involuntary ones are the hardest.**
2. **Transitions bring periods of deep introspection.**
3. **Transitions cause us to question who we are and who we'll be when they're over.**
4. **Transitions involve loss.**
5. **Transitions involve ambivalent feelings and therefore conflict.**
6. **Transitions are a part of life, because life is change.**
7. **Transitions are wonderful opportunities for evolving.**
8. **Some transitions have to be accomplished after the fact - a car accident that leaves you blind, for instance.**
9. **The more you fight a transition, the harder you'll make it on yourself.**
10. **Coaching is excellent for transitions.**

Appendix H

The Top 10 Ways to Become Change Proficient

1. **Resilient people thrive in constant change because they're flexible, agile, creative, adapt quickly, and synergistic.**
2. **Resilient people are curious, lifelong learners.**
3. **They're able to maintain their emotional stability, health and well being through trying times, which provides energy.**
4. **They can focus outwards, test reality well, and take action.**
5. **They can focus inward and have strong inner "selfs."**
6. **They have a talent for serendipity -- being able to find valuable or agreeable things not sought for.**
7. **They use problem-focused coping rather than emotion-focused coping.**
8. **They're able to learn from experience, including past adversities.**
9. **They have minds and habits that create bridges, not barriers, to a better future.**
10. **The struggle to bounce back from adversity can develop strengths and abilities you never dreamed possible.**

This piece was originally submitted by Susan Dunn, M.A., Author of The Resilience Course, The EQ Coach, sdunn@susandunn.cc

Appendix I

The Top 10 Ways To Manage Change Effectively

1. **Accept change as a fact of life.**
2. **Commit yourself to lifelong learning.**
3. **Get healthy then stay healthy.**
4. **Look at change as an opportunity.**
5. **Develop and maintain a strong network and support team.**
6. **Develop your spirituality.**
7. **Engage in rituals.**
8. **Eliminate the tolerations in your life.**
9. **Keep a daily journal.**
10. **Engage in meditation.**

About the Submitter:

Submitted by Mershon Bell, mershon@mershonbell.com, or http://www.mershonbell.com

DESIGN, IMPLEMENT AND MAINTAIN AN INFORMATION SECURITY MANAGEMENT SYSTEMS WITH ISO/IEC 27000-SERIES

LTC Gabriel Ion CIUPITU

UM 02416 Bucuresti

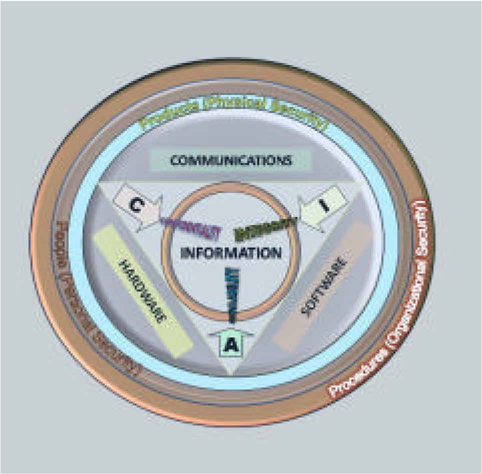
Introduction

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide

– *integrity*, which means guarding against improper information modification or destruction, and includes ensuring information *nonrepudiation* and authenticity;

– confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;

– *availability*, which means ensuring timely and reliable access to and use of information[12].


Products (Physical Security)
COMMUNICATIONS
C
I
INFORMATION
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

While **Information security** (ISec) describes activities that relate to the protection of information and information infrastructure assets against the risks of loss, misuse, disclosure or damage, **Information security management** (ISM) describes controls that an organization needs to implement to ensure that it is sensibly managing these risks.

An *information security management system* (ISMS) is, as the name implies, a set of policies concerned with information security management.

The key concept of ISMS is for an organization to design, implement and maintain a coherent suite of processes and systems for effectively managing information accessibility,

[12] U.S. Code collection > TITLE 44 > CHAPTER 35 > SUBCHAPTER III > § 3542. Definitions

thus ensuring the confidentiality, integrity and availability of information assets and minimizing information security risks.

1. The ISO/IEC 27000-series

Known as the 'ISMS Family of Standards' or 'ISO27k' for short, the ISO/IEC 27000 - series comprises *information security standards* published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO27k series provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS) and covers more than just privacy, confidentiality and IT or technical security issues.

The standards are the product of ISO/IEC JTC1 (Joint Technical Committee 1) SC27 (Sub Committee 27), an international body that meets in person twice a year.

ISMS family of standards is intended to assist organizations of all types and sizes to implement and operate an ISMS. The ISMS family of standards consists of the following International Standards, under the general title *Information technology — Security techniques*:

- ISO/IEC 27000:2009, *Information security management systems — Overview and vocabulary*
- ISO/IEC 27001:2005, *Information security management systems — Requirements*
- ISO/IEC 27002:2005, *Code of practice for information security management*
- ISO/IEC 27003, *Information security management system implementation guidance*
- ISO/IEC 27004, *Information security management — Measurement*
- ISO/IEC 27005:2008, *Information security risk management*
- ISO/IEC 27006:2007, *Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27007, *Guidelines for information security management systems auditing*
- ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

It is important that SC27's remit extends well beyond the ISO27k standards, covering identity management, biometrics and other aspects of information security.

From ISO/IEC 27011 to 27019 are dedicated Sector-specific ISMS implementation guidelines, in order to help certain industries implement the ISO27k standards. These are likely to contain advice on the application of typical information security controls already noted in ISO/IEC 27002 within each industry, but may include new information security controls that are specific to certain industries.

ISO/IEC 27011 provides ISMS implementation guidance for the telecomms.

ISO/IEC 27012 provides ISMS implementation guidelines for eGovernment services.

ISO/IEC 27015 provides ISMS implementation guidelines for the financial services sector.

The following industry sectors will also be covered by ISMS implementation guidelines[13]:

- *The energy sector* and/or *utilities* - electricity generation and distribution, oil and gas refining and distribution etc.;
- *The healthcare sector* potentially including primary/local healthcare, hospitals, health boards, pharmaceuticals and more. As with the finance sector, it remains to be determined what will happen to ISO 27799 and other healthcare information security standards developed independently of SC27 and thus officially outside of ISO27k;
- *The defense sector* (armed forces and defense contractors/suppliers, maybe including aerospace) for whom security and information security are clearly vital, although

[13] http://www.iso27001security.com/html/other_27k.html

national interests may preclude or at least complicate international cooperation on common ISMS guidelines;

- *The transportation sector* potentially including train and bus companies, airlines etc.;
- *The food sector* potentially ranging from primary production (farms) through wholesale distribution to retail outlets (shops);
- *The media sector* (news, publishing etc.) for whom information is of course a vital input and the primary product;

Countries/nations define their most important and valuable industries differently. Holiday spots might define *the tourism sector* as vital, for instance, while something like *bauxite mining* might be crucial to just a few. ISMS implementation standards could potentially be developed to cover any sector.

2. ISO/IEC 27001 and ISO/IEC 27002

It is important for any organization to assess its information security risks and then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. The risks to these assets can be calculated by analysis of the following issues:

- *Threats to your assets.* These are unwanted events that could cause the deliberate or accidental loss, damage or misuse of the assets (a list is showed in Annex no. 1 and in annex no.2 the Top 10 information security threats for 2010 according to Perimeter E-Security[14]).
- *Vulnerabilities*. How susceptible your assets are to attack
- *Impact*. The magnitude of the potential loss or the seriousness of the event.

Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents.

The formal set of specifications against which organizations may design, implement and maintain their Information Security Management System (ISMS) is ISO/IEC 27001:2005[15].

The objective of the ISO 27001 standard is to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System"[16]. Regarding its adoption, this should be a strategic decision for an organization. Further, "The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the process employed and the size and structure of the organization"[17].

ISO 27001 consists of 134 best security practices which organizations can adopt to build their Security Infrastructure and covers the next 11 Domains:

1. Security Policy
2. Organizing Information Security
3. Asset Management
4. Human Resource Security
5. Physical & Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance
9. Information Security Incident Management

[14] http://www.net-security.org/secworld.php?id=8709 on 31-Ian -10

[15] ISO/IEC 27001:2005 Information technology -- Security techniques -- Specification for an ISMS

[16] idem.

[17] ISO/IEC FDIS 27001:2005 Information technology-- Security techniques – Information security management systems -- Requirements

10. Business Continuity Management
11. Compliance

ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It also specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. It is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

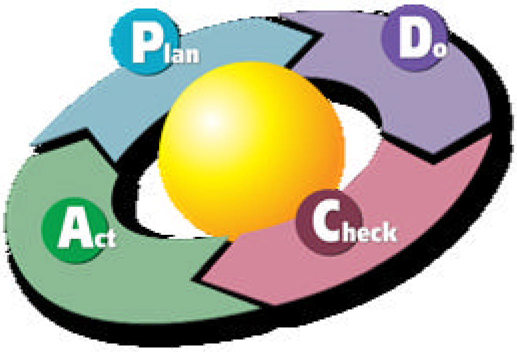
ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following:

- use within organizations to formulate security requirements and objectives;
- use within organizations as a way to ensure that security risks are cost effectively managed;
- use within organizations to ensure compliance with laws and regulations;
- use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- definition of new information security management processes;
- identification and clarification of existing information security management processes;
- use by the management of organizations to determine the status of information security management activities;
- use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons;
- implementation of business-enabling information security;
- use by organizations to provide relevant information about information security to customers.

PDCA Model

The PDCA cycle involves four basic steps – Plan, Do, Check and Act. These are:

- The **Plan** phase is about designing the ISMS, assessing information security risks and selecting appropriate controls.
- The **Do** phase involves implementing and operating the controls.
- The **Check** phase objective is to review and evaluate the performance (efficiency and effectiveness) of the ISMS.
- In the **Act** phase, changes are made where necessary to bring the ISMS back to peak performance.



The adoption of the PDCA model reflect the principles as set out in the OECD Guidelines (2002)[18] governing the security of information systems and networks. This Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

[18] OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org

ISO 27001 defines the four phases of the PDCA model, as follows:

Plan (establish the ISMS) - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

Do (implement and operate the ISMS) - Implement and operate the ISMS policy, controls, processes and procedures.

Check (monitor and review the ISMS) – Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

Act (maintain and improve the ISMS) - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS

ISO/IEC 27001:2005 outline

The ISO IEC 27001 2005 standard is an information security management standard. It defines a set of information security management requirements.

ISO/IEC 27001:2005 has the following sections:

0 Introduction - the standard uses a process approach.

1 Scope - it specifies generic ISMS requirements suitable for organizations of any type, size or nature.

2 Normative references - only ISO/IEC 27002:2005 is considered absolutely essential to the use of '27001.

3 Terms and definitions - a brief, formalized glossary, soon to be superseded by ISO/IEC 27000.

4 Information security management system - the 'guts' of the standard, based on the Plan-Do-Check-Act cycle. Also specifies certain specific documents that are required and must be controlled, and states that records must be generated and controlled to prove the operation of the ISMS (*e.g.* certification audit purposes).

5 Management responsibility - management must demonstrate their commitment to the ISMS, principally by allocating adequate resources to implement and operate it.

6 Internal ISMS audits - the organization must conduct periodic internal audits to ensure the ISMS incorporates adequate controls which operate effectively.

7 Management review of the ISMS - management must review the suitability, adequacy and effectiveness of the ISMS at least once a year, assessing opportunities for improvement and the need for changes.

8 ISMS improvements - the organization must continually improve the ISMS by assessing and where necessary making changes to ensure its suitability and effectiveness, addressing nonconformance (noncompliance) and where possible preventing recurrent issues.

Annex A - Control objectives and controls - little more in fact than a list of titles of the control sections in ISO/IEC 27002, down to the second level of numbering (*e.g.* 9.1, 9.2).

Annex B - OECD principles and this International Standard - a table briefly showing which parts of this standard satisfy 7 key principles laid out in the OECD Guidelines for the Security of Information Systems and Networks.

Annex C - Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard - the standard shares the same basic structure of other management systems standards, meaning that an organization which implements any one should be familiar with concepts such as PDCA, records and audits.

In sections 4 to 8 are listed the information security requirements.

In addition to control objectives and controls, ISO 27002 also provides implementation guidance and other information. While ISO IEC 27001 expects you to meet every requirement, it does allow you to exclude selected Annex A control objectives and controls if you can justify doing so. Briefly put, you may exclude or ignore Annex A control objectives and controls whenever they address risks you can live with, and whenever doing so will not impair your ability and obligation to meet all relevant legal and security requirements.

A number of certification bodies are accredited by national standards bodies (such as the British Standards Institution and the National Institute of Science and Technology) to review compliance with ISO/IEC 27001 and issue certificates. Certification is entirely optional but is increasingly being demanded from suppliers and business partners by organizations that are concerned about information security. Certification against ISO/IEC 27001 brings a number of benefits above and beyond simple compliance, in much the same way that an ISO 9000-series certificate says more than “We are a quality organization”. Independent assessment necessarily brings some rigor and formality to the implementation process (implying improvements to information security and all the benefits that brings through risk reduction), and invariably requires management approval.

In fact ISO 27001 is an information security management standard and it defines a set of *requirements* that must be met if you want your ISMS to be formally certified. As a development *methodology*, it explains *how* to create an ISMS, but it tell nothing about what kind of elements make up an ISMS. That's what ISO 27002:2005[19] is all about.

ISO 27002 lists all the bits and pieces that combine to make up an ISMS. It presents a detailed list of generally accepted information security management practices.

What ISO/IEC 27002:2005 is

ISO/IEC 27002:2005 is a code of practice for information security, officially titled *Information Technology - Security Techniques - Code of Practice for Information Security Management*. It establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management[20].

Short presentation of ISO/IEC 27002:2005

ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management:

- security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management;
- compliance.

The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is a common basis and practical guideline for developing organizational security standards and effective security management practices, and help build confidence in inter-organizational activities.

The standard details hundreds of specific security controls which may be applied to secure information and related assets. After the introduction, scope, terminology and structure sections, the ISO/IEC 27002 specifies some 39 control objectives to protect information assets against threats to their confidentiality, integrity and availability. These control objectives in effect comprise a generic

[19] ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of Practice for Information Security Management

[20] http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice/legislationpolicystandards/securitystandards/isoiec27002/section7/page33377.html

functional requirements specification for an organization's information security management controls architecture.

There is one control objective for each second level heading in sections 6 through 15 of the standard (e.g. 8.2), or for the first level headings in the main sections with no second levels.

It comprises 115 pages organized over 15 major sections. These are as follows:

Section 0: *Introduction* It starts from 'What is information security?' and explains how to make use of the standard.

Section 1: *Scope* It gives information security management recommendations for those who are responsible for initiating, implementing or maintaining security.

Section 2: *Terms and definitions*

Section 3: *Structure of this standard* give details about the guts of the standard control objectives, suggested controls and implementation guidance.

Section 4: *Risk assessment and treatment* gives general guidance on selecting and using appropriate methods to analyze information security risk;

Section 5: *Security policy* advise management define a policy to clarify their support for information security, meaning a short, high-level information security policy statement laying down the key information security directives and mandates for the entire organization

Section 6: *Organization of information security* recommends a suitable information security governance structure should be designed and implemented. This section is divided in two parts:

6.1 *Internal organization*

6.2 *External parties*. It states that information security should not be compromised by the introduction of third party products or services and risks should be assessed and mitigated when dealing with customers and in third party agreements

Section 7: *Asset management*. This section suggests that organization should be in a position to understand what information assets it holds, and to manage their security appropriately. It is also divided in two parts:

7.1 *Responsibility for assets* - All [information] assets should be accounted for and have a nominated owner.

7.2 *Information classification*

Section 8: *Human resources security* stands that the organization should manage system access rights *etc.* for 'joiners, movers and leavers', and should undertake suitable security awareness, training and educational activities.

8.1 *Prior to employment* is about responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff Security and included in contracts

8.2 *During employment* - give an idea about management responsibilities regarding information security should be defined and stands that employees and third party IT users should be made aware, educated and trained in security procedures and also that a formal disciplinary process is necessary to handle security breaches.

8.3 *Termination or change of employment* offer the security aspects of how should be managed a person's exit from the organization or change of responsibilities

Section 9: *Physical and environmental security.* Valuable IT equipment should be physically protected against malicious or accidental damage or loss, overheating, loss of mains power *etc.*

9.1 *Secure areas* describes the need for concentric layers of physical controls to protect sensitive IT facilities from unauthorized access.

9.2 *Equipment security.* Critical IT equipment, cabling and so on should be protected against physical damage, fire, flood, theft *etc.*, both on- and off-site. Power supplies and cabling should be secured. IT equipment should be maintained properly and disposed of securely

Section 10: *Communications and operations management.* This section of the standard describes security controls for systems and network management.

10.1 *Operational procedures and responsibilities.* IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Duties should be segregated between different people where relevant (*e.g.* access to development and operational systems should be segregated).

10.2 *Third party service delivery management.* Security requirements should be taken into account in third party service delivery (*e.g.* IT facilities management or outsourcing), from contractual terms to ongoing monitoring and change management.

10.3 *System planning and acceptance* covers IT capacity planning and production acceptance processes.

10.4 *Protection against malicious and mobile code* describes the need for anti-malware controls, including user awareness. Security controls for mobile code 'associated with a number of middleware services' are also outlined.

10.5 *Back-up* covers routine data backups and rehearsed restoration.

10.6 *Network security management* outlines secure network management, network security monitoring and other controls. Also covers security of commercial network services such as private networks and managed firewalls *etc*

10.7 *Media handling.* Procedures should be defined for securely handling, transporting and storing backup media and system documentation and disposal of backup media, documents, voice and other recordings, test data *etc.* should be logged and controlled

10.8 *Exchange of information* stands that information exchanges between organizations should be controlled (though policies and procedures, and legal agreements), and comply with applicable legislation. Security procedures and standards should be in place to protect information and physical media *in transit*, including electronic messaging (email, EDI and IM) and business information systems

10.9 *Electronic commerce services* - The security implications of eCommerce (online transaction systems) should be evaluated and suitable controls implemented. The integrity and availability of information published online (*e.g.* on websites) should also be protected.

10.10 *Monitoring* covers security event/audit/fault logging and system alarm/alert monitoring to detect unauthorized use. Also covers the need to secure logs and synchronize system clocks.

Section 11: *Access control* refers to logical access to IT systems, networks and data must be suitably controlled to prevent unauthorized use.

11.1 *Business requirement for access control.* The organization's requirements to control access to information assets should be clearly documented in an access control policy, including for example job-related access profiles (role based access control).

11.2 *User access management.* The allocation of access rights to users should be formally controlled through user registration and administration procedures, including special restrictions over the allocation of privileges and management of passwords, and regular access rights reviews.

11.3 *User responsibilities* set that users should be made aware of their responsibilities towards maintaining effective access controls *e.g.* choosing strong passwords and keeping them confidential.

11.4 *Network access control.* Access to network services should be controlled, both within the organization and between organizations. Policy should be defined and remote users (and possibly equipment) should be suitably authenticated. Remote diagnostic ports should be securely controlled. Information services, users and systems should be segregated into separate logical network domains. Network connections and routine should be controlled where necessary.

11.5 *Operating system access control.* Operating system access control facilities and utilities (such as user authentication with unique user IDs and managed passwords, recording use of privileges and system security alarms) should be used. Access to powerful system utilities should be controlled and inactivity timeouts should be applied.

11.6 *Application and information access control.* Access to and within application systems should be controlled in accordance with a defined access control policy.

11.7 *Mobile computing and teleworking* affirms that There should be formal policies covering the secure use of portable PCs, PDAs, cellphones *etc.*, and secure teleworking ("working from home", "road warriors" and other forms of mobile or remote working).

Section 12: *Information systems acquisition, development and maintenance.* Information security must be taken into account in the Systems Development Lifecycle (SDLC) processes for specifying, building/acquiring, implementing and maintaining IT systems.

12.1 *Security requirements of information systems.* Automated and manual security control requirements should be analyzed and fully identified during the requirements stage of the systems development or acquisition process, and incorporated into business cases.

12.2 *Correct processing in application systems.* Data entry, processing and output validation controls and message authentication should be provided to mitigate the associated integrity risks.

12.3 *Cryptographic controls.* A cryptography policy should be defined, covering roles and responsibilities, digital signatures, non-repudiation, management of keys and digital certificates *etc.*

12.4 *Security of system files.* Access to system files (both executable programs and source code) and test data should be controlled.

12.5 *Security in development and support processes.* Application system managers should be responsible for controlling access to [or development] project and support environments. Formal change control processes should be applied, including technical reviews. Packaged applications should ideally not be modified. Checks should be made for information leakage for example *via* covert channels and Trojans if these are a concern. A number of supervisory and monitoring controls are outlined for outsourced development.

12.6 *Technical vulnerability management* should be controlled by monitoring for the announcement of relevant security vulnerabilities, and risk-assessing and applying relevant security patches promptly.

Section 13: *Information security incident management.* Information security events, incidents and weaknesses (including near-misses) should be promptly reported and properly managed.

13.1 *Reporting in information security events and weaknesses.* An incident reporting/ alarm procedure is required, plus the associated response and escalation procedures. There should be a central point of contact, and all employees, contractors *etc.* should be informed of their incident reporting responsibilities.

13.2 *Management of information security incidents and improvements.* Responsibilities and procedures are required to manage incidents consistently and effectively, to implement continuous improvement (learning the lessons), and to collect forensic evidence.

Section 14: *Business continuity management* describes the relationship between IT disaster recovery planning, business continuity management and contingency planning, ranging from analysis and documentation through to regular exercising/testing of the plans.

Section 15: *Compliance* consists of:

15.1 *Compliance with legal requirements.* The organization must comply with applicable legislation such as copyright, data protection, protection of financial data and other vital records, cryptography restrictions, rules of evidence *etc.*

15.2 *Compliance with security policies and standards, and technical compliance* stands that managers and system owners must ensure compliance with security policies and standards, for example through regular platform security reviews, penetration tests *etc.* undertaken by competent testers.

15.3 *Information systems audit considerations* stands that audits should be carefully planned to minimize disruption to operational systems. Powerful audit tools/ facilities must also be protected against unauthorized use.

A summary of ISO/IEC 27002 (eye test[21]) is listed in Annex no. 3.

3. Implementation of a ISMS using 27k series

Information security is a management issue, a governance responsibility. The design and implementation of an Information Security Management System is a management role, not a technological one. It requires the full range of managerial skills and attributes, from project management and prioritization through communication, sales skills and motivation to delegation, monitoring and discipline. A good manager who has no technological background or insight can lead a successful ISMS implementation, but without management skills, the most technologically sophisticated information security expert will fail at the task[22].

In order to drive Information Security Program, ones should:

- Understand Information Security Concepts
- Understand requirements of ISO 27001
- Conduct Risk Assessment
- Prepare Risk Treatment plans
- Prepare Statement of Applicability
- Develop ISMS Manual
- Develop strategy and plans for ISMS roll out
- Monitor and review progress of ISMS activities
- Drive the team for achieving ISO 27001 certification.

Essential steps to a successfully ISMS implementation

The nine steps issued by Alan Calder for ISO 27001 ISMS implementation and what should do the auditor is listed below:

1. **Establish ISMS – Determination of Scope and Develop ISMS Policy**
   - ✓ Understand the requirement of the standard
   - ✓ Determine the details to define the scope of ISMS
   - ✓ Identify Management's intent to implement ISMS
   - ✓ Determine various roles and responsibilities
   - ✓ Assignment – (Writing the scope statement, ISMS Policy)
2. **Establish ISMS – Define Risk Assessment Approach**
   - ✓ Risk Assessment Concepts
   - ✓ Understand Risk Analysis techniques (Qualitative v/s Quantitative)
   - ✓ Define Risk Assessment approach
3. **Establish ISMS – Identify, Analyze and Evaluate Risks**

[21] http://www.isaca-edmonton.ca/eventDocuments/12

[22] Calder A. - Nine *essential steps to an effective ISO 27001 ISMS implementation,* http://www.infibeam.com/books/info/alan-calder/nine-steps-to-success-an-iso-27001/1905356129.html

- ✓ Identification of Assets
- ✓ Classification and Valuation of Assets
- ✓ Identify threats and vulnerabilities
- ✓ Determine the likelihood
- ✓ Estimate risk levels and impacts
- ✓ Establish a criteria for risk acceptance
- ✓ Assignment – (Conduct RA)

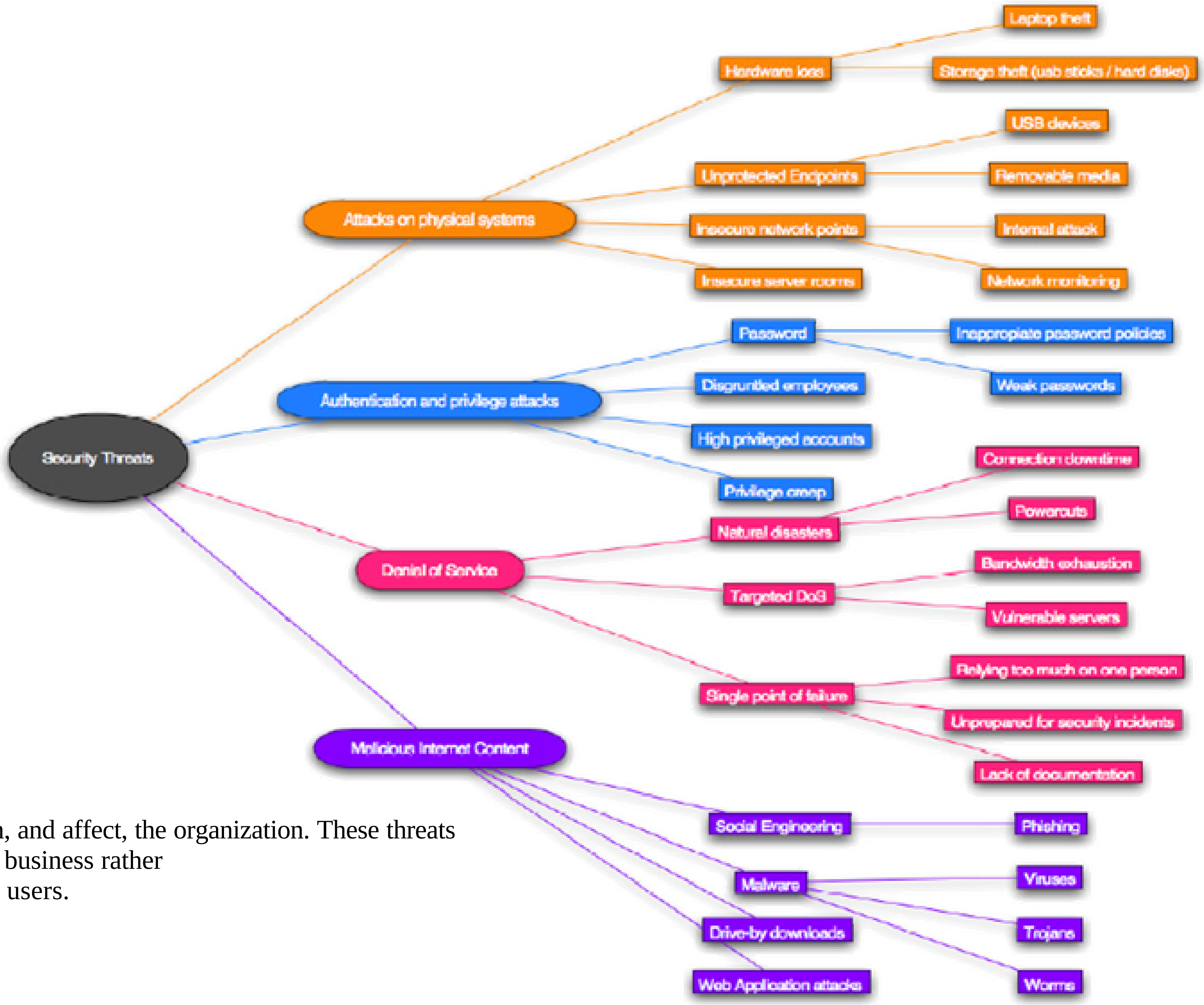
4. **Establish ISMS – Identify and Evaluate options for Risk Treatment**
   - ✓ Develop Risk Treatment Plans
   - ✓ Selecting appropriate Control Objectives and Controls
   - ✓ Prepare Statement of Applicability
   - ✓ Assignment
5. **Establish ISMS - Documentation**
   - ✓ Understand ISMS Documentation Requirements
   - ✓ ISMS Mandatory Documents, Policy Framework, Procedures
   - ✓ Assignment – (Develop a sample Policy)
6. **Implement and Operate ISMS**
   - ✓ ISMS Roll out plans, resource management
   - ✓ Strategy and Plans to spread ISMS awareness across the user base
   - ✓ Security incident response
7. **Monitor and review ISMS**
   - ✓ Internal audit charter
   - ✓ Internal audit policy
   - ✓ Internal Audit program
   - ✓ Management review
8. **Maintain and Improve ISMS**
   - ✓ Corrective Actions
   - ✓ Preventive Actions
   - ✓ Continual Improvement
9. **Certification Audit**
   - ✓ Accreditation Schemes
   - ✓ Certification Body
   - ✓ Certification process for ISO 27001
   - ✓ Integrated Management Framework
   - ✓ Other important ISO standards

References

1. U.S. Code collection > TITLE 44 > CHAPTER 35 > SUBCHAPTER III > § 3542. Definitions;
2. http://www.iso27001security.com/html/other_27k.html
3. http://www.net-security.org/secworld.php?id=8709 on 31-Ian -10
4. ISO/IEC 27001:2005 Information technology -- Security techniques -- Specification for an Information security management systems (ISO/IEC standard)
5. ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems – Requirements (ISO/IEC standard)
6. http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice/legislationpolicystandards/securitystandards/ isoiec27002/section7/page33377.html
7. http://www.isaca-edmonton.ca/eventDocuments/12
8. Calder A. - *Nine essential steps to an effective ISO 27001 ISMS implementation*, http://www.infibeam.com/books/info/alan-calder/nine-steps-to-success-an-iso-27001/1905356129.html

Annexes

Annex no. 1 – Main security threats that affect a small and medium-sized business



Threats that are likely to have an impact on, and affect, the organization. These threats specifically target small and medium-sized business rather than enterprise companies or home users.

Figure 1. Security threat map

Annex no. 2
Top 10 information security threats for 2010 according to Perimeter E-Security:[23]

1. Malware

Last year, Malware was listed as the second highest ranked threat to organizations on Perimeter E-Security's list of top threats. There are many methods to install malware on systems, including the use of client-side software vulnerabilities. Browsers remain a top target for vulnerabilities. In 2009, the FBI reported that for the first time ever, revenue from cybercrime had exceeded drug trafficking, estimated at taking in more than one billion annually in profits.

2. Malicious insiders

Malicious insiders were listed as the top threat for 2009, but have fallen to the 2nd spot for 2010. With the downturn in the economy last year, it was no surprise that many desperate and disgruntled employees attempted to exploit the companies they currently or previously worked for. There is no way to eliminate the threat of malicious insiders completely, but through good security policies and followed procedures, the incidents could be a fraction of what they are today. With the economy still suffering and still high unemployment levels, Malicious Insiders will continue to be a threat.

3. Exploited vulnerabilities

Vulnerability exploit is at the heart of hacking and data breaches. Worms, viruses, malware, and a host of other attack types often rely on vulnerability exploit to infect, spread and perform the actions cyber criminals want. And yet, organizations are still not doing what they need to for patch management. Hackers are more often exploiting client side vulnerabilities and other vulnerabilities associated with 3rd party applications.

4. Careless employees

Careless and untrained insiders will continue to be a very serious threat to organizations in 2010. Insiders can be broken down into three categories: careless & untrained employees, employees that are duped or fall prey to social engineering type attacks, and malicious employees. Protecting a network and critical and sensitive data is done very differently for each type. Policies, procedures, training and a little technology can make a world of difference in reducing an organization's risk to careless insiders.

5. Mobile devices

Mobile devices have become a plague for information security professionals. There are worms and other malware that specifically target these devices such as the iPhone worm that would steal banking data and enlist these devices in a botnet. Theft is still a major cause of data breaches as mobile devices, especially laptops, are the main culprits. Tens of thousands of laptops are stolen each year and often these have sensitive data that require public disclosure as a data breach.

6. Social networking

Social networking sites such as Facebook, MySpace, Twitter and others have changed the way people communicate with each other, but these sites can pose serious threats to organizations. One main problem is that there is a trust component to these sites which makes them fertile ground for identity thieves. There is also a personal safety issue. Social networking sites are a stalker's dream come true. Social networking sites are breeding grounds for SPAM, scams, scareware and a host of other attacks and these threats will continue to rise.

7. Social engineering

Social engineering is always a popular tool used by cyber criminals and phishing is still a popular method for doing just that. In fact, these new venues make social engineering even more effective. This year will have an added measure of complexity when it comes to social engineering attacks. Beginning sometime mid-2010, domain names will be expanded to

[23] http://www.net-security.org/secworld.php?id=8709, on 2-Feb-10

include Japanese, Arabic, Hindi and even Greek characters, and with all of these characters being available for domain names, no longer will looking at a domain help one determine if it's legitimate or not.

8. Zero-day exploits

Zero-day exploits are when an attacker can compromise a system based on a known vulnerability but no patch or fix exists, and they have become a very serious threat to information security. Zero-day vulnerabilities are being discovered in traditionally very secure protocols such as SSL and TLS. The zero-day vulnerability could also be in providers.

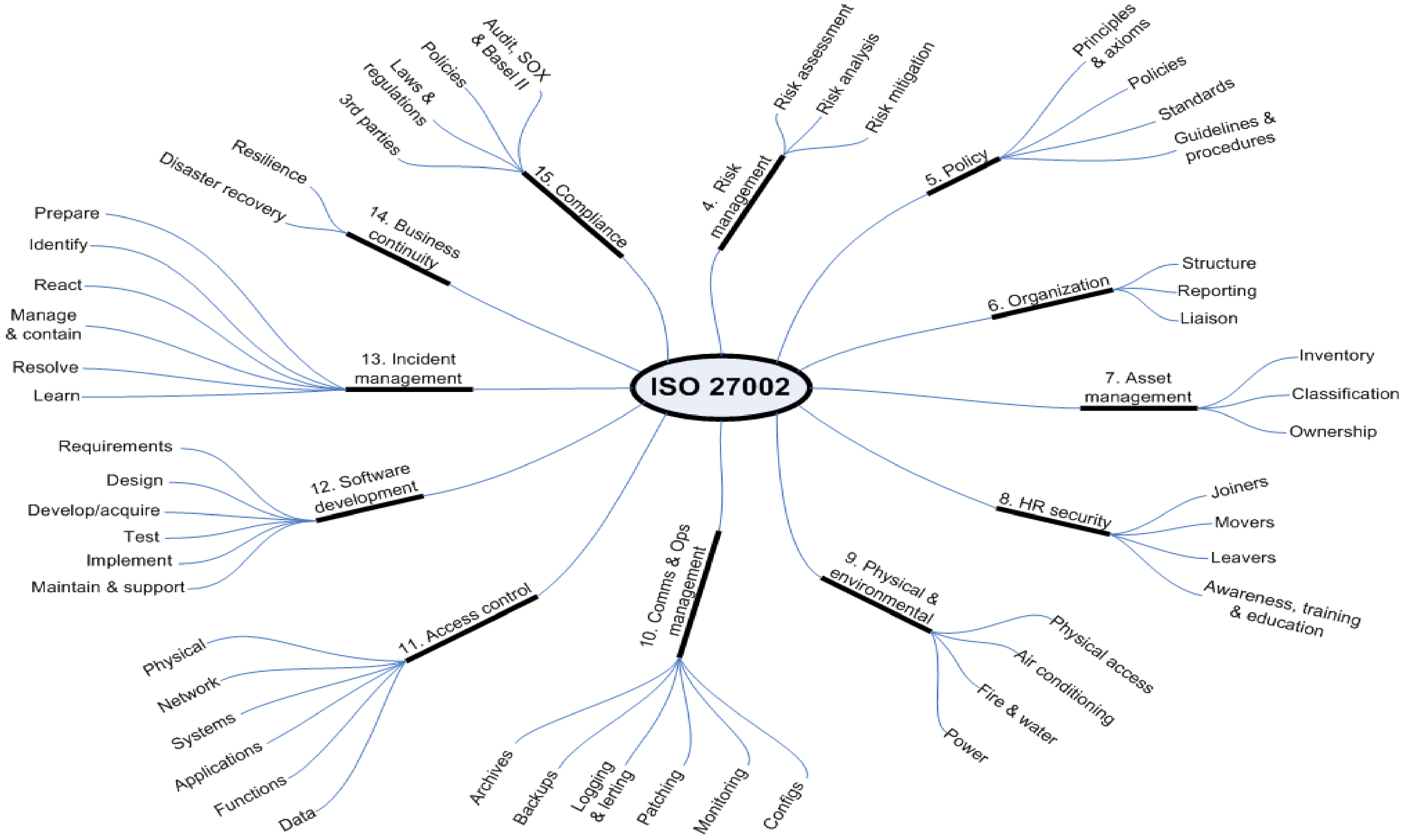
9. Cloud computing security threats

Using cloud based (i.e. Internet based) applications may not be as secure as once thought with many stories in 2009 regarding cloud based security issues. Many are calling for forced encryption to access "in the cloud" services. As cloud computing grows in popularity over the next few years, cloud security will become a very big issue.

10. Cyber espionage

Cyberespionage is a threat that's being heard more and more all the time and there have been a flood of stories in 2009 on this subject. Most of these incidents surround government bodies and agencies and therefore have not been a huge threat to most individual organizations. However, since cyber espionage has major implications for the government, it is a rising threat that must be closely monitored.

Annex no. 3 - ISO 27002 Summary (Eye Test)24



[24] http://www.iso27001security.com/html/27002.html#Section4

DATA SENSITIVITY AND IMPACT OF THREATS

Civilian Ileana Adriana PACURARU

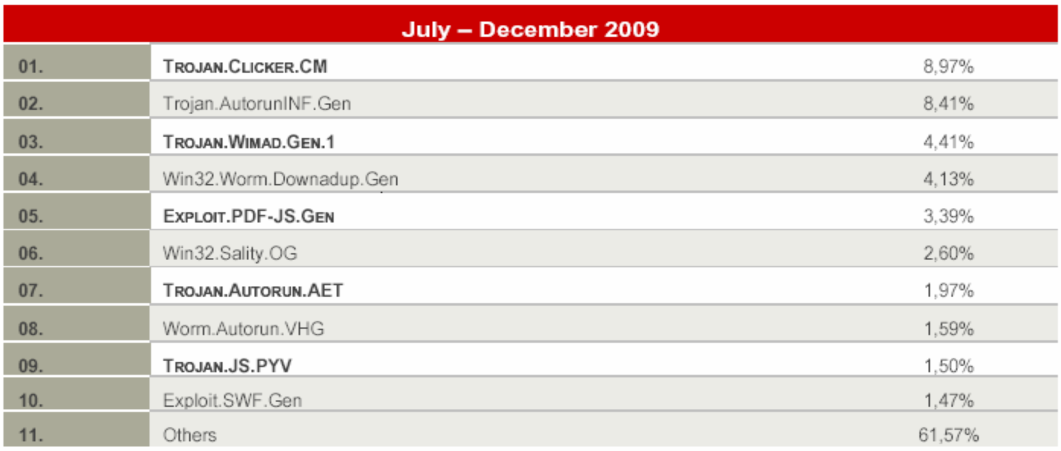
UM 02316 Craiova

Introduction

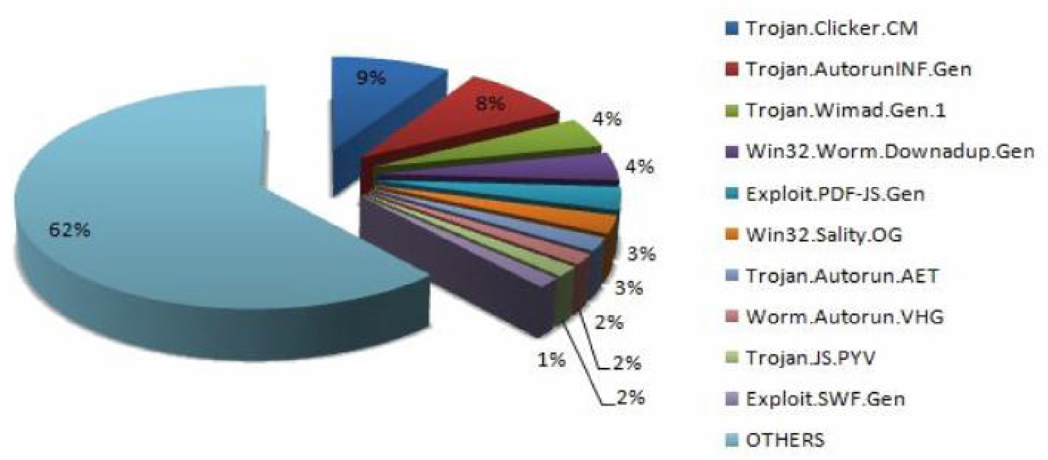
Finding vulnerabilities on your systems and networks is the first step to mitigating potentially extensive damage through network attacks. Today's threats can prevent organizations from accomplishing their mission by causing significant downtime, altering information and inserting fraudulent information in its place, or removing and destroying information altogether.

According the *CSI/FBI 2003 Computer Crime and Security Survey*, the total amount of annual losses caused by computer crime for the 251 organizations that responded was $201,797,340. According to this same survey, the largest loss came from theft of proprietary information.

According the Bitdefender H2 2009 E-Threats Landscape Report – Malware and spam trends, this is top 10 malware threats for H1 2009:



July – December 2009		
01.	Trojan.Clicker.CM	8,97%
02.	Trojan.AutorunINF.Gen	8,41%
03.	Trojan.Wimad.Gen.1	4,41%
04.	Win32.Worm.Downadup.Gen	4,13%
05.	Exploit.PDF-JS.Gen	3,39%
06.	Win32.Sality.OG	2,60%
07.	Trojan.Autorun.AET	1,97%
08.	Worm.Autorun.VHG	1,59%
09.	Trojan.JS.PYV	1,50%
10.	Exploit.SWF.Gen	1,47%
11.	Others	61,57%



1. Data sensitivity

Computer security efforts are based on the need to protect sensitive information in applications and critical data processing capabilities such as facilities, computers, networks and applications. The DHHS Automated Information Systems Security Program (AISSP) Handbook gives us guidelines for determining security level requirements based on:

- *sensitivity of* data —the need to protect data from unauthorized disclosure, fraud, waste, or abuse
- *operational criticality of* data *processing capabilities*—the ramifications if data processing capabilities were interrupted for a period of time or subject to fraud or abuse

Sensitive information can be:

- drug formulas
- grant applications and pre-contract award information
- ongoing confidential research
- performance review information for NIH personnel
- patient records
- personnel records
- identification of individuals who are barred from receiving federal contracts
- arrest/crime records at NIH
- information regarding funding and budgets

1.1. Levels of data sensitivity

Sensitivity levels are determined by the type of information in an automated system. Level 1 applies to information with the least amount of sensitivity and Level 4 applies to information with the greatest amount of sensitivity.

- **Level 1—Low Sensitivity** - Information at this level requires a minimal amount of protection. This level includes information that is considered to be in the public domain, such as employee locator files. At this level, any disclosures could be reasonably expected not to have an adverse effect.
- **Level 2—Moderately Sensitive** - includes data that are important to NIH, and therefore must be protected against acts that are considered to be malicious and destructive. This level includes information that pertains to workload, staffing, correspondence, memoranda, and other document files whose release or distribution outside the federal government and/or within NIH needs to be controlled. Access to Level 2 data needs to be restricted only to a limited degree. The data must be protected from unauthorized alteration or modification due to its value to the organization; however, it may be disclosed in some format eventually. Moderately sensitive data can include information that must be protected to meet Privacy Act requirements.
- **Level 3—High Sensitivity** - This level covers the most sensitive information at NIH and requires the greatest security safeguards at the user level. This data could include computerized correspondence and document files that are regarded as highly sensitive and/or critical to an organization, and therefore must be protected from unauthorized alteration, modification, and/or premature disclosure; proprietary information that has inherent informational value, such as drug formulas, trade secrets, and early research findings; financial data that is used to authorize or make payments to individuals or organizations; clinical trial data; grant application review data; automated systems or records subject to the Privacy Act for which unauthorized disclosure would constitute a clearly unwarranted invasion of personal privacy. Highly sensitive data must be protected from unauthorized disclosure.
- **Level 4—High Sensitivity and National Security** - This level of data does not apply to NIH. The important thing to remember about sensitivity levels is that you must take active steps to protect all sensitive data /information.

1.2. Data sensitivity classification

Objective: to classify data as to "sensitivity", in order to assure appropriate security measures throughout the lifecycle of organizational information and information processing facilities.

Applicability: data sensitivity classification should occur for all significant information collections of the organization, and for the information processing facilities used to access, store or transmit that information.

Sensitivity criteria: Sensitivity classification should be based on confidentiality, integrity and availability dimensions of the data relevant to all stakeholders.

data sensitivity classification matrix			
	Low sensitivity rating	**Moderate sensitivity rating**	**High sensitivity rating**
Externally-imposed requirements	None.	Contractual obligation to data subjects or to another organization for moderate data confidentiality, integrity or availability protections.	Statutory, regulatory or private certificatory requirement for high level of confidentiality, integrity or availability protections (e.g., AHCA, FDA, FERPA, GLBA, HIPAA, JCAHO, NIH, PCI); or contractual obligation to data subjects or another organization for high-level of data protections. Some types of data within this category may require added protection levels reflecting "special status" (e.g. certain kinds of health data covered by HIPAA and state laws)
Internally-imposed requirements	None.	Organizational (internal policy) requirement for some data confidentiality, integrity or availability protections. May be based on risks to: • continuity of operations • financial viability • reputation	Organizational (internal policy) requirement for high data confidentiality, integrity or availability protections. May be based on risks to: • continuity of operations • financial viability • reputation
Risks to operational continuity	Low or none.	Moderate.	High.
Risks to financial viability	Low or none.	Moderate.	High.

