REGIONAL DEPARTMENT
OF DEFENSE RESOURCES MANAGEMENT
STUDIES

THE 7th EXPLORATORY WORKHOP

"INFORMATION SECURITY MANAGEMENT

IN THE 21ST CENTURY"

ISSN: 2286 - 2765

ISSN-L: 2286 - 2765

COORDINATOR: Advanced Instructor PhD eng. **DANIEL SORA**

National Defense University "Carol I" Publishing House
Bucharest 2014

THE 7th EXPLORATORY WORKHOP
"INFORMATION SECURITY MANAGEMENT
- IN THE 21ST CENTURY"

WORKSHOP COMMITTEE

COL.eng. Daniel SORA, Advanced Instructor PhD.
COL.eng. Cezar VASILESCU, Professor PhD.
CAPT.eng. Florin OGÎGĂU-NEAMȚIU

SESSION CHAIRMEN

COL.eng. Daniel SORA, Advanced Instructor PhD.

COL.eng. Cezar VASILESCU, Professor PhD.

THE 7th EXPLORATORY WORKHOP "INFORMATION SECURITY MANAGEMENT - IN THE 21ST CENTURY"

June 18th 2014

Proceedings of the workshop unfolded during the

INFORMATION SECURITY MANAGEMENT COURSES

conducted by the Regional Department
of Defense Resources Management Studies

January 13th – February 07th 2014
and
May 26th – June 20th 2014

Brasov
ROMÂNIA

This page is intentionally left blank

CONTENTS

CREATING A COMPUTER EMERGENCY RESPONSE TEAM

Author:
1st lt AL-MERAIKHI Nawaf

INTRODUCTION

Maintaining safe computer information systems assets in an interconnected computing environment is a great challenge and becomes more and more difficult as new "E" services and products emerging. Organizations realize that fact, and know that there is no one solution can be affective for securing data and information systems; instead a multi-layered security strategy is required (defence in depth). The more efficient layer that most organizations are including in their defence strategy is the creation of a Computer Emergency Response Team, generally called a CERT.

The Computer emergency response teams (CERT) are expert groups that handle computer security incidents. Alternative names for such groups include computer emergency readiness team and computer security incident response team (CSIRT).

The name Computer Emergency Response team is the historic designation for the first team (CERT-CC) at Carnegie Mellon University (CMU). The abbreviation CERT of the historic name was picked up by other teams around the world. Some teams took on the more specific name of CSIRT to point out the task of handling computer security incidents instead of other tech support work, and because CMU was threatening to take legal action against individuals or organisations who referred to any other team than CERT-CC as a CERT. After the turn of the century, CMU relaxed its position, and the terms CERT and CSIRT are now used interchangeably.

As the organization begins to build its own Computer Emergency Response capability, it looks to determine the best strategy for putting such a structure in place. It doesn't only want to know what has worked well for others, but also wants some guidance on the process and requirements it must follow to establish an effective CERT.[1]

I. CERT Responsibilities

The history of CERTs is linked to the existence of malware, especially computer worms and viruses. Whenever a new technology arrives, its misuse is not long in following. The first worm in the IBM VNET was covered up. Shortly after, a worm hit the Internet on November 3, 1988, when the so-called Morris Worm paralysed a good percentage of it. This led to the formation of the first computer emergency response team at Carnegie Mellon University under U.S. Government contract. With the massive growth in the use of information and communications technologies over the subsequent years, the now-generic term 'CERT'/'CSIRT' refers to an essential part of most large organisations' structures with almost the same responsibilities:[2]

a. Handling computer security incident reports and activity related to networks connected to the internet.
b. Provides a focal point for all incident notification in the organization.
c. Providing the coordination and necessary support for organizations involved in incidents.
d. Increase security awareness in community.
e. Maintains an early warning to networks involved in malicious activities.
f. Identifying new trends and correlating security events.
g. Helps new Computer Security Incident Response Teams (CSIRTs) to establish their activities.
h. Increasing the level of security and incident handling capacity of the networks connected to the internet.

II. Drivers

The most known motivators driving the organizations for creating their own CERTs may include:[3]

i. The increasing number of computer security incidents being reported.
j. The increasing number and type of organizations being affected by computer security incidents.
k. More focused awareness by organizations on the need for security policies and practices as part of their overall risk-management strategies.

---

[1] http://en.wikipedia.org/wiki/Computer_emergency_response_team
[2] http://www.cert.br/about/

l. The new laws and regulations that impact how organizations are required to protect information assets.
m. The realization that systems and network administrators alone cannot protect organizational systems and assets.

III. Questions

Organizations have many questions they want to answer helping them to design their response capability. They are also interested in knowing what other teams in similar industry sectors are doing. Typical questions being asked include but are not limited to the following:[4]

a. What are the basic requirements for establishing a CERT?
b. What type of CERT will be needed?
c. What type of services should be offered?
d. How big should the CERT be?
e. Where should the CERT be located in the organization?
f. How much will it cost to implement and support a team?
g. What are the initial steps to follow to create a CERT?

The most challenging fact that CERTs are as unique as the organizations they serve, and as a result, no two teams are likely to operate in the exact same manner. It is important for the organization to decide why it is building a CERT and what it wants that CERT to achieve. Once this is determined, then the unique set of answers to the above questions can be formulated.

IV. Best Practices

Although CERTs differ in how they operate depending on the available staff, expertise, budget resources, and unique circumstances of each organization, there are some basic practices that apply to all CERTs. The steps are as follows:

Step 1: Obtain management support and buy-in
Step 2: Determine the CSIRT strategic plan
Step 3: Gather relevant information
Step 4: Design the CSIRT vision
Step 5: Communicate the CSIRT vision and operational plan

---

[3] http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm

[4] http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm

Step 6: Begin CSIRT implementation

Step 7: Announce the operational CSIRT

Step 8: Evaluate CSIRT effectiveness

IV.1. Obtain Management Support and Buy-In

Without the management approval and support, creating an effective incident response capability can be extremely difficult. This support must be shown in numerous ways, including the provision of resources, funding, and time, to the person or group of people who will act as the project team for implementing the CERT. This also includes executive and business or department managers and their staffs committing time to participate in this planning process; their input is essential during the design effort. Along with obtaining management support for the planning and implementation process, it is important to get management commitment to maintain CERT operations for the long term.

IV.2. Determine the CERT Development Strategic Plan

Think about how to manage the development of the CERT. What administrative issues must be dealt with, and what project management issues must be addressed? Are there specific time frames to be met? Are they realistic, and if not, can they be changed?

Where do the team members come from? You want to ensure that all stakeholders are represented. If anyone has a background in these areas, consider having them participate on the team. How do you let the organization know about the development of the CERT? A memo sent from the CIO, CEO, or other high-level manager announcing the project and asking each key stakeholder and area to provide assistance in any way possible is a good way to start.

IV.3. Gather Relevant Information

Gather information to determine the incident response and service needs and Take a look at the types of incident activity currently being reported within your organization. This helps determine not only what type of services to offer, but also the types of skills and expertise the CERT staff will need.

Meet with key stakeholders to discuss not only their incident response needs, but to achieve an initial consensus on the expectations, strategic direction, definitions, and

responsibilities of the CERT. Your definition of what a CERT is and does may be very different from your manager's definition or the definition of another part of your organization. Use these discussions with the stakeholders to outline and identify how each group will need to interact with the CERT. The stakeholders could include but are not limited to:

a. **Business managers.** They need to understand what the CERT is and how it can help support their business processes.
b. **Representatives from IT**. How do the IT staff and the CERT interact? What actions are taken by IT staff and what actions are taken by CERT members during response operations? Will the CERT have easy access to network and systems logs for analysis purposes? Will the CERT be able to make recommendations to improve the security of the organizational infrastructure?
c. **Representatives from the legal department**. When and how the legal department involved in incident response efforts? Legal staff may also be needed to review non-disclosure agreements, develop appropriate wording for contacting other sites and organizations, and determine site liability for computer security incidents.
d. **Representatives from human resources**. They can help develop job descriptions to hire CERT staff, and develop policies and procedures for removing internal employees found engaging in unauthorized or illegal computer activity.
e. **Representatives from public relations**. They must be prepared to handle any media inquiries and help develop information-disclosure policies and practices.
f. **Any existing security groups**, including physical security. The CERT will need to exchange information with these groups about computer incidents and may share responsibility with them for resolving issues involving computer or data theft.
g. **Audit and risk management specialists**. They can help develop threat metrics and vulnerability assessments, along with encouraging computer security best practices across the constituency or organization.

There may also be some resources available for review that will help in your information gathering. These may include:

a. **Organization charts** for the enterprise and specific business functions.
b. **Topologies** for organizational or constituency systems and networks critical system and asset inventories
c. **Existing disaster-recovery or business-continuity plans**

d. **Incident-management plans**
e. **Parental or institutional regulations**
f. **Security policies and procedures**

Reviewing these documents serves a dual purpose: first, to identify existing stakeholders, resources, and system owners; and second, to provide an overview of existing policies to which the CERT must adhere. As a bonus, these documents may contain text that can be adapted when developing CERT policies, procedures, or documentation. Take a look at other CERTs' websites, and check their missions, charters, funding scheme, and service listing. This may give you ideas for organizing your team. Review any books or other publications about incident handling or CERTs.

Attend courses or conferences that include sessions for developing incident response strategies or creating CERTs. These venues can provide you with opportunities to exchange ideas and interact with others in this field.

IV.4. Design Your CERT Vision

As the information gathered and as you build your understanding of management expectations, you can begin to identify the key components of the CERT. This allows you to define the vision for the CERT and its goals and functions.

It is important to achieve clear agreement on the definition and expectations for the CERT being formed. What the CERT staff thinks the team will do and what the managers and general constituency think the CERT will do may be completely different. The main focus is to prevent and respond to incidents. The vision for the CERT must include a clear explanation of where these CERT functions fit into the current organizational structure and how the CERT interacts with its constituency. The vision explains what benefits the CERT provides, what processes it enacts, who it coordinates with, and how it performs its response activities and in creating your vision, you should:

a. Identify your constituency.
b. Who does the CERT support and serve?
c. Define your CERT mission, goals, and objectives.
d. What does the CERT do for the identified constituency?
e. How does the CSIRT support its mission?
f. Determine the organizational model. How is the CERT structured and organized?

g. Identify required resources. What staff, equipment, and infrastructure are needed to operate the CERT?
h. Determine your CERT funding. How is the CSIRT funded for its initial startup and its long-term maintenance and growth?

IV.5. Communicate the CERT Vision

Communicate the CERT vision and operational plan to management, your constituency, and others who need to know and understand its operations. As appropriate, make adjustments to the plan based on their feedback. Communicating your vision in advance can help identify process or organizational problems before implementation. It is a way to let people know what is coming and allow them to provide input into CERT development.

IV.6. Begin CERT Implementation

Once management and constituency understand CERTs operation and buy-in is obtained for the vision, begin the implementation:

a. Hire and train initial CERT staff.
b. Buy equipment and build any necessary network infrastructure.
c. Develop the initial set of CERT policies and procedures.
d. Define the specifications for and build your incident-tracking system.
e. Develop incident-reporting guidelines and forms for your constituency.

The process for reporting an incident includes a detailed description of the mechanisms for submitting reports: phone, email, web form, or some other mechanism. It should also include details about what type of information should be included in the report.

The process for responding to an incident details how the CERT prioritizes and handles received reports. This includes how the person reporting an incident is notified of its resolution, any response time frames that must be followed, and any other notification.

IV.7. Announce the CERT

When the CERT is operational, announce it broadly to the constituency or parent organization. It is best if this announcement comes from sponsoring management. Include the contact information and hours of operation for the CERT in the announcement. This is an excellent time to make available the CERT incident-reporting guidelines. You may also want

to develop information to publicize the CERT, such as a simple flyer or brochure outlining the CERT mission and services, which can be distributed with the announcement.

IV.8. Evaluate the Effectiveness of the CERT

Once the CERT has been in operation for a while, management will want to determine the effectiveness of the team and use evaluation results to improve CERT processes and ensure that the team is meeting the needs of the constituency. The CERT, in conjunction with management and the constituency, will need to develop a mechanism to perform such an evaluation.

Information on effectiveness can be gathered through a variety of feedback mechanisms, including:

a. Benchmarking against other CERTs.
b. General discussions with constituency representatives.
c. Evaluation surveys distributed to constituency members on a periodic basis.
d. Creation of a set of criteria or quality parameters that is then used by an audit or third party group to evaluate the team.

It may be helpful to review previously collected information on the state of the constituency or organization before the implementation of the team. This information can be used as a baseline in determining the effect of the CERT on the constituency. Information collected for comparison may include:

a. Number of reported incidents.
b. Response time or time-to-live of an incident.
c. Number of incidents successfully resolved.
d. Information reported to the constituency about computer security issues or ongoing activity.
e. Attentiveness to security issues within the organization.
f. Preventative techniques and security practices in place.

V. CERT Success Metrics

The likelihood of totally eliminating attacks from outside or inside the organization is zero. CERTs are similar to fire departments; they have significant support costs but, when activated, they are literally worth their weight in gold. Consequently, crafting a series of

success metrics is usually one that is left to the very last minute. Here are a few suggestions that should be considered during the CERT creation process:[5]

a. How many incidents did the CERT address in a given time period? (Time periods could be measured in months, quarters, or years.)
b. What were the estimated amounts of financial damage averted by CERT intervention?
c. What has been the impression of CERT's technical expertise with their constituency?
d. What are the average time and employee resources needed to address each specific incident type?
e. What is the documentation completed by individual CERT members relative to the actions taken with each incident?
f. What recognition or awards were presented to the CERT?
g. Post incident feedback from constituency. Basically, this mechanism is one where a questionnaire form is provided to the victim-business unit and the results compiled by the CERT as part of their success metrics. Particular emphasis in these questionnaires should be placed on the anonymity of the person completing them, if so desired.
h. Were significant changes brought to the organization's policies and procedures suggested by the CERT as a result of their intercession with a critical incident?

VI. CERT Development Life Cycle

In various forms, CERTs have been in existence for more than 20 years. In some cases, they have performed magnificently and made substantial contributions to their organizations; while in other cases, they have foundered and sometimes failed. The levels of CERT competence and success in the organization are tied to their development life cycle. Consequently, these are the stages of the CERT life cycle:[6]

a. Initiation and proposal. Here is the stage where it all begins. Usually, someone makes a proposal to senior managers testing the idea and follows with a written proposal containing:
    1) Necessity studies
    2) Plan

[5] http://www.iseca.org/downloads/2954_1749_AU0010_C04.pdf
[6] http://www.iseca.org/downloads/2954_1749_AU0010_C04.pdf

3) Resource requirements
4) Structure
5) Lines of reporting and authority
6) Staffing
7) Funding
8) Training needs
9) Deliverables
10) Success metrics

Often the employee who will serve as the unit manager begins a small ad hoc CERT team as a pilot program. This allows the organization time to get accustomed to the concept and its execution before submitting a formal proposal. Additionally, if immediate success is realized, it makes selling the proposal much easier if a good reputation is already earned. Most employees have not heard of CERT in this phase and do not have any expectations, yet.

b. Developmental. This phase is marked by the formation of the CERT. Much of their direction will be guided by what is done at this time. In this phase, staffing is selected or recruited, an infrastructure is created, an office site is established, equipment and tools are procured, funding is allocated, duty rosters are developed ensuring that the function-point is available to screen trouble calls at all hours, policies and procedures applicable to the CERT are instituted, and the team is advertised as operational.

At this stage, precedence and reputation are going to be earned. When the fledgling CERT responds, literally every critical eye will be focused on how it performs, how it interacts with managers, and how it interacts with its constituents. Of all times, this is not the one for judgment errors or other failings. The future of the team hinges on its ability to respond quickly and bring the emergency under control with a satisfactory solution. Failing to define and obtain senior management's approval of operational requirements, drafting deficient policies and procedures, forming meaningless outside liaison contacts, and training is staff poorly can quickly spell doom for the team and its effectiveness. On the other hand, if successful the team can move on to the next stage of development.

c. Establishment. In this phase startup and development problems are resolved. Constituents know when they should notify the CERT and know what its course of action is when it arrives. In some instances, CERTs are loaned or

contracted to other organizations to assist in critical incidents. Through contracts and mutual assistance agreements, CERTs may be deployed at business sites belonging to other organizations on a value-added basis. In this fashion, the cost of their existence is somewhat defrayed.

In this phase, senior managers have accepted the CERT and formally recognized its efforts. At some time in this phase, the organization and team members realize the CERT's existence is indefinite.

Plans are made for team progress by developing an institutional knowledge base. Team members might be considered promotions, relocation, rotation, or other work assignments. Working with the human resources unit, well-qualified prospective candidates are located and incentives provided, motivating them to consider team membership. The CERT manager is also anxiously engaged in providing mentors for employees to upgrade training and professional certifications for her employees.

d. Post establishment. This phase includes the expansion of the team to include operations and requirements not part of any previous phases. Usually these activities include the CERT providing constituency training, delivering presentations as guest-lecturers, authoring articles for peer-review publications, and substantial research and analysis.

CONCLUSIONS

The length of time it will take to design, plan, and implement a team will vary with each organizational situation. Most of CERTs become operational across a wide range of times, from two months to two years. It is important to realize that it can take about 12-18 months to work out the processes and procedures, especially for a large, distributed enterprise. After the team is operational, it can take another 12-18 months to obtain a good level of trust and comfort with your constituency. Many teams show a large growth in the number of incidents reported over their first year of operation. The longer you are in operation, the more your constituency will understand the work you are doing and the more likely they will report incidents to you.

Resources

1. http://en.wikipedia.org/wiki/Computer_emergency_response_team
2. http://www.cert.br/about/
3. http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm
4. http://www.sei.cmu.edu/products/courses/cert/creating-csirt.html[Creating a CSIRT Workshop (CERT/CC one-day workshop)].
5. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305 [Handbook for Computer Security Incident Response Team].
6. http://www.iseca.org/downloads/2954_1749_AU0010_C04.pdf

More Information on Creating a CERT

1. http://www.auscert.org.au/render.html?it=2252 [Forming an Incident Response Team, This paper was written by a former member of the Australian Computer Emergency Response Team].
2. http://www.ietf.org/rfc/rfc2350.txt [Expectations for Computer Security Incident Response (RFC 2350)].
3. http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymattersmar99.cfm [Avoiding the Trial-by-Fire Approach to Security Incidents].

ENEMY AT THE GATE: THREATS TO INFORMATION SECURITY

Author:
MAJ EPADZE Goderdzi

INTRODUCTION

After introducing this product, you will be able to do the following:

- Describe the challenges of securing information;
- Define information security and why it is important;
- Identify the types of attackers that are common today;
- Basic steps of an attack;
- Describe the five basic principles of defense;
- Users security training importance;
- Information Systems vulnerabilities;
- Information systems protection, detection, and reaction;
- Information Assurance, And computer Network Defense;
- Risk managements, threat level and category;
- Intrusion system against attack.

CHALENGIES OF SECURITY

This chapter introduces network security fundamentals that form the basis of the Security. It begins by examining the current challenges in computer security and why it is so difficult to achieve. It then describes information security in more detail and explores why it is important. Finally, the chapter looks at who is responsible for these attacks and at the fundamental defenses against attackers.

TODAY'S SECURITY ATTACKS

Despite the facts that information security continues to rank as the number one concern of IT managers and tens of billions of dollars are spent annually on computer security, the

number of successful attacks continues to increase. Information regarding recent attacks includes the following:

- The antivirus for example, a user who clicks an advertisement on a web page offering a free online vulnerability scan suddenly sees a window that informs that the computers is infected. The pop-up window directs the user to click a bottom to purchase antivirus software to disinfect the computer. However this window cannot be closed even restarting the computer. Many users finally enter their credit card numbers to purchase the antivirus software. Then credit card number is transmitted to attacker for his good. At the same time, other malware software is installed on the computer while pop-up window is open and never goes away;
- A graphics processing unit (GPU), which is separate from the computer's central Processing unit (CPU), is used in graphics cards to render screen displays on computers. Today, some of the work of a CPU can be offloaded to a GPU to accelerate specific applications, most notably floating-point operations. A $500 GPU today can process about 2 trillion (teraflop) floating-point operations per second, whereas just 10 years ago, the fastest supercomputer in the world only ran at 7 teraflops and cost $110 million. Attackers are now using GPUs to break passwords. Researchers at the Georgia Tech Research Institute (GTRI) claim that an attacker with a computer that has a GPU could easily break a relatively weak password. They state, "Right now we can confidently say that a 7-character password is hopelessly inadequate." They go on to say that any password with fewer than 12 characters could be vulnerable very soon—if it is not already;
- "Firesheep" is a free, open-source ***Firefox browser extension*** introduced in late 2010. An attacker can install this add-on and then connect to an unencrypted wireless network at a coffee shop, hotel, or library. Once the attacker clicks Start Capturing, then anyone using the wireless network who visits a site that is known by Firesheep (such as Facebook, Twitter, Amazon, FourSquare, Dropbox, Windows Live, WordPress, or Flickr) will have their name and even their photo displayed. The attacker can then double-click the name and be logged in as that person to that account;
- An analysis of 700,000 recorded attacks on computers in one week revealed that about one out of every eight attacks came by **USB** flash drive devices. A user's USB device may become infected at home where they have less security. When they bring the infected device into the office to insert into their work computer, that computer is then infected. In addition, attackers leave infected USB flash drives in parking lots and other

common areas outside an office, tempting users to pick them up on the way to their office and to insert them into their computers;

Security attacks continue to be a major concern of all IT users, especially those personnel responsible for protecting an organization's information.

I. DEFINE INFORMATION SECURITY

What is information security? Exemplify the concept of Confidentiality, Integrity and Availability; analyze and differentiate among of attacks; explain the fundamental concept and best practices related to authentication, authorization and access control;

Before it is possible to defend computers against attacks, it is necessary to understand what information security is. In addition, knowing why information security is important today and who the attackers are is beneficial.

Defining Information Security - In General sense security may be defined as the necessary steps to protect a person or property from harm. Harm may come primarily from two different sources:

- A direct action that is interested to inflict damage or suffering.
- An indirect and non-intentional action.

Consider a typical house. It is necessary to provide security for the house and its inhabitants from these two different sources. For example the house and its occupants must be sure from the direct attack of criminal who wants to inflict bodily harm to someone inside or who wants to born the house. This security may be provided by looked doors, a fence, or a strong police presence. In addition, the house must be protected from indirect acts that are not exclusively directed against it.

The term of **information security** is frequently used to describe the tasks of securing information that is in digital format. This digital information is typically manipulated by a microprocessor, stored on a magnetic, optical, or solid- state storage device (like a hard drive, DVD, or a flash drive), and transmitted over a network.

Information security can be understood by examining its goals and how it is accomplished. **1st** all protective measures are properly implemented, but not only security measures have taken cannot be guaranty complete safety also. Information security cannot completely prevent attacks or guarantee that a system is totally secure.

Rather, information security creates a defense that attempts to ward off attacks and prevents the collapse of the system when a successful attack occurs. Thus, information security is protection. **2nd** information security is intended to protect information that provides value to

people and organizations. Three protections must be extended over information. These three protections are **confidentiality, integrity, and availability** or shortly CIO:

1. **Confidentiality**. It is important that only approved individuals are able to access important information. Any user must be responsible, within the span of their control, to ensure that no actions are taken which could degrade or compromise the confidentiality levels of the programs, services and information handled by the system;
2. **Integrity.** Integrity insures that the information is correct and no unauthorized person or malicious software has altered the data. Make sure that no action are taken which could degrade or compromise the required level of accuracy, completeness and dependability of the programs services and information being handled by systems and its assets;
3. **Availability.** Information cannot be "locked up" so tight that no one can access it; otherwise, the information would not be useful. Availability ensures that data is accessible to authorize users at required time and place.

In addition to Confidentiality, Integrity and Availability (CIA), another set of protection must be implemented to secure information. These are authentication, authorization, and accounting (AAA):

1. **Authentication**. Measures designed to provide protection against fraudulent transmission and imitative communication deception by establishing validity of a transmission, message, station or individual and Authentication ensures that the individual is who they claim to be (the authentic or genuine person) and not an imposter also.
2. **Authorization**. After a person provide authentication, there is given authorization, or the ability to access the required information. There must be implemented need to know principles.
3. **Accounting**. Accounting provides tracking events. This may include a record of who has accessed the web server, from what location, and at what specific time.

Information security involves more than protecting the information itself. Because this information is stored no computer hardware, manipulated by software, and transmitted by communications, each of this areas must also be protected. The third objective of information security is to protect the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information.

Information security is achieved through a combination of three entities. As shown in figure1-1 information, hardware, software, and communications are protected in three layers: products, people, and procedures. These three layers interact with each other. For example, procedures enable people to understand how to use products to protect information. Thus, a more comprehensive definition of information security is that which protects the integrity,

confidentiality, and availability of the information on the devices that store, manipulate, and transmit the information through products, people, and procedures.

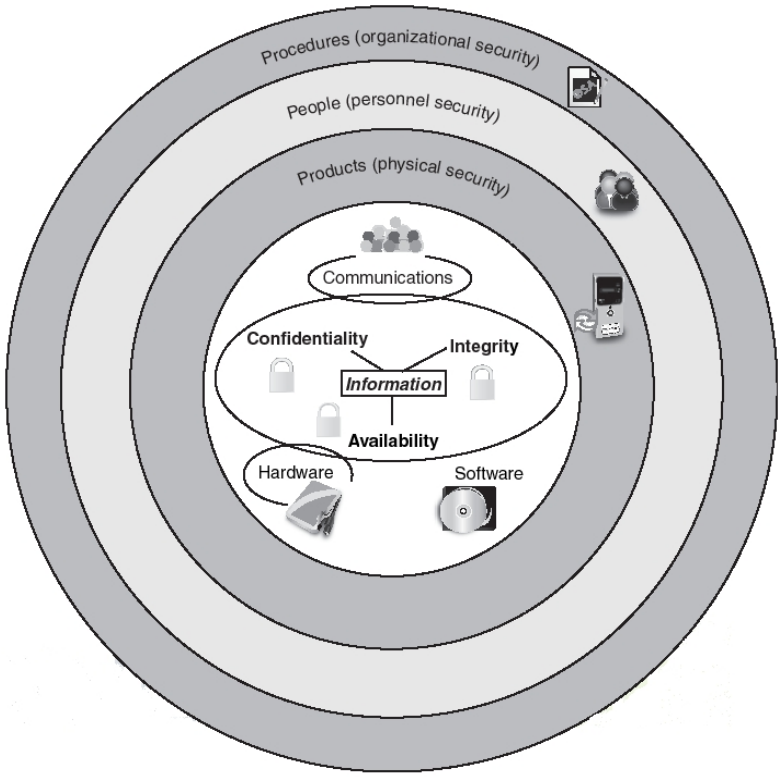


Figure 1-1 Information security Components

Understanding the importance of information security is important to organizations as well as to individuals. The goals of information security are many and include preventing data theft, thwarting identity theft, avoiding the legal consequences of not securing information, maintaining productivity, and foiling cyber terrorism.

Risk calculation; Risk = Treat x Vulnerability x Cost.

I.1. PREVENTING DATA THEVT

Securing is often associated with theft prevention, Preventing the data from being stolen is often cited by organizations as a primary goal of information security. Business data theft involves stealing proprietary business information, such as research for a new drug or a list of customers that competitors would be eager to acquire.

How does data theft happen? Data theft occurs at several different levels online. First, your data can be stolen by hacking into your social network and email accounts. Secondly, your data can be phished using emails that appear to be from valid sources. And last, your data can also be stolen by **wiretapping or eavesdropping** on your internet connection both via wire and wireless connections. The risks can be reduced through the security measures discussed

following topics. Internal threats are more difficult to anticipate but can be equally devastating to your business, or organization as external. Staff may remove data inadvertently or on purpose for financial gain or revenge. Data is very easily transported out of your office or organization using writable CDs or DVDs, USB drives, MP3 players or mobile phones. All of these devices can hold large amounts of data and are a discreet way in which an employ could copy data and walk out of the office or organization without your ever knowing. You need to think carefully about where you store a data and how you secure it physically and electronically, who has access to it and what devices you allow staff to connect to your computer network.

Ethereal and Wireshark provide criminal access to your traffic whether on wired or wireless connections. These softwares are free and available for anyone to use and download with minimal computer knowledge.

How protects data? There are several methods. First by choosing secure passwords and never shearing your account details with strangers, you will effectively secure your social and email accounts. Secondly, when you receive emails from business, make sure to double check URL and verify the authenticity of the sender every time to avoid giving your credentials to a phisher. Finally, to stop criminals from hijacking your account details and network traffic, use a VPN to encrypt all of your wired and wireless traffic.

I.2. TYPES OF ATTACKER

The type of individuals behind computer attacks are generally divided into several categories. This includes hackers, script kiddies, spies, insiders, cybercriminals, and cyberterorists. We will describe all them in this following section.

I.2.1. **Hackers** in the past, the term hacker was commonly used to refer to a person who used advanced computer skills to attack the computers. White hat hackers said that their goal was only to expose security flaws and not still or corrupt data. Although breaking into another system is illegal, they considered it acceptable as long as they did not commit theft, vandalism, or breach any confidentiality while trying to improve security by seeking out vulnerabilities. In contrast, the term black hat hackers were used to refer to attackers whose motive was malicious and destructive.

However, today the term hacker has been replaced with the more generic term attacker, without any attempt to distinguish between the motives. Although “hacker” is often used by the mainstream media to refer to an attacker, this term is no longer commonly used by the security community.

I.2.2. Script Kiddies

Script Kiddies are individuals who want to break into computers to create damage yet

lack the advanced knowledge of computers and networks needed to do so. Instead script kiddies do their work by downloading automated attack software (scripts) from Web sites and using it to perform malicious acts.

Today, these scripts have been replaced by attack software with menu system. This makes creating attacks even easier for unskilled users. Over 40 percent of attackers are conducted by script kiddies with low or no skills.

I.2.3. Spies

A computer spy is a person who has been hired to break into a computer and still information. Spies do not randomly search for unsecured computers to attack as script kiddies and other attackers do **;** rather are hired to attack a specific computer or system that contains sensitive information. Their goal is to break into that computer and take the information without drawing any attention to their actions. Spies generally possess excellent computer skills to attack and then cover their tracks.

I.2.4. Insiders

Another serious threat to an organization actually comes from an unlikely source it is employees, contractors and business partners often called insiders. In one study of 900 cases of business "data leakage," over 48 percent of the breaches were attributed to insiders who abused their right to access corporate information. In most instances, insider attacks are more costly than an attack from outsider.

I.2.5 Cybercriminals

There is a new breed of computer attackers known as cybercriminals. Cybercriminals are a network of attackers; identify thieves, spammers, and financial fraudsters. These cybercriminals are described as being more highly motivated, less risk-averse, better funded, and more tenacious than ordinary attackers.

Some security experts believe that many cybercriminals belong to organized gangs of attackers, often clustered in Eastern European, Asian, and third-world region. Cybercriminals often meet in online "underground" forums that have names like DarkMarket.org and theftservicies.com. The purpose of these meetings is to trade information and coordinate attacks around the world. Instead of attacking a computer to show off their technology skills (fame), cybercriminals have a more focused goal of financial gain (fortune). Cybercriminals use vulnerabilities to steal information or launch attackers that can generate income. This difference makes the new attackers more dangerous and their attacks more threatening. These targeted attacks against financial networks, unauthorized access to information, and the theft of personal information are sometimes known as cybercrime. Financial cybercrime is often divided into two categories. The first uses stolen data, credit card numbers, online financial

account information, or social Security numbers to steal from its victims. The second category involves sending millions of spam emails to peddle counterfeit drugs, pirated software, fake watches, and pornography.

I.2.6 Cyberterrorists

Many security experts fear that those terrorists will turn their attacks to a nation's network and computer infrastructures to cause panic among citizens. Known as cyberterrorists, their motivation may be defined as ideology, or attack for the sake of their principles or beliefs. A report distributed by the institute for Security Technology Studies at Dartmouth College lists three goals of cyberattack:

- To deface electronic information (such as Web sites) and spread misinformation and propaganda;
- To deny service to legitimate computer users;
- To commit unauthorized intrusions into systems and networks that result in critical infrastructure outage and corruption of vital data.

Cyberterrorists are sometimes considered the attackers that should be feared the most, for it is almost impossible to predict when or where an attack may occur. Unlike cybercriminals who continuously probe systems or create attacks, cyberterrorists can be inactive for several years and then suddenly strike in a new way. Their targets may include a small group of computers or networks that can affect the largest number of users, such as the computers that control the electrical power grid of a state or region.

I.3. DEFENSES OF AGAINST ATTACKS

Although multiple defenses may be necessary to withstand an attack, these defenses should be based five fundamentals: layering, limiting, diversity, obscurity, and simplicity. These principles provide a foundation for building secure system.

I.3.1 Layering

likewise, information security must be created in layers. Id only one defense mechanism is in place, an attacker only has to circumvent that single defense. Instead, security system must have layers, making it unlikely that an attacker has the tools and skills to break through all the layers of defenses. A layered approach can also be useful in resisting a variety of attacks. Layered security provides the most comprehensive protection.

I.3.2 Limiting

Limiting access to information reduces the treat against it. This means that only those personal who must use the data should have access to it. In addition, the type of access thy have should also be limited to what that person needs to perform their job. Some ways to limit access are technology-based (such as assigning file permissions so that a user can only

read but not modify a file), while the others are procedural (prohibiting an employee from removing a sensitive document from the premises). The key is that access must be restricted to the bare minimum.

I.3.3 Diversity

Diversity is close relating to layering. Just as it is important to prevent data with layers of security, the layers must be also different (diverse). This means that if attackers penetrate one layer, they cannot use the same techniques to break through all other layers.

Information security diversity may be achieved in several ways. For example, some organizations use security products provided by different manufacturers. An attacker who can circumvent a security device from manufacturer **A** could then use those same skills and knowledge to defeat all of the same devices used by organization. However, if devices from manufacturer **A** and similar devices from manufacturer **B** were both used the same organization, the attacker would have more difficulty trying to break through both types of devices because they are different.

I.3.4 Obscurity

Suppose a thief plans to steal the Jewels during a shift change of the security guards. When the thief observes the guar, however, he finds that the guards do not change shifts at the same time each night. Because the shift changes cannot be known for certain in advance, the planned attack cannot be carried out. This technique is sometimes called security by obscurity.

An attacker who knows that information could use it to determine the vulnerabilities of the system to attack it. However, if this information is concealed, it is more difficult to attack a system when nothing is known about it and is hidden from the outside. Obscuring information can be an important means of protection.

I.3.5 Simplicity

Because attacker can come from a variety of sources and in many ways, information security is by its very nature complex. Yet the more complex it becomes, the more difficult it is to understand. A security guard who does not understand how motion detectors interact with infrared trip lights may not know what to do when one system alarm shows an intruder but the other does not. In short, complex system can be a thief's ally.

The same is true with information security. Complex security system can be hard to understand, troubleshoot, and even feel secure about. As much as possible, a secure system should be friendly used for inside users. Complex security schemes are often compromised to make them easier for trusted users to work with, yet this can also make it easier for the attackers. In short, kipping a system simple from inside, but complex on the outside, can sometimes be difficult but reaps a major benefit.

I.4. USRERS SECURITY TRAININGS

With the user security trainings for all the employees in your organization you can achieve:

- Motivate your employees to actually policies and procedures;
- Stop employees from opening suspicions e-mail attachments;
- Thwart “weak link” targeting from internal and external threats;

Prevent damage from revenge hacking by disgruntled employees.

I.4.1 Security Awareness

Security awareness and training are often confused. Awareness changes user behavior; training provides a skill set. Reminding users to never share accounts or write their password down is an example of awareness. It is assumed that some users are doing the wrong thing, and awareness is designed to change that behavior. Security training teaches a user how to do something in right way. Examples include training new help desk personnel to open, modify, and close service tickets; training network engineers to configure a router; or training a security administrator to create a new account.

II. Vulnerabilities

The information age has enabled the Army to use information as an element of combat power. Supporting crises and contingency operations require the rapid expansion of IO (information Operations) capabilities beyond their normal peacetime limits. Deploying forces require secure video, database connectivity, and broadcast and receive capabilities for reach operations access to intelligence, logistics, and other essential support data.

The Soldiers’ mobility capabilities and force sustainment requirements depend on commercial reach operations infrastructures that include international telecommunications and the public switched networks. This increased reliance on reach operations information capabilities by the Soldier has created vulnerabilities to attack from various sources.

Networks and information systems are vulnerable to attack from adversaries who can quickly take advantage of weaknesses in design, ineffective or lax security procedures, or insufficient internal controls. An adversary who may not be a technological equivalent could initiate a covert or overt attack by using inexpensive, commercial off-the-shelf products and attacker tools obtained from the Internet. The attack can be from any location that has access to the Internet. Recent trends that have increased vulnerability include use of commercial services, commercial off-the-shelf hardware and software, the integration and consolidation of

stovepipe systems, moving toward an open systems environment, and extensive interfacing with government, industry, and public networks.

A vulnerability analysis should be conducted to assess the security status of networks and information systems. A vulnerability analysis should be conducted or requested at every organizational level. The analysis can ensure that the network or information systems security features are properly configured for optimum IA capabilities. Another critical component of an effective vulnerability analysis program is the periodic review of the IA tools in use to ensure that the latest version is installed. An effective program will identify unauthorized users and unauthorized use of the network or information system. Once unauthorized activity is identified and verified, established incident and vulnerability reporting procedures must be followed.

II.1. INFORMATION SYSTEMS SECURITY

IA programs within the Army must include the full range of security measures. Information systems security occurs only when a common set of technical procedures apply to all assets connected to the common-user LAN and throughout the WAN. Protection from intrusions into or via a WAN must begin with a cooperative information systems security effort between all of the services. All security measures taken to detect, respond to, react to, and report attacks and intrusions will adhere to public laws, MOD directives, and ARs. System administrators and network managers are required to complete IA security and awareness certification training. Specific information regarding measures to reduce the threat, vulnerabilities, and risks will be covered for the information systems under their purview.

II.1.1. LEVEL OF CONCERN

All information systems will be assigned a level of concern rating based on the confidentiality, integrity, and availability of the information processed, stored, or transmitted. The level of concern rating for each of these areas can be basic, medium, or high. The decision regarding the level of concern will be explicit for all systems.

II.1.2. PROTECTION LEVELS

Protection levels only apply to confidentiality requirements. Protection levels are based on the required clearance, formal access approval, and need-to-know of all direct and indirect users who receive information from the information systems without manual intervention and reliable human review. Protection levels indicate the implicit level of trust that is placed in the system’s technical capabilities. The service providers and the users must cooperate to implement the required level of protection. The Soldier must have assurance that his information systems have the level of protection or trust required for a successful mission.

II.2. PROTECTION, DETECTION, AND CAPABILITIES

Information and network systems are critical to the military's ability to conduct operations. The Soldier's assurance that networks and information systems are defended adequately against attack requires the ability to:

- Protect the information that computer systems and data networks pass and store.
- Detect when an intrusion into the network or information system happens.
- React to contain the damage and repair the network or information system.

II.2.1. PROTECTION

Information protection is active or passive measures that protect and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information. It denies enemies, adversaries, and others the opportunity to exploit friendly information and information systems for their own purposes.

Information protection includes information assurance, computer network defense, and electronic protection. All three are interrelated.

- Information assurance consists of measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and no repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
- Computer network defense consists of actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Ministry of Defense information systems and computer networks. Effective network defense assures Army computer networks' functionality. It detects and defeats intruders attempting to exploit Army information and information systems. Commanders and staffs remain aware of and account for information on regulated (Ministry of Defense) and no regulated (Internet) networks. They analyze how information from these mediums affects their operation; they take action to mitigate the associated risks.
- Electronic protection is that division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability

Information protection applies to any medium and form including hard copy, electronic, magnetic, video, imagery, voice, telegraph, computer, and human. Information protection involves determining the appropriate security measures based on the value of information protected. The protection measures should reflect the changing value of the information that pertains to each

operational phase of any given mission. Ensuring the protection of information is the responsibility of leaders, information producers, processors, and users.

The protection measures should consist of firewalls, IDSs, and software that harden these systems against intruders.

Army network and system managers must devise and implement comprehensive plans for using a full range of security means. The plans will include external and internal perimeter protection. External perimeter protection consists of COMSEC (communication security), router filtering, access control lists (ACL), security guards, and physical isolation serving as a barrier to outside networks such as the Non-Secure Internet Protocol Router Network (NIPRNET). Internal perimeter protection consists of firewalls and router filtering. Internal COMSEC barriers are also required. Local workstation protection consists of individual access controls, configuration audit capability, protection and intrusion detection tools, and security procedures.

Other considerations that must be addressed when protecting vital networks and information systems include:

- Developing comprehensive training programs. Programs should instill IA intrusion and detection doctrine, and operational procedures in all members of the command.
- Developing vigorous programs for sharing results of red team and vulnerability assessments.
- Programs that have a standard practice at the appropriate levels of information flow;
- Ensure intrusion protection and detection systems are employed at all levels of network management.
- Train to protect against, detect, react to, and restore from intrusions should become a common task

Other initiatives to enhance the architecture and limit intrusions into the NIPRNET are underway. These initiatives include routing communications through a limited number of gateways and closing access to networks through other connection points around the globe (thus easing monitoring tasks and responsibilities), and upgrading firewalls and IDS devices to help prevent unauthorized entries.

Protection against intrusions into friendly computer networks by denying unauthorized entry and access into these systems is essential for network and system protection. Operational Security procedures allow the commander to identify actions that adversary intelligence systems and intruders observe. It provides an awareness of the indicators that adversary intelligence systems might obtain. OPSEC identifies and selects information that is subject to exploitation by adversaries and identifies countermeasures that reduces risk to an acceptable level.

New global commercial capabilities (including imaging, positioning, and cellular systems) offer potential adversaries access to an unprecedented level of information about our forces. Army and other service personnel can send information directly from the battlefield via e-mail to points around the world from most areas of operation. These e-mails may contain sensitive or classified information, and if disclosed, could endanger personnel and compromise missions.

The Internet is the preferred communications platform for intruders to launch an attack or intrusion. Normally, the intruder's IP address is difficult to track, making it impossible to apprehend the perpetrator.

Security measures and procedures must actively and passively preserve the confidentiality, integrity, and functionality of information systems. Protection includes real and near-real-time measures that detect intrusions and then restore the affected device or system. Security measures that assist in protection include:

- Adopting vigorous IA protection programs.
- Denying unauthorized access.
- Hardening programs and gateways with specific software and hardware means.
- Developing procedures for quality assurance in all program and hardware acquisition.
- Strict access control for use of networked computers and other devices.

Transmission security secures information across the various networks. Trunk encryption devices, in -line encryption devices, COMSEC, frequency hopping, and time division techniques usually secure transmissions. Transmission security ensures information security when using one or more of these techniques or devices. All systems must operate in SECRET systems high mode to prevent the intrusion into information systems. Any non-secure system or device connected to, or entering, any secure network must have an inline encryption device in use between the network entry point and the entering equipment. This ensures complete network security.

COMSEC in networks and system devices is essential in order to protect the networks information. Specific keys enable secure encryption of the voice and data passed through transmission devices and computers.

Information security policies deny unauthorized persons access to classified or sensitive information during electrical transmission from the sender to the receiver. They establish requirements designed to prevent the disclosure of valuable information from other aspects of communications (for example, traffic flow and message analysis) and to enhance the authentication of communications.

II.2.2. DETECTION

Real-time security management and intrusion detection should be included in routine operations for NOSCs (network operations and security center). To detect occurrences that constitute

violations of security policies, selected events or occurrences (such as numerous log on attempts within a specified period) are monitored using conventional protection and detection tools and devices. When violations are detected, the network manager must prevent further violations and report the event to the commander, information assurance security officer (IASO), and regional computer emergency response team (RCERT)

NOSCs (network operations and security center) provide near real-time surveillance for networks and systems to detect suspicious security events and initiate preliminary defensive actions to block or contain the attack in order to minimize the operational impact. Robust and resilient infrastructure architecture isolates and controls the damage from attacks, and makes these systems readily repairable in case of attack. The fundamental criteria are that no single attack leads to failure of a critical function, and no single protection mechanism protects critical functions or systems.

Network managers and users must train in all aspects of information systems security on the systems they operate and maintain. They must maintain the audit functions and review audit information for detection of possible system abuse. They must also coordinate with the information assurance manager (IAM), information assurance network manager (IANM), IASO (information assurance security officer), and other appropriate agencies when violations occur.

Appropriate safeguards detect and minimize unauthorized access and inadvertent, malicious, or non malicious modification or destruction of data. Appropriate detection safeguards ensure security classification labels remain with data transmitted via a network to another information system.

Security management devices and IAVMs (information assurance vulnerability management) warn NOSC (network operations and security center) personnel of intrusion attempts, attacks, and other anomalies for networks and systems. The response to these alerts depends on the severity of the attack, intrusion, or breach. Appropriate reactive measures must be taken when problems occur. Network managers need to consider operational status or mission status before responding to alerts. The information systems protection concept envisions real-time security management as a component of NETOPS (network operations) as well as being incorporated into the operations. When detection occurs, network managers may need to take the following actions:

- Change boundaries and perimeters.
- Reconfigure firewalls, guards, and routers.
- Reroute traffic.
- Change encryption levels or re-keys.
- Zeroize suspected compromised communications.
- Re-establish a net without selected members.
- Change passwords and authentication.

II.3. PASSWORD CONTROL AND AUTHENTICATION

Passwords are an important aspect of computer security and are used to achieve authenticated access control at the workstation or host level for authenticating user's access to Army resources until *Common Access Card* is implemented or for personal use. A poorly chosen password may result in the undetected compromise of an Army network or unlawful usage of Army systems. As such, all users, employees, including contractors and vendors, with access to Army information systems, are responsible for taking the appropriate steps to select and secure their credentials. Basic password guidelines are:

- After generation, password handling and storage are at levels of the most sensitive data contained in the system. Password issuance is only available to users authorized to access the system.

At the time of password issuance, all users will be briefed on:

- Exclusiveness, classification, and uniqueness of each password.
- Safeguard measures required for classified and unclassified passwords.
- Prohibitions against disclosure to anyone, to include personnel assigned to the same project and holding identical clearances.
- Immediately informing the IASO (information assurance security officer) of password disclosure, misuse, or other potentially dangerous practices.
- One time issuance of password.
- Retirement of passwords when the time limit has expired or the user has transferred to other duties, been reassigned, retired, or been discharged or otherwise separated from the duties or the function for which the password was required.
- Passwords, as unique identifiers of individual authority and privileges, are strictly for use by one user.
- Disable remote device password save-functions incorporated within software or applications to prevent storage of plain text passwords.
- Protection of passwords against unauthorized observation on terminals and video displays.
- In addition to a password, a user can be authenticated by something the user possesses (token), or a physical characteristic (biometric).

III. INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE

Army commanders rely on information support to plan operations, deploy forces, and execute missions. By protecting the flow of information from attacks, intrusions, and interruptions, the commander can be assured of gaining and maintaining information superiority

IA is the defensive component of information operations that with concurrent use of validated intelligence defining the threat enables the availability, integrity, authentication, confidentiality, and non-repudiation of friendly information and information systems in the information environment that is now a component of the operational environment. IA provides protects the nets against exploitation, degradation, and denial of service. The MOD incorporates vigorous protection, detection, reaction, and restoration capabilities. This incorporation allows for effective defensive measures and timely restoration of debilitated networks and information system

IA capabilities reside in depth. Network and information system managers must actively monitor and evaluate the effectiveness of the IA systems used in their Area of Responsibility. They must maintain an awareness of the overall network status, incident reporting, and network management processes to integrate IA into the Network Operation activities, functions, and tasks. IA-trained personnel must be integrated into the Army at all echelons. This placement ensures the expertise to quickly determine the cause of and take appropriate action in response to IA issues as they affect the land nets.

IA encompasses a diverse field of network and information systems security disciplines. The Army Information Assurance Program focuses the Army's efforts to secure information and its associated systems and resources. It provides a unified approach to protecting classified and sensitive information by using the risk management approach for implementing security safeguards. The Army Information Assurance Program is not limited to information security; it covers other aspects of security such as COMSEC, emission security, operations security (OPSEC), physical security, personnel security, and industrial security.

The interactive nature of the Army's technical networks and information systems using the publicly available Internet in light of these threats makes them vulnerable to intrusions and disruptions.

The MOD strategy protects networks and information systems through a layered series of protective perimeters enhanced protect, detect, and react capabilities; and a supporting IA infrastructure. It is a long-term, dynamic strategy that incorporates IA/CND (computer network defense) tools and policy enforcement, and it uses current and evolving technology, policies, procedures, and trained, knowledgeable people. The strategy is flexible and adjusts to changes in technology that may pose new attack threats or offer new protection capabilities.

Commanders must develop comprehensive protection measures in anticipation of how an adversary may use elements of attack and intrusions to disrupt systems and networks. These measures keep in mind the guiding principles of the MOD strategy, including risk management, vulnerability assessment, levels of concern and protection, and the capability to detect and react to attacks and intrusions.

III.1. INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE FUNDAMENTAL ATTRIBUTES

The IA/CND (Computer network defense) mission essential task ensures the fundamental attributes of availability, authentication, confidentiality, integrity and non-repudiation of friendly information and information systems while denying adversaries access to the same information and information systems. The fundamental attributes are:

- **Availability.** Actions taken to allow the timely, reliable access to data and information services for authorized users.
- **Authentication**. A security measure designed to establish the validity of a transmission, message, originator, or as a means of verifying an individual's authorization to access specific categories of information.
- **Confidentiality**. Actions taken that assure information is not disclosed to unauthorized individuals, processes, or devices.
- **Integrity.** Assuring the quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. In a formal security mode, integrity is interpreted more narrowly to protect against unauthorized modification or the destruction of information.
- **Non-repudiation**. Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity in order to create a record of the parties that processed the data.

IA/CND (Computer network defense) incorporates those actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within MOD information systems and computer networks. IA incorporates protection, detection, and response capabilities while providing for restoration of information systems it provides and-to-end protection to ensure data quality and protection against unauthorized access and inadvertent damage or modification. CND (Computer network defense) activity employs IA protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information.

CND (Computer network defense) response actions include defensive and restoration actions. Response actions are deliberate, authorized defensive measures or activities that protect and defend MOD computer systems and networks under attack or targeted for attack by adversary computer systems and networks. CND (Computer network defense) response actions extend MOD's layered Defense in deep capabilities and increase MOD's ability to withstand adversary attacks. Objectives for using CND (Computer network defense) response actions include:

- Strengthening MOD's defensive posture and operational readiness.
- Halting or minimizing attack effects or damage.
- Supporting rapid, complete attack characterization.

IA and CND are focused on assured information protection and assured network and information system availability. The objectives of this focus are achieved by:

- Instituting agile capabilities (firewalls, password protect, intrusion detection, etc) to resist adversarial attacks through recognition of the attacks as they are initiated or are progressing.
- Efficient and effective response actions to counter the attack, and safely and securely recover from such attacks.
- Reconstituting capabilities from reserve or reallocated assets when original capabilities are destroyed.
- Maintaining correlation activities between user elements to ascertain hostile IA/CND events from other system outages or degradations.

III.2. THREATS AND LEVEL CATEGORY

Threats to the LWN are genuine, world-wide in origin, technically multifaceted and growing. They come from individuals and groups motivated my military, political, cultural, ethnic, religious, personal, or industrial gain. According to FM 3-13, the capabilities of adversaries operating in the information environment are:

- **First level**: lone or small groups of amateurs using common hacker tools and techniques in an unsophisticated manner without significant support.
- **Second level**: individuals or small groups supported by commercial business entities, criminal syndicates, or other transnational groups using common hacker tools in a sophisticated manner. This level of adversary includes terrorists and non-governmental terrorist organizations. Their activities include espionage, data collection, network mapping or reconnaissance, and data theft.
- **Third level**: individuals or small groups supported by state-sponsored institutions (military or civilian) and significant resources, using sophisticated tools. Their activities include espionage, data collection, network mapping or reconnaissance, and data theft.

- **Fourth level**: state-sponsored offensive IO, especially computer network attacks, using state-of-the-art tools and covert techniques conducted in coordination with military operations.

These events and incidents (both initiated by potential or actual adversaries or by Army users or administrators as a result of carelessness or non-compliance) are identified by the IA and CND (Computer Network Defense) communities into categories that include:

- **Category 1**: root level intrusion (incident) unauthorized privileged access (administrative or root access to a MOD system).
- **Category 2**: user-level intrusion (incident) unauthorized non-privileged access (user-level permissions) to a MOD system.
- **Category 3**: unsuccessful activity attempt (event) attempt to gain unauthorized access to the system that is defeated by normal defensive mechanisms. Attempt fails to gain access to the system (e.g., attacker attempt valid or potentially valid username and password combinations) and the activity cannot be characterized by as exploratory scanning.
- **Category 4**: denial of service (incident) activity that impairs, impedes, or halts normal functionality of a system or network.
- **Category 5**: non-compliance activity (event) activity that due to MOD actions (or non-actions) makes an IT system potentially vulnerable (e.g., missing security patches, connections across security domains, installation of vulnerable applications, etc.).
- **Category 6**: reconnaissance (event) an activity (scan or probe) that seeks to identify a computer, an open port, an open service, or any combination thereof for later exploit.
- **Category 7**: malicious logic (incident) installation of malicious software (e.g., Trojan, backdoor, virus, or worm).

The globalization of network communications and the IT marketplace creates vulnerabilities due to increased access to the information infrastructure from points around the world and the uncertainties of the security of the IT supply chain. Threats to the information systems and networks relied upon by strategic and tactical forces exist from various sources.

Attacks and intrusions compromise missions, corrupt data, degrade networks and systems, and can destroy hardware and software applications. These results hamper the effectiveness of support forces and the supported Soldier.

III.3. INTENTIONAL INTRUSION

Intentional intrusion into a network or system is a deliberate act. This act has proven to be one of the most challenging to protect against, detect, and react to. Examples of intentional intrusion include:

- **Unauthorized users, such as attackers.** Attackers are the source of most attacks against information systems in peacetime. They mostly target personal computers, but recently have targeted network communications, mainframes, and local area network (LAN) based computers.
- **Trusted insiders with legitimate access to a system.** They pose one of the most difficult threats to defend. Whether recruited or self-motivated, insiders can access systems normally protected against attack. While insiders can attack at almost any time, a system is most vulnerable during the design, production, transport, and maintenance stage.
- **Terrorist groups** who have access to commercial information systems (including the Internet).

They may obtain unauthorized access to an information network or direct attacks against the infrastructure (bombing). Terrorists use computer bulletin boards and Internet systems to pass intelligence and technical data across international borders. These organized groups pose a serious threat to the information infrastructure and national security of state.

- Foreign intelligence services that are active during peace and conflict and take advantage of the anonymity offered by the computer, bulletin boards, and the Internet. They hide organized collection or disruption activities behind the facade of unorganized attackers. Their primary targets are often commercial, scientific, and university networks. They may also directly attack military and government networks and systems.
- Opposing militaries or political opponents. While the adversary's activities are more traditionally associated with open conflict or war, opposing militaries or political opponents may invade computer and telecommunications networks during peacetime. Such strikes help frame the situation to their advantage preceding the onset of hostilities. Adversaries may also try to manipulate the news media and public opinion to their advantage.

III.4. ATTACKS

An intentional intrusion is an attack against computers or information systems. Some attacks have a delayed effect and others are immediate. Both the delayed and immediate attacks corrupt databases and controlling programs, and may degrade or physically destroy the system attacked. Timely attack detection is essential to initiating network restoration and network intrusion response capabilities. The following paragraphs discuss types of attacks.

Computer attacks generally aim at software or data contained in either end-user or network infrastructure computers. Adversaries aim at unobtrusively accessing information, modifying software and data, or totally destroying software and data. These activities can target individual computers or a number of computers connected to a LAN or wide area network (WAN). Computer attacks may take place during routine tactical operations and may be multifaceted to disrupt major military missions. These attacks can also take place during wartime and peacetime. Attacks can be part of a major nation-state effort to cripple the national information infrastructure. They can also come from mischievous or vengeful insiders, criminals, political dissidents, terrorists, and foreign espionage agents.

Malicious computer attacks can be intentionally designed to unleash computer viruses, trigger future attacks, or install software programs that compromise or damage information and systems. They may also involve unauthorized copying of files, directly deleting files, or introducing malicious software or data. Malicious software generally consists of executable software codes secretly introduced into a computer and includes viruses, Trojan horses, trap-doors, and worms. Malicious data insertion, sometimes termed “spoofing,” misleads a user or disrupts systems operation. For example, an attack disrupts a packet data network by introducing false routing table data into one or more routers. An attacker who denies service or corrupt data on a wide scale may weaken user confidence in the information they receive by corrupting or sending false data.

Physical attacks generally deny service and involve destruction, damage, overrun, or capture of the systems components. This may include end-user computers, communications devices, and network infrastructure components. A physical attack involves the overrun and capture of computer equipment that allows the adversary to employ a computer attack. Another form of physical attack is theft of items, such as cryptographic keys or passwords. This is a major concern since these items can support subsequent electronic or computer attacks.

Electronic attacks focus on specific or multiple targets within a wide area. Attacks against communications links include the following two types of signal intelligence operations: signal intercept and analysis to compromised data and emitter direction findings, and geo-location to support signal analysis and physical attacks. “Jamming” is another attack against communications

links. Jamming corrupts data and may cause denial of service to users. For example, the jamming of communications links supporting global positioning system users is a specific concern.

CONCLUSION

According to these researches and my experience, we have to stay always updated with new technologies and its responsibilities. One day we are well protected, but the other day may appear very devastating attacks. We need to implement and update new policies and regulations for army security operations. Implementation of policies in subordinated units must be controlled. Principle need to know must be implemented. Threats of information security are around us even the civilian sectors. There are cases of hacking companies and destroying their repudiations, stilling sensitive information or modifying the databases. CIA (Confidentiality Integrity and Availability) must be in place.

REFERENCES

- https://www.privateinternetaccess.com
- https://www.staysmartonline.gov.au
- Army Field Manual FM 6-02.71 NETWORK OPERATIONS;
- ACP 122F.

MOBILE SECURITY TENDENCIES

Author:
CMD eng. Gily COCALCU

INTRODUCTION

The complexity of today's technologies, regulations, business processes, security threats and a multitude of other factors greatly increases the risks faced by businesses today.

As global networks expand over the wide-interconnection of the world information systems, the smooth operation and communication and computing solution became vital. However, recurring events such as virus and worms attacks at the success at criminal attackers illustrate the weaknesses in current information technologies and the need to provide heightened security for these systems. Mobile devices are playing an ever-increasing role in changing the way and concept of information communication system. Mobile device technology is now advanced by the usage of smartphones and tablets.

Table I gives the number of mobile devices shipped worldwide in 2012 based on data from Canalys[1].