Risks to reputation and "good will"	Low or none.	Moderate.	High.
Civil (tort) and criminal risks	Low or none.	Moderate.	High.
Threat environment risk (capabilities and, if human, intentions of likely threats)	Low or none.	Moderate.	High.
Intangible risks that fall outside of other categories	Low or none.	Moderate.	High.
Data examples	Most "public" data of an organization: • most public web site content • information in the public domain • business contact (directory) information • blog and wiki postings • some organizational email (e.g., broadcast notices)	"Internal" data of an organization that is non-public: • some public web site content (particularly if high availability is required) • most email content • limited-distribution contact (directory) information • less-sensitive operational and financial data of the organization Intranet	Almost everything that is protected by statute or regulation: • identifiable clinical (health) data • identifiable research data • student transcripts • identifiable personal financial data (including credit card numbers, bank accounts) • more-sensitive operational and financial data of the organization • restricted-use identifiers (e.g., social security numbers)
Access security	No requirement.	Authentication and access controls required, but set of permitted users may be large.	Authentication required, possibly with multi-factor process. Set of permitted users is usually small. Need-to-know (a.k.a., minimum necessary) access enforced by strong access controls.
Storage security	No requirement. Backups or	Backups or redundant storage required.	Backups or redundant storage required. Encrypted storage

	redundant storage recommended.		(and transfer to storage) recommended. Encrypted storage particularly appropriate for mobile devices (or non-mobile devices in less secure settings) for "special status" data.
Transmission security	No requirement.	Transmission protections recommended, including use of encryption (e.g., SSL/HTTPS).	Transmission protections required, including use of encryption for message confidentiality, integrity and non-repudiation.

1.3. Information classification

Information of different types need to be secured in different ways. Therefore a classification system is needed, whereby information is classified, a policy is laid down on how to handle information according to it's class and security mechanisms are enforced on systems handling information accordingly.

A) Sensitivity classification

A classification system is proposed which classes information / processes into four levels. The lowest ❶ is the least sensitive and the highest ❹ is for the most important information / processes.

A)1. Concepts

- All data has an owner.
- The data or process owner must classify the information into one of the security levels- depending on legal obligations, costs, corporate into policy and business needs.
- If the owner is not sure at what level data should be classified, use level ❸.
- The owner must declare who is allowed access to the data.
- The owner is responsible for this data and must secure it or have it secured (e.g. via a security administrator) according to it's classification.
- All documents should be classified and the classification level should be written on at least the title page.

A)2. Class ❶: Public / non classified information - Data on these systems could be made public without any implications for the company (i.e. the data is not confidential). Data integrity is not vital. Loss of service due to malicious attacks is an acceptable danger.

Examples: Test services without confidential data, certain public information services, product brochures widely distributed, data available in the public domain anyway.

A)3. Class ❷: Internal information - External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g. the company may be publicly embarrassed). Internal access is selective. data integrity is important but not vital.

Examples of this type of data are found in development groups (where no live data is present), certain production public services, certain Customer Data, "normal" working documents and project/meeting protocols, Telephone books.

A)4. Class ❸: Confidential information - Data in this class is confidential within the company and protected from external access. If such data were to be accessed by unauthorised persons, it could influence the company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence. Data integrity is vital.

Examples: Datacenters normally maintain this level of security. Salaries, Personnel data, Accounting data, passwords, information on corporate security weaknesses, very confidential customer data and confidential contracts.

A)5. Class ➍: Secret information - Unauthorised external or internal access to this data would be critical to the company. data integrity is vital. The number of people with access to this data should be very small. Very strict rules must be adhered to in the usage of this data.

Examples: Military data, secret contracts.

2. Threats

2.1. Threats to Electronic Data

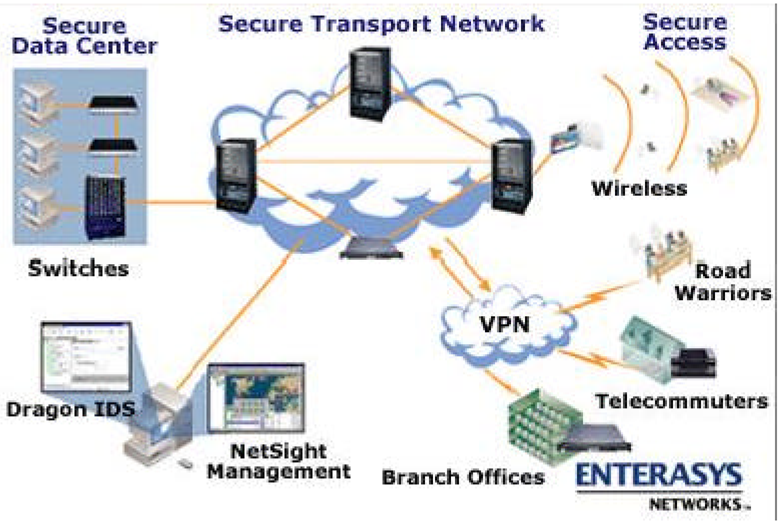
Intrusion & Attack Modality	**Dimension of Involvement**	**Attack Type (examples)**
Interference	Active	? **Spam** with junk mail (such as chain letters) to inform or annoy. ? **Denial of Service**: Overwhelm (ala IP Syn flooding, mail bombing, or Smurf with ICMP Echo Requests); Take advantage of software bugs (ala Buffer overflow, Ping of death, LAND) ? **Bacteria**: corrupt live data or destroy boot sector; Make back up data unrecoverable
	Passive	? **Worms** are self-propagating malicious code that executes unauthorized computer instructions. They can infect any component (boot record, registry, .exe & .com program files, macro scripts, etc.) They do not destroy data. ? **Viruses** are worms that harm data. ? **Rabbits** - runaway applications that consume all resources (memory on machines or bandwidth on networks).
Interception of message stream	Active	? **Connection/Session hijacking**: Active Telnet session seized ? **Spoofing**: Altering DNS namespace to setup Web Page Redirection
	Passive	? **Eavesdropping** with a wiretap: capture data in transit. Using a packet Sniffer (Protocol Analyzer) for network traffic analysis (see patterns in text flow, packet size, etc.). ? **Compromised Key** Disseminate sensitive information for illicit gain or to embarrass organizations and individuals. [Sircam]
Impersonation	Active	? **IP Address Spoofing** -- when a rogue site intercepts authenticated communications between legitimate users and presents altered content as legitimate. ? **Man-in-the-middle spoofing**: captured packets are tampered and reinserted into an active

		session pipe ? **Crack** (decrypt passwords and cyphertext by brute force or other means) ? **Replay** reusing a captured authenticator ? **DDoS** (Distributed Denial of Service) attack ? DNS Name Server cache loading
	Passive	? **Trap doors** (such as Sub7, NetBus patch, or Back Orafice) to bypass noraml security and allow unauthorized/undetected entry. ? **Trojan horses** inserted to reconfigure network settings or grant root access and permissions to an unauthorized person.

2.2. The Five Phases of Attack/Intrusion/Incursion

Corporate Security Policy typically define these activities as unacceptable:

1. Outside Reconnaissance Probing
2. Penetration - Inside Reconnaissance
3. Escalate Priviledge - Gain Foothold and Pillage
4. Expand Influence - Exploit and Cleanup to cover tracks
5. Profit



1. Outside Reconnaissance

Like a burglar casing the joint, obtain publicly available information as a normal anonymous user or potential customer. Network Reconnaissance of the footprint of the target system:

- traceroute to present potential access paths and vulnerable entry points through the target network.
- Look for Web server version information using. Grinder to scan a series of IP addresses.

Network enumeration - listing domain names and networks related to an organization from: - search of news articles, press releases, and newsgroup postings.

- keyword search in Whois database which may contain administrator contact and IP addresses
- nslookup to walk though DNS tables.
- NMAP(Network Mapper) open source utility developed by Fyodor reports the operating systems of OSs and firewalls. Some of its techniques:
  - Reverse ARP
  - Bogus flag probe

  - TCP ISN sampling
  - FIN probes
- WhatsUp from Ipswitch.com performs a tracert.

Telecom devices (such as PhoneSweep) programmatically dial large banks of phone numbers, log valid data connections, attempt to identify the system on the other end of the phone, and optionally attempt logon by guessing common usernames and passphrases. DNS Interrogation - If zone transfers are enabled over a network, a hacker can intercept it. OS and Service Detection - Use NMAP from Phrack to determine what OS and services are active on a subnet. IP stack signatures reveal the vendors, each with their own vulnerabilities (exploitable bugs). The LSA secrets hack exploits reg key HKLM\Security\policy\secrets which stores cached credentials, web/ftp passwords, and the machine account password as well as service accts.

2. **Inside Reconnaissance**

eTrust from Computer Associates can capture the packets of all protocols on a network and save (non SSL) pages viewed on desktops.

Use techniques which do not harm target machines.

Identify which machine names are alive with a ping sweep.

Identify which services are available on each machine using a UDP/TCP port scan/strobe**.**

Look for CGI scripts by walking through and capturing web pages.

DNS zone transfer

Identify which machines have NetBIOS vulnerabilities Traditionally, attacks against Windows 2000 have been against the SMB service. More recently, is through **IIS** web service, installed by default.

3. **Exploit**

Take advantage of vulnerabilities to break into target systems:

- Crack logon passwords using dictionary or brute-force attempts using
  - L0pht - pronounced “Loft" - for NT4 and LC3 for Win2000 from AtStake.com is based on pwdump
  - Locksmith works with Remote Recover or NTRecover from Winternals
  - Elcomsoft's tools to crack passwords in PDF files, etc.
  - Distributed.net
  - access data crak and Password crackers, Inc boast a library of software, techniques, and resources for a price
  - benchmarks of password cracking software.
  - lostpassword.com
- Obtain elevated privileges (root) by taking advantage of buffer-overrun holes or determine NIDS thresholds by sending large amounts of data.
- Modifying cookies to access other accounts.
- Sending shell commands in input fields.
- Modifying SQL query strings in GET commands.
- Initiate emails infected with worms and Trojan horse viruses

4. **Foot hold (Got Root!)**

Once elevated privilege is obtained:

- Hide evidence of intrusion in log files. Security Log Event ID
  - 612 - The audit policy has changed, perhaps maliciously.
  - 640 - A change has been made to the SAM database. (Was it you?)
  - 531 - An attempt was made to log on using a disabled account. (Why would anyone want to do this?)
  - 539 - A logon attempt was made and rejected because the account was locked out. (Why would anyone want to do this?)

- 529 - An attempt was made to log on using an unknown user account or using a valid user account but with an invalid password. (An unexpected increase in the number of these audits might indicate an attempt to guess passwords.)
- 517 - The audit log has been cleared. (Is an attacker attempting to cover her tracks?)
- 624 - A user account has been created. (Was it created by a trusted person?)
- 628 - A user account's password has been set. (Was this done by a trusted person?)

- Reduce detection **during future incursions:**
  - ▪ Replace services with backdoor trojan horses such as “Back Orafice” Example: the Melissa virus installed a program named “Explore".
  - ▪ Create accounts with full Privileges
  - ▪ Install a rootkit
- Provide services to other hackers, such as storing files on the compromised machine for others to obtain files. This is done by announcing availability on IRC (Internet Relay Chat).
- Use infected system to launch Distributed Denial of Service attacks on another target. This is done by installing zombies (evilbots) such as sub7 which enable infected machines to inflect other machines - achieving a “snowball effect" chain reaction.
- To reduce the chance of being filtered and to make it more likely that intermediate targets get themselves infected, a virus may be coded to
  - o Masquerade as the actual user and send emails from the address books of infected hosts. This is because most email filters do not filter out email specifically address to the recipient.
  - o Use enticing subjects (such as "naked wife", celebrity names, or - in the case of Sircam - words extracted from the intermediate host's personal files.
  - o Generate a list of 100 random IP addresses to scan for new servers to infect.

5. Profit from Attack

- Steal information (such as credit card numbers and passwords). On Windows client machines, sensitive files are typically stored in the default “My Documents” folder.
- Run up charges by using the modem to dial and reach a 900 number at a remote country such as Trinidad
- On client browsers, point the default website to a malicious site.
- Deface web pages served on web servers (such as IIS). Examples:
  - The first “Code Red" virus added “hacked by Chinese!" on websites.
  - The SunOS/Poisonbox.worm uses a Unicode buffer overflow vulnerability in the ssinc.dll on Microsoft IIS5 SP6a servers to replace index.htm/asp pages with one which displays “** CHINA Government" AND drop a renamed copy of cmd.exe (root.exe) to provide a trap door.

2.3. Prioritizing Resolutions and Determining Impact to Infrastructure

Once vulnerabilities have been determined, your organization will not be able to resolve all of them at once. Therefore, you'll want to prioritize the vulnerabilities according to which ones are most likely to be exploited, and which ones would have the highest damage impact if they were in fact exploited.

In prioritizing which vulnerabilities to resolve first, one thing you'll want to take into consideration is the sensitivity of the data on the systems that are impacted. For example, if you have an isolated lab environment that is used to test and stage new products that you are thinking of deploying on your network, the data on these systems is likely not as sensitive as the data on your primary DNS server. You need to have an understanding of what data on your network is highly sensitive. Even though you may not be able to rank the sensitivity of all the data from, say, 1 to 100, you should be able to at least assign sensitivity labels to data on your systems on a relative scale such as the following:

- Extremely sensitive
- Highly sensitive

- Moderately sensitive
- Minimally sensitive
- Non-sensitive

Any data that puts lives at stake should be categorized as extremely sensitive. Data that can be easily re-created, and is public read-only information, is non-sensitive. Some organizations make the mistake of fixing the most easy to exploit vulnerabilities first, instead of first fixing the vulnerabilities that can result in the highest impact of damage. Organizations need to inventory the data on all mission critical servers and assign sensitivity levels to it.

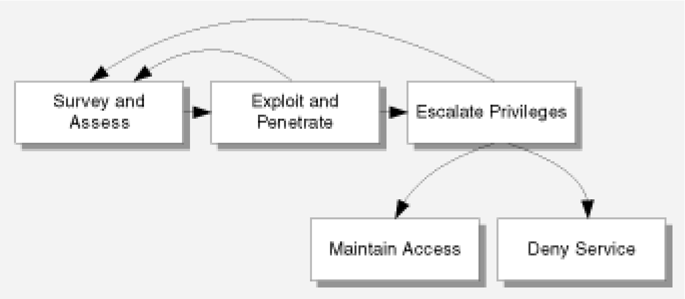
Calculating Data Sensitivity and Impact of Threats		
Data Sensitivity	Moderately High Sensitivity and Impact	**High Sensitivity and Impact**
High		
Low	Less Sensitive Low Impact	Moderately-Low Sensitivity and Impact
	Low	High
	Likelihood or Probability of Vulnerability Being Exploited	

3. Threats and Countermeasures

3.1. Anatomy of an Attack

By understanding the basic approach used by attackers to target your Web application, you will be better equipped to take defensive measures because you will know what you are up against. The basic steps in attacker methodology are summarized below and illustrated in this figure: **Survey and assess**

Exploit and penetrate
Escalate privileges
Maintain access
Deny service



Basic steps for attacking methodology

Survey and Assess

Surveying and assessing the potential target are done in tandem. The first step an attacker usually takes is to survey the potential target to identify and assess its characteristics. These characteristics may include its supported services and protocols together with potential vulnerabilities and entry points. The attacker uses the information gathered in the survey and assess phase to plan an initial attack. For example, an attacker can detect a cross-site scripting (XSS) vulnerability by testing to see if any controls in a Web page echo back output.

Exploit and Penetrate

Having surveyed a potential target, the next step is to exploit and penetrate. If the network and host are fully secured, your application (the front gate) becomes the next channel for attack. For an attacker, the easiest way into an application is through the same entrance that legitimate users use — for example, through the application's logon page or a page that does not require authentication.

Escalate Privileges

After attackers manage to compromise an application or network, perhaps by injecting code into an application or creating an authenticated session with the Microsoft® Windows® 2000 operating system, they immediately attempt to escalate privileges. Specifically, they look for administration privileges provided by accounts that are members of the Administrators group. They also seek out the high level of privileges offered by the local system account. Using least privileged service accounts throughout your application is a primary defense against privilege escalation attacks. Also, many network level privilege escalation attacks require an interactive logon session.

Maintain Access

Having gained access to a system, an attacker takes steps to make future access easier and to cover his or her tracks. Common approaches for making future access easier include planting back-door programs or using an existing account that lacks strong protection. Covering tracks typically involves clearing logs and hiding tools. As such, audit logs are a primary target for the attacker. Log files should be secured, and they should be analyzed on a regular basis. Log file analysis can often uncover the early signs of an attempted break-in before damage is done.

Deny Service

Attackers who cannot gain access often mount a denial of service attack to prevent others from using the application. For other attackers, the denial of service option is their goal from the outset. An example is the SYN flood attack, where the attacker uses a program to send a flood of TCP SYN requests to fill the pending connection queue on the server. This prevents other users from establishing network connections.

3.2. Understanding Threat Categories

STRIDE - Threats faced by the application can be categorized based on the goals and purposes of the attacks. A working knowledge of these categories of threats can help you organize a security strategy so that you have planned responses to threats. STRIDE is the acronym used at Microsoft to categorize different threat types. STRIDE stands for:

- **Spoofing**. is attempting to gain access to a system by using a false identity. This can be accomplished using stolen user credentials or a false IP address. After the attacker successfully gains access as a legitimate user or host, elevation of privileges or abuse using authorization can begin.
- **Tampering**. is the unauthorized modification of data, for example as it flows over a network between two computers.
- **Repudiation**. is the ability of users (legitimate or otherwise) to deny that they performed specific actions or transactions. Without adequate auditing, repudiation attacks are difficult to prove.
- **Information disclosure**. is the unwanted exposure of private data. For example, a user views the contents of a table or file he or she is not authorized to open, or monitors data passed in plaintext over a network. Some examples of information disclosure vulnerabilities include the use of hidden form fields, comments embedded in Web pages that contain database connection strings and connection details, and weak exception handling that can lead to internal system level details being revealed to the client. Any of this information can be very useful to the attacker.
- **Denial of service**. is the process of making a system or application unavailable. For example, a denial of service attack might be accomplished by bombarding a server with requests to consume all available system resources or by passing it malformed input data that can crash an application process.
- **Elevation of privilege**. occurs when a user with limited privileges assumes the identity of a privileged user to gain privileged access to an application. For example, an attacker

with limited privileges might elevate his or her privilege level to compromise and take control of a highly privileged and trusted process or account.

3.3. STRIDE Threats and Countermeasures

Each threat category described by STRIDE has a corresponding set of countermeasure techniques that should be used to reduce risk. These are summarized in STRIDE Table. The appropriate countermeasure depends upon the specific attack.

STRIDE Threats and Countermeasures

Threat	Countermeasures
Spoofing user identity	Use strong authentication. Do not store secrets (for example, passwords) in plaintext. Do not pass credentials in plaintext over the wire. Protect authentication cookies with Secure Sockets Layer (SSL).
Tampering with data	Use data hashing and signing. Use digital signatures. Use strong authorization. Use tamper-resistant protocols across communication links. Secure communication links with protocols that provide message integrity.
Repudiation	Create secure audit trails. Use digital signatures.
Information disclosure	Use strong authorization. Use strong encryption. Secure communication links with protocols that provide message confidentiality. Do not store secrets (for example, passwords) in plaintext.
Denial of service	Use resource and bandwidth throttling techniques. Validate and filter input.
Elevation of privilege	Follow the principle of least privilege and use least privileged service accounts to run processes and access resources.

3.4. Network Threats and Countermeasures

The primary components that make up your network infrastructure are routers, firewalls, and switches. They act as the gatekeepers guarding your servers and applications from attacks and intrusions. An attacker may exploit poorly configured network devices. Common vulnerabilities include weak default installation settings, wide open access controls, and devices lacking the latest security patches. Top network level threats include:

- **Information gathering**
- **Sniffing**
- **Spoofing**
- **Session hijacking**
- **Denial of service**

Information Gathering - Network devices can be discovered and profiled in much the same way as other types of systems. Attackers usually start with port scanning. After they identify open ports, they use banner grabbing and enumeration to detect device types and to determine operating system and application versions. Armed with this information, an attacker can attack known vulnerabilities that may not be updated with security patches.

Countermeasures:

- Configure routers to restrict their responses to footprinting requests.
- Configure operating systems that host network software (for example, software firewalls) to prevent footprinting by disabling unused protocols and unnecessary ports.

Sniffing - or *eavesdropping* is the act of monitoring traffic on the network for data such as plaintext passwords or configuration information. With a simple packet sniffer, an attacker can easily read all plaintext traffic. Also, attackers can crack packets encrypted by lightweight hashing algorithms and can decipher the payload that you considered to be safe. The sniffing of packets requires a packet sniffer in the path of the server/client communication.

Countermeasures:

- Use strong physical security and proper segmenting of the network. This is the first step in preventing traffic from being collected locally.
- Encrypt communication fully, including authentication credentials. This prevents sniffed packets from being usable to an attacker. SSL and IPSec (Internet Protocol Security) are examples of encryption solutions.

Spoofing - is a means to hide one's true identity on the network. To create a spoofed identity, an attacker uses a fake source address that does not represent the actual address of the packet. Spoofing may be used to hide the original source of an attack or to work around network access control lists (ACLs) that are in place to limit host access based on source address rules. Although carefully crafted spoofed packets may never be tracked to the original sender, a combination of filtering rules prevents spoofed packets from originating from your network, allowing you to block obviously spoofed packets.

Countermeasures:

- Filter incoming packets that appear to come from an internal IP address at your perimeter.
- Filter outgoing packets that appear to originate from an invalid local IP address.

Session Hijacking - Also known as man in the middle attacks, session hijacking deceives a server or a client into accepting the upstream host as the actual legitimate host. Instead the upstream host is an attacker's host that is manipulating the network so the attacker's host appears to be the desired destination.

Countermeasures:

- Use encrypted session negotiation.
- Use encrypted communication channels.
- Stay informed of platform patches to fix TCP/IP vulnerabilities, such as predictable packet sequences.

Denial of Service - denies legitimate users access to a server or services. The SYN flood attack is a common example of a network level denial of service attack. It is easy to launch and difficult to track. The aim of the attack is to send more requests to a server than it can handle. The attack exploits a potential vulnerability in the TCP/IP connection establishment mechanism and floods the server's pending connection queue.

Countermeasures:

- Apply the latest service packs.
- Harden the TCP/IP stack by applying the appropriate registry settings to increase the size of the TCP connection queue, decrease the connection establishment period, and employ dynamic backlog mechanisms to ensure that the connection queue is never exhausted.
- Use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks.

3.5. Host Threats and Countermeasures

Host threats are directed at the system software upon which your applications are built. This includes Windows 2000, Microsoft Windows Server 2003, Internet Information Services

(IIS), the .NET Framework, and SQL Server depending upon the specific server role. Top host level threats include:

- **Viruses, Trojan horses, and worms**
- **Footprinting**
- **Profiling**
- **Password cracking**
- **Denial of service**
- **Arbitrary code execution**
- **Unauthorized access**

Viruses, Trojan Horses, and Worms - A virus is a program that is designed to perform malicious acts and cause disruption to your operating system or applications. A Trojan horse resembles a virus except that the malicious code is contained inside what appears to be a harmless data file or executable program. A worm is similar to a Trojan horse except that it self-replicates from one server to another. Worms are difficult to detect because they do not regularly create files that can be seen. They are often noticed only when they begin to consume system resources because the system slows down or the execution of other programs halt. The success of these attacks on any system is possible through many vulnerabilities such as weak defaults, software bugs, user error, and inherent vulnerabilities in Internet protocols.

Countermeasures:

- Stay current with the latest operating system service packs and software patches.
- Block all unnecessary ports at the firewall and host.
- Disable unused functionality including protocols and services.
- Harden weak, default configuration settings.

Footprinting - Examples of footprinting are port scans, ping sweeps, and NetBIOS enumeration that can be used by attackers to glean valuable system-level information to help prepare for more significant attacks. The type of information potentially revealed by footprinting includes account details, operating system and other software versions, server names, and database schema details.

Countermeasures:

- Disable unnecessary protocols.
- Lock down ports with the appropriate firewall configuration.
- Use TCP/IP and IPSec filters for defense in depth.
- Configure IIS to prevent information disclosure through banner grabbing.
- Use an IDS that can be configured to pick up footprinting patterns and reject suspicious traffic.

Password Cracking - If the attacker cannot establish an anonymous connection with the server, he or she will try to establish an authenticated connection. For this, the attacker must know a valid username and password combination. If you use default account names, you are giving the attacker a head start. Then the attacker only has to crack the account's password. The use of blank or weak passwords makes the attacker's job even easier.

Countermeasures:

- Use strong passwords for all account types.
- Apply lockout policies to end-user accounts to limit the number of retry attempts that can be used to guess the password.
- Do not use default account names, and rename standard accounts such as the administrator's account and the anonymous Internet user account used by many Web applications.
- Audit failed logins for patterns of password hacking attempts.

Denial of Service - can be attained by many methods aimed at several targets within your infrastructure. At the host, an attacker can disrupt service by brute force against your application, or an attacker may know of a vulnerability that exists in the service your application is hosted in or in the operating system that runs your server.

Countermeasures:

- Configure your applications, services, and operating system with denial of service in mind.
- Stay current with patches and security updates.
- Harden the TCP/IP stack against denial of service.
- Make sure your account lockout policies cannot be exploited to lock out well known service accounts.
- Make sure your application is capable of handling high volumes of traffic and that thresholds are in place to handle abnormally high loads.
- Review your application's failover functionality.
- Use an IDS that can detect potential denial of service attacks.

Arbitrary Code Execution - If an attacker can execute malicious code on your server, the attacker can either compromise server resources or mount further attacks against downstream systems. The risks posed by arbitrary code execution increase if the server process under which the attacker's code runs is over-privileged. Common vulnerabilities include weak IIS configuration and unpatched servers that allow path traversal and buffer overflow attacks, both of which can lead to arbitrary code execution.

Countermeasures:

- Configure IIS to reject URLs with "../" to prevent path traversal.
- Lock down system commands and utilities with restricted ACLs.
- Stay current with patches and updates to ensure that newly discovered buffer overflows are speedily patched.

Unauthorized Access - Inadequate access controls could allow an unauthorized user to access restricted information or perform restricted operations. Common vulnerabilities include weak IIS Web access controls, including Web permissions and weak NTFS permissions.

Countermeasures:

- Configure secure Web permissions.
- Lock down files and folders with restricted NTFS permissions.
- Use .NET Framework access control mechanisms within your ASP.NET applications, including URL authorization and principal permission demands.

3.6. Application Threats and Countermeasures

A good way to analyze application-level threats is to organize them by application vulnerability category.

Threats by Application Vulnerability Category

Category	Threats
Input validation	Buffer overflow; cross-site scripting; SQL injection; canonicalization
Authentication	Network eavesdropping; brute force attacks; dictionary attacks; cookie replay; credential theft
Authorization	Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
Configuration management	Unauthorized access to administration interfaces; unauthorized access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
Sensitive data	Access sensitive data in storage; network eavesdropping; data tampering
Session management	Session hijacking; session replay; man in the middle

Cryptography	Poor key generation or key management; weak or custom encryption
Parameter manipulation	Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
Exception management	Information disclosure; denial of service
Auditing and logging	User denies performing an operation; attacker exploits an application without trace; attacker covers his or her tracks

Input Validation

Input validation is a security issue if an attacker discovers that your application makes unfounded assumptions about the type, length, format, or range of input data. The attacker can then supply carefully crafted input that compromises your application. When network and host level entry points are fully secured; the public interfaces exposed by your application become the only source of attack. The input to your application is a means to both test your system and a way to execute code on an attacker's behalf. Does your application blindly trust input? If it does, your application may be susceptible to the following:

- Buffer overflows
- Cross-site scripting
- SQL injection
- Canonicalization

Buffer Overflows

Buffer overflow vulnerabilities can lead to denial of service attacks or code injection. A denial of service attack causes a process crash; code injection alters the program execution address to run an attacker's injected code.

Countermeasures:

- Perform thorough input validation. This is the first line of defense against buffer overflows. Although a bug may exist in your application that permits expected input to reach beyond the bounds of a container, unexpected input will be the primary cause of this vulnerability. Constrain input by validating it for type, length, format and range.
- Limit your application's use of unmanaged code, and thoroughly inspect the unmanaged APIs to ensure that input is properly validated.
- Inspect the managed code that calls the unmanaged API to ensure that only appropriate values can be passed as parameters to the unmanaged API.
- Use the /GS flag to compile code developed with the Microsoft Visual C++® development system. The /GS flag causes the compiler to inject security checks into the compiled code. This is not a fail-proof solution or a replacement for your specific validation code; it does, however, protect your code from commonly known buffer overflow attacks.

Cross-Site Scripting - An XSS attack can cause arbitrary code to run in a user's browser while the browser is connected to a trusted Web site. The attack targets your application's users and not the application itself, but it uses your application as the vehicle for the attack.

Countermeasures:

- Perform thorough input validation. Your applications must ensure that input from query strings, form fields, and cookies are valid for the application. Consider all user input as possibly malicious, and filter or sanitize for the context of the downstream code. Validate all input for known valid values and then reject all other input. Use regular expressions to validate input data received via HTML form fields, cookies, and query strings.

- Use HTMLEncode and URLEncode functions to encode any output that includes user input. This converts executable script into harmless HTML.

SQL Injection - A SQL injection attack exploits vulnerabilities in input validation to run arbitrary commands in the database. It can occur when your application uses input to construct dynamic SQL statements to access the database. It can also occur if your code uses stored procedures that are passed strings that contain unfiltered user input. Using the SQL injection attack, the attacker can execute arbitrary commands in the database. The issue is magnified if the application uses an over-privileged account to connect to the database. In this instance it is possible to use the database server to run operating system commands and potentially compromise other servers, in addition to being able to retrieve, manipulate, and destroy data.

Countermeasures:

- Perform thorough input validation. Your application should validate its input prior to sending a request to the database.
- Use parameterized stored procedures for database access to ensure that input strings are not treated as executable statements. If you cannot use stored procedures, use SQL parameters when you build SQL commands.
- Use least privileged accounts to connect to the database.

Canonicalization - Different forms of input that resolve to the same standard name (the canonical name), is referred to as *canonicalization*. Code is particularly susceptible to canonicalization issues if it makes security decisions based on the name of a resource that is passed to the program as input. Files, paths, and URLs are resource types that are vulnerable to canonicalization because in each case there are many different ways to represent the same name.

Countermeasures:

- Avoid using file names as input where possible and instead use absolute file paths that cannot be changed by the end user.
- Make sure that file names are well formed (if you must accept file names as input) and validate them within the context of your application. For example, check that they are within your application's directory hierarchy.
- Ensure that the character encoding is set correctly to limit how input can be represented. Check that your application's Web.config has set the requestEncoding and responseEncoding attributes on the <globalization> element.

Authentication

Depending on your requirements, there are several available authentication mechanisms to choose from. If they are not correctly chosen and implemented, the authentication mechanism can expose vulnerabilities that attackers can exploit to gain access to your system. The top threats that exploit authentication vulnerabilities include:

- **Network eavesdropping**
- **Brute force attacks**
- **Dictionary attacks**
- **Cookie replay attacks**
- **Credential theft**

Network Eavesdropping - If authentication credentials are passed in plaintext from client to server, an attacker armed with rudimentary network monitoring software on a host on the same network can capture traffic and obtain user names and passwords.

Countermeasures:

- Use authentication mechanisms that do not transmit the password over the network such as Kerberos protocol or Windows authentication.
- Make sure passwords are encrypted (if you must transmit passwords over the network) or use an encrypted communication channel, for example with SSL.

Brute Force Attacks - rely on computational power to crack hashed passwords or other secrets secured with hashing and encryption. To mitigate the risk, use strong passwords. Additionally, use hashed passwords with salt; this slows down the attacker considerably and allows sufficient time for countermeasures to be activated.

Dictionary Attacks -This attack is used to obtain passwords. Most password systems do not store plaintext passwords or encrypted passwords. They avoid encrypted passwords because a compromised key leads to the compromise of all passwords in the data store. Lost keys mean that all passwords are invalidated. With the dictionary attack, an attacker uses a program to iterate through all of the words in a dictionary (or multiple dictionaries in different languages) and computes the hash for each word. The resultant hash is compared with the value in the data store.

Countermeasures:

- Use strong passwords that are complex, are not regular words, and contain a mixture of upper case, lower case, numeric, and special characters.
- Store non-reversible password hashes in the user store. Also combine a salt value (a cryptographically strong random number) with the password hash.

Cookie Replay Attacks - With this type of attack, the attacker captures the user's authentication cookie using monitoring software and replays it to the application to gain access under a false identity.

Countermeasures:

- Use an encrypted communication channel provided by SSL whenever an authentication cookie is transmitted.
- Use a cookie timeout to a value that forces authentication after a relatively short time interval. Although this doesn't prevent replay attacks, it reduces the time interval in which the attacker can replay a request without being forced to re-authenticate because the session has timed out.

Credential Theft - If your application implements its own user store containing user account names and passwords, compare its security to the credential stores provided by the platform, for example, a Microsoft Active Directory® directory service or Security Accounts Manager (SAM) user store. Browser history and cache also store user login information for future use. If the terminal is accessed by someone other than the user who logged on, and the same page is hit, the saved login will be available.

Countermeasures:

- Use and enforce strong passwords.
- Store password verifiers in the form of one way hashes with added salt.
- Enforce account lockout for end-user accounts after a set number of retry attempts.
- To counter the possibility of the browser cache allowing login access, create functionality that either allows the user to choose to not save credentials, or force this functionality as a default policy.

Authorization

Based on user identity and role membership, authorization to a particular resource or service is either allowed or denied. Top threats that exploit authorization vulnerabilities include:

- **Elevation of privilege**
- **Disclosure of confidential data**
- **Data tampering**
- **Luring attacks**

Elevation of Privilege - When you design an authorization model, you must consider the threat of an attacker trying to elevate privileges to a powerful account such as a member of the local administrators group or the local system account. By doing this, the attacker is able to take complete control over the application and local machine. The main countermeasure that you can use to prevent elevation of privilege is to use least privileged process, service, and user accounts.

Disclosure of Confidential Data - can occur if sensitive data can be viewed by unauthorized users. Confidential data includes application specific data such as credit card numbers, employee details, financial records and so on together with application configuration data such as service account credentials and database connection strings. To prevent the disclosure of confidential data you should secure it in persistent stores such as databases and configuration files, and during transit over the network. Only authenticated and authorized users should be able to access the data that is specific to them. Access to system level configuration data should be restricted to administrators.

Countermeasures:

- Perform role checks before allowing access to the operations that could potentially reveal sensitive data.
- Use strong ACLs to secure Windows resources.
- Use standard encryption to store sensitive data in configuration files and databases.

Data Tampering - refers to the unauthorized modification of data.

Countermeasures:

- Use strong access controls to protect data in persistent stores to ensure that only authorized users can access and modify the data.
- Use role-based security to differentiate between users who can view data and users who can modify data.

Luring Attacks - occurs when an entity with few privileges is able to have an entity with more privileges perform an action on its behalf. To counter the threat, you must restrict access to trusted code with the appropriate authorization. Using .NET Framework code access security helps in this respect by authorizing calling code whenever a secure resource is accessed or a privileged operation is performed.

Configuration Management

Many applications support configuration management interfaces and functionality to allow operators and administrators to change configuration parameters, update Web site content, and to perform routine maintenance. Top configuration management threats include:

- **Unauthorized access to administration interfaces**
- **Unauthorized access to configuration stores**
- **Retrieval of plaintext configuration secrets**
- **Lack of individual accountability**
- **Over-privileged process and service accounts**

Unauthorized Access to Administration Interfaces - Administration interfaces are often provided through additional Web pages or separate Web applications that allow administrators, operators, and content developers to managed site content and configuration. Malicious users able to access a configuration management function can potentially deface the Web site, access downstream systems and databases, or take the application out of action altogether by corrupting configuration data.

Countermeasures:

- Minimize the number of administration interfaces.
- Use strong authentication, for example, by using certificates.
- Use strong authorization with multiple gatekeepers.
- Consider supporting only local administration. If remote administration is absolutely essential, use encrypted channels, because of the sensitive nature of the data passed over administrative interfaces. To further reduce risk, also consider using IPSec policies to limit remote administration to computers on the internal network.

Unauthorized Access to Configuration Stores - Because of the sensitive nature of the data maintained in configuration stores, you should ensure that the stores are adequately secured.

Countermeasures:

- Configure restricted ACLs on text-based configuration files such as Machine.config and Web.config.
- Keep custom configuration stores outside of the Web space. This removes the potential to download Web server configurations to exploit their vulnerabilities.

Retrieval of Plaintext Configuration Secrets - Restricting access to the configuration store is a must. As an important defense in depth mechanism, you should encrypt sensitive data such as passwords and connection strings. This helps prevent external attackers from obtaining sensitive configuration data. It also prevents rogue administrators and internal employees from obtaining sensitive details such as database connection strings and account credentials that might allow them to gain access to other systems.

Lack of Individual Accountability - Lack of auditing and logging of changes made to configuration information threatens the ability to identify when changes were made and who made those changes. When a breaking change is made either by an honest operator error or by a malicious change to grant privileged access, action must first be taken to correct the change. Then apply preventive measures to prevent breaking changes to be introduced in the same manner. Administrative accounts must not be shared. User/application/service accounts must be assigned at a level that allows the identification of a single source of access using the account, and that contains any damage to the privileges granted that account.

Over-privileged Application and Service Accounts - If application and service accounts are granted access to change configuration information on the system, they may be manipulated to do so by an attacker. The risk of this threat can be mitigated by adopting a policy of using least privileged service and application accounts. Be wary of granting accounts the ability to modify their own configuration information unless explicitly required by design.

Sensitive Data

Sensitive data is subject to a variety of threats. Attacks that attempt to view or modify sensitive data can target persistent data stores and networks. Top threats to sensitive data include:

- **Access to sensitive data in storage**
- **Network eavesdropping**
- **Data tampering**

Access to Sensitive Data in Storage - You must secure sensitive data in storage to prevent a user — malicious or otherwise — from gaining access to and reading the data.

Countermeasures:

- Use restricted ACLs on the persistent data stores that contain sensitive data; Store encrypted data.
- Use identity and role-based authorization to ensure that only the user or users with the appropriate level of authority are allowed access to sensitive data. Use role-based security to differentiate between users who can view data and users who can modify data.

Network Eavesdropping - The HTTP data for Web application travels across networks in plaintext and is subject to network eavesdropping attacks, where an attacker uses network monitoring software to capture and potentially modify sensitive data.

Countermeasures:

- Encrypt the data.
- Use an encrypted communication channel, for example, SSL.

Data Tampering - refers to the unauthorized modification of data, often as it is passed over the network. One countermeasure to prevent data tampering is to protect sensitive data passed across the network with tamper-resistant protocols such as hashed message authentication codes (HMACs).

Session Management

Session management for Web applications is an application layer responsibility. Session security is critical to the overall security of the application. Top session management threats include:

- **Session hijacking**
- **Session replay**
- **Man in the middle**

Session Hijacking - occurs when an attacker uses network monitoring software to capture the authentication token (often a cookie) used to represent a user's session with an application. With the captured cookie, the attacker can spoof the user's session and gain access to the application. The attacker has the same level of privileges as the legitimate user.

Countermeasures:

- Use SSL to create a secure communication channel and only pass the authentication cookie over an HTTPS connection.
- Implement logout functionality to allow a user to end a session that forces authentication if another session is started.
- Make sure you limit the expiration period on the session cookie if you do not use SSL. Although this does not prevent session hijacking, it reduces the time window available to the attacker.

Session Replay - occurs when a user's session token is intercepted and submitted by an attacker to bypass the authentication mechanism. For example, if the session token is in plaintext in a cookie or URL, an attacker can sniff it. The attacker then posts a request using the hijacked session token.

Countermeasures:

- Re-authenticate when performing critical functions. For example, prior to performing a monetary transfer in a banking application, make the user supply the account password again.
- Expire sessions appropriately, including all cookies and session tokens.
- Create a "do not remember me" option to allow no session data to be stored on the client.

Man in the Middle Attacks - occurs when the attacker intercepts messages sent between you and your intended recipient. The attacker then changes your message and sends it to the original recipient. The recipient receives the message, sees that it came from you, and acts on it. When the recipient sends a message back to you, the attacker intercepts it, alters it, and returns it to you. You and your recipient never know that you have been attacked.

Countermeasures:

- Use cryptography. If you encrypt the data before transmitting it, the attacker can still intercept it but cannot read it or alter it. If the attacker cannot read it, he or she cannot know which parts to alter. If the attacker blindly modifies your encrypted message, then the original recipient is unable to successfully decrypt it and, as a result, knows that it has been tampered with.
- Use Hashed Message Authentication Codes (HMACs). If an attacker alters the message, the recalculation of the HMAC at the recipient fails and the data can be rejected as invalid.

Cryptography

Most applications use cryptography to protect data and to ensure it remains private and unaltered. Top threats surrounding your application's use of cryptography include:

- **Poor key generation or key management**
- **Weak or custom encryption**
- **Checksum spoofing**

Poor Key Generation or Key Management - Attackers can decrypt encrypted data if they have access to the encryption key or can derive the encryption key. Attackers can discover a key if keys are managed poorly or if they were generated in a non-random fashion.

Countermeasures:

- Use built-in encryption routines that include secure key management. Data Protection application programming interface (DPAPI) is an example of an encryption service provided on Windows 2000 and later operating systems where the operating system manages the key.

- Use strong random key generation functions and store the key in a restricted location — for example, in a registry key secured with a restricted ACL — if you use an encryption mechanism that requires you to generate or manage the key.
- Encrypt the encryption key using DPAPI for added security.
- Expire keys regularly.

Weak or Custom Encryption - An encryption algorithm provides no security if the encryption is cracked or is vulnerable to brute force cracking. Custom algorithms are particularly vulnerable if they have not been tested. Instead, use published, well-known encryption algorithms that have withstood years of rigorous attacks and scrutiny.

Countermeasures:

- Do not develop your own custom algorithms.
- Use the proven cryptographic services provided by the platform.
- Stay informed about cracked algorithms and the techniques used to crack them.

Checksum Spoofing - Do not rely on hashes to provide data integrity for messages sent over networks. Hashes such as Secure Hash Algorithm (SHA1) and Message Digest compression algorithm (MD5) can be intercepted and changed.

If an attacker intercepts the message by monitoring the network, the attacker could update the message and recompute the hash (guessing the algorithm that you used).

To counter this attack, use a MAC or HMAC. The Message Authentication Code Triple Data Encryption Standard (MACTripleDES) algorithm computes a MAC, and HMACSHA1 computes an HMAC. Both use a key to produce a checksum. With these algorithms, an attacker needs to know the key to generate a checksum that would compute correctly at the receiver.

Parameter Manipulation

Parameter manipulation attacks are a class of attack that relies on the modification of the parameter data sent between the client and Web application. This includes query strings, form fields, cookies, and HTTP headers. Top parameter manipulation threats include:

- **Query string manipulation**
- **Form field manipulation**
- **Cookie manipulation**
- **HTTP header manipulation**

Query String Manipulation - Users can easily manipulate the query string values passed by HTTP GET from client to server because they are displayed in the browser's URL address bar. If your application relies on query string values to make security decisions, or if the values represent sensitive data such as monetary amounts, the application is vulnerable to attack.

Countermeasures:

- Avoid using query string parameters that contain sensitive data or data that can influence the security logic on the server. Instead, use a session identifier to identify the client and store sensitive items in the session store on the server.
- Choose HTTP POST instead of GET to submit forms.
- Encrypt query string parameters.

Form Field Manipulation - The values of HTML form fields are sent in plaintext to the server using the HTTP POST protocol. This may include visible and hidden form fields. Form fields of any type can be easily modified and client-side validation routines bypassed. As a result, applications that rely on form field input values to make security decisions on the server are vulnerable to attack. To counter the threat of form field manipulation, instead of using hidden form fields, use session identifiers to reference state maintained in the state store on the server.

Cookie Manipulation - Cookies are susceptible to modification by the client. A number of tools are available to help an attacker modify the contents of a memory-resident cookie. Cookie manipulation is the attack that refers to the modification of a cookie, usually to gain unauthorized access to a Web site.

While SSL protects cookies over the network, it does not prevent them from being modified on the client computer. To counter the threat of cookie manipulation, encrypt and use an HMAC with the cookie.

HTTP Header Manipulation - HTTP headers pass information between the client and the server. The client constructs request headers while the server constructs response headers. If your application relies on request headers to make a decision, your application is vulnerable to attack. Do not base your security decisions on HTTP headers. For example, do not trust the HTTP Referer to determine where a client came from because this is easily falsified.

Exception Management

Exceptions that are allowed to propagate to the client can reveal internal implementation details that make no sense to the end user but are useful to attackers. Applications that do not use exception handling or implement it poorly are also subject to denial of service attacks. Top exception handling threats include:

- **Attacker reveals implementation details**
- **Denial of service**

Attacker Reveals Implementation Details - One of the important features of the .NET Framework is that it provides rich exception details that are invaluable to developers. If the same information is allowed to fall into the hands of an attacker, it can greatly help the attacker exploit potential vulnerabilities and plan future attacks. The type of information that could be returned includes platform versions, server names, SQL command strings, and database connection strings.