Device type	2012 shipments	2016 shipments	2012–2016 CAGR
Basic phone	122.0	58.0	−17.0%
Feature phone	770.8	660.9	−3.8%
Smartphone	694.8	1,342.5	17.9%
Tablet	114.6	383.5	35.3%
Notebook	215.7	169.1	−5.9%
Netbook	18.3	0.3	−64.2%
Total	1,936.2	2,614.2	7.8%

It’s no exaggeration to say that smartphones, tablets or various device models coming out every day, are becoming omnipresent in government fields and also in the large population and it’s no wonder. For the worker always on the move, everything from email to socialization, as well as news and entertainment, is now available in a convenient, very easy to carry device. These devices allow users to remain active, even when walking between destinations, stuck on public transit, or during downtime in meetings. Clearly, they’re here to stay. This work papers will show the various security risks and opportunities that arise with the ubiquity of modern mobile pocketable devices.

These devices are closest real mobile computers. Current-generation smartphones and tablets generally use ARM microprocessors with clock rates over 1 GHz, which have dual, or quad-core CPUs and even higher clock rates. They have gigabytes of storage, wireless, bluetooth, 3G or 4G built in connection and faster available networks. In this respect, current mobile devices are faster and better-equipped than desktop computers from a decade ago. This is an interesting opportunity mostly tablets and smartphone are more than adequate when it comes to raw resources in order to leverage decades of research into secure operating systems. Smartphones offered by most vendors can and will soon run full-blown Unix-style operating system kernels like Joomla OS. This means that security features ranging from virtualization and secure booting to information flow control and multi-level security can potentially be applied to creating high-assurance software within our phones.

In the "*pluribus Omni"* stakes society, when it comes to the socio-economical-political life and domains as government, military, private and public sectors, IT departments etc are looking to lock personnel out of social sites and push these users to do these activities on their own personal devices. As a result the usage of smart devices employed at their own usage by the personnel is on the rise. Nowadays Android market applications are rapidly increasing in availability and there are millions of applications available to download just by a single click. All these apps, before everything else, oblige the user to give his accord to store sensitive and private information on different servers.

"Safe" web sites can and will be compromised. In environments where social networking is banned, a typical firewall policy is to ban sites known to be undesirable and allow everything else (sometimes called a "blacklist" policy). More aggressive IT managers may default to banning everything, by default, and only allowing a handful of known-good sites (sometimes called a "whitelist" policy). The problem with blacklists is that they're always missing something bad. The problem with whitelists is that any arbitrary web site may fall victim to a security-related attack.

Most of the regular smartphone users have some information stored in their mobile phone that they consider sensitive and secret. An average user today has about 25 passwords to manage and if they find difficulties to memorize them, they tend to use weak or easy-to-memorize passwords. Even after choosing easy passwords they usually forget some of them after sometime anyway[2]. This information can be categorized as mobile data.

I. EVOLUTION OF MOBILE MALWARE

Smart devices increasingly store and provide access to a range of personal, corporate, financial and security-related data. While the availability and ease of access to such data via different types of network connections (e.g. Wi-Fi, cellular), the ability to download, install and use mobile applications, and the practicality of using networked services while on the go make the smart mobile device an inseparable companion to the modern man, they also provide the perfect breeding ground for malicious software. Cyber-criminals have not had continuous access to such varied sources of personal and financial data before the advent of the Smartphone. Increasing use of mobile payments presents a new area to exploit, and attackers have already devised covert ways to make direct financial gain from the mobile users, e.g. via premium calls and SMS[3]. Furthermore, the use of multiple communication technologies in smart devices allows attackers to cross service boundaries. For example, an attack carried out over Wi-Fi would allow the attacker to launch attacks over the mobile phone network.

Mobile malware attacks showed increasing levels of sophistication. From traditional social engineering lures, cybercriminals developed new methods of victimizing users throughout the year. The introduction of new methods can lead to more complex attacks in the future.

I.1. Driving the need for mobile security

More powerful and less expensive mobile devices are becoming ubiquitous and are as irreplaceable as any PC or laptop, significantly increasing the risks from loss and theft. Mobile handsets are becoming more powerful with each new release, to the point where the newest and smartest mobile devices are more like handheld computers than cellular phones.

In order to follow the growing mobile threat, there is an urgent need to detect, analyze and understand the new vulnerabilities and threats in the smart mobile ecosystem, which are a result of the evolution of mobile networks and smart devices, the changing way users interact with technology, the popularity of smart devices, and the heterogeneity of the wireless interfaces, supported platforms and offered services.

In order to advance in the fast moving field of cyber-security and to counter existing and potential mobile threats, we need to be proactive and work on predicting threats and vulnerabilities to build our defenses before threats materialize.

I.2. Malware: origins and destinations

Mobile malware uses various infection vectors in order to gain access to the device; the top two main categories of attacks based on the vulnerabilities they use are:

• *Exploiting* hardware or software vulnerabilities of devices to completely bypass the user and install malware. Some of the exploits used to attack smart devices are near field communication (NFC) technology, third-party kernel drivers, Android firmware vulnerabilities, and mobile web browsers. For example, some malicious websites use mobile browser exploits to install malware on the device without any user interaction other than visiting the site. Android firmware and third-party driver exploits have been used by malware to elevate their privileges and thus gain root access to the device, allowing them to practically do anything they want without the user's knowledge[4]

• *Social engineering* is by far the most common method used to infect smart mobile devices, where users are "tricked" into installing the malware themselves. Social engineering includes all techniques that exploit the human user, such as phishing, application repackaging, etc., in order to infect the device. Social engineering is popular since it does not require any technical investment by the attacker, i.e. the identification of a new exploit and the development of a delivery system that uses it. Upcoming malware will continue to employ social engineering in new ways; for example, we have already witnessed the first malicious QR codes, which need to be scanned by the user for their activation.

Independently of how it infects the device, once the malware is installed, it performs one or more malicious activities, such as:

- stealing user information;
- monitoring;
- adware;
- premium service abuse;
- click fraud;
- ransom;
- search engine optimization;
- e-mail spam and SMS;
- malicious downloading;
- botclient;
- rooting;
- Denial-of-service.

Smart devices are open to both traditional and mobile specific threats due to the multiple roles smart mobile devices play and the heterogeneity of mobile communication technologies and networked services[5].

We should expect to see a sharp increase in attacks against end-users and administrators who are accessing and controlling cloud-based services (both public and private clouds). Much of the focus is on the security of the cloud itself but very often the end-

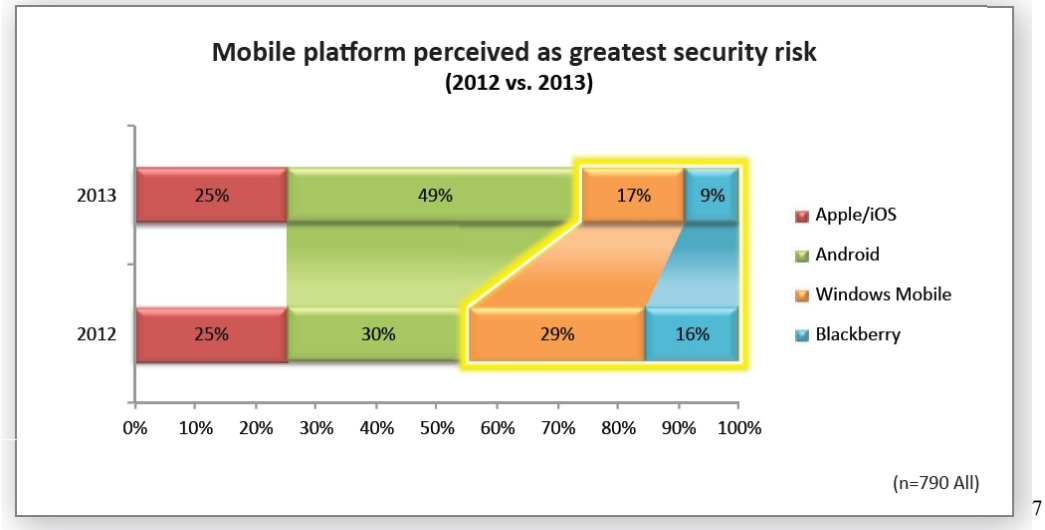
users are left to their own while connecting from less secure public networks. Administrators in particular will be targeted as they hold the keys to the cloud-based kingdom.

I.3. Which O.S. platform is most attacked?

Android is trusted less; Windows Mobile and BlackBerry are trusted more for security, according to check-point mobile security survey report June 2013[6]

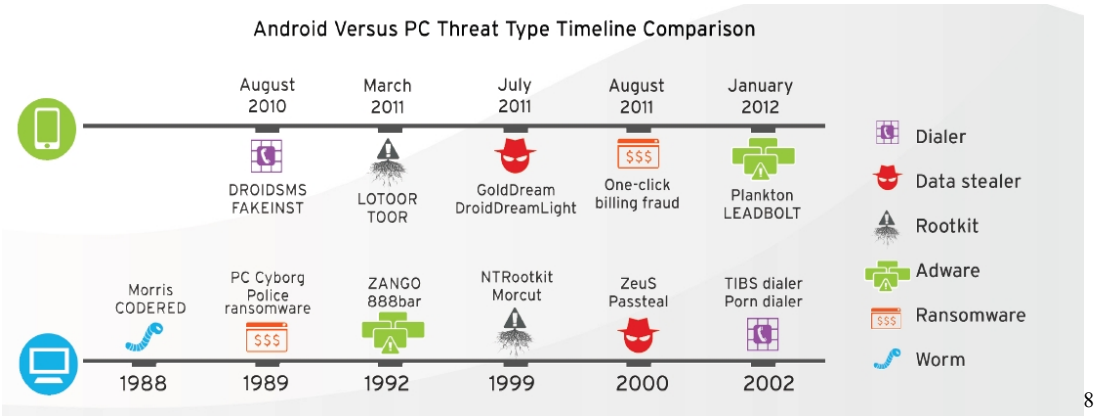
Participants were asked which of the most common mobile platforms they viewed as being the greatest risk to their corporate security. Android was by far the most frequent platform indicated (49%), followed by Apple/iOS (25%) and Windows Mobile (17%).

This question showed a dramatic change from the previous year. Android increased dramatically as the platform perceived to have the greatest security risk. Windows Mobile and BlackBerry both saw the number of IT professionals who viewed this as the most risky platform decrease by almost half.



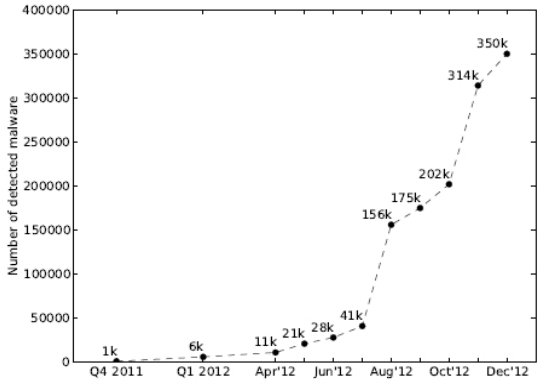
[7]

I.4. How fast is mobile malware growing?

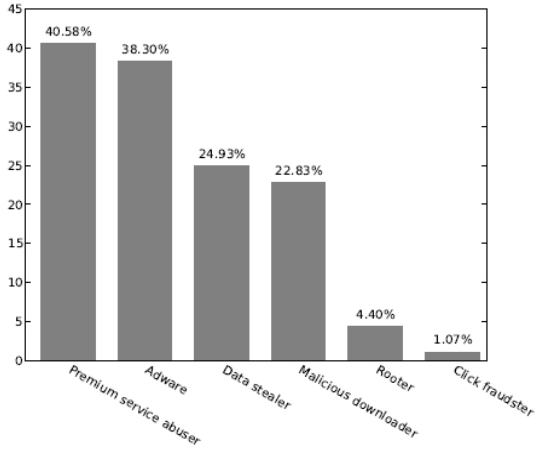


[8]

TrendLabs research shows that Android seems to be repeating history by way of Windows. The platform's growing dominance in the mobile landscape echoes that of Windows in the desktop and laptop space. And much like Windows, Android's popularity is making it a prime target for cybercriminals and attackers, albeit at a much faster pace.[9]



(a) The number of detected Android malware in 2012. The data shows a rapid increase in malware, especially in Q3-Q4 2012, which was due to aggressive adware.



(b) The distribution of malware types for the top ten Android malware families in 2012

- Growth of malware exposure from 2011 - 2012 [10]-

The growth of Android malware also indicates the speed by which cybercriminals are targeting multiple platforms.

II. RISKS IN MOBILE WORLD

Risk is the possibility of something adverse happening. Risks are generated by threats. The risks are different from final consumer or an enterprise point of view because of their value of damage is also different, even if they are affected by the same threat.

Any information stolen by data stealers may be used by cybercriminals for malicious schemes like following:

- Attacks are seeking corporate and personal data in the cloud:

As much as enterprises are relying on various cloud services for managing their customer private data, internal classified project plans and financial assets, we can expect to see that hackers attacks will be more interested to target endpoints, mobile devices and credentials as means to gaining access to corporate or personal clouds. It's very hard to guess what kind of forms future attacks will take—but we can presume randomly taking hostage not just your local classified projects or documents, but any type of cloud-hosted data. These attacks may not need any data encryption and could look like a blackmail—threats of publishing your confidential data or classified information. Cloud data access secure policies and hard to brake password settings are more important than ever. An enterprise security is

only as good as its weakest point, in many cases its employees or users' awareness and security training.

- Advanced persistent threats meeting financially motivated malware.

We can also predict a bigger successfully end-rate of advanced persistent threats (APT's) in doing some attacks for the purposes of industrial espionage will inspire old-school financial malware gangs to adopt their techniques. Because security vendors are struggling to improve layers of defense, OS security and user awareness, cybercriminals are forced to make more money from a smaller number victims. New attacks initiated by usual malware actors could include in future, components and delivery machine built or customized especially for a narrower target audience. Cross line which shows the difference between APT and traditional malware will continue to move in the future.

- Android malware is following an ascendant trend and is seeking out new targets:

In 2013 we've already seen the exponential growth in Android malware, not only in terms of the number of families and samples, but also the number of devices affected globally. In time while we wait that new security features in the Android platform to make a positive change in infection rates over time, their implementation will be slow, leaving most users exposed to ordinary social engineering attacks. Hackers will continue to explore new roads for Android malware monetization. Although cybercriminal's vulnerability paths on this platform are more limited than Windows, mobile devices are an attractive launching pad for attacks which are directed toward to social networks and cloud platforms.

- Continuous changing malware turning more specialized:

The financially-motivated malware, differing from various geographic and economic regions, like the case of country-specific social engineering techniques, will likely continue to grow in 2014, and will differentiate between consumer and business users. Also to be expected are specialized attacks in relation to the varying degrees of cyber-defense level and target value.

- Threat to the personal data from mobile apps/social networks:

The hot topic in 2014 will continue to be the mobile security. The socially engineered scams and data exfiltration attempts will have a wider attack surface particularly because of the adoption of emerging apps for personal and business communication. The cyber-crooks see your address book and your social connections graph as treasure for of all sorts. Mitigation will come by way of mobile and web applications control for business users.

- Penetrating defenses:

In this area we expect to see new weapons aimed at the latest cyber-defense mechanisms by way of the security vendors because reputation services, cloud security

databases, white listing and sandboxing layers will be attacked in new and sinister ways. More and more malware signed with stolen digital signatures, attempts to poison security data and telemetry analytics, new sandbox detection and bypass techniques, and increased use of legitimate tools for malicious purposes.

- Undermining hardware, infrastructure and software at the core:

Broad-scale compromise of the core infrastructure we all operate on is not only possible, but happening. There is a need to re-evaluate technologies and trusted parties. We can expect to see many more of these stories in this year. Most enterprises won't have the resources or skills to go digging for backdoors, but is wise to closely monitor the work of security researchers and media outlets for new revelations.

- An all-out hack-a-thon:

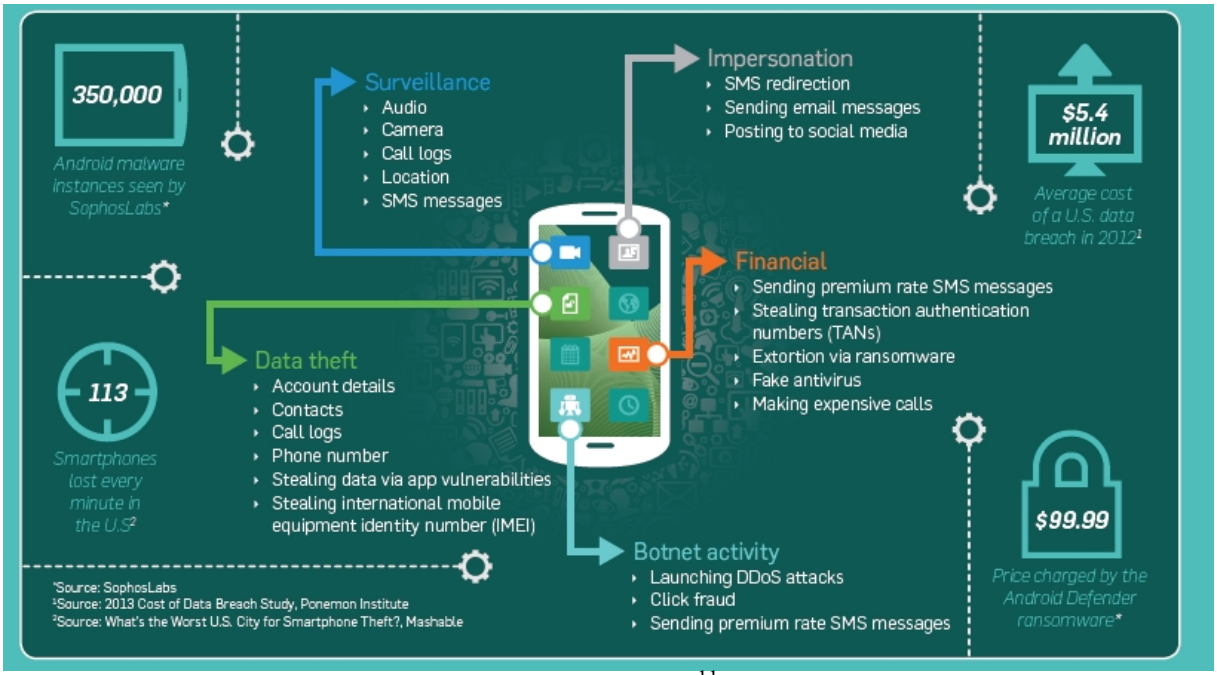
We continue to diversify the devices we use, and they hold sensitive business and personal data. The security is not as well developed on such devices as the traditional PC environment thus making embedded devices in our homes, offices and even cities represent interesting attack targets. The new electronic currencies, like Bitcoin, and payment techniques, like PayPal, make far more than just the credit card.

II.1. Risk for the end-user segment

Cybercriminals can, take advantage of a user's contact list for SMS phishing or sell stolen information in the underground market. Some frequently stolen data include:

•Location	•Phone number	•Contact list
•Network operator	•Text messages	•International Mobile Station Equipment Identity (IMEI)
•Phone ID and model	•Application Programming Interface (API) key	•International Mobile Subscriber Identity (IMSI)
•Application ID		

Anatomy of a Hacked Mobile Device: How a hacker can profit from your smartphone:



– An example -[11]

Your Android smartphone may look innocent. But when compromised by malware, it can illegally watch and impersonate you, participate in dangerous botnet activities, capture your personal data, and even steal your money.

With the continued development and proliferation of intelligent portable electronic devices there is a predictable rise in account compromises resulting from the credentials for those accounts being stored on unsecured devices. While the user may have selected a password of sufficient length, when it's stored on an unsecured device it may be easily recoverable by an attacker.

Premium service abusers topped the list of most commonly seen Android malware in 2012. Often disguised as popular apps, they are designed to trick users into installing them. We spotted a rogue version of the game "Bad Piggies," which was actually a FAKEINST variant. SMSBOXER variants spoof several best-selling Android apps, including "Angry Birds Space" and Instagram. GAPPUSIN variants, meanwhile, download other malicious apps and steal information from infected devices.[12]

II.2. Enterprise segment risk

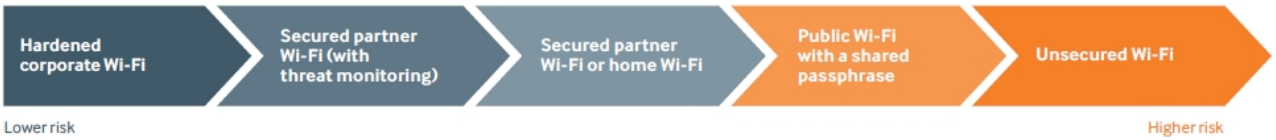
A common motivator for to introducing a mobile devices policy is 'top down' – in other words, senior management levels within an organization have perhaps identified business opportunities that require the use of mobile devices, or maybe they just want to support modern ways of working. Alternatively, the motivator could be 'bottom up', where

employees are pressuring IT staff and management to be allowed to use their beloved personal gadgets for work purposes.

Here are some threats from corporate use of mobile devices:

1. **Loss of corporate data due to:**
    - *Physical Compromise of Device:*
        - Device lost,
        - Device stolen,
        - Decommissioned device.
    - *Logical compromise of Device:*
        - Malicious app installed by user;
        - Compromise of user application;
        - Malware infects device;
        - Insecure corporate application enables access to data;
    - *User actions:*
        - User stores data inappropriately;
        - User tricked into disclosing data as a result of social engineering.
    - *Communications compromised:*
        - Cleartext data intercepted in transit;
        - Encryption key disclosed allowing data decryption;
        - Insecure encrypted connection.
    - *Contamination of device:*
        - User accesses information beyond their privilege;
        - Personal and corporate data combined.
2. **Trust relationship compromised** – compromised device used to pivot into secure environment:
        - Wi-Fi credentials used;
        - Poorly secured VPN environment.
3. **Security model weakened** - bypass of security controls:
        - User jailbreaks device
        - User bypasses application level control
        - User provisions own access

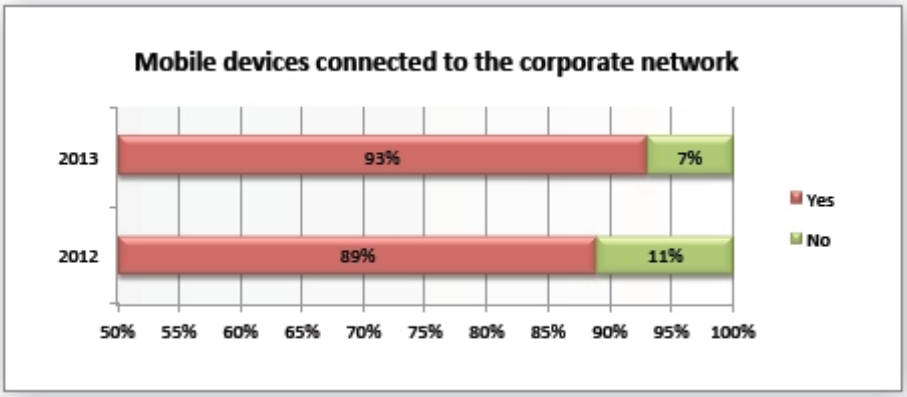
Risk of working from different networks:



-Graphic representation-[13]

Extensive use of mobile devices on corporate networks:

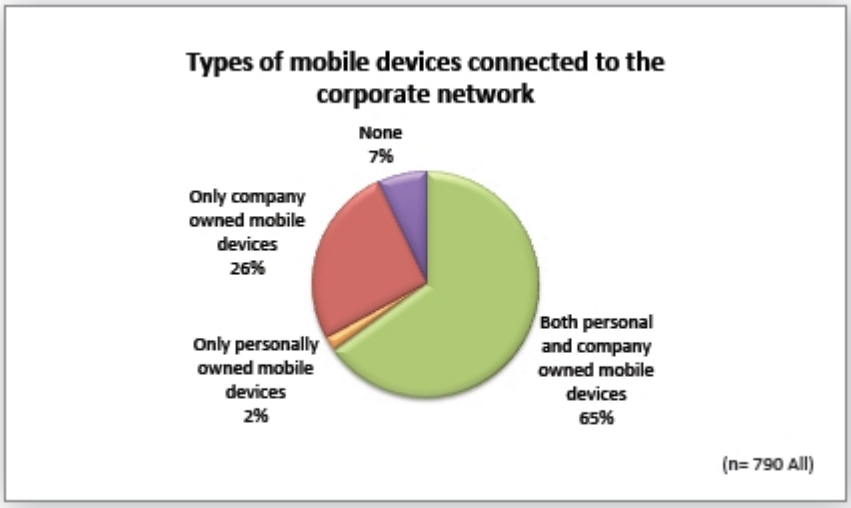
Participants in a check-point survey were asked if mobile devices, such as smartphones or tablets, connected to their corporate networks. Broad use of mobile devices was reported, with 93% saying that they had mobile devices connecting to corporate networks. This is an increase compared to 89% in 2012.



14

More corporate networks include personal devices:

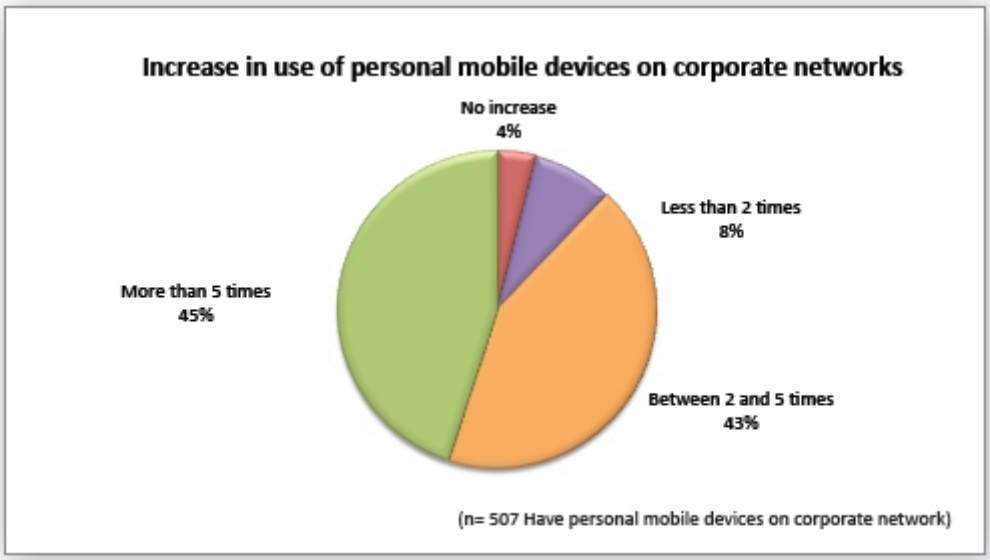
Just over two-thirds of organizations, 67%, have devices owned personally by employees, contractors, or others that connect to their corporate networks. This included 65% who allow both personal and company owned mobile devices, as well as 2% that had only personally owned mobile devices on their networks. This is an increase compared to 65% in 2012.



15

Personal mobile devices at work continue to expand

IT professionals whose companies do allow personally owned mobile devices to connect to corporate networks were asked how much growth there has been in the past two years. The vast majority, 96%, have seen an increase in the use of mobile devices connecting to corporate networks. For some companies, the increase was very dramatic with 45% saying they have more than five times as many personal mobile devices on their networks as they did two years ago.



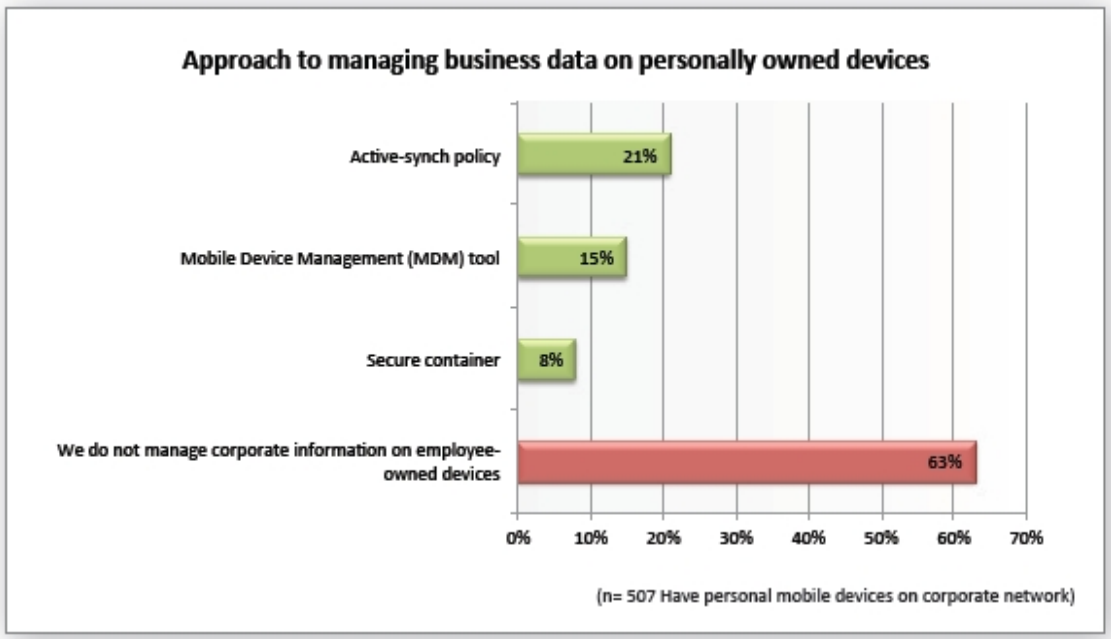
16

Securing corporate information greatest challenge in adopting BYOD

BYOD is causing challenges for corporate IT. Among companies that allow personal devices on their networks, the vast majority, 93%, reported that when employees use their own smartphones, tablets, or other devices to work with business information, it causes issues. Participants reported that the most common challenge faced by IT organizations in adopting BYOD was securing corporate information (67%), closely followed by tracking and controlling access to networks (63%).

Corporate information on personal devices not managed by IT

Almost two-thirds, 63%, of companies who have personally owned mobile devices connecting to their corporate networks do not manage the corporate information that resides there. Among those who do manage the information, active-synch policies were the most common (21%), followed by Mobile Device Management (MDM) tools (15%), and secure container (8%).



Larger companies were the most likely to manage corporate information on personally owned devices. Very few companies with less than 1000 employees, 17%, use a technical approach to information management on employee's mobile devices, significantly less than the comparable 66% of companies with more than 5000 employees.

More types of information on mobile devices today

Participants reported an increase in all types of information stored on mobile devices compared to last year. Corporate email, the most common type of corporate information reported, increased from 79% of mobile devices last year to 88% this year.

More companies have their most sensitive business information stored on mobile devices. Customer data stored on mobile devices increased from 47% in 2012 to 53% in 2013. Corporate information on mobile devices through business apps installed on mobile devices saw the greatest increase with a 17% rise from 2012 to 2013.

Possible loss of corporate information from mobile devices ranked most concerning

Working locations have also changed. Whereas, in the past, employees were likely to work from a location managed and secured by their employer, possibly with some form of internet portal-based home working, employees are now able to conduct business from almost any location. Before mobile working became possible, a sales person might have visited a potential client with brochures and forms, and then processed those forms back at an office. Now, however, they are likely to take a laptop and capture the information at the client's location, processing it and uploading it immediately by Wi-Fi or mobile internet connection. This introduces risk, as an organization can no longer rely on its physical security measures to protect data

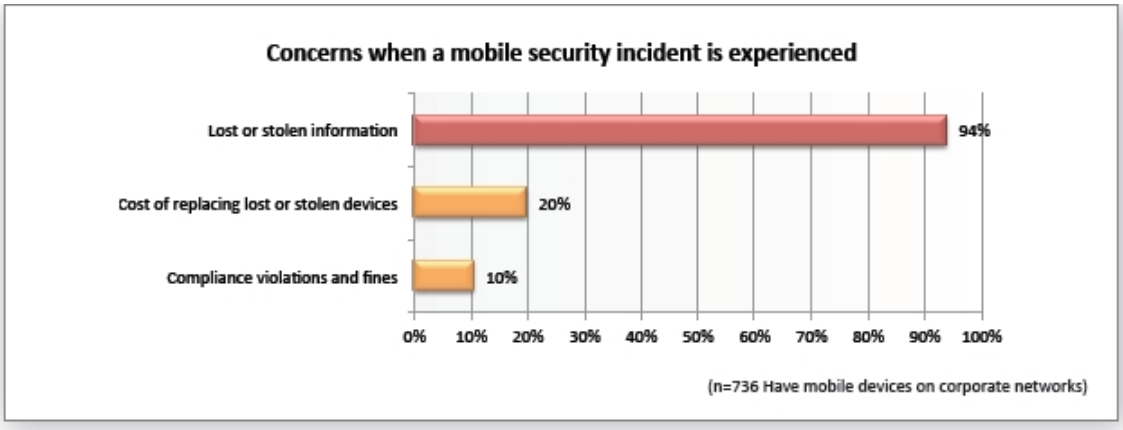
Mobile security incidents can have a wide range of impacts. Participants were presented with a list of possible impacts and asked to rank them from first to last with the first being the factor that was the most impactful and the last being the factor that was the least impactful. Lost or stolen devices was ranked number 1 as the factor that had the greatest impact on the vulnerability of mobile data, followed by malicious applications downloaded to the mobile device. The high rate of users changing or upgrading their mobile device was ranked last as a factor impacting mobile security.

Loss of corporate information greatest concern during a mobile security incident

Because of their movement need, employees are comfortable to use laptops, portable storage such as USB drives, smartphones and tablets. All these devices have risk profiles that are different from desktops, not least because of their portability. USB drives are able to store huge amounts of data, possibly even the majority of an organization's assets, in a small and readily losable form.

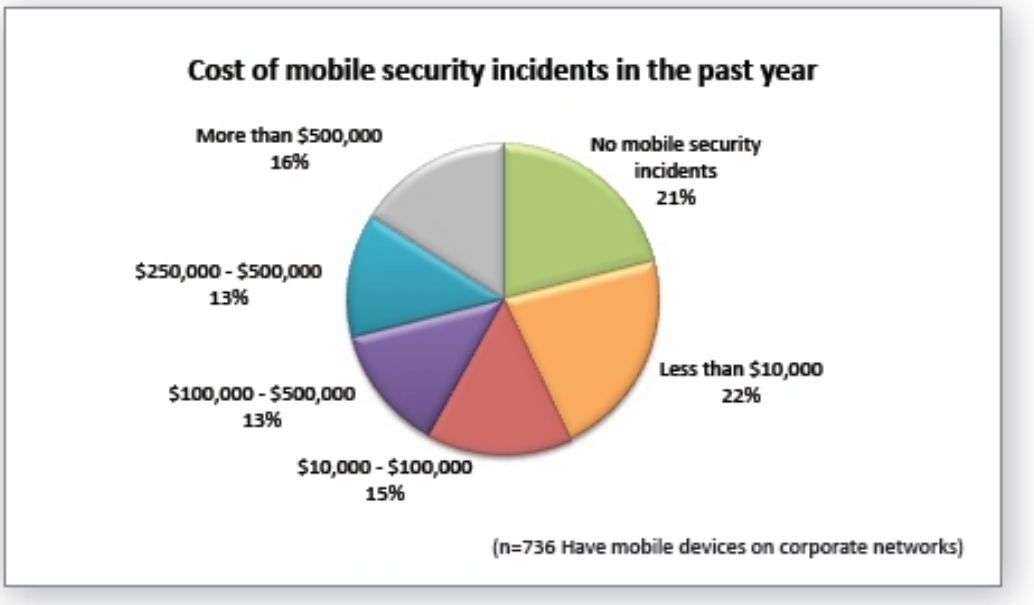
Mobile security incidents can have a wide range of impacts. Survey participants, who had mobile devices on their corporate networks, including both personal and business, were presented with a list of possible issues that could occur as a result of a mobile security incident and asked which most were concerning.

Possible loss of corporate information was by far the most concerning (94%). The cost of replacing the lost device ranked a distant second (20%).



Mobile security incidents are expensive

Once companies have mobile devices, security incidents happen and the costs are substantial. Most companies, 79%, which have mobile devices on their networks have had a mobile security incident in the past year. The majority, 57%, reported that the total costs of their mobile security incidents cost them from $10,000 to more than $500,000 in the past year. These costs included staff time, legal fees, fines, resolution processes, and so on.



Careless employees seen as a greater security risk than cybercriminals

Participants were asked which group of individuals was considered the greatest security risk — careless employees or cybercriminals who intentionally try to steal corporate information. Significantly more said careless employees pose greater security risks (66%) than cybercriminals (34%), which reinforces the importance of implementing a strong combination of technology and security awareness throughout an organization.

Another challenge arises as people become increasingly IT literate. In the past, very few employees would have attempted to break restrictions placed on them – and, had they tried, they would probably have failed to do so. Now, however, employees are generally more able to bypass poor controls and to seek advice via internet forums to help them bypass more advanced controls. Web searches for bypassing specific controls on mobile devices shows a large numbers of results. Hence technical controls cannot be trusted in isolation. Instead, it is vital that employees are educated – and then trusted.

Using mobile devices has also opened the easy way to share file via sites such as DropBox, Box, Google Drive and iCloud, which some IT specialist see as a great concern for security of corporate data.

As such, a mobile devices policy can be challenging to construct and implement. However, it is crucial to have one in place, as mobile devices will in all likelihood be used in the organization, regardless of official policies. If users are enabled and supported by the organization, then the risk is known and manageable.

In the absence of policies, that risk is still present, but unknown and unmanaged.

In this file-sharing matter organizations are divided when it comes to apply security policies with some allowing all employees to access these sites (35%) and some not allowing

any employees (25%) but most of them allowed some employees while preventing others (40%) according to checkpoint survey report released in June 2013.

Different organizations take different approaches to implementing a mobile devices policy. While one organization might choose to allow employees to use one of the top four smartphone platforms for emails, another might only want to allow the executive team to have iPads. It is entirely reasonable that an organization could start with a small project, such as tablets for executives, and then slowly widen the policies to encompass the majority of employees and devices.

III. SECURITY TENDENCIES IN MOBILE INFORMATION

III.1. Security by mobile platform

"The Secure Mobile Environment—Portable Electronic Device" (SME-PED, pronounced "smeee-peed") can be a solution, now being a military program that aims to give U.S. personnel a device analogous to civilian smartphones, yet also able to make top-secret phone calls and to interact at the secret level with the U.S. military's classified network (SIPRNET) resources. The core design of the current SME-PED smartphones involves four distinct electronics boards: a trusted crypto module, the semi-trusted "black" and "red" compute modules, and the untrusted RF module, which can be physically removed and replaced (e.g., to convert the SME-PED from GSM to CDMA, one would only need to replace the RF module, which clips onto the outside of the phone).The crypto board does more than just cryptography.

The civilian smartphones, compared with the SME-PED, must be cheap to manufacture because of the huge incentives to save money on the margin by the manufacturers.

Even thou, civilian smartphones still need appropriate machinery to separate different apps from interfering with one another, also a notion of a trusted path, so users can distinguish whether the app they see is the app they want, but also remote management and administration.

A recent study quantified these effects with SSL warnings[20], finding that poorly engineered web browser warnings would be ignored by virtually all users (around 90%) while even the best-designed warnings would only be heeded by half of the users. These studies were conducted with university students, who presumably have more experience with computers than the general population.

The obvious choice is to take it out of the hands of users. Every dangerous policy question could be answered on behalf of the users and thus provide for a safer experience. Apple's solution is a curious hybrid of enforcing a wide variety of rules in advance, prior to allowing apps into the iTunes Store, along with requiring apps to request permission for more invasive permissions at runtime.

An alternate approach is taken by Google's Android. Android phones, under the hood, are running a stripped-down Linux system, much like Apple iPhones run a stripped-down version of the Macintosh OS X system. Android leverages Linux's own protection system, giving each app its own Linux user-id[21], and marking the protection bits in the files system such that users can neither see nor edit each others' files.

Consider the issue of what permissions should be allowed by default. Should apps have the privilege to interrogate the address book? One iPhone game developer, Storm8, is being sued over allegedly copying users' address books[22]. In an Android-like system, the privilege to access the phone book need not be enabled by default, which would clearly defeat such an ex-filtration attack. On the other hand, if too many such privileges were denied, then more exceptions would be necessary to the default security policy in order to enable useful apps which have legitimate reasons to access resources like the address book. While there will probably never be a clear answer on default, one-size-fits-all security policies, we can imagine building a novel security policy from a rule that Apple requires for the purposes of saving power.

Another new release (14 Jan 2014) is the "blackphone" made by Silent Circle and Geeksphone with a strong commercial announcement: "Blackphone is the world's first smartphone to put privacy and control ahead of everything else. Ahead of carriers. Ahead of advertising. Blackphone is re-shaping the landscape of personal communications. ", a new Android-powered smartphone which- they said - will put privacy and control directly in the hands of its users.

The device is powered by a security-oriented Android™ build named PrivatOS, is a carrier- and vendor-independent smartphone giving individuals and organizations the ability to make and receive secure phone calls, exchange secure texts, transfer and store files, and video chat without compromising user privacy.

How much it will costs the privacy offered by this "blackphone" and if the price reflect its capabilities? I assume that we will find very soon.

III.2. The “NEMESIS” solution

The solution presented in this section is a collaborative research project NEMESYS (Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem) that was supported by the EU FP7, under grant agreement no. 317888 within the FP7-ICT-2011.1.4 Trustworthy ICT domain.

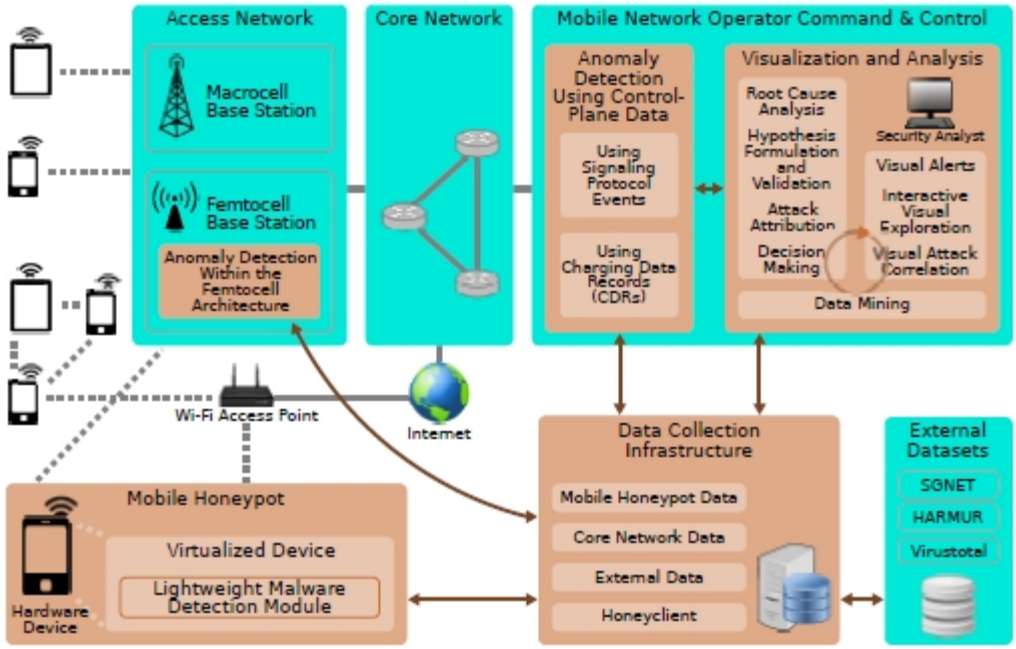
NEMESYS project wants to provide a new sight into the nature of next generation network security in the smart mobile ecosystem. The main innovation of NEMESYS is the research and development of novel security technologies for the identification and prediction of abnormal behavior observed on smart mobile devices, as well as for gathering and analyzing information about the nature of cyber-attacks targeting mobile devices, so that appropriate countermeasures can be taken to combat them.

The goal of the NEMESYS project is to develop novel security technologies for seamless service provisioning in the smart mobile ecosystem, and to improve mobile network security through a better understanding of the threat landscape by collecting and analyzing information about the nature of cyber-attacks targeting smart mobile devices and the core network so that appropriate counter-measures can be taken.

They are developing a data collection infrastructure that incorporates virtualized mobile honeypots and honeyclients in order to gather, detect and provide early warning of mobile attacks and understand the modus operandi of cyber-criminals that target mobile devices. By correlating the extracted information with known attack patterns from wireline networks, we plan to reveal and identify the possible shift in the way that cyber-criminals launch attacks against smart mobile devices.

Here are the components of the NEMESYS architecture in the following sections in more detail:

A. *Virtualized Mobile Client Honeypot*
B. *Data Collection Infrastructure*
C. *Anomaly Detection Using Control Plane and Billing Data*
D. *Root Cause Analysis, Correlation and Visualization*
E. *Integration and Validation*



- The NEMESYS architecture -[23]

As part of NEMESYS, they are developing a high interaction ***virtualized client honeypot*** for the Android mobile platform in order to attract and collect mobile attack traces.

They have chosen Android considering its popularity among mobile users and the extremely high ratio of malware targeting Android. Their virtualization technology logically partitions the physical device into two virtual machines (VM's): the *honeypot VM* and the *infrastructure VM*. The honeypot VM will host the largely unmodified mobile device operating system, and it will not have direct access to the device's communication hardware. The infrastructure VM will mediate all access to the communication hardware, and employ sensors to wiretap any communication and detect suspicious behavior. It will also provide the event monitoring, logging and file system snapshot facilities, as well as transmit threat information to the NEMESYS data collection infrastructure. It will host a lightweight malware detection module in order to identify malicious applications running on the honeypot VM. For this purpose, both signature-based and behavior-based approaches will be considered. In order to improve the efficiency of malware detection, they will identify and prioritize the most important attributes in the system state space to monitor.

Their virtualization technology will ensure that an attack is confined within the compromised device and that it will not put other devices in the network at risk. Furthermore, through this approach, they think that will be able to stop malware from abusing premium services and from subscribing the user to services without her knowledge. Thus, the user will be spared from any financial distress that may arise as a result of using the mobile honeypot. The virtualization solution also enable staking full snapshots of the honeypot VM files system

for further forensic analysis of an attack, as well as improving honeypot maintenance since a compromised honeypot could be restored more quickly.

Their initial research has shown that the infection vector of most mobile malware is social engineering, where users are "tricked" into installing the malware themselves. This observation has led them to the conclusion that the user should note ignored in the construction of an effective mobile honeypot.

To this end, they introduce the *nomadic honeypot* concept, which utilizes real smartphone hardware with the virtualization solution that will be developed within NEMESYS[24]. They plan to deploy nomadic honeypots by handing them out to a chosen group of volunteers, who will use the honeypot as their primary mobile device. It will be up to these human users to get the honeypot infected by visiting malicious sites, installing dubious applications, and so forth. Traces from malware and other types of mobile attacks collected and identified through the nomadic honeypots will be provided to the data collection infrastructure, which is described next.

The data collection infrastructure will gather and store mobile attack traces that will be provided by the virtualized mobile client honeypot and the honeyclient, and combine them with data from the mobile core network and external sources for enrichment, correlation analysis, and visualization. As an initial step in the design of this infrastructure, they identify available external data sources relating to wireline network attacks which will enable correlation of data from multiple heterogeneous sources. Examples of such data sources are the SGNET, HARMUR, and VirusTotal databases. A source aggregator is being designed and developed to harvest and consolidate data from these sources and the NEMESYS mobile honeypot in a scalable database. Scalable design of the database is important in order to be able to efficiently store and handle large heterogeneous data sets. Once data from multiple sources have been consolidated, they will be enriched by analyzing the data itself or accessing external sources. For example, TCP/IP stack fingerprinting in order to identify the remote machine's operating system, and clustering of the traces are passive methods of data enrichment. On the other hand, DNS reverse name lookup, route tracing, autonomous system identification, and geo-localization are methods to improve characterization of remote servers but these functions may require access to external sources, possibly in real time. As a final step, the data collection infrastructure will help in the definition of the appropriate inputs representing normal and malicious network activity, which will then be used as the fundamental representation of information in the visualization and analysis module.

The anomaly detection module that operates at the mobile network operator's site is used for the identification and prediction of abnormal behavior observed on smart mobile

devices and the mobile network. In addition to user-oriented attacks, mobile networks are vulnerable to a novel DoS attack called the signaling attack[25]. Signaling attacks seek to overload the control plane of the mobile network using low rate, low-volume attack traffic, based on the structure and characteristics of mobile networks. Unlike conventional DoS attacks that focus on the data plane, the signaling attack creates havoc in the control plane of a mobile network by repeatedly triggering radio channel allocations and revocations. In order to identify such DoS attacks against the mobile network and attacks against the mobile users in real time, we will use signaling data from control-plane protocols and sanitized (anonymized) CDR's from mobile users, respectively. For this purpose, we will use normal user behavior statistics, as well as synthetic "typical" user playbacks, to create traces of signaling events and billing data so as to characterize and extract their principal statistics such as frequencies, correlations, times between events, and possible temporal tendencies over short(milliseconds to seconds) and long (hours to days) intervals. They will then employ Bayesian techniques such as maximum likelihood detection, neuronal techniques based on learning, and a combination of these two in order to design and develop robust and accurate change detection algorithms to detect the presence of an attack, and classification algorithms to identify the type of attack when it is detected with high confidence. Novel femtocell architectures provide a specific opportunity for user-end observation of network usage, while they also have specifics for attacks within the femtocells[26]. To address attacks specific to femtocells, they look to conduct a survey and evaluation of how users may be monitored and attacks detected within a femtocell, and how these are linked to overall mobile network events.

The role of the ***visualization and analysis module*** is to process the data obtained from the data collection infrastructure and the anomaly detection module in order to identify and reveal correlations between network events, and to provide a visual analytics framework for the security analyst to perform hypothesis formulation and testing. The data provided to this module represents a large and heterogeneous data set that needs to be presented in a meaningful way to the operator without overwhelming her or restricting available views and actions on the data. In addition to mere representation of data, the visualization and analysis module aims to provide visual analytics tools to the operator. This task is compounded by different uses of visualization by the operator:

(i) real-time monitoring of the status of users and the mobile network,

(ii) exploratory data analysis. For real-time monitoring, the security status of a large set of mobile users and more importantly the mobile network need to be presented to the operator.

This includes providing early alerts for abnormal behaviour, DoS attacks, malware spreading among the users of the mobile network, etc. The analytics module must also provide visual analytics tools so the analyst can perform attack attribution and correlation analysis with the help of algorithms running in the background.

In order to effectively visualize and explore large sets of heterogeneous, dynamic, complex data, it is necessary to create multiple coordinated views of the data that allow a multifaceted perception and the discovery of any hidden attributes.

The analysis methods also need to be scalable for early network alerts and fast access to the underlying data. We will therefore focus on enabling a real-time analysis framework by means of incremental analysis and visualization methods[27], such as multi-level hierarchical screen visualizations that update smoothly rather than showing abrupt changes.

In order to ***evaluate and validate*** the technologies that are being developed and to demonstrate their impact to interested parties, NEMESYS aims to construct a virtual testing environment based on guidelines provided by industrial partners that is as close to a real mobile network as possible within feasibility limitations. The different modules being developed by various partners will be integrated in the virtual testing environment and validation tests will be conducted based on realistic use cases.

They aim to use the OPNET simulator as part of the virtual testing environment in order to conduct simulations of different types of mobile networks, e.g. UMTS and LTE, and to drive the large-scale networking experiments[28].

III. 3. How to protect your own device

With the constant changes in the mobile threat landscape, smartphone owners should secure their devices. Here are some very simple steps to protect devices against mobile threats:

The built-in security features are your best asset

Use phones that have security features and take advantage of them. Built-in security features (password, pattern, or PIN lock options) are designed to prevent outsiders from accessing your data in case your phone gets misplaced or stolen.

Device-lock passcode

The simplest precaution available to you and most effective for mobile security is setting up a lock screen password. Once up and running, no matter who has your device is

prevented from accessing your personal, social or other account data. You should know that you aren't limited to standard four-digit passcodes.

Keep a record of your IMEI

The International Mobile Equipment Identity (IMEU) is a 15-digit number that identifies your phone. This unique number provides police and law-enforcement agencies with a way to identify your smartphone among any others that may be recovered from any loss or theft. You can usually find it beneath the battery or alongside a SIM card slot.

Research apps before downloading

Cybercriminals often disguise malware by spoofing popular apps. Familiarize yourself with details of popular apps to ensure that you download the legitimate version. It is advisable to download from trusted stores.

Read permissions before installing apps

Malicious apps usually seek access to various kinds of data stored in a mobile device. Read permissions to check what type of actions an app will perform once installed. Be wary of apps that require more permissions than necessary.

Software updates.

Software updates are usually released to address issues like vulnerabilities or improve software performance.

Backup your files

A regular backup of contacts, media and documents is good practice on any computer, but it's even more important on smartphones and tablets, which are much more liable to get stolen or lost. Investigate your options for implementing a regular backup plan.

Invest in a security app.

Security apps can inform you if an app has malicious or suspicious behaviors. Some apps even protect data with features like remote wipe or privacy scanner. Tried-and-tested anti-malware software for smartphones and tablets does more than simply protect your device from digital threats. Bitdefender Mobile Security or for example, includes a range of tools to help recover a missing device.

Set BYOD policies at work.

Organizations should decide which employees will only be allowed to bring devices and what types of devices they will support. Set up procedures to take if a device is stolen, lost, or damaged.

CONCLUSIONS

World Wide Web was designed to be easy to use and not to be secure**.** Now, mobile devices are like the old computers on internet, very easy to use, in a light and easy to carry form, developing very fast according with costumers needs but lacking security where it matters.

The evolving and growing nature of the mobile threat in the smart mobile ecosystem is evident from the increasing marketshare of smartphones and tablets, the large amount of data due to smart devices, and the number of detected mobile malware. We must therefore address the mobile threat and understand the new and potential vulnerabilities, threats, and operating methods of cyber-criminals.

Due to the fulminate evolution of malware we have to keep up with cybercriminals and look forward to find new security solution for our indispensable bellowed mobile devices.

From my point of view, now we have some options to look upon. You can invest a large amount of money to buy a secure device like SME-PED or you can put the money on the new released "blackphone", which hopefully will be cheaper then the first, either sign up with a general GSM operator that has in place a high security network architecture, like the NEMESYS.

As an average Joe, that has no clue about the big picture you can skip the "spend tons of money" option and just use the low-security "features" described above, like block your phone, keep the record of your IMEI number or invest in a low cost security app and hope nobody will go rock'n'rolla on your mobile device and private data.

ENDNOTES & REFERENCES

[1]Canalys, 28 December 2013, http://www.canalys.com/newsroom/mobile-device-market-reach-26-billion-units-2016, 29 January 2013

[2] G, Sternberg, Why Aren't Users More Secure. 2010.

[3] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proc. 1st ACM W'shop on Security and Privacy in Smartphones and Mobile Devices (SPSM'11)*, 2011, pp.3–14

[4] S. Liebergeld and M. Lange, "Android security, pitfalls and lessons learned," in Proc. 28th Inter. Symp. On Computer and Information Sciences (ISCIS'13), Oct. 2013, to appear.

[5] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices," in *Proc. 2011 IEEE Symp. on Security and Privacy*, May 2011, pp. 96–11

[6] Checkpoint , 2013, http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report2013.pdf , 29 January 2014

[7] Opcit Checkpoint

[8] Opcit Checkpoint

[9]Mobile Threat and Security Roundup - Repeating history – 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-repeating-history.pdf, 29 January 2014

[10] Opcit Checkpoint

[11] Krebson Security, 2013, http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/, 29 January 2014

[12] Trend Micro, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence, 29 January 2014

[13] TrendLab, 2014, www.trendlab.com, 29 January 2014

[14] Opcit Checkpoint

[15] Opcit Checkpoint

[16] Opcit Checkpoint

[17] Opcit Checkpoint

[18] Opcit Checkpoint

[19] Opcit Checkpoint

[20] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: An empirical study of SSL warning effectiveness. In 18th USENIX Security Symposium, Montreal, Canada, Aug. 2009.

[21] Android Developers. Security and Permissions, Octomber 2009 http://developer.android.com/guide/topics/security/security.html, 29 january 2014

[22] R. Beschizza. iPhone game dev accused of stealing players' phone numbers. http://www.boingboing.net/2009/11/05/iphone-game-dev-accu.html., 29 january 2014

[23]The NEMESYS approach, 2013, http://arxiv.org/pdf/1307.0687v1.pdf , 29 January 2014

[24] S. Liebergeld, M. Lange, and C. Mulliner, "Nomadic honeypots: A novel concept for smartphone honeypots," in *Proc. W'shop on Mobile Security Technologies (MoST'13), together with 34th IEEE Symp. On Security and Privacy*, May 2013, to appear.

[25] P. P. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G/WiMax wireless networks," *Computer Networks*, vol. 53, no. 15,pp. 2601–2616, Oct. 2009.

[26] R. Borgaonkar, K. Redon, and J.-P. Seifert, "Security analysis of a femtocell device," in *Proc. 4th Inter. Conf. on Security of Information and Networks (SIN'11)*, Nov. 2011, pp. 95–102.

[27] S. Papadopoulos and D. Tzovaras, "Towards visualizing mobile network data," in *Proc. 28th Inter. Symp. on Computer and Information Sciences(ISCIS'13)*, Oct. 2013, to appear.

[28] Opcit The NEMESYS approach

THE WAYS TO ENSURE SECURITY OF MONGOLIAN INFORMATION SYSTEMS

Author:
LT NANCHIN NANDINTUGS

INTRODUCTION

Information security /IS/ is a natural issue originated from the technological advance that is steadily spoken in a wide range and a high level. E-news and information must be accurately transmitted from one person to another without losing their initial concepts. But it is already confirmed that the lost of initial concept of the information by the affects of external factors can influence the receiver's state of mind negatively, in other words, it can be used as "a weapon". It indicates that how important the e-information is and how important its accuracy is. Developed countries such as England, America and German which understood the importance of the IS have been paying attention to the accurate transmitting condition of e-information and expending their efforts and money. Recently developing countries are paying attention to this issue too. Nevertheless, even the developed countries have recognized that it is impossible to completely solve the danger of information loss and have been seeking ways to improve the situation more and to solve this issue perfectly in every respect. Because of this situation, even the conglomerates cannot keep their information but losing and incurring economic losses. Since the situation is like that in foreign countries, there is no way to not talk about the situation of Mongolia.

However development of information technological sector of Mongolia has noticeably grown as for its acceleration, Mongolian users have been working on the equipments that are made in foreign countries, make networks using the equipments and protect the information and it is still same now. It is not secure action to use the foreign equipments without doing appropriate investigation and it is too risky for the e-information security.

Countries all around the world are admitting that the information technology become one of the basic engines of the economy. Mongolia strongly adapted information technology to all sectors of the society to reach economic growth and put a goal to make it into an economic engine too. Nowadays information, information technology, information system and networks are considered as important and valuable assets of the organization and to steal,

copy, damage, break, change and delete the information would not only severely usurp the interest of the organization and the rights, freedom and interest of its customers and users but also national security. Therefore, IS was considered as the important issue not only for an individual, an organization and a country but also the world community.