Countermeasures:

- Use exception handling throughout your application's code base.
- Handle and log exceptions that are allowed to propagate to the application boundary.
- Return generic, harmless error messages to the client.

Denial of Service - Attackers will probe a Web application, usually by passing deliberately malformed input. They often have two goals in mind. The first is to cause exceptions that reveal useful information and the second is to crash the Web application process. This can occur if exceptions are not properly caught and handled.

Countermeasures:

- Thoroughly validate all input data at the server.
- Use exception handling throughout your application's code base.

Auditing and Logging

Auditing and logging should be used to help detect suspicious activity such as footprinting or possible password cracking attempts before an exploit actually occurs. It can also help deal with the threat of repudiation. Top auditing and logging related threats include:

- **User denies performing an operation**
- **Attackers exploit an application without leaving a trace**
- **Attackers cover their tracks**

User Denies Performing an Operation - The issue of repudiation is concerned with a user denying that he or she performed an action or initiated a transaction. You need defense mechanisms in place to ensure that all user activity can be tracked and recorded.

Countermeasures:

- Audit and log activity on the Web server and database server, and on the application server as well, if you use one.
- Log key events such as transactions and login and logout events.
- Do not use shared accounts since the original source cannot be determined.

Attackers Exploit an Application Without Leaving a Trace - System and application-level auditing is required to ensure that suspicious activity does not go undetected.

Countermeasures:

- Log critical application level operations.

- Use platform-level auditing to audit login and logout events, access to the file system, and failed object access attempts.
- Back up log files and regularly analyze them for signs of suspicious activity.

Attackers Cover Their Tracks - Your log files must be well-protected to ensure that attackers are not able to cover their tracks.

Countermeasures:

- Secure log files by using restricted ACLs.
- Relocate system log files away from their default locations.

Conclusions

By being aware of the typical approach used by attackers as well as their goals, you can be more effective when applying countermeasures. It also helps to use a goal-based approach when considering and identifying threats, and to use the STRIDE model to categorize threats based on the goals of the attacker, for example, to spoof identity, tamper with data, deny service, elevate privileges, and so on. This allows you to focus more on the general approaches that should be used for risk mitigation, rather than focusing on the identification of every possible attack, which can be a time-consuming and potentially fruitless exercise.

Knowledge of these threats, together with the appropriate countermeasures, provides essential information for the threat modeling process It enables you to identify the threats that are specific to your particular scenario and prioritize them based on the degree of risk they pose to your system.

Tools That Detect Vulnerabilities and Threats

Vendor Name	**Product Name**	**Vendor Web Site**
eEye	Retina	http://www.eeye.com/
Foundstone	FS1000	http://www.foundstone.com/
Harris	STAT	http://www.harris.com/
Nessus	Nessus	http://www.nessus.org/
nCircle	IP360	http://www.ncircle.com/
ISS	Internet Scanner	http://www.iss.net/
Qualys	QualysGuard	http://www.qualys.com/

Today's leading scanners are able to scan for thousands of vulnerabilities and threats at a time. Scanners are either intrusive, or non-intrusive. If you are using an intrusive scanner, you should only scan your network during off hours such as late at night or on the weekend. While intrusive scanners may perform additional tests, searching for deeper vulnerabilities, they also have the potential to bring down applications and servers. If you scan your network using a non-intrusive scanner, the only affect you should see on the operation of your systems and networks is increased network traffic, and possibly minute performance delays from the systems currently being scanned. Some scanners are designed specifically to scan applications, while others are designed to scan operating systems and applications.

References

1. http://209.85.129.132/search?q=cache:7uiESKpBpBoJ:www.kaspersky.com/threats+threats&cd=3&hl=ro&ct=clnk&gl=ro
2. http://209.85.129.132/search?q=cache:xvxHBTgchJgJ:www.mcafee.com/us/threat_center/default.asp+threats&cd=4&hl=ro&ct=clnk&gl=ro
3. http://209.85.129.132/search?q=cache:NzNY3AzwmsEJ:www.sans.org/top20/2000/+threats+top+10&cd=2&hl=ro&ct=clnk&gl=ro

4. http://209.85.129.132/search?q=cache:neOZsef38vQJ:threatinfo.trendmicro.com/+threats+top+10&cd=7&hl=ro&ct=clnk&gl=ro
5. http://www.boran.com/security/IT1x-4.html
6. http://irm.cit.nih.gov/sectrain/infosb.html
7. http://cve.mitre.org/cve/index.html
8. http://www.us-cert.gov/index.html.
9. http://msdn.microsoft.com/en-us/library/8dbf701c(VS.71).aspx
10. http://msdn.microsoft.com/en-us/library/aa302430.aspx
11. http://www.eeye.com/
12. http://www.foundstone.com/
13. http://www.harris.com/
14. http://www.nessus.org/
15. http://www.ncircle.com/
16. http://www.iss.net/
17. http://www.secprodonline.com/Home.aspx
18. http://download.bitdefender.com/resources/files/Main/file/H2-2009-Malware-and-Spam-Review-final.pdf

VOICE OVER IP SECURITY

2nd LT Eng. Adrian LUTEA

UM 01812 Balotesti

1. Introduction

Internet telephony is becoming more and more important. No matter in which country you are, a look through the windows of an internet cafe reveals numerous users of Skype—a software which was only released in 2004 and has now up to 6 million users being online at any time. The so-called Voice over IP (short: VoIP) technology offers cheap calls all over the world. Besides the popular Skype solution, there exist various other open protocols such as SIP or H.323. Moreover, VoIP functionality has been integrated into many instant messaging tools such as ICQ or Google Talk.

VoIP systems are an attractive alternative compared to traditional telephony for various reasons: use of existing internet infrastructure, cheap connections, no need for expensive hardware, and so on. However, so far, it is not clear whether these solutions can be used in security-critical environments. This document studies VoIP from a security perspective. We are interested in questions such as: Can Alice communicate securely with Bob over today's VoIP systems, that is, such that an attacker cannot follow their conversation (e.g., by decrypting the traffic)? Is it possible for the attacker to pretend being Alice such that Bob provides her with confidential information? Are man-in-the-middle attacks possible? And so on. We will also look at threats which may reduce the availability of a service, for instance denial-of-service (DoS) attacks. We study the security of state-of-the-art systems such as Skype, SIP, and H.323. We show that attacks are sometimes very easy, and give an example of a man-in-the-middle attack for SIP.

VoIP also introduces threats which have not existed in traditional telephony. One such

example is spam: Since making a call is almost free over VoIP, the distribution of unsolicited mail is attractive. We will show that VoIP spam (a.k.a. SPIT) is quite different from email spam, and it is harder to establish countermeasures, i.e., approaches such as Bayesian filters are useless. We will review and evaluate several existing solutions for the SPIT problem in detail, and then present our own approaches, for example a biometric framework which keeps away spammers by requiring them to contribute personal information.

The rest of this report is organized as follows. In the next section we give an overview of VoIP security in general. Section 3 focuses on a sample security problem in more detail, namely spam. We then look at the various VoIP implementations in use today and analyze their security (Section 5). Section 6 presents our SIP man-in-the-middle attack. Finally we conclude by giving recommendations on using VoIP today in security-critical environments and by stating some key challenges for VoIP security in the future.

2. How VoIP works

2.1. The Basics

The basic process involved in a VoIP call is as follows:

1. Conversion of the caller's analogue voice signal into a digital format

2. Compression and translation of the digital signal into discrete Internet Protocol packets
3. Transmission of the packets over the Internet or other IP-based network
4. Reverse translation of packets into an analogue voice signal for the call recipient.

The digitisation and transmission of the analogue voice as a stream of packets is carried out over a digital data network that can carry data packets using IP and other, related Internet-related protocols. This network may be an organisation's internal LAN, a leased network, the PSTN or the open Internet. The compression process is carried out by a *codec*, a voice-encoding algorithm, which allows the call to be transmitted over the IP network within the network's available bandwidth.

2.2. What you need to make a VoIP call

To make a VoIP call, the consumer user requires VoIP software and a broadband connection to the Internet. The software will handle the call routing to make sure the call reaches the intended destination as well as providing the codec. The software can be installed on a variety of hardware devices including traditional telephone handsets (using an adaptor that plugs into the telephone) or a PC or wireless device such as a Personal Digital Assistant (PDA). This use of software-enhanced end-user devices is one of the key distinguishing features of VoIP. Whereas the traditional telephone system contains its 'intelligence' within the network, VoIP makes use of the Internet model of intelligence at the *edge* of the network. This is often known as the end-to-end principle.

In order to make a call, an account with a VoIP service provider is also required. Different types of VoIP service are available, including services from traditional telephone carriers such as BT, and from specialised VoIP providers such as US firm Vonage and Luxembourg-based Skype. Some VoIP providers provide support only for PC-to-PC calls, while others provide the ability to make and receive calls from IP-enabled devices to users on the PSTN and on mobile networks.

UK telecoms regulator Ofcom advises UK consumers to carefully check the different services available from VoIP providers, including whether or not the provider offers a backup service to make calls via the PSTN if there is a problem with the broadband connection and offers access to the emergency services.

2.3. How VoIP is used

VoIP is operating in a heterogeneous environment that extends way beyond the Internet. Voice calls need to have the potential to be carried over a variety of different networks including local networks, PBXs, PSTN and the Internet. Advances in VoIP technology mean PC telephony software is available from many software developers. Gateway servers with voice-processing cards are also available, to act as an interface between the Internet and the PSTN, enabling users to make calls either from their PCs, or from an IP phone, into the traditional telephone networks. Calls can also be made using IP handsets, which look similar to traditional phones, but which are plugged into an IP-based network rather than into the traditional telephony network, and have more features and capabilities than traditional telephones. The result is that there are now a number of ways in which VoIP can be implemented:

- PC to PC. Both the caller and recipient use headsets plugged into their PC.
- PC to PSTN. Only the caller uses a headset. The recipient receives the call in the traditional way.
- PSTN to PSTN. The caller uses an IP adaptor on their traditional telephone and the call is received on a traditional phone. But the call travels over an IP network.
- IP phone to PSTN. The caller uses an IP phone, and the call transfers from the IP network to the telephone network via a gateway.
- IP phone to IP phone. The call travels over an end-to-end IP network.

It should be noted that there is confusion amongst communications professionals and industry commentators as to the use of terms like “VoIP”, “Internet Telephony” and “IP Telephony'.

3. Security

When dealing with modern information technology systems such as VoIP, security is omnipresent. There are mainly three key aspects of information security often referred to as the CIA triad: confidentiality, integrity and availability. There are additional aspects to security which are not included in the CIA triad, e.g., non-repudiation or accounting.

However, they are of minor interest to the users of VoIP systems, and hence we will not discuss them here. In this section, we first give a general definition of each of the three aspects of the CIA triad and discuss them with respect to the second; we give an overview on the most important security threats for VoIP in general. Section 6 will then look at more specific protocol and application threats.

3.1. Confidentiality

Definition: Confidentiality means that no information will be disclosed to unauthorized subjects. Information meets the confidentiality criterion when disclosure or exposure to unauthorized individuals or systems is prevented; it ensures that only those with the rights and privileges to access information are able to do so.

We have to distinguish between two information sources: (i) the audio signal and (ii) the call control. (i) Threats regarding the audio signal are eavesdropping and man-in-the-middle attacks. Thus, the confidentiality between the called and the calling party can be broken. (ii) The threats regarding call control or signaling are the exposure of information about users (also names, passwords, etc.), systems (e.g., system version) and patterns. This information can be used for attacking a system or the privacy.

Defense Strategies:

- physical protection (e.g., equipment rooms)
- use of Ethernet switching instead of shared media
- use of VLANs, VPNs where applicable (just like your data network!)
- encrypting conversations and call control, secure the media stream SRTP
- ensuring that routing tables, instructions, account codes are well maintained and password protected

3.2. Integrity

Definition: Integrity captures the trust that can be placed in the information. Data integrity assures that the information has not been altered between its transmission and its reception. There are two categories of integrity (i) source integrity and (ii) data integrity.

(i) Source integrity guarantees that the data comes indeed from the correct sender.

(ii) Data integrity is compromised when information has been corrupted, willfully or accidentally, before it is read by its intended recipient. Integrity in VoIP should ensure that packets get from one point to another without modification. Regarding the audio signal, the main threats are impersonation of user or injection of other audio. The consequences are hard to be estimated and can go from annoyance to severe incidents. With respect to call control or signaling the major threat is fraudulent use of telephony resources as toll fraud or impersonation.

Defense Strategies:

- use of encryption for secure communications
- changing default password, minimum length, enforce periodic change
- never exchanging passwords in clear text
- password maintenance, delete ex-employees, security codes.

3.3. Availability

Definition: Availability means that information or resources are accessible when required. Most often this means that the resources are available at a rate which is fast enough for the wider system to perform its task as intended. It is certainly possible to protect confidentiality and integrity, but an attacker can for example run a Denial of Service attack (DoS) to reduce the availability of resources.

For VoIP, availability means ensuring that communication services are accessible to the users, especially avoiding any adverse effects resulting from a DoS attack or computer worm. Typical DoS attacks seek to (i) crash or (ii) overload a system. The consequences are partial or total loss of telephony or related services. (i) The teardrop attack involved sending IP fragments with overlapping oversized payloads to the target machine. A bug in the TCP/IP fragmentation re-assembly code caused the fragments to be improperly handled, crashing the operating system as a result. Similarly, VoIP stacks can also suffer from malformed packets. A ping of death involves sending a malformed or otherwise malicious ping to a computer. Sending an oversized ping often crashes the target computer. (ii) The smurf attack, named after its exploit program, is a denial-of-service attack which uses spoofed broadcast ping messages to flood a target system.

Defense Strategies:

- rigorous virus updates, OS and software patches
- intrusion detection systems
- protect access from external sources (firewall)
- limit access from internal sources (firewall)
- use of 802.1 p/q (VLAN) to isolate and protect voice domain bandwidth from data domain DoS floods.

3.4. VoIP Security Threats

There are several security threats related to VoIP. Following we briefly list the most important ones:

- **Reconnaissance attacks**: intelligent gathering or probing for assessing the vulnerabilities of a VoIP system
- **Floods and Distributed Floods**: overloading a system resulting in a denial of service attacks
- **Protocol Fuzzing:** using semi-valid input to crash or confuse a system
- **Spoofing:** misuse of someone other's address or identity
- **Session Anomalies:** confusing signaling and call control for session hijacking or denial of service
- **Stealth Attacks:** frequent requests (calls) for annoying users
- **VoIP Spam:** transmitting unsolicited and unwanted bulk messages (see Section 4)

4. Spam over internet telephony (SPIT)

Although there exists only little VoIP spam today, it may become a big threat in the near future. As has been demonstrated by email spam (e.g., Nigeria scam industry), people are often taken in by these kind of advertisements. In this section, we first look at the characteristics of SPIT and argue why traditional solutions for email spam filtering fail.

Afterwards, several possible solutions are discussed and compared. For a good overview on the topic, note the NEC documents, the IETF draft on SIP, and the thesis by Radermacher.

4.1. Properties of VoIP Spam

At the heart of the SPIT problem lies the fact that sending advertisements comes (almost) for free, is often anonymous and not illegal, making VoIP an attractive medium for spammers. Unlike traditional telephone systems where the telemarketer had to pay for each call, advertisements can be sent in parallel to thousands of potential customers at no transmission cost.

In this respect, SPIT is similar to the email spam problem which many Internet users face today: As companies did no longer have to pay postmen to carry their advertisements to the people's mailboxes, but could send unsolicited email to virtually all inboxes for free, the amount of advertisement mail exploded. However, although email spam will still be a big challenge in the future, the numerous solutions proposed over the last years have helped to mitigate the problem significantly. For example in Spamato, users collaboratively filter spam with respect to suspicious text contents, suspicious sender domains, etc.

Unfortunately, many great mechanisms which work for email spam fail completely in the context of VoIP. There are many reasons. First, an email usually arrives at a server before it is finally downloaded by the user. Such a mail server can therefore apply many filtering strategies, for instance, it can check whether the text body of the email mentioned pharmaceutical products. In contrast, in VoIP, human voices are transmitted rather than text. To recognize voices and to determine whether the message is spam or not is still a very difficult task for a computer. What is more, a recipient of a call only learns about the subject of the message when she or he is actually listening to it.

Also from a user's perspective, SPIT is quite different from spam. Although a spam email is a nuisance, it is typically easy to delete such an email. But it can be really bad if a regular email from a friend is considered spam and not delivered to a user's inbox. That is, it may be tolerable if an email spam filter yields a large ratio of false negatives, but the filter should avoid false positives completely.

The situation looks different for SPIT. Receiving a spam email often means that the telephone rings, possibly waking users up in the middle of the night. On the other hand, if a call by a friend does not get through, the friend immediately recognizes that she or he has been filtered, and can try again—possibly using a different communication channel.

4.2. Existing Solutions

Having motivated the SPIT problem, in this section, we look at some potential solutions. We will see that there is no panacea for the spam problem, as all approaches come with some drawbacks. However, there are certain design mistakes that can easily be avoided.

For example, the VoIP phone numbers should not be as densely populated as regular phone numbers in order to avoid phone number guessing. Generally, we believe that SPIT will continue being a threat in future.

An overview and classification of SPIT prevention methods is depicted in Figure 1.

4.2.1. Content Filtering

As already mentioned, at the time a user learns about the contents of a call, the connection has already been established—the spam cannot be analyzed before it is actually delivered. Therefore, classic spam filtering techniques such as Bayesian spam filters or URL spam filters are useless. Moreover, even if the content is stored on a voice mail box, it is still difficult today for speech recognition technologies to decide whether it is spam or not.

4.2.2. Turing Tests and Cryptographic Puzzles

Fully automated SPIT of so called bots is one of the cheapest and most annoying things. To fight them, they can be challenged in several ways (so-called Turing tests).

1. Voice Menu: Before a call is put through, a computer asks the caller to press a certain key combination, for example "press #54".
2. Challenge Models: Before a call is put through, a computer asks the caller to solve a simple equation and to type in the answer, for example "divide 10 by 2".
3. Alternative Number: Under the main number a computer announces an alternative number. This number may even be changed permanently by a call management server. All of theses methods can even be enforced by enriching the audio signal with noise or music. This prevents SPIT bots from using speech recognition.

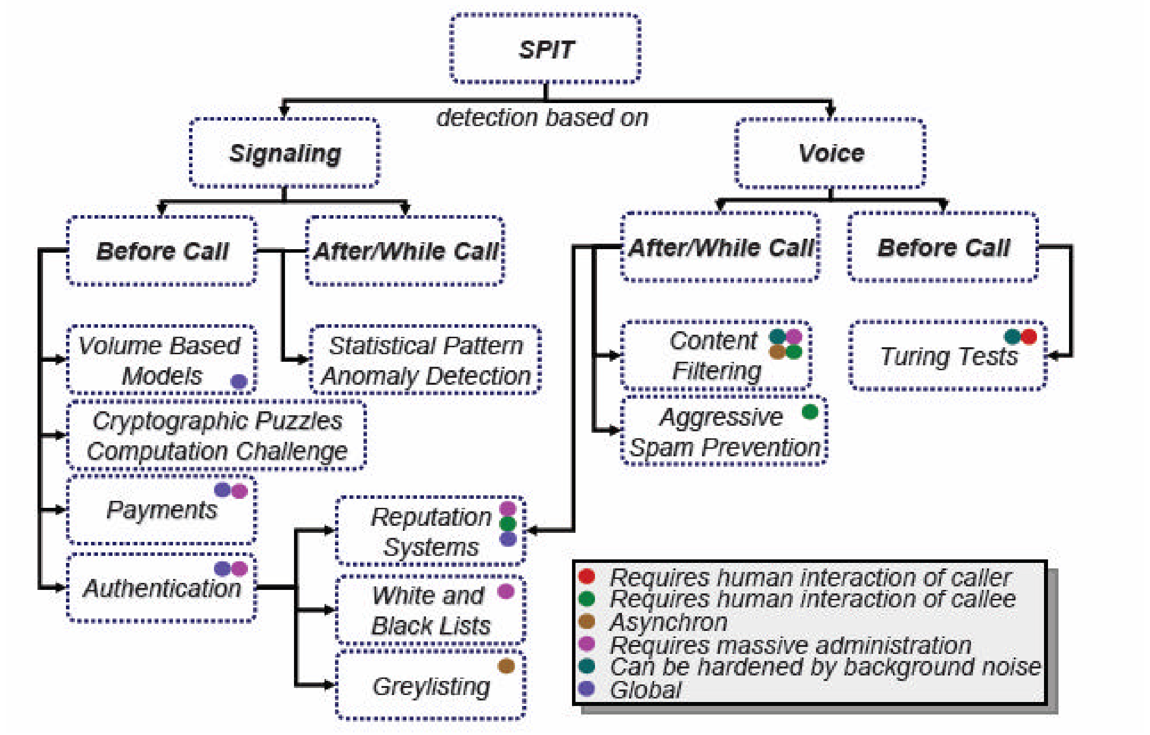

SPIT
detection based on
Signaling
Voice
Before Call
After/While Call
After/While Call
Before Call
Volume Based Models
Statistical Pattern Anomaly Detection
Content Filtering
Turing Tests
Cryptographic Puzzles Computation Challenge
Aggressive Spam Prevention
Payments
Reputation Systems
Authentication
White and Black Lists
Greylisting
Requires human interaction of caller
Requires human interaction of callee
Asynchron
Requires massive administration
Can be hardened by background noise
Global

Figure 1: Overview and Classification of SPIT Prevention Methods

Such Turing tests are attractive, as it is often hard for computers to decode audio questions. However, these puzzles can not be made too difficult as human beings must always be able to solve them. Therefore, there are concerns about this approach in the long run.

Cryptographic puzzles may also help to detain spammers. Whenever a caller tries to establish a connection, he has to solve a small puzzle consuming computational resources (CPU and bandwidth). Clearly, as the computational power is limited, the number of parallel connection requests remains small. The drawback of this solution is that a regular caller with a slow machine may also experience unacceptable delays due to the puzzle challenges. Finally, as spammers sometimes use virus-infected machines (so called zombies), their computational power can be large.

4.2.3. Payments

The main reason for the spam problem is the fact that the cost of sending spam is almost zero. A straight-forward solution would therefore be to charge the caller a small amount of money for each connection attempt. This amount should be so small that VoIP calls remain virtually free for regular users, but prohibitively high for spammers. This is of course a difficult trade off. What is more, the implementation of such a payment infrastructure may be an ambitious endeavor.

Another idea is to charge back the cost (payments at risk) if the receiver decides that the call is not spam. Unfortunately, today, Internet transactions always cost a minimum amount of money, e.g., 25 cents.

4.2.4. White and Black Lists

Very effective solutions to the SPIT problem are white lists. Thereby, a user explicitly states which persons are allowed to contact her. A similar technique is also used in Skype: If Alice wants to call Bob, she first has to add Bob to her contact list and send a contact request to Bob. Only when Bob has accepted this request, Alice can make calls to Bob.

Given that there are authentication mechanisms which prevent some attacker from pretending being Bob's friend Alice (address spoofing), unsolicited calls can be prevented.

In general, white lists have an introduction problem, as it is not possible to receive calls by someone who has not yet been put on the white list explicitly.

Black lists maintain addresses that identify spammers and can be used in addition to white lists. The drawback of black lists however is that addresses can often be spoofed or changed easily by spammers unless there are inter-domain authentication mechanisms.

White and black lists have been studied intensively also in the context of VoIP, and the interested reader may refer to. Also note that there are always two approaches to create white and black lists: these lists can either be generated manually, or they can be generated automatically using some statistical analysis of traffic or volume patterns.

4.2.5. Greylisting

Greylisting is a useful technique to filter spam emails, and it can also be applied to VoIP. Thereby, each call is blocked unless the same sender (w.r.t. IP address) tries to establish the call again within a certain time period. However, there are many concerns about this approach: First, it seems easy to circumvent the filter by just making second attempts. In addition, greylisting may block emergency calls from friends.

4.2.6. Reputation Systems

The idea of a reputation system is to give Alice a hint about the reputation of a caller before she answers the call. If the reputation is poor, she can decide not to accept the call. Unfortunately, reputation systems are often complex in distributed environments and susceptible to false praise. Moreover, if new identities are easy to acquire, a user with a negative reputation can just open a new account.

4.2.7. Volume Based Models

The idea here is that ISPs should restrict the number of VoIP connection requests their customers can execute over time. Of course, it is unlikely that ISPs will really collaborate in this respect, as they have incentives to be slightly less restrictive than their concurrence.

4.2.8. Authentication

Both SIP and H.323 support a vast variety of models for user authentication. Such authentication methods can be hardened for preventing anonymous VoIP traffic. However, a global authorization model is not realistic today.

4.2.9. Statistical Analysis of VoIP Signaling

The idea of static analysis of VoIP signaling is to monitor the signaling traffic on the recipients' access domain gateway. For each external identity observed in the signaling routing data, counters may be maintained for the number of times call setup and call termination requests went in or out of the access domain. These counters can then be statistically evaluated, for example by assuming that they have characteristic distributions.

If this assumption is violated, various actions can be taken such as:

- Warning: Display the text warning on the phone, use special ringing tone.
- Call delay: Switch the caller to the recipient's voice mail, reject the request and report the callerID and the missed call at a later time.
- Call cancellation: Drop the call setup on behalf of the recipient.

4.2.10. Aggressive Spam Prevention

Aggressive spam prevention mechanisms fall into two categories: (i) active publishing of incorrect information and (ii) counter attack on spammers. Proactive publishing of incorrect information, namely SIP addresses, is a possible way to fill up the databases of the spammers with existing contacts. This increases the cost for a successful delivery of spam. Counter attack on the infrastructure of spammers is a way to bring them out of business. This is most effective if many victims use this technique. But this method is quiet expensive and dangerous since it could be misused for distributed denial of service attacks.

5. A biometric framework for SPIT prevention

A major difficulty in coping with the SPIT problem is the fact that spammers can change their identity frequently. Methods such as blacklists fight an uphill battle in the presence of continuously altering identities. Therefore, it is vital in any spam filtering system to inhibit these so-called Sybil attacks.

Binding identities to persons can help to prevent Sybil attacks. In this section, we present a generic framework which tackles the SPIT problem. In this solution, global servers bind the users' identities to personal data; in our case, to biometric such as a voice. Consequently, unlike in other solutions, spammers cannot obtain new identities even if they change the ISP.

5.1. Concept and Architecture

The general architecture of our system is shown in Figure 2. We use a set of trusted authentication servers (A). Before a client (C) uses VoIP for the first time, he has to register with an authentication server. The goal of this procedure is to record the user's voice and bind it to his VoIP ID. This is done as follows. First, the client calls the server. The server then asks the client to repeat a sentence, for example, a phrase from Goethe's Faust. In order to enhance the security of this procedure, the phrases should be different for each registration request. Moreover, several different languages should be offered such that each client can use his mother tongue. After completing Step 1 (figure 2), the server stores the client's vo ice file and sends back credentials; in case of a PKI infrastructure, this is a server signed public key (Step 2). The client can now make arbitrary calls to other clients, authenticating him using his credentials (Step 3). Anyone receiving such a call verifies the identity by checking the credentials; this may involve contacting the authentication servers (Step 4).

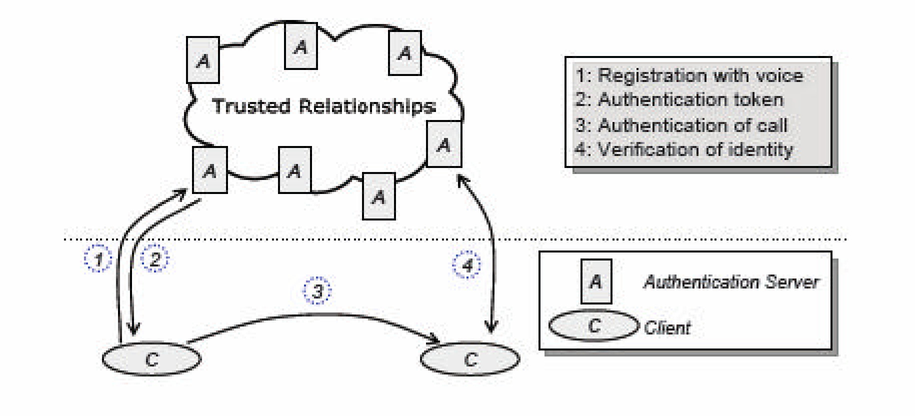


Figure 2: System architecture.

The key idea here is that it is impossible for a client to run a Sybil attack: A client who wishes to obtain additional identities is unmasked by the authentication server: The servers run a voice recognition software to reject duplicated registrations.

Observe that this approach has desirable properties. First, the solution is independent of a specific VoIP protocol and inter-operable: Authentication can be done centrally for all sorts of clients, e.g., SIP, Skype, etc. Moreover, an attacker cannot obtain new identities by switching to another provider either, as our approach is also ISP-independent. Also note that this solution is slightly different from many biometry-based systems in the sense that we do not use biometric data for the authentication, but only as a reference data to which we can compare future registration requests.

Step 1 is time consuming, but registration is executed very seldom (e.g., once a year). Step 3 on the other hand is performed before each call, and is a quick operation: It does not involve any sentence repeating or so, but only the credential verification (e.g., checking an RSA signature).

Having described the general ideas on a high level, in the following, we will describe two sample implementations. It turns out that several options are possible, for example an implementation using a public key infrastructure (PKI), or an implementation using Kerberos.

5.2. Implementation

We use SIP as the VoIP protocol and the cryptographic authentication protocol is either a PKI system or a Kerberos system.

5.2.1. Using a PKI

In case of a PKI authentication infrastructure, a client authenticates its calls based on an asymmetric certificate which proves his identity. The steps of authentication are the following (see Figure 3): The caller first checks if he has a valid certificate. If this is not the case it (re-)registers itself with its voice at a Certification Authority (CA). The CA verifies the caller's identity based on its voice and issues a certificate for the caller. This certificate contains the caller's VoIP ID and is signed with the private key of the CA; everyone who knows the CA's public key can verify this signature and therefore the caller's ID.1 The caller sends this certificate to the called, who can then check for revocation and decide to accept or deny the call.

5.2.2. Using Kerberos

The authentication infrastructure can also be realized with Kerberos. Thereby, a client is bound to authenticate its calls based on an once-ticket. In more detail, the steps of authentication are the following (see Figure 4). The caller first checks if he has a valid ticket-granting ticket. If this is not the case it (re-)registers itself with its voice at an Authentication-Server (AS). The AS verifies the caller's identity based on its voice and issues a ticket-granting ticket to the caller. This ticket-granting ticket enables the caller to get a ticket for a call to a certain called. This ticket is then used for authenticating the caller to the called. In this case, the verification procedure is symmetric.

5.2.3. PKI versus Kerberos

Both the Kerberos and the PKI based system fulfill the requirements of our authentication protocol. But there is a crucial difference between these two realizations. The Kerberos system allows for simple tracking of calls by the ticket-granting ticket server while the CA of a PKI system is unable to do so. In addition, there are also several differences between a Kerberos system and a PKI which are related to administration, communication and processing overhead. For example, while the registration step (Step 1) uses asymmetric cryptography in both cases, the Kerberos solution is typically faster in Step 3, as verification is based on classic cryptography only.

5.3. Conclusions

In this section we have proposed our own SPIT mechanism which binds clients to their identity by requiring clients to register their voice on central authentication servers. These servers ensure that the biometric data of each client is unique, and hence prevents clients from obtaining several accounts to white-wash their spamming activities.

We think that this approach may be interesting in other domains as well. However, there are several challenges in practice. For example, in truly global and inter-operable environments, the certification servers must be powerful in order to avoid bottle-necks.

Moreover, we have been told that today it is still hard to distinguish voices of thousands of users, as voice patterns are sometimes close to each other, and patterns can also be changed, for instance by using some background noise. Although we believe that technological progress will mitigate these problems, and that voice will also be transmitted in higher quality in future, this solution may currently problematic for large-scale usage.

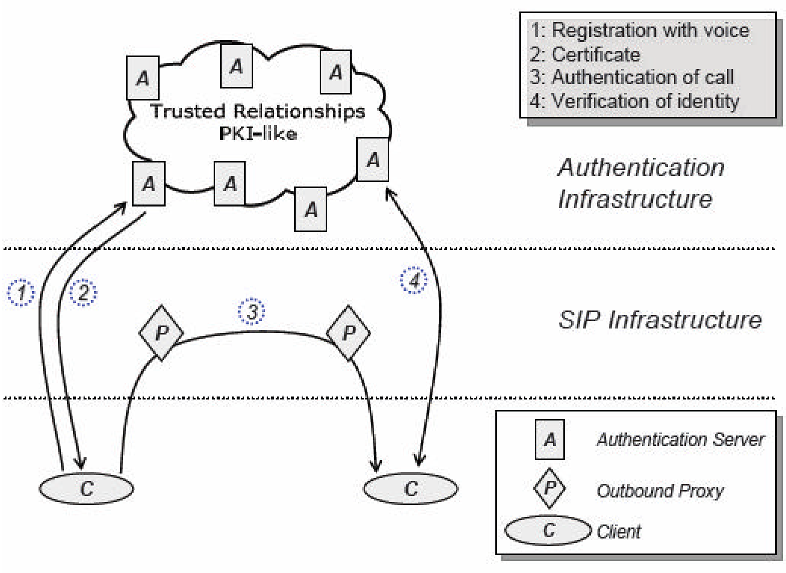


Figure 3: Biometric authentication for SIP based on PKI.

However, the general concept may be applied for different data in the meanwhile. For instance, one idea would be to ask all clients to register a unique and valid mobile phone number for each VoIP ID.

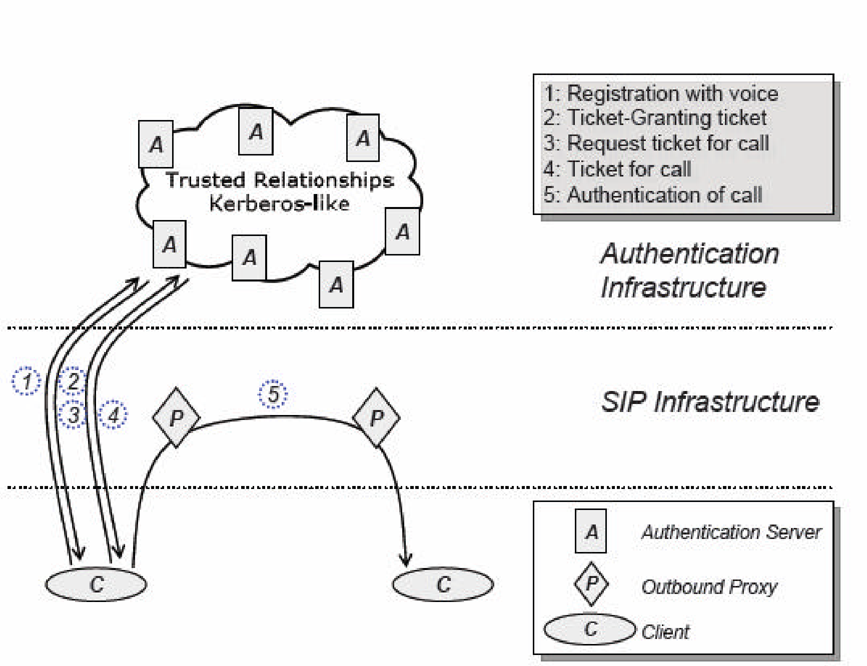


Figure 4: Biometric authentication based on Kerberos.

6. Protocols, codecs and applications

6.1. Session Initiation Protocol

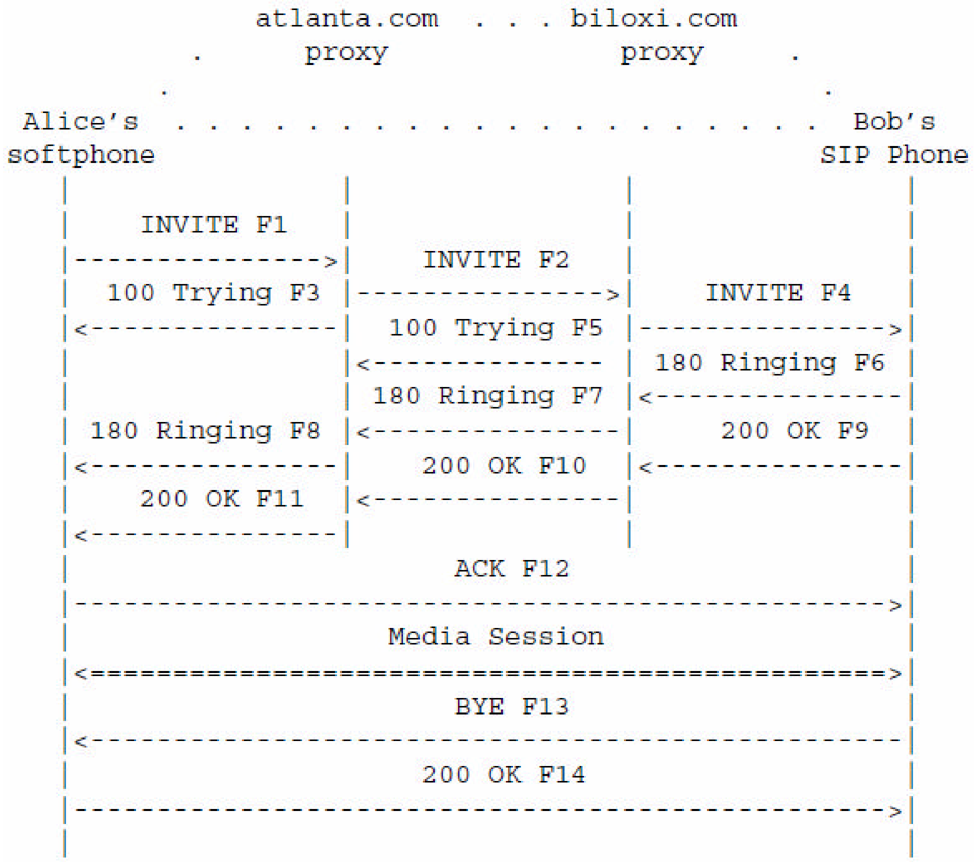
The Session Initiation Protocol (SIP) is an Internet Engineering Task Force (IETF) standard for IP telephony (RFC 3261). It is a text-based application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. SIP uses UDP, TCP or TLS as a transport protocol. The nature of the session established is defined by the content of the body of the request initiating the session. Most of the time, the Session Description Protocol (SDP, RFC 2327 [20]) is used to describe which kind of session is required (voice, video, instant messaging).

SIP is a request-response protocol. Therefore, every SIP entity is composed of two parts: the user agent client (UAC) which sends requests, and the user agent server (UAS) which responds to requests. In the SIP world, a user is represented by a type of Uniform Resource Identifier (URI) called SIP URI. The exact BNF can be found in. A typical SIP URI is in the form username@host (e.g., bob@biloxi.com).

For locating purposes, SIP enables the creation of a server infrastructure (network of proxy servers) to which user agents can send registrations, invitations to sessions, and other requests. A proxy server is usually responsible for a particular domain and can be found by running a DNS query. To resolve a SIP URI to an actual endpoint IP address, another SIP server role is defined: the registrar. Every SIP client has to register (using a SIP REGISTER request) with the server responsible for his domain if he wants to be reachable.

Basically, the registrar keeps a link between user SIP URI (called AOR, address-of-record) and user contacts (i.e., location). Note that a client can register several contacts for the same AOR. The links are stored in a database called the location service. It is important to note that the concept of proxy server and registrar are logical and not physical. A SIP server can play both roles.

To illustrate how SIP works, let us assume that Alice (sip:alice@atlanta.com) wants to start a voice session with Bob (sip:bob@biloxi.com). This example is taken from [44], a schema is shown below. Alice's SIP client has been configured to use the atlanta.com proxy for all her outgoing requests. Therefore, she sends a SIP INVITE (F1) to her proxy, which will forward it to Bob's proxy (F2). As Bob has registered, the biloxi proxy is able to forward the INVITE to Bob (F4). Bob will then accept the call and send a 200 OK. It will be acknowledged by Alice. Consequently, the media session can take place. The call can be terminated by Alice or Bob by sending a BYE.



```
                     atlanta.com  . . . biloxi.com
                 .      proxy              proxy     .
               .                                       .
       Alice's  . . . . . . . . . . . . . . . . . . . .  Bob's
      softphone                                        SIP Phone
         |                |                |                |
         |    INVITE F1   |                |                |
         |--------------->|    INVITE F2   |                |
         |  100 Trying F3 |--------------->|    INVITE F4   |
         |<---------------|  100 Trying F5 |--------------->|
         |                |<-------------- | 180 Ringing F6 |
         |                | 180 Ringing F7 |<---------------|
         | 180 Ringing F8 |<---------------|     200 OK F9  |
         |<---------------|    200 OK F10  |<---------------|
         |    200 OK F11  |<---------------|                |
         |<---------------|                |                |
         |                       ACK F12                    |
         |------------------------------------------------->|
         |                   Media Session                  |
         |<================================================>|
         |                       BYE F13                    |
         |<-------------------------------------------------|
         |                     200 OK F14                   |
         |------------------------------------------------->|
         |                                                  |
```

6.2. SIP Security

Client-Side Authentication SIP provides a stateless, challenge-based mechanism for authentication based on authentication in HTTP ([14]). For any incoming request, the user agent server may challenge the expeditor of the request to provide assurance of its identity.

In the first version of SIP (RFC 2543 [21]), "Basic Authentication" was allowed. In this authentication mode, the UAC sends the user credentials in clear text. Due to its poor security, this mode was deprecated in the new standard version ([44]). The recommended authentication mechanism is the "Digest Authentication".

In digest authentication mode, for every incoming request, the UAS will send a challenge:

```
WWW-Authenticate: Digest
realm="biloxi.com",
qop="auth,auth-int",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

The UAC of the client should then resend its invite with a special header stating its answer:

```
Authorization: Digest username="bob",
realm="biloxi.com",
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
uri="sip:bob@biloxi.com",
qop=auth,
nc=00000001,
cnonce="0a4f113b",
response="6629fae49393a05397450978507c4ef1",
opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

The response is a hash of the concatenation of the user password and different info present in some headers. This "Digest Authentication" mechanism provides message authentication and replay protection only. Nothing prevents an attacker from reading or modifying the message: there is no message integrity and confidentiality.

Server-Side Authentication SIP has no built-in mechanism to authenticate a server (proxy server, registrar, redirect server). However, it is recommended to use TLS (and check certificate validity). Servers should authenticate themselves using mutual TLS (MTLS). TLS provides a good hop-by-hop authentication.

Integrity and Confidentiality To create a session, most of the time, a SIP INVITE contains a body with session information. This body may be protected by S/MIME (RFC 1847, RFC 2633). This provides integrity and confidentiality, but may pose some interoperability problems as some firewalls might want to look at the body. Indeed, S/MIME provides end-to-end security. Moreover, to provide end-to-end integrity, a UAC may provide a copy of the whole message in the body part. This provides partial confidentiality, as the UAC may omit some headers in the "visible" version of the INVITE. Some other headers are mandatory and are visible.

Integrity may also be guaranteed by using transport or network layer security (TLS and IPSec respectively). Both methods encrypt the signaling traffic. In general, this is achieved by using certificates.

6.3. Threats and Mitigation

SIP does not provide real protection (no confidentiality, integrity or availability). Nonetheless, by using another standard, a lot of threats can be mitigated. The following threats have been described in.

Registration Hijacking

- The SIP registration mechanism is based on the From and To headers of the REGISTER requests. When receiving a REGISTER from a UAC, the registrar has to verify that the identity in the From has the permission to change the contacts of the address-of-record specified in the To. Without authentication, a malicious UAC could send a modified REGISTER, which de-registers valid contacts and registers new contacts. All subsequent requests will then be forwarded to the attacker endpoints.

- This threat can be mitigated by using “Digest Authentication” to authenticate the client.

Tampering with Message Bodies

- SIP message bodies are not encrypted, which means that a malicious proxy server may be able to modify the content of the body without notice. In case of a voice call, a malicious proxy may change the IP addresses in the INVITE request and OK response to make all RTP ([18]) packets transit by a malicious endpoints that can eavesdrop the conversation.
- To prevent such threats, the SIP client must use an end-to-end mechanism. A valid solution presented in Section 5.1.2 is S/MIME.

Tearing Down Sessions

- Once a dialog is established, subsequent requests can be sent to modify or terminate the dialog. It is then critical that the attacker cannot “sniff” the traffic and store important dialog info. If he is able to see the INVITE and the corresponding OK, he may be able to send a BYE to terminate the dialog, or send a re-INVITE with a different SDP to redirect all the media to a controlled endpoint.
- The most effective countermeasure to this threat is the authentication of the sender of the INVITE/BYE.

Denial of Service and Amplification

- Deployed SIP proxy servers often face the public internet. Hence, DoS is a probable threat, as it is easy to implement. An attacker may create bogus requests that contain a falsified source IP address (and the corresponding modification in the Via header) that identify a target host as the originator of the request. It will send these requests to a large number of SIP clients or servers, which are all going to reply to the target. Similarly, attackers might use falsified route header field values in a request that identify the target host and then send such messages to forking proxies that will amplify messaging sent to the target (Record-Route may also be used in a similar fashion). Unauthenticated REGISTER requests may lead to numerous DoS attacks. As stated before, an attacker may be able to de-register a user client, or register the same contact several times so that the user client gets flooded by requests. DoS by memory exhaustion is also possible if the attacker registers a huge number of contacts.
- Using client-side authentication is a good first step in preventing DoS. Moreover, to prevent standard DoS, the proxy server directly available from the public internet should not register any users, i.e., it should not be a registrar. Its role will be simply to forward the requests to the intern registrars. At worse, if the public proxy server is down, communication between users in the domain is still possible. Finally, the public proxy server should use mutual TLS.