I. WHAT IS THE INFORMATION SECURITY ?

1.1 Information Security

Information can be in various types. They can be printed on paper, written, archived as e-data, transmitted, recorded on various kinds of films or spoken between people. Information must be protected not regarding its origin and how it was stored. Information security can be provided with security policy, progress, rules, organizational structure and exercising control and administrative batch that includes software and hardware policies.

Information security can be explained in different ways.

For example

- Information assurance of society, institutes and organizations
- Information assurance that is protected from natural and artificial, intended and unintended force
- Measures that were taken to prevent to use information illegally, change, delete, damage and close the access possibility
- Precaution that can give chance to protect information and equipments from danger and threat and using its disadvantages wrong.

Based on the above mentioned facts, I think *"Information Security"* is the process of protecting information, data, related equipments and its substructure from any danger and threat to continuously provide work quality, minimize risks and to increase benefit of the investment and business opportunities.

The main purpose of the batch activities of information security is to protect benefits and interest of the subjects who are in information communication.

- Availability
- Integrity
- Confidentiality

Therefore, the first step of establishing information security system of the organization is to sort out the issues and to provide them. 2 important indications of information security are:

- Value of accumulated information resource
- Dependent of information technology

The system errors of some companies have only caused the problems for that companies, the errors of not few companies have been badly influenced to social and economic developments and losing the stability, affected directly to human health, and their ways of lives. Moreover some has been caused the problem for sovereignty of country.

Since current information system is complicated and complex, even it causes any problem without human participation. At any time, the problem reveals unto the software, becoming weak, fragile due to irrelevance of software and apparatus, and then it is necessary to note the combination of components of system. The principal and ways of making information system are getting changed. Year by year, errors and confusion are increasing, as a result of this, the more damages are increasing, the more recent young companies have been more taking notice and spending much for security of systems. Consequently, the companies can stand firmly against the increased damages and dangers.

1.2 Why is the security of information important to organizations?

We are turned unto information and technological society over the world, digital economy, electron democracy, web based government, business, banks, health, education, and agriculture are developing while habitual crime and complication are changing into forms - web based, because of those factors, new types of crime are getting revealed, which are highly harmful to system, wires, combination of complex data, their security and secrecy – the risks of security of information are getting bigger.

Therefore, the security of information is not only harmful to software; it is more complicated and complex issue for country, and its government. Few years before, security of system and computers are regarded to be vitally important, but today it is totally changed, we need to, and we face to make complex control of information security, to implement policy and program and rules for them by approving and doing action against all types of confusion, complication, crime as well in related to security of information system.

In accordance with all above, in Mongolia, it is important to make security and safeness of information system, and we are indicating four main reasons for this issue. By

approving and implementing programs, policies, rules and strategies of information system security, it is necessary for putting into effect the associate programs and actions.

Through the internet area, there are many attacks which are increased, damaged hugely as well as the inside crime of information security are attacked more and more. There are many attacks /about 1000/ including: to lose the information system of the companies, to steal or delete and change server, saved confidential materials, to break office programs while taking information by cheating the workers and employees of any companies.

Unfortunately Mongolian companies and organizations are recently not able to stand against such issues and attacks and it is clearly shown that the underdevelopment of information technologies and systems of companies of Mongolia. For current issues, for companies, it is hardly difficult to compete, make profit, save budgets, and to expand the companies without ensuring the information securities system and computer technologies, at last the companies may face to danger of failure.

<u>For about ensuring security of information date</u> :

- For the priority is to make shaped the people's understanding about security of data
- To obtain and increase the leadership and encouragement
- To provide human resource and developing their education
- To analyse and ensure security of information and confidential data of companies
- To set rules of activities of companies
- To develop program and technological activities and so on, for every level of activities should be settled and organized by policies.

Moreover, it is important to expand the international cooperation. Generally, it can be attacked to any places from every part of the world. But even the crime is revealed, whether it is solved or not – only it is depended on connection of world relationship. So when having good relationship with other countries, we can ensure security of confidential information.

<u>For about ensuring security of companies information</u>:

By search of National Information security agent of the USA, 98% of companies of the USA has been attacked in consistence with computer and technologies. For those attacks, mostly following issues are:

- Attacked by virus programs
- Stealing data

- to change, destroy, add or erase some of the data from inside or out resources.
- To use illegally the programs and equipments of computers
- Attack illegally to system
- to break website
- Denial of service (DoS)

In Mongolia, in accordance with the search made by 'National centre against the Cyber attack', in last 2 years or 2012-2014, hackers attacks are getting increased. For about the types of computer and web which have been more often attacked – 66 computers from affiliate offices of government, 40 from popular organizations, 64 from educational branch, 6 from banks, 64 from other companies, 10 from newspaper and information sectors, 80 from other websites –have been attacked. From those, 88 websites are still not updated, or frozen as hacked webs –including websites of branches of government, insurance office, energy and thermal station, police office and bigger technological and travelling/tourism companies. It shows that we are attacked by hackers in real. For specialists said that we/Mongolians attacked by cyber attack 14 years ago at first time.

How to manage and control the security of information and data of companies?

- to appoint the person who is responsible for controlling system of data and information daily for the companies to develop security system of data and information for companies.
- for small companies and organizations, the associate person who has a right to enter into administration system, all data, software and hardware, so the person should be knowledgeable for computer system.
- Since each employee has to be responsible for security of information, it is duty to implement any actions in just way.

• to implement the program for developing knowledge of information system for users.
• to organize the security course or training for technical workers.
• to make the regulations for ensuring the security of information and its control.
• If strategies of business have been changed, the changes of information system of your company have to be analysed by architecture of security since it might be influenced badly the system.

The examples indicated above based on real research are proved that it can be reached at hazardous consequences if we skip the security of information. It might be affected to

national security and sovereignty of country- it is directly faced us as risk for the country, researchers emphasized.

II. THE STATUS OF INFORMATION SECURITY IN MONGOLIA

New technologies of Information and communication and connection have already launched in Mongolia. And many types of online service, agreement, contract, payment, and communications are developing. But it is restricted to develop more this branch and social communication since the acts and laws on organizing information and communication are not settled. We don't know the international convention against cyber attack and it is wrong to skip the advice and organized regulations originated from international organizations in related to information security.

Due to those issues, understanding of people and the users are not getting better, and managing this kind of issues is led to great damages. The security of Mongolian technology is also influenced to information security. There are no manufacturers produced the software, technical equipment in Mongolia, and lack of property to buy good qualified programs and tools for security of computers, it is also so difficult to be studied for our students majoring in information and technologies, its security as well. Those factors are affected us to easily be attacked.

Within Mongolian area, we face following dangers of information and computer attack and divided by as follows:

- Danger due to human action-actions of crime group, criminals, and their illegal actions
- Technical dangers-non qualified equipment, software, tools and machines of security and warning, and dangerous delivering and so forth
- Natural danger-earthquake, hurricane, flood and other disasters of nature

In Mongolia, only 3 to 5 percent of governmental, bank, business and financial and nongovernmental organizations have solved the security of information system, having own appropriate regulations. Within the government of Mongolia, and within the entities, there are lack of policies related to information security, it is not implement the actions of information security yet, being not able to ensure information security, and its basic knowledge, it is not used other security system except for the filters of warehouses yet, and systems of recognition and analyzing is so weak.

The following examples prove the overview that indicates all above:

- In 1998, a person who had worked freight Forwarder Company took confidential information from the company when resigning, and selling to competitors.
- In 2006-2007, on the websites of some governmental companies are shown that Mongolian state is hacked, which repeated many times.
- In 2008, the program of software which made in a company was stolen by a person who had worked at that company, then the person advertised as he did the program on his own, selling to other company.

III. THE WAYS TO ENSURE SECURITY OF MONGOLIAN INFORMATION SECURITY

Today in order to succeed in sectors of technologies and information security, 4 level attitudes are being used:

1. Level of legislation
2. Governmental level
3. Procedural level
4. Program and technical level

For Mongolia, we can ensure the national security of information system by working as indicated levels and by developing international relationship progressively.

1. *Level of legislation is* very important to ensure security of information system. Legilation is reflected the identification of information security, and concentrating on main purpose of any research related to security of information, to provide those attitudes to each company, organize the training by coherencing with education.
2. *Main reason of Governmental level is* to create actions and programs for branch of information security, ensuring its implementation, to provide resources and controlling their process. The basis of program is the policy of information security, so each organization of Mongolia has to have own policy of information security, to implement the policy in reality, and it is vital to make them legally.
3. *The next level*, regulation procedure directs to people, not tools and equipments.

- Regulations related to manage human resource.
- Regulations related to real protection
- Regulations related to improve working skills
- Regulations related to ensure web system

- Regulations related to actions against the confusion and complexion

When analysing the regulations it is good to protect at any time, to divide the regulations, and to restrict protecting rights. When creating the regulations indicated above, it is noticed more on encouraging users, to serve, install or uninstall, change programs, organize, making prove for software service, and it is important to control the information flow in accordance with security of information system. Especially it is needed to make understanding to users that do not catch well. The purpose of regulation is to lead to stop confusion and complexion, to reduce the damages, to recover the criminals, preventing to not repeat such illegal actions. And when happening accident, attack as well, regulations related to that has to be implemented.

4. *Program technical procedural level is* to implement the actions in order to ensure proper work of equipment, tools, and machine, data and to control its standard of working. The speedy development of current information technologies is good side, but on the other hand it gives chance to criminals. Therefore, it is necessary to note for the branch by investing and improving the knowledge and it is final special limit of protecting the security of information.

<u>In Mongolia, technical and programing procedural level is to be led:</u>

- To prevent the complication of information security
- and it is effective if we take action for solving as following issues:
- purpose for complication and confusion
- decreasing criminals
- refreshing or updating the system

<u>The four levelled procedures of implementing policies and programs of information security:</u>

- to identify exact benefits for protection.
- to decide how to protect the weaker resources of information
- to implement appropriate protection based on necessity of work.
- To check the chosen protection at any time since it has to be effective and efficient.

<u>Program and technical actions would be succeeded if using following regulations</u>:

- To protect at any time, to not skip protective service
- to abide the standards of popularly agreed regulations, using the checked ways

- fastening the weaker or loosed parts
- to divide the implementing duties
- to use many types of protecting techniques
- information system has to be simple and possibly controlled by associate person

The company can ensure the security of information system by implementing program and technical procedures:

- Identification system
- Access control
- Audit control
- Encryption
- Filters of firewall
- Analysis of protective status
- To ensure safe and continual working
- Controls programs
- Virtual private network
- Intrusion detection system
- Safety zone

To ensure the issues of the high controlling information security of any company is main key of success. The issue of information safety is vital for the company and if the leader of the company understands it well, the company will be succeeded. It is wrong the company would understand well the security system is how important to the company after attacking to the server, and damaging by its huge properties.

It is important to invest based on analysis of risk and its results. Even though it is attracting to all if attacks from outside, it is not revealed if attack came from inside of the company. It is necessary to erase the hiding such criminals. In life, such attack causes hugely and damages marvellously –it is proved by the research made by security institute of federal police of the USA.

CONCLUSIONS

For Mongolia, to regard the security of information system as vital issue, to combine the legal environment is one of the most urgently important problem. Combining the legal environment in relevant to security of information system is to be identified with the international regulations and procedures.

Those regulations and principals are based on the main content of restricting or limiting rights of people and citizens when hiding the confidential information. The freedom of information is to purpose of supporting, analysing the open political policies, increasing participation of citizens.

Security status of confidential information is based on the principal of complex actions of individual, citizen, organization, partners and government, and the principal has to be kept all the time is important. Security status of confidential information is not only for country issue, but also effective and active procedures and actions of all countries of the world is base of it. It does mean that current legal environment and its implementation are one of important factor of it.

In this time, information technology is increasing at quick speed, so it is more important to hide, keep personal information or it can be revealed because of benefits of people- it is main issue for this.

In finally, as we can conclude that if security status of confidential information is only based on hiding the data, it can be affected to persons' rights, we have to organize the information perfectly well by preventing complication of individual rights, and the security of hidden information, its safeness, limits of hiding info and its duration and so forth –are have to be managed and we have to respect the freedom of popular information for people including to take information, to inform, and to demonstrate the information, its rights as well.

REFERENCES

1. Х. Энхтуул, “21 аймгийг өндөр хурдны интернэттэй болгоно,” *iPost.mn*, 21-May-2012. [Online]. Available: http://ipost.mn/news/read/664. [Accessed: 10-Mar-2013].
2. M. Rogers and D. Ruppersberger, “Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,” Washington DC, Oct. 2012.
3. Tatar, “‘Мэдээллийн Аюулгүй Байдал 2012’ Өдөрлөг,” *Oin Manaach*, 25-Dec-2012. [Online]. Available: http://manaach.blogspot.com/2012/12/2012.html. [Accessed: 10-Mar-2013].
4. С. Дөлмандах, “Тодруулга: SSL гэж юу вэ?,” *Технологи ба эрх чөлөө* , 31-Jul-2008. [Online]. Available: http://www.dulmandakh.com/2008/07/ssl.html. [Accessed: 15-Oct-2012].
5. “Бидний тухай | 3S LLC,” *3S LLC*. [Online]. Available: http://shop.sssmn.com/taxonomy/term/11. [Accessed: 10-Mar-2013].
6. ISO/IEC 27001 – Information security management. [Online]. Available: http:// ISO. org /ISO/ Home/ standards/management-standards/iso27001.htm.
7. “Huawei - A leading global ICT solutions provider,” *Huawei*. [Online]. Available: http://www.huawei.com/en/. [Accessed: 10-Mar-2013].

IT CRISIS - MANAGEMENT AND RECOVERY PROCESS WALKING IN THE GLORY OF SHADOWS

Author:
CMD eng Cristian ALEXANDROAIA

ABSTRACT

Making use of advanced planning capabilities can be definitely a flexible support for crisis management. Anyway, the complexity of the underlying domain often causes intractable efforts in modeling the domain as well as a huge search space to be explored by the system. A way to overcome these problems is to impose a structure not only according to tasks but also according to relationships between and properties of the objects involved.

I. OVERVIEW

I.1. Definition

A **crisis** (plural: "crises"; adjectival form: "critical" from the Greek κρίσις, krisis) is any event that is, or expected to lead to, an unstable and dangerous situation affecting an individual, group, community or whole society. Crises are deemed to be negative changes in the security, economic, political, societal or environmental affairs, especially when they occur abruptly, with little or no warning. More loosely, it is a term meaning 'a testing time 'or an 'emergency event'.

Crisis has several defining characteristics. Seeger, Sellnow and Ulmer say that crises have four defining characteristics that are "specific, unexpected, and non-routine events or series of events that create high levels of uncertainty and threat or perceived threat to an organization's high priority goals." Thus the first three characteristics are that the event is

1. unexpected (i.e., a surprise)
2. creates uncertainty
3. is seen as a threat to important goals

Crisis management is a situation based management system that includes clear roles and responsibilities and process related organizational requirements company-wide. The

response shall include action in the following areas: crisis prevention, crisis assessment, crisis handling and crisis termination.

The aim of crisis management is to be well prepared for crisis, ensure a rapid and adequate response to the crisis, maintaining clear lines of reporting and communication in the event of crisis and agreeing rules for crisis termination.

Crisis management consists of different aspects including:

- Methods used to respond to both the reality and perception of crises.
- Establishing metrics to define what scenarios constitute a crisis and should consequently trigger the necessary response mechanisms.
- Communication that occurs within the response phase of emergency-management scenarios.

Crisis-management methods of a business or an organization are called a crisis-management plan.

Crisis management is occasionally referred to as incident management, although several industry specialists such as Peter Power argue that the term "crisis management" is more accurate.

A crisis mindset requires the ability to think of the worst-case scenario while simultaneously suggesting numerous solutions. Trial and error is an accepted discipline, as the first line of defense might not work. It is necessary to maintain a list of contingency plans and to be always on alert.

Organizations and individuals should always be prepared with a rapid response plan to emergencies which would require analysis, drills and exercises.

The credibility and reputation of organizations is heavily influenced by the perception of their responses during crisis situations. The organization and communication involved in responding to a crisis in a timely fashion makes for a challenge in businesses. There must be open and consistent communication throughout the hierarchy to contribute to a successful crisis-communication process.

The related terms emergency management and business-continuity management focus respectively on the prompt but short lived "first aid" type of response (e.g. putting the fire out) and the longer-term recovery and restoration phases (e.g. moving operations to another site). Crisis is also a facet of risk management, although it is probably untrue to say that crisis

management represents a failure of risk management, since it will never be possible to totally mitigate the chances of catastrophes' occurring.[i]

Moving beyond the negative aspects of a crisis is a laborious process whose onset is traced in the values of the company, its relationships with its primary and secondary stakeholders but also in its leadership (authoritarian, democratic, laissez-fair, or contingent). Lastly, there are seven major potential positive results that a crisis can lead to (Meyers & Holusha, 1986):

1. Heroes are born.
2. Change is accelerated.
3. Latent problems are faced.
4. People are changed (a crisis shakes the system of values/beliefs)
5. New strategies evolve (organizational memory).
6. Early warning systems develop.
7. New competitive advantages appear.[ii]

I.2. Types of crisis

During the crisis management process, it is important to identify types of crises in that different crises necessitate the use of different crisis management strategies. Potential crises are enormous, but crises can be clustered.

Lerbinger categorized eight types of crises:

1. Natural disaster
2. Technological crises
3. Confrontation
4. Malevolence
5. Organizational Misdeeds
6. Workplace Violence
7. Rumours
8. Terrorist attacks/man-made disasters

Technological crisis

Technological crises are caused by human application of science and technology. Technological accidents inevitably occur when technology becomes complex and coupled and something goes wrong in the system as a whole (technological breakdowns).

Some technological crises occur when human error causes disruptions (human breakdowns). People tend to assign blame for a technological disaster because technology is subject to human manipulation whereas they do not hold anyone responsible for natural disaster. When an accident creates significant environmental damage, the crisis is categorized as mega damage. Samples include software failures, industrial accidents etc.

Examples: Chernobyl disaster, Exxon Valdez oil spill, Fukushima Radiation Disaster

II. Cyberspace

II.1. What is Cyberspace?

"Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services."

UK Cyber Security Strategy, 2011

Information and the ICT (Information and Communication Technologies) that store and process it are critical to humanity success. Your intellectual property, confidential or sensitive information provide competitive advantage, whether in the form of a product design, a manufacturing process or a negotiating strategy.

At the same time the need to access and share information more widely, using a broad range of connecting technologies is increasing the risk to the corporate information base. Compromise of information assets can damage companies Compromise of information through, for example, staff error or the deliberate actions of an outsider could have a permanent or at least long-term impact on a business. A single successful attack could destroy a company's financial standing or reputation.

Information compromise can lead to material financial loss through loss of productivity, of intellectual property, reputational damage, recovery costs, investigation time, regulatory and legal costs.

This could lead to reduced competitive advantage, lower market share, impact on profits, adverse media coverage, bankruptcy, or even, where safety-critical systems may be

concerned, and loss of life. In addition to an accurate picture of those information assets that are critical to business success, boards will wish to reassure themselves that they have regular up to date information on the threats and known business vulnerabilities to make informed information risk decisions.

We can all name companies whose cyber security has been very publicly compromised: where it has happened, this has caused tangible damage.

II.2. What is information?

Information, financial or about people and systems, is the lifeblood of any organization.

Yet, with increasing automation and interconnectivity of information systems, a compromise in one area could impact the entire organization and its customers.

Information is everywhere from customer facing systems (ATMs, points of sale, mobile phones), to business systems (research data and other intellectual property, management and customer relationship information) and operational systems (safety, protection, process control). When identifying information assets, all of these different areas need to be taken into consideration.

II.3. Actors / players in cyber field

There are many types of people who pose a risk to business information assets:

Cyber criminals - interested in making money through fraud or from the sale of valuable information;

Industrial competitors and ***foreign intelligence services***, interested in gaining an economic advantage for their own companies or countries;

Hackers who find interfering with computer systems an enjoyable challenge;

Hacktivists who wish to attack companies for political or ideological motives;

Employees, or those who have legitimate access, either by accident or deliberate misuse.

II.4. More than a technical threat

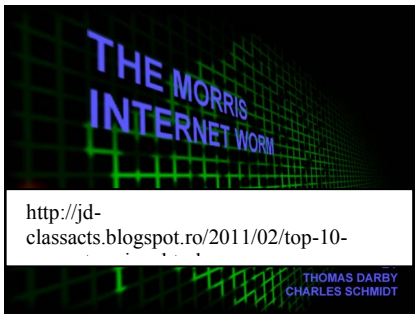
Many attempts to compromise information involve what is known as social engineering, or the skilful manipulation of people and human nature. It is often easier to trick someone into clicking on a malicious link in an email that they think is from a friend or colleague than it is to hack into a system,

particularly if the recipient of the email is busy or distracted. And there are many well documented cases of hackers persuading IT support staff to open up areas of a network or reset passwords, simply by masquerading as someone else over the phone.

The key is effective enterprise-wide risk management and awareness. Being aware of potential threats is a normal part of risk management across the private sector. Alongside financial, legal, HR and other business risks, companies need to consider what could threaten their critical information assets and what the impact would be if those assets were compromised in some way. The key is mitigating the majority of risks to critical information assets and being better able to reduce the impact of and recover from problems as they arise.[iii]

III. The history of cyber attacks - a timeline

1988 - The Morris worm - one of the first recognised worms to affect the world's nascent cyber infrastructure - spread around computers largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tapan Morris, who said he was just trying to gauge how big the Internet was. He subsequently became the first person to be convicted under the the US' computer fraud and abuse act. He now works as a professor at MIT.[1]



http://jd-classacts.blogspot.ro/2011/02/top-10-

DECEMBER 2006

NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked. Business Week reported that the plans for the latest US space launch vehicles were obtained by unknown foreign intruders.

http://www.dailymail.co.uk/sciencetech/article-1370915/NASA-systems-vulnerable-crippling-hacker-attacks.html

APRIL 2007

Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial. Some government online services were temporarily disrupted and online banking was halted. The attacks were more like cyber riots than crippling attacks, and the Estonians responded well, relaunching some services within hours or - at most - days.

[1] http://jd-classacts.blogspot.ro/2011/02/top-10-computer-virus.html

JUNE 2007

The US Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit the Pentagon's networks.

OCTOBER 2007

China's Ministry of State Security said that foreign hackers, which it claimed 42% came from Taiwan and 25% from the US, had been stealing information from Chinese key areas.

In 2006, when the China Aerospace Science & Industry Corporation (CASIC) intranet network was surveyed, spywares were found in the computers of classified departments and corporate leaders.

SUMMER 2008

The databases of both Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

AUGUST 2008

Computer networks in Georgia were hacked by unknown foreign intruders around the time that the country was in conflict with Russia. Graffiti appeared on Georgian government websites. There was little or no disruption of services but the hacks did put political pressure on the Georgian government and appeared to be coordinated with Russian military actions.

JANUARY 2009

Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization based in a former Soviet state, and paid for by Hamas or Hezbollah.

JANUARY 2010

A group named the "Iranian Cyber Army" disrupted the service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message.

The same "Iranian Cyber Army" had hacked into Twitter the previous December, with a similar message.

OCTOBER 2010

Stuxnet, a complex piece of malware designed to interfere with Siemens industrial control systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program.

JANUARY 2011

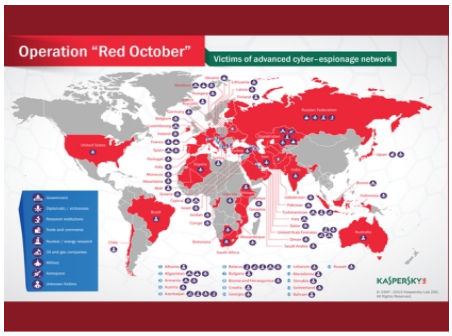
The Canadian government reported a major cyber attack against its agencies, including Defense Research and Development Canada, a research agency for Canada's Department of National Defense. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the Internet.

JULY 2011

In a speech unveiling the Department of Defense's cyber strategy, the US Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the Department of Defense were stolen.

OCTOBER 2012

The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007. Hackers gathered information through vulnerabilities in Microsoft's Word and Excel programmes. The primary targets of the [2]attack appear to be countries in Eastern Europe, the former USSR and Central Asia, although Western Europe and North America reported victims as well. The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures.



https://www.securelist.com/en/blog/785/

MARCH 2013

South Korean financial institutions as well as the Korean broadcaster YTN had their networks infected in an incident said to resemble past cyber efforts by North Korea.

IV. Respond to an incident and recover from disaster

Security protection measures cannot provide 100 per cent protection to systems because both technical and non-technical vulnerabilities will continue to exist regardless of the protective security regime. An essential part of any security strategy is therefore to recognize that residual risks to systems will continue to exist and have to be managed along with the ability to identify and respond to any other changes in the threat.

One of the issues that have to be considered is that normal information assurance approaches as applied to the office environment may not be suitable for process control

[2] https://www.securelist.com/en/blog/785/

systems. Such systems often face different challenges and constraints. Although the differences may be subtle, it is important to consider them when developing the information security requirement and preparing incident response plans in particular. Therefore, the main principles used here are protect, detect and respond.

The ability to respond effectively to security events will depend on the ability to monitor and detect security related events and the quality of the response plans in place. This in turn is dependent upon well secured and monitored systems, effective and clear governance and the skills and awareness of personnel.

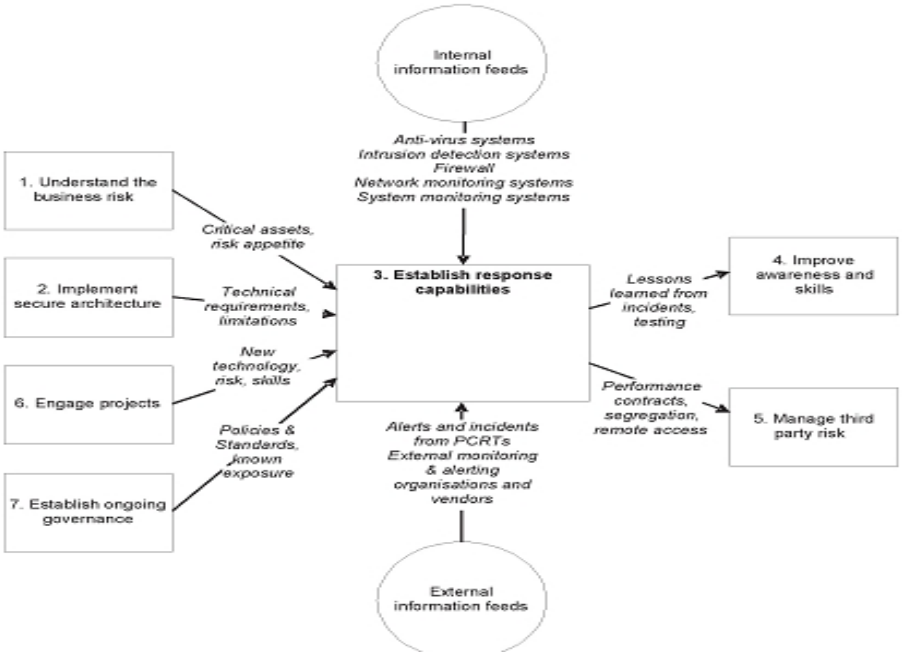


Fig. Establish Response capabilities

The capability to respond to both alerts and incidents is an important part of a process control security framework. Obtaining management support, determining responsibilities, establishing communication channels, drafting policies, and procedures, identifying pre-defined actions, providing suitable training and exercising the whole process prior to incidents enables a quick, effective and appropriate response which can minimize the impacts and their cost, possibly avoiding such incidents taking place in the future. Despite these advantages, many organizations do not have comprehensive cyber-attack response plans in place to cover process control systems.

IV.1. General principles - Good practice

Some examples of good practice principles are mentioned below:

IV.1.1. Process Control Security Response Team (PCSRT)

Process Control Security Response Team (PCSRT) is a core element of an organization's response capability and provides the foundation for effective monitoring, analysis and managing the response to alerts and incidents. The PCSRT must be involved at every step in the process of monitoring a situation, analysing any changes to the cyber threat and initiating appropriate responses.

A key requirement for a successful PCSRT is to ensure that the right people with the appropriate knowledge and skills are involved. The team can either be part-time or full-time and may be a central resource, a site resource or a combination of these.

In large organizations, it may be possible to have a Coordination Centre (CC) that can monitor and analyse events, advising local sites on appropriate actions and coordinating their activities. A CC can provide a better approach to incident response as it is usually ideally placed to share and obtain information from other groups such as business partners, vendors, other Incident Response Teams, law enforcement and infrastructure protection teams such as CPNI. A CC can also often provide an effective 24/7 operation using fewer resources than a collection of individual local teams. However, a CC also has disadvantages. For example, it may not have enough knowledge of the local sites to fully understand their operational environment or the personalities involved.

The alternative is that of a local site team that might be created using personnel who have a part time incident response role which is performed alongside their normal day to day activities. Local site teams will have extensive knowledge of local issues and operational environments. In practice, a hybrid approach is often preferable, i.e. a CC sharing information with local teams based at the operational sites. This model leverages the efficiencies of a CC in carrying out day to day monitoring, enabling the local site to concentrate on their normal core activities but responding to incidents or alerts when advised by the Centre.

One of the major difficulties in this area, regardless of the preferred operational model, is the availability of personnel with the necessary operational, interpersonal, technical and incident management skills. Significant training may be required before a team can become fully effective.

IV.1.2. Ensure appropriate incident response and activity continuity plans

In many organizations, there is often a variety of response and continuity plans in existence. Such plans include business continuity, disaster recovery, safety, health and environmental incident or other organizational and industry specific emergency plans.

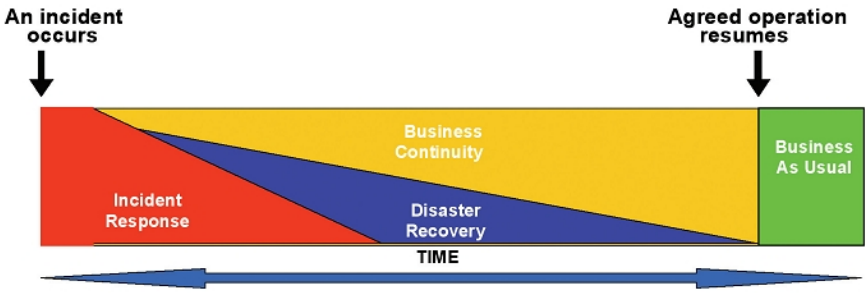


Fig. Response and continuity plans

The figure shows how incident response plans focus on the short period of time directly following an incident. Incident response plans are focused on providing an immediate response to events by implementing immediate actions. As incidents progress, the focus shifts to initiating business continuity (ensuring the business can continue to operate during the incident) and disaster recovery (restoration of lost or damaged data and systems). In establishing effective response plans for process control systems, there must be a focus on incident response, as digital security events often occur suddenly without notice and require a rapid and effective response in order to avoid incidents or minimize their impact if they cannot be avoided.

IV.1.3. Ensure plans are regularly maintained, rehearsed and tested

Despite careful planning, it is often found that plans and personnel behave differently in real life situations. All personnel should be trained in the execution of the plans which should be regularly tested to ensure that they perform in the manner they were designed.

Plans should be reviewed at least annually and more frequently for critical or high-risk systems. They should be modified following any changes to the threat or protective security requirement, the system itself or organizational structure. Lessons learned during an exercise or following incidents should also be incorporated into the plans.

IV.1.4. Establish an early warning system

Having a well-defined and rehearsed early warning system will enable organizations to respond rapidly and effectively to security alerts and incidents, minimizing their cost and disruption.

Many organizations have response and continuity plans in place but often they are not effective at identifying security incidents, determining the appropriate action and initiating the response plans.

A common problem is not having timely access to appropriate information from internal and external sources on which they can base decisions. Another issue is that they are

overwhelmed by a large volume of information that they cannot effectively process. Consequently, they are unsure of the problem and how to react to it.

An example of a high level incident triage process is outlined in Figure below which describes three key stages involved in responding to events.

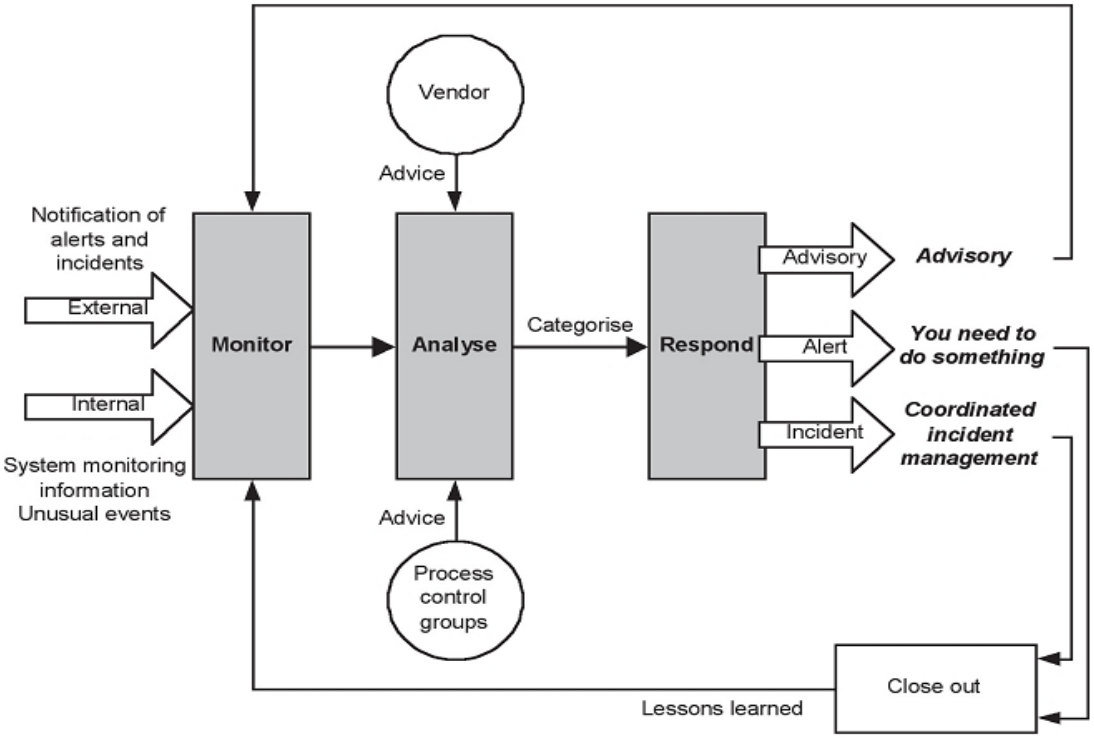


Fig. Monitor-Analyse-Respond triangle.

• **Monitor**– collecting information security data from inside and outside the organisation, such as alerts, virus infections, threats, patch notifications, incident notifications and data from network and performance monitoring systems

• **Analyse**– categorisation of the information received from the various sources into different levels and types of potential threat, filtering out the appropriate data for which a response is needed.

• **Respond**– how to respond based on the type and category of threat and the associated risk to the organisation.

IV.1.4. a. Monitoring stage

The normal state of operations is where both internal and external information feeds are monitored for any relevant events such as security alerts, malware and vulnerability notifications or abnormal system behaviour. A balance needs to be found between trying to process every scrap of information available, which would require a large resource effort, and collecting enough data such that important alerts or incidents are not missed.

Common **internal** information sources include:

- Firewall monitoring systems
- Intrusion detection systems
- System and network performance monitoring systems
- Virus and malware reports
- System fault reports
- Helpdesk reports.

Common **external** information sources

Examples of external information sources include:

- Infrastructure Protection Teams, e.g. CPNI
- Computer Security Incident Response Teams (CSIRTs)
- US-CERT
- CPNI Information Exchanges
- Hardware manufacturers
- Control systems and application software vendors
- Operating system vendors
- Antivirus companies
- External security monitoring organisations (e.g. outsourced firewall and IDS monitoring)
- Technical media
- Newsgroups
- Security forums
- Law Enforcement Agencies

Information from the various monitoring sources may be received in a variety of different forms, e.g. raw system logs, Emails, websites, RSS feeds, pager or even mobile phone text messages. The task of assessing this data can be time consuming so it is worth putting in place processes to filter out superfluous data and present only the important information, preferably in as clear a way as possible.

IV.1.4. b. Analyse stage

Analysing large volumes of system data and internal/external information feeds needs to be conducted quickly and effectively. For example, there is little value in taking ten days to determine that a new worm represents a problem to the organization as it may have infected systems far sooner!

It is important to have personnel with the right expertise contributing to the analysis of security alerts, incident reports and information feeds. Although control systems are now often based on standard IT technologies, there are differences between the two environments.

For example, personnel with networking skills and knowledge of application software will be able to understand the general IT issues but in the process control environment personnel with the relevant knowledge of those systems must also be involved.

Each alert needs to be assessed for the potential impact on the process control systems in use and any appropriate action agreed. The assessment can be complex and any resulting analysis needs to be expressed in a clear and concise manner before being communicated to PCSRT teams.

One useful way is to categorize the information based on the threat:

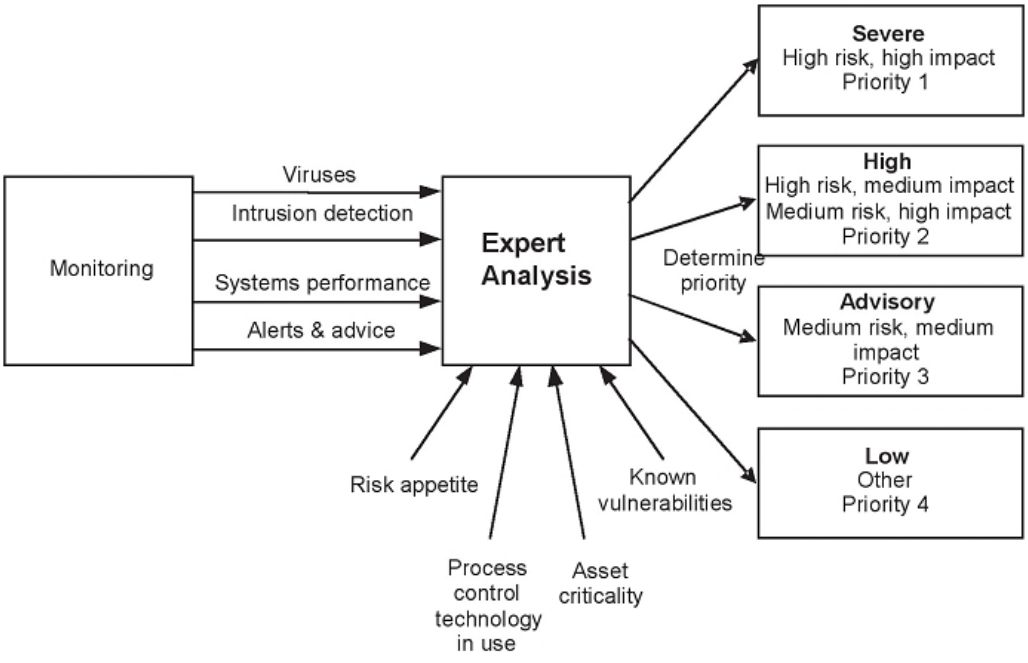
• Severe – a current incident or very high threat e.g. worm outbreak on the internet or on the corporate or process control network

• High – high threat vulnerability, e.g. important external activity

• Advisory – low threat vulnerability at present further monitoring is required, e.g. activity on the internet

• Low – little direct threat to the control system, e.g. Email virus where the function is not present on the process control system.

In order to simplify the decision making process it can be useful to have agreed predefined criteria for each category. It should be noted that not all threats will easily fit a predefined criteria. Such threats will need the experienced analysis of IT and process control specialists to interpret the available information and make appropriate decisions.



IV.1.4. c. Respond stage

This stage is about initiating the appropriate response to an incident in a timely manner. The trigger will normally be the results of the previous analysis stage. Typical situations are:

- Security alert (e.g. advance warning of a possible incident, increased hacker activity or possible malware problem)
- Vulnerability notification (e.g. a vulnerability has been identified or a software patch has been released for a control system)
- Malware infection (e.g. a worm or virus is detected in a control system)
- Hacker infiltration (e.g. a hacker has managed to compromise a control system).

IV.1.5. Establish processes and procedures

The procedures to include in a process control response plan need to take into consideration the operational environment, potential threats, vulnerabilities and experiences from previous incidents.

The following are ideas of some procedures that could be included in a response plan:

- Malware infection and removal
- Suspected hacker infiltration
- Denial of service (DoS) attack
- Disconnection of control system from other networks (if possible)
- Reconnection of control system to other networks
- Inability to view status of plant (loss of view)
- Inability to control the plant (loss of control)
- Emergency anti-virus and intrusion detection system signature updates
- Business as usual and emergency security patching processes.
- System backup and restore
- Confirmation of correct system operation (i.e. a procedure for verifying that a system is operating as normal).

IV.1.6. Establish incident reporting

There is a strong tendency for process control security incidents to be kept confidential and for organizations not to disclose incident information to external agencies in order to protect reputation and not to encourage external scrutiny.

However, there are advantages to sharing information about incidents. Sharing such information can allow further investigation by other agencies, the avoidance of similar

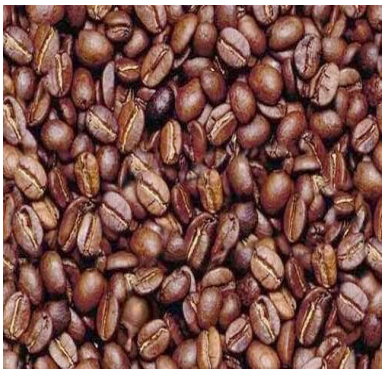
incidents in other organizations and develop a better understanding of the risks facing control systems.

IV.1.7. Ensure lessons are learned from incidents

It is important to ensure that following situations where a response to a digital security alert or incident has been required, any lessons or possible improvements to the process are identified and acted upon to ensure continuous improvement of the response processes.

Post incident reviews should be carried out both centrally and locally and could trigger updates to response plans, policy & standards and the enterprise risk profile.

V. Conclusions



There is a common need to resist, reduce, and fight cyber threats and respond to attacks and building an effective incident management capability is often a much more nuanced process.

Basic information risk management and incident response can stop up to 80% of the cyber attacks seen today, allowing companies to concentrate on managing the impact of the other 20%.

Cyber threats are a new and evolving form of attacks that presents a strategic threat to all type of entities and must be addressed. With some exceptions, the use of cyber attacks has historically been limited to espionage and political messaging. However, given the integration of information technology into virtually every aspect of modern society, the prospect of more direct and potentially devastating use of cyber attacks must be taken into consideration when developing your companies' incident management capability.

It is hoped that this paperwork can help leaders identify their own organizational solutions and build capabilities that best fit their organization's needs.

VI. Endnotes & Reference

[i] Wikipedia, 29 .01 2014, http://en.wikipedia.org/wiki/Crisis_management, 29.01.2014

[ii] http://maiorescu.blogspot.ro/2010/07/ulmer-rr-sellnow-tl-seeger-mw-2007.html

[iii] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

http://www.antiessays.com/free-essays/286982.html

http://en.wikipedia.org/wiki/Crisis_management

http://searchsecurity.techtarget.com/news/1265720/Black-Hat-2007-Lessons-of-the-Estonian-attacks

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

http://www.isaca.org/Journal/Past-Issues/2012/Volume-5/Pages/JOnline-An-Introduction-to-Crisis-Management.aspx

http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

http://www.cpni.gov.uk/advice/cyber/

Information Security Fundamentals, 2nd Edition_opt

NIST Special Publication 800-53, Revision 3

PUBLIC SYSTEM FOR SECURITY OF CYBER INFRASTRUCTURES - PSSCI

Author:
Col. Cristian-Teodor PĂUN

Introduction

„… More than a decade and a half since the Revolution of December 1989, the Romanian people overcome phase transition from totalitarianism to democracy and is firmly committed to the moral reconstruction, institutional modernization and civic responsibility, in full agreement with its core values, with values EU and NATO. Today - in a crucial moment in its history - Romania needs this national project realistic and pragmatic, able to harmoniously combine individual initiative with modern citizenship and responsible commitment.

The new security strategy is a major step in this direction and is focused in terms of its democratic purpose on ensuring the security of the individual, his life and family. As party convergence factor and cumulative national security aims to ensure democratic normality to aspiring society - citizens, communities and the state - based on efforts to complete keeping within the law, building of economic prosperity, social harmony and political stability. National security is achieved in the democratic order by: full exercise of rights and liberties; assuming conscious responsibility; improve the capacity of decision and action of the state; the Romania as an active member of the international community.National security is achieved through their own efforts and cooperation with allies and partners in accordance with national programs of EU security strategy and the strategic concept of the Alliance.

… It aims to harmonize national efforts with international commitments and identify ways to work able to prevent and counteract threats appropriate. Efforts are also aimed at promoting democracy, peace, and stability in other areas of strategic interest, reducing vulnerabilities, developing national capabilities and profound transformation of security institutions" mentioned mister Traian Băsescu, the President of Romania, in National Security Strategy, in 2007.

I. New concept system in cyber infrastructure protection

I.1. System Objective

The main objective of this project is to implement a system for ensuring interoperability between computer security components installed within the public so that through its functions contribute to the protection of fundamental systems, and the information within these authorities, as well as increasing availability and level of trust in public services specialized to citizens / business / public administration, ensuring, improving and creating

prerequisites for modernization of their systems, including minimizing the time devoted to activities for recovery / restoration as a result of an incident or cyber attack.

I.2. Interoperability of Security Operation System based on PSSCI

Thus, the newly created system will be managed hierarchically-centralized information generated as a result of the implementation of systems for cyber security, increasing the availability and confidence in public services provided to citizens online by public institutions and designed to protect information systems from the central authorities.

So, the system will ensure interoperability of security systems implemented within public institutions with National Cyber-security Center computer system on cooperation, information and response by creating a mechanism of early warning information and dissemination of information in real time, which will cover the following aspects:

- **Interoperability at the organizational level** to include as beneficiaries of the project public institutions managing cyber infrastructure of national interest (ICIN), including those that have SCADA systems, and creating a web portal which will have access to representatives of the involved institutions;
- **Interoperability at the semantic level** by establishing a common format for transmission and interpretation of events in the security systems;
- **Interoperability at the technical level** that requires the creation of VPN tunnels for secure connectivity between National Cyber-security Center and beneficiary institutions and implementing an automatic transmission security alerts.

PSSCI aims to strengthen the existing cyber security recipient infrastructures by adding security technologies not covered by the current systems and to standardize the types of alerts.

PSSCI web portal will be accessible from the Internet securely by authenticate users when accessing individual each time. There will be information on security incidents identified and, also, that will include recommendations to eliminate the risks. The portal will provide information on the state of cyber security statistics at national level.

II. SOLUTION REQUIREMENTS

II.1. Implementing principle

The project aims in terms of information security computer networks considered ICIN and incorporate a range of technologies configured on the principle of "defense in depth". They protect both information and information systems that provide transmission, transport and access. Will be set several levels of information protection and will be implemented safeguards adapted to the needs and specific protected area.

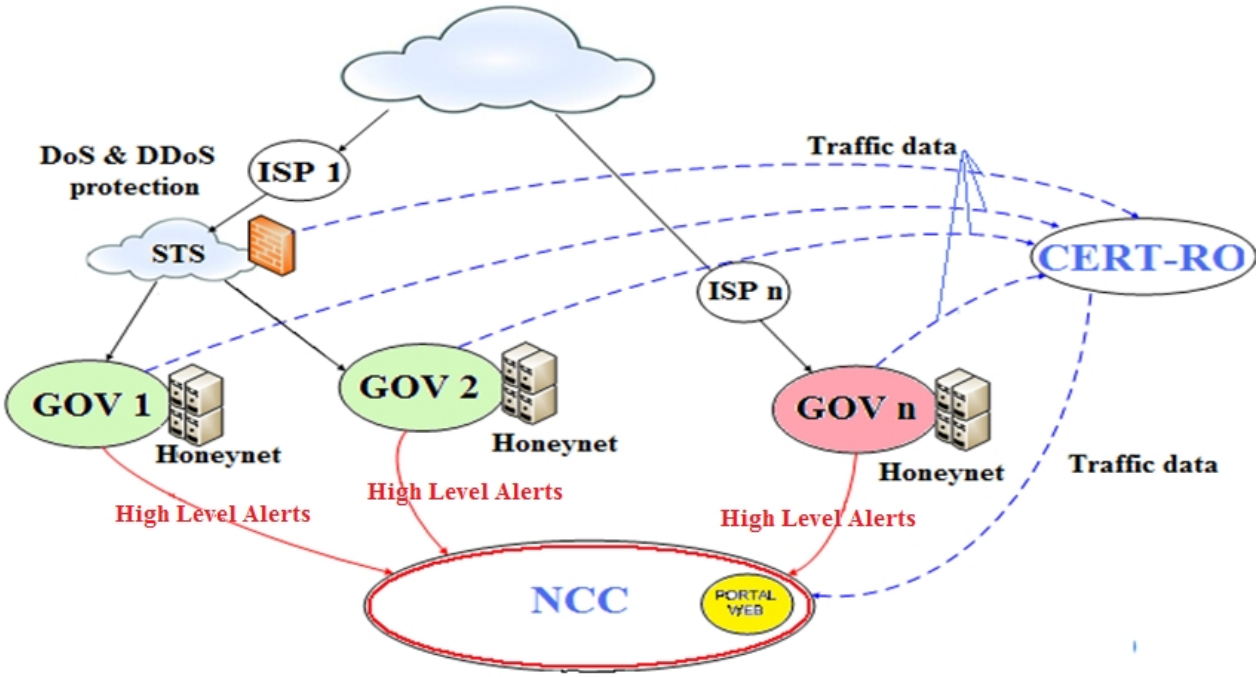
II.2. Implementing principle

The technical solution is based on a set of equipment that may have different manufacturers, but are aligned to international standards for interoperability and can be easily integrated in an existing computer network. Ensure that the following security principles: confidentiality, integrity and availability.

The project will implement a cyber security architecture type within each ICIN SOC in order to identify and analyze cyber events that can adversely affect the integrity, availability and confidentiality of services and information in the ICIN. Information security specialists within ICIN sites administer solutions implemented in the project, and thus can achieve faster action if a cyber security incident.

To obtain an overview of the state of national cyber-security project proposes an architecture for interworking between SOC and the National Cyber-security Center sites as

shown in Fig. One. Moreover, information collected through events cyber systems developed under this project will contribute to the National Early Warning System, managed by CERT-RO.



II.3. Operation approach

After identifying a cyber security incident in a ICIN analysis of this event will be conducted in the SOC's, but at the same time will be submitted technical information (logs) and high-level alerts (intelligence) to the National Cyber-security Center and technical information (logs) to CERT-RO, to supply the National Early Warning System.

The National Cyber-security Center are specialized multi-institutional teams of cyber security incident response to a request for prompt ICIN intervention, offering expert technical assistance and providing malware analysis. Laboratory will analyze the malware, identified in ICIN sites, within a management system that allows security events correlation and interpretation of global events.

By notifications and alerts offered all ICIN sites will inform under the National Cyber-security Center Alert and therefore the implementation of a prevention and coordination of defense against cyber attacks isolated or distributed. The project will provide training of specialized personnel in the ICIN sites to use systems and solutions that will be implemented, ensuring the smooth running of activities to prevent and counter cyber threats in the networks beneficiaries.

The implementation process will be conducted in accordance with a methodology checked to ensure control of the phases, activities and tasks, time planning, resource allocation, content and outcome stages, confirming the results and documentation of the implementation process.

II.4. Security provisions

The project will implement a high level national cyber security by securing independent of each ICIN and implementation of a centralized management of security incidents on national security and applied the following techniques: knowledge, prevention, detection, investigation and correction techniques to be implemented in all ICIN sites.

Knowledge provides information support to develop proactive and reactive measures to ensure cyber security. Knowing the scale of risks and threats derived from activities in cyberspace and how to prevent and counteract them, requires effective communication and cooperation between actors in this area.

Prevention consists of all actions taken to eliminate security breaches before they are exploited in order to prevent theft, destruction or alteration of confidential data. The project provided the following safety checks:

- Implementation of management security vulnerabilities;
- Securing Web traffic and e-mail;
- Implementing firewall policies tailored to the needs ICIN;
- Restrict user access to specific internal ports of workstations.

Security controls that fall within the role of information **detectives** have qualified people that a particular event occurred unauthorized or unwanted. The project covers this type of security measures by implementing the following controls:

- Centralized collection and monitoring of security events generated by network equipment and security system generate correlations and automated alerts;
- Identify malware anti-virus scan performed at several points of entry into the network;
- Detection of malicious network traffic considered, such as exploiting a vulnerability or non-standard network transport protocol.

Security incident **investigation** is to identify the causes of the incident, the affected systems analysis, identify the damage and protective measures against future similar activities.

The project will carry out these activities through the implementation of solutions and technologies that enable:

- Analysis of a central point of security events generated by computer network equipment ICIN;
- Analyze network traffic captured at the exit points in the Internet and the internal network zones ICIN for complete visibility.

Activities consist of all corrective actions necessary to address vulnerability or flaw identified in the ICIN computer network may consist and applying updates to certain applications or systems performing configuration changes or stopping the vulnerable services.

III. TECHNICAL DESCRIPTION OF PROJECT

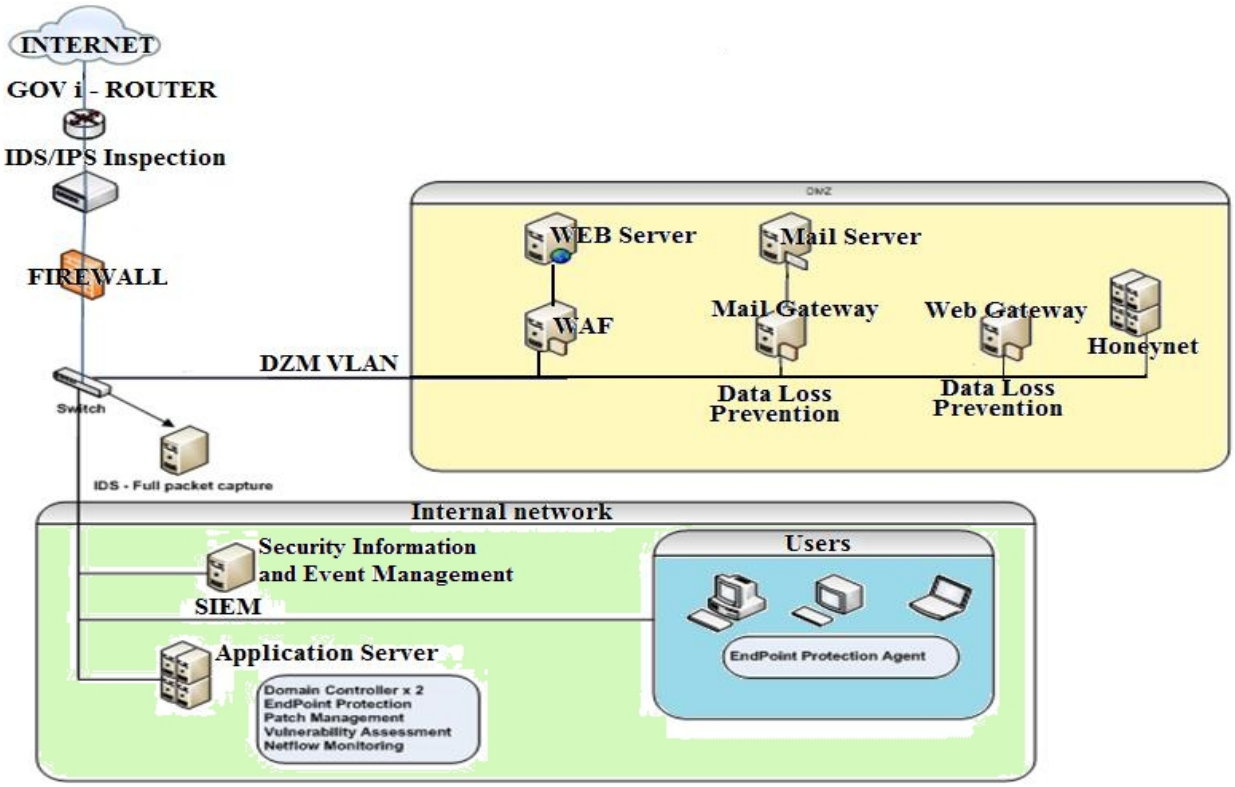
III.1. The functional requirements of the system

The solution proposed by architecture and solutions implemented, will meet the following requirements:

- Ensure optimal security level of the computer networks protected ICIN;
- Configure all equipment and solutions in accordance with manufacturers' recommendations and good practices in the industry;
- Providing opportunities for compromise identification methods currently known and proposal capabilities for identifying new attacks like "day-zero";
- Process automation, notifications and reactions to the widest possible scale;
- Prevent attacks by identifying security breaches before they run or fight against them in the early stages.

III.2. The functional architecture of the system

Network infrastructure project proposed for ICIN is shown in the following diagram.



The proposed infrastructure will strengthen cyber security in computer networks ICIN sites, by adding security technologies covered by the current systems. Network infrastructure defines two areas: internal and DMZ that will host various systems and technologies based on their role, thus ensuring a high protection of domestic resources ICIN external and internal threats:

- **The DMZ** will be placed ICIN systems while meeting its external environment and through which internal users will have access to Internet resources;

- In **the internal network** are handled confidential information ICIN so high protection is required. Towards this area there will be direct access from the Internet, but only through existing resources in the DMZ for certain services such as the e-mail.

Networking and security solutions that interface with the Internet are designed to create a first perimeter of defense against external factors:

- **Equipment Router** is responsible for routing network packets filtering and securing traffic source traffic management (QOS). It also supports key standards for packet switching of the two TCP / IP stack (IEEE 802.1Q, IEEE 802.3ad/LACP, IEEE 802.1d STP, IEEE 802.1w RSTP, MSTP IEEE 802.1s, IEEE 802.1x, IEEE 802.1 ab LLDP). Router will offer equipment and balancing traffic across multiple WAN interfaces, in cases of multiple Internet service providers.

- Role **Firewall solution** is to block unauthorized traffic to allow access from outside to inside or vice versa, only the traffic according to security policies ICIN. It also supports key standards for packet switching of the two TCP / IP stack (IEEE 802.1Q, IEEE 802.3ad/LACP, IEEE 802.1d STP, IEEE 802.1w RSTP, MSTP IEEE 802.1s, IEEE 802.1x, IEEE 802.1 ab LLDP). The solution will enable traffic filtering based on MAC, IP, protocol, VLAN-ID, and the possibility to define the filtering rules as ACL lists.

- By inspection **IDS / IPS** will be identified and blocked traffic deemed malicious before touching ICIN protected areas network, such as exploiting a vulnerability or non-standard network transport protocol (attacks on operating systems, attacks against web servers and databases against downloading files containing malware, scans network connections to server controls belonging to botnet networks, VOIP attacks, attacks IPv6 traffic malformed, invalid headers, segmentation protocol TCP / IP, IP fragmentation protocol, buffer overflow attacks, launching exploits the vulnerable applications). A solution of this type will allow

monitoring, real-time traffic analysis capabilities and has "deep packet inspection" detections when it will be announced in the following ways: alert GUI, SNMP or e-mail the results of those actions may be exported for viewing and to a solution of SIEM type. Arrangements for signature-based detection, anomaly traffic or " stateful protocol analysis". Solution can be configured through preventive actions when automatic detection. The solution may be located within the network ICIN in two ways: inline (blocking and alerting capabilities present) or passive (present alerting capabilities).

Firewall equipment, the internal network and the DMZ will be interconnected by equipment **type switch**. Traffic between these blocks will be separated by implementing VLANs, traffic will require segregation and isolation of these areas. By means of a switch port, for replication packages, all traffic will be captured ICIN network on a dedicated server for further analysis in the case of a security incident. Also, the server will be implemented this solution IDS software, freely available in the Internet, to identify malicious traffic that managed to pass the first security perimeter and identifying attacks launched from internal systems ICIN.

Next perimeter security will be achieved by protecting web services and e-mail ICIN. Security solutions at "**gateway**" **Web Gateway** and **E-mail Gateway**, are designed to protect users against cyber threats outside internal computer network ICIN, such as unsolicited email messages (spam), the transmission of malware informational messages via e-mail or accessing some websites that contained malware and infect visitors.

Web Gateway solution consists of a dedicated hardware will provide the following security services:

• Anti-malware capabilities:

o Malware detection and blocking;

o Control for groups of applications, such as VoIP, anonymsation, "Instant Messaging", online games, media, "peer-to-peer", "file sharing" and offers options to limit bandwidth per application, restriction and blocking certain functionality, eg loading a file lock on an application such as "Instant Messaging";

o Web 2.0 allows control;

o Identify anomalies certain protocols allowing identification and blocking botnet networks;

• URL filtering capabilities:

o Contains a predefined URL categories: pornography, social, mail service portal, anonymisation gambling, "web chat", "peer to peer" malicious portals;

o Allows creating a new category URL, change lists predefined categories, but also remove a web site in the pre-framed wrong;

o Filtering access by defined categories;

o Manually a certain URLs by keywords or by constructing regular expressions type "regex".

The solution will enable the application of security policies on user / user groups that will be picked from a LDAP server authentication is achieved by SSO them, or create Web Gateway solution and the local log. Logs generated are stored locally and transmitted to an external Syslog protocol for centralized collection and archiving a SIEM solution type. The solution allows you to create a specific policy protocols FTP, HTTP and HTTPS that can be locked downloading files by type (pdf, rtf, executable code, video, audio, images, etc..) And size. The solution will enable the creation of specific web pages that will be presented to the user in case of violation of security policies, and displaying a message disclosure policy.

E-mail Gateway solution consists of a dedicated hardware with the following functionality:

• Detection Capabilities confidential data found in files.

• Anti-malware capabilities:

o Malware detection and blocking attachments found in messages based on signatures, heuristics and reputation;

o Scanning archived attachments, including several levels;

o Moving to quarantine infected files;

• anti-spam capabilities:

o Provides a built quarantine and presents identification capabilities spam including the following methods: Heuristic, "Bayesian" based on reputation shippers, RBL "blacklists" and SURBL lists;

o Allows filtering emails for "whitelists", "blacklists" keywords and scan existing URLs in the body of messages;

o Spam detection for image in jpg, png and gif.

E-mail Gateway solution can be positioned within the network transparently ICIN "Inline". Logs generated are stored locally and transmitted to an external Syslog protocol for centralized collection and archiving a SIEM solution type.

If the public ICIN or collect information through a web application, offered as external service project provides its protection by implementing a **WAF solution** type. The role of this technology will be protection against known web attacks, eg Overflows, Cross-Site Scripting, Cross-Site Request Forgery, SQL Injection, Blind SQL Injection, OWASP Top Ten, and against advanced evasion techniques such.

Also, type WAF solution will provide protection against attacks using Java and PHP scripts and prevent unauthorized changes to protected web applications ("anti-defacement"). The solution will provide active and passive decrypt SSL sessions.

Following the identification of an attack, the solution enables the following actions configured in the security policy:

• Answers liabilities: raising a fault indicator that will allow the transition to an active response, increase customer logging source email and syslog alerting to a SIEM system;

• Active Replies: spoofed TCP Reset, blocking the source IP address, geo-location restrictions apply, redirect to pages error; The solution can be located in the network infrastructure in the following ways:

○ Inline transparently and reverse-proxy which involves redirecting traffic through DNS reconfiguration);

○ Sniffer by connecting to a SPAN port monitoring type or tap capture and traffic inspection.

Logs generated by the solution are stored locally and transmitted to an external Syslog protocol for centralized collection and archiving a SIEM solution type.

Within each system will be implemented ICIN of "Honeynet". Such technology presents vulnerabilities exposed and intentionally gives attackers an easy target for exploitation, but also allows security administrators to analyze the types of attacks directed at the system. The solution proposed for the implementation of "Honeynet" is made up of Open Source products and provide services capabilities to provide false information on the network structure of ICIN's a possible attacker. Under this system will simulate service (HTTP, HTTPS, SQL databases) and clients with various vulnerabilities exposed false. From Honeynet to network infrastructure ICIN will not be allowed network traffic.

The internal area to create additional level of protection ICIN infrastructure will be implemented following systems and technologies:

- **Management of security vulnerabilities**. The role of a management process security vulnerabilities is to identify possible security breaches, such as the lack of updates certain systems, the existence of open service configuration incorrectly or defective, indicating areas of network security administrator requires additional attention, before the existing vulnerabilities are known and exploited by a malicious user. Vulnerabilities is achieved by actively scanning the network and requires no local installation of software agents on scanned systems. Scanning network systems is accomplished without disrupting

ongoing activities and systems scanned. Such an approach allows for thorough inspection credentials introduction and elimination alerts of "false-positive". Specific requirements for general equipment management security vulnerabilities intended to be used in the project are presented in Annex 4.9, Annex 4.10 respectively.

- **SIEM**.(System Information and Event Management). Role of **SIEM solutions** such is centralized collection, aggregation, normalization and correlation of security events generated by network and security devices, servers, workstations, applications or any other device capable of creating entries and export them in a format supported by the solution. Through this technology will be implemented alerts, thresholds and related rules that will notify ICIN staff and will be the starting point in a possible investigation.

- **Monitoring events like Flow**. Flow monitoring events generated by equipment type network traffic anomalies can be identified and illegitimate connections between internal systems ICIN or to foreign destinations. Such solution is able to retrieve and process events received via protocols NetFlow (v5 and v9), IPFIX, sFlow, J-Flow, Netstream, AppFlow, Cflowd and Rflow, create traffic limits and alert in case of exceeding their . Limits may be imposed by traffic volume, rate, IP address, port.

In the SIEM solution, collected events can be stored in raw and normalized format, and the solution enables search and forensics type activities of both types of formats, having a search engine that allows the correlation of events captured from multiple data sources, apparently unrelated. The solution also enables integration with vulnerability scanning solutions and offers the possibility to create correlation rules based on this information, as well as running a script as a rule related action. Reporting component SIEM solution will include the existence of predefined templates, can create other templates, and run scheduled or on-demand reports, which can be exported in various formats and transmitted via a mail server.

Through SIEM solution will identify mechanisms, correlation and alerting those events that alter normality cyber security network infrastructure being sent to the National Cyber-Security Center alerts only high and very high (according to pre-established hierarchy within the SIEM 's).

To protect servers and workstations will be implemented **security technology at the "endpoint"**.

Such technology aims to protect all terminals in the network: servers and workstations and the following minimum capabilities: anti-virus scan, HIDS / HIPS and Firewall. Scanning and identifying malware, including compressed files, will be achieved by retrieving a database of signatures and heuristic analysis based on reputation. These functionalities will be implemented on the workstation.

Between ICIN sites expected to be protected by the implemented system project was identified institution, in terms of activities and services, requires an IT infrastructure to ensure a high level of computer security and maintenance services functionality under high stress.

Thus, if ICIN 44 (National Agency for Fiscal Administration) has identified the need to implement specific solutions dedicated this ICIN. As NAFA provides services nationwide to a large number of users and traffic features encountered in such services, equipment will be installed routers, large capacity to hold technical performance required to support network traffic volume pumped by NAFA.

Role router type solution is providing relevant functionality for retrieving and directing traffic at points of contact NAFA network with other networks and central government with which it interconnects, and to the Internet. The specifics of the institution's network to ensure both internal communication (i.e. between 250 offices in the territory, networks serving the central and own data centers) and, especially, the traffic generated by external users of services supported by NAFA and sized application for specific target groups between 500,000 and 5,000,000 of taxpayers, individuals and businesses.

The solution is for the installation of central, i.e. the outer perimeter of the network NAFA and must make operational both during operation in normal operating conditions and overload situations, including situations assimilated DDoS attacks (as primary insurance line exercise capacity in case of DDoS attack).

Functionality and performance have been provided specific border router, the typical configuration designed for a national network operator, i.e. redundant equipment as pairs (one pair for each data center) equipped with 10G interfaces. Since the information is circulated NAFA confidential or private equipment is necessary to implement IDS / IPS and firewall to identify and mitigate possible intrusion attempts on systems and services offered by Internet ICIN and exposed environment.

Firewall equipment will provide the ability to define security policies on network traffic within NAFA.

For the purposes of administering proactive security policies of the institution, the solution is designed to provide authentication capabilities concurrent users requesting internal crossing network perimeters of NAFA authentication terminals which access is requested, identifying the applications that generates sessions communication, URL filtering to which they are initiated and filter content data is transferred as a part thereof.

To ensure protection of reactive capacity in the domestic network perimeters of NAFA, the solution is designed to ensure concurrently integrated intrusion prevention capabilities and continuous filtration antimalware for both known threats and for specific atypical vectors propagation of Class 0-day attacks by functionality sandbox / Honeynet integrated.

The solution is for installation centrally concerned to define and defend the interior perimeter of the national network of NAFA and must make operational both during operation in normal operating conditions and overload situations, including situations assimilated attacks DDoS computer (the secondary line of defense to ensure the specific capacity in case of DDoS attack).

They were provided specific functionality, performance security gateway as redundant pairs of equipment (two pairs for each data center) to protect internal networks access independent and respectively to protect the network level servers application subject to the DMZ.

Core sandbox / Honeynet partner will jointly serve all gateways of the solution. To identify anomalies in the network traffic at NAFA monitoring systems are needed type traffic flow, which provides a holistic view of existing traffic.

The role of this solution is to provide visibility to the network traffic and independent means of networking and security equipment to the policies that were configured communications and security by exploiting metadata type Flow. The solution chosen should provide analytical data recovery capabilities Flow type, i.e. both those taken and those generated independently by behavioral analysis models based statistical machine suitable for precise determination of the resultant effect (on traffic) of communications and security policies implemented, and to detect traffic anomalies, and the impact of this and the action network distributed agents attack (botnet, or worm / virus outbreak) based load malware or models / propagation vectors unrecognized reactive mechanisms (IPS / Antivirus).

The solution needed to be implemented at least in segments aggregation and core operational data centers, primary and secondary, of NAFA.

For all workstations at the NAFA is required a solution within capabilities „**Port Device Control and Endpoint Security”** to mitigate order and security risks arising from the users of the network.

The role of this solution is to provide protection based on the proactive security policy of workstations NAFA internal networks, namely the level of access users.

The purposes of defining and managing policies effective use of resources by the application, the solution is designed to provide authentication and authorization capabilities of

applications whose performance will be permitted workstations NAFA access networks, i.e. effective control running at launch to ensure that they will be able to upload only authorized applications.

To ensure protection against unauthorized copying system data outside and against the introduction of unauthorized data from outside applications or launch external media unauthorized capabilities are necessary to control the use of local ports I / O station Working exclusively licensed peripherals.

However, at certain sites identified ICIN need to implement Unified Security Management platform that through integrated functionality (IDS, identifying and assessing vulnerabilities, software automatic update scan IT infrastructure to identify potential security risks, data aggregation various equipment for processing and correlation with a view to shaping the state of ICT infrastructure security system alerting on security incidents identified, detailed reporting security incidents, etc.) will provide a high level of security of their infrastructure.

For all ICIN need hardware resources and computational power to fulfill the security measures mentioned above will be covered by the purchase of next-generation servers. The project proposes development in the beneficiary institutions, of analysis and response capabilities against cyber attacks by specialized teams such CSIRT (Computer Security Incident Response Team). In this regard, the National Cyber-security Center (NCC) will support ICIN sites where a cyber attack and has the technologies needed for the performance.

The NCC will be developed under centralized management capabilities of national security events, security events are collected from all sites ICIN type SIEM solution exists. With it will build a picture of the national cyber-security can be identified similarities between alerts generated in several ICIN.

Also, security events will be saved in a log management solution for long-term storage and fast performance.

All the NCC will be developed laboratory investigations of malware by purchasing a solution of "sandbox" that simulates a network infrastructure and allows observation investigated the application behavior that will be filled with a solution of disassembling executable, malicious software (Windows and Linux) to analyze them in detail. Sandbox solution will simulate a network infrastructure and clients related to behavior analysis of executable files, scripts, DLLs, documents supported by Microsoft Office applications, files supported by Adobe Reader files supported by Adobe Flash Player and URLs.

Technology will support multiple simultaneous running malware in several system configurations. It will report the final analysis data static and dynamic analysis of the application, this will give information about the file type analyzed checksums of files involved, changes to the registry and file system, network connections created and the information conveyed by They etc..

In addition to the functionality offered by the solution of "sandbox" solution is needed to disassemble executables main characteristic of processor architectures, compilers and executable file formats.

Another direction of development in the NCC is the analysis of processes and applications running on the systems investigated and captured network traffic analysis, is proposed to purchase solutions such as "Host Forensics" and "Network Forensics".

When investigating a cyber attack highly complex sandbox solution will be complemented by an application of "host forensics" will provide CSIRT teams can collect data and artifacts from the stations operating system Microsoft Windows and allows you to run Remote specific activities process of "live response" without interfering with the activities of the users and without modifying the metadata files.

Retrieving data from the systems investigated is done according to criteria / filters that can be defined. The information to which access can be gained through this application can be found:

- Running processes and data:
    - Threads
    - Handles
    - Stacks used
    - Sockets created
- Open network ports;
- Existing network connections;
- Windows Registry Database;
- Event Logs;
- Hook System sites;
- Drivers and installed devices;
- Data on HDDs;
- Data from RAM.

The solution of "Forensic Host" will be filled with a solution for white list are files that will use a database of metadata about legitimate files (white list) and malicious files. Such a solution will minimize the time for conducting digital investigations host level by removing legitimate files known, allowing digital analysis focusing efforts on unknown files.

In addition to the solution of "**Forensic Host**" will use a solution of "**Network Forensics**" as a dedicated hardware device that CSIRT will allow teams to monitor and analyze network traffic in real time or offline and detect, based on predetermined rules, cyber security events.

Also, the solution of "**Network Forensics**" enables reconstruction of web pages, e-mail messages, Instant Messaging conversations and downloaded files, perform searches based on keywords, regular expressions, viewing and filtering by URL sites, displaying traffic statistics and filter catches analyzed traffic in a visual way by multiple criteria: time, IP address, port, protocol, application, user agent, file type, MAC address, domain, country source IP, user name, email address etc.. To assess the security of computer systems will use a special software solution for remotely detecting and testing vulnerabilities of networked equipment.

For continuous monitoring of vulnerabilities and track their evolution over time will use a vulnerability management solution

To fulfill these basic functions of the national cyber defense in the NCC will develop a medium type "cloud" virtualization technology through project covering hardware needs: storage capacity and computing power.

Virtualization solution enables the redesign and reconfiguration of the existing IT infrastructure to reduce the number of redundant rules and VLANs, providing a high level of security, flexibility and scalability both horizontally and vertically and provide the opportunity to add resources computing (minimal memory and processor) for all virtual machines without any downtime of applications and services running on virtual machines to optimize their performance for increased payloads.

In order to ensure optimal conditions of temperature inside will accommodate infrastructure planned to be installed at the National Cyber-security Center, use two air conditioning systems and to ensure a high availability of services implemented use 3 UPS equipment, rack-mountable, with a capacity of 10kVA/rack.

To equip these teams will be intervention kits that will include materials required investigators to perform analysis on site in case of a cyber event. The kit will consist of a laptop with high processing power, external hard drives for high capacity data storage and interest Managed switches for networking (allows replication packet capture and analysis while real network traffic). In order to achieve and the availability of complete and consistent information to be used in the analysis of cyber incidents, the NCC will be implemented analytical platform designed to extract data from many different sources and corroborate their offering integration capabilities data, advanced search, discovery and analysis.

Also, to conduct field investigations will use the server to provide the necessary computing power for running of multiple virtual machines (for analyzing log files, traffic, suspicious files and so on).

In each ICIN will implement a one-way transmission of data that will be used to separate networks that conveys data between different classification levels. Each type diode system will consist of two data server equipment and software component achieved using open source tools.

By implementing solutions for defending against DoS / DDoS positioned in the network infrastructure of the Special Telecommunications Service, the project will provide protection against these types sites ICIN threats.

Such an approach provides protection against attacks of the following types:

- DDoS:

- TCP;
- UDP;
- ICMP;
- Reflective flooding;
- protocol violation.

- Attacks on the dynamic routing protocols:

- BGP (Boarder Gateway Protocol)
- OSPF (Open Shortest Path First);
- EIGRP (Enhanced Interior Gateway Routing Protocol).

III.3. User management and access to system

In ICIN sites, user management will be done centrally through the LDAP protocol and authentication workstations will be satisfied by the Kerberos protocol.

Two systems will be configured with the Domain Controller role "DC" in each ICIN, similarly configured to ensure availability in the event of failure of one of them. All user accounts will be subject to security policies ICIN.

To access the resources of the Internet, internal users will transparently log in with SSO technology or re credentials in the Web Gateway solution. Will be developed Internet access policies based on user profile. Access to internal systems ICIN the Internet will be achieved by implementing secure VPN technology, which provides user authentication and confidentiality of information transmitted through the creation of encrypted tunnels.

External users (staff of partner institutions or domestic employees who undertake fieldwork) will be logged ICIN out of border, access is only given after successful authentication. For secure storage of digital certificates used to connect from the Internet to services and network resources will be used cryptographic hardware token.

III.4. System Security

Privacy and Security networks of ICIN sites is ensured by implementing security solutions and technologies in accordance with the principle of "defense in depth". They have created several lines of defense against external threats. Violations of security policies will be audited will be centrally stored and evidentiary basis for proving malicious behavior. The project aims to develop capabilities for identifying, analyzing and responding to cyber security incidents within each SOC ICIN by setting up sites and national level through the National Cyber-security Center.

III.5. Confidentiality Access to sensitive information

ICIN will be audited and identified actions that violate security policy. Communications, alerts and notifications between ICIN sites, CERT-RO and the National Cyber-security Center will be achieved only through secure channels that will ensure the confidentiality, authenticity and integrity of data transmitted.

Centralized security events collected in each ICIN, and the CERT-RO and the NCC will be stored in a secure data base where access is restricted by the base principle of „need to know".

Security methods include algorithms for integrity and stamping.

IV. RESOURCES

IV.1. Personnel and training

Human resources involved in the project are provided on one side of the beneficiaries, who will have the opportunity to prepare for cyber security specialist staff in managing computer networks owned and, on the other hand, by partner institutions in the project, including coordinating the implementation of security solutions proposed.

The project will provide an opportunity to develop new skills within the beneficiary institutions in terms of information security, which will support specific activities SOC sites.

To ensure the proper functioning of the proposed technologies and systems through this project will provide staff training ICIN and partner institutions in its implementation, responsible for the management and operation of technologies, both through training courses and by creating portal has a dedicated e-learning in which information is available about the equipment used, including work procedures required to operate the systems implemented.

The courses will be provided by manufacturing companies of security solutions or institutions established cyber security, unrelated to commercial interests and will provide advanced theoretical and practical basis for the identification and analysis of cyber attacks and malware.

The principle used in staff training is "Train the trainers" so that in the first phase will be two teams of instructors trained through specialized courses supported by certified specialists acquired technologies.

Courses will be acquired following a competitive procedure by certified instructors will provide the trainees training materials so that they can support further training of the ICIN sites. Course materials to be provided will include both printed documentation and electronic and virtual images of computer systems for training.

According to the schedule of activities during the conduct of this activity is 54 weeks. Courses will be given for each technology acquired in part, being identified 16 technologies that will be organized courses: Web gateway (1) e-mail gateway (2) SIEM (3) Monitoring network information type "flow" (4), Endpoint security (5), router (6), IDS / IPS (7), firewall (8) UTM (9), Switch (10) WAF (11), Network Vulnerability Mangement (12), web application management (13) Data diode (14) DDoS protection (15) and Unified Security Management (16).

To train specialists in the ICIN sites will take 19 instructors will be made available by the partners. Each instructor will be responsible for training the two technologies of the 16, so that they can cover during the six weeks allotted for each ICIN training in hand, all technology working in two teams of eight instructors who will run in parallel to two technology training the standard interval training (3-5 days). To this end beneficiaries will provide at least two specialists to be trained (each will be trained in the use of up to 8 technologies).

National Cyber-security Center staff and the experts appointed by the project partners will be available highly specialized training in the investigation of cyber attacks, malware

analysis and security event management through SIEM systems already in operation within these institutions or to be acquired by the project.

IV.2. Material resources

Resources for training materials, proposed solutions offered to users in the project are:

- Classrooms provided by the lead partner;
- Printed materials in electronic format on the management, use of solutions and best practices for implementation;
- Office equipment and telecommunications;
- Virtual machines or network equipment, as appropriate;
- Access to the portals of support offered by manufacturers of security solutions, where can be download study materials.

For the project will be used to material resources within the partner institutions and a set of office equipment and supplies purchased for use in deployment, complementing the existing ones. The partners of the project are:

- The Romanian Intelligence Service;
- The Ministry of Information Society:
- The Ministry of Defence
- The Special Telecommunications Service
- The Ministry of Interior.

V. MAINTENANCE AND SUSTAINABILITY

V.1 Maintenance

All solutions include hardware and software technical support and update service and will include:

- Support on-line and on-site within 24 hours, and remedial action in case of technical problems;
- Updates as appropriate: firmware, operating system security patches, migration to new versions, signatures;
- Technical assistance to ensure system availability and prevent defects in the operation;
- Security hardware resources.

All hardware and software, and all solutions will have purchased the warranty and will maintain the same level of performance as the delivery, security systems to prevent, detect and eliminate threats and / or their specific vulnerabilities throughout the period of life (up to the manufacturer to declare as "end of support").

V.2. Sustainability

Sustainability solutions and the scheme will be provided from a multiple perspective, namely:

- Human resources trained and competent in the ICIN that will ensure the sustainability and development of technical solutions;
- Technical and functional architecture of systems to enable: an extensibility and scalability; an increase in system load.

Beneficiary institutions will ensure, in accordance with the declaration of commitment, all human, material and financial resources in the post-deployment support functionalities implemented in the project.

NCC personnel will ensure interoperability purchased throughout the post implementation and functionality of the portal created in the project and made available to all partners / beneficiaries.

CONCLUSION

The integrated platform PSSCI provide:

- Guide lines for ICIN activities in security computer field:
- High standardization of security computer activities (how to make the gathering of incident and data about cyber attack, how make the detection and prevention, how establish the nature of any incident if is accidental or malicious);
- One infrastructure dedicated to inspection and analyses of malicious incident NCC;
- Dissemination in real time of any aspects threats;
- Evaluation of threats and establish the nation level of cyber security stage;
- Developing counter measures for known threats;
- Distribution of risk to controlled part of the system;
- Possibility to prevent the effects extension after attack to one or more critical infrastructure.

ESTABLISHING YOUR (SOC) SECURITY OPERATION CENTER

Author:
LTC Ahmed ALALI

INTRODUCTION

Security is becoming more and more established in the corporate structure—it is no longer acceptable for security to be a secondary function of an IT department. To address this challenge, organizations are investing in the development of Security Operations Centres (SOCs) to provide increased security and rapid response to events throughout their networks. Building an SOC can be a monumental task. Although the finer points of SOC deployment are very much network-specific, there are several major components that every organization must include: People, process, and technology. The three exist in all elements of security and should be considered equally critical components. This paper explains how strong people and well-defined processes can result in an operationally effective SOC. Proper planning is critical in the development and implementation phases. As with many security programs an iterative process is most effective in developing a refined set of procedures. This approach will allow an organization to more quickly recognize benefits from their investment, positioning them to take advantage of knowledge gained and lessons learned through the actual operation of the SOC. It is important to set appropriate expectations and timelines for the deployment of the SOC so the initial operational period is viewed as a period for refinement.

I. SECURITY OPERATION CENTER.

The first and most important component when implementing an SOC is to define the mission, charter, objectives, and responsibilities. Defining these core items will ensure its longevity and help avoid conflict with other companywide functions. To begin, create an SOC manual that formally documents each of the following items:

- Mission
- Charter
- Objectives
- Responsibilities

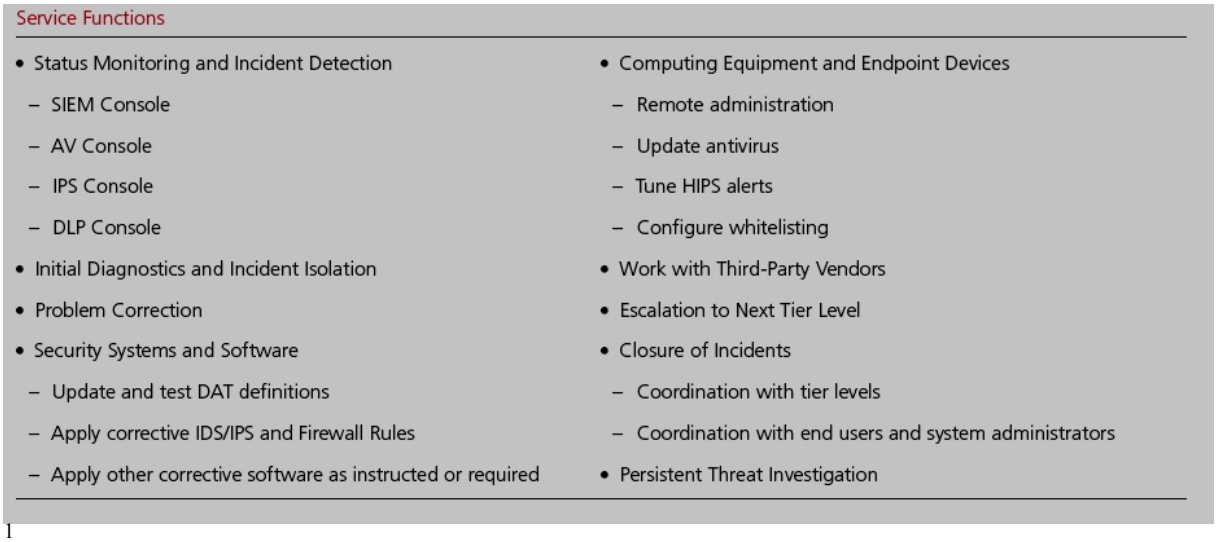
- Operational Hours

This manual will continually be used as a reference for the SOC staff and management. The definition statement should be clear and provide specific detail as described in the below example statement:

I.1. What is SOC.

"The SOC is responsible for monitoring, detecting, and isolating incidents and the management of the organization's security products, network devices, end-user devices, and systems. This function is performed seven days a week, 24 hours per day. The SOC is the primary location of the staff and the systems dedicated for this function."

The above example may not be comprehensive for some organizations and should be expanded upon with more specific details based on your organization's mission and objectives. Once the responsibility definition has been documented, a list of service functions for the SOC must be defined. These may include:



1

The service functions, once defined, will guide the daily processes and procedures for the SOC staff. Once each service is defined, each tier within the SOC can be assigned a series of responsibilities based on each individual's expertise within the tier level. For example, monitoring the AV and SIEM console may be a service function of every tier; however working with third-party vendors may be a service function only reserved for tier 2 or tier 3 SOC staff. Once each service function is defined, a series of documents must be developed to ensure the appropriate information is gathered during an event or incident and to ensure consistency across all SOC staff.

[1] Hp corporation

I.2. Determine the Process.

The number of processes and procedures for an SOC is determined by its scope, how many services are offered, the number of customers supported, and the number of different technologies in use. An established global SOC environment may have tens or even hundreds of procedures. At a minimum, the basic procedures that are required for maintaining the SOC are:

- Monitoring procedure
- Notification procedure (email, mobile, home, chat, etc.)
- Notification and escalation processes
- Transition of daily SOC services
- Shift logging procedures
- Incident logging procedures
- Compliance monitoring procedure
- Report development procedure
- Dashboard creation procedure
- Incident investigation procedures (malware, etc.)

Many of the procedures listed above may need to be customized based on the type of technology in use.

I.3. Required Templates.

A series of baseline templates should be created to help maintain documentation consistency by establishing the same format and basic information sets across policy and procedure documents. For example, templates for proper data input into ticketing systems and the GRC system will need to be developed to help ensure the appropriate technical information is gathered. A few key templates required are:

- Shift log templates for each use case
- Templates for each incident trouble ticket category

II. REPORTING.

As a primary function, regular reports will need to be generated and provided to different audiences within the organization. Usually a weekly report is prepared for incidents, detailing the activity within the SOC. These reports can be delivered to management and other members on the core escalation contact list.

II.1. Reporting Process.

The SOC manager should review all incident records regularly to ensure they were resolved within the parameters of the defined severity levels. The manager should also audit incident records that have exceeded standard resolution times to validate that the incident records were handled appropriately.

The SOC processes and procedures should be reviewed regularly and updated based on the report data reviews and audits. In addition, many other reports can be created depending on the type of data received or requested by management.

For a very detailed list of reports, refer to the "Operationalizing Information Security Putting the Top 10 SIEM Best Practices to Work" by Scott Gordon in the references section. Among these items are other key reports to measure staff on, including:

- Shift log metrics
- Trouble Ticket metrics

II.2. Understanding the Environment.

Without an understanding of the technical environment, it will be difficult to investigate and to understand if an actual attack has occurred. For this reason, the staff within the SOC must have the appropriate tools, diagrams, and knowledge of the network to perform their daily job. It is important to have both an electronic and a hard copy of the key network and application architecture diagrams. For any new SOC staff, navigating and understanding the environment should be included as part of their required basic training. This will also help meet SLAs and overall customer service within the SOC.

As a part of the SOC's service functions the security architecture will be defined and the SOC staff will have access to the different components and tools within that architecture. These may include, but are not limited to:

- SIEM monitoring and correlation.
- Antivirus monitoring and logging.
- Network and host IDS/IPS monitoring and logging.
- Network and host DLP monitoring and logging.
- Centralized logging platforms (system log, etc.).
- Email and spam gateway and filtering.
- Web gateway and filtering.
- Threat monitoring and intelligence.
- Firewall monitoring and management.
- Application white listing or file integrity monitoring.

- Vulnerability assessment and monitoring.

II.3. Developing Use Cases.

To ensure the SOC is effective, a series of Use Cases must be defined. The term "Use Cases" may be a little misleading—think of them as events that require SOC intervention and/or monitoring. For instance, a repeat attack from a single source is a Use Case. It's an actionable component of the SIEM in which the SOC was notified of through the network's primary monitoring tool. A Use Case may include the involvement of a Rule, Alarm, or even a Dashboard to meet the organization's requirements. Before defining Use Cases, it is important to have a firm grasp on the company policy, its assets, and the technical environment. A good way to develop Use Cases is by viewing the network from an attacker's perspective; think of a disruption to the environment. Another option is to look at the regulations the organization is subject to and evaluate the items that could become non-compliant. Below is a list of some important Use Cases to consider when initially setting up the SOC.

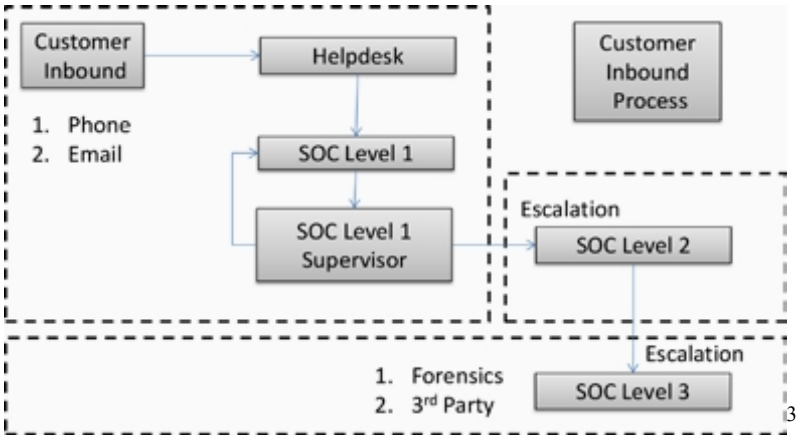
Use Case development is a critical component within a SOC and it must be understood. Below are two good write-ups that can be used to help understand the process for creating Use Cases as well as additional reporting that can be defined for the SOC environment.

Use Cases	
• Repeat attack from a single source	• Anomaly in DoS baselines
• Repeat attack on a single ID	• Anomaly in Recon baselines
• SMTP traffic from an unauthorized host	• Anomaly in Malware baselines
• Antivirus failed to clean	• Anomaly in suspicious activity baselines
• Excessive SMTP traffic outbound	• Anomaly in user access and authentication baselines
• Excessive web or email traffic outbound	• Anomaly in exploit baselines
• Excessive traffic inbound (streaming, web, etc.)	• Anomaly in network baselines
• Excessive access to a malicious website from a single internal source	• Anomaly in application baselines
• Excessive connections to multiple hosts from a single host	• Multiple logins from different locations
• Excessive exploit traffic from a single source	• Multiple changes from administrative accounts
• Excessive exploit traffic to a single destination	• Multiple infected hosts detected on a subnet
• Excessive port blocking attempts from Antivirus or other monitoring systems	• Unauthorized user access to confidential data
• Excessive scan timeouts from Antivirus	• Unauthorized subnet access to confidential data
• Accessing a malicious website from multiple internal sources	• Unauthorized user on the network
• Service account access to the Internet	• Unauthorized device on the network
• Service account access to an unauthorized device	• Unauthorized server connection to the Internet
• Scanning or probing by an unauthorized host	• Suspicious traffic to known vulnerable host
• Scanning or probing during an unauthorized time window	• Logging source stopped logging
	• Logs deleted from source
	• Device out of compliance (antivirus, patching, etc.)

[2]

III. STAFFING.

III.1. Staff and the SOC.



[3]

[2] HP corporation
[3] www.Mcaffe.com

Staff:

[4]

Staffing an SOC can be more difficult than expected. Two questions that Executives ask are:

1. How many employees do I need?
2. What skill sets are required?

The number of employees is dependent on the operating hours of the SOC. If the operations are maintained 24 hours a day, seven days a week, not only do shifts need to be considered, but you will also need to consider time off, sick days, and holidays. A standard 24-hour SOC must be maintained by at least seven staff members. If not, procedures should be put in place for off-hours monitoring. This enables the staff to have a one-hour overlap for shift transfer and a floater to cover any holidays or time off when needed. This is discussed in more detail in the Staffing Schedule section below.

Finding the right skills and hiring staff is a difficult task at the current time because there are a limited number of security professionals in the market. The security staff within the SOC must have a solid background in many different aspects of computer technology usually focusing on networks, applications, and in some cases, reverse engineering. In addition, a good manager or director is required to ensure documentation, optimization, and reporting are maintained appropriately.

Typical roles within an SOC may include:

[4]www. Mcaffe.com

- Security Analyst
- Security Specialists
- Forensics or Threat Investigators
- Manager or Director

III.2. Staffing Schedule.

When setting up an SOC, ensuring you have appropriate coverage is critical. Some SOC operations will support 24/7 operations, and others will have limited remote support after certain hours. The following tables are a partial representation of the staffing hours for an eight-week period. Each SOC engineer is assigned per the shift schedule for the eight-week period. These engineers are identified by **A** which reflects the morning shift in the SOC and the afterhours shift Monday through Friday. The **B** represents the afternoon shift in the SOC and the pager shift over the weekends.

SOC Schedule Week

Staff	Level	1	2	3	4	5	6	7	8
Manager	M								
SOC Engineer	SE	A	A	A	A	A	A	A	A
SOC Engineer	SE	B	B	B	B	B	B	B	B
Time Slot	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday		
00:00-00:30	A	A	A	A	A	B	B		
…….	A	A	A	A	A	B	B		
06:00-06:30	A	A	A	A	A	[5]B	B		
06:30-07:00	A	A	A	A	A	B	B		
07:00-07:30	AB	AB	AB	AB	AB	B	B		
07:30-08:00	B	B	B	B	B	B	B		

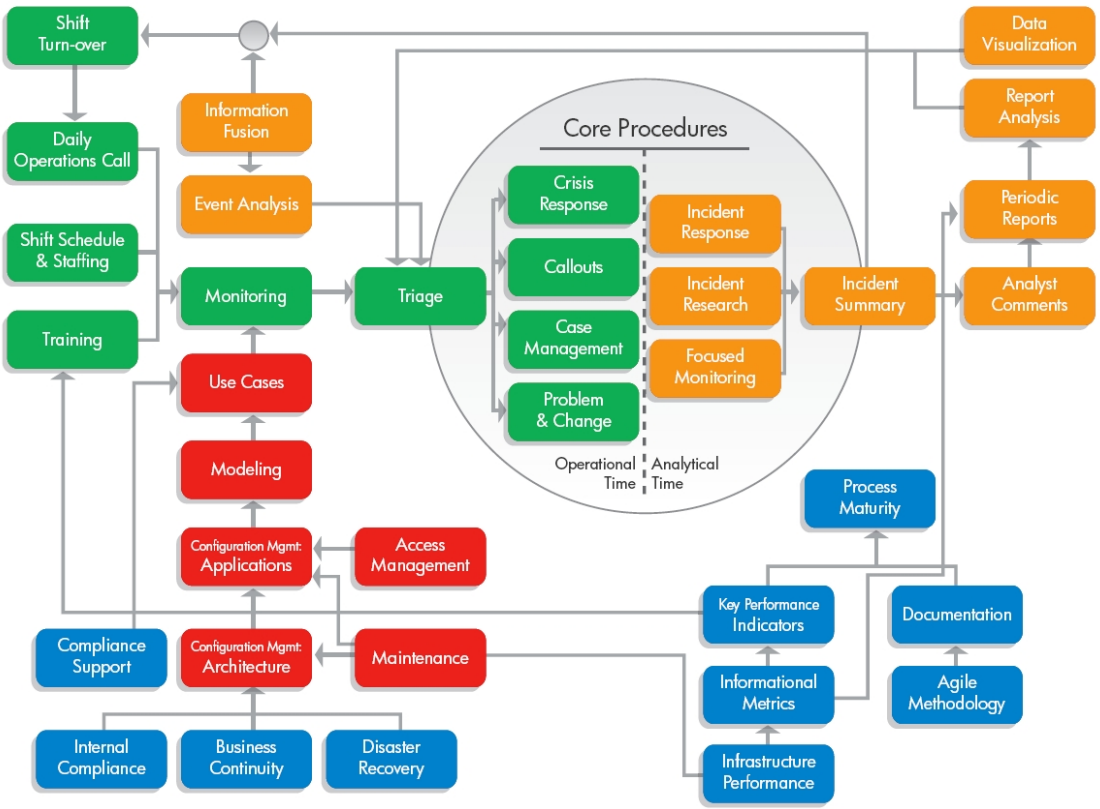
III.3. HOLYDAY COVERAGE.

One item typically overlooked is holiday coverage. In most cases, holidays should be treated as normal business days. There should be dedicated staff in the SOC for the given shift as described in the organization's staffing schedule. All responsibilities regarding standard shift schedules should also be in effect.

[5] www.oracle.com

IV. LOGS.

IV.1. Shift Logs, Incident Logs, and Turnover.



6

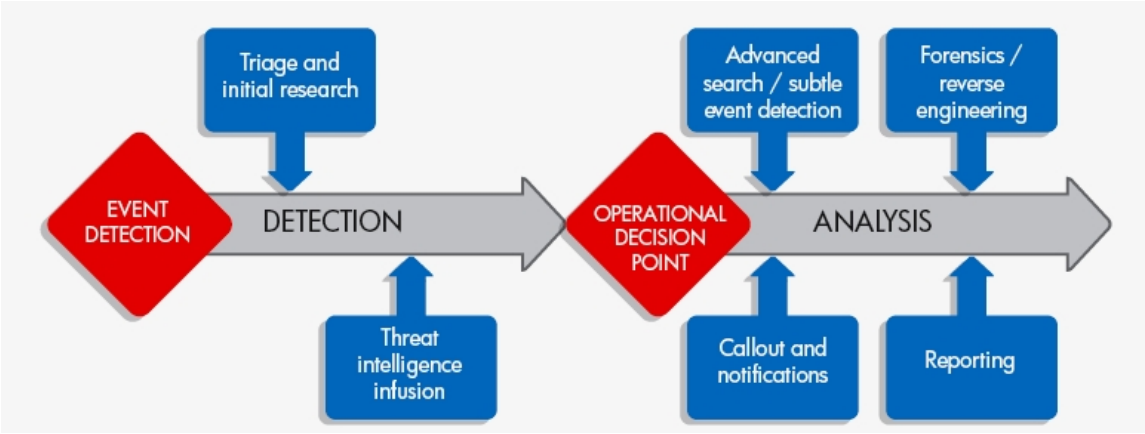
Shift logs must be maintained for audit and to ensure continuity of the SOC operations. SOC shift logs should be maintained daily for every shift. Shift logs can also be maintained in a database or GRC system and used regularly to help identify past issues and the resolution of those issues. Any significant event or incident should be recorded in the shift logs. This includes all high-priority incidents, incident records, escalation actions, and any procedural problem that has or could have a security impact. Some very specific shift log procedures that are typically overlooked are:

- Entries on the shift log are mandatory for each shift; a "blank" entry is not acceptable.
- If there is no activity or no open problems to turn over, put an entry in the log that says "No incidents to turn over".
- Shift log entries should use a defined format that includes the following:
  - Details of the event.
  - Impact of the threat to the organization or asset.
  - Description of the items found during the investigation while researching the event.

[6] www.oracle.com

- Recommendations for the next analyst that might be taking over the incident.

If possible, shift logs should be maintained in a secure role access controlled system such as a GRC. A typical example of a shift log is below.



[7]

Details: The SOC has detected traffic from <source IP / hostname> to <destination IPs> over <ports>. Information gathered would indicate the asset is infected with malware. Traffic activity is being reported by <device detecting traffic>.

Impact: Malware is performing a remote call back, possibly leaking data or expanding its presence in the network.

Description: <Detailed observations of the pattern and activity>

Recommendations: Find the source IP asset. Contain the device. If no signs of malware are found, determine the cause for the detected event and remediate. If signs of malware are found, perform the required antivirus updates and/or forensics on the machine. Remediate or clean the system prior to connecting it back on the network. In addition to shift logs, incident log entries should also be kept. Although incidents should be maintained in a ticketing system, daily log entries should be used to transfer incidents. This log should follow a defined format that includes the following information: Time stamp, staff initials, the incident record number, and a brief description of the incident or event. An example of a typical incident log entry is below.

Time	Incident Record #	Staff Name	Description of Event
07:30	No incidents to turn over	SOC Engineer name	N/A

[8]

[7] www.Mcaffe.com
[8] www.hp.com

IV.2. Event Management.

The core function and technology within an SOC are based on events from hundreds or even thousands of different systems. Essentially the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon. The management of events must include a list of instructions that apply on a 24x7 basis. This does not necessarily have to be the Incident Response Program Guide or Handbook. An event is any element that comes into the SOC and is monitored; while an incident on the other hand is an event that must be acted upon. As a part of event management, the SOC provides telephone and email assistance to its customers covering some of the following areas:

- Malware outbreak.
- Phishing attacks.
- Social Engineering calls.
- Access to the organization's security portal.
- Data Leak/Loss incidents.
- Customer account lockout.
- Customer inquiries.

Also defining the guidelines for the level-one SOC support is important. These may include:

- Open an incident ticket for any problems noticed and reported.
- Serve as the initial point of contact for customers on the organization's network.
- Maintain daily shift logs.
- Perform rudimentary testing and diagnosis.
- Validate that the incident is not a user error.
- Formally assign the incident to the SOC.

V. TRAINING.

No SOC analyst can be effective without appropriate training; luckily, there are very good options for building an effective training program. When crafting training plans, SOC managers should include both formal training on standard information security skills and on-the-job training (OJT) to maximize the analysts' effectiveness within the organization.

Formal training should include the SANS (System Administration and Network Security) "Intrusion Detection in Depth" training module and the GCIA (GIAC Certified Intrusion Analyst) certification. This is the industry standard in training analysts in the

fundamentals of TCP/IP, TCP/IP monitoring tools, and skills associated with advanced intrusion analysis. On-the-job training programs should provide an overview of important information security concepts, training on specific intrusion detection tools in use, analytical processes and procedures, and effective communication techniques. The SOC analyst will be required to effectively communicate and brief all levels of engineers and senior management during times of extreme stress, thus training in managing combative communication is invaluable. This training should also include the hierarchy of communication methods. Learning when to page, call, e-mail or assign a ticket is a critical skill. Additionally, it is important that any analyst learn to communicate in concise well-written papers and e-mails. SOC managers should create a program that has aspiring analysts writing analytical papers and then presenting their findings to their peers to hone written and verbal communication skills.

VI. Abbreviation.

Term	Complete form
SOC	Security Operations Center
IT	Information Technology
SIEM	Security Information & Event Management
AV	Anti-virus console
GRC	Governance, Risk Management and Compliance
SLA	Service Level Agreement
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
DLP	Data loss Prevention
IP	Internet Protocol
OJT	On-The-Job-Training
SANS	System Administration and Network Security
GCIA	GIAC Certified Intrusion Analyst
TCP	Transmission Control Protocol

CONCLUSIONS

Building and managing a security operations centre can improve an organization's ability to recognize and respond to malicious information security events. A SOC can also assist in ensuring organizations influence the full value of the often expensive investment in security technology and meet a plenty of regulatory compliance requirements. Approaching the challenge across the full scope of People, Process and Technology will ensure the SOC is up to the task of effectively and efficiently recognizing and responding to malicious events.

REFERENCES

1. Security Operation Centre Concepts & Implementation" by Renaud Bidou.
2. Fundamentals of Computer Security Technology – Edward G. Amoroso.
3. Analysis Techniques for Detecting Coordinated Attack and Probes – John Green, David Marchette, Stephen Northcutt, Bill Ralph.
4. Application-Integrated Data Collection for Security Monitoring – Magnus Almgren, Ulf Lindqvist – SRI International.
5. Oracle Optimized Data Centre http://www.oracle.com/us/corporate/features/optimized-data-center/index.html
6. Oracle Optimized Solutions http://www.oracle.com/us/solutions/oos/overview/index.html NIST, "Security Maturity Levels," 2012. [Online].
7. HP Company via (Meetings, Proposals, other documents).
8. Mcafee Company via (Meetings, Proposals, other documents).

ONLINE BANKING SECURITY

Author:
Lt. Alexandru PANEŞ

ABSTRACT

Online banking is the most popular method for electronic financial transactions[i] for people that value their time and also for those who want to skip conventional long waiting lines in the financial institutions regarded as a nuisance in today's "on the go" modern living environment. This study provides perspective for users and nonusers of online banking on aspects like basic definitions of what types are identifiable in the market and how it works basically, security threats you can aspect, mitigation and some examples on fraud prevention.

Keywords: e-banking, security threats, security measures, fraud prevention.

I. INTRODUCTION

I.1. What is online banking?

"Change is the process by which the future invades our lives"[ii]

Nothing can be truer when it comes to this fast changing world where the technological progress can be viewed as the shock of the future or as the blessing you were looking for. Increasingly more and more people go for any option that makes their life run more smoothly and affords them more convenience in handling day to day activities[iii]. Managing your bank account made easy through the use of the computer and the internet is one such activity. Known as internet or online banking, this has become a widespread and very popular way of handling banking duties. The concept of internet banking was formed back in the early 80's. Its actual use didn't come into play on a very widespread basis until the mid 90's when Presidential Savings Bank offered internet access to its banking services[iv]. Nowadays it is the exception to find a bank that does not offer online banking options to its customers. There are many banks, in fact, some existing only on the internet[v].

Use of internet banking can allow you to handle almost all your banking transactions online. You can access the account balances, past and present transactions, transfer funds from one account to another, pay bills, look up checks, reorder checks, stop payments, complete loan applications, and make contact through messaging with bank staff members. One of the most appealing parts of it all is being able to do these things 24 hours a day, seven days a week, and without leaving your home. You will also realize time savings, effort, gasoline and fees for parking when you chose to do your banking through the internet. You won't have to worry about getting to the bank before closing time.

Banks that today offer online banking services have firewalls and security features on their sites that will guarantee complete privacy and that account information is visible only to you. The process is the same with most banks, being rather simple and it requires only setting up access to the online account by either choosing or being assigned a username and password. Once you have logged in you will have access to your account information and will be able to see any transactions that have taken place as well as deposits, charges, and transactions that are in progress. This information can be printed off so that a written copy is available for records or in case proof is needed to verify something later on. When you are finished just log off properly, even if the banks have time triggered automated session log-off, so that your information is safe and can't be accessed by anyone else[vi].

I.2. Forms of internet banking

There are three kinds of Internet banking in the marketplace[vii]:

Informational: This is the basic level of Internet banking. Typically, the bank has marketing information about the bank's products and services on a stand-alone server. The informational systems typically have no path between the server and the bank's internal network. This level of Internet banking can be provided by the bank or outsourced. While the risk to a bank is relatively low, the server or Web site may be vulnerable to alteration. Appropriate controls therefore must be in place to prevent unauthorized alterations to the bank's server or Web site[viii].

Communicative: This type of Internet banking system allows some interaction between the bank's systems and the person. The interaction may be limited to e-mail, account inquiry, loan applications, or static file updates (name and address changes). Because these servers may have a path to the bank's internal networks, the risk is higher with this configuration than with informational systems. Appropriate controls need to be in place to prevent, monitor, and alert management of any unauthorized attempt to access the bank's

internal networks and computer systems. Virus controls also become much more critical in this environment[ix].

Transactional: This level of Internet banking allows persons to execute transactions. Since a path typically exists between the server and the bank's or outsourcer's internal network, this is the highest risk architecture and must have the strongest controls. Personal transactions can include accessing accounts, paying bills, transferring funds, etc[x].

I.3. How online banking works?

"In the 21st century there will be a lot of banking but there will be no banks"[xi]

E-Banking applications run on diverse platforms, operating systems and use different architectures. The product may support centralized (bank wide) operations or branch level automation. It may have a distributed, client server or three tier architecture based on a file system or a DBMS package. Moreover, the product may run on computer systems of various types ranging from PCs, open (Unix based) systems, to proprietary main frames. These products allow different levels of access to the persons and different range of facilities.

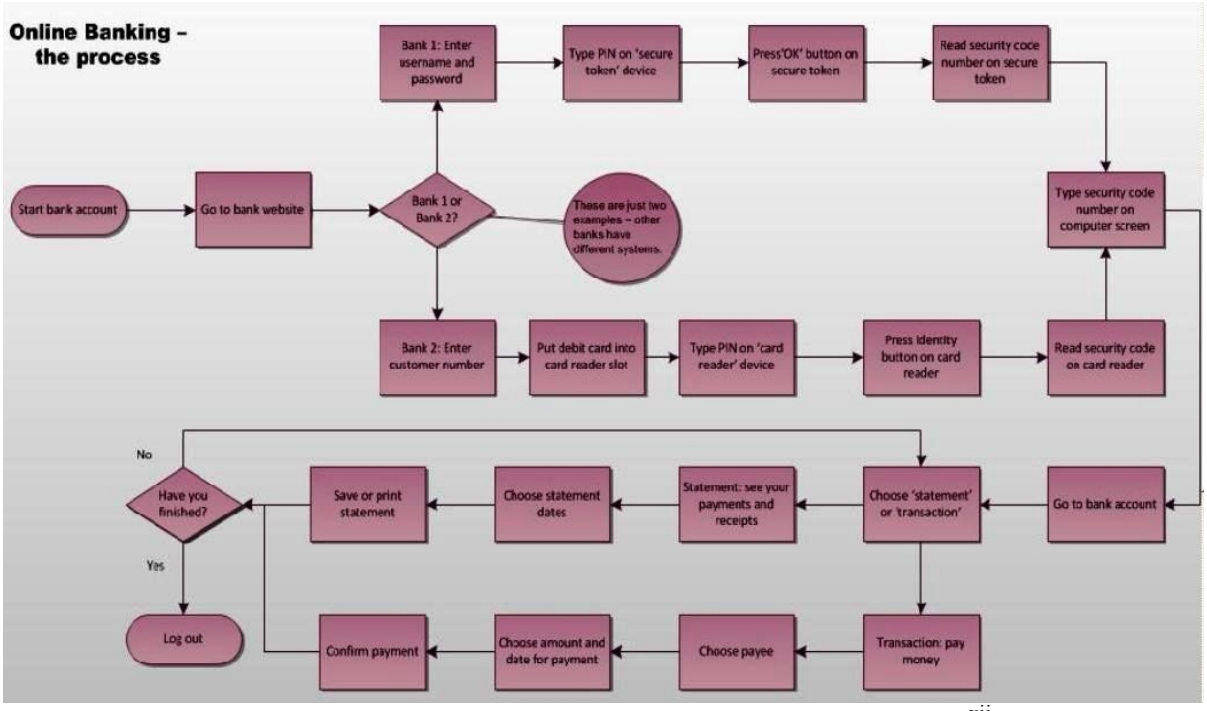


Diagram of online banking system – an example - [xii]

Contemporary online banking systems make use of varying forms of user authentication[xiii]:

- In most cases authentication is through a combination of potentially strong passwords and users ID's;

- Most of these systems ensure secure connections between the clients and the servers over SSL and many of them also have server side digital certificates;
- Some online banking systems in addition to the above features impose client side digital signatures and certificates;
- In other cases additionally there is the imposition of one time password or regular password modification policies, to users;
- Some systems also limit the number of login attempts as a security measure.

Despite all this technological wide variety it's still easy to access your online bank account with a basic computer that has a web browser installed on it. In order to use your electronic transfers and ditch out cash or cheques you just have to go and logon to your e-banking website using one of the authentication methods agreed upon with your bank. But, as with everything online, and everything relating to money, several security vulnerabilities still persist; partially due to design flaws and implementation bugs and in many cases due to the inherent weaknesses generally associated with the use of user ID's and passwords for authentication into systems. Black hat software experts can exploit these vulnerabilities in order to hack into online banking systems.[xiv]

II. SECURITY

II.1. Threats

"There is no security on this Earth. There is only opportunity"[xv]

It's a well known fact that information security is concerned with the protection of three characteristics of information: confidentiality, integrity, and availability employing the use of technical solutions and managerial actions. All the commercial operating systems up today are known to have vulnerabilities and weaknesses. These vulnerabilities in turn create opportunities for cyber threats to the information stored and used on these systems. Security threats can be classified like in the table below and can result in disclosure of informations, modifications, destructions, or denial of use.

The table below lists some threats to information security[xvi]:

		Accidental	Intentional
Internal	Human	• Acts by employees • Accidental entry bad data • Accidental destruction of data by employees • Administrative procedures • Weak/ineffective physical	• Acts by employees • Intentionally destroy data by employee • Intentional entry of bad data by employees • Unauthorized access by

		control	employees
	Non-human	• Mechanical and electrical • Program problems	• Mechanical and electrical • Program problems
External	Human	• Competitors • Media	• Hackers • Denial of Service Attacks • Social Engineering
	Non-human	• Fire • Earth • Wind • Water	• Computer Virus • Worms • Trojan • Spyware

There are three areas when it comes to internal threats: the application development department, the infrastructure, and the data center. Even thou there is also the risk from employees you can largely assume it's non-intentional. From the application development can arise threats based on logical errors from developing and programming. The application that is not programmed correctly can cause vulnerabilities and weaknesses in the security systems thus allowing for unauthorized individuals to access the private information. A programmer could also intentionally, by the use of a back-door inserted in the code, access data for personal gain or malicious purposes. The e-banking infrastructure possesses significant security risks by determining access level and privileges granted to employees. Granting access to information that is unnecessary to an employee's job functions increases the probably of a user compromising the data either intentionally or unintentionally. Data centers have the threat for the security of information because users enter, delete, and maintain important company data.

These threats include both negligence and deliberate acts by the users that encompass behaviors such as[xvii]:

- A lack of security common sense;
- Not applying security procedures;
- Taking inappropriate risks;
- Deliberate acts of negligence;
- Deliberate attacks.

These issues are mitigated by security awareness and personnel training. Being aware of security policies and procedures does not always result in employees following them. You can have results encompassed between positive cooperation and acceptance of the policies and procedures established at one end and resistance and repulsiveness at the other. Poor or unacceptable behavior by its users is one of the basis for security incidents and the only way to prevent this is by frequently make use of security audits.

The external threats make up for a significant challenge. These include from natural disasters (even thou it may look minimal you do have to put in place procedures to recover

any lost data by employing measures like backup and storage) to the more common viruses, worms, trojans, denial of service attacks and hackers. Leak of information is a risk that can generate bad publicity generated by the media. The threats of hackers and computer viruses are intentional acts to compromise the security of information systems in malicious ways. In order to mitigate this you have to identify possible threats by doing a threat analysis and put in place or develop countermeasures against these threats. Countermeasures are functions or features that reduce or eliminate vulnerabilities in the system.

II.2. Security measures

"A mechanism of some kind stands between us and almost every act of our lives"[xviii]

A big part of the threats that are now present can be either deterred or just minimized by use of various procedures. An example would be the threat of user errors that can easily be minimized by use of validating procedures on the data entry and more training for information users. There are threats that occur for malicious purposes. In order for this to happen there has to be first a motivation and second a capability for the hacker to carry this threat. The motivation can result from own personal gain, political or religious reasons, curiosity, revenge, etc. Even if motivation is present it must be accompanied by the capability to perform the act. Capabilities that enable a threat to be accomplished are access to facilities, software, technology, personality and education. These kinds of threats can be inhibited by having in place more security, thus requiring higher technical and educational capabilities to perform malicious attacks, or by operating in a harsh legal environment that would take the consequences very seriously when it comes to the improper use or harming the privately owned data. Another aspect that has to be taken under consideration is the amplification factor. This factor can result from peer pressure, fame, easy access to information, and increased skill and educational levels which result in higher capabilities.