Man-in-the-Middle Attack

- An attacker can easily set up a man-in-the-middle attack by using ARP spoofing/poisoning. He just has to spoof the MAC address of the SIP registrar. The attacker will receive all the requests and can modify them at will. Registration hijacking, Tampering with Message Bodies, Tearing Down Sessions are some attacks that are then easy to make. Moreover, client-side authentication will not help here as the attacker can just modify the packet and keep the challenge response intact.
- IPSec and TLS are the best solution to counter this kind of threat.

Eavesdropping

- As described in [37], an attacker can easily eavesdrop a conversation by launching a man-in-the-middle attack. Using ARP spoofing, the attacker will receive every packet destined to the attacked host.
- The best mitigation against eavesdropping is to encrypt the audio streams, by using SRTP for example.

6.4. Skype

Skype is a very popular peer-to-peer internet telephony software with more than 50 million users. Unfortunately, Skype is not open-source, and although there have been attempts to reverse-engineer certain parts of Skype, many algorithms remain unknown.

However, it has been conjectured that Skype has similarities with the file sharing tool KaZaA as the two projects share some developers. Communication typically happens directly between the participants in Skype. However, for name look-up operations and sometimes also for NAT-problems, peer-to-peer solutions are required. Concretely, it is possible to search the Skype network for other users, and hence to gather many user names. SPLIT attacks however are difficult: Bob can call Alice only after she has accepted his contact request and has added Bob to her friends'list.

Berson has performed a security evaluation of Skype Version 1.3. He found that Skype uses standard cryptographic primitives only, e.g., AES block ciphers, RSA public key cryptosystems, SHA-1 hash functions, RC4 stream ciphers, and so on. Berson concludes that Skype is robust against identity spoofing, traffic sniffing, replay attacks or man-in-the-middle attacks, and does not seem to contain any back doors or Trojans.

Skype operates a certificate authority, and every Skype client stores the central server's public key. A user authenticates itself with a unique username and password. The traffic of each session is encrypted by a 256-bit Rijndael cipher (AES). Primarily testing is done with 25 iterations of the Miller-Rabin test including all necessary test conditions. The decryption exponent (private key) is a sound Montgomery method variant of modular inversion. To protect against playback, peers challenge each other using 64-bit nonces.

However, Berson also points out some weaknesses. The CRC-type checksums are linear and may not be well-suited for detecting intentional modification of data, as has already been discovered in WEP. Moreover, a malicious program on the same machine could deduce some bits of the key by monitoring the shared resources such as CPU time and power, or storage. Finally, Berson mentions a parsing error which may lead to unpredictable behavior under malicious inputs.

6.5. H.323

H.323 is a binary-based protocol standard approved by the International Telecommunication Union (ITU) which supports real-time point-to-point multimedia data communications over non-guaranteed bandwidth, packet-based networks, such as the Internet.

H.323 is an umbrella specification as it encompasses various other ITU standards where the latest version (v5) was released in 2003.

In general, H.323 implementations include four logical entities, namely:

1. H.323 Terminals
2. Gateways (GW)
3. Gatekeepers (GK)
4. Multipoint Control Units (MCU)

A H.323 Terminal provides real-time two way communication with another H.323 terminal, gateway or MCU sending multimedia messages. H.323 terminals support audio codecs for example the G.711 codec and signaling using Q.931, H.245 and Registration, Administration and Status (RAS) protocols. Gateways are optional components and are only required when communicating between different networks for example between an IP-based network and Public Switched Telephone Networks (PSTNs). A Gateway provides data format translation, control-signaling translation, call setup and termination functionality as well as compression and packetization of voice. Gatekeepers are responsible for translating between telephone number and IP address and routing of calls. They also manage bandwidth and provide mechanisms for registration and authentication by terminals. All H.323 endpoints register with a single GK and build a H.323 zone. In order to support multi-terminal conferences, all terminals must establish a direct connection to an MCU.

Judging the security aspects of H.323 is difficult, as there is a plethora of associated protocols and vendor implementations. Per se, H.323 does not specify any cryptographic protocols, and several attacks have been reported. However, H.235 gives security recommendations for the H.3xx series; its scope is on authentication, privacy and integrity. H.235 also includes the ability to negotiate services and functionality in a generic manner.

6.5.1. H.323 Security

Media Security H.235 recommends securing the media streams by encrypting the audio stream with symmetric encryption. The encrypted stream is then encapsulated into a standard RTP packet. The encryption capabilities of the systems can be negotiated during signaling. DES, Triple DES and RC2 are intended as encryption algorithms.

Signaling Security TLS is recommended to authenticate the server components. Authentication of users is done during call control. It is done either during the initial call connection in the process of securing the signaling-channel (H.245) by support of challenge-response mechanisms or by exchanging certificates on the H.245 channel. Note that end-to-end authentication is not provided. Moreover, H.245 describes how to exchange certificates and how to use the Diffie-Hellman protocol to exchange keys. Verifying the certificate is left open.

6.5.2. Attack examples on H.323

DoS-Attack using signaling H.323 is a complex protocol suite and is therefore particularly exposed to implementation reported that a DoS attack can be performed by sending unexpected or incorrect signaling PDUs. Eavesdropping If RTP is used to transport the media, an attacker can easily eavesdrop the conversation by using ARP poisoning (man-in-the-middle attack). Gatekeeper registration attack Registration and deregistration requests can be faked if the gatekeeper does not enforce any authentication.

6.5.2. Codecs

Prior to the transmission of a voice call across an IP-based network a person's voice (which is an analogue sound wave) must be converted to a digital form and encoded. A certain amount of data compression can also take place in order to save bandwidth during the subsequent transmission. On receipt of the voice data at the other end this process must be reversed. A number of different voice-encoding algorithms are used (codecs) which have been standardized by the ITU as a series of recommendations known as the G-series (Sherburne and Fitzgerald, 2004). The common ones are G.711, which is in widespread use in the telecommunications industry within PSTN networks, and G.729. Codecs differ in the algorithms they use for sampling the analogue voice wave and the sophistication of the compression used. This in turn determines the amount of digital bandwidth required for the encoded sample. G.711, for example, requires a relatively higher bandwidth (of 64Kbps which in practice translates to 90Kbps in an actual VoIP implementation) whereas G.729 operates at 8Kbps (Nooning, 2005). However, ultimately there is a trade-off between the sophistication of the algorithms, the amount of bandwidth required and the quality of the voice signal received.

6.6. Tools

BackTrack is a Linux distribution distributed as a Live CD focused on penetration testing. It is preloaded with numerous security tools, such as Wireshark.

UCSniff is a VoIP Security Assessment tool that leverages existing open source software into several useful features, allowing VoIP owners and security professionals to rapidly test for the threat of unauthorized VoIP Eavesdropping**.**

VoIP Hopper is a security tool that rapidly runs a VLAN Hop into the Voice VLAN on specific Ethernet switches. VoIP Hopper does this by mimicking the behaviour of an IP Phone in Cisco IP phone environments. VoIP Hopper can be used to spoof CDP (as an IP Phone) and automatically creates a new Ethernet device based on the discovered Voice VLAN Identifier.

Wireshark is a powerful network protocol analyser. It runs on both Windows and Linux.

Cain & Abel is a powerful sniffing tool.

7. A sample attack on SIP: man-in-the-middle

In this section we present a sample attack on an Internet telephony application. Concretely, we show how to become a man-in-the-middle (man-in-the-middle attack) in the SIP VoIP system. The setting considered is as follows (cf Figure 5). Alice and Bob want to make a phone call. The attacker's aim is to become the man-in-the-middle in this connection, that is, all traffic does not ow directly between Alice and Bob, but indirectly via the man-in-the-middle. The attacker can therefore not only listen to the conversation and simply forward the data, but may also decide to cut important words, or replay some old sentences. For example, after having followed the conversation for some time, the attacker may have recorded a sufficiently large number of words and phrases (e.g., "yes", "no", numbers, etc.) in order to tell Bob—using Alice's voice—to pay a certain amount of money on the attacker's bank account. As SIP does not explicitly require encryption, such an attack can be achieved using ARP spoofing when all three clients are situated in the same local area network.

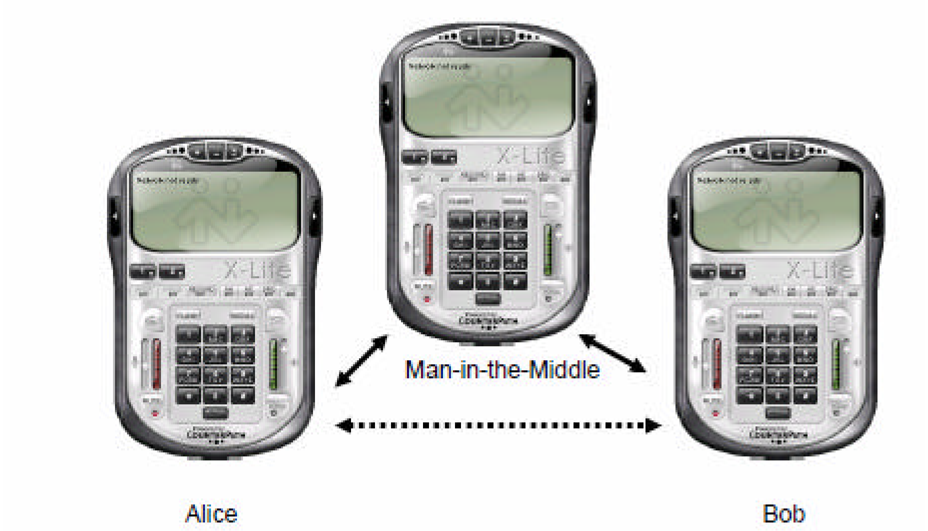


Figure 5: Setting of Man-in-the-Middle Attack. All clients are assumed to be in the same local network.

The attack works as follows. Most machines in the Internet have a hardware or MAC address (Ethernet address). However, this address is typically only visible within a local network; for global, Internet wide addressing and routing, IP addresses are used. The SIP telephony client also stores such an IP address for each contact, that is, Alice stores Bob's IP address 192.168.0.3, and Bob stores Alice's IP address 192.168.0.2. In our experiment, the attacker's IP address is 192.168.0.1. However, delivering packets to the hosts in a local network requires MAC addresses. Therefore, whenever Alice wants to communicate with Bob, she has to find out the MAC address which corresponds to Bob's IP address.

This mapping from IP addresses to MAC addresses is done by the so-called Address Resolution Protocol (ARP). Basically, the ARP protocol is a distributed algorithm in which the query "Who has IP address X?" is broadcast in the local network, and the corresponding client with IP address X responds with the message "Hello, I have IP address X! My MAC address is Y!". This protocol can be cheated, and the attacker can become the man in the middle. In order to do so, the attacker applies ARP spoofing: When Alice broadcasts a query for Bob's hardware address, the attacker answers with his own MAC address, and similarly when Bob looks for Alice' IP address. As a consequence, both Alice and Bob bind the attacker's MAC address to the IP address of Bob and Alice, respectively.

For ARP spoofing, we have used the tool Cain & Abel v.2.9.2. The tool is shown in Figure 6. Using the network sniffer, it is possible to explore the current IP and MAC addresses in the network. The result is shown in Figure 7: The attacker has found that Alice (IP address 192.168.0.2) has MAC address 00:0d:60:b0:5f:43, and Bob (IP address 192.168.0.3) has

00:0d:60:79:cb:13. The attacker can then execute the ARP spoofing/poisoning in order to become the man in the middle, see Figure 8: Cain & Abel then applies techniques to modify the ARP cache of Alice and Bob in order to become the man in the middle.

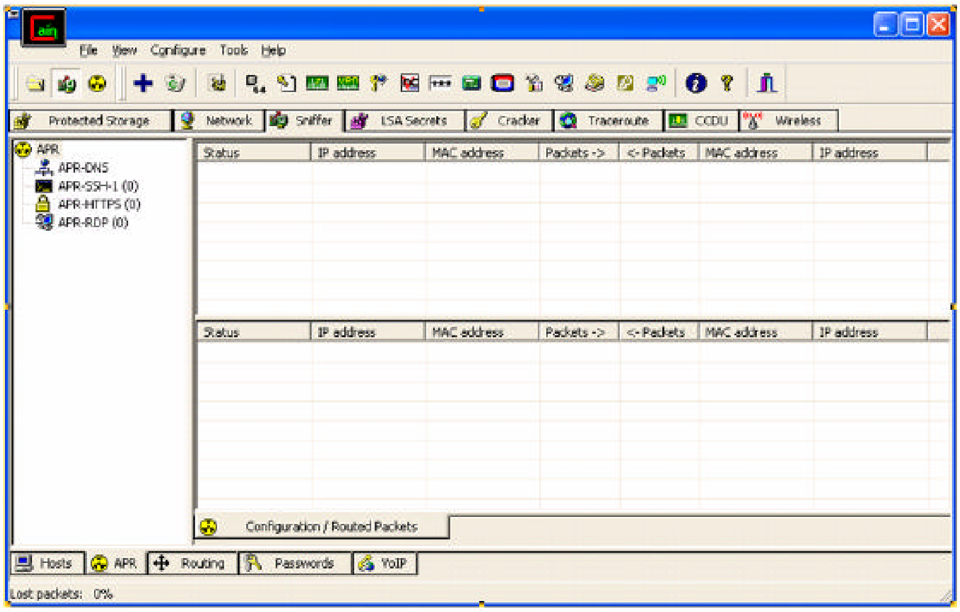
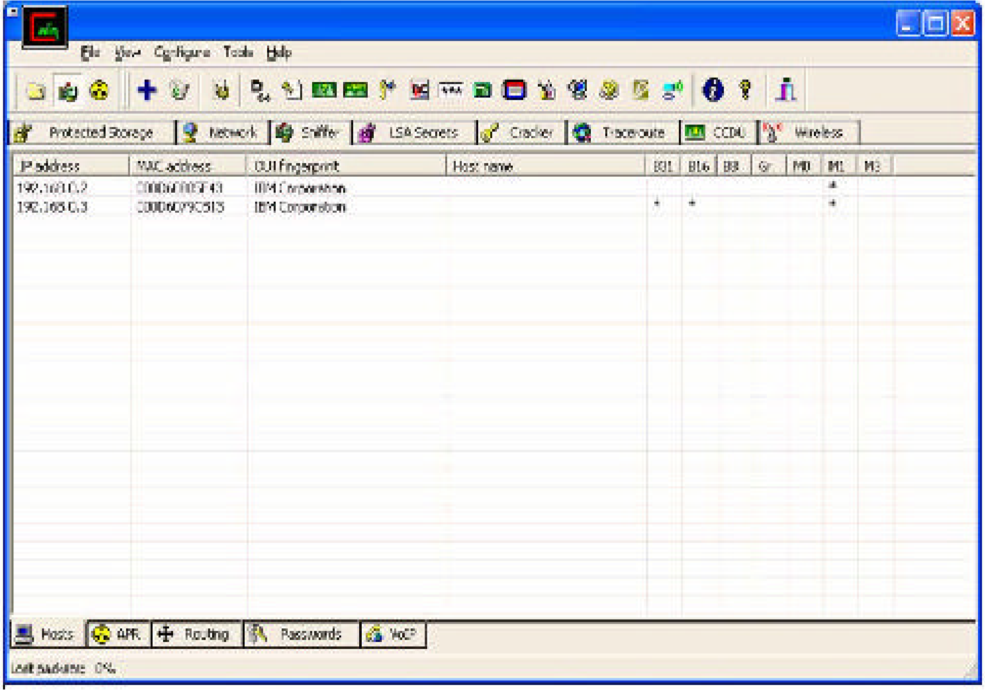


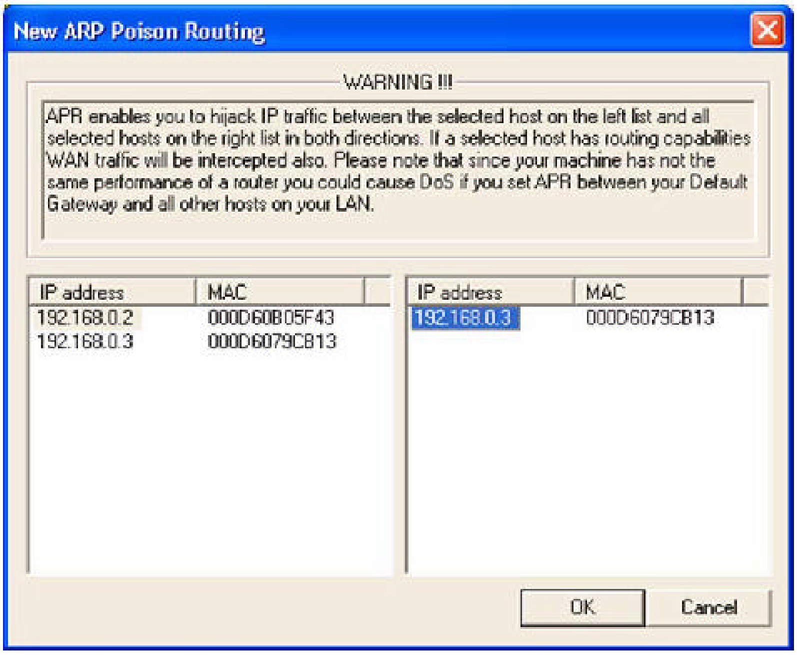
Figure 6: Cain & Abel.

Consequently, the traffic is routed through the attacker. We have used Cain & Abel to record the conversation on the attacker's machine. The following two figures (Figures 9 and 10) show the state of Bob's machine before and after the ARP spoofing. While before the ARP spoofing took place, Bob correctly believes that Alice has the MAC address 00:0d:60:b0:5f:43, he wrongfully assumes that the MAC address is 00:08:02:e5:7e:f5 after the attack



IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
192.168.0.2	000D60B05F43	IBM Corporation							*	
192.168.0.3	000D6079CB13	IBM Corporation		*	*				*	

Figure 7: Exploring Ip and MAC addresses with Cain & Abel



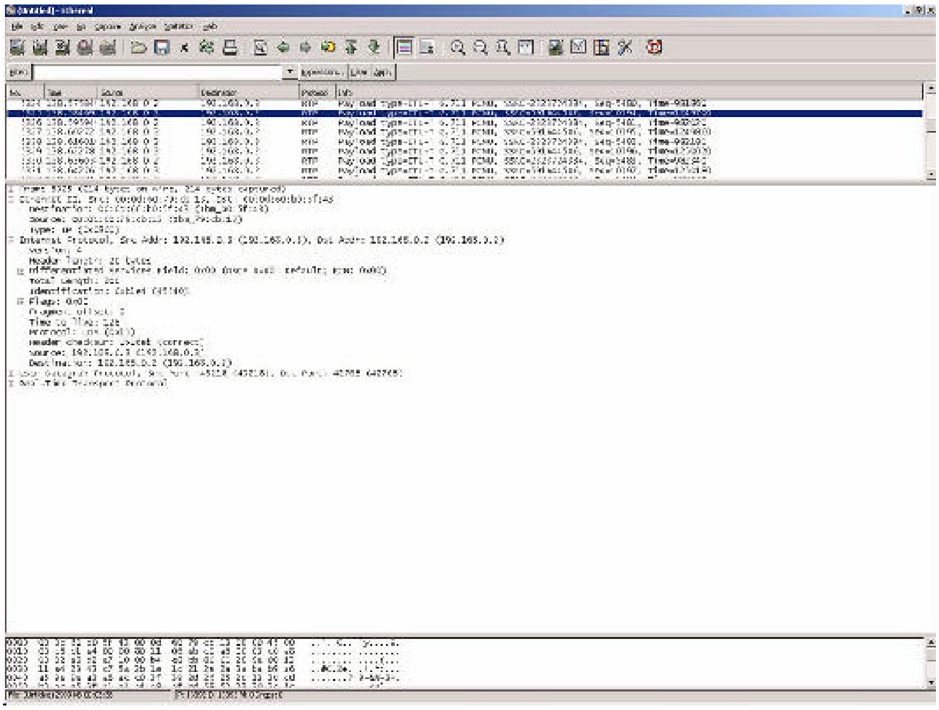
WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted also. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC
192.168.0.2	000D60B05F43
192.168.0.3	000D6079CB13

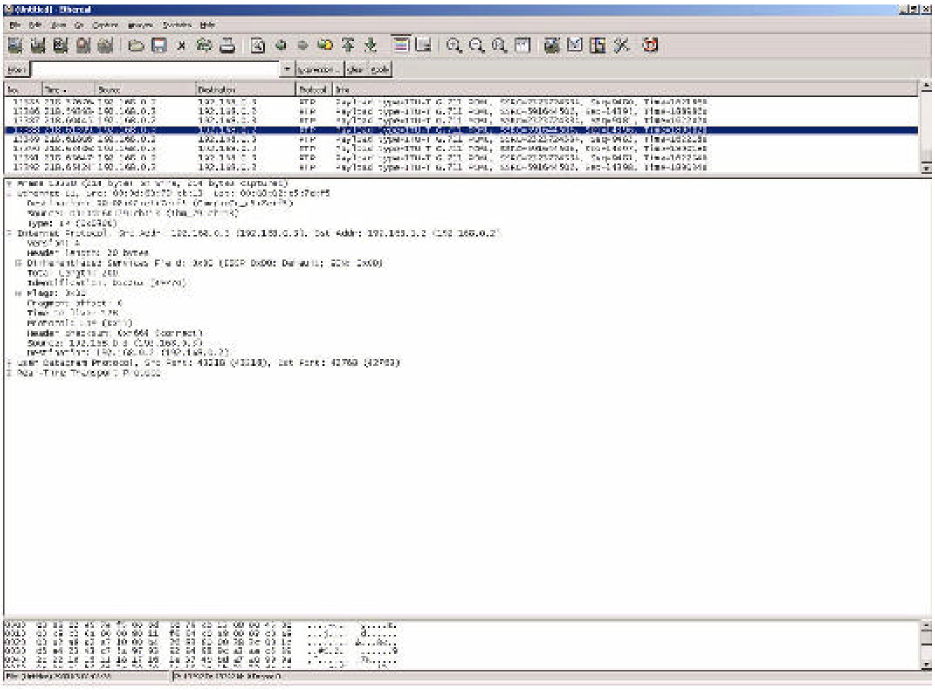
IP address	MAC
192.168.0.3	000D6079CB13

Figure 8: ARP Spoofing/Poisoning.



```
Internet Protocol, Src Addr: 192.168.0.3 (192.168.0.3), Dst Addr: 192.168.0.2 (192.168.0.2)
    Version: 4
    Header length: 20 bytes
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Source: 192.168.0.3 (192.168.0.3)
    Destination: 192.168.0.2 (192.168.0.2)
Real-Time Transport Protocol
```

Figure 9: Ethereal Network Sniffing Tool at Bob: Before ARP Spoofing.



```
No.    Time        Source        Destination   Protocol  Info
17386  218.59...   192.168.0.3   192.168.0.2   RTP       Payload type=ITU-T G.711 PCMU, SSRC=591649502, Seq=14391, Time=[illegible]
17392  218.65...   192.168.0.3   192.168.0.2   RTP       Payload type=ITU-T G.711 PCMU, SSRC=591649502, Seq=14398, Time=[illegible]

Frame [illegible] (214 bytes on wire, 214 bytes captured)
Ethernet II, Src: [illegible], Dst: [illegible]
Internet Protocol, Src Addr: 192.168.0.3 (192.168.0.3), Dst Addr: 192.168.0.2 (192.168.0.2)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 200
    Flags: 0x00
    Fragment offset: 0
    Header checksum: [illegible] (correct)
    Source: 192.168.0.3 (192.168.0.3)
    Destination: 192.168.0.2 (192.168.0.2)
User Datagram Protocol, Src Port: [illegible], Dst Port: [illegible]
Real-Time Transport Protocol
```

Figure 10: Ethereal Network Sniffing Tool at Bob: After ARP Spoofing.

Conclusions

The VoIP world is evolving rapidly and security issues are well discussed among researchers. However, the well-known systems (Skype, GoogleTalk, Yahoo, MSN, etc.) are closed-group systems, where a user has to be registered to interact with any other user.

Efforts to interconnect these systems are currently made. This could lead to a world-wide system, where new threats such as SPIT may emerge. Yet another world-wide system may appear if ISPs are willing to provide basic VoIP functionalities for hosted domain.

This document has surveyed security issues related to internet telephony. Today's state-of-the-art VoIP applications have promising properties, and it can be expected that VoIP will more and more replace the traditional telephone system. It also seems that many products are aware of security threats and incorporate countermeasures. For instance, while in traditional telephone systems, voice was transmitted plainly, Skype uses modern cryptography to hide the contents. VoIP security is a hot topic in literature as well. In 2006 alone, two books have been published.

As of today, we cannot rely only on a VoIP only solution to provide all the standard telephony functionalities we need, in particular because there is no world-wide VoIP coverage. An access to the "old" telephony network (PSTN) is still a must. Hybrid solutions exist and already offer enough security and flexibility to be deployed. In such a solution, the voice traffic is ideally routed on a different VLAN than the data traffic. Moreover, IPSec should be deployed and server components should only accept requests sent with TLS (and MTLS between two server components). To prevent unwanted communication costs, the PSTN Gateway should only be accessible via an authenticated server (MTLS) and dialing authorizations should be enforced. To prevent eavesdropping, SRTP should be used to secure the voice streams. Such a solution will prevent SPIT and external threats. DoS attacks from the inside are possible, but the threat already exists on the data network nowadays. Traffic monitoring should be used to stop such attacks as soon as possible.

There are still several security problems, and many VoIP hacking tools can be found online, e.g., on http://www.hackingvoip.com/sec tools.html. On the other hand, there are products such as Skype which are not open source, making it hard to find and repair security aws. We believe that there are inherent trade-offs, for example related to SPIT.

More intensive filtering may threaten the availability of communication partners. It has also been pointed out that many VoIP components use Web servers for configuration, and that the corresponding development tools often lack security features. Finally, the fact that machines today are increasingly well protected by firewalls, demilitarized (DMZs), etc., complicates many aspects of VoIP.

References

1. www.securityfocus.com/
2. csrc.nist.gov/pub lications/
3. www.ciscopress.com/bookstore/product.asp
4. www.hackingvoip.com
5. www.cs.utexas.edu/shmat/
6. www.wikipedia.com
7. www.baumann.info/public/
8. academypublisher.com/jsw/vol02/no02/
9. www.infosec.gov.hk/english/technical
10. www.ccip.govt.nz/newsroom/information-notes
11. www.cs.columbia.edu
12. Rainer Baumann, Stephane Cavin, Stefan Schmid - *Voice Over IP - Security and SPIT* , University of Berne
13. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries - *Security Considerations for Voice Over IP Systems* ,NIST 800-58
14. Peter Ingram – *Introduction in VoIP,* PITCOM
15. Jane Dudman – *Voice over IP:what it is, why people want it, and where it is going,* JISC Technology and Standards Watch.

MOBILE DEVICE SECURITY

2nd LT Nicolaie BOANGIU

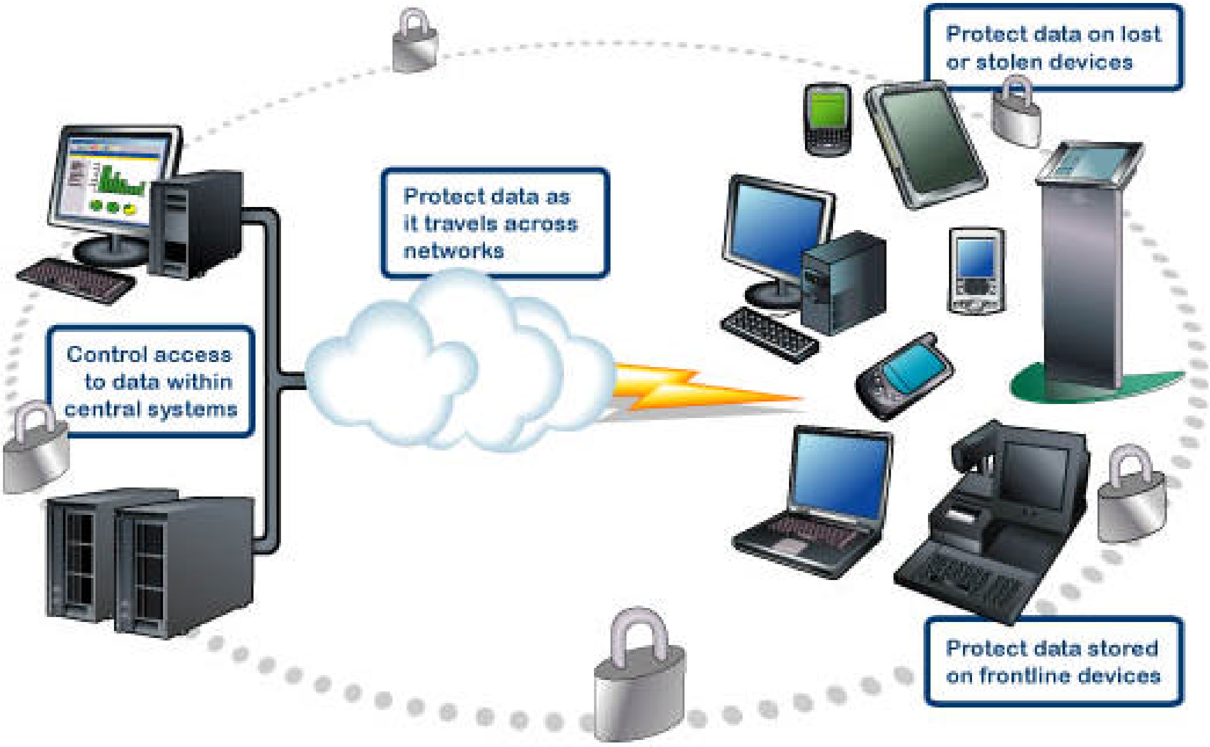
UM 01812/C Cîrcea

Introduction

Smart phones, PDA phones and other handheld mobile devices can make our lives easier, making it possible for us to keep in touch with the office, family and colleagues regardless of where we are. With fast 3G networks and wi-fi capabilities, we can stay connected and check our email, access the Web and more, without having to carry around laptop computers. In fact, today's handhelds are as powerful as the desktop computers of a few years ago. Almost all Windows Mobile phone is a full fledged Windows computer. They have at least 400 MHz processor, 64 MB of RAM and 128 MB of ROM, and 4 GB of storage on a mini SDHC card.

With all this computing power literally in the palms of our hands, many of us spend a lot of time, especially when traveling, working from our phones. We can use them to create, edit and store Word documents and spreadsheets, read PDFs and access other company files. But this poses a greater security risk than ever before. Not only may we be exchanging email messages that contain sensitive info, but we may also have confidential documents on the devices, as well as passwords for logging onto the company network or Web sites.

In some special environments mobile devices can be used to monitor or manage a sensitive process. It is a realistic view to have a military unit with digital maps, real time updated with the own missions and the latest information about enemies positions.


Protect data on lost or stolen devices
Protect data as it travels across networks
Control access to data within central systems
Protect data stored on frontline devices

But let's define mobile devices and their users, because behind those terms it is hiding a lot:

Mobile Devices: these include, but are not limited to, Portable Digital Assistants (PDAs), notebook computers, Tablet PCs, Palm Pilots, Microsoft Pocket PCs, RIM blackberrys, MP3 players, text pagers, smart phones, compact discs, DVD discs, memory sticks, USB drives, floppy discs and other similar devices**.**

User - Anyone with authorized access to business information systems, including permanent and temporary employees or third-party personnel such as temporaries, contractors, consultants, and other parties with valid access accounts.[25]

Modern digital environment is very complex, with a lot of devices and communication technologies. In such environment, security became a very complex mechanism because the threats are very various. The picture bellow shows a modern IT environment and the needs for protection.

1. Mobile devices in real world

1.1. Where mobile devices are used

It comes as no surprise that mobile devices are gaining wider acceptance and usage with each passing day. Small and convenient, they can easily be carried between work and home and used efficiently at each. But it is exactly the ease with which they are transported which makes them particularly liable to both loss and theft – thus becoming the source of a confidential information leak with major consequences for companies or individuals alike.

In a survey conducted between February 1st and March 1st, 2009, 1500 mobile device users participated in the survey, which was conducted on the websites of Zoom.CNews and InfoWatch. Percentages are rounded off to the nearest tenth of a percent. Where total percentages exceed 100%, this is due to multiple answers to a question being allowed.

Fig. 1 shows what mobile devices are in use. The laptop is the most widely used (47.3%). Next come the Smartphone (45.8%) and the pocket computer (26.6%). A significant proportion of respondents (30.4%) use other devices.

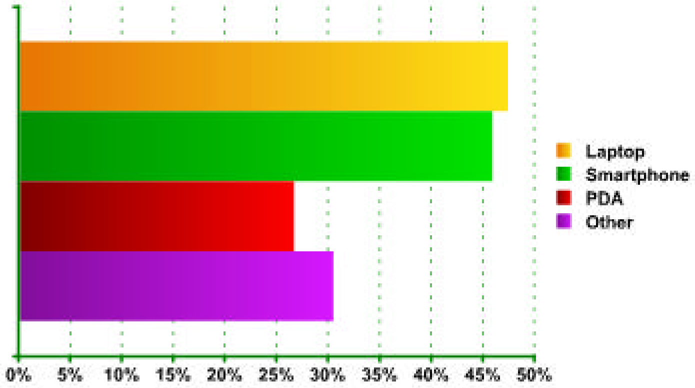


Fig. 1. Types of mobile device

The numbers here demonstrate the high take-up of mobile devices with many people having more than one. With each new device, the chances of an information leak naturally increase.

Fig. 2 demonstrates these tendencies. Here we can see that 8.5% of users have three times more likelihood of losing data than the 60.6% percent who have only one device.

[25] http://bccs.illinois.gov/pdf/Mobile-Device-Security-Policy.pdf

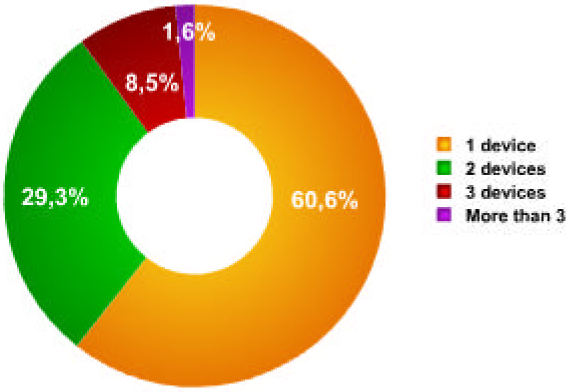


Fig. 2. Number of mobile devices

Fig. 3 shows the most common areas where mobile devices are used. The most popular usages are to store contact lists (friends / colleagues) and to check email (sending and reading). These options were chosen by 77.7% and 70.8% of respondents, respectively. In third place was Internet usage (63.8%), followed by diary use (33.5%) and online shopping (23.4%).

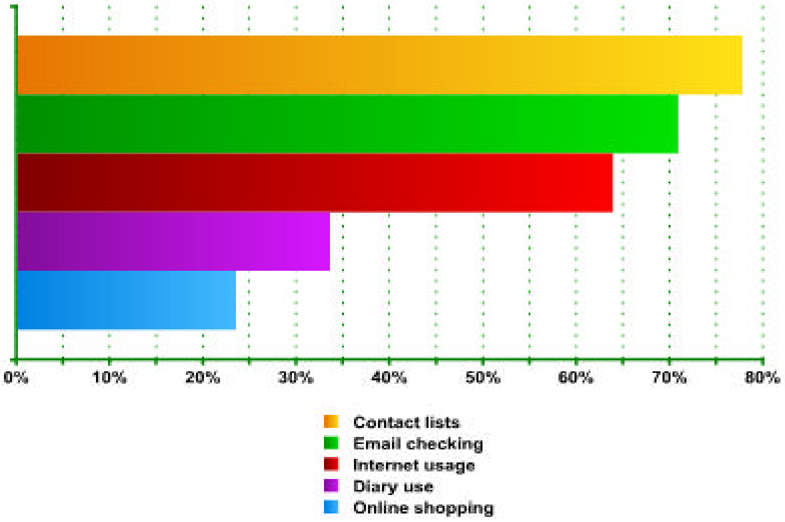


Fig. 3. Mobile device usage

By understanding the uses to which respondents put their mobile devices, it is possible to understand what kind of data they keep on them. Of primary importance is the fact that 77.8% of users keep records of their personal friends and colleagues on their portable devices. Such data is kept in the address book or in a contacts holder. A further 70.8% of respondents keep their personal and/or their business correspondence on their mobile device, along with access details to email accounts. The leakage of such data can not only lead to unwanted dissemination of private details, but also to blackmail, identity theft, industrial espionage, etc.

A less hazardous use of mobile devices is Internet usage. In the event of either loss or theft of the device, the most the thief can get his hands on is the history of web pages visited. However, if the user also makes purchases online – as 23.4% of respondents do – then such a leak can lead to direct financial losses since the browser often cache credit card information, user login and passwords to online shops as well as other details. All these items are highly valuable and interesting to criminals.

Lastly, diary use (33.5%) indicates that the mobile device user is likely a corporate employee. He has a packed schedule and uses the diary to plan his time. This data is also confidential or, at the very least, private. Therefore, its loss or theft can be a blow not only to the user, but also to the employer.

1.2. Top 10 most expensive device information's leaks[26]

Nr.	Incident	Date	Victims	Potential Cost
1	Leak of US military personnel and veterans' data	May 2006	28.7 million	$45 billion
2	Laptop stolen from Nationwide Building Society, UK	Aug 2006	11 million	$1.5 billion
3	A portable hard drive with company data stolen by insider at Dai Nippon Printing	Jul 2006	8.64 million	$1.2 billion
4	A laptop stolen from the US war veterans' medical centre in Birmingham with doctors' and patients' personal data	Jan 2007	1.8 million	$367 million
5	A mobile computer stolen from Computer Services (ACS) with personal client data	Oct 2006	1.4 million	$320 million
6	Laptop lost by subcontractor for Texas Guaranteed with TG's client data	May 2006	1.3 million	$237 million
7	Laptop stolen from a Boeing employee's car	Nov 2006	382,000	$147 million
8	Laptop stolen from CS Stars with names, addresses and Social Security numbers of New York workers	Jul 2006	540,000	$84 million
9	Laptop with personal data stolen from an employee of the accountancy firm Hancock Askew	Oct 2006	401,000	$73 million
10	Investigation at the Vassar Brothers medical centre found the loss of a laptop and backup disk with patient data	Jan 2007	257,800	$47 million

1.3. Sensitive data held on mobile devices

The next part of the survey regarded the data held on portable devices. It found that only 29.3% of respondents did not keep sensitive data on their mobile computers. Fig. 4 shows that the majority of users (68.1%) keep personal data on their mobile devices. And corporate and confidential documents as well as intellectual property are held by 16.5% and 14.9% of respondents. A mere 12.2% of respondents use their mobile devices to hold private client or partner data.

[26] http://www.viruslist.com/en/analysis

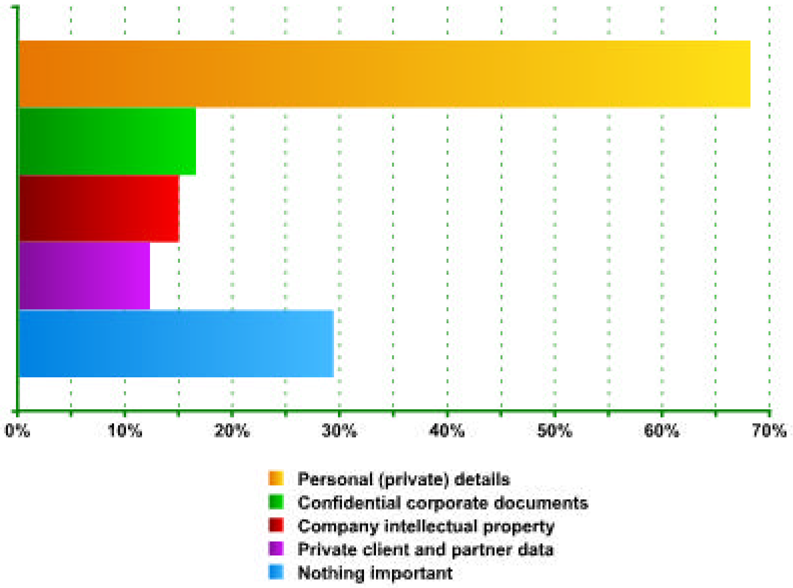


Fig. 4. Confidential information on mobile devices

Thus, the overwhelming majority (70.7%) of respondents keep some kind of confidential information on their mobile device. But how well is this data protected against leakage?

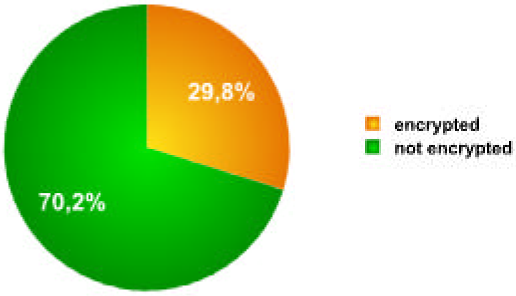


Fig. 5. Is data protected?

We know that only 29.8% of respondents use data encryption (see fig. 5). If we transpose this figure to mobile device users who keep confidential corporate documents, intellectual property or private client or partner data on their drives, then only 40.7% of them are using encryption. This means that more than half the respondents who keep valuable and secret data on their mobile devices do not protect their data at all. They are vulnerable to data leakage in the event of loss or theft of their devices.

We can also say that part of the reason for such an attitude is the fact that 83% of respondents had never lost a mobile device. However, 78.1% of those users who had been the victims of theft – or lost device – containing confidential data, admitted that they still did not use encryption. This indicates that we have a weak culture of information security and the main obstacle is laziness both on the part of individuals and companies.

2. MOBILE SECURITY THREATS

2.1. Actual IT context

A new report shows that IT managers are reluctant to take responsibility for managing mobile devices that are increasingly being used with enterprise applications. Against a backdrop of more employees bringing and using their own mobile devices in the office, analysts from Datamonitor are recommending that enterprise applications consider supporting a limited selection of devices rather than attempting to enforce an outright ban. This is especially pertinent when one considers that few employers want the hassle of one device for personal use, with a company-issued device for work. As it is, IT managers need to begin implementing mobile device policies to ensure that devices are properly secured against data breaches when they are lost or stolen.

Some of the specific security threats associated with mobile devices include:

- Loss or theft of the mobile device, resulting in exposure of data
- Interception of data that passes over the wi-fi or 3G network
- Capture of data via Bluetooth connections
- Mobile viruses (including email viruses)

As with laptops, mobile devices can present unique security threats, especially when employees are allowed to connect their personally owned equipment to the company network. A July 2008 survey showed that 89% of respondents said they use either personally owned or corporate issued smart phones to access corporate email and other company information, and over half of those surveyed said companies that do not issue smart phones should allow employees to store and access company information using their personal smart phones.

This can result in a nightmare for the IT department, if you must implement security measures for many different types of hardware and software. If no restrictions are in place, you may find yourself trying to provide secure access to various versions of Windows Mobile, RIM Blackberries, Apple iPhones, Symbian devices, Palm devices and Linux-based devices such as Google's Android phones that are expected to be available in the near future (the HTC Dream is expected to be released this fall).

2.2. The most significant threats for mobile device security

There are a good number of issues within mobile device security that require consideration which take on new relevance when the device of choice isn't a PC, but rather a handheld device. Today's smartphones really are PCs, with operating systems, storage, applications, and wireless access to enterprise networks. IT is actually replacing some of its users' PCs with a smartphone equipped with wireless broadband, a desktop-class browser, the ability to read and even edit office-suite files, and lots of storage for any kind of data. Getting the security element right the first time is more important than ever in this mobile environment.

Let's consider how mobile security threats figure in the world of smartphones by looking at a few common threats:

Mobile malware and viruses: Given the complexity of modern mobile operating environments, the same criminal apps that we've seen for many years on PCs can now plague handsets. Fortunately (so to speak), the socially challenged techno-nerds that produce this nonsense have seen fit to focus mostly on Windows. But as mobile device platforms become more common, this threat is clearly real. And it's not just a question of platform stability – the real issue for the enterprise is theft of sensitive information. In this era of Sarbanes-Oxley, the challenge here should give pause to everyone, from users in the field to the CEO.

Eavesdropping: Carrier-based wireless networks have good (but not, of course, perfect -- there is no such thing) link-level security, but, as is the case with PCs, end-to-end, upper-layer security is required for sensitive data. This means that data that an enterprise wants to protect should appear in the clear only to authorized users. Given that data on smartphones is seldom encrypted, and few actually secure (authenticate) access to their devices, this is another threat that needs to be taken very seriously.

Unauthorized access: This isn't a problem unique to wireless, of course, but as an ever-greater number of enterprise users make access from the road their primary means of staying connected, careful attention needs to be paid to AAA – authentication, authorization, and accounting. But setting up this capability on smartphones can be daunting, and two-factor authentication, which we always recommend, is not widely available today. And yes, even firewalls and intrusion-prevention techniques are important on today's smartphones.

Physical security: Finally, while many notebook computers are indeed lost or stolen every year, it's a lot easier to simply misplace a mobile device. Just for starters, hundreds of thousands of these have been left in the back of taxis around the world. A few unauthorized offshore phone calls could really irritate your CFO, to say nothing of the potential for the compromise of corporate secrets.