The security threats can be operationalized in five security aspects[xix]:

Security Policy – The policies are a set of rules that users must acknowledge and use as a guide when using a system governed by a set of policies. These policies are based on activities that are acceptable and those that are not. The descriptive aspect of the policies is set at making employees aware of the policies and procedures while the prescriptive aspect requires employees to internalize and follow the security guidelines. These policies are put into places like the host security, network security, and organizational security. They set the

rules that must be followed for host and network security. Users must also be trained and made aware of the policies and procedures.

Host Security – This aspect includes the authentication of users, effective control and access to system resources, securely storing data, and audit trial of the information being access. Authentication procedures are divided in two parts: identification and authentication of users. Authentication processes encompass knowledge based systems, token-based systems, and systems based on biometrics. The typical identification and authentication is based on username and password in order to gain access to the system. The security is achieved by not being able to randomly access the system. Nevertheless, threats exist and can be exploited using a reusable single user name and password by[xx]:

- Guessing;
- Social engineering;
- Eavesdropping;
- Capture and replay;
- Penetration;
- Brute force;
- Point of entry;
- Revealing secret.

By the use of a dictionary or a simple exhaustive search of short passwords you can break a short password. A general solution for all of the above includes having a password policy where users must create strong passwords and change them often. This way you will achieve a decrease in the percentage of the successful employment of guessing, capture and replay, and brute force attacks. It must be taken under consideration the problem of poor security habits by user not being able to remember their password and having to write it down on a piece of paper which can easily be obtained by others.

Here comes into place the Hash Visualization method, specially designed for users to overcome the difficulties of remembering passwords by having various pictures upon logging among which you have to identify a special selection. The idea is that users can remember visual images much easier than strong passwords, avoiding the need for users to write them down.

Network Security – It's a must to be highly integrated with aspects like security policies that can take preventative measures for security on networks, host security based on authentication of users who access the networks, and legal security. Network security includes passwords, authentication, firewalls and proxy servers among other things.

In order to create a secured network there are six items that need to be checked[xxi]:

- Change passwords quarterly;
- Download patches and updates;
- Hire a hacker;
- Monthly risk assessments;
- Communicate and review data security policy;
- Keep the network virus free.

Using strong passwords that change regularly you will obtain higher level of security on the network but at the risk of the user's inability to remember them and thus resulting in possible password leaks because of the improper handling. Patches and updates for all your software will increase security by ensuring that the latest security threats and vulnerabilities are accounted for as they are discovered. A hacker employed as part of the network security team can prove if your system is hack proof by using techniques to infiltrate. Firewalls are not sufficient on their own so tools such as intrusion detection software can help prevent access from unauthorized individuals and increase security. Antivirus software up to date can prevent the spreading of viruses across the network. All this will decrease the likelihood of falling victim to security threats but it will not be „bullet-proof".

Organizational Security – Users are the biggest threats to security because of social engineering tactics. This can be mitigated by educating employees about vulnerabilities and making them aware of proper procedures. Security awareness training is identified as the weakest link in information security.

There are five dimensions of security awareness[xxii]:

- Organizational;
- General public;
- Socio-political;
- Computer ethical;
- Institutional education.

The organizational dimension consists of various groups of people within that security awareness training should target. The general public dimension entails all users outside of the IT department. The social-political dimension is the security awareness training that is required by law. The computer ethical dimension is the prevention of activities that are interpreted as abuse. The institutional dimension describes what information should be included in a security awareness program. User awareness training is a people issue rather than a technical issue where training should be formalized. Without proper knowledge of procedures and awareness of security vulnerabilities, users will not be able to protect against potential threats[xxiii].

Legal Security – Is the legal actions that are in place within the possibility of prosecution against an attacker in order deter threats. This legal actions decrease the motivation to violate the security procedures. Legal security should be embedded within the security policy that is implemented within. All agents should be made aware of security policies and consequences. Each of the five aspects of security provides different means of securing information and they must all be addressed and used together to decrease the vulnerabilities of security threats.

The table below lists some security measures that have been identified in association with the different categories of security[xxiv]:

		Accidental	Intentional
Internal	Human	• Policies and Procedures • Security Awareness Training • Employee education • Ethics training	• Policies and Procedures • Audit procedures strengthened • Monitor computer usage • Reporting violations encouraged • Ethics training
	Non-human	• Update Software	• Company provided software only
External	Human	• Security Awareness Training • No outside connections	• Use of passwords • Encryption • Authentication (images, text, etc.) • Security questions • Auto terminal/account logoff • Install and configure a Firewall
	Non-human	• Backup procedures on schedules • Physical Security Measures • Backup Power Supply	• Authentication (images, text, etc.) • Use of virus scanning software • Protect vs. viruses/worms/trojans

The majority of technical solutions for information security are directed at external human threats. While internal threats have proved to be the biggest threat for security, external threats are the most recognized by the general population. It is important to protect your information from all viable threats. Nevertheless, you should also take in consideration how increased security could inhibit the users from taking proper measures to secure them.

III. EXAMPLES ON FRAUD PREVENTION

"We are stuck with technology when what we really want is just stuff that works"[xxv]

Although e-banking has not been a new presence in the last couple of years, almost no cases of fraud have been reported until recently. Starting with the year 2004, the reports on fraud cases went on up, skyrocketing, making the banks to look up for ways to protect their banking data channel, mainly because of the increasing risk of cyber-threats, materialized in the form malware, fraud and unauthorized access to accounts.

Evolving in a fast pace, quite troublesome, hacking has made the cyberspace a dangerous environment. Today, the perpetrators are more sophisticated and likely professionals; the conventional profile of a fraudster, that of a young hacker, just sitting at his laptop and altering the integrity of company data just for the fun of it, it's obsolete. The fraud in the online environment has becomed more formal, done on a larger scale and also it's nowadays a highly lucrative criminal enterprise with multiple parties working together to promote fraud against people. It's becoming the industry-wide problem.

There is not just one type of fraudster. They come in at least three flavours[xxvi]:

- *Joy riders* (people with a cause) – These are the wiki-leakers and other individual hackers, anonymous and otherwise, about whom one typically reads in the news. They generally target large, public companies and it is not financial information they're after but rather it's embarrassing corporate dirty laundry.
- *IP seekers* – Their goal is to confiscate information about a business, its dealings, its client roster, etc. They may sell this information to competitors or they may defraud the company's clients, or even the clients' clients, with ersatz emails and the like of those.
- Hunters of easy prey – a large and growing contingent, these fraudsters target banks' clients: small and midsize companies that are less likely to have and spend capital on building a robust IT security infrastructure. Their motivation is pure financial gain.

The patience is becoming the characteristic that is innate to the above mentioned fraudsters. Nowadays they don't hit indiscriminately but rather diligent, biding their time, they are behind massive research into the companies they target. It has come now to outsourcing to other developers in order to write malware for them.

III.1. Common e-Banking fraud schemes

There are two steps involved in most e- banking fraud schemes. In the first place, the perpetrator obtains the logon name and password needed to access the person's account. Then, in the second step, the perpetrator makes use of this information in order to make e-money transfers in other accounts from where he is legally able to withdraw them.

For the first step, perpetrators have employed different schemes in the past[xxvii]:

- The "*over the shoulder looking*" scheme occurs when a person performs financial transactions while being observed by a perpetrator. A fair number of cases have been reported where account access data was obtained by the perpetrator just by observing people at a public Internet access point.
- The "*phishing*" scheme involves using fake emails and/or fake websites. The word "phishing" derives from combining the words "password" and "fishing". Perpetrators send emails that appear to be from the person's bank that direct them to a fake website. This website impersonates the bank's website and prompts them for their account access data. Over the past years, most banks have executed customer education programs, thereby reducing the effectiveness of this scheme. It will, however, take awhile before all of them are smart enough to extinct phishing.
- The "*Trojan horse*" scheme is based on embedding a computer virus type software program onto the person's PC. Trojans often tie themselves into the keyboard driver and record keystrokes. Once a Trojan detects that the person opens an online banking website, it captures login name and password, and sends it to the perpetrator.

In 2003, phishing was the dominant fraud scheme. In 2004, banks experienced a sharp rise in Trojan fraud scheme attacks. In 2012 perpetrators outwitted the online banking identity security systems by a method called "*Man in the Browser*" attack[xxviii]. This type of attack is relatively easy to do in a public Wi-Fi hotspot environment. It could also easily happen on a home Wi-Fi network, if that Wi-Fi network isn't properly configured and allows a hacker to connect to that home network. An educated end-user and sound security practices by firms can protect the valuable data[xxix].

III.2. One time passwords

Some banks use "one time passwords", or OTP, to improve security. When a person activates his account for online banking, he will receive by regular mail from the bank a list of

OTP’s. Every time the person undertakes on a transaction he uses one OTP for verification. After it has been used the OTP becomes invalid. When the person runs out of OTP’s, he will be sent a new list, again by regular mail from the bank.

Although this approach effectively prevents "over the shoulder looking", it fails in preventing other fraud schemes. OTP’s are requested also in phishing emails and someone naive enough to give out his logon name and password will likely also provide OTP’s.

Another way is by using trojans and simply capture the OTP once entered. These trojans either falsify the person's input in the browser software, usually by adding an invisible character, or they can just crash the browser software. This will cause the transaction to be intercepted and at the same time the OTP provided to still be valid as it didn’t had time to expire. This still valid OTP can be used by the perpetrator to execute a fraudulent transaction.

III.2. a. Transaction specific

Both paper OTP lists and hardware tokens have a shortcoming fault because of the fact that each OTP is not transaction specific. In order to verify either a genuine or a fraudulent transaction you can use the same OTP. Overcoming this flaw can be done by the use of a "key generator" device, similar in looks to a pocket calculator, which generates an OTP based on primary transaction parameters, like the source account, target account, transaction amount, and a PIN. The key generator creates a transaction specific OTP only based on given parameters.

The transaction parameters and the generated OTP that are now entered in the e-banking application are verified by the bank's server, by performing the same calculations as the key generator and comparing both calculated values. If a perpetrator captures such an OTP, he cannot use it for a fraudulent transaction, since this OTP can only be used to verify a transaction with the same parameters as entered on the key generator. Because the key generator is a separate hardware device with no connection to the Internet, it is immune to getting attacked by malicious software.

Although the key generators have disadvantages like the high cost of the terminals, the requirement to be present in physical form, they still are, from the point of view of the security, a high efficiency measure when it comes to fraud prevention in the e-banking environment, capable of preventing fraud schemes that are known in this moment.

III.2. b. SMS

Another method to send OTP's to the person and thus avoiding some of the disadvantages of using key generators is by employ of SMS technology. In this approach the person first sends the complete transaction to the bank's server that generates a random number as OTP and resends it to the person's mobile phone as SMS. This transaction specific OTP is now entered into the online banking application and thus sent to the bank's server that verifies the transaction by comparing the transmitted OTP with the generated one.

This OTP is of no use to a perpetrator because the OTP transmitted by SMS is an effective fraud prevention measure because it can only be used to verify the transaction that is already received by the bank's server and cannot be altered anymore from the outside. This measure should be, in theory just as good as a key generator. The reality tells of a different story, one in which the weak point to this security measure is the mobile phone identification and thus in order to be effective as a fraud prevention method you need to have a thorough identity checking in case of any change of mobile phone number is performed.

Another disadvantage of this approach is that banks need to tie in their infrastructure with the infrastructure of a wireless operator. Wireless operators all over the world are investigating ways to leverage their existing infrastructure into new sources of profit. Most operators hence look into providing financial transaction services of various kinds. Banks hence may soon find themselves in a situation, where wireless operators offer their persons financial transactions using just the mobile phone and nothing else. The bank's offering would involve using first an Internet browser, than wait for an SMS, read it, go back to the Internet browser, type in the OTP and erase the SMS. For a person, the bank's offering appeals to be a lot more complex than the wireless operator's offering[xxx].

III.3. Hardware tokens

"Hardware tokens", featuring a crypto processor and a display, are the high-tech alternative to paper OTP lists, because they can display a new OTP, valid for a limited period of time, every 60 seconds. Because of this aspect they provide significant protection against "over the shoulder looking" and phishing schemes but when it comes to trojans it's a different matter because, even thou the OTP is only valid for a short time, and by this way reducing the time available for the perpetrator to exploit the data obtained by the implanted Trojan, the automated scripts employed nowadays on servers are able to perform fraudulent transactions

once the access data is received from the Trojan in the time limit provided by the expiration time for the OTP.

Additionally, there are Trojans that can be on play on the local computers and thus performing much faster, close to no delay, when it comes to fraudulent transactions. This renders the hardware token to fail when it comes to dealing with Trojan fraud schemes.

III.4. Smart cards and USB tokens[xxxi]

A different approach to authentication is based on smart cards that can contain crypto processors without a display, electrically connected to the person's PC using a card reader device or USB tokens, which are very similar to the cards but don't require a dedicated card reader as they are inserted in a port in the PC.

The process is based on an exchange of crypto keys between the bank's server and the owner of the accounts, thus enabling the bank to be reasonably sure the online transaction that originated from the genuine person is authorizable.

Even thou in the past some forms of smart cards have been flawed in security design and thus hack prone, the new generation will for sure provide a high level of fraud protection for the next years to come, making this a possible solution even if the inherent disadvantage, that of its need to be installed and configured as a specific hardware drive and electrically connected to the person's PC, will never be resolved.

III.5. Transaction monitoring

The adaptation of fraud prevention systems used with credit and debit card processing provides for a completely different approach to secure online banking. Since many years, fraud is a known phenomenon, when it comes to payment card processing and the technical security measures that have been put in place in payment cards as magnetic stripes or chips only provided a temporary relief from fraud losses.

Along this road, the deployment of transaction monitoring software proved to be the only measure able to limit fraud losses permanently, becoming nowadays the de-facto standard for fraud prevention with payment card processing worldwide.

Transaction monitoring occurs in the bank's data centre and for each transaction; the transaction monitoring software scrutinizes the current transaction's parameters, and compares it with the previous transaction of both the person and the counterparty of the transaction histories. By comparing the current transaction pattern to stored known fraud patterns, the

software can flag suspicious transactions "on the fly". Such transactions are then referred to a call centre for manual verification[xxxii].

The advantages to this method are multiple especially when you compare it to the others that were addressed before in this paper. In the case of the transaction monitoring approach there is no new device to be used by the person, no dependency on mobile phones and no person support problem with hardware driver installation, no one-time costs per person for a card reader or an USB token, and no per-transaction cost for sending SMS.

III.6. Comparison

But there are disadvantages to the transaction monitoring method, like the emergence of a new fraud pattern that is not stored in the transaction monitoring software or when by accident the current genuine transaction patterns resemble a known fraud pattern so much that the transaction monitoring system refers the genuine transaction to the call centre.

The first problem exists with any fraud prevention measure. Once perpetrators find a way to circumvent the measure, the door to fraud is open. The question becomes what can be done in this case. If the fraud prevention measure involves devices that are distributed to the persons, fixing the security problem becomes difficult[xxxiii]. Transaction monitoring provides a significant advantage in this case because it is centralized. By adding the new fraud pattern to the fraud detection logic in the bank's data centre, the entire system becomes instantly "immunized"[xxxiv].

The second problem also occurs with any fraud prevention measure. Any measure will impose a certain person disturbance. Smart cards and USB tokens may cause trouble when their hardware driver becomes incompatible with any change of the person's PC. And like hardware tokens and key generators, all extra electronic devices have certain likelihood to fail or get lost. OTP’s send by SMS may get lost or delayed, in particular with International roaming. Transaction monitoring software will inevitable generate a certain rate of false alarms. Banks must carefully determine which level of person disturbance they consider acceptable for the security level needed[xxxv].

III.7. Intelligent software

One of the common software products used for transaction monitoring and fraud prevention with card based payment systems is RiskShield[xxxvi]. The company, INFORM GMBH from Germany, has recently introduced a special version of RiskShield for online

banking. This product is currently in rollout with online banking operations of all major European banks[xxxvii].

RiskShield has countermeasures against all known online banking fraud patterns and has been designed to uses transaction data from other payment channels to refine its detection of certain fraud patterns, if such data is available and also merge all financial sequences into "transaction fingerprints" used to detect specific fraud patterns.

Other Fraud & Deviation Detection software you can find available on the market includes[xxxviii]:

- Alaric Systems "Fractals" card fraud detection and prevention systems using proprietary inference techniques based on Bayesian methods.
- Analyst's Notebook 6, from i2 Inc., conducts sophisticated link analysis, timeline analysis and data visualization for complex investigations.
- Aptelisense Compliance Automation Server advanced real-time fraud prevention and data compliance that requires zero change to applications or systems.
- ArcSight Antifraud Accelerator Solution.
- Austin Logistics FraudAlert, solutions for collections, marketing, and risk management for consumer credit and Internet transactions.
- Business Data Miners builds highly effective data-driven models and rules to mitigate credit risk and fraud losses; saved its clients over $100 million in the past 2 years.
- Centrifuge, offers analysts and investigators an integrated suite of capabilities that can help them rapidly understand and glean insight from new data sources.
- CPA Detective offers a sophisticated real-time fraud detection solution that evaluates the digital forensics of each visitor and returns the probability of fraud before buying, selling, or fulfilling on a lead or sale.
- CSC Fraud Analytics Suite, combines predictive data modeling technology, identity search technologies, fraud indicator business rules, company claims information and industry data sources to help flag suspicious claims as early as the first notice of loss.
- Dinkla Artificial Intelligence and Fraud Detection pages
- Equifax Fraudscan detects, validates, and verifies potentially fraudulent information automatically and simultaneously at the time of application.
- Equivax Gemini Verify Score Equifax's credit data with HNC's fraud-control program to offer an identity authentication score.

- FICO, (formerly Fair, Isaac), offering Falcon and other tools for risk management systems, including credit card fraud detection.
- Fraud Wiki, Fraud Detection and Prevention Wiki.
- FraudBreaker, web based fraud detection software that captures your transaction data and performs real time checks on a wide range of risk factors.
- Friss Fraud Solutions, the leader for fraud and risk detection and settlement in Netherlands; Delivered with best practice fraud indicators en standard interfaces.
- IDES Technologies, a global provider of fraud detection products to solutions providers and transaction processors, mainly for the financial services market.
- InferX, remote data mining solutions for law enforcement, intrusion detection, and related applications.
- Infoglide, developers of patented Similarity Search Engine for finding fraud in the insurance industry.
- International Compliance Association supports and educates compliance professionals in the fight against terrorist financing, corruption, money laundering and financial crime.
- The Lavastorm Analytics Engine (LAE) is designed to augment your current Fraud Management Solution, giving you the ability to keep pace with the rapidly changing fraud environment, while minimizing your costs and delivering rapid ROI.
- LEADMiner, a refinement of Numerically Integrated Profiling System (NIPS), developed for US government fraud detection and trade analysis.
- Magnify PATTERN: Detect™ for uncovering fraud and anomalies, such as fraudulent credit card transactions or network intrusions.
- Nestor, offering risk management products, including credit card fraud detection
- Neural Technologies Decider™, a suite of solutions for the finance industry for advanced modeling and scorecard development for detecting bad debt and application fraud
- NORA™ (Non-Obvious Relationship Awareness™), identifies potentially alarming non-obvious relationships among and between individuals and companies
- Oscar Kilo's Detect provides both a rule-based and statistical risk-engine, with applications to Credit Card fraud detection, accounting fraud, and more.

- Plug&Score, scorecard development software that can be used with any phase in the loan cycle from loan origination to fraud detection and prevention
- PredPol provides targeted, real-time crime prediction designed for and successfully tested by officers in the field.
- RootStream Detect, accounting errors and fraud detection software to make internal audits and assessments in accounting databases.
- SAS® Security Intelligence, an enterprise approach to fraud, compliance and security issues
- Searchspace, offers iTM™ - intelligent Transaction Monitor for fraud detection and more.
- Statsoft Solutions for Fraud Detection, focus on medical insurance fraud, Medicare fraud.
- Svivot SN-Sphere™, for creating effective intelligence related to networks (associations of people and organizations working together in a particular context).
- The Modelling Agency, offers PiCard(SM) Intelligent Procurement Card Monitoring System designed to actively detect misuse, target auditing team effort, reduce risk when moving from a purchase order System to credit cards, promote higher purchase card volume sooner, and forecast usage trends.
- StatConsulting, fraud detection based on customer behavior modeling using latest data mining methods together with traditional statistics.
- Xanalys, offering investigative solutions for fraud detection, law enforcement, intelligence, insurance, and more.
- Xtract Fraud Detector uses adaptive neural nets to analyze customer behavior and detect insurance claims fraud, payment card fraud, and more.
- Wizrule and WizWhy find unexpected rules in data and other applications for fraud detection.

IV. CONCLUSIONS

"Any sufficiently advanced technology is indistinguishable from magic"[xxxix]

The facilities deriving from e-banking applications give their users the flexibility of doing bank related transactions anytime, when that best suits them and in the process save time, but all this is done within a cyber-domain that will always present various security threats and that will always be exposed to them, even thou banks will employ the use of

protocols such as SSL and TLS and most of them hire security experts to conduct vulnerability assessments and find design flaws in their banking application and websites in order to find those flaws that prevent secure usage of the applications.

No matter what or how they do it, even the best designed e-banking sites or applications have flaws that can cause severe security breaches. Along with this, the overhaul security polices of the banks, until these days still don't have a standard format and those policies, are in some cases inadequate and by doing so they are leading to many security risks.

The safeguards and practices implemented by the banks, designed to assure their security posture in the cyber-warfare don't depend solely on them self, but also on the awareness of the users using the banking channel and the quality of end-user terminals because the hackers always choose the easiest way to attack. The easiest way seems to be attacking the users, so awareness and usability of users is also equally important to make online banking more secure. The security guarantee that is given by banks for users transactions is possible if both banks and users together give flawless security posture to online banking by removing all the given security flaws.

V. ENDNOTES & REFERENCES

"Computers are useless. They can only give you answers"[xl]

---

[i] Special Euro barometer 390, *Cyber Security Report,* , Brussels, 2012;

[ii] Toffler A. *Future Shock*, Ed. Bantam Books, New York, 1970;

[iii] Special Euro barometer 390, *Opcit;*

[iv] Presidential Bank, 10 July 2010, http://www.presidential.com/pk_marketspace.htm, 29 January 2014;

[v] Paras, H.K., 2014, http://www.hkparas.com/, 29 January 2014;

[vi] Wikipedia, 29 January 2014, http://en.wikipedia.org/wiki/Online_banking, 29 January 2014;

[vii] Internet Banking Comptroller's Handbook, October 1999 http://www.occ.gov/ 29 January 2014;

[viii] Internet Banking Comptroller's Handbook *Opcit*;

[ix] Internet Banking Comptroller's Handbook *Opcit*;

[x] Internet Banking Comptroller's Handbook *Opcit*;

[xi] *Apud* Bill Gates;

[xii] British Council, October 2012, http://esol.britishcouncil.org/internet-safety/internet-safety-online-banking, 29 January 2014;

[xiii] Ane Divine Jinor, *Pro-active Architecture and Implementation of a Secure Online Banking System that Uses Fingerprint Data as Part of Client Side Digital Signatures,* 2011;

[xiv] Ane Divine Jinor *Opcit*;

[xv] *Apud* General Douglas MacArthur;

[xvi]Aaron M. French *When Security Becomes Too Sophisticated for the User to Access Their Information* Journal of Internet Banking and Commerce vol. 17, no.2, 2012;

[xvii] Leach, Jason, *Improving User Security Behaviour. Computers and Security,* 2003, *Apud* Aaron M. French, *opcit*;

[xviii] *Apud* Sarah Patton Boyle;

[xix] Oppliger, Richard, *Security Technologies for the World Wide Web*, 2003, Apud Aaron M. French, *opcit*;

[xx] Feghhi, Jhon & co, *Digital Certificates: Applied Internet Security*, 1999 Apud Aaron M. French, *opcit*;

[xxi] Newhouse, Kevin, *Six Security Resolutions,* Credit Union Magazine, 2007 Apud Aaron M. French, *opcit*;

[xxii] Siponen, Martin *Five Dimensions of Information Security Awareness,* Computers and Society, 2001 *Apud* Aaron M. French *opcit*;

[xxiii] Aaron M. French *Opcit*;

[xxiv] Aaron M. French *Opcit*;

[xxv] *Apud* Douglas Adams;

[xxvi] SunTrust, 2012, https://www.suntrust.com, 29 January 2014;

[xxvii]INFORM, 2013, http://internetbankingfraud.com/, 29 January 2014

[xxviii] BBC News, 10 February 2012, http://www.bbc.co.uk/news/technology-16812064, 29 January 2014;

[xxix]Hoffman, Daniel, 13 February 2006, https://www.ethicalhacker.net/columns/hoffman/hacking-online-banking-and-credit-card-transactions-and-how-to-prevent-it, 29 January 2014;

[xxx] INFORM *Opcit*;

[xxxi] STORK.2 project aims at providing a high tech "good for all" e-ID solution to this (more info on https://www.eid-stork2.eu/);

[xxxii] INFORM *Opcit*;

[xxxiii] Hardekopf, Bill, 24 January 2014, http://www.forbes.com/sites/moneybuilder/2014/01/24/this-week-in-credit-card-news-how-thieves-hacked-target-danger-of-using-a-debit-card/ , 29 January 2014;

[xxxiv] INFORM *Opcit*;

[xxxv] INFORM *Opcit*;

[xxxvi]Risk Shield, http://www.inform-software.com, 29 January 2014;

[xxxvii]Market wired, 11 December 2013, http://finance.yahoo.com/news/sns-reaal-goes-live-riskshield-180000539.html, 29 January 2014;

[xxxviii] KD Nuggets January 2014, http://www.kdnuggets.com/solutions/fraud-detection.html, 29 January 2014;

[xxxix] *Apud* Arthur C. Clarke;

[xl] *Apud* Pablo Picasso – author's comment.

THE EU APPROACH OF CRITICAL INFRASTRUCTURE PROTECTION

Author:
Maj. Marius Cezar **TOMA**

INTRODUCTION

In order to understand the critical infrastructures protection capabilities it is necessary to reveal the EU approach, based on the practical implementation of activities under the prevention, preparedness and response work streams. Identifying, understanding and analyzing the evolution of the critical infrastructure protection framework are important in the context of the unprecedented development of these at national and regional level.

This research provides a stocktaking of the current and proposes EU programs regarding the critical infrastructure protection in order to underline the gaps related to the legal and implementation requests, to establish a framework for risk assessment, to design the national measures for protection and to increase the resilience of European critical infrastructure.

I. THE EU INITIATIVES AND THE LEGAL FRAMEWORK

Following the attacks in Madrid in March 2004, the European Union (EU) has decided to increase the involvement of civil society in measures designed to improve its protection. Therefore on June 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In response, on 20 October 2004, the Commission adopted a **Communication on critical infrastructure protection in the fight against terrorism** which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

The Council **conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks"** adopted by Council in December 2004 endorsed the intention of the

Commission to propose an European Programme for Critical Infrastructure Protection **(EPCIP)** and agreed to the setting up by the Commission of a Critical Infrastructure Warning Information Network **(CIWIN)**.

On 17 November 2005 the Commission adopted a **Green Paper on a European programme for critical infrastructure protection** which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network. The responses received to the Green Paper emphasized the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The importance of the key principles of subsidiarity, proportionality and complementarity, as well as of stakeholder dialogue was emphasised.

In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a **European programme for critical infrastructure protection ('EPCIP')** and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, man-made, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority.

In April 2007 the Council adopted **conclusions on the EPCIP** in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures ('ECIs') and the assessment of the need to improve their protection.

On 8 December 2008, the European Council adopted the **Directive 2008/114/EC** on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. This Directive constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, *inter alia*, the information and communication technology ('ICT') sector.

The general objective of EPCIP is to improve the protection of critical infrastructures in the EU. This objective will be achieved by the creation of an EU framework concerning the protection of critical infrastructures.

On 28 August 2013, the European Comission adopted a ***staff working document*** SWD(2013) 318 **on a new approach** to the European Programme for Critical Infrastructure Protection - **Making European Critical Infrastructures more secure.**

II. THE EU CIP CONCEPTS/DEFINITIONS

2.1 Principles

The following key principles guide the implementation of the **European programme for critical infrastructure protection**:

✓ **Subsidiarity** – The Commission's efforts in the CIP field will focus on infrastructure that is critical from a European, rather than a national or regional perspective. Although focusing on European Critical Infrastructures, the Commission may where requested and taking due account of existing Community competences and available resources provide support to Member States concerning National Critical Infrastructures.

✓ **Complementarity** - the Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectoral measures.

✓ **Confidentiality** - Both at EU level and MS level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need-to-know basis. Information sharing regarding CI will take place in an environment of trust and security.

✓ **Stakeholder Cooperation** – All relevant stakeholders will, as far as possible, be involved in the development and implementation of EPCIP. This will include the owners/operators of critical infrastructures designated as ECI as well as public authorities and other relevant bodies.

✓ **Proportionality** – measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved.

✓ **Sector-by-sector approach** – Since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors.

2.2 Definitions

Critical infrastructure (CI) means an asset, system or part thereof located in Member States, essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant **impact in a Member State** as a result of the failure to maintain those functions.[1]

European critical infrastructure (ECI) means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact **on at least two Member States**.

Risk analysis means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure.

Owners/Operators of ECIs' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI.

Protection means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability.

III. THE IDENTIFICATION AND THE DESIGNATION OF THE ECIs

3.1. THE IDENTIFICATION OF THE ECIs

Each Member State identifies potential ECIs which both satisfy the cross-cutting and sectoral criteria and meet the definitions set out in Article 2(a) and (b) of the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, (Official Journal of the European Union, L345/75).

Nevertheless, the Commission may assist Member States at their request to identify potential ECIs and may draw the attention of the relevant Member States to the existence of potential critical infrastructures which may be deemed to satisfy the requirements for designation as an ECI.

The cross-cutting criteria comprise the following:

(a) casualties criterion (assessed in terms of the potential number of fatalities or injuries);

(b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);

(c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

The cross-cutting criteria thresholds are be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The precise thresholds applicable to the cross-cutting criteria are determined on a case-by-case basis by the Member States concerned by a particular critical infrastructure. Therefore, Each Member State informs the Commission on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds.

The sectoral criteria take into account the characteristics of individual ECI sectors. In addition of that, there are relevant but optional guidelines for the application of the cross-cutting and sectoral criteria and approximate thresholds to be used to identify ECIs. These criteria are classified.

More precisely, at the EU level, there is a 3-step process for identification of the ECIs:

Step 1 - The European Commission together with the Member States and relevant stakeholders develop *multiple criteria* for the identification of ECI, on the basis of severity of the disruption or destruction of the CI, assessed taking into account:

- *Public effect* (number of population affected);
- *Economic effect* (significance of economic loss and/or degradation of products or services);
- *Environmental* effect;
- *Political* effects;
- *Psychological* effects;
- *Public health* consequences.[2]

Step 2 - Each Member State identifies those infrastructures which satisfy the criteria.

---

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75

Step 3 - Each Member State notifies the Commission of the critical infrastructures which satisfy the established criteria.

3.2 THE DESIGNATION OF THE ECIs

In this matter each Member State informs the other Member States which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI. Therefore each Member State on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI. The Commission may participate in these discussions but shall not have access to detailed information which would allow for the unequivocal identification of a particular infrastructure.

The designation of the ECIs is very collaborative process, having a less bureaucratic mechanism than it appears. A Member State that has reason to believe that it may be significantly affected by the potential ECI, but has not been identified as such by the Member State on whose territory the potential ECI is located, may inform the Commission about its wish to be engaged in bilateral and/or multilateral discussions on this issue. The Commission shall without delay communicate this wish to the Member State on whose territory the potential ECI is located and endeavour to facilitate agreement between the parties.[3] Moreover, the acceptance of the Member State on whose territory the infrastructure to be designated as an ECI is located, is required. The Member State on whose territory a designated ECI is located informs the Commission on an annual basis of the number of designated ECIs per sector and of the number of Member States dependent on each designated ECI. Only those Member States that may be significantly affected by an ECI shall know its identity. The Member States on whose territory an ECI is located informs the owner/operator of the infrastructure concerning its designation as an ECI. This information concerning the designation of an infrastructure as an ECI is classified at an appropriate level.

---

[2] COM(2006) 786 final, Communication from the Commission on a European Programme for Critical Infrastructure Protection

[3] Article 4 (2) - Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75.

IV. THE OPERATORS SECURITY PLANS

The operator security plan ('OSP') procedure identifies the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. All CI owners/operators designated as ECI must establish an OSP which identify the ECI owners' and operators' assets and, of course, establish relevant security solutions for their protection. The minimum contents of such OSPs include:

• identification of important assets;

• a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact shall be conducted;

• identification, selection and prioritisation of counter-measures and procedures with a distinction between:

✓ **permanent security measures**, which identify indispensable security investments and means which cannot be installed by the owner/operator at short notice. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems,

✓ **graduated security measures**, which are activated according to varying risk and threat levels.

Each Member State shall ensure that the OSP or equivalent is in place and is reviewed **regularly within one year** following designation of the critical infrastructure as an ECI. This period may be extended in exceptional circumstances, by agreement with the Member State authority and with a notification to the Commission.[4] Initially, according to the Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection - COM(2006) 787 final, article 5 (1), *each Member State shall require the owners/operators of each European Critical Infrastructure located on its territory to establish and update an Operator Security Plan and to* ***review it at least every two years***.

V. THE SECURITY LIAISON OFFICERS

The main role of the Security Liaison Officer is to be a point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority. Each Member State assesses whether each designated ECI located on its territory possesses a Security Liaison Officer or equivalent.

Each Member State of the EU implements an appropriate communication mechanism between the relevant Member State authority and the Security Liaison Officer or equivalent with the objective of **exchanging relevant information** concerning identified risks and threats in relation to the ECI concerned. This communication mechanism has to be without prejudice to national requirements concerning access to sensitive and classified information.

VI. A NEW APPROACH TO THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION

The new approach to EPCIP builds on a comprehensive review of the 2006 European Programme for Critical Infrastructure Protection1 and the Council Directive 2008/114/EC2, conducted in close cooperation with EU Member States and stakeholders.

By **ensuring a high degree of protection of EU infrastructures** and **increasing their resilience** (against all threats and hazards), it could minimise the consequences of loss of services to society as a whole. These objectives feature predominately in the Stockholm Programme[5] and in the EU Internal Security Strategy[6].

A part of this new approach is looking at the **interdependencies** between critical infrastructures, industry, and state actors. Threats to a single critical infrastructure can have a very significant impact on a broad range of actors in different infrastructures and more widely.

The effects of those interdependencies are not limited to single countries. Many critical infrastructures have a cross border dimension. In addition to **interdependencies between sectors**, there are also many interdependencies within the same sector but

---

[4]Article 4 (2) - Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75.

[5] Conclusions of the European Council of 10/11 December 2009 on 'The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014)'; 17024/09

[6] COM (2010) 673 final. The EU Internal Security Strategy in Action: Five steps toward a more secure Europe. Objective 2: Prevent terrorism and address radicalisation and recruitment. Objective 5: Increase Europe's resilience to crisis and disasters.

spanning a number of European countries. One such example is the European high-voltage electricity grid, composed of the interconnected national high-voltage electricity grids.

The review process of the current EPCIP[7], conducted in close cooperation with the Member States and other stakeholders, revealed that there has not been enough consideration of the links between critical infrastructures in different sectors, nor indeed across national boundaries. In order to properly protect the European critical infrastructures, and in order to build their resilience, it is necessary a new approach which will tackle this gap. To pilot the new approach, the needed start is by working with four critical infrastructures of European dimension: Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network **(the Four)**. These were selected on the basis of their pan-European nature and also their own interest in working with the Commission to explore an approach to CI protection and resilience, which takes better account of interdependencies. It is expected that other relevant infrastructures could then benefit from the processes and tools developed when carrying out the work with the Four.

Through work with the Four and developing the new approach, the EU, led by the European Commission, can both play a supporting role for Member States in their own CI protection and resilience work and facilitate better cooperation on CI protection and resilience within the EU. Given that many critical infrastructures are **privately owned**, better cooperation includes supporting the development of private-public structured dialogues.

The Four were selected on the basis of:

• their European nature due to their cross-border dimension. They are cross-border both physically (i.e. the infrastructures are located in the territory of more than one Member State) and at the level of the service provided (i.e. a disruption of service in one Member State can affect several other Member States — a domino effect);

• their representativeness — the selected cases cover the transport, space and energy sectors; and

• their operators/owners' interest to participate in this pilot and to share best practices.

EUROCONTROL is designated as the EU Air Traffic Management (ATM) Network Manager, managing the flow of approximately 30000 flights per day. The objective, tasks and functions of the Network Manager are regulated by the Commission

[7] Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), SWD(2012) 190 final

Regulation (EU) No 677/2011 of 7 July 2011 laying down detailed rules for the implementation of ATM network functions.

GALILEO is the European programme for a global satellite navigation system, which is partly owned by the EU and will provide services of vital importance for our citizens and economy.

The **Electricity Transmission Grid** and the **European Gas Transmission Network** are networks without national boundaries, which mean that a failure of one portion of the network could propagate to other areas, potentially involving several countries.

In its EPCIP Communication of 12 December 2006, the Commission sets out an overall policy approach and framework for critical infrastructure protection activities in the EU. The new approach will build upon this framework by focusing on its strengths and addressing the gaps identified in the review process. The four main focus areas of the current EPCIP are:

✓ **a procedure for the identification and designation of European critical infrastructures** and assessment of the need to improve their protection (addressed in detail in Council Directive 2008/114/EC). Council Directive 2008/114/EC is considered to be essential by a majority of stakeholders. Furthermore, the economic and political costs of adopting and implementing a new legislative instrument are expected to be high, especially given that only a short time has elapsed since the transposition and implementation of the current Directive. The majority of the CIP community expects that the benefits brought by the current Directive, notably in raising awareness, will continue to increase.

✓ **measures designed to facilitate the implementation of EPCIP**, including an Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, a CIP information-sharing process, and the identification and analysis of interdependencies. It is expected that CIWIN will continue to improve, serving as an important interactive tool for the development of the EU approach outlined here. That role can be filled by CIWIN's performance of several important functions:

a) using the network to showcase the evolution of selected cases of pan-European critical infrastructures and receive feedback from CIWIN users;

b) it aims to provide a toolbox, comprising risk assessment methodologies and the tools necessary to perform a risk analysis (e.g. templates);

c) it can become the host platform for several national CIP areas in Member States;

d) the network will include all relevant information regarding cooperation with selected third countries, such as the US, Canada and the EFTA countries.

✓ **funding for CIP-related measures and projects** focussing on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security- Related Risks' for the period 2007-2013. At EU level many actions have been undertaken to build knowledge on how to better protect critical infrastructures. There were funded over 100 diverse projects under the Programme **'Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks'** (CIPS) during the 2007-2012 period, addressing CIP and crisis management. These projects have a broad scope, covering all sectors, and including analyses of criticalities and dependencies.

Regarding **risk assessment** and **risk management** methodologies, the Commission has also funded numerous projects covering all sectors under the CIPS Programme. These include: the development of a risk assessment methodology to enhance security awareness in air traffic management; the assessment of resilience to threats to control and data management systems of electrical transmission networks; and an interactive risk assessment in the critical infrastructure field based on Earth Observation data and an integrated geographic information system. The studies indicate that risk assessment methodologies for CIP follow either: 1) a sectoral approach, where each sector is treated separately with its own risk methodologies and risk ranking; or 2) a systems approach, where critical infrastructures are treated as an interconnected network. Most work has been sectoral, but these methodologies show their limits when cross-sectoral issues need to be addressed, so a **systems approach** will be encouraged by the European Commission from now on.

✓ **the development of an EPCIP external dimension**. Member States have expressed the view that the external dimension is of particular importance for CIP. In particular, collaboration with the EFTA countries is considered a priority. To formalise this cooperation with the EEA, the Commission presented a proposal for a Council Decision for the expansion of the applicability of Directive 2008/114/EC to the EEA countries, which led to an EEA Joint Committee Decision on the identification and designation of European critical infrastructures. Both Norway and Iceland have recently notified the fulfilment of their constitutional requirements for the entry into force of the Decision. The proposed Regulation establishing an Instrument for Stability (IfS) — an external cooperation instrument — allows for assistance to protect critical infrastructure in third countries, in the fields of international transport (aviation and maritime), energy operations and distribution infrastructure, and electronic information and communication

networks (cyber security). Furthermore, to foster strategic partnerships beyond Europe, EU-US and EU-Canada expert meetings have been held yearly, most recently in May 2013. These meetings addressed mainly the need to strengthen cooperation by sharing knowledge, best practices and information on CIP, including the development of a global infrastructure security toolkit. Its purpose would be to promote the exchange of best practices, methodologies, analysis, lessons learned, and other useful materials between the EU, U.S. and Canada.

Prevention. The new EU CIP approach will begin by taking stock of the work done so far in order to provide an update on the progress in security measures and the evolving interdependences with other sectors (ICT, water, etc.). Another path is working with the Four to set up tools for **risk assessment and risk management.** These in particular are related to the Group on Earth Observation (GEO) – such as the Supersites Initiative – and to the development of hazard risk assessment methodologies for low-probability – high consequences events that could be applied in future "stress tests" for critical infrastructures. Regarding the ICT sector, the EU Cybersecurity Strategy – An Open, Safe and Secure Cyberspace – identifies actions that will further contribute to the cyber resilience and security of infrastructures covered by EPCIP. The strategy's proposals include coordinated prevention mechanisms, improved preparedness and the involvement of the private sector.

Where appropriate, the EU will share the knowledge among the Four to identify opportunities to strengthen existing protection plans and will promote a dialogue between the critical infrastructure operators and the actors upon whom they rely; and foster exchanges of best practices and the development of scenario exercises, guidelines and recommendations.

Preparedness. According to its strategy, the EU will support the development of preparedness strategies based around contingency planning, stress tests, awareness raising, training, joint courses, exercises and staff exchange. The establishment of such structures can also be supported by promoting incident reporting, which can be encouraged as a means to improve the level of knowledge on the performance of critical infrastructures during a disruptive event (e.g. the extent of cascading effects, overall impact, etc.). The aim is to increase **consideration by the Member States and other actors reliant upon critical infrastructures of how they can prepare in response to events affecting European critical infrastructures.** Member States and other actors

could share, on a voluntary basis, information on incidents in relation to the Four which could affect them. By getting this dialogue going, the EU can further improve the overall preparedness level.

Furthermore, it will be explored the possibility of linking the civil protection training network, envisaged in the proposal for a new Union Civil Protection Mechanism, with relevant critical infrastructure training activities. In addition, joint exercises with the relevant sectors or with the Civil Protection Mechanism may highlight the complementarity of EU preparedness measures.

Response. Having facilitated dialogue on preparedness, the European Commission can then help identified actors think about their response to events, having the aim to strengthen the links between the critical infrastructure community and early warning systems, as early warning tools for natural disasters can point to potential threats to critical infrastructures. That leads people to think about the mechanisms for on-going communication between the Four and other actors reliant upon them until functionality is restored.

Given that the current Union Civil Protection mechanism only focuses on the immediate response to an incident, it is compulsory to know how the mechanism could further promote the use of recovery specialists to help with the **long-term recovery of critical services,** to be deployed at the request of Member States.

CONCLUSIONS

The EU will continue to develop the protection and resilience measures already in place, looking to improve their utility. In addition, the new approach looks to increase the dialogue between critical infrastructures and all those actors across Europe who would be impacted by any event affecting functionality. This will be done under the prevention, preparedness and response framework, having identified relevant pan-European critical infrastructures. The Commission's role remains one of facilitating and supporting the work of critical infrastructures, Member States, and industry and providing services which those actors can use to improve CIP across Europe. It is also important that, in parallel with this new approach, Member States and the private sector continue their efforts of identifying European Critical Infrastructures – building on their work so far and on the results of the projects already pursued. CIWIN will continue to be a support tool in this process.

The application of the work streams in these four pan-European critical infrastructures should provide the necessary indicators to allow for the shaping of an **EU approach towards CIP**. It would be based on the results achieved and the gaps identified through working with the Four, and seek to provide useful tools for improving protection and resilience, including through providing for **strengthened risk mitigation, preparedness and response measures**. The following step could be to **implement this approach** in **regions** where Member States are interested in cooperating with each other. Examples could potentially include a resilience concept for the overall critical transport infrastructure around the Baltic Sea, and a programme for supply chain criticalities in the Danube region. The reshaped programme should also be aligned with the time frame for the new Multiannual Financial Framework 2014-2020 (of relevance here, Internal Security Fund — Police) and emphasise the strategic role of the **funds available** for the implementation of activities at all levels, clearly linking them with the key priorities described here. Instead of funding a large number of diverse projects, a few large cross-border strategic projects could be launched to implement the agreed EU tools and methodologies.

REFERENCES

1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75;
2. Conclusions of the European Council of 10/11 December 2009 on 'The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014)'; 17024/09;
3. Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final;
4. The EU Internal Security Strategy in Action: Five steps toward a more secure Europe. Objective 2: Prevent terrorism and address radicalisation and recruitment. Objective 5: Increase Europe's resilience to crisis and disasters, COM (2010) 673 final;
5. Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), SWD(2012) 190 final;
6. Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure, SWD(2013) 318 final.

FREEWARE INTRUSION DETECTION / INTRUSION PREVENTION SYSTEMS: BENEFITS AND DISADVANTAGES

Author:
Dmitrii MEICO

INTRODUCTION

During the last years the Internet has become a critical infrastructure for many countries in the world. More and more organizations transfer their business and some of them are totally dependent on it. Many people cannot imagine their lives without the Internet. This situation opens new possibilities for cybercriminals for performing illegal actions and creates new challenges for information security personnel to keep their informational systems protected.

The most important issue that is to be given greatest consideration is the security of an environment. No mater how complex it is – be it a host, local network or a cloud – it still faces the threats like vulnerability scans, distributed denial of service attacks malicious infections and so on. All these attacks can affect the business continuity. That is why it is essential to identify these attacks at any early stage itself, so that the attacker can be blocked and avoid further effects. One of commonly protection techniques used to do it is to deploy an intrusion detection (IDS) or intrusion prevention system (IPS) which is able to identify the intrusions before attack can take place and can give a notification that it is possible to have an attack

There are several open source IDS and IPS present. Some of them are Snort, Bro, and Suricata etc. They are very strong and efficient in identifying attacks.

The purpose of this paper is to provide an overview of these freeware IDS/IPS and to define what are their benefits and disadvantages.

I. OVERVIEW OF INTRUSION DETECTION / PREVENTION TECHNOLOGY

I.1 Definition and functions of intrusion detection and intrusion prevention systems

Intrusion detection system is a type of security management system used for networks (sometimes referred as NIDS) and computers (sometimes referred as HIDS).

An IDS detects intrusions – attacks from outside the organization – and misuse – attacks from within the organization – by gathering and analyzing information from various areas within a network or a computer to identify possible security breaches. An IDS use two methods of detection – signature based detection and anomaly based detection.

Intrusion detection functions are[1]:

- Monitoring and analyzing user and system activities
- Tracking user policy violations
- Analysis of abnormal activity patterns
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analyzing system configurations and vulnerabilities

A HIDS usually acts as passive component of information protection – it inspects system's configuration files to detect inadvisable settings; password files to detect inadvisable passwords; and other system areas to detect policy violations.

A NIDS is considered the active component of information protection: mechanisms are set in place to reenact known methods of attack and to record system responses.

There are a couple of methods in which IDS can block malicious communication:

- IDS may send a TCP reset packet if the attacker has opened a TCP connection to the victim
- IDS may send various UDP packets to disrupt a UDP connection
- IDS can communicate with the firewall and install a rule drop all packets from the attackers IP Address

---

[1] Margaret Rouse, "intrusion detection", May 2007, http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection/

Like an IDS, an intrusion prevention system (IPS) monitors network traffic[2]. However, because an attack can be carried in one packet of data it's crucial to block communications before it can reach the target. Another important aspect, which should be considered, is that an IPS has to have enough performance to process all of the packets in an acceptable time limit; otherwise it will have either to drop the traffic either to forward it without inspection.

I.2. Signature based detection

Signature based detection uses known pattern of illegal action to detect malicious attack which is similar to the way a virus scanner works. To create a signature unique characteristics of an attack are used. Each time an IDS gets the packet it examines it against set of signatures it has in order to decide whether it can be considered an attack or not.

Advantages of Signature Based Detection[3]:

- Considered to be much more accurate at identifying an intrusion attempt.
- Ease of obtaining precise, detailed information about the alert.
- Less false positives.

Disadvantages of Signature Based Detection:

- Only attempts, which match the pattern could be detected, so it's necessary constantly update the signature database.
- There is a period of time between a new type of an attack is identified and vendors release the update, during this time the assets will stay unprotected.
- IDS or IPS can be overwhelmed by matching each packet with each signature of the database, what can cause dropping legitimate traffic, allowing malicious to pass undetected or create unacceptable delay.

I.3 Anomaly based detection

An anomaly is anything which is considered abnormal. Anomaly detection can be divided into two types: static and dynamic.

---

[2] Margaret Rouse, "intrusion prevention", May 2007, http://searchsecurity.techtarget.com/definition/intrusion-prevention/

[3] Brandon Lokesak, "A Comparison Between Signature Based and Anomaly Based Intrusion Detection Systems".

Static assumes that some system files or behavior should always remain constant and if monitored file changes an anomaly will be detected. Static anomaly detection could detect only changes in software but not in hardware.

Dynamic uses a profile or a baseline to perform its function. Baseline must be defined by network security administrator. It defines what is considered normal and what limits measured parameters could excide in order to stay normal.

Advantages of Anomaly Based Detection:

- Can detect unknown threats.
- Minimal maintenance after system is deployed.
- Baseline can tuned to be more accurate and cause less false positives longer the system stays in use.

Disadvantages of Anomaly Based Detection

- Until baseline is established network will stay unprotected.
- If malicious activity looks like normal event the system will never trigger an alarm.
- Many false positives at the beginning of operation

II. FREEWARE INTRUSION DETECTION / INTRUSION PREVENTION SYSTEMS

II.1 Snort

Snort is an open source network intrusion detection and prevention system. It was created by Martin Roesch in 1998. Uses both signature and anomaly based detection methods. Support many hardware platforms and operation systems: Linux, OpenBSD, FreeBSD, NetBSD, Solaris, MacOS and Windows. Snort uses signatures made by Source fire, standard set of signatures can be also extended by community-issued or handwritten signatures.

Snort can operate in the following modes :

- Sniffer – reads packets and display in console
- Packet logger – logs network packets to disk.
- Network intrusion detection mode – monitors network traffic and analyses it against enabled signatures and rules.

The Snort has modular architecture. It is composed of a packet decoder, preprocessor, detection engine, and output plug-ins.

Snort uses LIBPCAP to capture packets from the network interface device. After the packets are sniffed they are passed to the decoder, which through LIBPCAP decodes the protocol packet elements at different levels of OSI model. Extracted information is stored in a data structure which is ready to be processed by the preprocessor and detection engine. The pre-processor verifies if protocol in which was encapsulated data correspond to protocol specifications and rules, established by network security administrator. The most important component of Snort architecture is detection engine. It compares extracted information against loaded signatures and defined rules. If Snort is deployed in inline mode it can immediately drop the packet. After signature match happens or anomaly is detected the detection engine sends the signature ID to the output plug-ins. Output plug-ins are used to represent this information in human readable format and using common data containers like CSV or XML[4].

Snort Benefits:

- Is able to track sessions for: TCP, UDP and ICMP communications.
- Can detect multiple network protocol anomalies.
- Can check for TCP hijacking.
- Able to detect NMAP port scans.
- Detect viruses in email attachments.
- Detect different expoits
- Large community support
- Plenty of administrative front-ends

Snort Disadvantages:

- No hardware acceleration.
- Limited file extraction

II.2 Suricata

Suricata is an open source NIDS developed by Open Information Security Foundation (OISF), which is founded by Department of Homeland Security U.S. and consortium of members. It that was officially released in July, 2010.

---

[4] The Snort Project, "Snort Users Manual 2.9.3", May 23, 2012.

Suricata was created as a multithread alternative to Snort, which allows to use hardware acceleration (CPU and GPU cores) to increase useful amount of processing power.

In terms of detection Suricata also uses signature and anomaly based detection methods. Suricata comes with optimised set of Snort rules, which take advantages of the Suricata engine. Suricata preprocessors are used to detect protocol anomalies. If Suricata is deployed inline, then prevention functionality could be activated.

Benefits[5]:

- High performance, scalable through multi threading
- Protocol identification
- File identification, extraction, on the fly MD5 calculation
- TLS handshake analysis, detect/prevent things like Diginotar
- Hardware acceleration support: Endace, Napatech, CUDA, PF_RING.
- Rules and outputs compatible to Snort syntax
- useful logging like HTTP request log, TLS certificate log, DNS
- logging
- Lua scripting for detection

II.3 Bro

Bro is an open-source, Unix-based Network Intrusion Detection System (NIDS) developed by Vern Paxson, Berkley National Lab in 1998.

As other IDS it uses signature and anomaly based detection. The system can run on Linux, Solaris and FreeBSD. It supports, with use of special converter, Snort rules. Bro was designed to operate at high-speed (Gbit/Second), high-volume intrusion detection.

In table 3.1 are presented technical requirements for Bro IDS[6].

Table 3.1 Bro IDS requirements

Item	**Requirements**
Processor	1 GHz CPU for 100 Mbps monitoring with <= 5,000 packets/second 2 GHz CPU for 1 Gbps monitoring with <= 10,000 packets/second

[5] Éric Leblond, "Suricata 2.0, Netfilter and the PRC", Stamus Networks, 2014.
[6] Vern Paxson, "Bro User Manual", version 0.9, draft, 2004.

	3 GHz CPU for 1 Gbps monitoring with <= 20,000 packets/second 4 GHz CPU for 1 Gbps monitoring with <= 50,000 packets/second
Operating System	FreeBSD, Linux or Solaris
Memory	2-3 GB is recommended
Hard disk	10 GB minimum, 50 GB or more for log files recommended.
User Privileges	superuser to install Bro, with Bro then running as user bro.
Network Interfaces	3 interfaces are recommended: 2 for packet capture (1 for each direction), and 1 for host management. Capture interfaces should be identical. For some network taps, both directions of the link are captured using the same interface, and the separate host management interface, while prudent, is not required.
Other Software	Perl version 5.6 or higher libpcap version 0.7.2 or higher

How Bro works[7]:

1. Bro passively sniffs all network traffic.
2. Using libpcap Bro filters down high-volume stream.
3. "Event engine" transforms filtered stream into high-level, policy-neutral events reflecting underlying network activity. For example: at connection-level: connection attempt, connection finished; at application-level: ftp request, http-reply; at activity-level: login success.
4. "Policy script" processes event stream, incorporates: context from past events, site's particular policies and takes following actions: records to disk, generates alerts, and executes programs as a form of response.

At figure 3.1 is presented Bro traffic analysing process.

[7] Brian L. Tierney, "An Overview of the Bro Intrusion Detection System", Lawrence Berkeley National Laboratory.

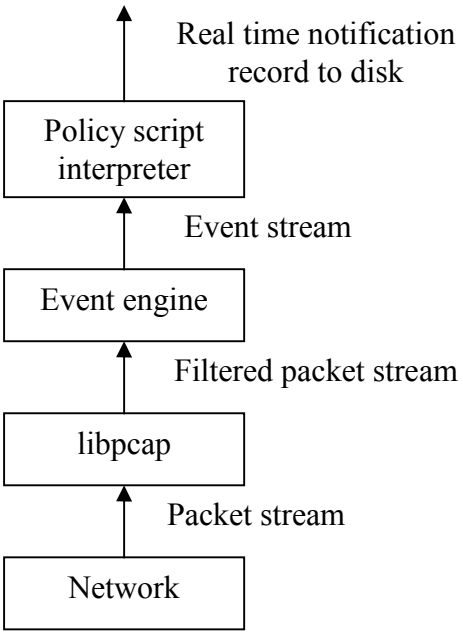


Figure 3.1 – Bro traffic analysing process

Bro features and benefits:

- **Network based** – Bro is a network-based IDS. It collects, filters and analyses incoming and outgoing traffic that passes through a specified by a security administrator network location. Bro does not use or require installation of client software on each individual, networked computer.
- **Custom Scripting Language** – Bro policy scripts are written in the Bro language. They contain the "rules" that describe what types of activities are considered malicious. The language is very powerful comparing to Snort and Suricata, and allows to create much more complicated and precise rules.
- **Pre-written Policy Scripts** – Bro comes with a rich set of policy scripts designed to detect the most common Internet attacks while limiting the number of false positives i.e., alarms that confuse uninteresting activity with the important attack activity. These supplied policy scripts will run "out of the box" and do not require knowledge of the Bro language or policy scripts mechanics.
- **Powerful Signature Matching Facility** – Bro policies incorporate a signature matching facility that looks for specific traffic content. For Bro, these signatures are expressed as regular expressions, rather than fixed strings. Bro adds a great deal of power to its signature-matching capability because of its rich language. This allows Bro to not only examine the network content, but to understand the context of the signature, greatly reducing the number of false positives. Bro comes with a set of high-value signatures, selected for their high detection an low false

positive characteristics, as well as policy scripts that perform more detailed analysis.

- **Network Traffic Analysis** – Bro not only looks for signatures, but also analyses network protocols, connections, transactions, data volumes, and many other network characteristics. It has powerful facilities for storing information about past activity and incorporating it into analyses of new activity.
- **Detection Followed by Action** – Bro policy scripts can generate output files recording the activity seen on the network (including normal, non-attack activity). They can also send alarms to event logs, including the operating system syslog facility. In addition, scripts can execute programs, which can, in turn, send e-mail messages, page the on-call staff, automatically terminate existing connections, or, with appropriate additional software, insert access control blocks intro a router's access control list. With Bro's ability to execute programs at the operating system level, the actions that Bro can initiate are only limited by the computer and network capabilities that support Bro.
- **Snort Compatibility Support** – The Bro distribution includes a tool, snort2bro, which converts Snort signatures into Bro signatures. Along with translating the format of the signatures, snort2bro also incorporates a large number of enhancements of the standard set of Snort signatures to take advantage of Bro's additional contextual power and reduce false positives.

Bro disadvantages[8]:

- Complicated to set up
- Small community of users

CONCLUSIONS

An IDS or IPS is a necessary tool in any environment as it gives the possibility to monitor network and detect ongoing threads. Deploying IDS requires research, planning, time and effort, but results worth it. It's important to configure it properly, to know what rules are enabled and from which intrusions an IDS or IPS protects. Information security is not a patch,

[8] Joe Schreiber, "Open Source Intrusion Detection Tools: A Quick Overview", 2014 http://www.alienvault.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview

which can be deployed once and then forgotten, so and IDS or IPS system has to be monitored and tuned accordingly the situation.

In the work was provided an overview of freeware intrusion detection / intrusion prevention systems, discovered their benefits and disadvantages. The most important thing to consider – an intrusion detection or prevention systems are not a panacea; they are a small part of overall defense mechanism which assures that information is protected.