And all of these are further complicated by the double-duty personal/business use that is typical of today's smartphones. More often than not, in fact, enterprises allow -- perhaps most often by not explicitly prohibiting -- the use of personal devices for corporate functions. Since a personal smartphone isn't managed by the enterprise, it is clearly an invitation to trouble. As the saying goes, you can't manage what you can't secure, and you can't secure what you can't manage.

3. HOW TO SECURE MOBILE SOLUTIONS

3.1. Secure mobile devices

In the second chapter of this work paper on mobile device security, we looked at the key mobile security threats plaguing the highly mobile world and discovered, not surprisingly, that these are pretty much the same as we find in computing in general. The implication is clear -- you need strategies and tools that are remarkably similar to those you've been using on desktop and notebook PCs for some time. Let's review the key requirements for building your mobile device security toolkit and examine the solutions available.

Viruses and malware: Antivirus software for the mobile device operating system (OS) is available from a few vendors today, but it's hard to recommend. Viruses aimed at the mobile OS are rare, and most mobile users take the "Macintosh" approach: "Hey, I've got a Mac, viruses are aimed at PCs, so the risk is low." That is in fact currently the case, but it's still best to educate your users in the basics here -- don't visit arbitrary websites, don't download anything that's not authorized by IT, and use mobile device management capabilities from your carrier or implemented within the enterprise to verify and control the configuration of your mobile devices.

Encryption: Carrier networks have good encryption of the airlink in every case, but the rest of the value chain between client and enterprise server remains open unless explicitly managed. Always use a VPN connection when dealing with sensitive data.

Authentication and authorization: These requirements fit in nicely with the RADIUS or similar solution that you're already using (right?) for remote access. You might also look into obtaining -- or enabling (if your mobile OS is already equipped) -- firewall functionality, just as you already do on your laptops and notebooks.

Physical security: Mobile devices will get lost; that's why authentication and encryption are so important. Mobile device management can handle the "phone home" or "remote wipe", depending upon your preference. But plan for device loss; it will happen much more often than you think it will.

3.2. Secure mobile solutions

Tying IT all together -- the key to any successful networking (or IT) operation is management. Mobile device management is rapidly gaining awareness and popularity, with a good number of vendors now providing solutions for both carriers and enterprises, and there are more on the way. The key is to extend operational, real-time network management out to the very edge of the network, even if that edge is a mobile device being used.

Bellow we have an example of comprehensive security solution for mobile environment:

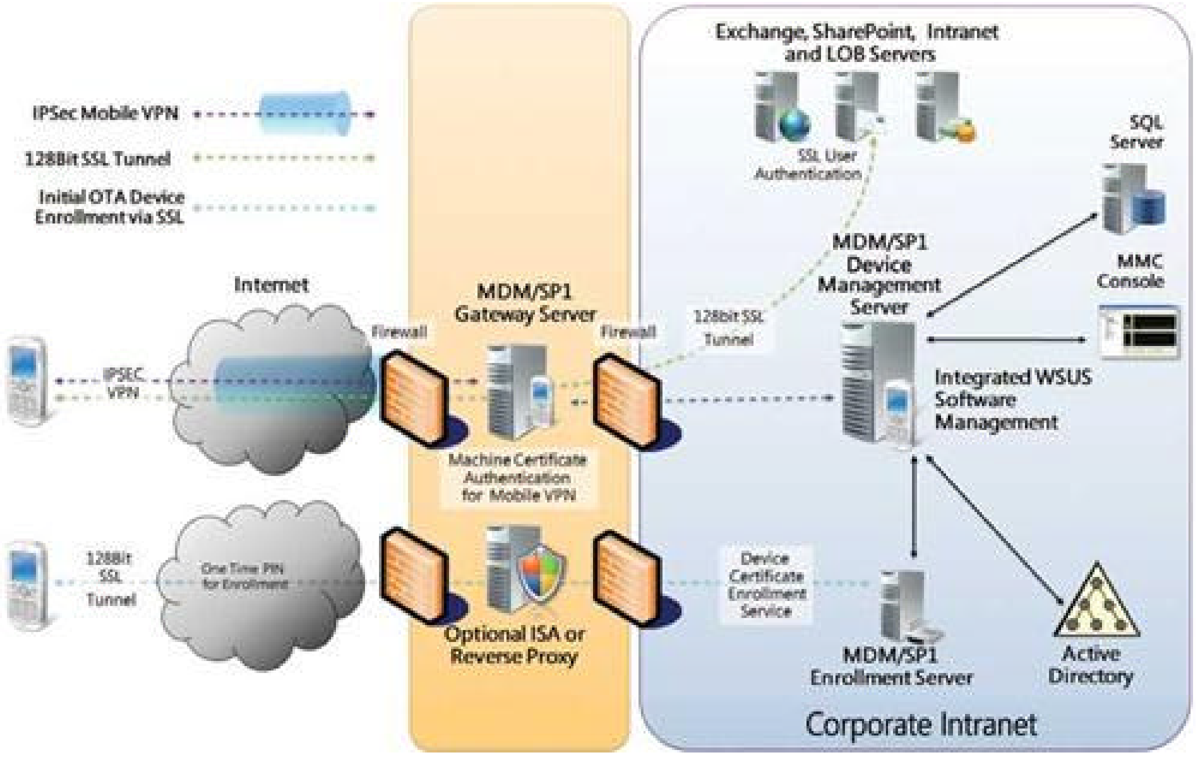

Exchange, SharePoint, Intranet and LOB Servers
SSL User Authentication
SQL Server
IPSec Mobile VPN
128Bit SSL Tunnel
Initial OTA Device Enrollment via SSL
MDM/SP1 Device Management Server
MMC Console
Internet
MDM/SP1 Gateway Server
Firewall
Firewall
128bit SSL Tunnel
IPSEC VPN
Integrated WSUS Software Management
Machine Certificate Authentication for Mobile VPN
128Bit SSL Tunnel
One Time PIN for Enrollment
Device Certificate Enrollment Service
Optional ISA or Reverse Proxy
MDM/SP1 Enrollment Server
Active Directory
Corporate Intranet

Fig. 6. Mobile device management

Additionally, for an enterprise device security management are necessary supplementary functionalities. For example, using Microsoft products, but not only, we can use supplementary mechanism to secure our devices.

Digital certificates: Windows Mobile can use digital certificates for network authentication, whereby the Exchange server checks the mobile device's root certificate in order to create an SSL connection so that communications between the server and device are encrypted.

Remote wipe: You can perform a remote wipe of the Windows Mobile device via Exchange synchronization or Outlook Web Access (OWA). All user data, keys and passwords and configuration settings are overwritten.

Storage card protection: With Windows Mobile, you can encrypt the data on the storage card. When you do so, it can be read only on the device that encrypted it. This can be done via Exchange Server 2007 policies so that it can be controlled by the administrator, not left up to the user. Exchange Server 2007 can also perform a remote wipe of the storage card.

Propagation of policies: Enterprise policies can be delivered to Windows Mobile devices when they synchronize with the Exchange server. Devices that do not comply with policies will not be allowed to synchronize with Exchange.

With all these options and requirements, where should we start in building the right mobile security strategy and arsenal for our organization? Believe it or not, the place to begin is with the carrier. Carriers are actually strongly motivated to provide the most reliable services to their customers and of course to maintain the integrity of their own networks. Many have implemented anti-spam technologies, for example, at least in part to cut traffic loads on the precious bandwidth they provision. Many are also implementing mobile device management capabilities, provided as a value-added service to their customers. No carrier, of course, will have all of the pieces you need, and it is recommended that file and network encryption and authentication be handled by the enterprise. It is a long way to go in terms of ease of use, but the pieces are indeed now falling into place. Within just a very few years, the mobile security solutions required by even the most demanding applications will be commonplace, and very cost-effective in the bargain.

Conclusions

The proliferation of mobile devices in today’s corporate environment makes life more convenient for users, and more complex for IT administrators who are trying to protect their networks from the threats that can be introduced when unmanaged user-owned devices connect to it. By establishing and enforcing mobile device usage policies and carefully considering what types of devices will be allowed, and by using the security technologies built into mobile operating systems devices and the features incorporated in server side solutions, you can provide accessibility without compromising security.

References

1. InfoWatch (http://www.infowatch.com/)
2. Mobile IT, IT Wireless, Mobile Enterprise, Enterprise Wireless, Wireless Enterprise Solution - FierceMobileIT (http://www.fiercemobileit.com/)
3. VirusList.com (http://www.viruslist.com/)
4. http://www.shinder.net/

SOCIAL ENGINEERING

2^{nd} LT Valentin BURTAN

UM 02415 Bucuresti

Introduction

Intruders and hackers are on the lookout for ways to gain access to valuable resources such as computer systems or corporate or personal information that can be used by them maliciously or for personal gain. Sometimes they get their chance when there are genuine gaps in the security that they can breach. Often times, in fact more often than one can guess, they get through because of human behaviors such as trust – when people are too trusting of others, or ignorance – people who are ignorant about the consequences of being careless with information. Social Engineering uses human error or weakness to gain access to any system despite the layers of defensive security controls that have been implemented via software or hardware. The ultimate security wall is the human being, and if that person is duped, the gates are wide open for the intruder to take control.

1. General considerations

1.1. What is social engineering?

Wikipedia defines social engineering as "the art of manipulating people into performing actions or divulging confidential information" (Wikipedia). Note that not all information gathered by a social engineer may be classified as confidential, but can still assist them in their attack. For example, a simple question like "What's your superiors name?" may bring a social engineer a step closer to stealing your superiors identity. Social engineering is most commonly referred to when talking about computer system and network security. In fact, most social engineers are also proficient at using computers (which isn't a requirement of being a social engineer) as well as being a skilled social engineer which can be a very lethal combination. Social engineering is derived because of a human characteristic to trust other people. People have a tendency to sympathize with anyone that claims to be in trouble or believing anyone who comes around claiming to be a trusted person without officially checking their credentials first. A social engineer knows this and anticipates this. When a social engineer attempts an attack on your company, a person may ask a couple of questions off the top of their head that they believe will confirm this persons identity, but a social engineer has spent ample time anticipating your every question and move and is ready with a reply on hand.

Are you and your company prepared?

This type of attack can be prevented by proper training to ALL associates of a company. A company has a duty to every employee to inform and prepare them for social engineering attacks. If it fails to do so, it will become a victim of such attacks.

1.2. Impact of Social Engineering on the organization

Information Security is essential for any organization 'to continue to be in businesses. If information security is not given priority, especially in the current environment with the threat of terrorism looming in the background every day, even a small gap in security can bring an organization down.

The financial cost could be punitive to the organization and to the individual. So much so, that insurers are now beginning to cover losses arising out some kinds of security breaches.

Cyber attacks cost U.S. companies $266 million last year - more than double the average annual losses for the previous three years, according to a report released by the San Francisco-based Computer Security Institute (CSI) and the San Francisco FBI Computer Intrusion Squad. The study found that 90% of 273 respondents detected some form of security breach in the past year. But this is probably an underreported figure. Less than half the companies in one survey were willing or able to quantify the loss.

There is also the cost of loss of reputation and goodwill, which can erode a company's base in the long run. For example, a malicious individual can get access to credit card information that an online vendor obtains from customers. Once the customers find out that their credit information has been compromised, they will not want to do any more business with that vendor, as they would consider that site to be insecure. Or they could initiate lawsuits against the company that will lower the reputation of the company and turn away clientele.

Something similar happened with PayPal, the online payment company. PayPal customers received email that asked the account holder to re-enter their credit card data. PayPal purportedly had had some trouble with one of its computer systems. The e-mails looked like the genuine article, with PayPal logos and typefaces, even the security lock symbols and a link that resembled the official PayPal link. When accountholders provided the information, the hacker was able to harvest it.

Security experts concur when it comes to identifying where security violations

can occur, and who causes them. Over time, the experts have come to the conclusion that despite the impression of the hacker being an outsider wanting to get 'in', the majority of violations are caused by either disgruntled employees or non-employees who have legitimate system access because of their job in the organization. According the FBI nearly 80% of all attacks are caused by such authorized users.

In most cases, once the individual is wearing the cloak of respectability, others do not automatically view their activity with suspicion: every honest person assumes that others are similarly well intentioned. The intruder also takes advantage of the natural tendency to relax one's guard when things appear to be secure.

In short, companies spend billions of dollars every year in improving hardware and software in order to block malicious attacks. But all this is of no use if end users do not follow good security practices. From an interview of Kevin Mitnick, an infamous hacker in the 1980s and 1990s, with the BBC News Online :

"The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you."

What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time organizations overlook that human element.

2. The cycle of a social engineering attack

Is there a common pattern associated with a Social Engineering attack? The answer is 'Yes'. As reported by Gartner in a paper titled *'Management Update: How Businesses Can Defend against Social Engineering Attacks*' published on March 16, 2005, any criminal act has a common pattern. Such a pattern is evident with Social Engineering, and it is both recognizable and preventable. For the purpose of this paper, this pattern will be known as 'The Cycle'. Figure 1 illustrates 'The Cycle', which consists of four phases (Information Gathering, Relationship Development, Exploitation and Execution). Each Social Engineering attack is unique, with the possibility that it might involve multiple phases/cycles and/or may even incorporate the use of other more traditional attack techniques to achieve the desired end result.

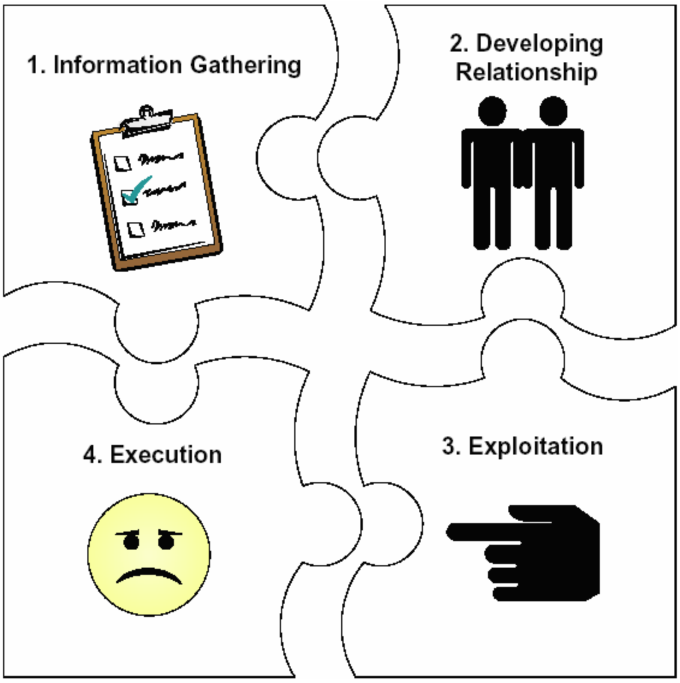


Figure 1: The Cycle

1. **Information Gathering:** a variety of techniques can be used by an aggressor to gather information about the target(s). Once gathered, this information can then be used to build a relationship with either the target or someone important to the success of the attack. Information that might be gathered includes, but is not limited to:

- a phone list;
- birth dates;
- an organization's organizational chart.

2. **Developing Relationship:** an aggressor may freely exploit the willingness of a target to be trusting in order to develop rapport with them. While developing this relationship, the aggressor will position himself into a position of trust which he will then exploit.

3. **Exploitation:** the target may then be manipulated by the 'trusted' aggressor to reveal information (e.g. passwords) or perform an action (e.g. creating an account or reversing telephone charges) that would not normally occur. This action could be the end of the attack or the beginning of the next stage.

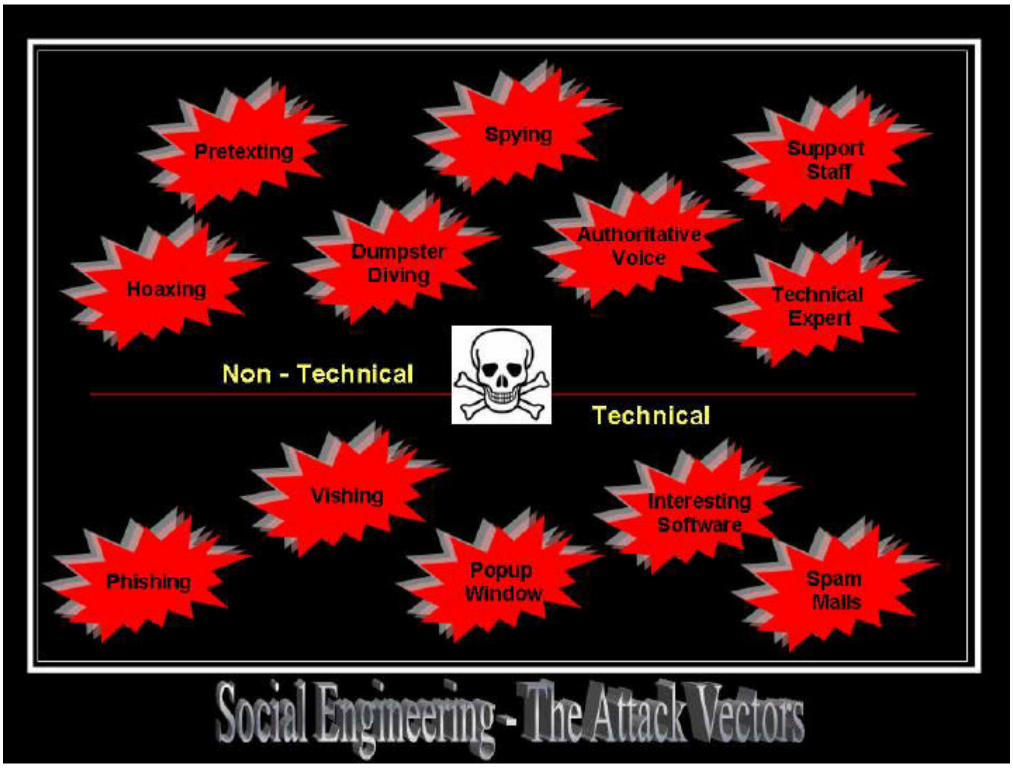
4. **Execution:** once the target has completed the task requested by the aggressor, the cycle is complete.

3. Categories of social engineering

There are two main categories under which all social engineering attempts could be classified – computer or technology based deception, and purely human based deception.

The *technology-based approach* is to deceive the user into believing that he is interacting with a 'real' application or system and get him to provide confidential information. For instance, the user gets a popup window, informing him that the computer application has a problem, and the user will need to re-authenticate in order to proceed. Once the user provides his ID and password on that pop up window, the damage is done. The hacker who has created the popup now has access to the user's id and password and is in a position to access the network and the computer system with credentials of that user.

Attacks based on *non-technical approach* are perpetrated purely through deception; i.e. by taking advantage of the victim's human behavior weaknesses (as described earlier). For instance, the attacker impersonates a person having a big authority; places a call to the help desk, and pretends to be a senior Manager, and says that he / she has forgotten his password and needs to get it reset right away. The help desk person resets the password and gives the new password to the person waiting at the other end of the phone. The attacker now has all the access to perform any malicious activity with the credentials of actual user.



3.1. Technology-based approach

Phishing

This term applies to an email appearing to have come from a legitimate business, a bank, or credit card company requesting "verification" of information and warning of some dire consequences if it is not done. The letter usually contains a link to a fraudulent web page that looks legitimate with company logos and content and has a form that may request username, passwords, card numbers or pin details.

Vishing

It is the practice of leveraging Voice over Internet Protocol (VoIP) technology to trick private personal and financial information from the public for the purpose of financial reward. This term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. However, with the advent of VoIP, telephone services may now terminate in computers, which are far more susceptible to fraudulent attacks than traditional "dumb" telephony endpoints.

Spam Mails

E-mails that offer friendships, diversion, gifts and various free pictures and information take advantage of the anonymity and camaraderie of the Internet to plant malicious code. The employee opens e-mails and attachments through which Trojans, Viruses and Worms and other uninvited programs find their way into systems and networks. He or she is motivated to open the message because it appears to offer useful information, such as security notices or verification of a purchase, promises an entertaining diversion, such as jokes, gossip, cartoons or photographs, give away something for nothing, such as music, videos or software downloads. The outcome can range in severity from nuisance to system slow-down, destruction of entire communication systems or corruption of records.

Popup Window

The attacker's rogue program generates a pop up window, saying that the application connectivity was dropped due to network problems, and now the user needs to reenter his id and password to continue with his session. The unsuspecting user promptly does as requested, because he wishes to continue working, and forgets about it. Later it is heard that there has been an attack on the system, but it never realized that he /she was the one who opened the gate!

Interesting Software

In this case the victim is convinced to download and install a very useful program or application which might be 'window dressed' as a CPU performance enhancer, a great Whitepaper on 'Social Engineering - An attack vector most intricate to tackle!' system utility or as a crack to an expensive software package. In this case a 'Spyware' or a 'Malware' (such as a key logger) is installed through a malicious program disguised as an interesting message or a legitimate program.

3.2. Non-technical approach

Pretexting / Impersonation

This is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone. It's more than a simple lie as it most often involves some prior research or set up and makes use of pieces of known information (e.g. date of birth, mother's maiden name, billing address etc.) to establish legitimacy in the mind of the target.

Dumpster Diving

Seldom would someone think that throwing away junk mail or a routine company document without shredding could be a risk. However, that is exactly what it could be, if the junk mail contained personal identification information, or credit card offers that a 'dumpster diver' could use in carrying out identity theft. The unsuspecting 'trash thrower' could give the Dumpster Diver his break. Company phone books, organization charts and locations of employees, especially management level employees who can be impersonated to the hacker's benefit. Unshredded procedure and policy manuals can help the hacker to become knowledgeable about the company's policies and procedures, and thus be able to convince the victim about their authenticity. The hacker can use a sheet of paper with the company letterhead to create official looking correspondence. A hacker can retrieve confidential information from the hard disk of a computer as there are numerous ways to retrieve information from disks, even if the user thinks the data has been 'deleted' from the disk.

Spying and Eavesdropping

A clever spy can determine the id and password by observing a user typing it in (Shoulder Surfing). All that needs to be done is to be there behind the user and be able to see his fingers on the keyboard. If the policy is for the helpdesk to communicate the password to the user via the phone, then if the hacker can eavesdrop or listen in to the conversation, the password has been compromised. An infrequent computer user may even be in the habit of writing the id and password down, thereby providing the spy with one more avenue to get the information.

Acting as a Technical Expert

This is the case where an intruder pretends to be a support technician working on a network problem requests the user to let him access the workstation and 'fix' the problem. The unsuspecting user, especially if not technically savvy, will probably not even ask any questions, or watch while the computer is taken over by the so called 'technician'. Here the user is trying to be helpful and doing his part in trying to fix a problem in the company's network.

Support Staff

Here a hacker may pose as a member of a facility support staff and do the trick. A man dressed like the cleaning crew, walks into the work area, carrying cleaning equipment. In the process of appearing to clean your desk area, he can snoop around and get valuable information – such as passwords, or a confidential file that you have forgotten to lock up, or make a phone call impersonating you from your desk. Or take the case of the deceptive telephone repairman. The intruder can pose as a repairman and walk up to your phone and fiddle around with the instrument, and the wiring etc, and in the process spy on your workplace for valuable information that has been left unsecured.

Hoaxing

A *hoax* is an attempt to trick an audience into believing that something false is real. Unlike a fraud or con (which is usually aimed at a single victim and are made for illicit financial or material gain), a hoax is often perpetrated as a practical joke, to cause embarrassment, or to provoke social change by making people aware of something. It also may lead to sudden decisions being taken due to fear of an untoward incident.

Authoritative Voice

The attacker can call up the company's computer help desk and pretend to have trouble accessing the system. He / she claims to be in a very big hurry, and needs his password reset immediately and demands to know the password over the phone. If the attacker adds credence to his / her story with information that has been picked up from other social engineering methods, the help desk personnel is all the more likely to believe the story and do as requested.

4. Who is affected by social engineering attacks?

Everyone in a company is responsible for a company's integrity. A company can spend billions of dollars on all kinds of security equipment, but it only takes one person for a company's security to be compromised. While a janitor may not need as much training as an IT helpdesk or secretary, it is important not to forget anyone in a company. A good training program should address issues such as Data retention (what can be thrown away vs. shredded) and data classification (What level of security do I need to treat this document as and what does this level of security mean to me?), Employee Identification and physical access protocols, as well as consequences to not following these procedures and who to contact if you have questions or need to report suspicious behavior. Training can be reinforced by doing role playing with employees so they can get interactive training that will help reinforce what they have learned. Below is a general list of employees a company may have and recommended training.

Training Levels

- ***High*** **–** This level represents people who should be expecting social engineering attacks and/or have the privileges to significantly change or render the network useless. An I.T. helpdesk is a good example of this because they are used to helping people all day as well as having a fair amount (if not more) of network privileges that typically include adding or removing users as well as changing their passwords.
- **Medium –** This level represents people who may have contact with the general public and/or may have some level of access of network access. These people may not have the authority to make network changes, but they can certainly run commands or go to another computer and do a number of things from there. Training should be focused on confirming a person's identity before they give out any information or do any favors.
- **Low –** This level includes people who have little or no network access. This includes security guards and janitors. The training at this level should include training on social engineering tactics, and in some situations may emphasize not letting anyone in after hours as well as not doing any favors for anyone for ANY reason. The training at this level may skip certain tactics if necessary that may not apply to everyone.

A company will obviously have to have a social engineering training plan made to fit the company's needs and positions since no 2 companies are just alike. For a lot of positions where the employee may not work for a highly targeted department and may not do any work remotely, a low to medium strategy may be all that is needed, however do not forget to reinforce the training they do receive. A great social engineering strategy plan may be short lived if it is not reinforced with occasional mock social engineering attempts or short little tips emailed or posted regularly in a bulletin that everyone receives.

- **Helpdesk** – A helpdesk should be trained thoroughly in thwarting social engineering attempts. A busy helpdesk may get many requests and inquiries through email, IM, in-person, or telephone and at any time, a social engineer can attempt to persuade them that they are a legitimate user and need some sort of assistance. A helpdesk's main goal is to help, and that is exactly what a social engineer will be looking for. The helpdesk should be trained to be friendly while at the same time using good judgment and skepticism before proceeding to assist a user. Before they start assigning usernames and privileges, they should be asking themselves if the user is who they claim to be and why and if this user NEEDS these privileges or information.
- **I.T. Administrator** – While IT Administrators may not get as many phone calls as a busy helpdesk, they can still be prime targets because they can control the entire network, and if there's one person a social engineer would like to have running commands and transferring files on a network, it would be the administrator which is why they should have a high amount of social engineering training. Administrators are generally more aware of computer based tactics because they understand the intricacies of a computer network and how devastating one command can be, but they are still vulnerable when it comes to other types of social engineering tactics such as simply just calling and asking for something.
- **Receptionist** – A receptionist is a broad term when it comes to responsibilities and a training plan will have to be made to fit their job. If they are at a company's front door and answering calls all day, they should probably be trained more for in-person persuasion tactics and phone tactics. If they are a personal secretary for a CEO and do a lot of online work and emails, they should probably be trained more for online tactics as well as phone calls where someone needs a favor because the CEO told them to call the secretary for that information. Depending on the job function, a medium amount of training should be sufficient for a receptionist.
- **Telecommuter** – A telecommuter should be moderately to very well trained for social engineering attacks simply because their home network is simpler and because of that, it is a lot simpler for someone to compromise the corporate network remotely as well as a higher chance of success and remaining anonymous due to the telecommuters lack of high-end networking equipment that would exist if that user were to be at the office instead.
- **HR department** – The HR department holds personal information for every employee and even if not everyone in the company wishes to actively protect their company from a social engineer, they should have an interest in protecting their own personal information from being stolen. Not only is this a good point to make in any company training on this subject, the HR department should safeguard their employees data at all costs and pointing out how everyone's personal data is protected should motivate employees to do the same. The HR department may or may not be in regular communication with other departments sending classified information but if they are, there should be a procedure to follow before giving out any information. This department should be highly trained for social engineer attacks and should have procedures to confirm who is requesting data from this department.
- **R&D department** – While a R&D department won't be answering phone calls and responding to emails from unknown users all day, they will however be a prime target for those people who are wanting to see what the company is up to. The department should have very secure servers and possibly a VPN, it is recommended that the R&D department should at least be aware of scams and how someone can use social engineering to get into their servers and steal their blueprints and files. A moderate amount of training should be sufficient, possibly less depending on the situation.
- **Company Executives** – Company executives can take a lot of forms. Some may need a lot of training some may only need a minimal amount of training. Some may not even wish to be bothered by this, but you have to remind them that this involves the entire company and can affect them directly. A moderate amount of training should be sufficient for executives, but it varies greatly on the role that these people play.

5. Examples

In this chapter, I will show examples of many ways a social engineer can infiltrate an organization and get what they want and have almost no chance of having their true identity compromised.

• *Telephone*

The first example is how easily a social engineer can use the telephone to achieve his goal. A lot of attacks will use the telephone because they are used so much in our daily routine and people who use the telephone often to communicate with clients they may not know personally tend to trust people a little easier than most and all a social engineer may really have to do is learn a few key words or jargon and may be able to talk a person into giving out information that the general public shouldn't have. Another reason people may give for trusting people on the phone so quickly is they do not want to seem rude or bothersome to that customer if it turns out their credentials are valid. However, it is quite the opposite, that person will feel more secure knowing that your company is checking for credentials instead of just taking anyone who calls in claiming to be them at face value.

This example is one that I have heard of personally happening locally and it didn't take much more than a short google search (or possibly the local white pages might have worked too.) and a short phone call.

Paul had the desire to get into someone's hotmail account that he knew but had little technical knowledge. He only needed to get in there once or twice and didn't really care too much about them knowing that their email had been broken into. He knew a little information already on that person but nothing more than a name and an email address. The first thing Paul did was go to the local college that provided free internet access to anyone who could walk up to a console and hit enter as to remain somewhat anonymous. Next he went to Hotmail and clicked on "forgot your password?" (as a lot of times people will have security questions that really do not serve them well.) and it asked for some verification like city/town, zip code which he had already and if not, it could have probably been easily Googled. After that step it asked the security question "What is your pet's name?" Oh simple. He went on Google, pulled up the person's phone number, went to a quiet payphone and dialed them up. When they answered Paul said "Hi, I am a local biology student doing a term paper on household pets and I just have a couple questions. I am on the last part of the paper and I only have a few more pieces of data to gather before I am finished. Can you help me?" A couple of seconds of silence passed and she said "Sure, fire away" The first question was how many pets do you own and what kind of pets are they? She answered 3 dogs 2 cats immediately. Next Paul asked "What are their names?" a few seconds passed and he continued with "My paper has a chapter on the most popular animal names in it." She answered promptly and he asked the final question "and what are their ages?" to reduce the likeliness of her remembering the question that he asked that he was interested. After she answered that question, Paul thanked her for her time and she shockingly said "Oh that was easy" as if she was prepared to give out more information. Paul wasn't completely stupid and waited a couple of days to pass before attempting the names then anxiously came home from work one day and attempted the names. The first 2 didn't work and as he was thinking oh crap, time to come up with a Plan B, he typed in the 3rd name and success he was at the reset password screen which also gave him a temporary password to login.

The moral of this story: Be careful what you give out, it may seem innocent and innocuous, but it can be just what a social engineer needs to break into your system. On a side note, I don't like security questions. There are times that I use them, but not for everything, simply put they annoy me, I am password responsible, and if I had not heard about the above, I am likely to make up something vulnerable that someone could Google. Every time I help someone setting up an email or something similar, they always ask "what is a security question and why do I care?" and a lot of times they will initially make up something just as vulnerable until I intervene. As for myself, I am not too bad at remembering passwords, so I make cryptic security questions if I absolutely have to, otherwise I say, "if I can't remember the password, it probably wasn’t that important.“ This may or may not work with everyone, but just being aware of what can happen will naturally make the next security question you have to make more secure.

Another example:

The First Call:

Andrea Lopez answered the phone at the video rental store where she worked, and in a moment was smiling: It's always a pleasure when a customer takes the trouble to say he's happy about the service. This caller said he had had a very good experience dealing with the store, and he wanted to send the manager a letter about it. He asked for the manager's name and the mailing address, and she told him it was Tommy Allison, and gave him the address. As he was about to hang up, he had another idea and said, "I might want to write to your company headquarters, too. What's your store number?" She gave him that information, as well. He said thanks, added something pleasant about how helpful she had been, and said goodbye. "A call like that," she thought, "always seems to make the shift go by faster. How nice it would be if people did that more often."

The Second Call:

"Thanks for calling Studio Video. This is Ginny, how can I help you?" "Hi, Ginny," the caller said enthusiastically, sounding as if he talked to Ginny every week or so. "It's Tommy Allison, manager at Forest Park, Store 863. We have a customer in here who wants to rent Rocky 5 and we're all out of copies. Can you check on what you've got?" She came back on the line after a few moments and said, "Yeah, we've got three copies." "Okay, I'll see if he wants to drive over there. Listen, thanks. If you ever need any help from our store, just call and ask for Tommy. I'll be glad to do whatever I can for you."

Three or four times over the next couple of weeks, Ginny got calls from Tommy for help with one thing or another. They were seemingly legitimate requests, and he was always very friendly without sounding like he was trying to come on to her. He was a little chatty along the way, as well -"Did you hear about the big fire in Oak Park? Bunch of streets closed over there," and the like. The calls were a little break from the routine of the day, and Ginny was always glad to hear from him.

One day Tommy called sounding stressed. He asked, "Have you guys been having trouble with your computers?" "No," Ginny answered. "Why?" "Some guy crashed his car into a telephone pole, and the phone company repairman says a whole part of the city will lose their phones and Internet connection till they get this fixed." "Oh, no. Was the man hurt?" "They took him away in an ambulance. Anyway, I could use a little help. I've got a customer of yours here who wants to rent Godfather II and doesn't have his card with him. Could you verify his information for me?" "Yeah, sure." Tommy gave the customer's name and address, and Ginny found him in the computer. She gave Tommy the account number. "Any late returns or balance owed?" Tommy asked. "Nothing showing." "Okay, great. I'll sign him up by hand for an account here and put it in our database later on when the computers come back up again. And he wants to put this charge on the Visa card he uses at your store, and he doesn't have it with him. What's the card number and expiration date?" She gave it to him, along with the expiration date. Tommy said, "Hey, thanks for the help. Talk to you soon," and hung up.

• *Online*

The next example is about social engineering using phishing and popups online. Public awareness has risen over the past few years regarding phishing and popups. While most of them can be disregarded just by using a decent spell checker and a popup blocker, some can be more convincing. Be aware of the information that you give out online. I have noticed that this section will be more applicable to people who do not use their computer often, as a lot of regular computer users can spot an average online scam in about 10 seconds or less.

Bob was surfing the web on a nice sunny afternoon and had noticed a recent barrage of pop-ups in which one of them said “Your computer is infected with Spyware, click here for a free scan”. Well it looked like a legitimate windows message because it had the XP theme and a red X at the top, so it must be legitimate he thought so he clicked it. It took him to a page and asked him to fill out some information like name, email, phone, etc. Soon after a scan began which claimed to clean out all spyware on the computer, but the popups continued and soon enough his inbox was filled with junk.

On the same day, Joe was checking his email and had noticed that one of them was from security saying that they had detected that his email had a virus and that he needed to download the attachment and run it to get rid of this virus. It was very colorful and had a lot of "WARNINGS" and "IMMEDIATE ATTENTION REQUIRED" labels all over. Without a second glance (not noticing who the email was from, or why they were emailing him, or even the misspellings in the email), Joe panicked and download the attachment and ran it. The attachment said the virus had been deleted and he went about his business feeling proud that he fixed his email problem and that no emails were lost.

Training and awareness of these types of scams are key. Knowing what to look for in emails to tell if its authentic or not, and not clicking on any popups and why will greatly improve awareness of this type of attack.

• *Dumpster Diving*

In this example, a social engineer will prove that someone else's trash is another mans treasure. If your trash could be used against you or your company, dispose of properly.

Since dumpster diving is more passive and can actually be done while you are asleep, this is more of a description of what can happen.

A social engineer was out behind a company he was profiling poking around in their dumpster. The dumpster was in the open and had no lock on it so he looked down in the trash can and found a bag that appeared to have lots of documents inside. Inside were invoices, bills, and other important documents. The company earlier that week had some repair done on a laser printer as an invoice stated. That social engineer can now call the company he is going after claiming that he works with the repair company which opens the door for a number of attacks he can use. If the social engineer found a customer list or even a bill to another company, he can call up posing as a customer and get classified information that only the real customer should have. Furthermore, should he have found network diagrams or usernames and passwords, he could do even more damage, possibly without any further attacks.

• *Shoulder Surfing*

Shoulder surfing is when a social engineer watches what you are doing and can also be done remotely (both by cameras and software). This is also a mostly passive technique, as I wouldn't expect anyone to be coming up to you while you were at the coffee shop sending emails, sit down next to you, and say "Hey, mind if I watch you for a while?" I don't suggest going out into the public doing business on your laptop in clear sight, but sometimes it may be unavoidable and you need to be aware of your surroundings. For instance, if you work in a public place and have to operate a computer of some sort (like a POS register) anyone can watch you enter your employee ID and password to get on the register. Also, if you are in a public place with a laptop, be careful of what's on your laptop as well. It may be obvious, but some people leave usernames and passwords taped to their laptop, and not only can that be seen in public, if the laptop gets stolen, they already have credentials. ATMs are also used a great deal and sometimes may not always be as secluded as we all think. A social engineer with a pair of binoculars may be hiding in the bushes watching you enter your pin, and may happen to get a glimpse of your name. If you happen to be in a computer lab, there will probably be computer cameras around. For all you know, those cameras could be public and anyone with an internet connection can logon, zoom in, and see what anyone in the room is doing. The best thing to do is be aware of your surroundings; you never know who may be watching you.

• *Reverse Social Engineering*

Reverse social engineering is a more advanced method of social engineering and requires some reconnaissance before a successful attack is employed. It involves the user asking for assistance from the attacker so the victim is at the mercy of the social engineer. This is one of the hardest types of attacks to detect because when a victim contacts the social engineer, they have no doubt they are who they say they are and will most likely not question them at all. There are many ways that a social engineer may be able to get a user to contact them for help but here is one example.

This particular social engineer had managed to gain access to a small switch inside a company that connected a couple of users. The social engineer then might contact those users and introduce themselves and say that if they ever have any network connectivity problems to call them immediately. Sometime in the near future the attacker would then kill connectivity to that switch and wait for one of the users to give them a call. At this point, the social engineer is in control and can control the victim in whatever way the social engineer desires. If successful, the end result will be that the victim will have given away some piece of information (server name, username/password, network topology), the social engineer will have fixed whatever problem they have caused, and the user's problem will have been corrected without the victim even considering that they may have just given out some confidential data.

• *Persuasion*

Persuasion is This example is from the Official Certified Ethical Hacker Review Guide chapter on social engineering.

The facilitator of a live Computer Security Institute demonstration showed the vulnerability of help desks when he dialed up a phone company, got transferred around, and reached the help desk. "Who's the supervisor on duty tonight?" "Oh, it's Betty." "Let me talk to Betty." [He's transferred.] "Hi Betty, having a bad day?" "No, why?…Your systems are down." She said, "my systems aren't down, we're running fine." He said, "you better sign off." She signed off. He said, "now sign on again." She signed on again. He said, "we didn't even show a blip, we show no change." He said, "sign off again." She did. "Betty, I'm going to have to sign on as you here to figure out what's happening with your ID. Let me have your user ID and password." So this senior supervisor at the help desk tells him her user ID and password. (Graves, 2007)

6. Counter-measures

Is there an effective way to fully protect against Social Engineering an attack? The answer is 'No'. For the simple reason that no matter what controls are implemented, there will always be the possibility of the 'human factor' being influenced by a social, political and/or cultural event.

Nevertheless, as with any threat, there are ways in which to reduce the likelihood of success. This can be achieved by having an appreciation of the threat, and knowledge of both the techniques that could be used and the counter-measures that can be implemented.

6.1. Controls

Below is a list of core controls that can be implemented to protect against such an attack. However, when considering which of these controls to implement, it is important to ensure that they –

- do not disrupt normal day to day operations;
- are robust enough to block a variety of malicious actions occurring concurrently;
- can establish the difference between an attack and normal day-to-day activity.

Core controls that can be implemented:

• **Management buy-in:** managers require an understanding of their role to be able to define what requires protection, and why. This understanding should ensure that appropriate

protective measures are taken to protect against associated risks.

• **Security policy:** a sound security policy will ensure a clear direction on what is expected of staff within an organization. For example, support teams should only offer assistance for a defined range of activities.

- **Physical security:** a key control that involves restricting physical access to computer facilities and systems for staff, contractors and visitors. For example, in order to remove the possibility of people overstating their authority, the use of access badges indicating an individual’s status (e.g. employee, contractor, and visitor) is recommended. In addition, employees should be encouraged to look at the badges.
- **Education/Awareness:** a simple solution that can be used to prevent these types of attacks. For example, a knowledgeable user can be advised that he/she should never give out any information without the appropriate authorization and that he/she should report any suspicious behavior. A good training and awareness program focusing on the type of behavior required will undoubtedly pay for itself. This program might even provide users with a checklist on how to recognize a possible ‘Social Engineering’ attack.
- **Good security architecture:** smart infrastructure architecture will allow personnel to concentrate on more important duties. For example, by ensuring outbound firewall access

controls are configured just as carefully as inbound controls, an administrator will know exactly how the networked environment will respond under certain events. This understanding will ensure that the administrator is able to avoid spending time following up on 'false positives'.

- **Limit data leakage:** reducing the amount of specific data available will ensure that the attack is not an effortless exercise. For example, websites, public databases, Internet registries, and other publicly accessible data sources should only list generic information, such as main organization phone number and job titles instead of employee name(s) [for example, 'site administrator' instead of 'Joe Bloggs'].
- **Incident response strategy:** a documented response strategy will ensure that, if under pressure, a user will know exactly what procedures to follow. For example, if a user receives a request, he/she should verify its authenticity before acting on the instructions he/she has received. If, however, he/she has already acted on the request, then he should alert the administrator. It will then be the responsibility of the administrator to check with the users to ensure no other user has followed the instructions of the request.
- **Security culture:** building an information security culture within an organization starts with making people aware of security issues, providing them with tools to react, and encouraging two-way communication between security personnel, managers and employees. The creation of a security culture should be considered a long-term investment, which requires a constant effort to maintain and grow.

6.2. Maintaining Preparedness

Once the controls have been implemented, there are two ways for an organization to maintain a state of ongoing preparedness for such an attack. The first is to perform regular reviews of the controls that have been implemented. These reviews will ensure that an acceptable standard is maintained on an ongoing basis. The second and the least common approach used, is to simulate an attack. This type of review depends on the information that can be obtained from the public domain about the organization, as well as the value it could offer, versus the resource-intensive overhead. It should also be noted that many organizations are not comfortable with this type of review.

Conclusions

With the abundance of confidential information that organizations must protect, and with consumer fraud and identity theft at an all time high, security has never been as important as it is today for businesses and individuals alike. Social engineering is a technique used by hackers and other criminals to persuade people to divulge confidential information, or allow unauthorized access, for their personal gain or for malicious purposes. Techniques such as impersonation, phishing and dumpster diving are used by social engineers to achieve their goals. Although social engineering attacks are difficult to defend against because they involve the human element, it is possible for organizations and individuals to protect themselves by being trained on the importance of security and gaining awareness of the possible social engineering attacks that they may encounter.

Individuals and organizations can try to protect their confidential information by storing their data on a system that requires password-only access, putting that system in a secure room that allows only authorized admission, and by spending as much money as possible on security tools to protect that data. Even after implementing all of these necessary Safeguarding Against Social Engineering precautions, they are still susceptible to social engineering attacks because every security measure involves some sort of human intervention.

While training people on different methods used by social engineers will help prevent some attacks from being successful, methods change and countless other schemes can be used. The only viable solution to protecting against these threats is by generating overall awareness. Once people are aware of the critical data that they possess, the crucial need to protect it, along with the strong possibility of exploitation, subsequently a strong defense will be built and social engineering attacks will begin to decline.

References

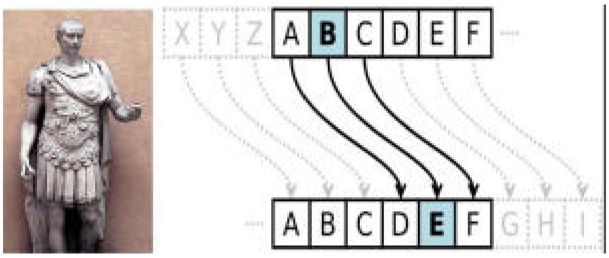
1. http://www.securityfocus.com/infocus/1527/
2. http://www.socialengineeringdb.org
3. http://www.sans.org/reading_room/whitepapers/engineering/
4. http://en.wikipedia.org/wiki/Social_engineering_%28security%29
5. http://en.wikipedia.org/wiki/Dumpster_diving
6. http://www.windowsecur ity.com/articles/Social_Engineers.html http://www.cert.org/advisories/CA-1991-04.html Ashish Thapar, Whitepaper on *“Social Engineering - An attack vector most intricate to tackle!”*

ENCRYPTION, KEY MANAGEMENT AND PKI

Civilian Iuliana Mirela STERIAN

UM 02545 Bucuresti

Cryptology is the science of communicating and deciphering secret writings. Julius Caesar used one of the earliest recorded cryptographic systems during Rome's battle at Gaul in 58 BC. Able to securely deliver messages to his commanders, Caesar's campaigns were highly successful and assured his future in Rome.



In 1945, nearly 2000 years later, the National Security Agency and the Central Intelligence Agency began using electronic forms of cryptic communication. It wasn't until 1976 that doctoral student Whitfield Diffie and Stanford processor Martin Hellman developed the concept of a public key cryptosystem. Their paper, entitled "New Directions in Cryptology," would become the foundation of public key infrastructure

Soon after Diffie and Hellman's paper was published, three inventors from MIT – Ron Rivest, Adi Shamir and Le Adleman developed the first usable public key encryption system, complete with digital signatures. Known as RSA, the system became the best known and most widely adopted public key infrastructure cryptosystem. The public key would be used for securing or "locking" messages and the private key for decoding or "unlocking" them.

The need to encode information and keep it private is hardly new, of course. According to the Roman historian Herodotus, "secret writing" saved Greece from conquest at the hands of the Persian despot Xerxes in 480 B.C., and has played a part in many wars, not to mention national affairs of lesser violence ever since.

1. Introduction to security systems

1.1. Security basics

The requirement and basic principles for security solutions can easily be derived from a few fundamentals. Computer systems are used to process increasing amounts of data in a fast, convenient, and reliable way. Most of the data is in some way important to individuals for performing their job duties, or to a whole organization for conducting their business. In fact, most business data is handled by computers nowadays, which includes electronic mail, asset information, customer databases, process control information, and so on. Some of the data is considered critical because an organization would suffer damage if the data was lost or incorrect.

The same is true for the computer systems themselves because their proper functioning becomes critical for companies. Access to computer systems is not limited by physical access to the computer itself because computers are normally connected through an any-to-any network. An issue that comes up is improper use of computers, be it inadvertent or malicious. Improper use of computers also potentially means access to critical data.

To have a better understanding of security systems and services, some security terms with explanations are listed below:

Authentication is the process of verifying the validity of a claimed individual and identifying who he or she is. Authentication is not limited to human beings; services, applications, and other entities may be required to authenticate also.

Data Confidentiality: Sensitive information must not be revealed to parties that it was not meant for. Data confidentiality is often also referred to as privacy.

Data Integrity assures that the data is not altered or destroyed in an unauthorized manner.

Non-Repudiation: Assurance that a sender cannot deny being the source of a message, and that the recipient cannot deny the receipt of a message.

Key Management deals with the secure generation, distribution, authentication and storage of keys used in cryptography.

A Public Key Infrastructure (PKI) provides the technical framework (including protocols, services, and standards) to support applications with five security capabilities: user authentication, data confidentiality, data integrity, non-repudiation, and key management.

1.2. Encryption

Encryption is simply the translation of data into a secret code so that only authorized users can understand it. Encryption has played a vital role in data communications since the first computer networks were established, but it is especially critical for companies that are venturing into public networks.

Encryption is a technology that can, if properly used, protect data from being disclosed to unauthorized parties. Sometimes, especially when legal obligations are involved, means must be in place such that a creator of a document cannot later decline to have created that document.

1.3. Symmetric encryption versus asymmetric encryption

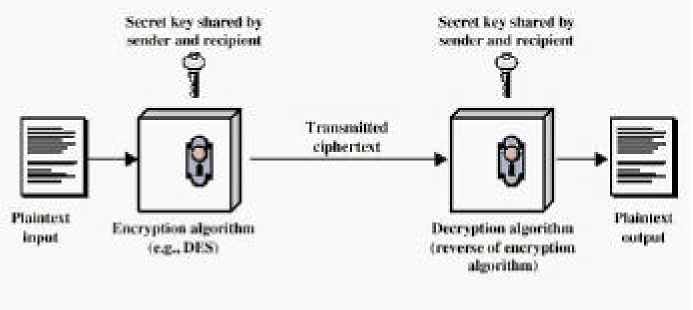
There are two basic types of encryption Symmetric, sometimes called Conventional or Secret Key Encryption and Asymmetric also called Public Key Encryption. Both types are used to achieve Confidentiality.

Symmetric	**Asymmetric**
One key used by both the sender and receiver to encrypt and decrypt data.	Two keys are used, one to encrypt data and one to decrypt data.

Figure1: Symmetric and asymmetric encryption

Encryption is one of the most effective ways to achieve data security, since in order to understand and use encrypted data you must first posses the key that enables you to decrypt it.

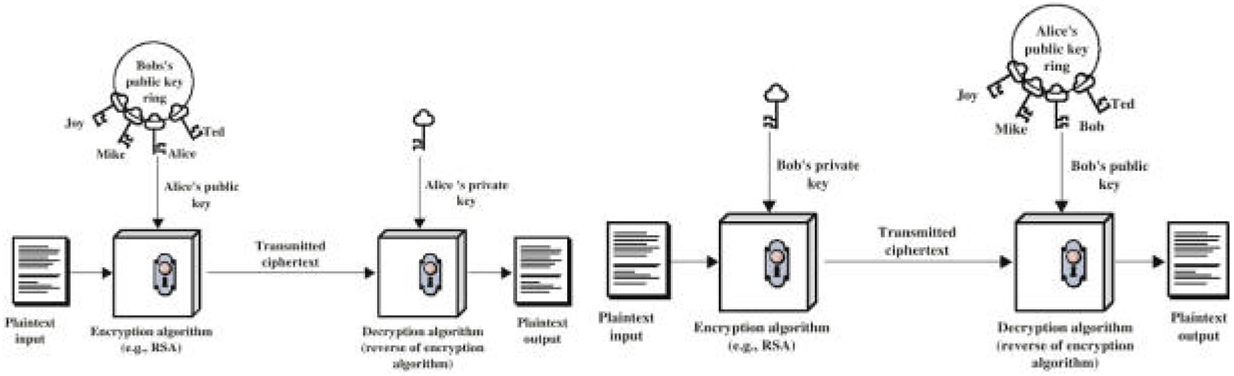
1.3.1. Symmetric encryption


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

The most common of the Symmetric or secret-key encryption is called the Data Encryption Standard (DES). Although this type of encryption does fulfill the first requirement of security, Confidentiality, it has some disadvantages. The first is that you have to distribute the secret key, and keep it secret. This can cause a problem, especially if there are a large number of people who need the key. A second disadvantage is that this type or encryption does not support non-repudiation. There is no way to prove who the encrypted message came from. This type of encryption therefore is not totally suitable instead a system known as public-key encryption is now gaining popularity.

1.3.2. Asymmetric or public-key encryption

The second type of encryption, and one that's use is increasing is Public Key Encryption. This type of encryption uses two keys; one to encrypt and one to decrypt. In order to have two way encrypted communications each person must have two keys. One key is your private key. This key is not shared with any one. The other key is your public key. You send your public key to anyone you want to send you an encrypted message. (Public keys are not secret, and are sometimes available through an online service).



2. Key management

2.1. Keys

The term key refers to some information (usually a binary number of a specific length) that is used with a cryptographic algorithm for encryption and/or decryption purposes. During data encryption, the key affects how the data is scrambled. During data decryption, only the correct key is allowed to get back the original data. For secret key cryptography, the encryption key is the same as the decryption key. For public key cryptography, the encryption key is different from the decryption key. This basic concept is illustrated in figure:

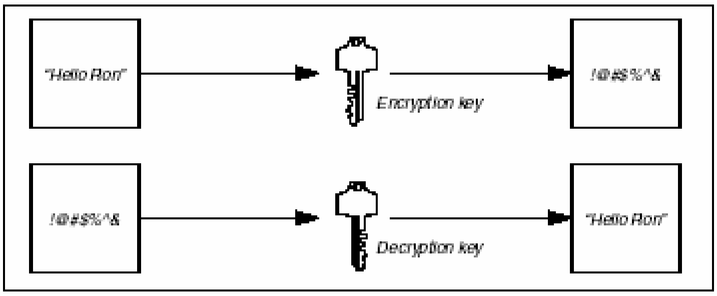


Figure2: Encryption key versus decryption key

There has been a common misconception that by breaking the cryptographic algorithm all the messages can be decrypted. Please note that cryptographic algorithms are usually widely known or can be broken. Therefore, it is not the cryptographic algorithm that protects the data, but much more the key. For secret key cryptography, the key has to be kept securely by the communicating parties. For public key cryptography, the private key is kept by the key owner in a safe place. Moreover, the public key and private key are generated by complex computations. For both cases, the keys are very important for the encryption and decryption processes. A private key should not be easily calculated from other known information, for example, the well-known public key or the published algorithm. Thus, decryption without the correct key is very difficult or even impossible for all practical purposes.

2.2. Secret key versus public key cryptography

If data is transmitted over the network intact, someone else on the network may be able to look at the data. This is very insecure. A better way is to scramble the data to other forms based on some criteria before the transmission. This is called encryption. When a recipient receives the scrambled data, he or she can change it back to something meaningful (if he or she knows the way to do so). This is called decryption.

Many algorithms have been developed to describe how to scramble (encrypt) data. Cryptography is the science of how to do encryption and decryption.

The most widely used cryptographies are secret key cryptography and public key cryptography. They are used to build schemes or protocols to secure information transmission.

2.2.1 Secret key cryptography

The first commonly-used cryptography is secret key cryptography. The reason for this name is because any two communicating parties have to keep a secret between them of how to encrypt and decrypt the data. In secret key cryptography, a single key, called a symmetric key or a secret key is used for both the encryption and decryption processes. That is why secret key cryptography can also be referred to as symmetric cryptography.

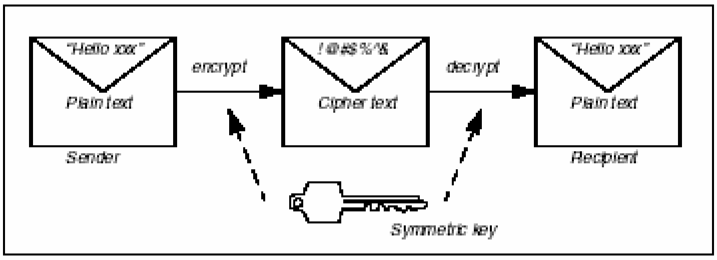


Figure 3: Secret Key Cryptography

Encryption and decryption using a secret key is usually fast and easy, due to a less complex computation when compared with public key cryptography (to be introduced in the next section). This is why secret key cryptography plays an important role for data encryption and decryption in many Internet security protocols, as in, for example, the Secure Sockets Layer (SSL) protocol.

Here are some commonly used examples of symmetric key cryptosystem:

- Data Encryption Standard (DES): 56-bit key plus 8 parity bits, developed by IBM in the middle 1970s
- Triple-DES: 112-bit key plus 16 parity bits or 168-bit key plus 24 parity bits (that is two to three keys)
- RC2 and RC4: variable-sized key, often 40 to 128 bits long to summarize, secret key cryptography is fast for both the encryption and decryption processes. However, it is a nightmare for users to maintain a large number of secret keys, unless some kind of infrastructure can help users to store and manage keys in an easy manner.

2.2.2. Public key cryptography

Another commonly-used cryptography is called public key cryptography. In public key cryptography, an asymmetric key pair (so-called a public key and a private key) is used. The key used for encryption is different from the one used for decryption. Public key cryptography requires the key owners to protect their private keys while their public keys are not secret at all and can be made available to the public. The computation algorithm relating the public key and the private key is designed in such a way that an encrypted message can only be decrypted with the corresponding other key of that key pair, and an encrypted message cannot be decrypted with the encryption key (the key that was used for encryption). This is a very important design principle of public key cryptography, where messages are encrypted using a recipient's public key. If this encrypted message could be decrypted with the encryption key (that is the recipient's public key, which is obtainable in public), everyone could decrypt and read the message from the sender. So, an encrypted message in public key cryptography cannot be successfully decrypted by the encryption key.

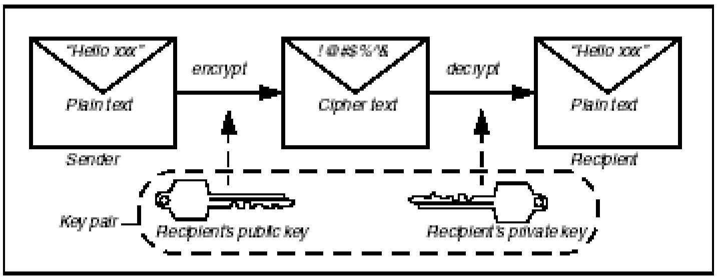


Figure 4: Principle of public key cryptography

In fact, everybody can send encrypted messages to a recipient using the recipient's public key which, by definition, is publicly available. Only the recipient is able to decrypt these messages because only he or she is in possession of the corresponding private key. However, the recipient cannot be sure if the message is really from a specific sender, since everybody can see the recipient's public key and can fake to be that sender. Even though the public key is widely distributed, it is practically impossible for computers to calculate the private key from the public key. So sometimes, public key cryptography is not used to encrypt the whole message, but only to encrypt a small, fixed-length summary of the whole message. Here are a few commonly-used examples of public key cryptosystem:

- Rivest, Shamir, and Adleman (RSA): variable-sized key, generally 512-2048 bits
- Elliptic curves: variable-sized key, 160 bits, comparable security to RSA 1024 bit

One may think that public key cryptography is a replacement of secret key cryptography.

3. Basic elements of public key cryptography

Another unresolved issue is the following: when a sender signs (encrypts) a message with his or her private key, and the recipient decrypts the message with the sender's public key, although the recipient can read the message, the recipient cannot be sure whether the sender's public key is really from the sender, or from someone else, since no one can certify to the recipient that this public key is really from that sender.

This section, describe how to apply the public key cryptography to other security designs, such as digital signatures and certificates, so as to resolve the above issues.

3.1. Digital signatures

To have better authentication, the idea of digital signatures was introduced. For a clearer understanding, it is good to think of a digital signature as a signature that we use to sign checks or other legal documents. A digital signature is created by first generating a message digest from the source message using a hash function. Then, the message digest is encrypted with the sender's private key. This encrypted message digest of the original message is called the digital signature.

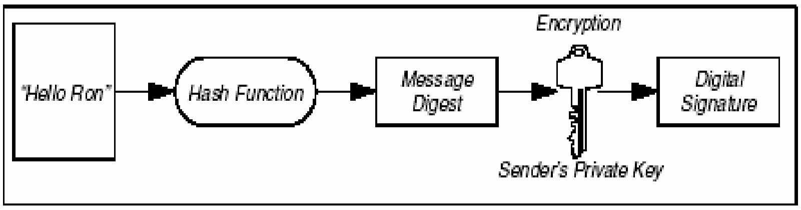


Figure 5: Generation of a digital signature

Before explaining how a digital signature improves user authentication and data integrity in a communication, we need to understand what a hash function is. A hash function is not an encryption mechanism, but a tool for creating a digest of a message. A hash function should have three main characteristics:

- It takes a message of any size and generates a small, fixed-size block of data from it (called a message digests or hash value). Re-executing the hash function on the same source message will always yield the same resulting digest.
- It is not predictable in operation. That means, a small change in the source message will have an unpredictably large effect on the final digest.
- It is irreversible. In other words, there is no way to derive the source message from the digest.

Therefore, the message digest calculated by the hash function can be thought of a good fingerprint of the original message.

Here is how the whole thing works together. During a communication, the digital signature is appended to the original message and sent to the recipient. When the recipient gets the whole message, it will break it into the message and the digital signature. How can the recipient be sure that the message received is really original, that is, the message was not altered and was sent by the real sender? The recipient can do the following steps to check:

1. For the message part, create a message digest using the same hash function.
2. For the digital signature, decrypt it with the sender's public key, which results in the message digest.
3. Compare the two message digests obtained in steps 1 and 2.
4. If the two message digests are the same, this ensures the message was not altered and that it is from the real sender.

Therefore, by appending a digital signature to a message, this assures the recipient that the sender is really the person who created the message and the message has not been changed along the communication path, that is, user authentication is observed and data integrity is preserved.

3.2. Certificates

The mechanism for doing this authentication is by using certificates. Certificates, also called digital certificates, act very much like passports; they provide a means of identifying individuals. Unlike passports, digital certificates can also be used to identify non-human entities, such as server systems or applications. Another difference between a digital certificate and a passport is that a certificate can (and should) be distributed and copied without restriction, while people are normally very concerned about handing their passports to someone else.

Certificates do not normally contain any confidential information and their free distribution does not create a security risk.

More technically speaking, certificates are digital documents that associate an individual or End-Entity (EE) with its specific public key. A certificate is a data structure containing public key, pertinent details about the key owner, and, optionally, some other information, all digitally signed by a trusted third party, usually called a Certificate Authority (CA).

There are three basic ways to distribute certificates:

- Manually

- Certificate Servers
- Public Key Infrastructure

Manually normally means either you exchange certificates by unsecured E-mail or physically exchanging diskettes. This is time consuming, and you have to keep track/manage all the Certificates, keeping them up to date, and ensuring they are valid.

Certificate Servers are the next level up. This is basically a database that allows authorized users to store and retrieve digital certificates. These are usually maintained within a company for there own use.

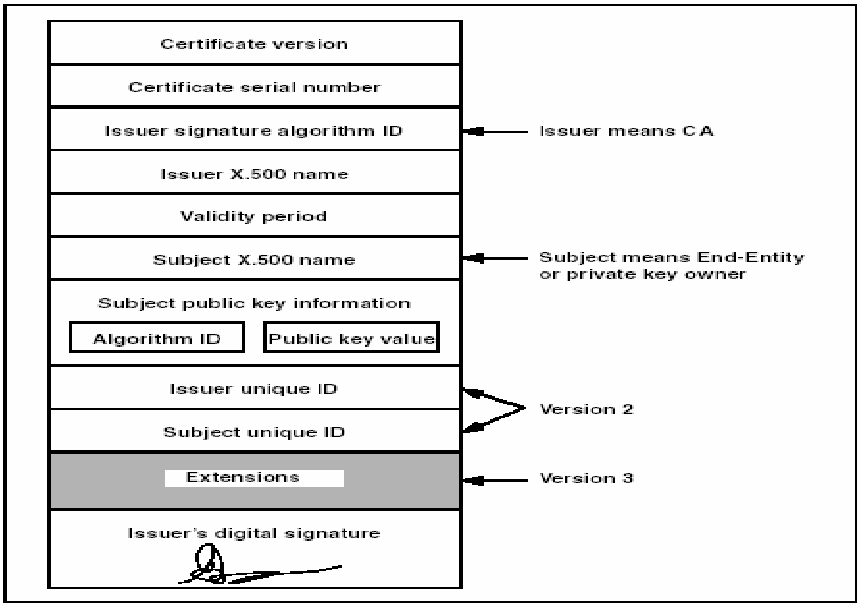


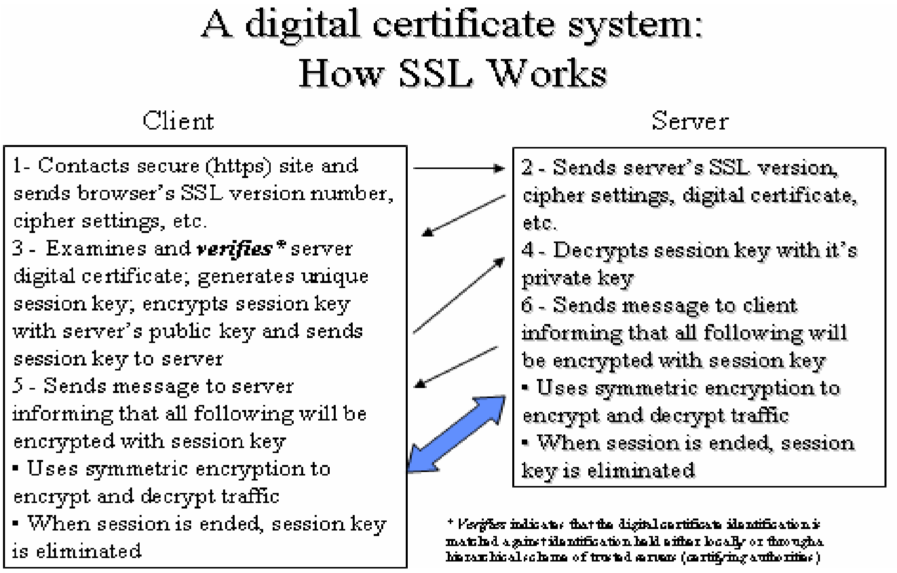
Figure 6:.X.509 Certificate Format

The important fact to know and understand about digital certificates is that a trusted party (therefore, also called an authority) certifies that the enclosed public key belongs to the entity listed in the certificate. The technical implementation is such that it is considered impossible to alter any part of a certificate without easy delectability.

When a sender wants to send a message to a recipient, he or she does not attach the public key to the message, but the certificate instead. (Optionally, the certificate can be published to and later retrieved by the recipient from a public place, such as a public electronic directory.) The recipient receives the message with the certificate and then checks the signature of the third party on the certificate. If the signature was signed by a certifier that he or she trusts, the recipient can safely accept that the public key contained in the certificate is really from the sender. This prevents someone from using a fraudulent public key from impersonating the public key owner.

The owner (entity) that is listed in the certificate and associated with a public key can be identified in various ways. In a simple form, the owner is only identified (represented) by his or her e-mail address. Such certificates are common for secure e-mail communication, but they are not sufficient to represent an individual for doing electronic business, especially when large liabilities or money amounts are involved. In such cases, a Certificate Authority may elect to do a thorough validation of an applicant before signing and issuing a digital certificate.

A digital certificate also normally includes additional information that describes or limits the scope of use.



A digital certificate system:
How SSL Works

Client

1- Contacts secure (https) site and sends browser's SSL version number, cipher settings, etc.
3 - Examines and ***verifies**** server digital certificate; generates unique session key; encrypts session key with server's public key and sends session key to server
5 - Sends message to server informing that all following will be encrypted with session key
▪ Uses symmetric encryption to encrypt and decrypt traffic
▪ When session is ended, session key is eliminated

Server

2 - Sends server's SSL version, cipher settings, digital certificate, etc.
4 - Decrypts session key with it's private key
6 - Sends message to client informing that all following will be encrypted with session key
▪ Uses symmetric encryption to encrypt and decrypt traffic
▪ When session is ended, session key is eliminated

* *Verifies* indicates that the digital certificate identification is matched against identification held either locally or through a hierarchical scheme of trusted servers (certifying authorities)

Figure 7:.Digital Certificates

4. Public key infrastructures

4.1. PKI Basics

Public Key Encryption allows you to maintain privacy/confidentiality and digital certificates allows you to know if a public key truly belongs to the purported owner. For security you need both the public key and the certification (normally packaged together) for every person you wish to send an encryption message to. If this is a small group of people, no problem you can do it manually. However if you need to send messages or files to a large and changing group you are going to have a real headache if you try and do it manually.

A PKI is basically a collection of an operating system and application services. These services include:

PKI Services

Manage keys:

- Issue new keys
- Review or revoke existing keys
- Manage the trust level attached to keys from different issuers.

Publish keys:

- locate and retrieve public keys
- tell whether a specific key is valid or not.

Use keys:

- moving keys around
- providing easy-to-use applications that perform public-key cryptographic operations

4.2. PKI Components

The Infrastructure is composed of hardware, software, policies and procedures. It provides basic security and trust. It is based on the digital certificates, binding the users' digital signature to their public key.

PKI should consist of:
• A Security Policy • Certificate Authority (CA) • Registration Authority (RA) • Certificate Distribution System • PKI-enabled Applications

- **Security Policy**- the organization should have an overall information security policy this contains information on how the organization will control the use of cryptography and how it will handle keys. The level of controls placed on the information should match the level of risk.
- **Certificate Practice Statement (CPS): -** If a PKI system is operated by a Commercial Certificate Authorities (CCAs) or a Trusted Third Party, then it requires a CPS. A CSP is a document about the enforcement of the security policies. It often includes definitions on the CAs construction and operation, how certificates and keys are managed.
- **Certificate Authority (CA):** This is the basis of the trust of the system, managing the public key certificates. The CA issues certificates by binding the identity of a user or system to a public key with a digital signature. It also assigns and track operation dates and revokes certificates. Your organization can operate its own CA, or use a commercial CA or Trusted Third Party.
- **Registration Authority (RA):** This is the interface between the user and the CA. It authenticates the user and submits the certificate request. The quality of will determine the level of trust.
- **Certificate Distribution System:** The distribution of the Certificates can be done either by the user, through a directory service or by a server.
- **PKI-enabled applications:** Various applications can use PKI. Some examples are:
  - ➢ Communications between web servers and browsers
  - ➢ E-mail
  - ➢ Electronic Data Interchange (EDI)
  - ➢ Credit card transactions over the Internet
  - ➢ Passing personnel data over the Internet
  - ➢ Virtual Private Networks (VPNs)
  - ➢ Transactions with your bank or credit union

Conclusions

Security has become a major focus throughout the entire I/T industry. With the advent of the Internet and the new ways of doing business it enables, organizations experience some market pressure to be present on the World Wide Web, but, at the same time, have to ensure that such connections to the outside world do not pose any risks to them. Even inside the organizations, information that is available on interconnected computers may need to be protected from unauthorized access. This fact, in turn, requires methods that protect information in transfer and means are required that uniquely identify individuals. Several technologies are available today and even widely used that solve part of these problems, such as the encryption of data for secure data transmission or the use of personal passwords for authentication. Most of these systems, however, are islands in the whole and it has become clear that security must be designed and implemented from a higher-level perspective.

The Internet has emerged as a vehicle for both general commerce and corporate business, increasingly being used like a remote extension of the private communications networks that connect to it. Security cannot be stressed enough when sending sensitive data through the public Internet; in the case of online commerce, ensuring it is a requirement for maintaining customer confidence. PKI is an outstanding means of providing powerful, open data encryption and the services that support it.

PKI brings the security and trust of the physical world to the electronic world. Through strong encryption, asymmetric keys, digital signatures and trusted third-party verification, PKI meets the legal standards required to conduct verifiable and secure on-line transactions

PKI creates a climate where information piracy and fraud are absent and both parties accept legal standards. PKI is a catalyst that will lead to greater acceptance of Internet-based products and services.

References:

1. http://world.std.com/~franl/crypto.html Cryptography: The Study of Encryption This page points to several different cryptographic sources
2. http://theory.lcs.mit.edu/~rivest/chaffing.txt Confidentiality without Encryption new security technique that can be used instead of encryption.
3. http://world.std.com/~franl/crypto/rsa-guts.html The Mathematical Guts of RSA Encryption
4. http://www.rsasecurity.com/rsalabs/faq/2-1-6.html RSA Security: What is a hash function? General explanation with links to the algorithms
5. http://www.cdt.org/crypto/risks98/ The risks of key recovery, key escrow and trusted third-party encryption
6. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf Security Requirements for Cryptographic Modules
7. http://csrc.ncsl.nist.gov/cryptval/des/des.txt

TELECOMMUNICATIONS LAWS, POLICIES AND STANDARDS

LTC Ionel TIGANUS

UM 02052 Constanta

Introduction

Communications is now in Romania, as for most countries of the world, a strategic sector of national economy. The scale of investment attracted, especially the rapid expansion and the ability to induce a multiplicative effect of economic growth, especially through the potential to stimulate development of other sectors have transformed communications in the last twenty years in one of the main drivers of the economy, both in each level of the world, and globally.

Electronic communications sector in Romania known a clear orientation to a specific profile of competitiveness. Thus, the development offers its own infrastructure based on user has access to a success in our country, against the backdrop of rising demand, fuelled by increasing purchasing power and increasingly sophisticated consumer preferences Romanian users who could not be covered by insufficient supply of traditional fixed networks underdeveloped. In contrast, development of infrastructure access services provided by another operator (telephone services based on carrier pre-selection and Internet access services based on unbundled local loop access) was practically nonexistent, despite the introduction of a regulatory framework at the level of European best practice. Currently in Romania there are no less than 6 mobile phone companies that provide or are preparing to provide services on its own infrastructure, over 35 operators providing access to its fixed telephone network and hundreds of electronic communications networks used for providing access to broadband.

However, the convergence phenomenon occurred because of new technology gives a powerful impetus to increasing direct competition between companies offering fixed and mobile network operators increasingly gaining more ground segment services to fixed.

Thus, in terms of end users, maximizing choice between several suppliers and ensuring maximum benefit from the services available at a given price level, are essential tools to directly increase their satisfaction, in terms of price or value of use of services.

In this context and taking into account the need for full alignment with the standards of universal service as set out in Directive 2002/22/EC shall be revised by the Ministry of Communications and Information, hereinafter the Document MCSI policy and strategy implementation universal service in electronic communications sector, the document adopted by Order of the Minister of Communications and Information Technology no. 184/2004. The new strategy includes objectives and appropriate measures will be implemented no later than 31/12/2012.

1. IT&C Policy and strategy

Accession to NATO and Romania join the European Union had to establish, to support these goals, some structures and adopt strategies to that effect, as follows:

- Establishing strategic importance due to MCIT for the development of IT & C at the national level (initiative followed later by other countries in the region);
- Establishing the Group for Promoting IT (GD nr.217/2001);
- Strategies for crossing Romania on the Information Society:
  - HG 1007/2001 - Strategy computerization of public administration;
  - HG 1440/2002 - National strategy on promoting the new economy and implementing the Information Society;
  - Strategy "Knowledge Economy" conducted jointly with the World Bank;
  - Strategy ''Horizon - 2025 "section" telecommunications, information technology and postal services'';
- Romanian Government strategy to stimulate and support the development communications sector during 2002-2012;
- Policy and strategy document on the implementation of universal service in electronic communications sector;
- Government development strategy of broadband electronic communications in Romania for the period 2009 - 2015;

2. European policy on information security

Internet primarily interested in both large and small companies. Virtually no business in a developing country with a minimum average not have created Web pages, you will find more about services and products. Also, consumers and manufacturers can communicate instantly via the Net, which gives them the possibility of mutual information and communications to very inexpensive. However, they did not "cast" yet to do business or managing large scale Internet. Why is this retainer? Reasons given most often are related to security of online transactions.

Concerns about network security and information systems increased proportionally with increasing number of users of networks and turnover.

Security has reached a critical point, representing an essential requirement for electronic business and the operation of the entire economy.

Combining several factors made the security of information and communication constitutes one of the key points on the agenda of EU policy:

- Governments have realized the dependence of their economies and citizens of the smooth operation of communication networks and have begun to review security arrangements.
- The Internet has created a global link, connecting millions of networks, large and small, millions of computers and other devices such as mobile phones.

This greatly reduced the economic costs of accessing information vital for remote attacks.

Consistent with this, the board of the Stockholm concluded *"the Council and Commission will develop a comprehensive strategy on security of networks, including implementation activities in practice"*.

With only a few years ago, network security was a problem state monopoly, offering specialized services based on public networks, particularly for telephone networks.

These things have changed considerably with developments in the context of an enlarged market, among which we liberalization, convergence and globalization:

- *Networks are now mostly privately owned and managed by private companies*. Communication services are provided on the basis of competitiveness, security of being part of the supply market;
- *Networks and computer systems converge*. They are interconnected, providing the same types of services and more, sharing the same infrastructure. Terminals (computers, mobile phones etc..) Became an active element in the architecture and networks can be connected to different networks.

- *Networks are international.* An important part of communication today is done transfrontarier, via the third countries (sometimes without the user to do so). Therefore, any solution to the security risks to consider this.

2.1. The need for public policies

Protecting computer networks is becoming increasingly seen as a priority for politicians, particularly because the need for protecting data to provide a functioning economy, for reasons of ensuring national security and promote electronic commerce. This led to a substantial set of legal precautions in the EU Directives on data protection and the EU framework for telecommunications.

Operators adopt a rate ascending Internet standards or their links in some way their networks to the Internet. However, the Internet was not designed with security measures, but on the contrary, was developed to provide access to information and facilitate information exchange. This was the basis of its success. Investment in security often are only effective if people proceed in the same way. Therefore, cooperation to create security solutions is required. But cooperation only works if a critical mass of players involved, which is difficult to obtain. Interoperability between products and services will allow competition among security solutions. But substantial costs are involved as coordinating be generalized global solutions, and some players are tempted to impose a solution on the market in their possession. How many products and services still use their own solutions, there is no advantage in using safe standards, which provide additional security, only if all other offers.

As a result of these flaws, the European telecommunications and data protection already requires legal obligations for operators and service providers in order to ensure a certain level of security in communications and computer systems. Recommendation for a European policy on network and information security can be described as follows:

- First, the legal provisions at EU level should be effectively applied, it asked for a common understanding of security issues and specific measures to be taken. The legal framework will have to evolve in the future, for example, in connection with cyber crime, electronic signature, etc..
- Second, certain market imperfections have concluded that market forces do not "pump" sufficient investment in technology and security practices. Good policies can revive the market and at the same time, can improve the functionality of the legal framework.
- Finally, the communications and information services are offered without taking into account the boundary. So a European policy is necessary in order to ensure domestic market for such services to benefit from common solutions and to enable effective global action.

2.2. Awareness of hazards

Many users (private / public) are still not aware of possible threats encountered using communication networks or solutions already exist to meet them. Security issues are complex and risks are often difficult even for experts to foresee. Lack of information is one of market imperfections, which security policies you should consider.

The problem is that users find the right information, they can understand, which are up to date and meet their own needs. Finally, providers of public telecommunications service available are obliged by EU law to inform their subscribers about the risks posed by a network security breach and possible remedies, including the cost involved (cf. art. 4 Directive 97/66 EC).

The aim of the initiative to raise awareness of citizens, government and business is therefore to provide information accessible, independent and you can rely on network and information security.

2.3. A European warning and information system security information

Even if users are aware of security risks, they all must know about the new threats. Attackers malevolent, almost inevitably, will find new vulnerabilities to circumvent the protection of the safe. Continuously develop new software applications and services, providing a better quality of service, making the Internet more attractive, but in the process, unintentionally open up new vulnerabilities and risks.

So it takes a quick warning system that will alert all users with a source of information and rapid and reliable advice on how it can act against attacks.

Business also needs a mechanism for confidential reporting of attacks, without risking the loss of public confidence. Much work in this area is made by Computer Emergency Response Teams (CERTS) or similar entities. For example, Belgium has organized a virus alert system which allows Belgian citizens information about the alerts caused by viruses in two hours. However CERT sites operate differently in each Member State, making complex cooperation, if not difficult. CERT existing sites are not always well equipped and their tasks are often not clearly defined.

Global cooperation is carried out by CERT / CC, which is partly funded by the U.S. government and CERT sites in Europe is dependent on the publication of information by the CERT / CC.

2.4. Develop technological support

Investment in networks and information security are currently the best. This is the case both in terms of technological support and research to discover new solutions. In the context of new technologies inevitably bring with them and new risks, ongoing research is vital. Secure Networks and the information is already included in Information Technologies (IST) Program of the EU's 6th Framework Research Program.

Research at the technical level cryptography is in an advanced stage in Europe. Belgian Rijndael algorithm called Advanced Encryption Standard won the contest organized by the U.S. Institute of Standards (NIST). NESS project (New European methods for Signature, Integrity and Encryption) of IST has launched an expanded level competition in meeting the requirements of new encryption algorithms for multimedia applications, mobile commerce and smartcard.

2.5. Standardization and Certification

For improved security solutions to be successful, they must be implemented jointly by prominent market players and preferably based on open international standards. One of the main obstacles to the adoption of many security solutions, such as electronic signature, was the lack of interoperability between different implementations.

If two users wish to communicate securely between different platforms, interoperability must be ensured. Using standardized protocols and interfaces should be encouraged, including compliance testing. Open standards, preferably based on open source software could help remove bugs as quickly and greater transparency. Also, security assessment contribute to increasing confidence of users. Using common criteria for evaluation in many countries facilitate mutual recognition, they have also entered into an arrangement with Canada and the U.S. for mutual recognition of IT security certificates (Council Recommendation 95/144/EC on security evaluation criteria information technology, implemented in most Member States).

Certification processes taking place in business and management information systems security is supported by the European cooperation for Accreditation (EA).

Examples are the initiatives eEurope and smartcard initiatives in implementing public key infrastructure (PKI) program launched within Exchange Data between Administrations (IDA). It lacks standardization efforts, but a large number of standards in competition leads to market fragmentation and the presence of non-interoperable solutions. Therefore, standardization and certification activities ongoing need for better coordination and also need to keep up with the introduction of new security solutions.

2.6. Legal framework

There are several legal texts that influence security of communications networks and computer systems. Due to convergence of networks, security issues bring together legal rules and traditions of various sectors. These include telecommunications (incorporating all communication networks), computer industry, the Internet has functioned mainly based approach "hands off" (negative clearance) and electronic commerce is becoming increasingly the subject of specific legislation. In relation to security, provisions for damage to third parties, cyber crime, electronic signatures, rules on the protection and export relevant data.

Protecting privacy is a key policy objective in the European Union. He was recognized as the basic law under Article 8 of the European Convention on Human Rights. Articles 7 and 8 of the EU Charter of Fundamental Rights also stipulates the right to respect for private and family life, home, communication and personal data. Article 5 of the Directive on Data Protection in Telecommunications obliges Member States to ensure confidentiality in public telecommunications networks. In addition, Article 4 of that Directive requires public service providers and networks to take technical and organizational measures to ensure security services. These provisions have implications for the security needs of networks and information systems used by those persons or organizations, such as e-commerce providers.

Framework Program of EU telecommunications services contains several provisions relating to network operations security (meaning availability of emergency networks) and network integrity (meaning ensuring normal operation of interconnected networks). Commission proposed a new framework of rules for electronic communication services in July 2000.

Computer crimes triggered a broad discussion in the EU about how to react to criminal activities using computers and computer networks.

Criminal laws of the Member States should provide and unauthorized access to computer networks, including personal data security. There are problems in investigating these irregularities and there is an insufficient inhibition of hackers. Criminal laws against intrusion into computer networks are also important to facilitate judicial cooperation between Member States. Legitimate concerns over electronic crime requires effective legal investigations.

2.7. Security in Government applications

eEurope Action Plan aims to foster better interaction between citizens and government. How much of the information exchanged between citizens and administration to a confidential (medical, financial, legal, etc..) Security is vital to ensure successful implementation of the plan. Furthermore, developing e-government makes government to become the example for demonstrating the effectiveness of security solutions and market player with the ability to influence development in the field by buying decisions they make.

The problem for government is not only to acquire that information and communications systems security requirements, but also develop a security culture of the organization. This can be taken out by setting organizational security policies tailored to the needs of the institution.

2.8. International cooperation

The network is as safe as the weakest link of them, and Europe can not insulate the rest of the global network. Consequently, security issues set out above require international cooperation.

The European Commission is already contributing to the work of international fora such as G8, OECD, United Nations. The private sector deals with security issues in organizations such as the Global Business Dialogue (www.GBDe.org) or the Global Internet Project (www.GIP.org).

2.9. Information security plan eEurope 2005

As information society is becoming increasingly important for both business and society, ensuring security for both the infrastructure itself and the information circulating on it, is a critical point. For the Internet to be a reliable medium of computer Society should be made available, the information transmitted or stored to be kept confidential, we must ensure who is the author of information and that it was not altered.

Other challenges are also among the objectives of eEurope 2005 Plan:

- *Network security and information* against accidental or criminal attacks;
- *Cybercrime* on the harmonization of legislation of member countries;
- *Secure communication for e-government*, to develop a secure trans-European networks, which can be vehicula secret or confidential information (Project IDA-Interchange of Data between Administrations).

3. European Integration

In January 2001, Romania is in a position to conduct negotiations on the chapter of telecommunications under the auspices of the declaration of the European Commission report in 2000, that "no substantial progress in transposing the acquis in telecommunications. Further efforts are needed to develop the regulatory framework. Moreover, Chapter 19 was given as an example to all official chapter meetings open prematurely and without foreseeable chance of completion. Ministry of Communications and Information Technology had been further than the handicap of years of privation as a body of central public administration able to design and implement a coherent policy to adapt to new technological conditions and harmonization with Community law.

The adoption, in 2001 and 2002, the package of laws harmonized with relevant Community legislation has made the most important stage of the scheme of the Ministry of Communications and Information Technology. Legal provisions have had in creating a framework for business development in the field of Communications and Information Technology, one of the most dynamic economic sectors, which can be an engine for national development. Romania was the first country to implement national legislation in the new directive adopted at Community level in communications, thus making competition and training full time opening the telecommunications market, established in January 1, 2003.

On November 8, 2002, in Brussels, Romania Chapter provisionally closed 19 negotiation to join the European Union, which refers to telecommunications and information technology.

3.1. Information technology

The concept of e-government is based on use by the central government based on information technology applications. E-government ensures the provision of public services and information 24 hours in 24, 7 days / week and debirocratizarea government. MCIT launched during 2001-2004 a series of pilot projects, some of which were extended nationally.

3.2. Projects launched by the MCIT and extensive national

***National Electronic System* (www.e-guvernare.ro)**

It was established by Law 161/2003 and the only point of access to services and public interest for natural and legal persons provided by central government. Electronic public services provided by companies dedicated SEN are:

1. Declaration on the nominal record of liabilities insured and the state social insurance budget - CNPAS
2. Declaration on the establishment and payment obligations to fund health insurance payable by persons other than those operating under an individual employment contract - CNSAS:
    - Declarations of contributing to the unemployment - ANOFM
    - Declaration of payment obligations to the state budget - MFP
    - Statement of income taxes - MFP
    - The bill on VAT – MFP

***The electronic system of awarding licenses for international transport of freight* (www.autorizatiiauto.ro)**

It was launched in November 2003 and ensure transparency of the assignment of authorizations to transport. System 1900 is used by international freight carriers and in 2004 were awarded over 330,000 electronic authorization from 8733 to 2003. Starting in November

2004 in SEAP may view the program scheduled to transport the traffic district, intercounty between two inter-county and surrounding counties.

***The electronic procurement (ESPP)* (www.e-licitatie.ro)**

Was released on March 4, 2002. By the end of 2004 this system was completed over 350,000 transactions, with a saving of over 100 million Euro.

Other projects undertaken by MCIT jointly with other public institutions in 2001-2004 are: computerization of the government meetings, electronic information systems and payment of local taxes (59 localities have made such systems), electronic data-collection statistics , customs declaration online, integrated information system aimed online, electronic voting system used by military and police personnel on official missions in Iraq, Afghanistan, Bosnia-Herzegovina and Kosovo in the 2003 referendum for the Constitution.

The 'knowledge economy'

Was initiated in 2004 with support from World Bank and aims to create approximately 300 local virtual network serving as knowledge centers in rural areas to provide information and services to citizens. These networks will connect major institutions in rural communities with social, economic and education in local communities - schools, city hall, library, houses of culture - information networks and national and global transaction.

In 2004 MCIT launched two systems dedicated action to prevent and combat cybercrime:

- www.eFrauda.ro - to receive complaints concerning unlawful pre apparent nature of information society services
- www.ceris.ro - center expertise and IT security incident response

At the request of MCIT, ASRO adopted the first standard for security systems - ISO 17799, which most countries use it as a reference standard in auditing information systems.

Communications and postal services

MCIT has completed the 2002 regulatory framework necessary for a liberalized market, which promoted self-regulatory forms, so that Romania is the first European state with legislation on electronic communications brought into line with EC Directives of 2002. Preparation consisted liberalization both in promoting unrestrictive regulatory framework for new entrants to the development of alternative communications infrastructure and the establishment of ANRC, which provides continuous monitoring of the existence of competition in the market for electronic communications and intervenes where necessary. Since June 14, 2002 was implemented the new numbering plan necessary to ensure the numbering resources in the communications market liberalization. In the new numbering was introduced figures showing a new operator or service. Remained unchanged 00 for international access codes and one for long-distance.

Electronic communications market was fully liberalized on January 1, 2003, so that during 2003 most foreign investments were focused on electronic communication segment. In two years of opening to competition over 2400 companies have submitted notifications for the provision of electronic communications. As a result of increased competition on prices of international calls fell by 60% and the number of fixed and mobile subscribers reached 13.5 million, with more than 9 million mobile charges.

Implementation of universal service

It began in 2004 with the installation of telephones, public pay phones and offset part of the net cost of access to communications services for low income families.

Unique National System for Emergency Calls (112)

Is an important component of universal service is provided in one of the important directives for this sector policies of the EU acquis.

4. Romania's position on telecommunications and information technology

4.1. The liberalization of telecommunications markets

The liberalization of telecommunications markets is a basic reference point of the reform process. The Romanian legislation adopted since 1991, have been liberalized following markets:

- Terminal equipment (liberalized in 1991, the equipment is subject to approval type);
- Data (liberalized in 1992, the lines are leased from Romtelecom);
- Mobile communications (liberalized in 1992, licenses are granted within available spectrum);
- Satellite communication services, transport and distribution of radio and television (liberalized in 1992, National Radiocommunications Company provides transportation services of the national radio and television programs produced by the Romanian Radio Broadcasting Corporation and the Romanian Television);
- VSAT (liberalized in 1992).

Latest restrictions on fixed voice telephony and the provision of leased circuits, have been raised since January 1, 2003, since which marked the full liberalization of services markets and telecommunications networks.

4.2. Information Society

Romania is involved in the overall European effort to develop the Information Society. National priorities in this area are consistent with the strategic objectives defined in the initiative "eEurope +" and the recommendations of the Ministerial Conference in Warsaw in May 2000. Romania's priorities for the transition to the Information Society are: modernization of public administration and public services, improving living standards by using information technology in areas like health, environment and transport sector development, information technology, workforce development in light of the Information Society, adaptation of education and development of digital content. To achieve these objectives, in 2001-2004 under the coordination of government runs a number of projects to facilitate wide access to the Internet, education and training, stimulate commerce, providing rapid access of citizens and companies to government services, switching to e-government.