REFERENCES

1. Margaret Rouse, "intrusion detection (ID)**",** May 2007, http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection/
2. Margaret Rouse, "intrusion prevention", May 2007, http://searchsecurity.techtarget.com/definition/intrusion-prevention/
3. Brandon Lokesak, "A Comparison Between Signature Based and Anomaly Based Intrusion Detection Systems".
4. The Snort Project, "Snort Users Manual 2.9.3", May 23, 2012.
5. Éric Leblond, "Suricata 2.0, Netfilter and the PRC", Stamus Networks, 2014.
6. Vern Paxson, "Bro User Manual", version 0.9, draft, 2004.
7. Brian L. Tierney, "An Overview of the Bro Intrusion Detection System", Lawrence Berkeley National Laboratory.
8. Joe Schreiber, "Open Source Intrusion Detection Tools: A Quick Overview", 2014 http://www.alienvault.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview

FUTURE OF INTERNET SECURITY-IPSEC

Author:
LTC Yusuf ROUSAN

Abstract

IPSec is a set of protocols and cryptographic algorithms that provides authentication, verification and encryption at the IP networking layer and is a widely deployed mechanism for implementing Virtual Private Networks (**VPNs**). This paper will describe the overview of IPSec, protocol and standards which apply to IPSec, it will also focus on the advantages of IPSec (**network layer security**) over security at other layers. It will analyze the various weaknesses that have been or could be identified within this powerful security protocol. There is also an attempt to show the IPSec/QoSS (**Quality of Security Service**) scenario which has many uses including virtual private networks (**VPN**) that stretch across global networks. This paper will also discuss the present status of IPSec and from here where it will go in the future.

I. Introduction

IPSec provides security at the IP network layer of the TCP/IP protocol stack. This means that all IP packets can be protected, irrespective of the upper layer protocol being carried in the packet payloads, and that no re-engineering of applications is required in order to take advantage of the security provided by IPSec. The security provided by IPSec can also be made transparent to end users. For these reasons, IPSec forms the basis of many Virtual Private Networking (**VPN**) solutions, where it is used to provide security for communications over an untrusted network such as the Internet.

Internet Security protocol (**IPSec**) is a protocol suite for securing connections at Internet Protocol (**IP**) layer. IPSec is a large specification, covering a large variety of connections. IPSec has two protocols for providing security. One of them is Authentication Header (**AH**), which is, as the name suggests, is just a security header. The other is Encapsulated Security Payload (**ESP**) which encrypts the whole packet. IPSec also has two modes of operation: transport mode, which is designed to offer secure connection for higher layer protocols, and tunnel mode, which is used to create secure connections through unsecure networks. Both modes can use **AH**, **ESP** or both, and all these combinations rely on Internet

Key Exchange (**IKE**) to create the security associations upon which the secure connections are created. All these can be used both in **IPv4** and **IPv6** networks, with only minor differences from the protocol perspective. Finally, IPSec can be used with a large variety of encryption algorithms. The actual algorithms used are negotiated when the connections are established.[1]

II. IPSec Overview

IPSec is an Internet Engineering Task Force (**IETF**) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the Packet level. It was designed to provide authentication (verifies that the packet received is actually from the sender), integrity (ensures that the contents of the packet did not change in transit), and confidentiality (conceals the message content through encryption).

IPSec contains Encapsulating Security Payload (**ESP**), provides confidentiality, authentication, and integrity. ESP provides all the encryption services. It also contains Authentication Header (**AH**), provides authentication and integrity, which protects against data tampering and unauthorized retransmission of packets. The last component it has, is the Internet Key Exchange (**IKE**), which provides key management and security association management. The aforementioned features of IPSec are accomplished through packet header modification. IPSec introduces the concept of the Security Association (**SA**). An SA is a logical connection between two devices transferring data. An SA provides data protection for unidirectional traffic by using the defined IPSec protocols.[2]

IPSec = AH + ESP + IPcomp + IKE

AH AND ESP: Protection for IP traffic AH provides integrity and origin authentication ESP also confidentiality.

IPcomp : Compression.

IKE : Protection Sets up keys and algorithms for AH and ESP.

II.1. IPSec protocol suite

IPSec protocol suite has been discussing and developing in (**IETF**) IPSec working group. The fundamental concept of IPSec is to provide authenticated or security IPSec tunnel, such that any packet, going through this tunnel, has the confidentiality to verify that the packet is real be authenticated by the routers of the both end of the tunnel. If a packet goes

through this tunnel, but not been authenticated will be dropped. In IPSec, there are two types of protocols in doing tunnel authentication: [1,4]

a. Authentication Header (AH) protocol provides support for data integrity and authentication of IP packets.

b. Encapsulating Security Payload protocol provides confidentiality services, including confidentiality of message contents, and also provides options for authentication of IP header.

II.1.i. IPSec Authentication Header (AH)

It provides integrity and authentication, which protects against data tampering and unauthorized retransmission of packets and access control through IKE, its also provide an optional anti-replay protection, and data source authentication but does not offer data privacy, and provides data origin authentication for as much of the IP packet as is possible using a MAC algorithm. Certain fields of the IP packet header cannot be input to the MAC calculation because they may change during the packet's transit across a network and so are unpredictable to the receiver. In AH mode there is no encryption of the payload, only the header is involved. The AH protocol adds its cryptographic protection by inserting a bit sequence called the Authentication Header into IP packets. Figure (1) depicts the IPSec AH header format.

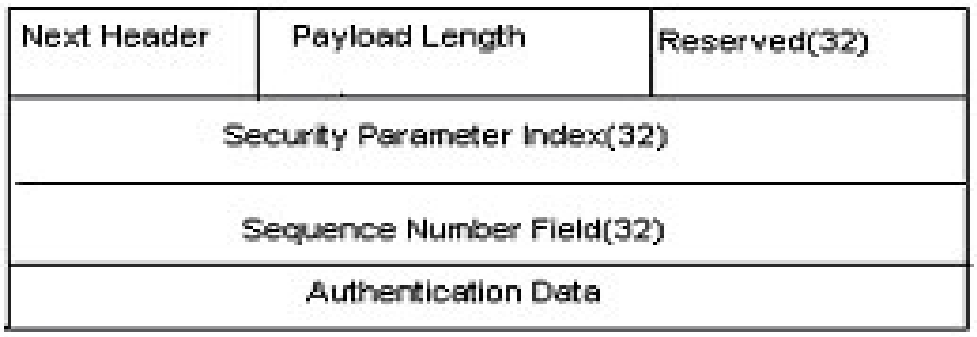


Figure 1. Authentication Header

The IP Authentication Header(AH) is used to provide connectionless integrity and data origin authentication for IP Datagrams and to provide protection against replay attack. AH is based on the use of the integrity check value with an algorithm specified in the SA. It avoids IP-Spoofing attack. Authentication Header consists of the following fields: [1,3,4]

1. Next Header: Data protocol transmitted inside IP(e.g. TCP, UDP, etc.).
2. Payload length: Length of Authentication Header.
3. Security Parameter Index(**SPI**): Identification of the SA of this datagram.

4. Sequence Number: Counter monotonically incremented with each packet.

5. Authentication Data: It contains the Integrity Check Value(**ICV**).

6. Reserved: (**32 bits**) for future us.

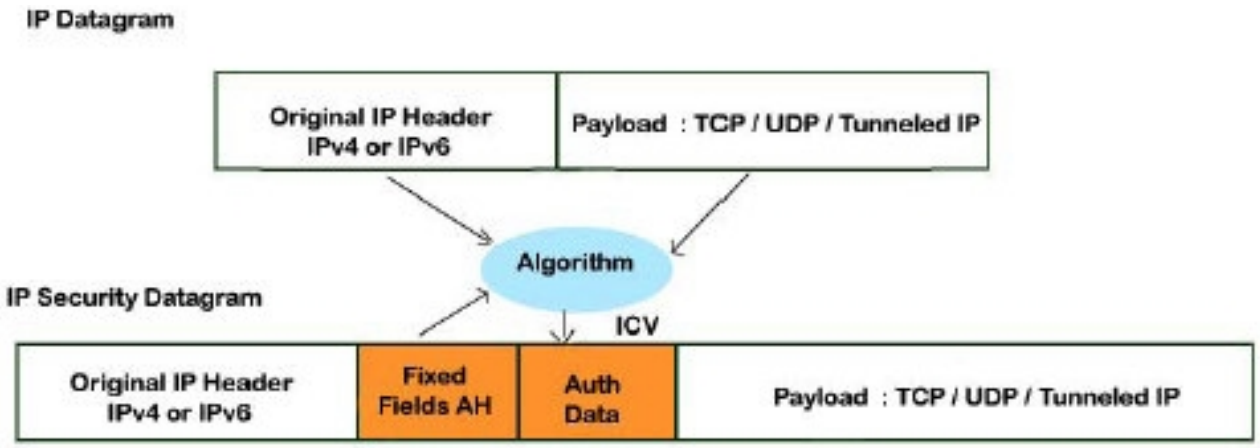


Figure 2. "Authentication Data"

II.1.ii. IPSec Encapsulating Security Payload (ESP)

Encapsulated Security Payload (**ESP**) offers almost all the features of AH, and additionally it also provides confidentiality by encrypting the payload. As proven by practice, ESP is sufficient for almost all needs and it is the only required protocol, IPSec solutions are free not to implement AH. Encapsulating Security Payload protocol including confidentiality of message contents, and also provides options for authentication of IP header.

The Encapsulating Security Payload provides confidentiality, authentication, and data integrity. An ESP can be applied alone or in combination with an AH. Figure (3) depicts the ESP header format.[1,3,4]

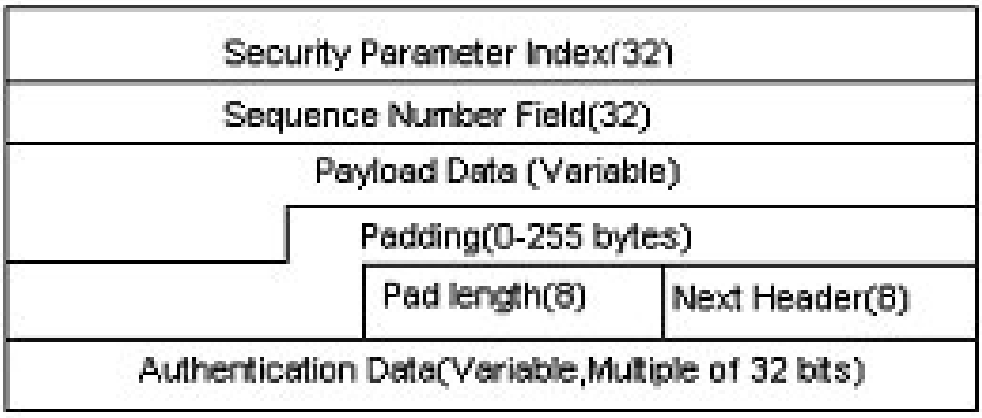


Figure 3. IPSec ESP Header Format

Encapsulating Security Payload includes: [3]

1. Security Parameter Index(**SPI**):Identification of the SA of this datagram.

2. Sequence Number: Counter which is incremented with each packet.

3. Payload Data: Encrypted Data of the IP protocol.

4. Padding: Extra bytes needed if the encryption algorithm needs complete text blocks.

5. Pad length: Number of padding bytes.

6. Next Header: Data protocol in the payload data.

7. Authentication Data: ICV computed over all the datagram (Except Authentication Data Field).

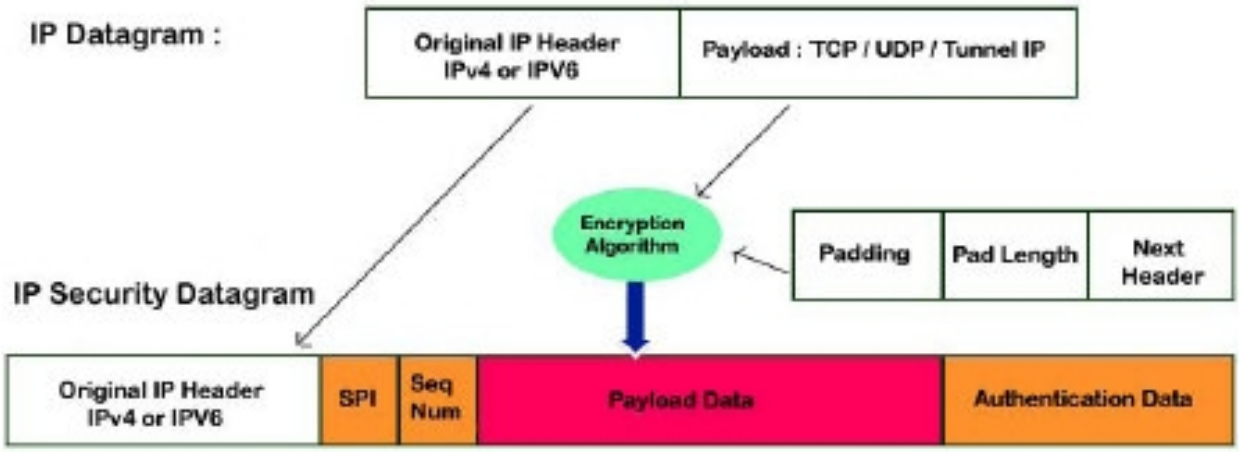


Figure 4. " ESP Computation "

II.2. Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is the backbone of IPSec protocol. Every established connection must have a Security Association (SA) established, and IKE is used to create those associations based on the security policy defined. In the current protocol you must have a way to authenticate the peers of every connection. IKE offers a variety of methods to provide this: the two most commonly used methods are pre-shared secret and public key cryptography. With pre-shared secrets, both ends must have the same secret configured before the establishment of IPSec connection. This means, that you need a different secret for every pair of hosts, which becomes extremely cumbersome even with relatively small number of hosts. With public key cryptography hosts use two keys, one private and the other public. One key is used to encrypt, and the other key can be used to decrypt. This means, that the hosts can give the same public key to every peer, thereby lessening the amount of secrets needed with multiple connections. Although public key algorithms help in reducing the amount of secrets needed, the public keys must still be delivered to the peers before the connections can be

established. To help this, IKE includes a mechanism for using certificates to establish trust networks, where you can first get the public key via unsecure media, and then use a trusted party to confirm the legitimacy of the key. While the key management is relatively simple within a single organization, the establishment of trust networks between different organizations has proven to be a difficult task. This issue is even more relevant in public IPSec key management, which currently is practically non-existent. That said, it is often unfeasible to provide authentication for the peers, and currently the only alternative to a full authenticated IPSec connection is to not use any network layer protection.[1,4]

II.3. IPSec Technologies

IPSec combines several different security technologies into a complete system to provide confidentiality, integrity, and authenticity. In particular, IPSec uses: [5]

1. Diffie-Hellman key exchange for deriving key material between peers on a public Network.
2. Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks.
3. Encryption algorithms, such as DES,3DES for encrypting the data.
4. Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as MD5 or SHA for providing packet authentication.
5. Digital certificates signed by a certificate authority to act as digital ID cards.

II.4. IPSec Operation

IPSec, like most network security protocols, has a session protocol for the protection of data, and an authenticated key exchange protocol for establishing a shared session key. The session protocol is called the *Encapsulating Security Payload* (ESP). It takes care of the encryption and/or authentication of individual IP packets. There is another session protocol, the *Authentication Header* (AH), but its use is no longer recommended. The session keys are negotiated with the Internet Key Exchange (IKE). of which there are two versions (IKEv1 and IKEv2). The shared session state between two IPSec nodes is called a *security association* (SA). An SA determines the session protocol mode, the cryptographic algorithms, and the session keys used between the nodes. The SAs come in pairs, one for each direction. Security associations are typically created by IKE, but they can also be configured manually by the system administrator.

In addition to the protocols and associations, an important part of the IPSec architecture is the security policy. Each host has a *security policy database* (SPD) that

determines an *action* for each packet: whether the packet should be protected, discarded, or allowed to bypass IPSec processing. The SPD maps the protected packets to the right SAs, and triggers IKE to create an SA pair if no suitable one exists. The policy applies to both outbound and inbound packets. For outbound packets, an SA is used to add the encryption and message authentication code as required by the policy. For inbound packets, the policy determines what kind of protection the packet must have. Inbound packets that do not have the right protection, i.e., ones that were not received via the right SA, are discarded by IPSec.

The SPD is an ordered list of rules, each one of which consists of *selectors* and an action. The packet headers are compared against the selectors and the first rule with matching selectors determines the action to be taken on the packet. The exact packet-matching algorithm has changed over versions of the IPSec specification and varies from implementation to implementation; we stick to what is common between many implementations. The selectors are typically ranges of packet-header values, e.g., source and destination IP addresses and port numbers.

There are two different types of IPSec application protection provided by IPSec and there are also different modes for IPSec to operate upon. The first application is a VPN, in which encrypted and authenticated tunnels connect geographically separate parts of a private network, The second IPSec application is host-to-host communication. In that case, the IPSec SAs are established between end hosts and encryption and authentication are performed by the end hosts themselves. This kind of SA is usually set up in transport mode, although tunnel mode can also be used.[6]

IPSec is designed to provide high-quality, interoperable cryptographic based security for IPv4 and IPv6 datagrams. IPSec achieves these objectives by using two traffic security protocols: authentication header (AH) and encapsulating security payload (ESP), and through the use of cryptographic-key management procedures and protocols such as Internet Key Exchange (IKE) protocol. The IP AH protocol provides data origin authentication, connectionless integrity, and an optional anti-replay service. The ESP protocol provides data confidentiality, limited traffic flow confidentiality, connectionless integrity, data origin authentication, and anti-replay service. There are two modes of operation of both AH and ESP: transport mode and tunnel mode. The IKE protocol is used to negotiate the cryptographic algorithm choices to be utilized by AH and ESP, and put in place the necessary cryptographic keys that the algorithms require.

The protocols that IPSec utilizes are designed to be algorithm independent. The choice of algorithms is specified in the Security Policy Database (SPD). The available choice of

cryptographic algorithms depends on the IPSec implementation; however, a standard set of default algorithms are specified by IPSec to ensure interoperability on the global Internet. IPSec allows the user or administrator of a system or a network to control the granularity at which the security service is offered. For example, an organization's policy might specify that data traffic that originated from certain subnets should be protected with both AH and ESP and that the encryption should be done with triple-DES with three different keys. On the other hand, the policy might specify that data traffic from another site should be protected with only ESP and that this traffic should be afforded encryption with AES (Advanced Encryption Standard). IPSec is able to differentiate between the security services it offers to different data traffic by the use of security association (SA).[4]

II.5. Operating Modes of IPSec

The type of operation for IPSec connectivity is directly related to the role the system plays in the VPN or the SA status. As shown in Figure (5), there are two modes of operation for IPSec VPNs:

- Transport mode
- Tunnel mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. A more dramatic method, Tunnel mode, encapsulates the entire IP packet to tunnel the communications in a secured communication. Transport mode is established when the endpoint is a host, or when communications are terminated at the endpoints. If the gateway in a gateway to host communications were to use Transport mode, it would act as a host system, which can be acceptable for direct protocols to that gateway. Otherwise, Tunnel mode is required for gateway services to provide access to internal systems. Transport mode must be used for secure end-to-end connections between hosts or devices acting as hosts, while tunnel mode is used for IPSec connections between security gateways and between security gateways and hosts.[1,7]

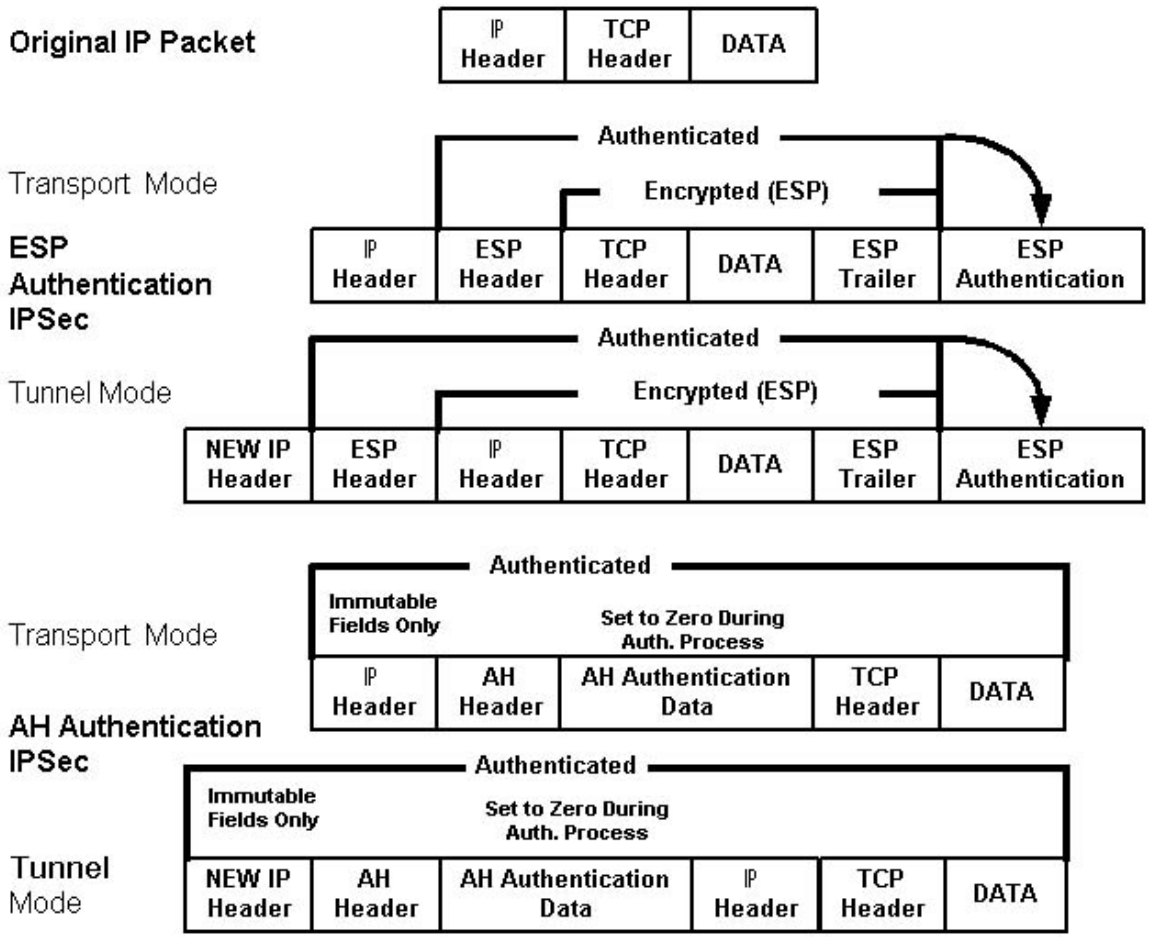


Figure 5. IPSec transport mode and tunnel mode

II.5.i. Transport Mode

In Transport mode, the IP packet contains the security protocol (**AH or ESP**) located after the original IP header and options and before any upper layer protocols contained in the packet, such as TCP and UDP. When ESP is utilized for the security protocol, the protection, or hash, is only applied to the upper layer protocols contained in the packet. The IP header information and options are not utilized in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data. With the use of AH as the security protocol, the protection is extended forward into the IP header to provide integrity of the entire packet by use of portions of the original IP header in the hashing process. In Transport mode, only the Transport layer of the IP packet is transformed [7]

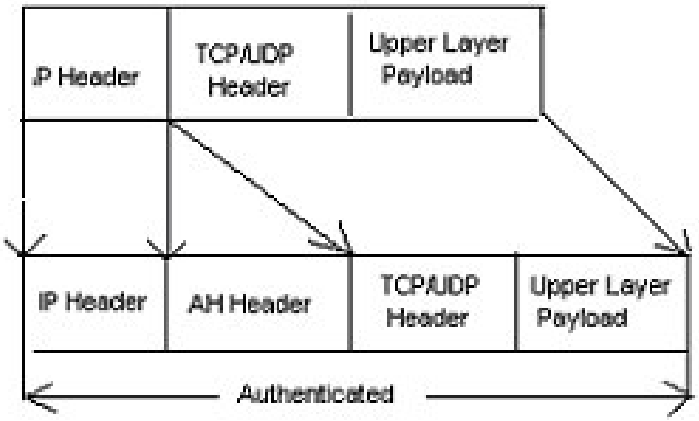


Figure 6. AH in Transport Mode

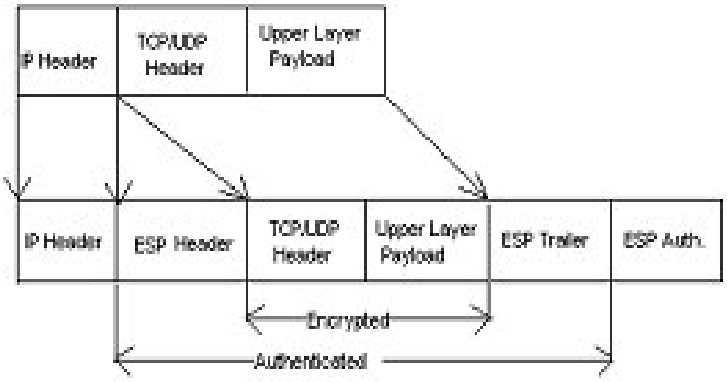


Figure 6. ESP in Transport Mode

II.5.ii. Tunnel Mode

Tunnel mode is established for gateway services and is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. Tunnel mode is required for gateway to gateway and host to gateway communications. Tunnel mode communications have two sets of IP headers:

- Outside
- Inside

The outside IP header contains the destination IP address of the VPN gateway. The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header. As with Transport mode, extended portions of the IP header are utilized with AH that are not included with ESP authentication, ultimately providing integrity only of the inside IP header and payload.

The inside IP headers Time To Live (TTL) is decreased by one by the encapsulating system to represent the hop count as it passes through the gateway. However, if the gateway is

the encapsulating system, as when NAT is implemented for internal hosts, the inside IP header is not modified. In the event the TTL is modified, the checksum must be recreated by IPSec and used to replace the original to reflect the change, maintaining IP packet integrity. During the creation of the outside IP header, most of the entries and options of the inside header are mapped to the outside. One of these is Type of Service (ToS),which is currently available in IPv4.[7]

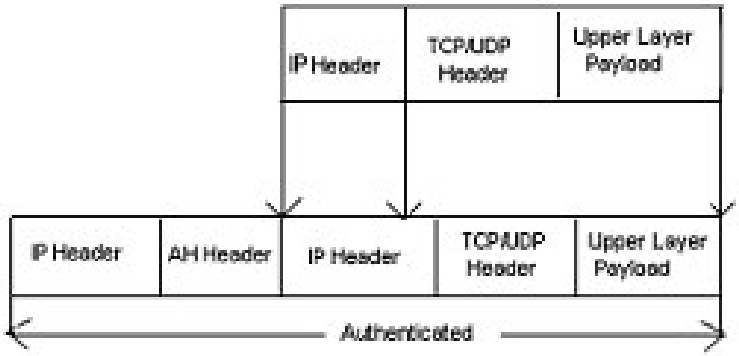


Figure 7. AH in Tunnel Mode

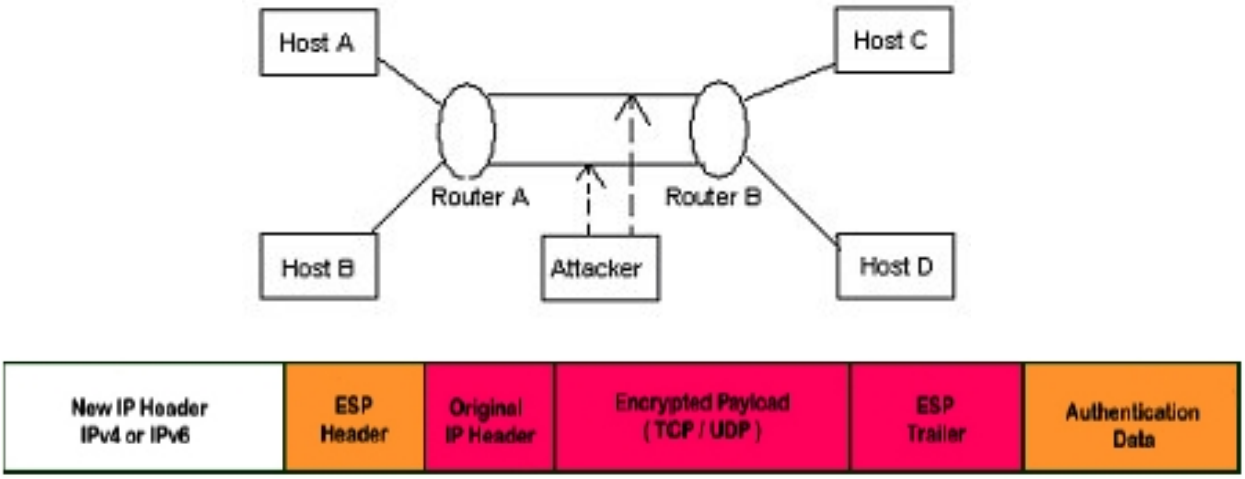


Figure 8. ESP in Tunnel Mode

III. IPSec vs. Other Layers Security

A solution to the Internet security problem exists. The key to understanding this solution lies in learning about the network layer in IP networks. To isolate problems that occur when networks are being constructed, it is useful to imagine a network as a series of layers. Each layer solves problems that are unique to that layer. Stated simply, an IP network has three layers: the physical layer, the IP network layer, and the application layer. Each layer provides services to the layer above it. The physical layer (the lowest level) consists of the

actual equipment: electrical cables, network cards, and/or radio links where information travels. In addition, the physical layer contains simple data-carrying protocols that provide an interface for higher level protocols. In an IP network, different parts of the network use different types of physical media – Ethernet in some places, point-to-point lines in others.

Above the physical layer, the network layer (the IP layer in IP networks and the level where IPSec operates) sends information from network node to network node across the whole network. The network layer uses the lower level protocols to move the data, and it uses its own routing logic to find the best subnets through which to send the data. Above the network layer are higher level protocols that set up links between nodes for different types of communications. Also above the network layer is the application layer where applications run. Applications use the capabilities of the network layer to determine how to move data from network node to network node. The network layer in turn uses the physical layer to move data from one computer's network card to the next.

The most important thing to remember about IP networks is that the network layer is entirely uniform. It is the only layer that is uniform. As a result, any communication going through an IP network (e.g., the Internet)
has to use the IP protocol. In other network layers, different protocols operate for different reasons (depending on the network's architecture and types of communication). However, eventually all communications have to go through the network layer, and for all IP networks there is only one protocol in that layer - IP. Consequently, if the IP (network) layer is secure, the network is secure The international group organized under the Internet Engineering Task Force (IETF) has developed a way to secure the IP layer. That method is called the IP Security (IPSec) protocol suite.

The IPSec protocol suite has a foundation of powerful new encryption technologies. The suite adds security services to the IP layer in a way that is compatible with both the existing IPv4 IP standard and the emerging IPv6 standard. Essentially, if the IPSec suite is used where IP is normally used (in the network layer), communications are secured for all applications and for all users more transparently than would be the case if any other approach was employed. With IPSec, a secure VPN can be built that is as secure as a private network. The incredible part is that the VPN resides on an unsecured, public network (e.g., the Internet). With IPSec, a secure VPN can be created as needed, on demand, and with any other device that is using the IPSec standard. Because IPSec works with both existing and future IP standards, regular IP networks can still be used to carry data. The sending device has to be IPSec-compliant, and the receiving device has to be IPSec-compliant, but the rest of the

network between the sender and recipient does not have to be IPSec compliant. The primary strength of the IPSec group's approach is that their security works at a low network level. As a result, IP is transparent to the average user, and IPSec-based security services are also not seen, functioning behind the scenes to ensure that all network communications are secure. IPSec's power and flexibility promise to make it the international standard. IPSec meets a broad range of security needs and allows different networks around the world to interconnect and to communicate securely. In addition, IPSec offers almost infinite scalability with transparent and reliable service, no matter how demanding a company's security needs.[14]

IV. Vulnerability of IPSec

One of the most urgent security problems facing administrators of networked computer systems today is the threat of remote attacks on their systems over the Internet, based on vulnerabilities in their currently running software. Particularly damaging have been self-propagating attacks, or "worms", which exploit one or more vulnerabilities to take control of a host, then use that host to find and attack other hosts with the same vulnerability. The obvious defense against such attacks is to prevent the attack by repairing the vulnerability before it can be exploited. Typically, software vendors develop and distribute reparative "patches" to their software as soon as possible after learning of a vulnerability. Customers can then install the patch and prevent attacks that exploit the vulnerability. Vulnerabilities in IPSec can be broken into following categories: [8]

IV.1. Cut-and-Paste Attack

This attack will only be possible on two networks that use IPSec as a tunnel between the two routers that link the networks. There is also a requirement that the attacker has access to a second machine in each of the two networks. The attack works by an attacker sniffing that is possible in Ethernet-based IP networks. Ethernet LANs make up a large part of most networks. Ethernet technology has the advantages of being cheap, universally available, well-understood, and easy to expand. It has the disadvantage of making sniffing easy. In most Ethernet LANs, packets are available to every Ethernet node on the network. Conventionally, each nodes network interface card (NIC) only listens and responds to packets specifically addressed to it. Its relatively easy, however, to put many Ethernet NICs in what is called promiscuous mode, meaning they can collect every packet that passes on the wire.

There's no way to detect such a NIC from elsewhere on the network, because the NIC doesn't do anything to the packets when it picks them up. A type of software colloquially called a sniffer, after the original network analysis tool designed to do this. Network General's

Sniffer can take Advantage of this feature of Ethernet technology. Such tools can record all the network traffic going past them. As such they are a necessary part of the tool kit of any network diagnostician working with Ethernets allowing them to determine quickly what is going through any segment of the network. However, in the hands of someone who wants to listen in on sensitive communications, a sniffer is a powerful eavesdropping tool. **[9,10]**

The attack works by an attacker sniffing a legitimate encrypted packet from Host A to Host B as in figure (9). Attacker also sniffs a planned packet sent from Host C to Host D. Attacker copies encrypted data from Host A's packet into a packet from Host C to Host D. Router B is tricked into decrypting Host A packet for Host B and sending it to Host D. This exploit is not as straightforward as it may appear, as there are some other requirements relating to the sequence numbers used in IPSec packets and ensuring that Host A genuine packets don't reach Router B before the false packets do. IPSec includes various replay-attack protection methods that would make this attack a little more difficult to successfully carry out in a real world situation.

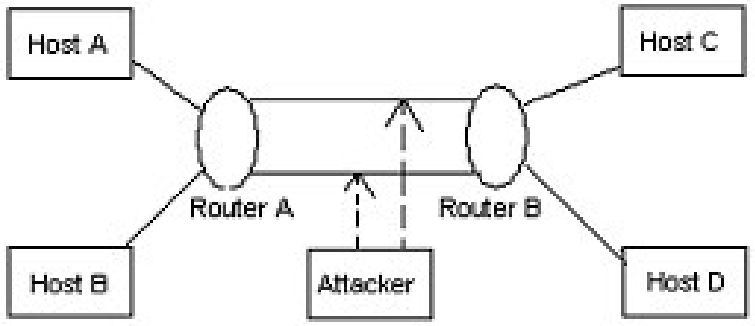


Figure 9. Cut-and-paste attack example

IV.2. Session Hijacking

Session hijack attacks are defined as taking over an active TCP/IP communication session without their permission or knowledge. This can occurs when someone takes over a TCP session between two machines. This can happen when an unauthorized user redirects the TCP stream through another machine, bypassing the protection offered by simple login, one-time password, or ticketing authentication systems such as Kerberos. Since most authentications occur only at the start of a TCP session, this allows the hacker to gain access to a machine. TCP connections are vulnerable to anyone with a TCP packet sniffer and generator located on the path followed by the connection. Session hijack attacks are usually waged against users that are members of large networks containing a substantial number of open sessions. Network protocols like FTP, Telnet, and rlogin are especially attractive to the

attacker, because of the session oriented nature of their connections, and the length of their communication sessions. Additionally, FTP, TELNET, and rlogin do not implement any security during logon, authentication, or data transmission. In fact, data sent using these protocols are sent in clear text which can be easily be viewed by anyone monitoring the network.

There are three different types of session hijack attacks: active, passive, and hybrid. The active attack is when the attacker hijacks a session on the network. The attacker will silence one of the machines, usually the client computer, and take over the clients' position in the communication exchange between the workstation and the server. The active attack also allows the attacker to issue commands on the network making it possible to create new user accounts on the network, which can later be used to gain access to the network without having to perform the session hijack attack.

Passive session hijack attacks are similar to the active attack, but rather than removing the user from the communication session, the attacker monitors the traffic between the workstation and server. The primary motivation for the passive attack is to provide the attacker with the ability to monitor network traffic and discover valuable data or passwords. The final type of session hijack attack is referred to as the hybrid attack. This attack is a combination of the active and passive attacks, which allow the attacker to listen to network traffic until something of interest is found. The attacker can then modify the attack by removing the workstation computer from the session, and assuming their identity. So, these are the types of attacks which can occur due to weaknesses in IPSec protocols. [9,11].

IV.3. IPSec is Not End-End

IPSec framework has been standardized for IP layer security while ATM cell encryption has been implemented in hardware to support Gigabit network traffic on the hand firewall vendor such as checkpoint has deployed solution for not only blocking unauthorized traffic in different protocol layers but also interacting in a limited sense with security management products such as intrusion detection through the IPSec protocol. so each of these security mechanisms may solve a particular problem and there is significant overlap among the security service they provide. IPSec can't provide end to end security because IPSec encrypts an IP connection between two machines that is different from encrypting messages between users or application. The trend now focus on development of individual security mechanisms and protocols to solve particular security problem.[12]

V. IPSec/Quality of Security Service

Quality of Security Service (**QoSS**) refers to the ability to provide *security* services according to user and system preferences and policies. This way security and security requests can be managed as a responsive “service” for which quantitative measurement of service “efficiency” is possible. The enabling technology for both QoSS and a security adaptable infrastructure is variant security, or the ability of security mechanisms and services to allow the amount, kind or degree of security to vary, within predefined ranges. IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPSec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

The set of security services that IPSec can provide includes access control, connectionless integrity, data origin authentication, rejection of replayed packets (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol. IPSec provides traffic security "through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. The set of IPSec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and or sites organizations.

When these mechanisms are correctly implemented and deployed, they ought not to adversely affect users, hosts, and other Internet components that do not employ these security mechanisms for protection of their traffic. These mechanisms also are designed to be algorithm-independent. This modularity permits selection of different sets of algorithms without affecting the other parts of the implementation. For example, different user communities may select different sets of algorithms if required. The IPSec mechanism provides services, including confidentiality, integrity and authenticity, through the establishment of Security Associations (SA) among the entities that wish to communicate. The SA is a simplex connection that affords security services to the traffic carried by it and it essentially is a management construct used to enforce a security policy in the IPSec environment. There is a set of parameters associated with each SA, which includes, among others: SA lifetime, encryption and/or authentication algorithms and keys, and protocol mode

(tunnel/transport). The SAs can be generated manually, but that approach does not scale well. The Internet Key Exchange (IKE) along with the Internet Security Association and Key Management Protocol (ISAKMP) address the problem of establishing and maintaining SAs through the use of an automated daemon.

The IPSec protocols themselves do not include an approach for managing the policies that control which host is allowed to establish SAs with another host and what kind of characteristics the SAs should have. We are using the Open BSD's implementation of IPSec. This implementation addresses the SA management problem by including a trust management system, Key Note, and providing an additional check in the IPSec processing it makes sure that the SAs to be created agree with a local security policy that can be expressed in the trust management system's language. When IPSec SAs are established between two entities wishing to communicate, they are used until their negotiated lifetime expires (if the SAs are not for some reason violently interrupted/discarded). But the characteristics of the negotiated SAs cannot respond to dynamic modifications of the environment's security requirements, for example they cannot adapt to changes in threat conditions, critical time transmissions, and network congestion/traffic.

To have a QoSS aware IPSec, we enable the IKE daemon to negotiate SAs, and enable the Trust Management System to enforce local policy for them, in accordance with the system's QoSS parameters (network mode, security level). Also if there is a change in a QoSS parameter, currently active SAs must be renegotiated to conform to the current set of security requirements as expressed by the local policy.[13]

VI. IPSec Future

Where do we go from here? IP version 4 has played a main role in the internetworking environments for many years, it has proved flexible enough to work on many different networking technologies and however it has become a victim of its own success - explosive growth, the heavy demands for new IP addresses; the lake of IPv4 addressing space was the basic problem. To solve the address exhaustion and other scalability problem the IETF (Internet Engineering Task Force) provide an optional new version of IP called IPv6 (also called IPng: IP next generation). IPv6 uses a 128 bit IP address made up at eight 16 bit integers separated by colons; IPv6 contains many new features including native security.

NGISec (New Generation Internet Security) provides “end-to-end secure communications in LANs, VPNs, and network-to-network connections”. NGISec, including use of IKE (Internet Key Exchange), and it allows reuse of the existing IPSec infrastructure,

aims to ensure compatibility with other protocols, specifically NAT, ICMP and QoS protocols, and to enable the end-host to perform the majority of encryption-related tasks, provides tunneling facilities and end-to-end encryption in a similar manner to client-implementation.

CONCLUSION

IPSec is an excellent set of protocols that need for transporting secure Communications in the Internet. The IP Security Protocol Working Group will develop these mechanisms to protect client protocols of IP. A security protocol in the network layer will be developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality. One of the most important things about the protocol suite is not its robust design, but the simple fact that it is an open standard and an Internet standard, so any number of vendors and service providers can specialize and cooperate to provide the total range of IPSec equipment and services you need.

IPSec at the network layer has certain advantages over other security layers but there are vulnerabilities in this powerful security tool. These weaknesses can be in the IPSec protocol suite. It can be avoided by having a comparative study of other technologies implemented within IPSec and choosing the best of them. There are further recommendations for implementing IPV6-IPSec while concerning things like IPSec/QoSS (Quality of Security Service), data compression with IPSec encryption and authentication for fast secure network transactions.

REFERENCES

[1] Eerikki Aula, " Better – Than – Nothing Security ", Tkk T-110-5290 Seminar on Network Security, 11/12 – 12 – 2006.

[2] " IP Security Protocol – Based VPNs ", White Paper From SANS Institute Reading Room Site,2001.

[3] Mohammad Heidari, " IPv6 Security Consideration ", 2004.

[4] Chien – Lung Wu and S.Felix Wu and Ravindar Narayan, " IPSec/PHIL(Packet Header Information List): Design, Implementation and Evaluation".

[5] " IPSec ",White Paper From Cisco System,1998.

[6] Tuomas Aura, Michael Roe, and Anish Mohammed, " Experiences With Host-to-Host IPSec ", Microsoft Research.

[7] Jim Tiller, Network Security Consultant, " IPSec Virtual Private Network : A Technical Review ", White Paper From NetworkCare, 2000.

[8] Helen J.Wang, Chuanxiong Guo, Daniel R.Simon, and Alf Zugenmaier, " Vulnerability-Driven Network Filter's For Preventing Known Vulnerability Exploit's ", Technical Report MSR-TR-2003-81 From Microsoft Corporation, February, 2004.

[9] " Vulnerability's of IPSec: A discussion of Possible Weaknesses in IPSec Implementation and Protocol " White Paper From SANS Institute Reading Room Site,2001.

[10] " Understanding the IPSec Protocol Suite ", Technical Paper from NewBridge Network, March, 2000.

[11] " Session Hijacking in Window's Network ", White Paper From SANS Institute Reading Room Site, October, 2008.

[12] Z.Fu, H.Huang, T.Wu, S.F.Wu, F.Gong, C.Xu, and I.Baldine, " ISCP: Design and Implementation of AN Inter-Domain Security Management Agent (AMA) Coordination Protocol ", Q-7803-5930-5 (c) IEEE, 2000.

[13] " Demonstration of Quality of Security Service Awareness for IPSec", white paper from the center for INFOSEC studies and Research, September, 2002.

[14] " IPSec", white paper from Information Resource Engineering.

[15] Jos´e Carlos Brustoloni, " Automatic VPN Client Recovery from IPSec Pass-through Failures", Supported in part by NSF ITR medium ANI-0325353.

CLASSIFICATION OF INFORMATION

Author:

Inga KAPLINA

INFORMATION CLASSIFICATION – WHO, WHY AND HOW

"Security of Information is the application of general protective measures and procedures to prevent detect and recover from the loss or compromise of information"

ABSTRACT

Many companies, governmental or military institutions consider initiatives like risk analysis and information classification. A number of studies have previously been conducted on keyword analysis in order to provide a comprehensive scheme to classify information systems (IS) research. However, this studies appeared prior with the emergence of areas such as electronic commerce, electronic government and numerous others. People have definitely already encountered information systems in many different areas of their lives (responsible for the publication test results, (in-) ability to withdraw money from the ATM and etc).

Many companies look to information technology support organizations to identify the information that should be protected, the level of protection what should be provided, as well as the technology solution.

This paper will clarify why information classification is necessary, efficient and effective means for information protection requirements. Last, it will offer a method for classifying information.

INTRODUCTION

WHY INFORMATION CLASSIFICATION IS IMPORTANT

WHAT IS INFORMATION SECURITY? We are sometimes asked the most basic of information security question of all: "What is information security?". This can actually be

surprisingly difficult to define. However, the introduction to the standard itself characterizes information security as the preservation of what is often known as CIA:

> **Confidentiality** - Ensuring that information is accessible only to those authorized to have access; (Protection of personal information. The Freedom of Information and Protection of Privacy Act (FOIP) and the Health Information Act govern the collection, use and disclosure of personal information. The FOIP Act also governs the management of personal information – its protection, retention, and accuracy. Security standards support the effective application of the Act in the conduct of day-to-day business.)
>
> **Integrity** - Safeguarding the accuracy and completeness of information and processing methods;
>
> **Availability** - Ensuring that authorized users have access to information and associated assets when required.

It further explains that "information security is achieved by implementing a suitable set of controls", and that these need to be "established to ensure that the specific security objectives of the organization are met".

Information is heart of today's businesses. Client databases, product definitions, e-mail stores and much more now support the around-the-clock demands of today's economy. IT organizations must have well executed plans in place to effectively manage and protect that data, both today and for the long term, to ensure their success and viability.

All the institutions all over the world need to protect their information today more than ever. The increasing need for protecting information is obvious. Signs are prevalent in the news, publications, and in the turn of recent business and world events. For example:

- Information technology has recently been selected as a weapon of choice for terrorists. The potential is there to cripple economy.
- The Internet is being used more and more for critical business transactions. It is common knowledge among business professionals that transacting business over the Internet without appropriate protection measures puts consumer and company information at considerable risk for fraud and theft.
- Some governmental regulations hold organizations responsible for implementing protection controls for information privacy, access, storage and exchange. Companies that don't comply can be assessed steep financial penalties.

All information, however, is not equal. Active and online data that has a particularly high value needs to be available at all times for rapid access by multiple organizations and applications. Some data requires 100 percent, instant accessibility around the clock, with no

tolerance for downtime. Some data is more valuable to certain organizations than it is to others. And some changes in value over time, while other data simply requires archiving for occasional access or long-term storage.

Understanding the value of data and thus how quickly it needs to be accessed and by whom - is fundamental to all elements of an information lifecycle management program.

WHAT IS DATA AND INFORMATION CLASSIFICATION

Search the Internet on data or information classification, and you'll find references among pages on security policy and risk management. Close examination of this information leaves one wondering where risk management begins and security policy and information classification end.

"A security policy is a high-level plan stating management's intent pertaining to how security should be practiced within an organization, what actions are acceptable, and what level of risk the company is willing to accept." [1] For example, an information security policy might state that risk analysis must be performed or company information must be classified. Considering their non-specific nature, information security policies should be viewed as the minimal requirement for fulfilling an organization's information protection responsibilities.

Data and Information Classification is the process that defines the performance and availability characteristics of an organization's different sets of data and recommends an appropriate storage technology that meets the needs of each classification.

Effective Data and Information Classification begins by establishing a goal for what you want to do with that data or information.

I. CHAPTER - SECURITY CLASSIFICATION

I.1. WHY MUST SOME INFORMATION BE CLASSIFIED?

Security research seeks to develop the technologies and knowledge for building capabilities needed to ensure the security of citizens from threats such as terrorism, natural disasters and crime, while respecting fundamental human rights including privacy; to ensure optimal and concerted use of available and evolving technologies to the benefit of civil security, to stimulate the cooperation of providers and users for civil security solutions, improving the competitiveness of the security industry and delivering mission-oriented research results to reduce security gaps.

Some of the information produced throughout these projects could also potentially be exploited by adversaries. Vulnerability analyses, comprehensive accounts of previous incidents or detailed knowledge about the design, operation and capabilities of countermeasures all represent information which could be utilized by opposing forces to plan terrorist attacks or avoid detection of criminal activities. Information is assigned a security classification when its unauthorized disclosure could reasonably be expected to adversely impact the security of citizens.

However, the classification of information also precipitates related costs, in terms of administrative arrangements, limits on the dissemination of research outcomes, restrictions on the freedom of information for citizens and potential judicial consequences in case of compromise. Therefore information should be classified when the potential consequences of its unauthorized disclosure warrant the costs of its protection.

II. CHAPTER - CLASSIFICATION LEVELS

II. 1 - ESTABLISHING INFORMATION CLASSIFICATION CRITERIA

It is essential to classify information according to its actual value and level of sensitivity in order to deploy the appropriate level of security. A system of classification should ideally be:

- simple to understand and to administer
- effective in order to determine the level of protection the information is given.
- applied uniformly throughout the whole organization (note: when in any doubt, the higher, more secure classification should be employed).

With the exception of information that is already in the public domain, information should not be divulged to anyone who is not authorized to access it or is not specifically authorized by the information owner. Violations of the Information Classification Policy should result in disciplinary proceedings against the individual.

It is also sensible to restrict the number of information classification levels in your organization to a manageable number as having too many makes maintenance and compliance difficult. The following five levels of classification cover most eventualities:

Top Secret:

Highly sensitive internal documents and data. For example, impending mergers or cquisitions, investment strategies, plans or designs that could seriously damage the organization if lost or

made public. Information classified as Top Secret has very restricted distribution indeed, and must be protected at all times. Security at this level is the highest possible.

Highly Confidential:

Information which is considered critical to the organization's ongoing operations and could seriously impede or disrupt them if made shared internally or made public. Such information includes accounting information, business plans, sensitive information of customers of banks (etc), patients' medical records, and similar highly sensitive data. Such information should not be copied or removed from the organization's operational control without specific authority. Security should be very high.

Proprietary:

Procedures, project plans, operational work routines, designs and specifications that define the way in which the organization operates. Such information is usually for proprietary use by authorized personnel only. Security at this level is high.

Internal Use Only:

Information not approved for general circulation outside the organization, where its disclosure would inconvenience the organization or management, but is unlikely to result in financial loss or serious damage to credibility/reputation. Examples include: internal memos, internal project reports, minutes of meetings. Security at this level is controlled but normal.

Public Documents:

Information in the public domain: press statements, annual reports, etc. which have been approved for public use or distribution. Security at this level is minimal.

Care should always be applied regarding a user's possible tendency to over classify their own work. It can sometimes be erroneously surmised that the classification level can reflect directly on the individual's own level of importance.

III CHAPTER - HOW IS INFORMATION CLASSIFIED?

III.1 - METHODOLOGIES

Conventionally, the classification of information is attained through the use of a risk assessment methodology which quantifies the protection (confidentiality) requirements of a document and the financial, personal, operational and/or society harm which would be generated by its unauthorized disclosure. There are many ways to implement an information classification system. Except for the military, there are no set formulas. The key is to facilitate

employee compliance of company endorsed information protection measures. To successfully implement information classification, a company must transition from recognizing that it should classify its data to recognizing that it can. Toward that end, this paper will demonstrate a six-step, common sense approach to data classification, assembled from recurring suggested activities and supporting concepts encountered throughout research.

III.2 - IDENTIFY ALL INFORMATION SOURCES THAT NEED TO BE PROTECTED

Common approaches for gathering data include written surveys, questionnaires and personal interviews. One research source also proposed the use of an expert system for information classification. (This idea sounded promising until follow-up research revealed no vendor offerings tailored to information classification.) If information sources haven't been compiled for other initiatives, the best sources might be developers, operating system and database administrators, business champions, and departmental and senior managers. During the information gathering process, consideration should be given to how recent trends in distributed computing and widespread use of desktop productivity tools might challenge the identification (and consistent protection) of information in its various forms.

Completion of this step should produce a high level description of information sources, where the data resides, existing protection measures, data owners (i.e., individuals responsible for establishing policy), data custodians (i.e., individuals responsible for maintaining the information), and the type of resource (i.e., file, application, backup tape).

Information can be listed separately or can be grouped when the same set of protection measures apply to the group, also referred to as a domain. Four common domains are: geography, organization, technology, or application lifecycle. Examples where domain level classes might apply are similar operating systems or all applications under development that don't need to be recovered immediately.

The information identified in this initial stage will be expanded and made more granular in subsequent steps and iterations. Attachment 1 provides examples of information sources initially identified in Step 1. (attach. 1)

Having compiled all known sources of information, the next step is to identify desired protection measures.

IV CHAPTER - TYPES OF INFORMATION

While these categories are not exhaustive, they do constitute a comprehensive representation of the types of information produced by projects. Further, while some overlap may

undoubtedly exist between these denominations, the differences between the types of information are generally sufficient to identify which category specific deliverables pertain to.

IV.1 *Threat Assessment*

A threat assessment estimates the likelihood of a malicious act against an asset, with particular reference to factors such as intention, capacity and potential impact.

IV.2 *Vulnerability Assessment*

A vulnerability assessment identifies gaps or weaknesses in networks, services, systems, assets, operations or processes which can be exploited during malicious acts, and often contain suggestions to eliminate or diminish these weaknesses.

IV.3 *Specifications*

Specifications information refers to exact guidelines on the design, composition, manufacture, maintenance or operation of threat substances or countermeasure substances, technologies and procedures.

IV.4 *Capabilities*

Capability describes the abilities of an asset, system, network, service or authority to fulfil its intended role. Capability refers in particular to the capacity of units, installations, systems, technologies, substances and personnel charged with security-related functions to carry these out successfully.

IV.5 *Incidents/Scenarios*

Incidents/Scenarios concern the provision of detailed information on real-life security incidents and potential threat scenarios. Reports on past incidents may include details not otherwise publicly available, and may demonstrate the real-life effects of particular attack methods, yet they may sometimes refer to security gaps which have since been addressed. In contrast, devised scenarios are commonly derived directly from existing vulnerabilities, yet these may contain a lower level of detail, particularly of the attack preparation phase.

IV.6 *Time dimension: reclassification/declassification*

The temporal limitations to be placed on the classification of information pertaining to the various types of information and specific subject areas has to be setup on a case by case basis with Commission's service.

These temporal limitations may involve a reclassification (upgrade or downgrade), declassification or extension of the duration of the current classification of the classified information.

IV.*7 Widening of the dissemination*

Taking into account the rules laid down in Commission Decision 844, the widening of the dissemination of classified project deliverables may be possible to entities not foreseen at the start of the research even if these entities are located in Third Countries, provided that the European Union has a security agreement with the Third Country in question. This extension of the dissemination will be evaluated on a case-by-case basis, and will be subject to a justifiable need-to-know, as well as to the existence of the necessary security measures in accordance with the relevant security agreement.

V CHAPTER – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SECURITY FRAMEWORK

In today's world, threats to the security of information and information technology assets are constant. The ICT Security Framework establishes a comprehensive plan to enable these assets from disruption, unauthorized access or corruption of the electronic information. This information security classification is consistent with the ICT Security Framework. Supporting this framework are security policies, security architecture, technical standards and documents of best practices.

VI CHAPTER – INFORMATION SECURITY CLASSIFICATION IN PRACTICE

Implementing information security classification will mean that all institutions should consider practices related to:

- labeling information assets;
- storing information;
- transmitting information;
- disposing of unneeded information;
- protecting the integrity of information;
- allowing appropriate access and disclosure; and

- establishing accountability

This section provides examples of practices in these areas. The practices identified are not intended to be prescriptive. It is unlikely that they will implement security classification to all information assets at the same time. Rather, the timing of applying information security classification will be based on the result of a threat and risk assessment and may very well be tied to the implementation of Electronic Information Management (EIM) technology. The actual practices that are implemented will depend on the business reason for applying security classification as well as established administrative protocols (in the case of print information assets) and information technology protocols (in the case of electronic information assets).

VI.1 LABELING INFORMATION ASSESTS

Implement standard security labels for information assets. The actual labeling procedure will vary depending on the medium in which the information is stored. Table 2 identifies some common labeling methods for various types of information assets.

Table 1 - Sample Labelling Methods

Type	Procedure
Hard copy documents	Rubber ink-stamps for each level may be needed to mark hardcopy documents received from outside the organization
Electronic mail	Identify security classification in subject line of e-mail, if classified as confidential, or restricted
Electronic documents	Identify security classification in document metadata. If the electronic document is to be printed or viewed in pdf format, the security classification should appear on every page, including the cover page (this can be done by including the classification in the header/footer or by use of a watermark). Information about the ministry or department which created the document and date of creation should be included

Data, databases and business applications	Identify classification in system/application metadata. Labels may be required for online screen displays and reports generated by IT systems
Other media	The security classification may be identified on adhesive labels applied to other media such as diskettes, CDs, DVDs, and videocassettes. A message with the classification label should be displayed when the information stored on the media is accessed

VI.2 STORING INFORMATION

Depending on the security classification, information assets will need different types of storage procedures to ensure that the confidentiality, integrity, accessibility, and value of the information are protected.

Table 2 - Identifies storage procedures for printed and electronic information in the various classification categories.

Classification	**Print/Hard Media**	**Electronic Files**
Unrestricted	No special storage requirements	No special storage requirements Regular back-ups to ensure availability and integrity
Protected	Secure location (e.g., locked office; locked file room)	All media under physical and/or logical access control of protected zone (e.g. group authorized access)
Confidential	Secure location with restricted access;	All media under physical and/or logical access control of confidential zone (e.g., authorized access and authenticated access)

	Clean desk policy	
Restricted	Stored in highly secure zone, with access tracking; Clean desk policy; Audit trail for all access points (e.g., signatures)	All media under physical and/or logical access control of restricted zone (e.g., singled or double authentication, encrypted data, audit and monitoring)

NOTE: Various classes of information located in one common medium/location should have the highest classification of all information located in the medium. This is important to ensure that highly classified information is not put at risk. Physical security of any media should include fire/flood/theft protection.

VI.3 TRANSMITTING INFORMATION

When transmitting information that is protected, confidential or restricted, special procedures will be needed. Examples of these procedures are identified in Table 3. The following policies on the transmission of protected, confidential and restricted information are also applicable: Information Technology Baseline Security Requirements Policy on the Transmission of Personal Information via Electronic Mail or Facsimile and Information Technology Baseline Security Requirements

Table 3 - Sample Transmission Procedures

Classification	**Print/Hard Media**	**Electronic Files**
Unrestricted	No special procedures	No special procedures
Protected	Sealed envelope; First class mail	If electronic message contains personal information, personal information must be transmitted in such a way to prevent interception, modification, or unauthorized receipt en route or at the destination (e.g.,

		password protected file; encryption; personal information sent in separate e-mail)
Confidential	Sealed envelope, stamped confidential; Receipt confirmation required;	Message sent in such a way to prevent interception, modification, or unauthorized receipt en route or at destination; Recipient confirmation required; Audit of access points (suggested);
Restricted	Tamper evident packaging (e.g. double-sealed envelope with inside envelope signed to revealed evidence of tampering)	Message sent in such a way to prevent interception, modification or unauthorized receipt en route or at destination (e.g., encryption used to send/authenticate message); Complete audit trail of each access point;

VI.4 – SECURE DISPOSAL OF INFORMATION

Confidential electronic and paper information must be disposed of securely to minimise the risk of unwanted disclosure. Staff must be sure to handle information securely. Achieving and demonstrating good standards of information handling is particularly important to the research interests.

Confidential information is information which if improperly disclosed or lost could cause harm or distress. This includes personal data as defined by the Data Protection act, i.e. information about a living individual where that individual could be identified, and other valuable or sensitive information not in the public domain.

When disposing of information in electronic form precautions must be taken when control of a device that may have information stored locally is to be reassigned to someone else. (Such devices include: computers, mobile phones, USB drives, cameras, rewritable CDs/DVDs etc.) When devices that store confidential information are to be repaired, then that information should first be removed. However, if removal of the information prior to repair is not possible the work should be carried out by a company subject to a suitable agreement. In general, locally installed licensed software should be removed from IT equipment before disposal or transfer of control. Equipment must be kept in a secure location until collected. Where it is considered necessary to be extra-careful then a secure deletion tool should first be

used before collection. Departmental procedures must ensure that locally stored confidential information is removed as appropriate before a device is reassigned to another person. This should be done routinely at the time the device is returned using a secure file or drive level deletion tool. Not doing so may breach the terms of the licence.

The standard method of deleting a data file, on many types of system, may leave its contents recoverable. This is helpful if a mistake has been made, however, it is insecure if the intention is to prevent anyone else being able to "un-delete" and read the file. (Tools for recovering files deleted in the standard way are available for various systems.)

Entire PC hard drives can be "securely wiped", such that the data is made unrecoverable, using a free utility such as "Boot and Nuke". Specific files and folders can be deleted under Windows using the free tool "SDelete". These tools can be downloaded from the Internet.

Dispose of unwanted paper documents that do not contain any confidential information by recycling. Where documents contain confidential information, assess whether the disclosure of the information could cause harm. If so, or if you are uncertain, place the documents in a shredding bag and store the bag securely until it is collected for shredding.

VI.5 Protecting the classified of information

Confidentiality, Integrity, Availability: The three components of the CIA Triad

Integrity refers to the fact that information is current, complete, and only authorized changes are made to it. The integrity of information processed by and stored in information systems can be addressed by assigning the appropriate rights (e.g., read only, modify). If the threat to the integrity of information is significant, electronic files should be saved as read only files with changes to be made only by the author (this may be handled by access rights based on user account, work group or physical access to a specific devise). In these cases, procedures should be in place for transfer of rights when the author leaves the organization. In some cases, stronger control such as encryption may be required. If encryption is used, a process related to key escrow must be established to ensure the availability of the information. What is the CIA triad? CIA refers to Confidentiality, Integrity and Availability - Confidentiality of information, integrity of information and availability of information. Many security measures are designed to protect one or more facets of the CIA triad.

VI.5.1 **Confidentiality**

When we talk about confidentiality of information, we are talking about protecting the information from disclosure to unauthorized parties. Information has value, especially in today's world, e.g. bank account statements, personal information, credit card numbers, trade secrets, government documents and others. Every one has information they wish to keep a secret. Protecting such information is a very major part of information security.

A very key component of protecting information confidentiality would be encryption. Encryption ensures that only the right people (people who knows the key) can read the information. Encryption is VERY widespread in today's environment and can be found in almost every major protocol in use. A very prominent example will be SSL/TLS, a security protocol for communications over the internet that has been used in conjunction with a large number of internet protocols to ensure security.

Other ways to ensure information confidentiality include enforcing file permissions and access control list to restrict access to sensitive information.

VI.5.**2 Integrity**

Integrity of information refers to protecting information from being modified by unauthorized parties. Information only has value if it is correct. Information that has been tampered with could prove costly. For example, if you were sending an online money transfer for $100, but the information was tampered in such a way that you actually sent $10,000, it could prove to be very costly for you.

As with data confidentiality, cryptography plays a very major role in ensuring data integrity. Commonly used methods to protect data integrity includes hashing the data you receive and comparing it with the hash of the original message. However, this means that the hash of the original data must be provided to you in a secure fashion.

VI.5.3 Availability

Availability of information refers to ensuring that authorized parties are able to access the information when needed. Information only has value if the right people can access it at the right times. Denying access to information has become a very common attack nowadays. Almost every week you can find news about high profile websites being taken down by attacks. The primary aim of attacks is to deny users of the website access to the resources of the website. Such downtime can be very costly. Other factors that could lead to lack of availability to important information may include accidents such as power outages or natural disasters such as floods.

How does one ensure data availability? Backup is key. Regularly doing off-site backups can limit the damage caused by damage to hard drives or natural disasters. For information services that is highly critical, redundancy might be appropriate. Having a off-site location ready to restore services in case anything happens to your primary data centers will heavily reduce the downtime in case of anything happens.

VI.6 Allowing appropriate access and disclosure

Certain types of information will require controlled access and logs to track access and disclosure activities. Table 4 outlines the access restrictions and any special audit trail that should be maintained.

Table 4 - Allowing Appropriate Access and Disclosure

Classification	**Access Restrictions**	**Audit/Activity Files**
Unrestricted	Open to the public and all employees, contractors, sub-contractors and agents	None
Protected	Authorized access (employees, contractors, sub-contractors and agents) on a "Need-to know" basis for business related purposes	Periodic audits to show protection is, in fact, occurring
Confidential	Limited to individuals in a specific function, group or role	Pre-clearance based on position or contractor, sub-contractor or agent relationship; Log of access/actions; Periodic audits of adequate protection;
Restricted	Limited to named individuals (positions)	All access or actions will be logged and subject to non-repudiation processes as appropriate

VI.7 Establishing accountability

A clear accountability regime for all personnel will be important to ensure the protection of information assets. Accountability is nothing to fear. Some see it as just a strategy to monitor people's performance or to teach people to be more self reliant in the performance of their job. In reality, it is a powerful tool that can help to avoid mistakes. Accountability brings employees past the place of knowing how and why they do their jobs to a realization of how what they do fits into the bigger picture.

To build accountability first of all it should be defined the areas that need accountability. Accountability is a tool that can easily be customized to needs and adjusted as things change over time.

Generally, any sharing of classified information will involve:

- security clearances for individuals who have access to classified information;
- a Memorandum of Understanding related to access, use, disclosure of the information;
- appropriate security safeguards for handling classified in formation (e.g., labelling, storage, transmission);
- education and training of individuals with access to ensure requirements are met.
- not disclose, release or provide access to the information to a third party;
- implement procedures necessary to prohibit publicity concerning the existence of any sensitive information ;
- maintain accountability and control procedures to manage the dissemination of, and access to the information.

CONCLUSIONS

This Information Security Classification guidelines have been developed by the various institutions to assist in establishing effective security classification practices. The objectives of the guideline are to:

- ensure personal information and confidential information are protected from unauthorized use and disclosure;
- protect the intellectual property of the Government of Alberta;
- facilitate the identification of information to support routine disclosure and active dissemination of information;

- facilitate the sharing of information with other jurisdictions to support e-government and integrated service delivery;
- ensure information shared between the institutions for public safety is adequately protected.

Implementing the Security Classification - Implementing information security classification will mean that they need to consider and implement appropriate practices related to:

- labeling information;
- storing information;
- transmitting information;
- disposing of unneeded information;
- protecting the integrity of information;
- allowing appropriate access and disclosure; and
- establishing accountability.

In cases where information has been classified in the national interest (i.e., Confidential, Secret, Top Secret), there are special requirements to satisfy the security policy. These include requirements for security screening of employees, specific handling requirements.

Finally, he CIA triad is a very fundamental concept in security. Often, ensuring that the three facets of the CIA triad is protected is an important step in designing any secure system. However, it has been suggested that the CIA triad is not enough. Alternative models such as the Parkerian hexad (Confidentiality, Possession or Control, Integrity, Authenticity, Availability and Utility) have been proposed. Other factors besides the three facets of the CIA triad are also very important in certain scenarios, such as non-repudiation.

- Classification: The Cornerstone for Successful Information Lifecycle Management
- Data Classification is PERSPECTIVE
- Protecting
- Responsibilities
- Policy

ATTACHMENT 1 – Page 1

Step 1 - Identify all information sources that need to be protected					
Information Source	Information location	How information is protected now (access approvals needed, monitoring, backups)	Data Owner (persons who know value of information to company)	Data Custodians (persons responsible for safeguarding information)	Format of the information (database, file, application)
Customer Database	Windows1	. Must log in; · Access given per job function; · Monitoring?	Customer Service VP	· Database Admin; · Security Admin;	Database
Product Database	Unix1	· Manager approves access	Customer Service VP	· Database Admin; · Security Admin;	Database
Financial Database	Unix2	· Must log in · CFO approves access · Monitoring?	Controller	· Database Admin; · Security Admin;	Database
HR Database	Unix2	· VP of HR approves access · Backup?	HR VP	· Database Admin; · Security Admin;	Database
Customer/ Product Admin Application	Web1	· Manager approves access	Customer Service Manager	· Web Support; · Customer Service;	Web

TTACHMENT 1 – Page 2

Step 1 - Identify all information sources that need to be protected					
Information Source	Information location	How information is protected now (access approvals needed, monitoring, backups)	Data Owner (persons who know value of information to company)	Data Custodians (persons responsible for safeguarding information)	Format of the information (database, file, application)
Accounts Payable Application	Web2	· Manager approves access · Monitoring?	AP Manager	· Web Support	Web
Accounts Receivable Application	Web2	· Manager approves access · Monitoring?	AR Manager	· Web Support	Web
Payroll	Web2	· Manager approves access · Monitoring?	Payroll Manager	· Web Support	Desktop
Privileged account passwords	Various systems and databases	· Encrypted · Manager approves · Access based on job function · Event monitoring	System and Database Support Administration	· ?	System
Word and Excel Files	Fileserver1	· Don't know	Employee	· Windows Support · Security Admin	Documents
Business Partner X customer list	Customer Database	· Product Management can see but cannot be published to customers or employees.	Product Manager	· ?	Data in a database

REFERENCES

1. Dod Information Security Program: Protection of Classified Information, N5200.01, Vol.3, 24.02.2012, 19.03.2013;
2. SANS Institute, InfoSec Reading Room
3. EU Guide for classification of information emanating from Security research, 11.07.2013
4. EMC^2 Where information lives; Data Classification: The Cornerstone For Successful Information Lifecycle Management, 2003
5. Discovering Information Systems , Jean-Paul Van Belle, Mike Eccles, Jane Nash
6. Information assurance services, University of Leicester
7. IT SECURITY COMMUNITY BLOG
8. Information Management, Alberta, Canada

CYBERTERRORISM

Author:
CPT. Cristian RIZEA

Introduction

Cyberterrorism, whether targeting the Internet or conducted by means of the Internet, represents a serious threat, since many essential aspects of today's society are completely dependent upon the functioning of computer systems. When analysing this threat and evaluating legal responses, it is necessary to distinguish among three phenomena:
(a) *attacks via the Internet* that cause damage not only to essential electronic communication systems and the IT infrastructure but also to other infrastructures, systems, and legal interests, including human life;
(b) *dissemination of illegal content*, including threatening with terrorist attacks; inciting, advertising, and glorifying terrorism; fundraising for and financing of terrorism; training for terrorism; recruiting for terrorism; and dissemination of racist and xenophobic material; as well as
(c) *other logistical uses of IT systems* by terrorists, such as internal communication, information acquisition, and target analysis.

The *existing international conventions* and other instruments that promote the harmonization of national substantive and procedural law and international co-operation are applicable to these misuses of the Internet for terrorist purposes: The computer-specific provisions of the Council of Europe's Cybercrime Convention that address national substantive law, national procedural law, and international co-operation can be used in cases of terrorism. Furthermore, the substantive and procedural rules as well as the rules on international co-operation found in international instruments on terrorism, on money laundering and financing of terrorism, and on general mutual assistance and extradition are also applicable in the cyberterrorism context. As a result, the basic question to be addressed – that of the existence of „terrorist-specific"

gaps in „computer-specific" conventions and „computer-specific" gaps in „terrorist-specific" conventions – can be answered in the negative as far as the application of the conventions is concerned.

The confirmed applicability of existing international instruments in the cyberterrorism context thus limits future consideration to the second question to be addressed, namely, whether the aforementioned „computer-specific" and „terror-specific" instruments have *general gaps*, i.e., gaps that are not specific to the use of the Internet for terrorist purposes. A comprehensive answer to this second question, which would require an in-depth analysis of all legal issues arising both in the cybercrime as well as in the terrorism context, exceeds the scope of this paper. However, an analysis of the main problems that arise in the context of cyberterrorism leads to the following evaluation and recommendations:

(a) A serious problem common to *all existing international instruments* is the insufficient number of states parties. This is especially true with respect to the Cybercrime Convention and the Convention on the Prevention of Terrorism, the two most important international instruments for fighting cyberterrorism and other terrorist use of the Internet. Therefore, signing, ratification, and implementation of these two conventions should be supported, and any additional courses of action undertaken in this context should be carried out in such a way as to avoid hindering or distracting from this process.

(b) The *Convention on the Prevention of Terrorism* – and its catalogue of offences, in particular – must be examined for provisions in need of amendment. At present, serious threats to commit terrorist acts are not adequately covered either by this Convention or by other Council of Europe conventions, and this deficit is not fully compensated by the instruments of other international organisations. Considering the effects of threats to commit terrorist acts, there is a need for action in this area – possibly in the form of a protocol to the Convention.

(c) The *Cybercrime Convention* should be evaluated with regard to its ability to cover newly emerging or newly discussed technical advances, particularly in the area of forensic investigative techniques (such as online searches or the use of key logger software). In the fast-paced, technical environment of cybercrime, such evaluations, which frequently lead to revisions and updates, are an absolutely normal process, especially when dealing with high risks such as those posed by terrorism. Should a decision be taken to supplement the Cybercrime Convention with a follow-up protocol addressing new investigative techniques, the possibility of excluding the political exception clause for some of the Convention's offences – especially in serious cases of data and system interference – might also be considered.

An additional provision dealing with serious attacks on IT-based or general infrastructures is not essential. It would suffice for countries to make sure that their domestic statutes on data and system interference provide sanctions appropriate for cases involving terrorist attacks against computer systems. Indeed, such „effective, proportionate and dissuasive sanctions" are already required by the Cybercrime Convention, and it can be left to the national legislatures to achieve this result by means of sentencing rules, aggravated offences on data interference, or infrastructure offences.

(d) *New international efforts* should focus on the development of repressive and preventive measures that target the dissemination of illegal content on the Internet and that are both effective and respectful of civil liberties. This could be done either with a special focus on illegal terrorist content or in a more general way that would encompass other types of illegal content as well. As far as the substantive law is concerned, this would also require harmonized rules regarding the responsibility of Internet providers. These rules could then serve as the basis for international notice and takedown procedures. The necessary developments in the areas of criminal procedure and international co-operation will require specific regulations that are based on technical control mechanisms in the Internet and that do not unduly inhibit the free exchange of information. The Council of Europe, with its long tradition of balancing security interests in criminal matters with the protection of human rights, would be the ideal institution to tackle the difficult problems posed by the development of such international standards and procedures for regulating illegal content in computer networks. Due to the global nature of the Internet and its strong resistance to national control mechanisms, an initiative in this area could even lead to new forms of co-operation that might recognize the global cyberspace as a common heritage of mankind, a heritage in need of new mechanisms of governance implemented by new institutions.

I. Threat Analysis: Use of the Internet for Terrorist Purposes and Cyberterrorism

The threat that is posed by terrorist use of the Internet is the subject of an ongoing controversial discussion. While some authors claim that, to date, not a single instance of cyberterrorism has been recorded, others argue that terrorists already routinely make use of the Internet. One reason for these differences in opinion is that neither terrorism nor cyberterrorism[1] is a well-defined term. Instead, definitions of cyberterrorism[1] range from

[1] *B. Foltz*, Cyberterrorism, computer crime, and reality, Information Management & Computer Security, 15.03.2004, Vol. 12, No. 2, pp. 154-166; *M. Conway*, Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet, First Monday, 04.11.2002, Vol. 7, No. 11; *M. Gercke,* "Cyberterrorismus" – Aktivitäten terroristischer Organisationen im Internet, CR 2007, pp. 62-68 (63).

common use of the Internet by terrorists (e.g., sending emails) to real criminal cases involving either virtual or physical losses. The specialists will not be able to provide an extensive definition. Instead, based on a broad working hypothesis of terrorism, they can give an overview of use that terrorists can make of the Internet.

To achieve this goal, it is not sufficient merely to analyze current cases of cyberterrorism or terrorist use of the Internet. Instead, it is necessary to identify possible targets, risks, and other forms of terrorist Internet use. The threat analysis in this chapter is therefore based on an analysis of cybercrime- and cyberterrorism literature as well as on specialized security reports and everyday news reports. This broad approach was chosen to obtain an expanded view, not only of the real occurrences of cyberterrorism and other uses of the Internet, but also of possible future forms of utilization.

The most commonly discussed use is a terrorist attack carried out via the Internet. Such an attack could be directed either at other IT-infrastructures, such as computers, servers, and routers or at objects in the „physical world," such as buildings, planes, trains, or even human life (part A.). Apart from such IT-based attacks, terrorists can use the Internet to disseminate content to the public. Since Internet connections are widely available and offer various advantages over conventional communication, terrorist organisations can put them to use: for example, to communicate with the public in order to present terrorist point of views or disseminate threats, to find new supporters, and/or to distribute information to followers. Finally, the Internet can also be used for other purposes. Not only does it enable terrorists to engage in confidential communication among themselves, it also contains a multitude of information that was hard to obtain in former times. Satellite images and construction plans – even for complicated designs – are freely available through the Internet. Therefore, the Internet as a planning instrument and as a tool for internal communication and preparation will be another focus in the following analysis of threats posed by terrorists and their use of the Internet.

1. Attacks via the Internet

The Internet is just as available for terrorists and terrorist organisations as it is for anybody else. In addition, cybercrime, i.e., criminal acts committed with the help of computer networks, has been common since the early days of computer technology. Therefore, the possibilities cybercrime has to offer can also be committed with a terrorist intent. Terrorists, however, have not yet claimed responsibility for any concrete acts. Additionally, the digital traces often do not allow investigators to determine whether the reason for the breakdown of a system was a mere system failure or the result of a purposeful attack. Even if an attack seems

highly likely, it is not possible to determine with certainty whether it was the result of the purposeful aggression of a terrorist group or an arbitrary experiment by a ten-year-old schoolgirl who tried out a program she found while browsing the Internet. For this reason, some authors have claimed that, up to now, not a single instance of cyberterrorism has been recorded.[2]

However, the threat of cyberterrorism and the other uses terrorists could make of the Internet do not remain either unreal or unrealistic. Since information on how to manipulate or misuse Internet services is widespread and often publicly available, not only security specialists but also terrorist organisations can gather such information and put it to use. Furthermore, the use of Internet-based attacks would seem to be highly attractive for terrorist purposes for the following reasons:

– Attacks can be launched from anywhere in the world. An Internet connection is available at most locations or can be initiated from most up-to-date mobile phones;

– Attacks are quick. Especially in cases of Distributed Denial-of-Service (DdoS) attacks, but also in many other scenarios, the attacker is not dependent on a fast Internet connection. Instead, he or she can exploit the connection speed of the victim. Worms and viruses can spread at the fastest possible rate without the need for any further involvement of the attacker;

– Since actions on the Internet can be disguised by anonymizing services or using similar camouflage techniques, in many cases it is extremely difficult to trace evidence back to the true perpetrator;

– Finally, use of the Internet is cheap. In most cases, only a small bandwidth connection is needed, which is highly affordable in most countries. Damage that can be caused via the Internet, however, an be very costly: IT-experts need to be involved constantly in order to fix newfound security flaws, and, if cases involve physical damage as well, these costs are additionally incurred.

In the following two parts, IT-based attacks will be analyzed in more detail. Next part will cover attacks on IT-infrastructure. The aim of such assaults can either be to gather protected information or to sabotage the system or data contained within the attacked system. Another aim can be to manipulate a physical infrastructure whose operation is controlled by an IT-system. Part 3 will deal with IT-based attacks that threaten human life. As explained above, these scenarios are discussed in the literature as possible threats or have already become known to the public as actual incidents. However, in most – if not all – of these cases, it is not known whether *terrorists* have also made use of these possibilities. So, to a certain extent, it is

---

[2] *U. Sieber,* The Threat of Cybercrime, in: Council of Europe (ed.), Organised Crime in Europe, Strasbourg 2005, pp. 81-218 (173).

necessary to speculate on which possibilities terrorist organisations would have if they were to accumulate knowledge themselves – or if they were able to hire security specialists to launch such attacks on their behalf.

2. Attacks on Infrastructure

The first group of attacks consists of those directed against infrastructure. In general, IT-based attacks are directed against other IT-infrastructures, resulting in a violation of IT-systems or –data. However, since an IT-infrastructure often controls other (physical) infrastructures, these digital attacks can have an effect on „real world objects" as well. These attacks are basically the same as those launched by „common" cybercriminals, but with a terrorist interest or intention.

a) Aims and objectives

When looking at the aims pursued by terrorist attacks on an IT-infrastructure, various objectives can be distinguished:

– By circumventing security measures, attackers can corrupt the *integrity* and *confidentiality* of computer systems and data;

– By rendering systems useless, a loss of *availability* can be caused. This can lead to serious results, especially if mission-critical IT-systems are affected;

– Finally, if IT-systems are connected to other critical infrastructures, such as transportation, power, or water facilities, *physical harm* apart from a loss of integrity of the system itself can be the result.

However, these are only primary objectives. In contrast to a common hacker or cybercriminal, a terrorist typically takes a long-term perspective. In order to achieve his or her goals, a terrorist pursues an underlying agenda when committing attacks on IT-systems. Upon a closer look, three different aims can be identified: the causing of economic confusion, the discrimination of the opponent, and the generation of monetary income for the terrorist organisation. Economic confusion and the discrimination of the opponent both aid in establishing the aforementioned long-term goal, whereas the generation of monetary income is often needed to keep the organisation running, to buy food for members, or to produce information materials for followers.

The first two aims, economic confusion and the discrimination of the opponent, are closely linked to one another. Both intend to show the vulnerability of industry and state security and the lack of technical knowledge of the other party. At the same time, successful attacks

demonstrate the competence of the attacker and thereby create fear on the part of others who are also vulnerable to similar attacks.

However, as far as cybercriminals are concerned, such publicity is often considered undesirable. This is especially true if attacks are launched with the intent of gathering information rather then destroying resources. In these cases, terrorists might also prefer not to claim responsibility for a successful attack. However, even in cases of destructive attacks, terrorists might choose to remain incognito for two reasons. First, if it becomes known that a certain incident was the result of a hacking attack by terrorists, pity and solidarity for the victims might be the result. However, if the impression arises that a breakdown was the result of technical incompetence, a lack of trust would be the outcome.[3] Therefore, terrorists – in some situations – might have an interest in not „showing their faces" when attacking digitally. A second aspect is that public knowledge of cyberterrorist attacks might result in an increased security level in many areas, making successful aggressions even more difficult to achieve. An unknown source of mysterious breakdowns, however, could instead lead to greater fear that could, in turn, be exploited by terrorist intents.

According to some organisations, the fiscal losses resulting from cybercrime attacks are costing businesses $ 48 billion annually and cost consumers $ 680 million in 2013. These numbers would increase rapidly if terrorist attacks aimed at causing maximum damage were to take place. However, in order to create economic confusion, more targeted aggressions are necessary. In a potential scenario, terrorists could combine the distribution of information to investors about an upcoming attack, e.g., against a company, with a targeted DdoS attack against a few major banks or stock exchanges.[4] The rapid spread of false business information and even a temporary blockage of communication could seriously damage the economy and – furthermore – could result in long-lasting consequences and lack of confidence in the reliability of financial services. The results could be even more disastrous if they were to be combined with a classical physical attack on resources. Since institutions such as banks or stock exchanges are vital for the economic well-being of a country, they could be promising targets for terrorists.

This was already tested in 1999, when the group called „J18" invited people to plan individual actions focusing on disrupting „financial centres, banking districts and multinational corporate power bases."[5] The events were initiated as a protest against financial centers on the occasion of the meeting of the G8 in Cologne, Germany, and led to teams of hackers from Indonesia,

---

[3] *J. Dunnigan,* The next war zone, New York 2002, p. 219.

[4] *G. Giacomello,* Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism, studies in conflict & terrorism, Vol. 27 (2005), p. 387-408 (392).

[5] *D. Denning*, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, http://www.totse.com/en/technology/cyberspace_the_new_frontier/cyberspc.html.

Israel, Germany, and Canada attacking the computers of at least 20 companies, including a stock exchange and Barclays Bank. Exposing the vulnerability of such institutions was also one of the outcomes of a war game of the U.S. Naval War College in 2002. It was discovered that the telecommunications infrastructure in the United States was hard to bring down because many redundancy measures had been implemented. However, this was not true for the financial system. The financial funds transfer system (*Fedwire*) that exchanges money among U.S. banks and the electronic transactions network (*Fednet*), in particular, were found to have only one primary installation and three backups, all of which could easily be located with the help of the Internet – and therefore lend themselves to a targeted attack.

b) Types of attacks

Four different types of attacks that could be interesting to terrorists can be distinguished. The first makes use of so-called bot-nets that can be instructed to administer large-scale attacks against targets. Tools and know-how for the acquisition and use of such networks are widely available and can also be put to use by terrorist organisations (1). The second type of attack does not operate on a large scale but uses conventional hacking techniques to gain access to specific computers (2). A third type of attack combines one of the aforementioned two types with a conventional bomb attack, thereby effectively cumulating effects in the virtual and physical worlds (3). Finally, a fourth type of attack also aims at the physical world: it manipulates IT-systems that serve as control systems (e.g., for railway or airport traffic) and is thereby able to cause damage, especially to physical goods (4).

(1) Large-scale attacks

The first example of the use of computers to attack IT-infrastructure is the implementation of large-scale DdoS attacks[6] with the help of so-called bot-nets. In these cases, viruses and Trojan horses are used to control other computers. These computers are turned into so-called „zombies" that are forced to report to a bot-net on a regular basis. These zombies are, in turn, controlled by a bot-master that instructs them, for instances, to send spam or forward thousands of requests to a particular site in order to make it inaccessible to its users.[7] Currently, bot-nets can also be being rented, that is, dubious companies can pay money to have spam sent by bot-nets. By doing so, these companies cover their tracks since the spam messages originate from thousands of different computers instead of from the company itself. In other cases, operators of bot-nets are paid to bring down competing businesses.[8] For a

[6] *L. Janczewki/A. Colarik,* Managerial Guide for Handling Cyber-Terrorism and Information Warfare, London 2005, p. 85ff.
[7] *Symantec Corp.,* Internet Security Threat Report XI (March 2007)
[8] *B. Bidder,* Angriff der Cyber-Söldner, Der Spiegel 31/2007, pp. 74-76.

terrorist organisation, the operation of a bot-net could be highly interesting since, on the one hand, bot-nets can be rented to third parties as a source of income. On the other hand, they can also be used for their own terrorist purposes, e.g., sending emails with terrorist content (e.g., propaganda) or bringing down an opponent's (for example, government) sites. Examples of this technique (executed either with bot-nets or by supporters) are the FloodNet attacks of pro-Israeli hackers that brought down Hizbollah's website or the electronic attack carried out during the allied air strikes on Kosovo and Serbia in 2000 that completely disrupted the internal and external communications of NATO troops.[9] Even the thirteen root servers of the Internet domain name system (DNS) have been the targets of DdoS attacks.

With a view to the legal problems that result from DdoS attacks, it is important to stress that – as already mentioned above – the *reason* for or the motivation behind a DdoS attack cannot be determined. In 2001, for example, an online demonstration was launched against the German airline „Lufthansa" to call attention to the involvement of the company in the deportation of illegal alien residents. Over 13,000 people took part in this demonstration and opened the web page of the company at the same time. The Lufthansa server was unable to reply to the sudden peak of requests so that the web page was unavailable to customers during this time-frame. Since – in this case – the company was informed about the campaign before it took place, it was aware of the reason for the downtime. However, Lufthansa customers not involved in the demonstration who attempted to access the web page could not know whether the error message was the result of a server problem, a (legitimate) online demonstration, or a criminal DdoS attack. Had the operator not been informed, they would have experienced the same uncertainty: whether the failure is due to a terrorist attack or mere sudden increase in interest on the part of customers (perhaps due to media coverage) cannot be determined by IP-packets.

(2) Hacking attacks

While the aforementioned large-scale attacks are a way to bring down a system and to suppress data flow, they do not enable access to protected data. If, however, a security weakness of a system can be exploited, access can be gained. This makes it possible either to shut down a computer or hinder its service in other ways, or to gain access to information that would otherwise be inaccessible. The hacking techniques used to access computers can also be used by terrorists to access and control government computers. The hacking of web servers

[9] *B. Foltz*, Cyberterrorism, computer crime, and reality, Information Management & Security, 15.03.2004, Vol. 12, No. 2, p. 154-166.

often results in so-called defacements,[10] in which the entry page of the website is replaced with another site that informs the user that the server has been hacked. Often, this replacement page is also used to give clues as to who the hacker was (by using nicknames), to send out greetings to fellow hackers, and also publicly to demonstrate how weak the security system of the attacked server was. Especially in cases in which the web server belongs to a security agency, the damage to the public's confidence in the trustworthiness and abilities of the affected agency is much higher than the monetary loss. For example, according to a recent study, 85% of IT-executives believe that U.S. government agencies are not adequately prepared for cyberterror attacks. By hacking and defacing a governmental site, a terrorist group can prove its existence and also its dangerousness. Al-Qaeda, for example, hacked the website of Silicon Valley Landsurveying Inc. In order to deposit a video file showing the hijacked (and later beheaded) *Paul Marshal Johnson*. By publishing the link to the stored video, the organisation could simultaneously demonstrate its technical as well as its conventional dangerousness. In another case, pro-Palestinian hackers used a coordinated attack to break into 80 Israel-related sites and deface them.

Even though web servers are seldom connected to other security-relevant services, the general public does not know this. Therefore, the damage to the image of the respective agency is the same. Furthermore, if a hacking attack is successful on a server actually carrying relevant data, a terrorist could make use of such a situation. For example, terrorists could attempt to steal or irreversibly damage vital data, such as the Social Security database, financial institution's records, or even secret military documents. Older and even more recent attacks have shown that even top-secret military computers and sensitive nuclear research centres[11] are not immune against all attacks. Therefore, such scenarios are threats that need to be considered.

However, those cases in which the attack does not become publicly known are even more dangerous. In the Internet, many tools that can be used to exploit known security vulnerabilities are freely available. If, for example, by means of a defacement, it becomes known that such a weakness has been exploited, the security hole can be fixed and another attack based on the same weakness prevented. If, however, a custom-made attack has been launched, it will not be detectable by any scanner available on the market. In one case, for example, a security company prepared USB sticks with a custom-designed, newly developed Trojan horse that could not be detected by virus scanners. Twenty of these sticks were „lost"

---

[10] *L. Janczewski/A. Colarik*, Managerial Guide for Handling Cyber-Terrorism and Information Warfare, London 2005, p. 5-6.

[11] *M. Vatis*, Cyber attacks during the war on terrorism: a predictive analysis. 22.09.2001, http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf, p. 5.

on the premises of a credit union. Of these, 15 sticks were found by employees – and promptly connected to the company network where the Trojan started to collect passwords and other valuable information and emailed this data back to the creators. Such an attack would be a powerful way for a terrorist organisation to start counterespionage. The same is true for so-called „Zero-Day exploits." These are exploits that are not yet known to the manufacturer (or, in some cases, to anyone else). Therefore, neither patches nor bug fixes are available against these attacks, nor can virus scanners detect them. In particular, the fact that it is not known at all that the security systems are being violated makes such an attack especially dangerous. Zero-Day exploits do not have to be developed by terrorists themselves. Instead, a black market has evolved that has the potential to put these dangerous instruments into the hands of all interested parties. Finally, custom-made Trojan horses could also be implemented via legal channels. In the year 2000 for example, Japan's Metropolitan Police Department used a software system to track 150 police vehicles, including unmarked cars. It turned out that this software had been developed by the Aum Shinrikyo cult – the same group that gassed the Tokyo subway in 1995. Additionally, members of this cult had developed software for at least eighty firms and ten government agencies. This was possible because the software developers were engaged as subcontractors, thus enabling personnel clearance of the subcontractor to be easily circumvented.

(3) Hybrid attacks

Apart from the „established" ways of rendering a system inaccessible, *hybrid* attacks are also being discussed as ways to cause the greatest possible damage. To carry out a hybrid attack, a classic bomb attack could be launched. At the same time, however, the communication devices of police or ambulances could be hindered by way of a DdoS attack, resulting in even greater losses and confusion. Many security specialists agree that this would be a likely scenario. The same idea is possible in another scenario that is aimed against national financial networks (such as *Fedwire* or *Fednet*). A hybrid attack against those networks or against transfer networks such as SWIFT would be able, it is said, to wreak havoc on the entire global economy.

(4) Attacks resulting in physical damage

When a system is being attacked – either by a large-scale DdoS or a specialized hacking attack – usually only the system itself is affected. However, in some settings physical damage can also occur. This can be achieved mainly by a manipulation of SCADA systems.[12]

[12] *F. Cohen,* Cyber-Risks and Critical Infrastructures, in: Alan O'Day (Ed.), Cyberterrorism, pp. 1-10.

SCADA is an acronym for „Supervisory Control And Data Acquisition." Basically, SCADA-systems are used to measure and control other systems. In many cases, these systems are connected to the Internet in one way or another. Even though, for security reasons, this is not advisable, the need to cut costs and the ability to remotely control several SCADA-systems centrally instead of having one person control one system on-site increases the interconnectivity of such systems. However, each system that is accessible to legitimate users through the Internet is also the potential victim of an illegitimate hacker. Additionally, many control systems are based on the Windows- and Unix operating systems. In this way, publicly known security weaknesses in these operating systems can be exploited in these control systems. The power-down of energy systems in 2003 in the United States and Eastern Canada impressively demonstrated their dependence on SCADA systems and the hard-to-understand interdependency of linked computer systems. Even though 21 power plants were brought down, the reason was not a terrorist or even purposeful attack. Instead – as far as is publicly known – it was a mere coincidence that these systems were shut down by the W32.Lovsan worm: this worm was using the same port to exploit a weakness on individual personal computers that was being used by the plants to communicate with each other. However, had this weakness been known to terrorists, the same result – 60 million households without electricity – could have been initiated by a criminal organisation. Finally, a combination of the above-mentioned DdoS attacks and SCADA systems of critical infrastructure could lead to considerable physical damage.[13]

Result

According to current literature, *cybercriminals* can attack anything that is important to modern society and connected to the Internet or accessible via other communication lines.[14] Therefore, *terrorists* in general can also use the same techniques and acquire the same knowledge as other criminals. The telecommunications, energy, and financial services sectors would seem to make interesting targets for such attacks.

3. Attacks on Human Life

The attacks described in the previous part can likely cause severe damage. However, in general, no human lives would be endangered. Therefore, it is questionable whether such attacks are an interesting option for terrorists. Even though the power cut of 2003 in the

---

[13] *G. Giacomello,* Bangs for the Buck: A Cost-Benfit Analysis of Cyberterrorism, Studies in Conflict & Terrorism, Vol. 27 (2004), pp. 387-408 (391).

[14] *U. Sieber,* The Threat of Cybercrime, in: Council of Europe (ed.), Organised Crime in Europe, Strasbourg 2005, pp. 81-218 (174).

United States was caused by a computer worm, no panic erupted, there were only a few injuries, and hospitals and emergency services continued to function properly. The security hole was subsequently fixed, so a second attack based on the same weakness is not likely. From a terrorist's point of view, attacks are more interesting and efficient if they cause fear in the public and the possibility of repeatability at any point in time seems highly likely. This is especially the case if human life can be endangered or the attack results in other kinds of physical harm.

Attacks using control systems

The scenarios that are being discussed and that could directly result in lost lives have, for the most part, not yet taken place (at least this has not become known to the public) and often involve an attack on SCADA systems. The results of such attacks could hamper the functioning of the affected industries. In the worst case, however, attacks could not only bring companies to a standstill or cause them to shut down for a longer period of time, but also affect lives. If, for example, hackers were to gain control over SCADA systems controlling hydroelectric dams, a surprise opening of the gates could cause flooding of the surrounding areas. Two cases are known in which attackers managed to enter such a system; however, they did not do any harm. Additional cases have not been officially verified. However, materials found in computers of captured terrorists show that these scenarios are actually being evaluated. Furthermore, systems operated by private companies are often claimed to be less secure than those operated by the military – even though a dysfunction can cause severe harm in both areas.

Apart from the manipulation of hydroelectric dams, the tampering of control systems for railway or air traffic is also being discussed. This tampering could, at the least, affect service or – in a worst case scenario – mean colliding trains or airplanes, which could possibly cost hundreds of lives.[15] The greatest risks would arise if the control systems of nuclear power plants were accessed (as has already happened). In this case, a plant could either be powered down or an attacker could try to overheat the system. This – again in a worst case scenario – could result in a nuclear catastrophe. The same holds true for an electronic intrusion into a military control centre, possibly resulting in a missile launch.[16]

However, these situations rely on the failure of all other security measures at the same time, a scenario which is not as realistic as other possible situations. Furthermore, military facilities

---

[15] *G. Giacomello,* Bangs for the Buck: A Cost-Benfit Analysis of Cyberterrorism, Studies in Conflict & Terrorism, Vol. 27 (2004), pp. 387-408 (398); *G. Weimann,* Sum of All Fears?, Studies in Conflict & Terrorism, 28 (2005), pp. 129-149 (138).

[16] *B. Foltz*, Cyberterrorism, computer crime, and reality, Information Management & Computer Security, 15.03.2004, Vol. 12, No. 2, pp. 154-166.

that are able to launch missiles are often not connected to the Internet („air-gapping"), making a remote launch simply impossible. However, since the military also makes use of increased connectivity and remote controlling in order to save the lives of soldiers, it is not completely unlikely that this situation will change over time. Furthermore, the military also uses civilian technology, thereby opening additional loopholes for security risks. Also, the human factor is often underrated: literature often distinguishes only between „computer only" and „human only" scenarios. The cases of hacking into a hydroelectric dam, however, show that – especially with the help of an insider – many security measures which would normally prevent a computer attack can be circumvented and that the additional knowledge of an insider can also be extremely helpful, especially when it comes to an electronic attack.

Long-term developments

Whereas the situations mentioned above can result in a one-time catastrophe, other ideas being discussed involve long-term scenarios that could be initiated by cyberterrorists. These scenarios include the manipulation of machinery, for example in the production of food or medication. If the alteration is not detected by internal quality-management, consumers could be contaminated or poisoned. Other possible targets include the weapons-production process, where manipulation could lead to useless ammunition. However, since these production areas are usually high-risk areas for other reasons as well, security measures are high, and production computers are seldom linked to public networks. However, if this were the case, risks would rise considerably.

Result

Since the attacks on human life require access to systems that not only control IT-infrastructure but that can also be abused to cause physical harm, a focus of such attacks is on the military production, energy services, and transport sectors. The latter is of particular interest since successful attacks can result in heavy losses of human life. Furthermore, fear – a terrorist constant – could be significantly heightened, even if such an attack was a one-time possibility that could not be repeated. Therefore, the great amount of time, knowledge, and (possibly) money that would need to be invested in a terrorist attack could „pay off" if it affected human lives.

II. Dissemination of Content

Internet use apart from attacks that are launched via the Internet may be of more interest for terrorist groups. Using the network to communicate with the public or with each other gives organisations new possibilities in a „war of ideas." This part will therefore focus on the use of the Internet for the dissemination of terrorist content to the public. For terrorist organisations, this is an important way (1.) to explain the reasons and motivation behind the terrorists' struggle, (2.) to disseminate threats and propaganda, (3.) to recruit supporters and train new members, and (4.) – in some cases – also to finance further activities.

1. Presentation of Terrorist Views

When terrorist organisations want to communicate their points of view, aims, and ambitions, they are typically faced with the problem that they hardly have any possibility to do so because they have to work undercover. Of course, leaflets are a way to justify assaults, and „mouth-to-mouth" propaganda can be used to recruit new members. However, both alternatives are time-consuming and risky, and they do not reach a large group of people. Additionally, terrorists are faced with the problem of how to communicate with (and possibly influence) the media.

With the help of the Internet, though, this has changed. Almost every terrorist organisation of any importance has its own website. Many of them contain detailed information on leaders, the history of the organisation, aims, or recent successes. Facts are put together for relevant target groups and in different languages in order to ensure that even foreigners can compare media news with the views of the relevant organisation. The most popular terrorist sites attract tens of thousands of visitors each month and make use of the „censorship resistance" of the Internet.

2. Propaganda and Threats

The opportunities for a terrorist organisation offered by a website are manifold: everything is virtually possible, from a mere presentation of viewpoints, to a general glorification of terrorism or justification of recent acts of violence (or threatening to perform new acts), up to and including the incitement of further (also digital) terrorist acts by the reading audience and recruits. All of this information can be presented in an impressive way that makes use of every available multimedia option. Other messages, such as the latest threats against German and Austrian involvement in Afghanistan, are also no longer forwarded as mere text-messages. Instead, professional-looking videos with German subtitles are sent out – often

directly to TV stations that incorporate the material and broadcast it in their programs. The Internet has therefore become the most important means by which terrorist organisations communicate with their supporters and other interested parties.

Terrorist websites, however, have one big disadvantage: only those interested in the organisation itself will be able to find it among the millions of other websites. Even they can be seriously hindered by government organisations that strive to make websites of terrorist organisations inaccessible. Therefore, organisations try to find new possibilities for propaganda and advertising. A more decentralized approach also makes it harder for the government to control content and could also make propaganda available for those capable of being influenced or open to the views of the organisation but not actively looking for it. It is perhaps for this reason that many propaganda videos have shown up on video-sharing-platforms such as YouTube. These videos often depict terrorism in a glorious light. Frequently, assault scenes are accompanied by modern music and graphics with a fresh look. Apart from videos, Internet radio shows can be also launched. These videos and radio shows allow organisations to spread their body of thought among young viewers who are vulnerable to influence and may stumble over such videos while looking for a new pop song.

Apart from footage that has been introduced in video platforms such as YouTube, the anonymity of website operators is another factor that can be put to use by terrorist organisations. While in the past only a few well-established organisations were able to produce newspapers, magazines, or TV shows, the Internet makes it possible for virtually anyone to launch their own periodicals or otherwise use the power of the media. Viewers are often unable to verify whether the news being broadcast is true or false. This again can be exploited by organisations that express their own views under the name of a seemingly neutral authority. With the help of several well-styled and –prepared websites that claim a certain viewpoint, interested parties and even journalists may have difficulty distinguishing propaganda from fact. By means of the same technique, opinions can also be altered and influenced if a seemingly large proportion of news services suddenly criticise certain governmental actions where, in reality, these news services are in fact operated by one and the same organisation. Finally, even traditional mass media make increasing use of the Internet as a source of stories and illustrated footage. By attractively presenting viewpoints and opinions, terrorist organisations can increase their chances of introducing these opinions into products of the mass media.

3. Recruitment and Training

When it comes to recruitment and training, the Internet again offers terrorists an excellent platform, as all contents can be easily deposited, mirrored between different locations in order to circumvent censorship or deletion, and anonymously gathered by those interested in this information. For example, special interests that might, in the past, have attracted a librarian's attention can now be pursued in the Internet, and information can be accessed without causing any suspicion. For some types of attacks, handpicked information has been already compiled, e.g., on bombs, poisons, or many other dangerous goods. The „Mujahadeen Poisons Handbook," for example, contains various „recipes" for homemade poisons and poisonous gases for use in terrorist attacks. Modern terrorists amend these handbooks by adding extra information on hostage taking, guerrilla tactics, and special bombs. For example, al-Qaeda prepared the „Encyclopedia of Jihad," which runs to thousands of pages. Young terrorists can gather such information from the Internet in order to prepare their assaults. However, the danger that appears to originate from many of these compilations should not be overestimated: even though these documents are clearly labelled, many of them contain the same information that can be found in most standard chemistry books for university students. Even training materials for interested terrorists are available through the Internet. Therefore, some authors claim that the Web has become „an open university for jihad."[17] Others agree and state that using the Internet for cyberplanning might be a more important and realistic option for terrorists than specialized cyberattacks.[18]

4. Fundraising and Financing

Some organisations use their websites as a source of financing or fundraising by selling CDs, DVDs, T-shirts, badges, flags, or books over the Internet. Other websites give supporters the opportunity to donate money directly with their credit card, or they provide bank account details for contributions. In doing so, organisations can also establish a link to supporters and candidates for possible recruitment. Apart from websites operated by the terrorist organisation itself, hundreds of support websites commonly appear and disappear. As with any other movement, they are often linked by web rings that allow visitors to quickly find similar websites. For example, Yahoo! Has pulled dozens of sites in the Jihad Web Ring, a coalition of 55 Jihad-related sites.

---

[17] *S. Coll/S. Glasser,* Terrorists turn to the web as base of operations, The Washington Post, 7 August 2005, Section A01.
[18] *T. Thomas,* Al Qaeda and the Internet: the danger of "cyberplanning", Parameters, Spring 2003, pp. 112-123 (112).

III. Use of the Internet for other Purposes

In addition to the use of the Internet for IT-based attacks and communication with the public, terrorists can also benefit from other possible uses that are seemingly „harmless," such as sending emails or visiting websites.

1. Individual Communication

Many of the aforementioned advantages of the Internet are also applicable to IT-based communication: it is cheap, fast, often anonymous, and widely accessible. And, since encryption technologies are extensively available, it is also secure, even if messages have to be transported over public networks. Whereas the communication between a terrorist organisation and the public depends on good visibility, messages between terrorists or terrorist groups depend to a high degree on good camouflage and secure communication channels. Even though the Internet is basically an open network, its advantages predestine it for this communication task and make it an outstanding command and control mechanism. Customary text-based techniques such as email, chat rooms, or mailing lists can be used, as can real speech by voice-over IP (VoIP). Since many companies offer these services free of charge, no organisation has to operate its own service. Instead, many different and cost-free services can be used – alternatively or even simultaneously. The organisers of the 9/11-attacks, for example, had opened multiple accounts on largely anonymous email services such as „Hotmail." Additionally, since the text-based techniques operate on the basis of process-and-store mechanism, new information can be gathered at any convenient point in time, so that terrorists neither have to be online all the time, nor do they have to entrust third-parties with the task of accepting personal messages for them. Additionally, with the help of modern mobile phones, the Internet can be accessed virtually everywhere.

In essence, the digital transportation of information enables loosely interconnected groups to maintain contact with one another. This even goes so far as to allow terrorist groups that fight for different political goals and are located in different geographical areas to communicate with each other and exchange information, such as on weapons or tactics.

Even if terrorists fear that their messages might be intercepted, they can take appropriate measures. They can either disguise the message itself or use conventional encryption techniques. To hide messages, two techniques, in particular, are being discussed. For example, an organisation could hide messages in pictures with the help of steganography. These pictures can be put on any public website, for example a classic photo site such as webshots.com. In turn, other members of the organisation could download the picture and

decrypt the message. The entire process is concealed because no one (except for the terrorists) knows that the pictures contain a secret message. Furthermore, the course of action is completely inconspicuous because it is an everyday event that does not draw any attention to itself. The second technique involves the use of free mailer email accounts. However, the account is used in an unconventional way: instead of logging in, writing, and sending an email, the password is not just known to one person but to two – sender and recipient. The sender logs onto the account and writes but does not send the message. Instead, the message is saved as a draft. Later, the recipient logs onto the same account and reads the message in the draft folder. By means of this technique, the message never leaves the system, so that no traces of an email remain on any system – governmental filtering systems are successfully circumvented.

However, even if the organisation decides to send messages as proper emails, it can do so because all of the messages can be encrypted. Good encryption programs are available to the public as open-source software; thus, terrorists can be sure that no hidden backdoor is contained in the program. If the right encryption parameters are used, even up-to-date technology is not able to decrypt the message without the right key. Thousands of encrypted messages, for example, were found by federal officials on the computers of arrested al-Qaeda terrorists Abu Zubaydah and Ramzi Yousef, who was tried for the previous bombing of the World Trade Center. However, terrorists might also send unencrypted emails – if for example, they desire the content of their communication to become known. Since it is common knowledge that the surveillance of telecommunications is on the rise, such information could be purposefully disseminated in order to conceal other – real – attack plans that concentrate on other objects.

2. The Internet as a Planning and Support Instrument

Apart from its function as an instrument of communication, the Internet also serves as a planning tool that can be used for real-world as well as for digital attacks. Information, such as satellite maps, that was only available to experts until recently is now a common good. These graphics are already being used by terrorists, and they can easily be combined with other data, such as street names. As a result, for example escape routes can be planned with great precision even before a territory is inspected in person. This information can be combined with other information that is often freely available on the websites of companies, governmental institutions, and news services. For example, reports of security weaknesses in airports or transport companies could be gathered and used. According to a terrorist training manual, such public sources can make up at least 80% of all information on the opponent that

is required. Actual findings on terrorists' computers show that these kinds of information are in fact downloaded and used for planning purposes. Furthermore, according to some authors, terrorist organisations even use databases to gather, sort, and evaluate details of potential targets in the United States. Against this background, it is reasonable that governments around the world have begun to ask providers of digital maps for disclosure of certain – security-relevant – information.

Additionally, the compilations of specialized information mentioned above (such as the „Mujahadeen Poisons Handbook") are available for the planning and support of (mostly conventional) attacks. Therefore, the claims of some authors – that the Web has become „an open university for jihad" and that cyberplanning might be a more important and realistic option for terrorists than specialized cyberattacks – cannot be dismissed.

CONCLUSIONS

When looking at IT-based attacks, it is difficult to decide whether the phenomenon is just an exaggerated "cyber angst" or whether cyberterrorism is indeed an imminent threat. To identify what terrorists might do in the future, technical know-how combined with imagination is needed. In the literature, this debate is fuelled by the many different definitions of cyberterrorism and terrorist use of the Internet, ranging from very narrow to very broad. A narrow definition is often followed by the assumption that cyberterrorism does not pose a threat, has never occurred, and cannot do any serious harm, whereas proponents of a broad definition take a more cautious point of view and claim that the threat is real.

Realistically, one has to look at the possibilities and drawbacks of digital attacks and compare the necessary investments on the part of a terrorist organisation with the potential results. In addition, everything that *could* be done with the help of computers is often equated with what *will* be done. For a rational evaluation, however, many different aspects have to be taken into account. An example of a real disadvantage of digital assault is that such attacks are often not repeatable since security flaws can and will be fixed once they are discovered. Therefore, terrorists have to assess carefully whether their investments in terms of time, personnel, and money are worth a one-time attack. Furthermore, apart from the attacks described above in which human lives are endangered, many scenarios result only in the unavailability of computer service, which is a common phenomenon even without terrorist attacks. Thus, neither public fear nor extensive media coverage can be expected from computer-related cyberterrorist attacks; cyberterrorism in this area is largely quiet. Finally, attacks in security-relevant areas require highly developed computer skills and, very often, knowledge of exact circumstances. Therefore, experts claim that it could take from two to four years of

preparation for a structured cyberattack against multiple systems and networks. Also, the tremendous costs that accompany such a long preparation time might be a serious hindrance.

REFERENCES

1. *B. Foltz*, Cyberterrorism, computer crime, and reality, Information Management & Computer Security, 15.03.2004, Vol. 12, No. 2, pp. 154-166.
2. *M. Conway*, Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet, First Monday, 04.11.2002, Vol. 7, No. 11.
3. *M. Gercke,* "Cyberterrorismus" – Aktivitäten terroristischer Organisationen im Internet, CR 2007, pp. 62-68 (63).
4. *U. Sieber,* The Threat of Cybercrime, in: Council of Europe (ed.), Organised Crime in Europe, Strasbourg 2005, pp. 81-218 (173).
5. *J. Dunnigan,* The next war zone, New York 2002, p. 219.
6. *G. Giacomello,* Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism, studies in conflict & terrorism, Vol. 27 (2005), p. 387-408 (392).
7. *D. Denning*, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, http://www.totse.com/en/technology/cyberspace_the_new_frontier/cyberspc.html.
8. *Symantec Corp.,* Internet Security Threat Report XI (March 2007).
9. *B. Bidder,* Angriff der Cyber-Söldner, Der Spiegel 31/2007, pp. 74-76.
10. *L. Janczewki/A. Colarik,* Managerial Guide for Handling Cyber-Terrorism and Information Warfare, London 2005, p. 85ff.
11. *M. Vatis*, Cyber attacks during the war on terrorism: a predictive analysis. 22.09.2001, http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf, p. 5.
12. *F. Cohen,* Cyber-Risks and Critical Infrastructures, in: Alan O'Day (Ed.), Cyberterrorism, pp. 1-10.
13. *S. Coll/S. Glasser,* Terrorists turn to the web as base of operations, The Washington Post, 7 August 2005, Section A01.
14. *T. Thomas,* Al Qaeda and the Internet: the danger of "cyberplanning", Parameters, Spring 2003, pp. 112-123 (112).

APPLICATIONS OF BIOMETRICS IN 21st CENTURY

Author:
MAJ Ioan Aurel MACAVEIU

INTRODUCTION

Biometrics is a very useful domain because can be applied for **authentication** - verifying that a person is who he declares or pretends to be - and for **identification** - determining who is the person based on the measured biometric factor.

The term ***biometrics*** refers to technologies that measure and analyzes human physiological or behavioral characteristics for authentication or identification purposes. Some of the most widely used characteristics or biometric factors are fingerprints, irises, voice patterns and the spatial geometry of the face.

We should understand why biometrics is needed more than ever. Physical access control, say to a building, room, etc. is generally based on locks and keys, on badge readers or on few-digit pin codes which are easily lost or stolen.

With biometrics the access control factor is **something you are**, a measureable physiological or behavioral characteristic, which is often more difficult to fake, steal or imitate than a password or a key.

Chapter 1 PERFORMANCE OF BIOMETRICS

Section 1 METRICS USED TO RATE THE PERFORMANCE OF A BIOMETRIC FACTOR, SOLUTION OR APPLICATION

We can use different metrics to rate the performance of a biometric factor, solution or application, but the most common performance metrics are the **False Acceptance Rate** FAR and the **False Rejection Rate** FRR, that are key metrics for biometric solutions, some biometric devices or software

First time when a user uses a biometric application, he needs to **enroll** to the system. The system requests fingerprints, a voice recording or another biometric factor from the user, this input is registered in the database as a **template** which is linked internally to a user ID. The next time when the user wants to authenticate or identify himself, the biometric input is compared to the template(s) in the database which responds with acceptance (match) or rejection (no match).

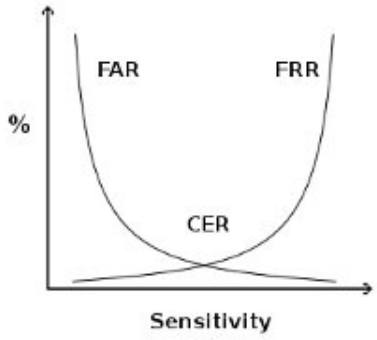
1. ***False Acceptance Rate and False Rejection Rate***

The **FAR** or False Acceptance Rate is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a template. The FAR is normally expressed as a percentage, following the FAR definition this is the **percentage of invalid inputs which are incorrectly accepted**.

The **FRR** or False Rejection Rate is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template. The FRR is normally expressed as a percentage, following the FRR definition this is the **percentage of valid inputs which are incorrectly rejected**.

One person is insufficient to establish an overall FRR for a solution.

False Accept Rate is also called **False Match Rate**, and False Reject Rate is sometimes referred to as **False Non-Match Rate**.



A graphical representation of FAR and FRR errors, indicating the CER

2. The **Crossover Error Rate** or CER is the rate where both accept and reject error rates are equal.

The matching algorithm in a biometric software or device uses a (configurable) threshold which determines how close to a template the input must be for it to be considered a match. This threshold value is in some cases referred to as **sensitivity**, it is marked on the X axis of the plot. When you reduce this threshold there will be more false accept errors (higher FAR)

and less false reject errors (lower FRR), a higher threshold will lead to lower FAR and higher FRR.

3. ***Failure to Enroll Rate (FER)***

The **Failure to Enroll Rate** or FER is the percentage of the population which fails to complete enrollment. Those failures can be due to lack of training on how to enroll, to environmental or ergonomic conditions, or to certain demographics which make that the biometric factor is simply not suitable with a certain percentage of the population.

4. ***Speed***

Most manufacturers of biometric devices and software can give clear numbers on the **time it takes to enroll** as well on the **time for an individual to be authenticated** or identified using their application. If speed is important then take your time to consider this, 5 seconds might seem a short time on paper or when testing a device but if hundreds of people will use the device multiple times a day the cumulative loss of time might be significant.

5. ***Number of templates***

If a biometric device will be used by many different users then the number of templates it can store might become an issue. Most stand-alone devices have limited memory and therefore only allow a **limited number of enrolled users**.

Section 2 FACTORS USED IN BIOMETRIC SOLUTIONS

We can divide the biometric solutions into two groups, based on the type of biometric factor they use

1. solutions based on a **physiological** factor, examples are fingerprint recognition and iris recognition
2. solutions based on a **behavioral** factor, examples are voice pattern recognition and keystroke dynamics

For the factors which could be used as a biometric solution to be applied for *authentication* or *identification*, it must meet the following criteria:

- **Universality** - the biometric factor must be something that each person has.
- **Uniqueness** - with the factor it must be possible to separate individuals from another.
- **Permanence** - how well the biometric factor resists the effect of time.

- **Collectability** - it must be possible and not overly expensive or time consuming to measure the factor.
- **Acceptability** - biometrics is not always very well accepted. This is generally dependent on people's view is on how invasive a certain technique is
- **Circumvention** - how easily it is to imitate the biometric factor.
- **Performance** - in general terms the speed, the accuracy and the robustness.