Information Technology Promotion Group (GPTI), established in March 2001 as a task force headed by the Prime Minister and seven other ministers having composition, provides a unified and coordinated approach to implement Information Society in Romania. Main tasks of GPTI aims to develop strategy and approval of all major projects in information technology and communications initiated by public institutions, national companies or those in which the state is controlling shareholder, and such projects benefiting these companies.

4.3. Adaptation and implementation of the acquis communautaire

Regulatory Framework

Primary legislative framework for regulatory activity is currently provided by telecommunications law no. 74/1996 (Official Gazette No. 156 of July 22, 1996). This legislation is worthy of being enshrined in a relatively modern legal basis for the development of this sector in Romania, and the necessary related to market liberalization of the sector. Law no. 74/1996 reflects the EU policy in the telecommunications sector, defining and fundamental objectives:

- guaranteeing the free flow of information, secrecy and inviolability of communications via telecommunications, regardless of technology used;
- liberalization of the design, installation, maintenance, operation and interconnection of networks and telecommunications equipment, the supply of telecommunications services and other activities in this area;

- operating activities of telecommunications networks and services to meet user requirements in terms of economic efficiency, in compliance with specifications and technical standards and quality.

The last goal that is now the basis for regulatory activity of this sector in Romania, having defined the guiding principles: providing basic telecommunications services in accordance with the principle of universal service, ensuring the optimum user access to services and telecommunications networks, by measures on the distribution, availability and quality, ensuring effective competition in telecoms markets, pursuing efficiency in network operations and provision of telecommunications services.

Law no. 74/1996, Minister of Communications Order no. 76/1994 on the application of open network leased line services and the Order no. 175/1998 on the interconnection of telecommunications networks contain provisions concerning the application of open network clause (Open Network Provision) and the behavior of operators with dominant market position, provisions that have implemented the basic principles contained in Directives 90/387/EEC, 90/388 / EC, 92/44/EEC, 96/19/EC, 97/33/EC and 98/10/EC.

Law no. 74/1996 contains several provisions on tariffs and accounting for telecommunications services, ensuring the implementation of relevant provisions of Directives 96/19/EC and 97/33/EC. The pricing is envisaged to cover the cost of services performed in the long term, avoiding abuse of dominant position, providing the optimum service for beneficiaries, prohibiting cross-subsidization, ensuring fair competition.

Regulatory power sector are currently exercised by the Ministry of Communications and Information Technology, whose organization and functioning are established by Government Decision no. 20/2001 (Official Gazette No 16 of January 10, 2001). Ministry of Communications and Information Technology is responsible also define a policy and communications strategy and information technology sector and promote normative acts performed transposition of the acquis communautaire. The Ministry is assisted in its work with the General Inspectorate for Communications and Information Technology, established by Government Decision no. 180/2002 (Official Gazette No 158 of March 5, 2002).

General Inspectorate for Communications and Information Technology carries out duties of supervision and monitoring obligations contained in the regulations, licenses and permits issued in electronic communications, mail, audiovisual and information technology, management and monitoring of radio spectrum with non-governmental award, control and certification of compliance with technical standards of electronic communications, postal, broadcasting and information technology.

General Inspectorate for Communications and Information Technology spectrum monitoring performed by two systems - System Inspections Radio (Radis), operational since late 2001, and National Integrated System Management and Monitoring of spectrum use (NSMS), whose implementation is will be completed by mid 2002.

Regulatory activity is based on a continuous interaction and consultation with stakeholders. The communications minister orders no. 394/1996 and 137/1997 was established by the Telecommunications Advisory Council, a body which ensures consultation between the Ministry of Communications and Information Technology, as a public authority responsible for regulating telecommunications and strategy, and all parties involved and interested in developing this sector .

The first legislation adopted by the Government in this package is the order no. 34/2002 on access to electronic communications networks and associated facilities, and interconnection of, presented in the section on access and interconnection. This package will also contain basic provisions on the regulatory framework for electronic communications networks and services, including establishment of national regulatory authority for the sector, establish the principles of regulatory activities that will run the authority, allocation and assignment of radio frequencies, numbering resources management, authorization of electronic communications networks and services, including granting rights to use radio frequencies and numbers, universal service and users' rights relating to electronic communications networks and services, competitive market for electronic communications services.

Work to develop new legislation focuses on four Directives (the Framework Directive, the Authorization Directive, Access Directive, Universal Service Directive) and the Radio Spectrum Decision within the composition of the new common regulatory framework for communications networks and services electronic EU and the draft Commission Directive on competition in markets for electronic communications (Directive to liberalize).

In the second quarter of 2002 was finalized, approved and entered into force normative act on the general regulatory framework for electronic communications networks and services. This document will contain the main provisions concerning the establishment, organization, functioning and powers of the National Regulatory Authority for Communications (ANRC). The status and powers ANRC meet established by the new framework. ANRC is independent of operators, service providers and equipment suppliers, while realizing the effective separation of structurally between regulatory functions and activities associated with the exercise of rights deriving from the state as a shareholder in companies having a business purpose in domain.

5. National strategy for universal service implementation

5.1. General information relevant

Access to a minimum set of electronic communications services is considered a fundamental right of citizens, essential for their integration into the community and, more broadly, in the information society. Electronic communications services beyond the personal and business side of communication is an essential tool for the public provision of all types of information, goods and services, both by the government (social services, education or health, for example) and the private sector (information society services). Those without access to electronic communications services is likely to be marginalized in society XXI century.

As a result of increasing competition and overall economic and social developments that led to the facts of Romania near the natural limits of growth in the availability of services, may be considered partial or full use of available funds to finance increased availability of services telephone and broadband Internet services.

Increase the use and ensure the quality and accessibility of the internet connection in all sectors of economic and social life lead to achieving Information Society desire, offering the entire society can fully benefit from the advantages of access to information essential to new directions in which going Romania.

5.2. Priorities, policies and existing legal framework

Assumptions and priorities implementation of universal service

Actions taken to date to implement the universal service are taken into account the particular situation in Romania to the situation in other European countries, especially European Union member states. While in most countries of the European Union was possible quasi-automatic designation as universal service provider to the national fixed network operator, was holding the monopoly, because of its well-developed network, which can be relatively easily extended to any new user in Romania the situation was radically different, due to considerably lower penetration rate. Thus, while the European Union Member States serve all users can be achieved at reasonable cost, Romania sign short-term costs of all households in the fixed network would be very high, requiring a massive increase in network. In addition, relief of Romania, dominated by mountains at a rate of 30%, should be made more difficult thereby.

Given the above, MCSI focused, according to the document of policy and strategy on implementation of universal service in electronic communications sector, approved by Order of the Minister of Communications and Information Technology no. 184/2004, on 2 lines of short-term development: ensuring access of rural communities isolated from the public telephone network via telecentres and ensure affordability of access to public telephone network at a fixed point for certain disadvantaged categories of users, following the long-term objective is the provision of access to public telephone network, fixed point.

Legal and regulatory policy of universal service in the European Union.

Ensure a level determined by the quality of services included in universal services at an affordable price for all users was established as an objective of Community policy in the context of the adoption package of measures to prepare when full liberalization of the telecommunications market.

But, with the European regulatory framework review, completed by the new package of directives adopted in 2002, rules relating to universal service were reviewed and grouped in Directive 2002/22/EC on universal service and users' rights relating to networks and electronic communications services. Under the directive, each Member State is required to ensure the availability of a minimum set of services for all end users at an affordable price and quality conditions determined.

Legal and regulatory national policy of universal service

The legislative framework on universal service is based on Law no. 304/2003 on universal service and users' rights relating to electronic communications networks and services, republished, 'the universal service law, national provisions transposing the Directive 2002/22/EC on universal service and users' rights relating to networks and electronic communications services.

MCSI, as coordinator and guarantor of development of electronic communications market in Romania, has the power to set policy and strategy for implementation of universal service. In this regard, MCSI set goals to be reached to ensure the possibility of communication for all citizens, respecting the principles of transparency, objectivity, proportionality and non-discrimination and taking into account possible negative effects on competition restriction.

6. Government development strategy broadband electronic communications in Romania for 2009 – 2015

6.1. Introduction

The fundamental objectives of the Lisbon Strategy - to support economic growth and job creation - one of the main tools identified was to develop a knowledge-based economy in conjunction with stimulating information and communication technology sector (ICT). Thus, were recognized benefits of using ICT equipment and services on the creation of information society, able to foster increasing economic competitiveness and social cohesion.

Action plans that eEurope 2002, eEurope 2005, i2010, which endorsed the implementation of the objectives of the Lisbon strategy, focused on the desire to create an "information society for all" by extending the level of access and use of the Internet, as a medium to disseminate information and providing services and content, creating new markets, thereby increasing productivity in the economy. To carry out action plans, the EC proposes three priorities:

- Creating a single market and competitive Information Society;
- Increased investment in ICT research;
- Promoting an inclusive information society.

Given that spread the benefits of the Internet is becoming increasingly dependent on the availability of high-speed Internet access to citizens and companies, increased use of broadband communications services was identified as a major objective.

In this context, it has become clear and Romania need to develop a national strategy that supports the development of broadband electronic communications (engl. "broadband") as a key factor in building the information society. This strategy, medium term, should incorporate the realities and perspectives of all holders of interests in the market, so that it can become a vector alignment of all relevant resources to promote broadband services in Romania.

The document was structured in five main components as the major directions of analysis:

- Defining the concept of broadband electronic communications and presentation of anticipated development of broadband communications services;
- Analysis of current situation in Romania;
- Defining general principles and strategic objectives;
- Develop Action Plan;
- Identifying needs and funding options.

The development stage of strategic options and define the priority intervention measures, consultations were held with key authorities and were taken into consideration suggestions and recommendations collected from the market in collecting the information.

6.2. Defining the concept of broadband communications

Broadband's beyond the technical or lexical definition, regardless of the media (TV, radio, optical) or the speed attribute to him, defines the degree of networking that you use and hence the quantity information that we have access at any time.

The essence of the concept of broadband communications, can be understood only if interpreted as a set of technological opportunities that allow rapid transmission of large amounts of data in order to ensure access to a wide range of digital services. Bandwidth is required for different online services varies significantly depending on them.

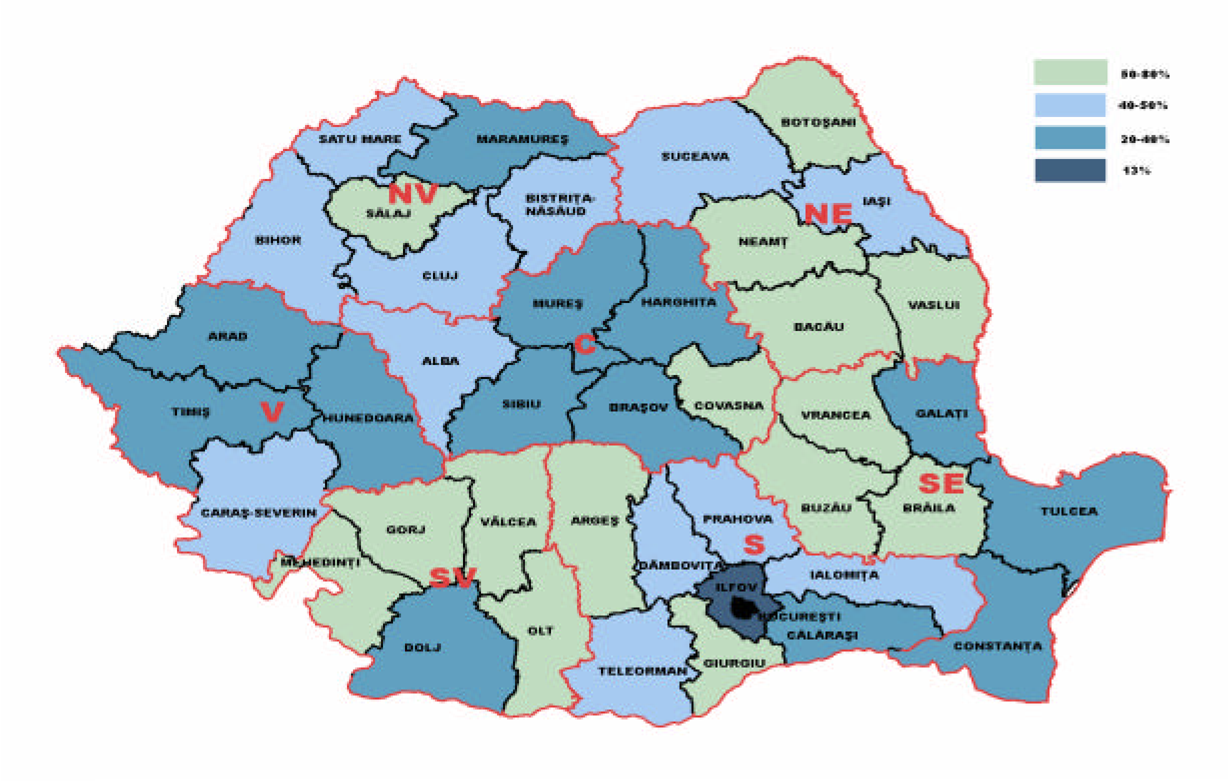
National Regulatory Authority for Administration and Communications (ANCOM) establishes a general definition that is based only on quantitative dimension of Internet connections, indicating the transfer speed of 144 kbps as a threshold for delineation of the broadband connections narrowband.

To monitor the development of broadband availability is necessary but expanding the general definition of quantitative indicators that can be changed gradually according to changes in the characteristics of end-user demand, but according to offer applications and services. Defining uniform and permanent broadband is hampered by issues such as the dynamism of technological innovation, the different level of development on various levels, the level of coverage with network infrastructure and the difference recorded in terms of popular applications.

Considering all these aspects, in the provision of electronic communications services broadband will use the following concept: "broadband is the type of electronic communications, which, through a variety of technological solutions available, provides access to the Internet, with a minimum transfer speed of 1 Mbps shared (gradually increasing amount) and a minimum grade of 98% monthly availability, providing the maximum degree of interactivity and access to the full spectrum of applications and digital content can be accessed by the Internet. "

Percentage of population without access to broadband:

Percent	**County**	**Nr of counties**
50%-80%	Vâlcea , Vaslui, Mehedinti, Salaj, Neamt, Gorj, Olt, Buzau, Braila, Vrancea, Giurgiu, Bacau, Botosani, Covasna, Arges	15
40%-50%	Iasi, Dâmbovita, Prahova, Ialomita, Caras-Severin, Bihor, Satu Mare, Teleorman, Alba, Suceava, Bistrita-Nasaud, Cluj	12
20%-40%	Tulcea, Mures, Calarasi, Dolj, Arad, Hunedoara, Timis, Galati, Sibiu, Harghita, Maramures, Constanta, Brasov	13
13%	Ilfov	1



Thus, taking into account information in the table above and the fact that there must be an exact definition of areas where access to electronic communications broadband is limited in different circumstances, we will define the disadvantaged in terms of access as any locality with more than 10,000 inhabitants, which are present at most two Internet service providers.

6.3. Benefits expected from the development of broadband communications services

The benefits of access to broadband not take the form of performances recorded by the activities, the latter may be executed without access, but more difficult in an area smaller, geographically limited. The great benefit is that it allows carrying out a new form. This possibility and its influence on the society just started to appear. Work from home via the electronic communications are solutions to problems such as unemployment, transport or environment.

Another example is e-education that offers an alternative to traditional learning, making it the applicant to be independent of time and space managed by specific institutions, creating the possibility of adjusting the pace of progress on individual ability and need . Access to broadband will also play a major role for applications that appear as the emergence of new needs arising from the information society and knowledge economy.

Research and development: Globalization and the opening by large companies to research and development centers in areas with major human potential, where operating costs are reduced, involving an exchange of specialized information worldwide distribution, access to specific applications and large generators data traffic. At the same time imply the existence of broadband communications infrastructure and availability of human resources experience with new technologies, including communications.

Economy: The degree of interconnection between business and the digital communication is still at an early stage and developing new business models is dependent on attracting a critical mass of users. In the context of current developments in Romania and openness to European and global economy, businesses will become a major consumer broadband services. In this respect, the effect is to establish a mutual drive on which business development to increase demand and thus stimulate competition and the emergence of value added services. In addition, broadband sector development can contribute to Romania's attractiveness as a destination for foreign investment.

Cultural and recreational activities: Electronic communications broadband can have a significant impact on the cultural activities and recreation, by providing high accessibility, changing consumer behavior and by providing access to a large number of options. Also, on the growth performance of broadband, interactive online environment increases attracting users.

Public administration: Public administration is providing public information, and collection services, education and health., All of great importance to citizens. And broadband technologies can improve government efficiency and flexibility, can help increase availability and access to government services.

Private companies: For the company's broadband is a facilitator of applications and e-Business practices, creating new business opportunities and helping companies to achieve productivity gains based on improved access to information and transactions. Both companies and employees broadband communications are designed to diminish the importance of tracing by allowing the establishment of offices in small towns, rural or isolated and facilitating teleworking.

7. Programs and strategies for the ministry of national defense area and data communications

7.1. The transformation in communication and informatics

The transformation process in this area will focus on achieving and automation system C4I2SR Romanian army and at the same time will correlate and assist with objective of reshaping the structure of command and control and force structure. The system will facility and information network infrastructure to ensure a new approach to management information from a global architecture, service oriented performance in all areas of application (operational, administrative, logistical, medical, etc.) .

First, during the completion of the basic structures (2005-2007) effort was directed on achieving interoperability requirements in the field, in the deployable structures. In the same period, will complete the conceptual basis for Objective C42ISR systems and infrastructure to achieve new architecture command and control of the Romanian Army. By the end of this period was monitored and short-term objectives relating to the process of transformation and reorganization of units that are subordination specific field of Communications and IT activity.

During the operational phase of integration into NATO (2008-2015) will continue providing the level of interoperability in terms of scope, gradually, to the structures which have the target date at this time. In the years 2008 and 2009, attention has focused on achieving specific capabilities to the division headquarters deployable structures and its composition. Also, it will trigger and run the process of implementing the concepts in the field, developed and based on the previous stage. Meanwhile, intensified the process of making integrated information communication system and the Defense Ministry that will provide necessary support to exercise command and control at all levels in the country and in theaters of operations, and support appropriate planning processes and battle space management. This will facilitate networking with similar systems of NATO member countries of NATO and the European Union, to meet our commitments.

In the long term, between 2015-2025, in the stage of full integration into NATO and the European Union, long-term goal is to interconnect their systems and data communications with other entities at the national administrative and operational responsibilities in the field, synchronization with NATO transformation requirements in the field, under the concept of Network Enabled Capability. In the same period, will implement the requirements of interoperability in the field in all structures, regardless of their destination .

7.2. Programs and strategies

- Resizing and modernization of Communications Permanent (RTP) / National Military Communications Network (RMNC) to implement the feature network capability (NEC), extending and increasing its capacity in the theaters of military operations and representations in Brussels and Romania Mons;

- Making communications systems Command, Control, Communications, Computers, Information, Surveillance and Reconnaissance (C4I2SR), tactical radio networks with integrated services development and encrypt the information conveyed by radio equipment;
- Expand encrypted by videoconference, including theaters of operations and military representations of Romania;
- Making Information System of military action (SISAM) and computer subsystems major components: Logistics Information System (LIS), financial accounting Information System Platform (SIFCON), Management Information System Human Resources (SIMRU) Medical Information System (SIMED);
- Making other information systems components of Integrated Information System of the Ministry (SIIMAN), Distance Learning, Military Education Information System (SIMILEA);
- Achieving network information infrastructure to implement NEC Extension of private data of the Ministry of Defense, accredited to the level of "secrecy";
- Extension of the Defense Ministry data, accreditation at the "secret service" in the representative of Romania in Brussels and Mons and the staffs of the categories of forces;
- Making Book Management Center Integrated Information System of the National Defense.

System Encryption subscriber of RMNC.

Coordination of implementation of the objectives of force in its area of responsibility:

- Extended NGCS in the military units available to NATO and tactical networks achieve interoperability, the units with those of other countries belonging to NATO;
- modernization messaging;
- systems to support internal and external commands;
- communications and information systems security.

Satellite communications (Satcom) to forces deployed Making a radio center international links through to ensure links with all units SMG (sub-units, formations) sent international mission.

Preparation of officials from the Ministry of Defense in Informatics Accreditation has two centers for training in informatics ECDL public officials.

8. Programs and strategies of telecommunications service special on IT & C

Medium term development strategy and long-established policy of special telecommunications telecoms special and how to implement this policy in the national telecommunications environment.

8.1. Special telecommunications objectives

In setting specific telecommunications policy, the strategy seeks the following objectives:

- Providing the P2P communication services, the client (the profile and quality of service is continuously negotiable), as close to the beneficiary on a medium C4I2 compatible;
- Providing continuous connectivity for subscribers that require communication and computer facilities (computer interconnect computing) at national level;
- Providing an interface for access to infrastructure can absorb technological changes in computers, communications and information services;

- Creating an environment (support) design / operation based on standards and / or special methods (specific) implementation services.

Specific community special is that network subscribers:

- Expand the strategic environment, operational and tactical part operating in / organizations;
- Amend by their missions, political and technological developments;
- Dynamics services provided is flexible and stable point of view of the transmission, integrity and cost.

Adopted policy defines two priority areas are identified methods for achieving these goals:

- Unification requests Telecommunication state (the bandwidth required for various data services, voice and video) on a single backbone in the country;
- Providing connectivity portejata national network (the current beneficiaries of interconnections to a single bus) for locations of users;
- Unification applications depend on network flexibility;
- Providing network connectivity to sites of government agencies must ensure the individual needs of network security information for each beneficiary.

8.2. Mission Strategy

Special telecommunications strategy establishes the operating framework for a unified telecommunications infrastructure to meet long-term state, effectively and economically, the needs of special protected telecommunications voice, video and data to public authorities (as defined by lists of subscribers in the SNA and central government Local and nominated by the organic law of organization and functioning of the Special Telecommunication Service).

Since the telecommunications network is key for dignitaries and officials from the state is necessary, in addition to communication services, it should provide a measure of government support and support for the position of defense. System designed for these applications is organized hierarchical structure of C3I.

8.3. Specifications unified infrastructure

To have achieved their goals, in the network, objectives and it proposes Manager (Special Telecommunications Service) are:

- Provides communication platform for access to security resources in the SNA;
- Provides key network services for government agencies in SNA and public administration;
- Centralize access (authorization) to network services and data communications;
- Provides open interfaces for interconnectivity government agencies SNA and public administration;
- Provides continuous dynamic users need a special network.

8.4. Special infrastructure modernization policy

To upgrade communications infrastructure is increasing operational availability.

Network operator must assume responsibility for network services:

- Planning;
- Installation;
- Supervision;
- Development.

The objectives of modernization:

- Reduction of functional dependence to traders;
- Ensure rapid reconfiguration of network resources according to operational requirements;
- Develop a long-distance optimal topologies;

- Infrastructure development of mobile access to subscribers;
- Identification and use of alternative transport information (WLL, microwave, shortwave, satellite).

Developments to modernize:

- Ensure access to communications infrastructure the needs of the entity responsible for generating network, and recipients;
- Achieving critical core of special communications infrastructure to enable vital services to ensure continuity of telecommunications;
- Identify and use elements of alternative infrastructure (especially telecommunications state);
- Diversification of services (particularly broadband);
- Integration of common infrastructure services;
- Customizing subscribers (on the word customer);
- Increase communication privacy;
- Increased security of information and communication systems;
- Integration of mobile infrastructure with fixed networks;
- Integrated network unit.

Conclusion

Romania fully supports the EU acquis in telecommunications, postal and information technology in place on March 31, 2002 and did not request any transitional period or derogation.

Romania is ready to consider further development of the acquis and to proactively inform the Membership Conference or Association Council on implementing legislation and measures adopted to implement the new acquis or, if appropriate, on the difficulties that may arise the implementation of the new acquis.

Romania made with regard to this chapter, the information provided during the screening process and agree to continue their transmission by Member States of the European Union.

Romania has taken unilaterally on January 1, 2007 as a working hypothesis to conclude preparations for accession to the European Union.

Romania assumes the working basis for harmonization of national legislation four directives of the European Parliament and Council (Framework Directive, the Authorization Directive, Access Directive, Universal Service Directivaprivind), the European Parliament and Council Regulation no. 2887/2000 on unbundled local loop access, and the draft Commission Directive on competition pieteleserviciilor electronic communications, which are part of the package which establishes the new regulatory framework for electronic communications infrastructure and associated services. Since the national legislation adopted by the end of 2001 followed transposition Community acts underlying the old regulatory framework, the analysis of that legislation, for economy of expression, this position paper refers to directives and decisions included in package Regulations 1998.

References

1. Document revised position 2 of Romania, Chapter 19 - Telecommunications and Information Technology, Intergovernmental Conference on Accession to the European Union in March 2002.
2. Order of the Ministry of Communications and Information Technology no. 184/2004, on implementation of universal service in electronic communications sector (objective and appropriate measures will be implemented no later than 31/12/2012). 3. Decision on approval of the government strategy of broadband electronic communications development in Romania for the period 2009 to 2015, 2008.
3. The strategy of transforming the Romanian Armed Forces, ed. 2007
4. The strategy of medium and long term development of special telecommunications ed. 2002

POSTAL AND SHIPPING SERVICES IN USA - CRITICAL INFORMATION INFRASTRUCTURES

LTC. PhD. eng. Cezar VASILESCU

Executive Summary

> *"Critical Infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters".*[27]

The subject of this paper is information assurance issues regarding Postal Services and Shipping in United States of America as Critical Infrastructures (as defined in the USA Patriot Act). Since September 11, 2001, United States of America has followed a long march to get better homeland security. Virtually every nation has a national strategy for defending its homeland. It is a blueprint or concept for how that nation integrates its use of the instruments of national power in order to attain its defensive objectives. Virtually no nation other than the United States of America publicly promulgates and globally disseminates its approach, which the United States of America does by means of a Congressionally-mandated document known as the "National Strategy for Homeland Security". The purpose of this paper is to inform you about the standing of Postal and Shipping and its relationship with the global information infrastructure.

Current status. Postal Service is now on the way up to positive transformation and recovery after September 11 and anthrax crisis.

Legal. Postal and Shipping sector is considered officially a Critical Infrastructure starting with 2002 when the Homeland Security Act was released.

Stakeholders and Partners. The key stakeholder groups for Postal Service consist of Customers, Mail Service Providers, Industry Associations, Employees, Congress and Regulators, Competitors, Suppliers and Foreign posts.

Risks, Threats and Vulnerabilities. Risk assessment, risk mitigation, and evaluation and assessment as processes of risk management show the risk impact and recommend risk-reducing measures.

Information Technology. The Postal Service information system grants real-time information to provide more consistent information to customers about mail processing and delivery status. Tracking mail online is useful today but with a part of vulnerability.

Net Centricity. The Postal Service network will continue to provide customers with appropriate data and information.

Personal Assessment. Postal Service approach to computer security is comparable to what you see in the rest of the federal government and private sector. They are using a public-key infrastructure and digital certificates. They were one of the first government agencies to implement PKI in conjunction with the launch of PC Postage since 1999.

[27] United States of America Congress, (2001, October), Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

Conclusions. As a trusted and treasured national asset, the Postal Service faces a variety of security challenges which require aggressive investigative, preventive, and security responses.

Introduction

To protect United States of America's Critical Infrastructure in the new era becomes an extraordinary challenge, taking into account the complexity and wide opening type of society we met here and also seeing a big array of potential targets. United States of America's comprehensive plan to secure the homeland encompasses every level of government and the cooperation of the public and the private sector[28]. Moreover, America's Critical Infrastructure is in continuous change with the same speed the marketplace is changing. American Nation learned a terrible lesson on September 11. American soil is not immune to evil or cold-blooded enemies capable of mass murder and terror.[29]

American Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.[30]

Cyberspace is the nervous system of these infrastructures—the control system of the country. Cyberspace comprises interconnected computers, servers, routers, switches, and fiber optic cables that make the critical infrastructures work. Thus, the healthy functioning of cyberspace is essential to the economy and national security.

Unfortunately, recent events have highlighted the existence of cyberspace vulnerabilities and the fact that malicious actors seek to exploit them. Therefore we can see that the United States of America has a stated vision in protecting Critical Infrastructure and Key Assets.

National USA Vision

> *"The United States will forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructure and key assets from terrorist attack. Our country will continue to take immediate and decisive action to protect assets and systems that could be attacked with catastrophic consequences. We will establish a single office within the Department of Homeland Security to work with the federal departments and agencies, state and local governments, and the private sector to implement a comprehensive national plan to protect critical infrastructure and key assets. The national infrastructure protection plan will organize the complementary efforts of government and private institutions to raise security over the long term to levels appropriate to each target's vulnerability and criticality. The federal government will work to create an environment in which state, local, and private entities can best protect the infrastructure they control. The Department of Homeland Security will develop the best modeling and simulation tools to understand how our increasingly complex and connected infrastructures behave, and to shape effective protection and response options. The Department of Homeland Security will develop and coordinate implementation of tiered protective measures that can be tailored to the target and rapidly adjusted to the threat. The Department of*

[28] The White House (2002, September), *The National Security Strategy of the United States of America*, Washington, DC, p. 6

[29] Office of Homeland Security, (2002, July), *National Strategy for Homeland Security*, Washington, DC: U.S. Government Printing Office, p. 1

[30] Office of Homeland Security, (2003, February), *The National Strategy to Secure Cyberspace*, Washington, DC: U.S. Government Printing Office, p. 1

Homeland Security, working through the Department of State, will foster international cooperation to protect shared and interconnected infrastructure".[31]

Commercial Postal and Shipping companies are in the process of organizing themselves as a Critical Infrastructure to identify and address specific protection issues within their industry. While the United States Postal Service (USPS) has worked with many of these companies to address critical infrastructure protection issues, there is further work to be done in this area.

Assisted by USPS, the Department of Homeland Security will engage the industry's major players in an effective dialogue to address critical infrastructure protection issues that cross the entire sector. USPS has identified five areas of concern for the postal system:

- Points of entry and locations of key facilities;
- The mail's chain of custody;
- Unique constitutional and legal issues;
- Interagency coordination; and
- The ability to respond in emergency situations.

The fact that there are numerous points of entry into the postal system complicates its protection. Compounding this problem is the fact that these access points are geographically dispersed, including the multitude of postal drop boxes nationwide. Effective, affordable technology to scan mail and provide early warning of potential hazards is under current evaluation. The location of many key postal service facilities can also aggravate risk-management challenges. Several major USPS facilities are collocated with or adjacent to other government agencies or major transportation hubs. Relocating these facilities to mitigate risk is often constrained by limited resources, a lack of available, alternative sites, and other pressing local imperatives.

Current Status

Americans depend deeply on the Postal and Shipping sector. Each day, they place more than two-thirds of a billion pieces of mail into the US postal system; and each day more than 300,000 city and rural postal carriers deliver that mail to more than 137,000,000 delivery addresses nationwide. In all, the vast network operated by the United States Postal Service (USPS) consists of a headquarters in Washington, D.C., tens of thousands of postal facilities nationwide, and hundreds of thousands of official drop-box locations. USPS employs more than 749,000 full-time personnel in rural and urban locations across the country and generates more than $60 billion in revenues each year.

Together, USPS and private-industry mailing and shipping revenues exceed $200 billion annually. The postal system is highly dependent on and interconnected with other key infrastructure systems, especially the transportation system. USPS depends on a transportation fleet composed of both service-owned and contactor-operated vehicles and equipment. Mail also travels daily by commercial aircraft, truck, railroad, and ship. Because of these dependencies, many key postal facilities are collocated with other transportation modalities at various points across the United States of America. The expansiveness of the national postal facilities network presents a significant, direct protection challenge. Additionally, the size and pervasiveness of the system as a whole has important implications in terms of the potential secondary effects of a malicious attack.

The Fall 2001 anthrax attacks underscore this concern. In addition to localized mail stoppages across the United States of America, the tainted mail caused widespread anxiety that translated into significant economic impact. Historically, the American public has placed great trust, confidence and reliance on the integrity of the postal sector. This trust and confidence are

[31] Office of Homeland Security, (2002, July), *National Strategy for Homeland Security,* Washington, DC: U.S. Government Printing Office, p. 31

at risk when the public considers the mail service to be a potential threat to its health and safety. Consequently, USPS continues to focus on the specific protection issues facing its sector and is working diligently to find appropriate solutions to increase postal security without hampering its ability to provide fast, reliable mail service.

United States Postal Service is in its continuous transformation. In the almost 4 years since publication of the first *Transformation Plan*, in 2002, the Postal Service has delivered on its promise of focus and results. The new transformation plan, *Strategic Transformation Plan 2006–2010* builds on the foundation of the earlier plan and continues its momentum.

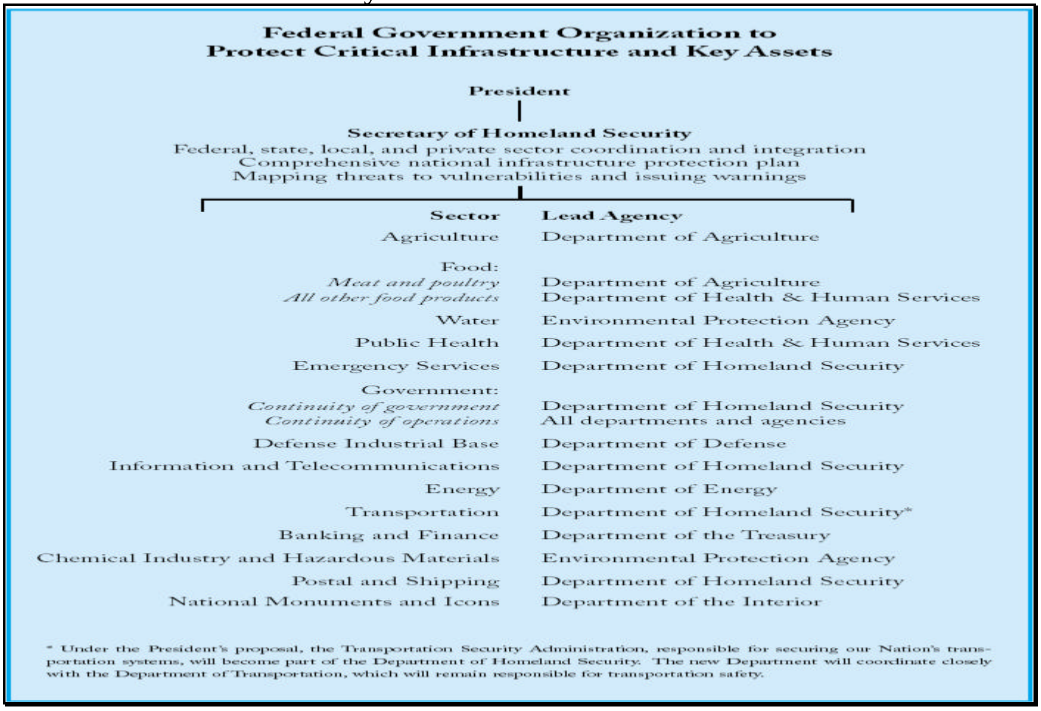
In 2002 the Postal Service was emerging from the multiple shocks of an economic slowdown, September 11, and the anthrax attacks. Mail volume fell, and America's confidence in the mail was undermined. The *2002 Transformation Plan* became the roadmap to recovery. It reinstalled confidence among postal employees and set challenging but achievable targets in service and cost management.

Today, service is the best it has ever been for all classes of mail. Productivity growth has been steady and strong. More than 80,000 jobs have been reduced through attrition and cumulative savings of at least $13 billion will have been realized by the end of 2005. Better service and stable rates have attracted new business. Direct mail volume is up 10 percent in 2 years. So far, at least, increases in direct mail revenue have offset losses caused by competitive, technological changes that are moving bills and payments online.

Legal

The US government’s definition of “critical infrastructure” has evolved over the years, and at any given time has left considerable room for interpretation. Furthermore, since the 1980's, the number of sectors included under that definition has generally expanded from the most basic public works to a much broader set of economic, defense, government, social and institutional facilities, as illustrated in Appendix A. The list may continue to evolve and grow as economic changes or geopolitical developments influence homeland security policy. Postal and Shipping sector pops up in the category of “critical” in 2002 with the Homeland Security Act.

According to this Act the domain of Postal and Shipping is given in the accountability to the Department of Homeland Security.



Federal Government Organization to Protect Critical Infrastructure and Key Assets

President

Secretary of Homeland Security
Federal, state, local, and private sector coordination and integration
Comprehensive national infrastructure protection plan
Mapping threats to vulnerabilities and issuing warnings

Sector	**Lead Agency**
Agriculture	Department of Agriculture
Food:	
Meat and poultry	Department of Agriculture
All other food products	Department of Health & Human Services
Water	Environmental Protection Agency
Public Health	Department of Health & Human Services
Emergency Services	Department of Homeland Security
Government:	
Continuity of government	Department of Homeland Security
Continuity of operations	All departments and agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy	Department of Energy
Transportation	Department of Homeland Security*
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

* Under the President's proposal, the Transportation Security Administration, responsible for securing our Nation's transportation systems, will become part of the Department of Homeland Security. The new Department will coordinate closely with the Department of Transportation, which will remain responsible for transportation safety.

Figure 1: Federal Government Organization to Protect Critical Infrastructure[32]

United States Postal Service is established, as an independent establishment of the executive branch of the Government of the United States for postal services. It's the law, is the United States Code.

The current structure of USPS was set by the Postal Reorganization Act (PRA) of 1970. Before passage of this Act, the Post Office was an executive branch department and Congress was heavily involved in such basic decisions as postage rates, annual wage increases, patronage appointment of local postmasters, and selection of commemorative stamp issues. Postage rates were set by law, and because raising them was politically difficult, the substantial annual postal deficit – often as much as 25% of costs – was covered by appropriated funds. Postal workers engaged in a disruptive and illegal strike in 1970, forcing Congress to address the state of the enterprise.

The basic policy of Postal Service consists of:

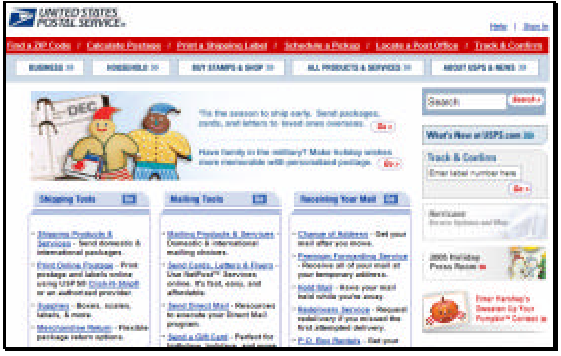
- The United States Postal Service shall be operated as a basic and fundamental service provided to the people by the Government of the United States of America, authorized by the Constitution, created by Act of Congress, and supported by the people. The Postal Service shall have as its basic function the obligation to provide postal services to bind the Nation together through the personal, educational, literary, and business correspondence of the people. It shall provide prompt, reliable, and efficient services to patrons in all areas and shall render postal services to all communities.
- The Postal Service shall provide a maximum degree of effective and regular postal services to rural areas, communities, and small towns where post offices are not self-sustaining. No small post office shall be closed solely for operating at a deficit, it being the specific intent of the Congress that effective services be insured to residents of both urban and rural communities.
- As an employer, the Postal Service shall achieve and maintain compensation for its officers and employees comparable to the rates and types of compensation paid in the private sector of the economy of the United States of America.
- Postal rates shall be established to apportion the costs of all postal operations to all users of the mail on a fair and equitable basis.
- In determining all policies for postal services, the Postal Service shall give the highest consideration to the requirement for the most expeditious collection, transportation, and delivery of important letter mail.
- In selecting modes of transportation, the Postal Service shall give highest consideration to the prompt and economical delivery of all mail and shall make a fair and equitable distribution of mail business to carriers providing similar modes of transportation services to the Postal Service.
- In planning and building new postal facilities, the Postal Service shall emphasize the need for facilities and equipment designed to create desirable working conditions for its officers and employees, a maximum degree of convenience for efficient postal services, proper access to existing and future air and surface transportation facilities, and control of costs to the Postal Service.

Federal Agencies and Commissions:

- Postal Rate Commission;

[32] Source: Office of Homeland Security, (2002, July), *National Strategy for Homeland Security*, Washington, DC: U.S. Government Printing Office, p. 32

- United States Postal Service (USPS).



Stakeholders and Partners

There are many reasons why the Postal Service should solicit stakeholder input as part of its development process. First, it is required by federal law. The Government Performance and Results Act (GPRA) of 1993 require agencies to engage with stakeholders to identify the impact of agency actions, and to solicit their thoughts, opinions, and ideas as business activities and strategic plans are generated. Second, the Postal Service understands the impact of stakeholder involvement in the past successes and recognizes that continued stakeholder involvement is needed. It makes fundamental business sense to solicit ideas from all constituencies with an interest in a robust and healthy Postal Service.

The postal stakeholder community is a very diverse and sometimes divided community of interests. The Postal Service devotes significant resources to work with stakeholders to better understand the various groups, propose and evaluate reasonable compromises among them, and to assess the effectiveness of postal programs, products, and services.

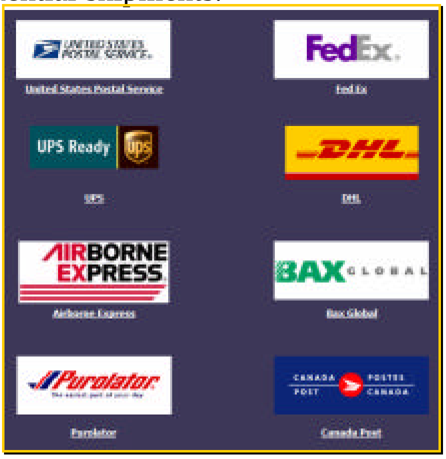
Certain requirements do tend to emerge consistently from key stakeholder groups:

- *Customers* - Timely, reliable, and accurate delivery; products and services that meet needs; responsive, knowledgeable, and courteous employees; convenient access and ease of use; timely, reliable, and accurate information; confidence, security and trust; affordable, reasonable prices; consumer and information protection.
- *Mail Service Providers, Industry Associations* - Effective consultation and responsive problem solving; ease of use and payment; seamless integration; growth and profit opportunities; reasonable standards consistently applied; investments in infrastructure; lowest possible prices.
- *Employees* - Fair employment practices; competitive wages and benefits; safe and secure workplace; relevant and effective training; opportunity to contribute; fair and effective supervision; open and honest communication; development opportunities and job security; recognition for performance.
- *Congress and Regulators* - Universal service; adherence to legislative and regulatory requirements; transparency; effective management and control systems; effective consultation and response; public services; community and corporate responsibility; high ethical standards.
- *Competitors* - Level playing field; fair competition.

- *Suppliers* - Fair and efficient purchasing processes; effective consultation; timely, relevant and accurate information; profit opportunities.
- *Foreign posts* - Effective and efficient mail exchange.

In the private sector there are significant competitors in shipping, logistic management and supply chain management with worldwide presence. Three of these are FedEx, UPS and DHL.

FedEx is a network of companies that share a rich heritage of innovation and industry leadership. While each company has a unique history, collectively they exhibit the "absolutely, positively" dedication to providing specialized solutions for shipping, information and global trade. Originally called FDX Corp., FedEx Corp. was formed in January 1998 with the acquisition of Caliber System Inc. Through this and future purchases, FedEx sought to build on the strength of its famous express delivery service and create a more diversified company that included a portfolio of different but related businesses. In September 2004, FedEx Corp. acquired Parcel Direct, a leading parcel consolidator, and later re-branded it FedEx SmartPost. The acquisition complements the FedEx alliance with the US Postal Service and provides customers in the e-tail and catalog segments with a proven, cost-effective solution for low-weight, less time-sensitive residential shipments.



UPS was founded in 1907 as a messenger company in the United States and has grown into a $36 billion corporation by clearly focusing on the goal of enabling commerce around the globe, package delivery and providing specialized transportation and logistics services globally. Every day, they manage the flow of goods, funds, and information in more than 200 countries and territories worldwide.

DHL is a company that has built the world's premier global delivery network by trailblazing express shipping in one country after another in roughly 35 years. DHL is the global market leader of the international express and logistics industry.

Risks, Threats and Vulnerabilities

Many of the American nation’s critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks.

Cyber attacks can burst onto the American nation’s networks with little or no warning and spread so fast that many victims never have a chance to hear the alarms. Even with forewarning, they likely would not have had the time, knowledge, or tools needed to protect themselves. In some cases creating defenses against these attacks would have taken days. A key lesson derived from these and other such cyber attacks is that organizations that rely on networked computer systems must take proactive steps to identify and remedy their vulnerabilities, rather than waiting for an attacker to be stopped or until alerted of an impending attack.

Managing threat and reducing vulnerability in cyberspace is a particularly complex challenge because of the number and range of different types of users. Cyberspace security requires action on *multiple levels* and by a diverse group of actors because literally hundreds of millions of devices are interconnected by a network of networks. The problem of cyberspace security can be best addressed on five levels[33]:

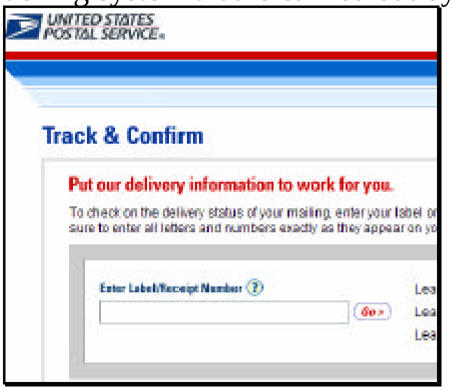
- Home user/Small business;
- Large enterprises;
- Critical sector/Infrastructure;
- National issues and vulnerabilities;
- Global.

Postal and Shipping sector can be related at the last three levels, surprising but real becoming addressing the global level.

The impact of a successful attack depends upon the value of the target. If the impact of a security failure is small, allocation of inadequate resources to security systems and processes can also be small[34]. For example, the loss of some routine office correspondence might occasion little concern. Failure of the entire CONUS postal service could be devastating to the American nation. Obviously, as the value of the target rises, the impact of a successful attack goes up as well, and so our sense of risk increases.

Why is electronic information vulnerable? The primary reason is that it is computer readable and thus much more vulnerable to automated search than is intercepted voice or postal mail transmissions. Once the information is collected (e.g., through an existing wiretap or a protocol analyzer on an Internet router), it is relatively simple for computers to search streams of electronic information for word combinations of interest (e.g., "USPS," "en-route," and "tracking" in the same message)[35].

Tracking services provide detailed information. You will see the item scanned at acceptance, as it travels, and when it is delivered. Services that confirm delivery are designed to be a low cost alternative to full tracking. Instead of seeing the acceptance information and updated scans as the item is en-route delivery confirmation services provide assurance of delivery or of attempted delivery. But is tracking secure and non-vulnerable? Let's take the tracking system that is carried out by United States Postal Service.

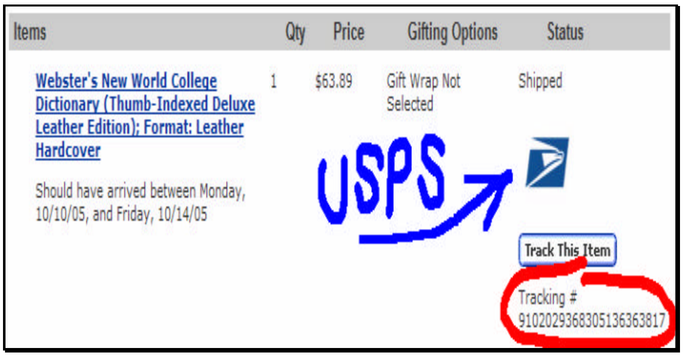


Track & Confirm

Put our delivery information to work for you.

To check on the delivery status of your mailing, enter your label or
sure to enter all letters and numbers exactly as they appear on yo

Enter Label/Receipt Number ?



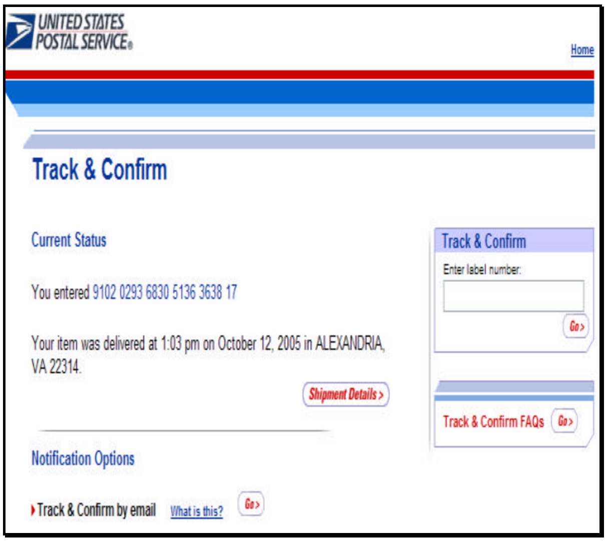
Items	Qty	Price	Gifting Options	Status
Webster's New World College Dictionary (Thumb-Indexed Deluxe Leather Edition); Format: Leather Hardcover Should have arrived between Monday, 10/10/05, and Friday, 10/14/05	1	$63.89	Gift Wrap Not Selected	Shipped Track This Item Tracking # 9102029368305136363817

One needs only a label/receipt number to track a package. This is a 22 digits number and easily to obtain or determine. It can be done either determining by random method or directly from the vendor's web-site. In this case the vendor is Wal*Mart and the carrier USPS.

[33] Office of Homeland Security, (2003, February), *The National Strategy to Secure Cyberspace*, Washington, DC: U.S. Government Printing Office, p. 7

[34] Ryan, D.J. and Ryan J.J.C.H. (1995, December), *Risk Management and Information Security*. In the 11th Computer Security Applications Conference, New Orleans. Retrieved on October 5, 2005 from http://www.danjryan.com/Risk.htm

[35] Dam, K.W. and Lin H.S. (1996), *Cryptography's Role in Securing the Information Society*, Washington, DC, National Academies Press, p. 31



Track & Confirm

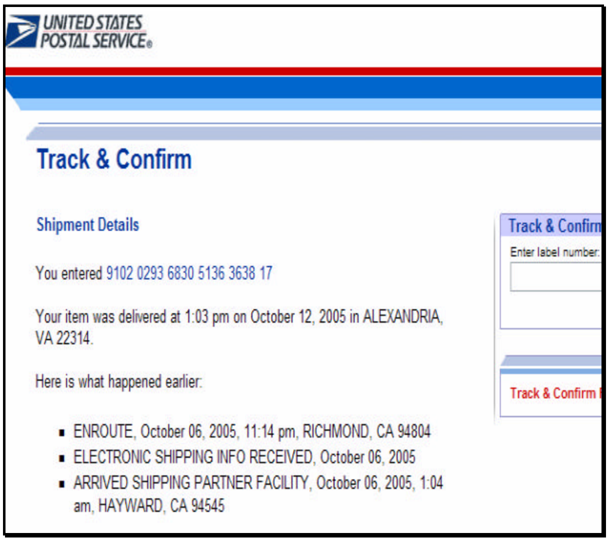
Current Status

You entered 9102 0293 6830 5136 3638 17

Your item was delivered at 1:03 pm on October 12, 2005 in ALEXANDRIA, VA 22314.

Notification Options

Track & Confirm by email What is this?



Track & Confirm

Shipment Details

You entered 9102 0293 6830 5136 3638 17

Your item was delivered at 1:03 pm on October 12, 2005 in ALEXANDRIA, VA 22314.

Here is what happened earlier:

- ENROUTE, October 06, 2005, 11:14 pm, RICHMOND, CA 94804
- ELECTRONIC SHIPPING INFO RECEIVED, October 06, 2005
- ARRIVED SHIPPING PARTNER FACILITY, October 06, 2005, 1:04 am, HAYWARD, CA 94545

Detailed information could be obtained by one who possesses only 22 digits tracking number.

Information Technology

For the postal and shipping industry, the question is not whether change will come, but how quickly new challenges and opportunities will arrive. Clearly, mailers who are prepared for new initiatives before they are launched stand to gain the most. Conversely, mailers who constantly struggle to "catch up" miss golden opportunities to significantly reduce their costs, improve service to their customers, market more effectively to prospects, and get a leg up on their competitors. The choice of a mail automation solution and vendor clearly does make a difference, and prospective buyers should base their decision not only on how effectively the solution and vendor function in the current environment, but on how well they anticipate and respond to arising new rules and opportunities.

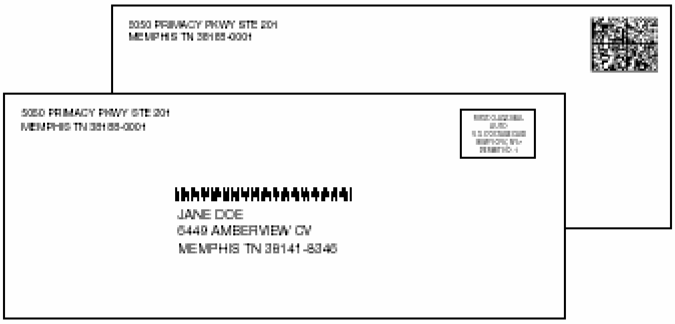
Many, if not most, mail automation vendors are ready for the as called "software/vendor readiness" indicators. But only a fraction of the companies are highly readiness. The more indicators achieved, the higher the likelihood the vendor and its software are well suited to the rapidly changing mailing environment. Besides benefiting themselves, businesses that make strategically sound vendor/software choices contribute to the overall success of the mailing industry. Operating more efficiently with less manual intervention means deeper cost reductions, both for mailers and the USPS, which in turn translates to decreased potential for rate increases. At the same time, mail is delivered on a timelier basis and with greater precision, elevating the general status of mailers in the minds of recipients and the public at large.

Presort Accuracy Validation and Evaluation (PAVE) certification

The United States Postal Service, in cooperation with the mailing industry, has developed a process of evaluating presort software known as Presort Accuracy Validation and Evaluation (PAVE) certification. The process is available only to software and hardware manufacturers who actually develop presort software or manufacture presorting equipment either for retail or for internal use. PAVE provides a common platform to measure the quality of presort products and determines their accuracy in sorting address files according to the requirements set forth in the *Domestic Mail Manual* (DMM).

The purpose of PAVE is to improve the accuracy of presorted mailings, thereby improving the flow of your mail. There are two levels of certification: Gold and Standard. Products that achieve Standard certification participate in an extensive manual review of all documentation. The *USPS Qualification Report*, PS forms, bar-coded tray and sack tags, and other user documentation are analyzed for compliance with DMM regulations. Products that achieve Gold certification participate in the same extensive manual review of documentation but are also electronically analyzed. Electronic evaluation allows for in-depth examination for each piece of the test mailing to ensure compliance, particularly with sequencing routines, optional endorsement lines, numeric translations for bar-coded container tags, and other elements of a mailing that are not easily inspected via the manual process. For testing purposes, PAVE supplies software developers with address files that include all necessary information pertaining to each address.

The PAVE certification process verifies only the sort accuracy of the software. It does not verify addressing information or the assignment of addressing components. Through the testing process, addressing components such as, In-County eligibility, Zip+4, and eLOT are provided to the developer. While some presort products can and do provide this information as a value added service, many presort programs rely upon the end user to furnish accurate address components. PAVE does not verify where or how software companies acquire the aforementioned information, it is the ultimate responsibility of the mailer to verify that the address information is correct. Incorrect components could effect the proper outcome of presort and the mailer could be subject to additional postage fees. The PAVE Certified Products List contains products that have passed the rigorous testing procedures of the PAVE program. The list is organized alphabetically by company name. Each product's listing includes sales contact information and indicates the certified presort categories, presort-related options supported, hardware, software platforms, and price range. Some products also provide postage statement facsimiles, bar-coded tray/sack tags, and additional documentation for the mailer's use.



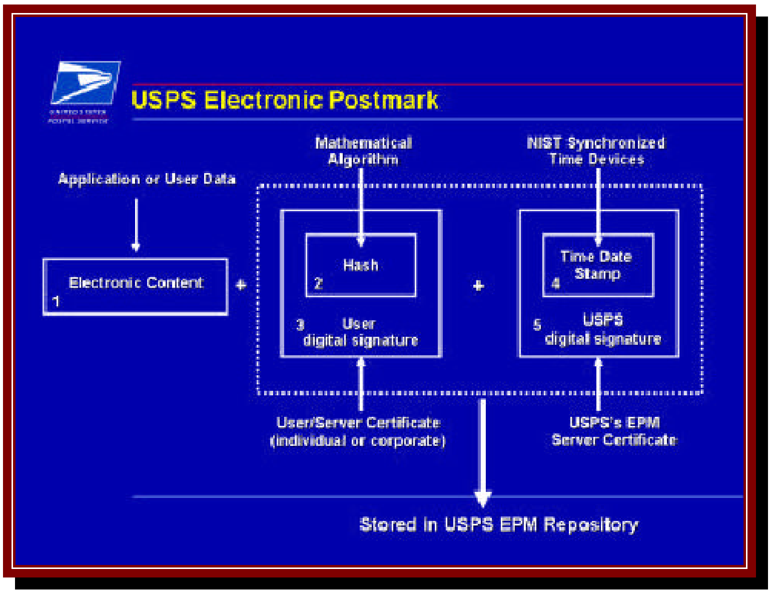
The 4-state barcode (front envelope) includes sorting, tracking, service, and customer information — all in a single code. The information-based indicia (in the "stamp" area of the rear envelope) provide secure postage for Internet and meter users. It also offers the future capability to include service and tracking information. The Postal Service developed and set standards for these codes to dramatically increase the amount of information carried while requiring minimal space on the envelope.

USPS Electronic Postmark

The advent of the Internet increased the need for efficient communication of electronic information with the same level of trust and value that the public has come to expect from the USPS in the physical environment. The USPS Electronic Postmark (USPS EPM) was created to facilitate secure electronic communication for government and commercial systems and has the potential to strengthen the security, privacy, and productivity of communication in the nation's electronic future.

The USPS EPM is a web-based security service. It includes trusted time stamps and content authentication technology, as well as aspects of non-repudiation. The trusted time stamps are derived from the National Institute of Standards and Technology (NIST), the official US source of time for commerce.

The USPS EPM service combines trusted time stamps with content authentication technology. This combination proves document authenticity when a resulting USPS EPM is associated with a document or transaction that can later be verified using the USPS EPM repository. Finally, the service enables digital signing applications by including support for digital certificates.



USPS Electronic Postmark

Application or User Data

Electronic Content 1

+

Mathematical Algorithm

Hash 2

3 User digital signature

+

NIST Synchronized Time Devices

Time Date Stamp 4

5 USPS digital signature

User/Server Certificate (individual or corporate)

USPS's EPM Server Certificate

Stored in USPS EPM Repository

The combination of these technologies maintained in the USPS EPM repository provides third party evidence to support non-repudiation of electronic transactions and is designed to detect the fraudulent tampering or inadvertent altering of electronic data. Additionally, the USPS EPM supports applications so that they can comply with the ESIGN legislation (Public Law 106-229 – enacted in June 2000) which made electronic signatures the legal equivalent of their paper counterparts in many situations.

Net Centricity

To better compete in the package marketplace, the Postal Service will increase the capability for customers to track packages. For most of its package services the Postal Service now provides confirmation of delivery only (Delivery Confirmation and Signature Confirmation). However, customers expect more information about package status; they want to know when a package enters the postal network, where it is en-route, when delivery is expected, and when delivery occurs. The Postal Service will work with customers and partners to determine how best to address these requirements.

Offering this expanded level of visibility will require a tracking and distribution barcode on all packages and network coverage of automated package sorting equipment to ensure that cost-effective passive scans of packages are obtained. In 2006 the Postal Service will deploy 300,000 Intelligent Mail devices (IMDs) to help collect information on mail. The IMD is a hand-held scanner with the capability to read current barcodes as well as the newer 4-state barcode and information-based indicia. These features, along with the IMD's electronic signature capture, will supplement in-process scanning to make more mail visible from the time a piece is received until it is delivered. The ultimate goal is to better integrate postal data with customer information, extending visibility even further — starting with creation of the mail piece all the way through to delivery. The Postal Service will continue to evaluate the potential of evolving technology such as radio frequency identification devices (RFID) to collect information.

Personal Assessment

The Internet has changed the mission and goals of the Postal Service. Their electronic-business goals promote the use of the best available technology to enhance the value, availability and accessibility of all the postal services. The information platform has multiple components, which are interfaced with one another. They are streamlining the whole information system to provide better information to customers and actionable information to employees in their delivery, transportation, retailing and processing operations.

Transportation information system grants real-time information to provide more consistent information to customers about mail processing and delivery status. Tracking mail online is useful today but with a part of vulnerability.

Carriers today carry portable terminals with them to record delivery of several products. It is anticipated that enhancing this technology in the future to include communications functions, and ultimately to turn the device into each carrier's PC.

One of the most significant challenges is the issue of scale. USPS web site is very active because people are always looking for ZIP codes, post office locations and the like.

Postal Service approach to computer security is comparable to what you see in the rest of the federal government and private sector. They are using a public-key infrastructure and digital certificates. They were one of the first government agencies to implement PKI in conjunction with the launch of PC Postage since 1999.

Conclusions

The Postal Service's commitment to improved service continues with protecting the mail, employees, and customers. As a trusted and treasured national asset, the Postal Service faces a variety of security challenges which require aggressive investigative, preventive, and security responses. The Postal Service will continue to align its resources to provide vital services that secure end-to-end delivery of mail, protect employees in their work environment, protect the Postal Service infrastructure, and protect and educate consumers through fraud awareness initiatives. The Postal Service will work collaboratively with internal and external groups to ensure new postal products and services are secure, thus maintaining customers' confidence in the mail and satisfying their personal and business needs.

Bibliography

- The White House (2002, September), *The National Security Strategy of the United States of America*, Washington, DC
- Office of Homeland Security (2002, July), *National Strategy for Homeland Security*, Washington, DC: U.S. Government Printing Office, pp. 29-46, 55-62
- Office of Homeland Security (2003, February), *The National Strategy to Secure Cyberspace*, Washington, DC: U.S. Government Printing Office, 13-17, 19-52
- Office of Homeland Security (2003, February), *The Physical Protection of Critical Infrastructures and Key Assets,* Washington, DC: U.S. Government Printing Office, 5-15, 67-69
- Office of Homeland Security (2003, December), *Homeland Security Presidential Directive/HPSD-7*, Washington, DC
- United States of America Congress (2001, October), *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, Washington, DC
- United States of America Congress (1993, January), *Government Performance and Results Act of 1993*, Washington, DC
- United States Postal Service Strategic Transformation Plan 2006-2010 (2005, September) Retrieved on October 12, 2005 from http://www.usps.com/strategicplanning/stp2006_2010/contents.htm
- Moteff, J. and Parfomak, P. (2004, October), CRS Report for Congress – Critical Infrastructure and Key Assets: Definition and Identification. Retrieved on October 12, 2005 from http://www.fas.org/sgp/crs/RL32631.pdf
- Schneider, F.B. (EDT) (1999), *Trust in Cyberspace*, Washington, Nat'l. Academies Pr.

- Dam, K.W. and Lin H.S. (1996), *Cryptography's Role in Securing the Information Society*, Washington, DC, National Academies Press
- Ryan, D.J. and Ryan J.J.C.H. (1995, December), *Risk Management and Information Security.* In the 11th Computer Security Applications Conference, New Orleans. Retrieved on October 5, 2005 from http://www.danjryan.com/Risk.htm

PROTECTING THE PRIVACY OF PERSONAL HEALTH INFORMATION

LTC. PhD. eng. Cezar VASILESCU

ABSTRACT

The purpose of this paper is to discuss the impact of Information Assurance (IA) on the Public Health sector of America. It will provide a critical analysis of the Public Health care sectors infrastructure and relate the impact of Information Technology (IT) and security issues associated with the same to the sector. The Department of Homeland Security (DHS) has identified Public Health as one of the nation's critical infrastructures and key asset along with agriculture and food, water, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.

The analysis will provide details on how the five attributes of information assurance (confidentiality, integrity, availability, authentication, and non-repudiation) will be applied to protecting vital personal medical data as it relates to the Public Health sector. More directly, the analysis is going to provide insight to the governing policies and regulations that apply to "Protecting the Privacy of Personal Health Information" through the use and application of the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Information assurance disciplines and HIPAA rules will be outlined to show the effects they have on the nation's Public Health sector. Information Assurance products, procedures and policies will be described as they relate to Public Health threats, vulnerabilities, mitigation and risk assessment or management decisions, as they apply to each area. Recently, several natural catastrophes and the probability of a Pandemic have caused the Public Health administrator to review internal processes and procedures. In addition, the attacks on September 11, 2001, to strategic areas in America to include the Pentagon and the financial district of New York have given cause to emphasize security from all perspectives. Because Information Assurance is an evolving subject there is now a need to include this strategy as an important element in security planning.

In conclusion, this analysis will address the importance of Information Technology as it applies to connecting the Public Health sector world wide through the use on the National Health Information Infrastructure initiative using networked systems. It will detail the importance of having a well thought out strategic plan. As well as, it will ensure the goals and objectives of this critical and vital infrastructure measures up to the outcome of providing Health service, and products that are kept private and secure, yet accessible upon demand.

1. INTRODUCTION

In the last decades USA is operating under a state of alert. It has been compromised by those that have little or no regard to this nation's value; or respect for its democracy. The terrorist attacks on September 11, 2001, caused a temporary disruption to the country's civil liberties and its economic base. The attack however did not cause this nation to stop operating, but rather, it brought the nation together across public and private sectors. It unveiled the need for the leaders of this great nation to put in place measures that would attempt to prevent such an attack from ever occurring again. Unfortunately, the terrorists underestimated the nations resolve, and the fact that it would not take corrective action to protect its critical infrastructures.

On that fatal Tuesday morning the nations Public Health system was put to the test. The first responders were hindered significantly by the loss of communication network lines. The local hospitals were not sufficiently staffed or prepared to receive the vast number of causalities and injures that were filing into their emergency rooms. Traffic flows were disrupted and in some areas even came to a stand still. Airports were temporarily closed, and many financial transactions were restricted or could not be completed at all. This was a real eye opener that the nation's critical assets were not independent of each other, but rather interrelated and must be protected as an entire enterprise. The attack on the World Trade Center towers in New York, and the Pentagon in Arlington VA., were strategically planned to demonstrate how vulnerable many of our Nation's key assets were as targets of penetration and destruction. This attack had a direct impact on several of the nation's critical infrastructures and demanded immediate attention and action.

"As a result, on October 8, 2001, the President of the United States established the Office of Homeland Security within the White House, and as its first responsibility, directed it to produce the first National Strategy for Homeland Security. The purpose of this Strategy is to mobilize and organize our Nation to secure the U.S. homeland from terrorist attacks. During the next two years, there were several national strategic plans written to deter acts of terrorism and protect our key assets"[36] The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets was produced soon after the attacks, and identified several major sectors requiring protection such as agriculture and food, water, public health, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Principles and efforts that are vital to the national security, governance, public health and safety, economy, and public confidence are what make protecting these critical infrastructures so important to this country. Of these critical infrastructures, the focal point for this critical analysis is the Public Health sector.

2. SCOPE

This white paper is going to provide a critical analysis on the importance of Information Assurance as it relates to the critical infrastructure protection in the Public Health sector. It will discuss how the use of IT will align and connect public and private health systems, from both the local and international perspective through the use of the National Health Information Infrastructure initiative. It will show how private agencies along with federal, state and local government entities must partnership together to ensure proper resources are being invested to guard against physical vulnerabilities that may pose a threat to the Nations' core infrastructures and the public health sector. Being alert to health threats and imposing necessary preventive measures for those threats that are present as a result of movement throughout airports, ground travel and seaports in no longer enough. Public Health caregivers must be prepared to take action immediately upon detection or the presence of any such threat, and pass that knowledge on to other shared facilities, or health care providers. Being able to share public health information electronically has become the nation's number one priority to meet the objective of data sharing. It is vital that information is received in real time and in some cases *just in time* to prevent outbreaks or the spread of contagious diseases.

However, once we decide to use the internet and other electronic means to share databases we must become cognizant of cyberspace security and methods to prevent malicious intrusions. The nation is living in the global information era, and cyber terrorism can be as destructive with the intrusion of a network as flying an airplane into the side of a building.

[36] Office of Homeland Security, National Strategy for Homeland Security, July 2002.

Nothing should be taken for granted, and stakeholders of the private and public sectors must take a proactive role in providing safeguards to protect citizen's health information while moving forward into the 21st century using information technology.

It is unknown what assets within the Nation's Critical Infrastructure will be the target of the next terrorist attack, or even when and where the next attack will take place. However, this uncertainty gives rise to concerns as to whether effective measures have been taken to identify potential threats and whether proper protections have been put in place to minimize or prevent serious loss. Have leaders conducted the proper risk analysis and assessments and implemented proper procedures to mitigate the least amount of impact and cost to the organization or private stakeholders?

Information Technology is the mechanism that will connect health care providers, records management, private and public health facilities and general users together. It reaches around the world and must maintain structural and data integrity. This paper will provide methodology, policy, and procedures that will yield that outcome. As more information is maintained and stored electronically, the more important it becomes to impose measures that will detect, protect and correct this data. Health records are among the most sensitive data that are acquired, used, and disclosed by government and the private sector. Health information reveals a great deal about an individuals personal facts and this information must be kept confidential and safe. Security safeguards, policies and procedures will ensure medical information moves throughout the internet in a timely, efficiently and protected manner. There is an increased potential for information to be compromised as the nation develops a national health information infrastructure, which would be required to move to a computerized system of sharing. This technological advancement will present significant risks to individual privacy and must be addressed.

3. ORGANIZATIONAL GOVERNANCE

Under the direction of the President, the Department of Homeland Security (DHS) was created uniting 22 plus federal entities with the common purpose of improving homeland security. Per this agreement the Secretary of DHS acts as the President's principal policy advisory and coordinating agent for major interagency policy issues related to Homeland Security, including the critical infrastructure and key assets protection mission area.[37] Operating under this structure, each protected critical infrastructure and key asset is aligned with a lead agency at the cabinet level where one such cabinet exists. The Public Health sector fits that criteria and falls under the lead agency of the Department of Health and Human Services (HHS). Within the HHS chain of command the Assistant Secretary of Health reports through the Deputy Secretary to the Secretary of Health and Human Services. The Office for Civil Rights (OCR) has been delegated the responsibility to manage the Information Technology, Information Assurance, and Privacy Rules for HHS. Health information privacy provides the foundation for this report's theme, *"Protecting the Privacy of Personal Health Information"*.

The Department of Health and Human Services is required to uphold all existing regulations enacted by Congress, OMB, and Presidential Directives. Congress has also called on HHS to issue a patient privacy protection regulation which has resulted in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA includes provisions designed to encourage electronic transactions and also required new safeguards to protect the security, privacy, and confidentiality of health information. The final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g. enrollment, billing and eligibility verifications) electronically".[38]

[37] The National Security Strategy of the United States of America, September 2002.

[38] http://irm.cit.nih.gov/policy/DHHS_Seclev.tml

4. STAKEHOLDERS AND PARTNERS

"The Public Health critical infrastructure stakeholders includes the Federal Government, State and local governments, Health care provider organizations, Health care provider membership and trade organizations, Health care plans and purchasers, Standards development organizations, the information technology industry, consumer and patient advocacy groups, community organizations, and academic and research organizations".[39] It is essential for all stakeholders to participate in developing the national action plan to protect this critical infrastructure

5. GOVERNAMENTAL REGULATIONS

Federal requirements and governance for the nations' critical infrastructures provides the guidance and oversight for Information Security and Protection. Many of the governmental regulations are Acts that have been mandated by Congress as well as several Presidential Directives, which was as a direct result of the act of terrorism against our country. Regulations that provide for the establishment of the Public Health sectors mission, vision, goals and objectives are those that are mandated by Congress as a mechanism to provide guidance and oversight. Rules and Acts that called for agencies to establish Strategic Plans, IRM Plans, CIO's and reporting strategies for measuring key objectives and relating them to performance measures are listed as the following: GPRA, PMA, Clinger-Cohen Act, and the Paperwork Act.

However, regulations that are more directly related to Information Security Protection can be identified as the following: Homeland Security Act of 2002 (HSA), Computer Security Act of 1997, Government Information Security Reform Act (GISRA), OMB Circular A-130 Appendix III, Privacy Act of 1974, Clinger-Cohen Act of 1996, and the Health Insurance Portability and Accountability Act (HIPAA) of 1996

6. PUBLIC HEALTH SECTOR-STATUS

The public health sector is extremely large and diverse in the services and products it provides to our citizens. Public health workers are seen as first responders in the event of a natural disaster. They take the lead for any pandemic, flu outbreak, environmental breach, nation wide immunizations; and the medical provider to the poor and disenfranchised. The sector consists of state and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, and pharmaceutical stockpiles. These facilities are relied upon for mitigating and recovering from the effects of a natural disaster or deliberate terrorist attack, and needs to be protected to prevent a disruption of its operations. Even if the hospital or public health facilities were not the main target, they could be affected by secondary contamination involving chemical, radiological, or biological agents.[40]

Core functions of the public health sector are the collection, storage, and use of information about the population's health that will lead to healing and prevention of disease and loss of life. In addition, public health surveillance focuses on identifying and controlling persons with communicable diseases; to collect and analyze behavioral information regarding, alcohol and drug use; seatbelt and bicycle helmet use; smoking; exercise; and sexual practices. In an effort to assess environmental risks, data is also collected on pediatric blood lead levels and incidence of cancers, birth defects, and pulmonary diseases.[41]

[39] http://www.aspe.hhs.gov/sp/nhii/index

[40] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

[41] The public Health Information Infrastructure: A National Review of the Law on health Information Privacy, Lawrence O. Gostin, Zita Lazzarine, and Verla Neslund, JAMA, 10\996 vol.275, pp. 1921-1927

Currently, health care delivery relies on paper based medical records, from prescriptions to medical histories and life-critical hospital charts. Patient care today relies on an increasingly antiquated, costly, and error-prone system of pen-and-paper notations. These are all variables to why health care has become so expense that many poor and disenfranchised citizens can not afford coverage. Health care expenses and health care insurance continues to rise, prescription costs are unaffordable for the majority of the elderly, and many of the nation's citizens go with out any health care coverage at all. This situation is not confined to just the United States, this is a problem that exists globally. Despite funding that has been set aside and lobbying that have taken place on Capitol Hill, health care in this Nation is still a serious concern. Irregularity and lack of quality health care, as well as poor communication between hospitals and other health care providers, all play a vital part into the potential for avoidable errors. Using the current paper system, information is slow to be transmitted, and thereby causes a delay in patient treatment or notification to proper authorities. This delay can have a negative effect on the patient or the community involved.

However, with the use of a National Health Information Infrastructure medical records and vital information can be transmitted over data lines, and medical care can be monitored and provided as needed.

7. PUBLIC HEALTH INFORMATION TECHNOLOGY

Information technological innovations have not been explored to its fullest to reduce the high cost of medical care, pharmaceuticals, reduction in medical errors, and to provide consistent quality care as seen in other critical infrastructures. Significant IT investments in other industries such as finance and transportation have improved quality of products and services as well as lowered errors and costs. American citizens are able to bank on line, make airline reservations over the phone, shop for clothing or groceries on line, pay bills on line, send emails and numerous other activities, yet the medical and health sector is still mainly paper-based. To date there are no telemedicine hot lines, pharmacy's that you can call and order medication on line, etc, which could reduce reportable errors in pharmacist trying to read illegible writing. This is not to say the health care sector doesn't already have requirements to report errors in care delivery, but rather to point out the IT investment has been relatively small and the value of the data collected is limited.

To address the establishment of standards for collection, coding and classification of patient safety information HHS has recommended the formation of The National Health Information Infrastructure (NHII) initiative. NHII is being described as "a set of technologies, standards, applications, systems values, and laws that support all facets of individual health, healthcare, and public health."[42] These distinct requirements are intended to work collaboratively, creating a secure, interconnected repository of data from which providers and other health officials may learn and make sound healthcare related decision. This concept is a collaboration of many public and private organizations that are attempting to confront the crisis in the health care delivery system. The Institute of Medicine (IOM) estimated that as many as 44,000 to 98,000 deaths occur each year as the result of medical errors".[43] This is alarming number to have happen in a country where the healthcare system is among the best in the world. These results were the catalyst of the PITAC report, but alone is still is not enough. Events such as the World Trade Center disaster and the anthrax attack in 2001, and later, the proliferation of the West Nile Virus and SARS have underlined the need for a nation capability to quickly share and respond collaboratively to major health related threats. Americans deserve safe care, and patient safety is indistinguishable from quality care, in as much the use of improved information systems and national data standards is critical to support patient safety as a standard of care in all clinical settings.

[42] http://wwwHIPAAadvisory.com

[43] http://web.lexis-nexis.com/universe/document

A 2004 GAO report on Public Health Preparedness states, "Although states have developed many important aspects of public health preparedness, since April 2003, no state is fully prepared to respond to a major public health threat".[44] In an effort to move closer to a prepared state the President's Information Technology Advisory Committee (PITAC) submitted the following recommendation in a report entitled *Revolutionizing Health Care Through Information Technology*. This is a first step in moving closer to a framework for 21st century health care information infrastructure. There are four core elements of this framework: Electronic Health records for all Americans that provide every patient and his or her caregivers the necessary information required for optimal care while reducing costs of administrative overhead; computer-assisted clinical decision support to increase the ability of health care providers to take advantage of state-of-the-art medical knowledge as they make treatment decisions (enabling the practice of evidence-based medicine); computerized provider order entry-such as for test, medicine and procedures- both for outpatient care and within hospital environment; secure, private, interoperable, electronic health information exchange, including both highly specific standards for capturing new data and tools for capturing non-standard-compliant electronic information from legacy systems.[45]

Although, the nation has made considerable progress in the research and development arena, such as treatment for cancer, HIV, diabetes and various other diseases, the same progression have not been applied to our health information systems. Patient's vital medical information is scattered across medical records by many different caregivers in many different locations; physicians keep information about drugs, drug interactions, managed care formulas and recent research in memory; physicians don't always have the best information to select the best treatments readily available. Collectively these conditions lead to unnecessary medical errors. To meet these challenges and as a part of the Health Information Technology Plan, the President has outlined a plan to ensure that most American will have electronic records within the next 10 years and he proposed funding of $100 million dollars towards this objective.[46]

Benefits envisioned with these electronic health records will be information that can be shared privately and among and between health care providers when authorized by the patient. Medical information such as x-ray results, laboratory test results, dental records, drug allergies, medical history's, etc, can be presented upon arriving in the doctor's office or health facility on an electronic chip. Electronic health records will also aid in tracking and identifying symptoms of a potential outbreak or contagious disease, by sharing centralized databases among health care facilities and providers across the country.

8. PUBLIC HEALTH NETWORKING INFRASTRUCTURE

The Public Health Information Network (PHIN) is CDC's vision for advancing fully capable and interoperable information systems in the many organizations that participate in public health. PHIN is a national initiative to implement a multi-organizational business and technical architecture for public health information systems. With the acceptance of information technology as a core element of public health, public health professionals are actively seeking essential tools capable to address and meet the needs of the community.[47] Since the anthrax attacks in 2001, PHIN has sought to support core public health functions by assuming that public health has near real-time access to health care and health related data critical in implementing effective community based interventions to reduce mortality and morbidity resulting from intentional acts of terrorism or naturally occurring disease outbreaks.

The Health Alert Network (HAN) is another project being developed at the Centers for Disease Control (CDC) as part of their Public Health Emergency Preparedness & Response

[44] GAO report Public Health Preparedness/GAO-04-458-T
[45] http://www.nitrd.gov
[46] http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html
[47] http://wwwphin.gov

Program. The project is intended to ensure communication capacity at all local and state health departments, capacity to receive distance learning offerings from CDC, and to ensure capacity to broadcast and receive health alerts at every level. These are all programs that are attempting to bring the Public Health sector into the 21st century and to be prepared to react to event such as that of Katrina and those catastrophes abroad.

9. PUBLIC HEALTH CRITICAL INFRASTRUCTURE PROTECTION

The department of Health and Human Services (HHS) is the Lead Agency for the Public Health Services Sector. The goal of the CIP program is to develop a comprehensive program, including the identification of critical assets and protection of the critical infrastructures that pertain to the health care and human services sectors. This concept includes protection of laboratory and personal health services from physical attack and disruption, loss of confidentiality and integrity of information and loss of availability of services.[48]

Health records are among the most sensitive data that are acquired, used and disclosed by government and private sector. Health information reveals a great deal of personal facts about individuals which may lead to stigma and discrimination when possessed and misused by government official's employers, insurers, and by friends and family. The increasing potential for disclosure of this information within a rapidly developing national health information infrastructure, facilitated by massive computerization of records and other technological developments, presents significant risks to individual privacy.[49] Despite the sensitive nature of individually-identifiable health information, protecting the privacy and security of these records has been historically de-emphasized when compared with statutory protection allotted to other types of personal information (e.g., banking, and investment records, tax information, etc.). While it is important to respect the autonomy of individuals, excessive privacy can impede goals of the health care system. Health care professionals can use computerized data to improve clinical care for patients, health services researchers can better assess the quality of services, government and health service managers can gain administrative efficiencies, health insurers, including Medicare and Medicaid can prevent fraud and abuse, and public health authorities can improve surveillance and epidemiologic investigation with the community.

Health information privacy refers to an individual claim to control the circumstance in which personally identifiable health information is collected used and disclosed. Protecting this information involves enabling the person to whom the information relates to control its acquisition, use and disclosure. While privacy relates to acquisition and use, confidentiality denotes individual privacy interest that arises out of a specific relationship with the person about whom the information is gathered. The security of health information is distinct from individual interest in privacy and confidentiality. Security refers to technological, organizational, or administrative processes designed to protect data systems from unwarranted access, disclosures, modification, or destruction

The Privacy Act of 1974, The Freedom of Information Act of 1966, and The Electron Communication Privacy Act of 1986, generally applies only to government collections, use, or disclosures of health information, and thus do not confer protections to health information in the private sector. These statutes do not provide comprehensive protection of health information regardless of its subject or holder. However, the Health Insurance Portability and Accountability Act (HIPAA) seek to reduce the administrative and financial burden of health care by standardizing the electronic transmission of health-related data. In addition to security provisions which require health care providers to ensure the confidentiality of their electronic information, HIPAA requires Congress to pass legislation to set uniform standards for the transmission of health insurance information, including recommendation for security measure to

[48] Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, January 2001

[49] http://www.critpath.org

protect private medical information [50] Basically the privacy regulation ensures protection for patients by limiting the ways health plans, pharmacies, hospitals, and other covered entities can use patients personal medical information. Regulations protect medical records and other individually identifiable health information, whether it is on paper, in computers or communication orally.

The growing use of the Internet by both the public and private sector is quickly making network an important medium for information exchange. Building an interoperable health-information infrastructure, to ensure records follow the patient and caregivers have access to this information immediately to make treatment decisions is crucial. Information Technology makes this process possible and current workstation and network security protections are in place to manage this process. However the National Strategy to Secure Cyberspace, and Office of Management and Budget has placed a higher importance on information security and seeks to have additional measures put in place. While the Internet allows for easy connectivity, such ease is counter-balanced by inherent issues concerning the ability to protect the privacy and integrity of information and to ensure that information is accessible only by those for whom it was intended. Information can be protected by the appropriate use of security controls, including encryption, authentication integrity verification and assurance of non-repudiation applied to the transmission process. The CDC/ATSDR Health Information Systems has additionally implemented policy requirement for authentication using industry standard X.509 certificates, secure tokens, and other applicable means as identified; an encryption engine; and access control through the firewall by data routing to program using an application server.

In 2004, Cyber Security Industry Alliance (CSIA), a public policy and advocacy group comprised exclusively of security software, hardware and service vendors to address key cyber security issues, has released its recommendation for the development of a secure electronic healthcare system. These recommendations are designed to support the nation's first strategic framework report to the 10 year initiative to develop electronic health records and other uses of health information technology, which was announced by HHS through the Presidents transformation plan. CSIA's recommendation covers the confidentiality, integrity and availability of a national healthcare-information infrastructure as well as foster compliance with the Health Insurance Portability and Accountability Act.

The recommendations include confidentially to protect patient information from unauthorized access or disclosure by: deploying strong authentication and authorization controls to ensure that only authorized users gain access to a system; only those part of the system necessary to perform their responsibilities; encrypting data; and communication wherever appropriate so that healthcare data in transit and at rest is protected from unauthorized interception or eavesdropping; properly disposing of retired data, software and hardware to ensure that unauthorized user cannot recover it later; validating data to ensure integrity of data entered through web interfaces; conducting frequent system audits to ensure only authorized user are accessing, entering, or changing information; using digital signatures to verify that data in transit or data at rest has not been modified by unauthorized parties. The recommendation also include availability to ensure redundancy and protection for critical information systems by: providing for redundancy to avoid downtime due to equipment failure, denial-of-service attacks, or scheduled maintenance; using a private data backbone to avoid problems from network bottlenecks and outages that occur on the Internet due to fluctuation in data flows, developing a rapid incident response mechanism to shorten periods of unavailability due to attacks, intrusion, events and their investigation; support information sharing networks, such as the existing healthcare Information Sharing and Analysis Center, to ensure timely dissemination of cyber threats, vulnerabilities and attacks.[51]

10. PUBLIC HEALTH GLOBAL INFORMATION INFRASTUCTURE

[50] Ibid

[51] http://proquest.umi.com/pqdweb?index`

It has been noted as the relationship and importance Information Assurance and Information Technology plays as it relates to the Public Health sector. It has also been noted that information such as medical records, research data, infectious diseases, vaccines, environmental hazards, and national outbreaks, and whether it is of personal or public matter is collected and shared by the internet. We have discussed the importance of this data being protected using policies and regulations against any malicious terrorist attack or human error.

What should also be noted is that this responsibility is of national interest to both national governments and international agencies and organizations. The public health system has been tested in as far away places as Surat, India; the former Soviet Union; Kikwit, Zaire; Asia; earthquake in Pakistan; and in our own homeland with Hurricane Katrina in New Orleans. It is imperative to be able to mobilize, package, and deploy both medical supplies and personnel in a matter of hours and understand what the basic needs are from the location in need. Information Technology has allowed that to happen and, in most cases, very effectively.

It is up to the national leaders to continue to build strong and reliable infrastructures that will facilitate this sharing of information, which is accessible via the Internet. Protecting our critical infrastructure of Public Health is and will continue to be an ongoing activity to ensure we have established solid Strategic Plans with goals and objectives that support the philosophy of managing risk, threats and vulnerabilities. "It has also been noted that the global public health system has failed as it relates to the millions of people without medical insurance, deterioration of public medical care services to the poor, and a nation decline in immunization coverage among children".[52] New threats to the public health system as it relates to globalization can also be directed to the fact that air travel and importation of food from developing countries facilitates dissemination of infectious diseases. International challenges can still be viewed as those of threats of bioterrorism and biologic warfare. U.S. bio incidents have thus far been domestic.

[52] Betrayal of Trust: The Collapse of Global Public Health, Laurie Garrett, SBN 078685229, 2000

11. CONCLUSION

Protecting the Privacy of Personal Health Information continues to be a matter of national concern. With the implementation of the HIPAA rule, and other governing policies the Public Health sector has made great strides in protecting personal medical information.

As a critical infrastructure the public health sector is a vital commodity to our nation. It is imperative that federal, state and local governments continue to set necessary policies and procedures in place to protect it. As demonstrated by the Hurricane Katrina emergency, state and local governments still need to develop a better response plan to a major public health threat and disaster. Budgets must be established to ensure plans and procedures detailed in the HIPAA plan are in place to safeguard the Public Health critical infrastructure. For this nation to be in a position to react and provide the health care services in the event of another natural disaster or cyber attack, leaders must continue to work with federal, state, and local governments to recognize these threats to our infrastructure and work together to put forth the best plan available. The nation must be ready when the next threat comes its way!

REFERENCES

- National Strategy for Homeland Security, Office of Homeland Security, July 2002.
- The National Security Strategy of the United States of America, September 2002.
- The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets, February 2003.
- The National Strategy to Secure Cyberspace, February 2003.
- http://www.glr.com/govt/medical/personalhealthcare/html
- http://www.csoonline.com/whitepapers/041502cisco/index/html
- "*What is Information Assurance*", Shim Enterprise, Inc, Dr. Walter L. McKnight: 1732 Westerly Drive, Brandon, Fl 33511.
- Government Accountability Office, *BIOTERRORISM: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies,* GAO-03-139, May 2003.
- http://www.gao.gov/htext/d05628.html
- http://www.tricare.osd.mil/tmaprivacy
- http://www.hhs.gov/ocr/HIPAA/assist.html
- http://www.hhs/gov/ocr/index.html
- http://www.pcworld.com/howto/article/0,aid,118786,00.asp
- http://www.apha.org.united
- http://www.ecora.com
- "The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy", Lawrence O. Gostin, Zita Lazzarini, Verla S. Neslund, and Michael T. Osterholm, JAMA, 1996 vol.275, pp1921-1927.
- CRS Report for Congress, "*Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats Vulnerabilities and Consequences*", RL32561, September 2, 2004.
- National Institute of Standards and Technology, *"Risk Management Guide for Information Technology Systems"*, Special Publication 800-30, July 2002.
- Military Health System Information Assurance Program Office, *"Military Health System Information Assurance Policy Guidance"*, March 5, 2004.
- DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 2003.
- "Trust in Cyberspace", Fred B. Schneider, ISBN:0-309-06558-5, 352 pages, 1999.
- Public Health Risks of Disasters, Communication, Infrastructure, and Preparedness – Workshop Summary, http://books.nap.edu/catalog/11201.html.

- http://kubrart.ahima.org/epedio/groups/public/documents/ahima/pub_bok_017116.html
- “Betrayal of Trust: The Collapse of Global Public Health”, Laurie Garrett, SBN 0786865229, 2000.
- Department of Health and Human Services, *“Justification of Estimates for Appropriations Committees”*, Office for Civil Rights, Fiscal Year 2006.
- Government Accountability Office, *Public Health Preparedness: Response Capacity Improving, but Much Remain to be Accomplished*, GAO-04-458T, February 12, 2004.
- Department of Homeland Security, Office of Inspector General, Emergency Preparedness and Response Could Better Integrate Information Technology with Incident Response and Recovery, OIG-05-36, September 2005.
- The White House President George W. Bush (2004). Retrieved on November 25 from http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html
- Electronic Medical Records; *CSIA prescribes 10 steps for a secure national electronic healthcare system*, Letter on the CDC & FDA, Aug 22, 2004. pg 25.
- http://porquest.umi.com/pqdweb/index
- Secure Data Network Standards and Procedures, Centers for Disease Control and Prevention (CDC), July 15, 1999, HISSB Adopted SDN Document V5.
- Report of the President of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, January 2001
- The National Health Information Infrastructure: *Implications for Providers, Patients and the Future of Healthcare Delivery*. http://www.HIPAAdvisory.com/action/ehealth/nhii.htm
- Centers of Disease Control and Prevention, *Public Health Information Network (PHIN),* obtained 11/25/05

ALPHABETICAL INDEX OF AUTHORS