These criteria also depend on how the biometric factor is applied; technological differences have a high impact on the suitability of the biometric

Chapter 2 PRACTICAL APPLICATIONS OF BIOMETRICS

Section 1 ACCESS CONTROL

To get access to a secured area or system is mostly a two-step process:

- **Identification**, the process by which the user professes an identity by providing a username, a pincode or some other form of ID.
- **Authentication**, the process of verification or testing to make sure that the user is who he claims to be.

Mobile harddisk with fingerprint reader

We can use biometrics for both steps, identification requiring a one-to-many search in the templates database and authentication a one-to-one comparison of the measured biometric with the template that is associated to the claimed identity.

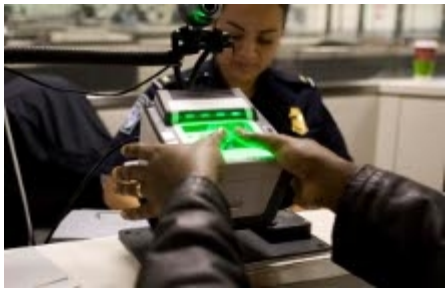
There exist three types of authentication factors: *something you know* (e.g. password), *something you have* (e.g. token device, badge) and *something you are*. Biometrics fall in the third category, which is by definition the most secure because most companies still struggle to implement good password practices and when token devices or badge readers are used they get lost or are shared among colleagues.

A lot of commercial, biometric **access control** solutions are available, and many more are in development.

- Access control to computer systems (workstations): USB fingerprint readers, voice and face recognition software using standard camera and microphone hardware, etc.
- Door security: doors with biometric locks using iris recognition, fingerprint readers, etc.
- Portable media such as USB sticks and mobile harddrives with integrated biometric access control and mostly encrypting your data using a built-in algorithm.
- Safes with biometric locks

Section 2 FINGERPRINT RECOGNITION

Fingerprint recognition refers to the automated method of identifying or confirming the identity of an individual based on the comparison of two fingerprints. **Fingerprint recognition** is one of the most well known biometrics, and it is by far the most used biometric solution for authentication on computerized systems. The reasons for fingerprint recognition being so popular are the ease of acquisition, established use and acceptance when compared to other biometrics, and the fact that there are numerous (ten) sources of this biometric on each individual.



Fingerprint reader used for border control

There exist four main types of fingerprint reader hardware:

1. **Optical readers** are the most common type of fingerprint readers. The type of sensor in an optical reader is a digital camera that acquires a visual image of the fingerprint. Advantages are that optical readers start at very cheap prices. Disadvantages are that readings are impacted by dirty or marked fingers, and this type of fingerprint reader is easier to fool than others.

2. **Capacitive readers**, also referred to as CMOS readers, do not read the fingerprint using light. Instead a CMOS reader uses capacitors and thus electrical current to form an image of the fingerprint. CMOS readers are more expensive than optical readers. An important advantage of capacitive readers over optical readers is that a capacitive reader requires a real fingerprint shape rather than only a visual image. This makes CMOS readers harder to trick.

3. **Ultrasound readers** are the most recent type of fingerprint readers; they use high frequency sound waves to penetrate the epidermal (outer) layer of the skin. They read the fingerprint on the dermal skin layer, which eliminates the need for a clean, unscarred surface. All other types of fingerprint readers acquire an image of the outer surface, thus requiring hands to be cleaned and free of scars before read-out. This type of fingerprint reader is far more expensive than the first two, however due to their accuracy and the fact that they are difficult to fool the ultrasound readers is already very popular.

4. **Thermal readers** sense, on a contact surface, the difference of temperature in between fingerprint ridges and valleys. Thermal fingerprint readers have a number of disadvantages such as higher power consumption and a performance that depends on the environment temperature.

After a fingerprint image is acquired by the fingerprint reader hardware, this fingerprint must be interpreted. It must be processed in such a way that read-outs can be efficiently compared and matched against each other.

Application of fingerprint recognition

Because it is one of the cheapest biometric solutions, fingerprint recognition already knows many different applications. We only list a few examples here:

- Logical access control, for example there exist numerous fingerprint reader devices and software for access control to personal computers
- Physical access control, for example locks with a fingerprint reader
- Time and attendance management
- Biometric alternative to loyalty card systems

Suitability of fingerprint recognition

We use the following 7 criteria to evaluate the suitability of fingerprint recognition:

Universality: Only very few people miss all 10 fingers. Most fingerprint recognition software allows enrolling multiple fingers which avoids that an individual is no longer granted access after injury.

Uniqueness: It is generally accepted that fingerprints are unique to an individual. However, there is a risk that fingerprints of two different individuals match if the fingerprint image is of insufficient quality. Therefore the False Acceptance Rate (FAR) is highly dependent on the quality of the fingerprint reader.

Permanence: Fingerprints do not change with ageing, but as people age they lose collagen which makes their fingerprint harder to read and this can lead to significantly more false rejects with elderly people.

Collectability: Fingerprints are easy to acquisition, the cheapest fingerprint readers available use a digital camera. Fingerprint readers that are more difficult to fool, such as CMOS readers, are even not overly expensive.

Acceptability: Fingerprints are easily accepted as soon as people reflect that they leave their fingerprints everywhere and that no sensitive information, such as medical conditions, can be derived from fingerprints.

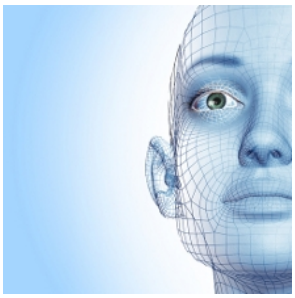
Circumvention: A finger can be cut off, this is no joke it already happened. Fingerprint sensors with liveliness detection can resolve this issue.

Performance: In terms of speed, accuracy and robustness the devices actually on the market should cover any need, except maybe for big corporations and government applications where matching algorithms might become a bottleneck

Section 3 FACE RECOGNITION

Face recognition uses the spatial geometry of distinguishing features of the face. It is a form of computer vision that uses the face to identify or to authenticate a person. An important difference with other biometric solutions is that faces can be captured from some distance away, with for example surveillance cameras. Therefore **face recognition** can be applied without the subject knowing that he is being observed. This makes face recognition

suitable for finding missing children or tracking down fugitive criminals using surveillance cameras.



Software analyzes the spatial geometry of the face

Difficulties that often arise with face recognition are

- Variable image lighting and background make it more difficult for software to locate the face in the image.
- Parts of the face are covered, e.g. long hair, and make it more difficult for the software to locate the face in the image and to recognize the face.
- Subject does not look directly into the camera, when the face is not held in the same angle the software might not recognize the face.
- Using different types of cameras (with different lighting, resolution, etc.) makes it more difficult for the software to recognize the face.
- The face of a subject changes with ageing.

Application of face recognition

Face recognition can be used together with **surveillance** cameras to automatically identify missing children, unwanted subjects in casino's or fugitive criminals for whom a picture is registered in a central database.

Suitability of face recognition

Universality: For some people face recognition might not work as well as for others. For example long hair or a beard might give face recognition systems extra difficulty, and not all marketed solutions will deal with this equally well.

Uniqueness: Face recognition cannot distinguish identical twins.

Permanence: As you age your face will most likely change. Also injury, plastic surgery or more temporary changes such as sunglasses, make-up or growing a beard might have an impact.

Collectability: Faces are easy to collect, direct contact with the biometric device is not required and the subject might not even know that an image of his face is being collected.
Acceptability: There certainly are privacy concerns when using a surveillance system to track people's whereabouts. However applying face recognition for access control will be easier accepted than other biometric solutions because no direct contact is required with a reader, and in general people do not consider taking a photograph as being intrusive as might be the case with biometric solutions such as iris recognition or fingerprint recognition.

Circumvention: This is very much dependent on the technical implementation, much depends on the quality of the camera, the control of the surroundings (e.g. background) and on the matching algorithm.

Performance: Speed might be an issue for surveillance systems, imagine having the matching algorithm verifying the faces of travelers on an airport: a high number of verifications with images that are taken without subjects looking directly into the camera.

We can conclude that face recognition is most interesting because the subject is not necessarily aware that his identity is being verified, this is very useful for surveillance applications.

Section 4 **SPEAKER RECOGNITION**

Voice recognition or **speaker recognition** refers to the automated method of identifying or confirming the identity of an individual based on his voice. Beware the difference between speaker recognition (recognizing who is speaking) and speech recognition (recognizing what is being said).

Basically identification or authentication using speaker recognition consists of **four steps**:

1. voice recording
2. feature extraction
3. pattern matching
4. decision (accept / reject)

Application of speaker recognition

Voice recognition is mostly used for telephone based applications, such as for telephone banking and hotel or flight bookings.

Suitability of speaker recognition

Universality: Obviously for people who are mute or having problems with their voice due to severe illness this biometric solution is not useable.

Uniqueness: Because of the combination of physiological and behavioral factors the voice is a unique feature of an individual, the voice has more unique features than a fingerprint.

Permanence: An issue with speaker recognition is that the voice changes with ageing, and is also influenced by factors such as sickness, tiredness, stress, etc.

Collectability: Voice recordings are easy to obtain and do not require expensive hardware. The real advantage of voice recognition is that it can be done over telephone lines or using computer

Acceptability: Speaker recognition is unobtrusive; speaking is a natural process so no unusual actions are required.

Circumvention: A major issue with speaker recognition is spoofing using voice recordings. The risk of spoofing with voice recordings can be mitigated if the system requests a random generated phrase to be repeated, an impostor cannot anticipate the random phrase that will be required and therefore cannot attempt a playback spoofing attack.

Performance Robustness is very dependent on the setup, when telephone lines or computer microphones are used the algorithms will have to compensate for noise and issues with room acoustics. Furthermore speaker recognition is, because the voice is a behavioral biometric, impacted by errors of the individual such as misreading and mispronunciations.

Section 4 **IRIS RECOGNITION**

Iris recognition refers to the automated method of identifying or confirming the identity of a subject by analyzing the random pattern of the iris. **Iris recognition** is relatively

young, being only commercially developed the last decade mostly due to previous patent limitations.

The following sequence applies to both enrollment and recognition:

1. **Capture iris image.** The camera acquires an image from the iris; lighting is mostly done with Near Infrared (NIR) light because with NIR there is less noise in the image due to reflections when compared to visible light. Also NIR light does not cause harm or discomfort to the subject.

2. **Finding iris in the image.** One of the challenging parts of iris recognition is for the algorithm finding the concentric circular outside boundaries of pupil and iris. Often part of the iris is covered by eyelids or eyelashes, which even more complicates this step.

3. **Convert image.** The set of pixels which cover the iris on the image are then transformed into a bit pattern that preserves required information for template comparison but allows faster and statistical meaningful comparison. Dr. Daugman's algorithms, referred to as IrisCode ™, translates the visible characteristics from the image into a 512 byte code, the template, which allows extremely quick searches and a very low false acceptance rate.

When a subject tries to authenticate or identify himself, the generated IrisCode is compared with templates stored in the database. A test of statistical independence determines whether the IrisCode resulting from the scan and a stored IrisCode template are from the same iris.

IrisCode ™ is based on an algorithm developed and patented in the nineties by **Dr. Daugman**. This is nowadays the most used algorithm in commercial devices, thanks to its speed of matching with very low false match rates. Suitability of iris recognition.

Universality: Iris recognition is said to have a very low FER (Failure to Enroll Rate), i.e. the smallest group of people which can not use the technology.

Uniqueness: The patterns of the iris are highly variable, and considered unique for each individual. The patterns are formed randomly during embryonic gestation, therefore even genetically identical twins have different iris patterns.

Permanence: The iris has the great advantage that it is internal, and thus well protected, but externally visible. Furthermore the iris does not change with ageing, one enrollment should be sufficient for a lifetime with the exception of damage due to accident or disease.

Collectability: The shape of the iris is almost completely flat and thus very predictable, much more than that of the face. Also an image can be taken from 10 cm up to a few meters away. Therefore no expensive 3D cameras are needed and the impact of a different viewing angle is far less than for example with face recognition.

Acceptability: Contrary to retina scans the iris can only reveal very little medical information about the subject. Furthermore subjects do not have to be in direct contact with the biometric device or camera, which is an objection that is often raised against fingerprint recognition. **Circumvention:** A common issue with all biometric solutions is liveliness detection, for non-supervised applications *liveliness detection* is absolutely required.

Performance: Iris recognition using IrisCode ™, which is used in most commercial iris recognition products, is well suited for one-to-many identification because of high speeds of comparison. Furthermore the IrisCode matching algorithm has a very low, even unprecedented false acceptance rate.

Section 4 **KEYSTROKE DYNAMICS**

Keystroke dynamics or typing dynamics refers to the automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard. **Keystroke dynamics** is a behavioral biometric, this means that the biometric factor is 'something you do'.

The raw measurements used for keystroke dynamics are dwell time and flight time.

- **Dwell time** is the time duration that a key is pressed
- **Flight time** is the time duration in between releasing a key and pressing the next key

When typing a series of characters, the time the subject needs to find the right key (flight time) and the time he holds down a key (dwell time) is specific to that subject, and can be calculated in such a way that it is independent of overall typing speed. The rhythm with which some sequences of characters are typed can be very person dependent. For example someone used to typing in English will be quicker at typing certain character sequences such as 'the' than a person with French roots.

Keystroke dynamics can be used for authentication, and then it is used mostly together with user ID / password credentials as a form of **multifactor authentication**.

Suitability of keystroke dynamics

Universality: This biometric solution can be used by all individuals that are able to use a keyboard.

Uniqueness Unlike physiological biometric factors, there can be no such thing as an absolute match with behavioral biometrics. Therefore it is difficult to discuss uniqueness of a typing pattern.

Permanence: A major problem with keystroke dynamics is that a subject's typing rhythm varies considerably in between days and even within the same day. There are numerous reasons for this: tiredness, switching computers / keyboards, mood, influence of alcohol and medications, etc.

Collectability: An important advantage of keystroke dynamics is that there is **no special hardware needed** as with other biometrics, a standard computer keyboard is sufficient.

Acceptability: Depending of the country or state you are in using key logging software might be a direct violation of local laws.

Circumvention: It is certainly difficult, if not impossible to mimic another person's typing rhythm.

Performance: Behavioral biometrics has higher variations because they depend on a lot of (external) factors such as ergonomics, fatigue, mood, etc.

Chapter 3 BIOMETRIC PASSPORT

A **biometric passport**, also known as an **e-passport**, **ePassport** or a **digital passport** is a combined paper and electronic passport that contains biometric information that can be used to authenticate the identity of travelers. It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or center page, of the passport.

The passport's critical information is both printed on the data page of the passport and stored in the chip. Public Key Infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented.

Section 1 Data protection

Biometric passports are equipped with protection mechanisms to avoid and/or detect attacks:

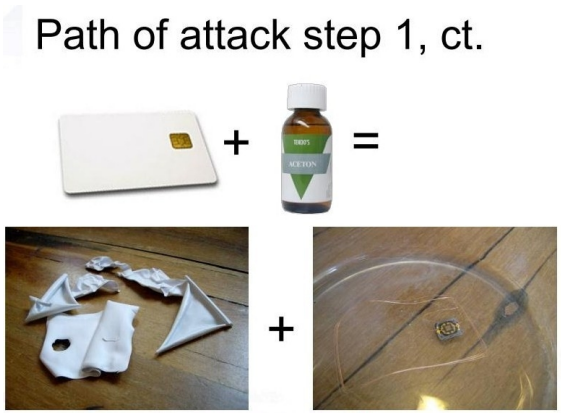
- Non-traceable chip characteristics. Random chip identifiers reply to each request with a different chip number. This prevents tracing of passport chips. Using random identification numbers is optional.
- Basic Access Control (BAC). BAC protects the communication channel between the chip and the reader by encrypting transmitted information. Before data can be read from a chip, the reader needs to provide a key which is derived from the Machine Readable Zone: the date of birth, the date of expiry and the document number. If BAC is used, an attacker cannot (easily) eavesdrop transferred information without knowing the correct key. Using BAC is optional.
- Passive Authentication (PA). PA prevents modification of passport chip data. The chip contains a file (SOD) that stores hash values of all files stored in the chip (picture, fingerprint, etc.) and a digital signature of these hashes. The digital signature is made using a document signing key which itself is signed by a country signing key. If a file in the chip (e.g. the picture) is changed, this can be detected since the hash value is incorrect. Readers need access to all used public country keys to check whether the digital signature is generated by a trusted country. Using PA is mandatory.
- Active Authentication (AA). AA prevents cloning of passport chips. The chip contains a private key that cannot be read or copied, but its existence can easily be proven. Using AA is optional.
- Extended Access Control (EAC). EAC adds functionality to check the authenticity of both the chip (chip authentication) and the reader (terminal authentication). Furthermore it uses stronger encryption than BAC. EAC is typically used to protect fingerprints and iris scans. Using EAC is optional.
- Shielding the chip. This prevents unauthorized reading. Some countries – including at least the US – have integrated a very thin metal mesh into the passport's cover to act as a shield when the passport cover is closed. The use of shielding is optional.

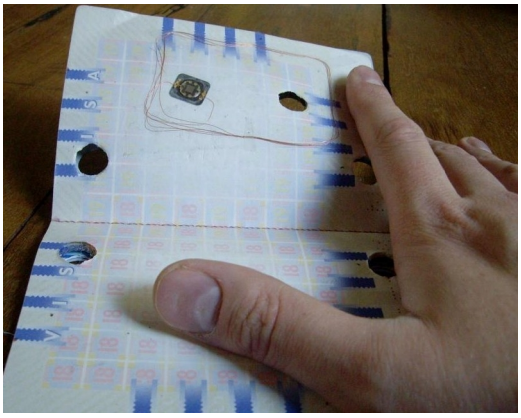
Section 2 Attacks

Since the introduction of biometric passports several attacks are presented and demonstrated:

- Non-traceable chip characteristics. In 2008 a Radboud/Lausitz University team demonstrated that it's possible to determine which country a passport chip is from without knowing the key required for reading it. The team fingerprinted error messages of passport chips from different countries. The resulting lookup table allows an attacker to determine from where a chip originated. In 2010 Tom Chothia and Vitaliy Smirnov documented an attack that allows an individual passport to be traced, by sending specific BAC authentication requests.
- Basic Access Control (BAC). In 2005 Marc Witteman showed that the document numbers of Dutch passports were predictable, allowing an attacker to guess/crack the key required for reading the chip. In 2006 Adam Laurie wrote software that tries all known passport keys within a given range, thus implementing one of Witteman's attacks. Using online flight booking sites, flight coupons and other public information it's possible to significantly reduce the number of possible keys. Laurie demonstrated the attack by reading the passport chip of a Daily Mail's reporter in its envelope without opening it.
- Passive Authentication (PA). In 2006 Lukas Grunwald demonstrated that it is trivial to copy passport data from a passport chip into a standard ISO/IEC 14443 smartcard using a standard contactless card interface and a simple file transfer tool. Grunwald used a passport that did not use Active Authentication (anti-cloning) and did not change the data held on the copied chip, thus keeping its cryptographic signature valid. In 2008 Jeroen van Beek demonstrated that not all passport inspection systems check the cryptographic signature of a passport chip. For his demonstration Van Beek altered chip information and signed it using his own document signing key of a non-existing country. This can only be detected by checking the country signing keys that are used to sign the document signing keys. To check country signing keys the ICAO PKD can be used. Only 5 out of 60+ countries are using this central database. Van Beek did not update the original passport chip: instead an ePassport emulator was used. Also in 2008, The Hacker's Choice implemented all attacks and published code to verify the results. The release included a video clip that demonstrated problems by using a forged Elvis Presley passport that is recognized as a valid US passport.
- Active Authentication (AA). In 2005 Marc Witteman showed that the secret Active Authentication key can be retrieved using power analysis. This may allow an attacker to clone passport chips that use the optional Active Authentication anti-cloning mechanism on chips – if the chip design is susceptible to this attack. In 2008 Jeroen van Beek demonstrated that optional security mechanisms can be disabled by removing their

presence from the passport index file. This allows an attacker to remove – amongst others – anti-cloning mechanisms (Active Authentication). Note that supplement 7 features vulnerable examples in the same document that – when implemented – result in a vulnerable inspection process.





- Extended Access Control (EAC). In 2007 Luks Grunwald presented an attack that can make EAC-enabled passport chips unusable. Grunwald states that if an EAC-key – required for reading fingerprints and updating certificates – is stolen or compromised, an attacker can upload a false certificate with an issue date far in the future. The affected chips block read access until the future date is reached.

Section 3 OPPOSITION

Privacy proponents in many countries question and protest the lack of information about exactly what the passports' chip will contain, and whether they impact civil liberties. The main problem they point out is that data on the passports can be transferred with wireless RFID technology, which can become a major vulnerability. Although this could allow ID-check computers to obtain a person's information without a physical connection, it may also allow anyone with the necessary equipment to perform the same task. If the personal information and passport numbers on the chip are not encrypted, the information might wind up in the wrong hands.

Most security measures are designed against untrusted citizens, but the scientific security community recently also addressed the threats from untrustworthy verifiers, such as corrupt governmental organizations, or nations using poorly implemented, unsecure electronic systems. New cryptographic solutions such as private biometrics are being proposed to mitigate threats of mass theft of identity. These are under scientific study, but not yet implemented in biometric passports.

Another concern is that the photograph looks blurry and less clear, as a result of the way it has been prepared.

CONCLUSIONS

Although biometrics applications are not yet seen everywhere, new technology begin to appear including gadgets used in everyday life, a good example would be mobile phones. One of these is the iPhone 5s, which is equipped with fingerprint authentication Touch ID. While it starts with some trendy new technology to get everyone really jazzed about biometrics, the iPhone is only the beginning. Pretty soon these kinds of security measures will be everywhere in a Big Brother dream come true.

The biometrics hacking team of the Chaos Computer Club (CCC) has successfully bypassed the biometric security of Apple's TouchID using easy everyday means. A fingerprint of the phone user, photographed from a glass surface, was enough to create a fake finger that could unlock an iPhone 5s secured with TouchID. This demonstrates – again – that fingerprint biometrics is unsuitable as access control method and should be avoided.

As a conclusion, biometrics can be our friend, but also our enemy, with advancing technology and cyber enemies using science discoveries into their own purposes. the same time, biometrics requires considerable funds when we want sophisticated security systems, making it inaccessible to many, despite its usefulness.

REFERENCES

1. Tom Chothia and Vitaliy Smirnov - A Traceability Attack Against e-Passports
2. Henning Richter, Wojciech Mostowski and Erik Poll - Fingerprinting Passports
3. www.wikipedia.org
4. http://www.griaulebiometrics.com
5. http://www.biometric-solutions.com
6. Jeroen van Beek - ePassports reloaded goes mobile
7. http://www.activistpost.com/2013/09/a-warning-against-biometric-security.html

INFORMATION SECURITY IN UNMANNED AERIAL VEHICLES' (UAVs) COMMUNICATIONS

Author:
MAJ Marius MUSCALU

INTRODUCTION

The unmanned aerial vehicle (UAV) has been for years a focal point of the aerospace and defense community, as well as a bright spot in an otherwise bleak economic picture. The Unmanned Air Vehicles (UAVs) technology has rapidly improved over the last two decades in terms of materials, engines, aeronautics, guidance, navigation and controls (GNC).

This has resulted in dramatically size decrease, improved speed, payload, endurance, operation range and reliability. But more importantly, advances in electronics and computer technology has produced new intelligent UAVs that can even perform onboard processing, imaging and networking with each other in autonomous group flyers and the other units. The impressive growth and advancement of unmanned technologies show few signs of slowing, as militaries worldwide continue to adopt and adapt unmanned aircraft systems (UAS) for a variety of missions.

UAVs provide invaluable support especially for military missions such as intelligence, surveillance, target acquisition & identification, reconnaissance, surveillance, terrain mapping, and more. UAV systems combine air vehicles, sensor suites and ground-based exploitation segments as part of a network-enabled capability. Furthermore, UAV systems are multi-sensor, multi-mission and multi-platform solutions, designed to meet a broad range of military requirements. Therefore, UAV systems place great emphasis on interoperability, survivability, persistence, endurance and flight operations in military.

Some early UAVs are called drones because they are no more sophisticated than a simple, radio-controlled aircraft being controlled by a human pilot (or operator) at all times. More sophisticated versions have built-in control and/or guidance systems to perform low-level human pilot duties, such as speed and flight path surveillance, and simple pre-scripted navigation functions such as convoy and war fighter tracking.

Unmanned aerial vehicles and systems continue to grow in sophistication and complexity, spurring the aerospace and defense community to increasingly abandon use of the term "drone"-which often carries negative connotations. UAVs present some of the most

difficult design challenges. It is because of the need to package a high level of computing power and data collection/distribution components within minimal size, weight, and power (SWaP) constraints-all while preserving ruggedized capabilities to operate in very demanding environments.

In this respect, secure communication links are vital for UAV operation, both to control the UAV based on mission objectives and to deliver data reliably to mission controllers on the ground. Encryption and decryption are inherent requirements, adding complexity and cost in the UAV electronics.

Since the US Federal Aviation Administration (FAA) re-authorization bill was signed in February 2012, giving the green light for commercial operation of UAVs, the industry has been abuzz with new opportunities for implementation. These unmanned systems are no longer primarily associated with war and combat situations. With a deadline of Sept. 15, 2015 for full integration into U.S. airspace, it is highly likely that UAVs will play an increasing role in most critical infrastructure operations.

Industries such as public safety, land/crop surveying and oil/gas are being eyed as key markets that can benefit from the use of unmanned systems for monitoring and surveillance. For several applications, such as wildfire monitoring and border protection, UAVs can even be used to protect people and save lives.

As this implementation of UAVs continues to expand, airspace will naturally become more crowded. It is going to be critical for UAVs to be operationally sound and designed with secure data transmission in mind. Therefore, the communications network in which the UAV operates plays an essential role in meeting security requirements and without its C2 link, a UAV cannot operate. Additionally, UAVs with unsecure and unproven C2 links are vulnerable to failure and even hijacking.

I. GENERAL DESCRIPTION OF UAVs

I.1. Types

Military UAVs are basically categorized in three types in terms of range/altitude and endurance:

- Tactical UAV (TUAV)
- Medium Altitude Long Endurance UAV (MALE UAV)
- High Altitude Long Endurance (HALE UAV).

TUAVs are small and inexpensive with limited payload, range and endurance. Flying altitude is more than 5 000ft and range (up to 50 km) is usually limited to line of sight of the ground control station. Typical payloads for a TUAV are 50 kg. These UAVs are used for

surveillance purposes. Typical examples of the TAUV are Phoenix (UK), Sender (UK), Hunter (Israel/US), and Vulture (South Africa).

MALE UAVs are relatively large and expensive with considerably enhanced performance over the TUAV. Flying altitude is more than 20 000ft. Payloads can be up to 300 kg, with much greater range (over 200 km) and endurance than the TUAV. These UAVs are used for reconnaissance purposes. Typical example UAV systems are Spectator (UK), Hermes 450 (Israel), TIHA (Turkey), Predator (US), Houros (France/US).

HALE UAV can be substantive craft with endurance in excess of 12 hrs, and payload capacities of up to 800kg and above. These UAVs are used for strategic surveillance purposes. Typical examples of such UAV systems include: Global Hawk (US), Hermes 750 (Israel). However, Uninhabited Combat Air Vehicles (UCAVs) are another UAV application more debated by the UAV Community.

I.2. Design

Technically, the UAV system can be characterized by an air system and a ground system, interconnected by data links, control links, and integrated into a technical and decision-making environment. Several sensor/payload packages will be required in order to perform different military missions. Depending upon the size of the UAVs, those sub-systems are combined together to enhance mission capability.

To analyze UAVs vulnerabilities, it is important to understand what components an UAV is made of and how these components interact. In order to analyze UAVs on a common basis, we described UAVs in terms of component models.

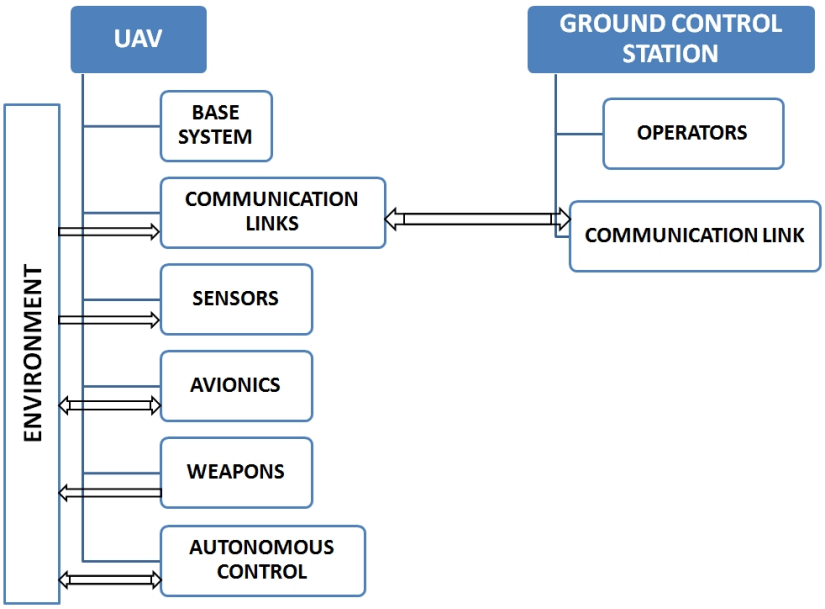


Figure 1 Extended UAV component model with information flow

The “UAV base system” is the foundation of the UAV linking together the UAV components. It is needed to allow inter-component communication and controls the sensor, navigation, avionic and communication system. It may be considered as an UAV “operating system”. The base system also allows the integration of further optional components such as special sensors or weapon systems.

The UAV sensor system consists of the sensory equipment of the UAV together with integrated pre-processing functionalities. For common military UAVs these sensors are often cameras with different capabilities. UAVs may be equipped with further sensors, such as INS, GPS and radar.

The UAV avionic system is responsible for the conversion of received control commands to commands of the engine, flaps, rudder, stabilizers and spoilers.

The in-flight communication of UAVs is always wireless and may be divided into two types:

- direct, line-of-sight (LOS) communication and
- indirect- mostly - satellite communication (SATCOM).

The information flow within the extended UAV component model may differ, according to the UAV type. The exact internal communication may be relevant for an attacker, if the attacker already has access to the internals of the system. Otherwise it is not essential.

Unless physical access to the UAV is given, an attacker must access and influence the UAV externally. Luckily for an attacker, UAVs are highly dependent on external input and therefore provide multiple input channels. Due to the “wireless nature” of UAVs, these channels are wireless and hence difficult to harden.

There are several information flows between an UAV and its environment but the two most important operational connections are:

- the bidirectional information flow between the communications system and the ground control station (GCS)
- the information flow from the environment to the sensors.

However, additional influences between the environment and the UAV must be considered. These influences are the changes of the attitude of the UAV induced by the avionics, the result of weapons on the environment and the influence of the environment on the communication links.

An extended UAV component model, along with the information flow between the UAV system and the environment and between UAV components themselves is presented in the picture below.

II. UAV DATA LINKS

One of the most critical components of a UAV system is the data link between the UAV itself and the ground control station (GCS). Data Link system should be able to collect their data and transmit them to the GCS. Hence, the success of UAV's missions conducted is extremely dependent on the availability of robust, high performance communication data links. In addition, using high capacity data links on UAVs has became an inevitable need because of the developments in the optical and electronic sensor field. This requirement is met by using digital based data links through satellite or in the Line of Sight (LOS). These digital data links used primarily in military applications provide the capabilities of high data transmission rate in a low bandwidth, jam resistance, transferring image, data and voice information in one link packet, improved speed and robust link protocol, high resolution data, dynamic sampling rate, and secure and observable data.

Commonly used frequency bands for UAVs are UHF/VHF, S and C bands, but these analog data links do not meet the demand of desired data link rate of today. Therefore, more efficient frequency bands of L, X and Ku are used in UAV systems today. However, such a near-term solution still has some performance gaps.

Today, extensive research and development effort is dedicated to data link systems for UAVs. These data link systems constitute a new family of communication system which merges the demands for mobility, high data rates and ultimate security. The most widely used UAV communication links and technology trends are data links such as CDL, TCDL, TDDL, HIDL and DVA.

II.1. Common Data Link (CDL)

The Common Data Link (CDL) program is designed to achieve data link interoperability and provide seamless communications between multiple Intelligence, Surveillance, and Reconnaissance (ISR) collection systems operated by armed services and government agencies. CDL provides full-duplex, jam resistant, digital microwave communications between the ISR sensor, sensor platform, and surface terminals. The CDL Program establishes data link standards and specifications identifying compatibility and interoperability requirements between collection platforms and surface terminals across user organizations.

CDL is a full-duplex, jam resistant spread spectrum, point-to-point digital link. The uplink operates at 200kbps-and possibly up to 45Mbps. The downlink can operate at 10.71 - 45 Mbps, 137 Mbps, or 234 Mbps In addition; rates of 548Mbps and 1096Mbps will be supported. The CDL family has five classes of links:

- Class I - Ground-based applications with airborne platforms operating at speeds Mach 2.3 at altitude up to 80,000 ft.
- Class II - Speeds up to Mach 5 and Altitudes up to 150,000 ft.
- Class III - Speeds up to Mach 5 and Altitudes up to 500,000 ft.
- Class IV - Terminals in satellites orbiting at 750nm.
- Class V - Terminals in relay satellites operating at greater altitudes.

II.2. Tactical Common Data Link (TCDL)

The aim of the Tactical Common Data Link (TCDL) is to develop a family of CDL-compatible, low-cost, light weight, and digital data link with the capability to support a wide range of Intelligence, Surveillance and Reconnaissance (ISR) applications. The TCDL is a secure data link currently being developed by the U.S. military to send secure data and streaming video links from airborne platforms to ground stations. The initial TCDL design will be targeted for UAV applications (e.g., Predator and Outrider). In the future TCDL design is expected to be extended to additional manned and unmanned applications.

The TCDL can accept data from many different sources, then encrypt, multiplex, encode, transmit, demultiplex and route this data at high speeds. It uses a Ku narrow band uplink that issued for both payload and vehicle control, and a wide band downlink for data transfer. The TCDL uses both directional and omni-directional antennas to transmit and receive the Ku band signal. The TCDL was designed for UAV's, as well as manned non-fighter environments. The TCDL transmits radar, imagery, MPEG II video and other sensor information at rates from 1.544 Mbps to 10.7 Mbps over the range of 200 km, these rates will expand to 45 and 274 Mbps, and finally it has the option of flexible I/O support. The TCDL return link must be designated to operate in the 14.4 to 14.83 GHz band, and the forward link must operate in the 15.15 to 15.35 GHz band. The TCDL design goal for LOS slant range is 200km at 15 000ft above ground level.

II.3. Tactical Digital Data Link (TDDL)

The Tactical Digital Data Link **(TDDL)** is a new generation advanced digital data link system developed specifically designed for UAVs and other unmanned aerial platforms

requiring highly secure communication combined with extended range and excellent reliability. The TDDL provides point-to-point, full-duplex, jam-resistant and digital microwave communications between sensor platforms and control terminals. Software Defined Radio (SDR) technology used in TDDL allows for flexibility and programmability of coding modulation and data rates and includes provision for interoperability with TCDL and STANAG 7085.

The TDDL has high data rates, extended range, provision for airborne relay, range and direction measurement options, low latency, selectable bit rate, high video quality for target identification/tracking, Forward Error Correction, variable rate interleaving, direct sequence waveform, efficient spectrum utilization, anti-jamming: SpSp, FH(optional), provision for encryption, digital video compression, MPEG 2/4 compatibility, multiple sensors/payloads, interfaces for SAR and FLIR sensors, lightweight airborne terminal, convection cooled, compact packaging, high reliability, very low life-cycle costs, Built-In Test and Built-In Calibration.

The TDDL has range up to 200 km without relay, data rate for uplink is about from 9.6 to 200 kbps, for downlink 1.6 to 10.71 Mbps, modulation is BPSK for uplink, quadrature phase-shift keying (QPSK) for downlink, error correction codes are convolution, concatenated, interleaving, control interfaces are Mil-Std-1553B, RS-422, 10/100 Base-T; remote operation via F/O interface available, less than 6 kg low weight.

The TDDL has wide range of frequency bands of Ku and band from 14.40 to 15.35 GHz. And other bands (S, C, X) are also available. Transmitter power output is about from 2W to 10W. Power consumption is less than 200W. Airborne antenna options are omni, sector or one-axis steerable. On the other hand, ground base antenna options are omni, one-axis steerable, or 2-axis directional antenna with integrated pedestal and monopulse tracking system or GPS based tracking. It also has airborne relay configuration for over-the-horizon missions.

II.4. High Integrity Data Link (HIDL)

The HIDL consists of airborne and surface-based terminals with a full-duplex, narrow- and jam-resistant data link operating in broadcast mode to control at least two UAVs simultaneously up to ranges of 200 km. It has a requirement of being able to operate with the wideband TCDL. It will operate at 225 - 400MHz (UHF) and 100 kbps bandwidth. The HIDL is being developed on the basis of a new NATO standard, STANAG 4660.

The HIDL is a robust digital data link and will assist operators in making safe UAV takeoffs and landings on ships and also allow the transfer of sensor photos and data to naval vessels and other surface terminals for operators to study and disseminate. HIDL also offers variable data rate from 3 Kbps to 20 Mbps, backup for CDL, uses time and frequency diversity for resistance to jamming, uses any available RF channels, even if non-contiguous, low latency for safe control during launch and recovery.

The HIDL's command & control (C2) link was developed to cope with the most challenging operational requirements. It is provided robust C2 of UAV using a secure anti-jam waveform and offers highly reliable RF connectivity in all environments. With the decreasing availability of the RF spectrum, HIDL importantly has the ability to control multiple UAVs simultaneously. In addition to these benefits of HIDL, it includes over-the-horizon relay functions.

II.5. Digital Video over Analog (DVA)

The Digital Video over Analog (DVA) is a new technology which enables simple conversion of older FM analog video links to encrypted digital links. The DVA converts to an encrypted digital video link without replacing any of the RF equipment in either the UAV or the ground. The improved digital performance increases UAV video link range by a factor of four while using only a quarter of the bandwidth of analog video links.

The DVA can transmit 2 Mbps of IP data simultaneously with compressed FMV (Full Motion Video) using the same FM video transmitter that was designed for a single analog video channel. A digital link is essential for the newer IP-based payloads and the overall need to use bandwidth efficiently. The DVA receive unit outputs both NTSC video and an Ethernet stream with H.264 compressed video and Key-Length-Value (KLV) metadata, which is a smarter data encoding approach, elementary streams embedded in an MPEG2 transport stream.

In Table 1, it is given examples of different configurations of military UAVs used in various countries. For instance, Global Hawk carries an EO/IR sensor and a SAR with moving target indicator (MTI) capability, allowing day/night, and all-weather reconnaissance. Sensor data is relayed over CDL LOS (Xband) and/or beyond LOS (BLOS) (Ku-band SATCOM) data links to its mission control element, which distributes imagery to up to seven theater exploitation systems.

Name	Data link
Heron /Israel	Direct LOS Relay for Beyond LOS(BLOS) via SATCOM Ground-based data relay
Global Hawk /USA	Wideband SATCOM (either Ku or UHF) CDL for direct down link of imagery LOS
Predator/ USA	C-band LOS SATCOM (UHF and Ku)
Tipchak /Rusia	Real-time digital data link
EADS/SIDM /France	LOS SATCOM
Tiha /Turkey	Direct LOS (C and UHF) SATCOM (X-band) BLOS, data relay
Bateleur /South Africa	LOS, BLOS(Ku band) 750km/4000km range
Fire scout /VTUAV /USA	L-3 Comm TCDL 280 Km LOS distance

Table 1 – UAV different types of data link

The characteristics of main data link used in UAV communication technologies are described in table below:

System	Data link Type	Data Link Rate	Data type	Frequency Band	Range
CDL	LOS	10.71, 137, or 274 Mbps Downlink	Data, Video, Image	I,X,S,Ku Band, UHF	> 200 km
TCDL	LOS/BLOS	1.544 to 10.7 Mbps Downlink	Data, Video, Image	Ku Band, UHF	> 200 km
TDDL	LOS/BLOS	1.6 to 10.71 Mbps Downlink	Data, Video, Image	S,C,X,Ku Band	200 km w/o relay
HIDL	LOS/BLOS	3 Kbps to 20 Mbps Downlink	Data, Video, Image	UHF	200 km w/o relay

Table 2 – Data link characteristics

III. UAV VULNERABILITIES TO CYBER ATTACKS

The large diffusion of UAVs imposes a serious analysis under the security perspective. The vehicles are equipped with high technology components, each system could be potentially subject to cyber-attack with serious repercussions. The nightmare of military security experts is the hijacking of the vehicle by remote attacker that could gain the access to the vehicle using it against the forces that manage it.

The UAVs manage a huge quantity of information during a mission. They acquire information from the field using various sensors, GPS systems and cameras, they execute specific flight plans and manage data related to asset located on the territory and for example, in military context they have the exact location of troops on the battlefield including the basics of landing. A possible violation of the control system of a drone could represent a drama because the militias that launched it, they could lose the control of the vehicle and the attacker silently could have access to sensitive information for the evolution of conflict.

The interest in UAV cyber security has been raised greatly after the Predator UAV video stream hijacking incident in 2009, where militants used cheap, off-the-shelf equipment to stream video feeds from a UAV. With greater funding and skills, the possible damage due to a cyber attack is a major concern. The U.S. Army, Air Force, and Department of Defense have all shown clear interest in defending against cyber attacks on deployed UAVs.

There are several ways to cyber attack an UAV but basically, the attacks should be directed either on the sensors or on UAV's communication links, in both cases the consequences of the attack being really serious.

III.1. ATTACK ON UAV'S SENSORS

a) GPS spoofing attack

The principle behind the GPS spoofing attack is to send fake geographic coordinates to the UAV's control system and, by doing so, to deceive the on board system in relation to the UAV position and to hijack the vehicle in a different place for which it was commanded.

An UAV could be directed somewhere using its GPS but a spoofer can make the UAV think that it's somewhere else in space and theorethically, it can be made to land/crash on a selected target. This scenario wouldn't be too hard for a very skilled attacker, who has the ability to manipulate the unencrypted signals sent to the UAV and spoof these signals.

"GPS spoofing" is the principal threat to GPS receivers that are fooled into tracking fake GPS signals. Unlike in case of GPS jamming , when signals are basically interrupted and

they no reach the GPS anymore, in the case of spoofing the targeted receivers are deceived into believing a reality induced by the attacker.

The GPS receiver installed on the UAVs works exactly as any other GPS devices, observing the signals from a set of satellites and using the relative delays of the signals to solve the equations which determine the position of the vehicle and the time offset of the receiver (Fig.2) .

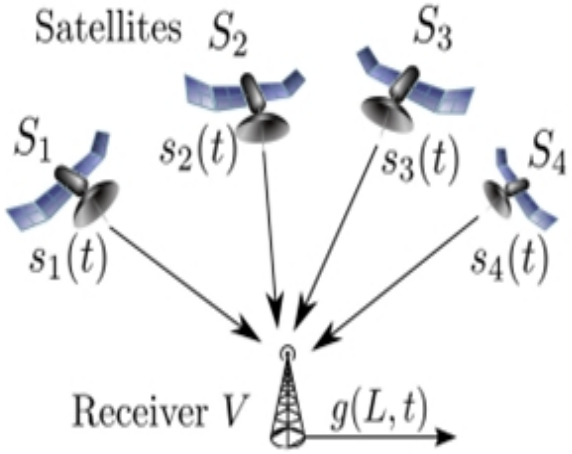


Figure 2 – GPS Satellites

In the attack scenario, the victim uses a GPS-based localization system which is synchronized to the legitimate satellites. The attacker starts sending own spoofing and jamming signals forcing the victim to synchronize to the attacker's signals.

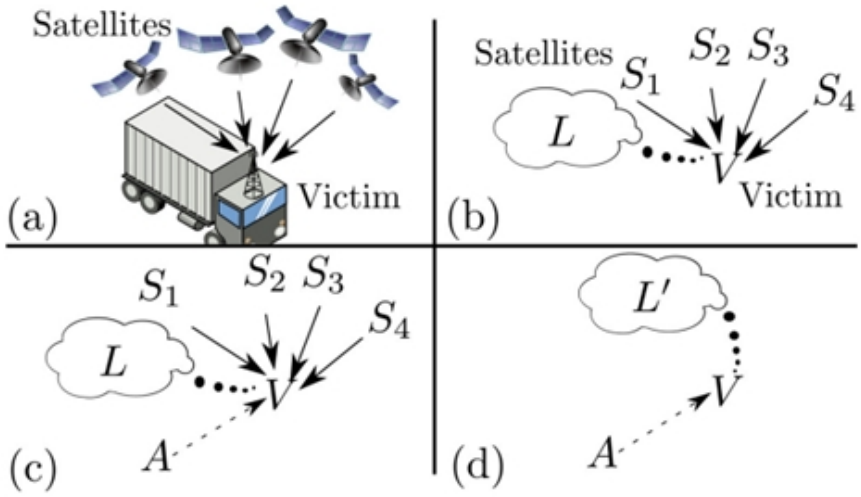


Figure 3 – GPS Spoofing attack

During the attack, the GPS signals can be spoofed by a hacker that could gain complete control of wireless traffic by intercepting, injecting, modifying, replaying, delaying, and blocking messages without temporal constraints for individual receivers.

There are meaningful differences between attacks against civil and military GPS systems.

Attacks on civilian (unauthenticated) GPS

The attacker can delay signals or send them prematurely, due the absence of authentication mechanisms he can modify the content of received GPS signals or arbitrarily generate the spoofing signals using the public GPS parameters. On standard GPS receivers plausibility or consistency of the data content in the received GPS signals is not verified and a hacker could use a GPS signal generator to create specifically crafted GPS messages to be send to the target, modifying the claimed locations of the satellites.

Attacks on military (authenticated) GPS

The attacks against the military system present a greater difficulty due to the implementation of authentication mechanisms. The attacker could not generate valid GPS signals, but he can capture and relay existing ones (e. g. By separating signals from different satellites using high-gain directional antennas and broadband transceivers (called Selective-Delay in).

Note that neither the spreading codes nor the data content of the signal need to be known by the attacker for a successful selective-delay attack. The hackers can operate on a delay time of signals and amplify or attenuate them.

The spoofing generation methods could be divided into three main categories:

GPS Signal Simulator – GPS signal simulator is concatenated with an RF front-end generates authentic GPS signals. The GPS signals generated by the attacker do not essentially synchronize to the real signals. Despite that the techniques appears very noisily it could be efficient against commercial GPS receivers especially if the spoofing signal power is higher than the authentic signals. The GPS signal simulator is easily detectable by antispoofing techniques such as amplitude monitoring and consistency checks among different measurements.

Receiver-Based Spoofers – GPS receiver is concatenated with a spoofing transmitter. This system first synchronizes to the current GPS signals and extracts the position, time, and satellite ephemeris, then it generates the spoofing signal. This technique is hard to detect but it is complex to realize due to the high correlation with victim receiver.

The technique appears impossible to be realized in the case of military systems such as the control system of UAVs.

Sophisticated Receiver-Based Spoofers – Spoofer know exactly the level position of the target receiver antenna phase center to synchronize perfectly the spoofing signal code and carrier phase to those of authentic signals at the receiver. This type of spoofer can take advantage of several transmit antennas in order to defeat direction of arrival anti-spoofing techniques. This is very complex technique, the realization of this type of spoofers being very difficult. This kind of attack is considered impossible to realize in majority of cases due to the geometry and movement of the target receiver antenna(s).

The principal prevention against these attacks is the use of cryptographic techniques, receiver and transmitter use mutual authentication processes avoiding interferences of external sources. These techniques are used only in the military sector but they should be implemented in civil sector, too.

On December 4th 2011 Iranian government captured near the Iran-Afghanistan border an Unmanned Aerial Vehicle model Lockheed Martin RQ-170 used by US force for reconnaissance missions, the event was exploited by Iran forces to make propaganda on its technological capabilities but it was mainly an opportunity to study the components that equipped the drone including the data managed for its missions.

The public was surprised by the perfect condition of the vehicle captured by Iranian forces, the status of the vehicle was visible in the images broadcasted by Teheran inducing security experts to think that the Iranian cyber units were able to hack the aircraft or in any case to force him to a secure landing causing a system failure.

Iranians claimed that they first jammed its communications links, which disconnected it from ground controllers and made it switch to autopilot; it also interrupted the secure data flow from the GPS satellites. The drone was forced to search for unencrypted GPS frequencies normally used by commercial aircraft. At this point, the Iranians said, they used a technique called “spoofing” – sending the plane wrong GPS coordinates, tricking it into believing that it was near its home base in Afghanistan. And so it landed on Iranian territory, directly into the welcoming arms of its kidnappers.

The US rejected the hacking scenario, insisting that its flying robot simply had malfunctioned. Military drones usually have a back-up system to guide them home automatically if contact with operators is lost. But that clearly didn’t work.

Todd Humphrey, assistant professor at the University of Texas at Austin’s Radio navigation Laboratory, has demonstrated with his research that hacking a civilian drone in not so complicated. The professor did it in front of the Department of Homeland Security, in various interviews and presentation the researcher revealed that using a limited budget and

with a small group of individuals, he is able to send signals to an Unmanned Aerial Vehicle's GPS receiver, hijack the aircraft in mid-air, and control its route.

Humphrey demonstrated to Homeland Security agents that spending around $1,000 on equipment and designing an application able to send signals to the drone's GPS receiver he is able to gain complete control of the vehicle.

"The navigation systems of these drones have a variety of sensors," "…but at the very bottom is a GPS unit — and most of these drones that will be used in the civilian airspace have a civilian GPS unit which is wide open and vulnerable to this kind of attack. So if you can commander the GPS unit, then you can basically spoon feed false navigation information in the navigation center of these drones." explained Humphreys.

Another report issued in March this year states that a U.S. surveillance drone flying over the Crimea region of Ukraine has been hacked by Russian forces. This is just one of many indications that the twenty-first-century global battlefield will take place in cyberspace. Radio and other frequencies which cover the electromagnetic spectrum is the new contested domain.

b) GPS jamming

Using jamming techniques against drones, it is possible interrupt the GPS receiving transmitted to the UAVs. In this scenario the aircraft could potentially lose the capability to monitor its route and to calculate its location, altitude, and the direction in which it is traveling.

Due large diffusion of low cost GPS jammer according principal industry experts, GPS jamming would become a serious problem, that's way security industry is also searching for alternative methods for navigating a UAS that not rely on GPS and that could integrate modern control systems.

GPS signals result very vulnerable to jamming attacks that differently from spoofing attacks have the unique intent block reception of information at receiver side, incidents related to GPS jamming are have occurred several times in the past.

GPS jamming is also used as an electronic warfare mean, the North Korea has used this technique to interfere with global positioning system signals of South Korea's two largest airports near Seoul and across the center of the Korean peninsula. Fortunately, no accident was registered but it demonstrates that the employment of this kind of cyber attack is taken into consideration at state level.

In 2010, South Korean Defense Minister Kim Tae-young declared that North Korea had imported truck-based jamming systems from Russia that is able to interfere with GPS

signals in a radius of 100 kilometers, since there various GPS-jamming incidents were observed in the area.

Jamming the communication, then the operator becomes blind and the UAV will fly until it crashes or it will land due an emergency procedure or the fuel is finished.

A solution to the attacks is production of equipment having spoofing or jamming detectors and used encrypting GPS signals, like the military does.

III.2. ATTACK ON UAV'S COMMUNICATION LINKS

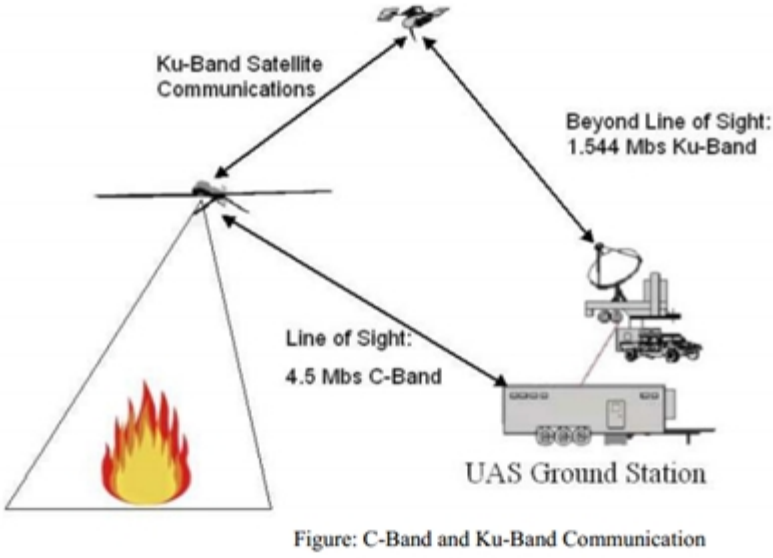


Figure 4 – UAV communication links

For most UAVs, the satellite link tends to use the K_u-Band. The LOS communication with the GCS is often based on the C-band or WiFi b-/g- or n-standard.

a) TCDL Ku-band communication

The TCDL uses a narrowband uplink at 15.15 GHz - 15.35 GHz and a wideband downlink at 14.40 GHz - 14.85 GHz. The TCDL may be operated both with directional and omnidirectional antennas and has ranges of 200 km at rates from 1.5 Mbit/s to 10.7 Mbit/s and low bit-error-rates. It may be used to transmit sensor data of any kind, especially radar, images and video signals.

One characteristic of K_u-band-based communication is that it is susceptible to rain/ snow fade. Due to the high frequencies used the signal may become disturbed by air humidity.

However, K_u-band-based communication is harder to overhear and hence harder to actively disturb than other comparable communication links.

b) LOS Communication: C-Band

Generally, the C-band describes the electromagnetic spectrum ranging from 4 GHz to 8 GHz. The C-band is used by a wide range of applications, such as weather radar systems, satellite communication, cordless phones and WiFi communication.

The frequencies relevant to uplink/downlink of most UAV communication systems investigated are 4.4 - 4.94 GHz and 5.25 - 5.85 GHz.

The C-band communication is less susceptible to air humidity than K_u-band communication. Nevertheless, due to the variety of applications, several COTS- devices exist that may interfere the radio signal and cause signal distortion.

UAVs tend to use omnidirectional antennas for C-Band communication, heightening the threat of interception by third parties.

c) LOS Communication: WiFi a/b/g/n

WiFi, synonymously described as "WLAN", refers to any communication based on the IEEE 802.11-standard. The frequencies used and the transmission rates differ according to the used standard. WiFi a, referring to the IEEE 802.11 a standard, ranges from 5.15 GHz - 5.75 GHz at transmission rates of 54 Mbit/s. The b and g standard operate in the frequency range of 2.4 GHz - 2.4835 GHz at 11 Mbit/s (b), respectively 54 Mbit/s (g). The WiFi n standard may operate both at 2.4 GHz as well as in the 5 GHz range. Due to the use of MIMO (Multiple Input Multiple Output), the n standard may transmit over longer distances and higher rates (up to 600 Mbit/s). To cover longer distances and achieve higher rates, the n standard uses multiple data streams and up to 4 antennas.

Due to its multiple applications and free usage, the b and g standard must expect signal interference. The frequencies above 5 GHz are restricted; hence interferences through civil applications are less likely. However, this may change in the near future (5-GHz-WLAN)

Because of the omnidirectional antennae used in the WiFi standards, WiFi is susceptible to eavesdropping. Precautions such as tunneling and encryption may be taken, but the general risk of eavesdropping - compared to other media - is still heightened as no knowledge of the signals direction is needed to tap the signal.

An example of eavesdropping in UAV's communication is the incident happened in the summer of 2009 in Irak. Militants in Iraq have used $26 off-the-shelf software to intercept live video feeds from U.S. Predator drones, potentially providing them with information they need to evade or monitor U.S. military operations. Shiite fighters in Iraq used software programs such as SkyGrabber -- available for as little as $25.95 on the Internet -- to regularly capture drone video feeds, according to a person familiar with reports on the matter.

U.S. military personnel in Iraq discovered the problem in 2009 when they apprehended a Shiite militant whose laptop contained files of intercepted drone video feeds. In July, the U.S. military found pirated drone video feeds on other militant laptops, leading some officials to conclude that militant groups trained and funded by Iran were regularly intercepting feeds. The potential drone vulnerability lay in an unencrypted downlink between the unmanned craft and ground control. Since then, all modern US UAV have been equipped with new encryption devices and all Predators and Reapers are to see their video communications secured this year.

III.3. CYBER-ATTACKS MALWARE BASED AGAINST UAVs

An UAV, more in detail the software that equips its component could be hit by malicious code able to infect civil of military environments. The menace is concrete and it probably already happened in US military networks. In October 2011, Wired Magazine reported a virus infected drone remote control system, in particular the malware captured strokes on a keyboard in drones' cockpits at Creech Air Force Base in Nevada, made it tricky for the pilots who remotely fly assault drones like the Predator and Reaper.

Military network security specialists weren't sure whether the virus and its so-called "keylogger" payload had been introduced intentionally or by accident; it may have been a common piece of malware that just happened to make its way into these sensitive networks. The specialists didn't know exactly how far the virus has spread. But they were sure that the infection had hit both classified and unclassified machines at Creech. That raised the possibility, at least, that secret data may have been captured by the keylogger, and then transmitted over the public internet to someone outside the military chain of command.

The malware used did not appear sophisticated but security experts spent a couple weeks before to completely immunize the system.

CONCLUSIONS

The various types of attacks described and the intense activities of foreign governments and cyber terrorists must set a maximum level of alert for UAV manufacturers. In future years these technological marvels will crowd the skies, security must be first requirement and a multilevel approach is necessary to prevent incidents caused by the different cyber threats. In US only, the number of medium and large Unmanned Aerial Vehicles — RQ-4 Global Hawk-class, MQ-9 Reaper, and MQ-1 Predator-class unmanned aircraft systems — will grow from approximately 340 in [Fiscal Year] 2012 to approximately 650 in FY 2021.

The mission to secure UAV communications is not simply due to the evolution of methods of attack and the sophistication level of the agents used, it is absolutely necessary a joint effort of defense manufacturers, industry, government and private companies.

Wireless communication devices that leverage data encryption capabilities, adhering to FIPS and AES standards, are already heavily relied on for mission-critical government and defense applications, especially when it comes to unmanned systems and UAVs. There are a lot of specific security and data encryption standards to support the reliable transmission of data in Unmanned Aerial Systems.

Furthermore, some wireless technologies that are proven to be reliable and secure in nature can further add to the overall data security scheme. For example, frequency-hopping spread spectrum wireless technologies can leverage coordinated, rapid changes in radio frequencies that literally “hop” in the radio spectrum, thus evading detection and the potential of interference.

Furthermore, some leading wireless data link solution providers also can deliver multiple user defined cryptography keys (as many as 32 user-defined keys in some cases), allowing users to change key positions on demand.

With a secure data link in place, UAVs are far less likely to suffer from technical errors. This is a very important consideration because not only will there be more aircrafts operating in commercial airspace, but many will transport critical information where failure to operate is not an option.

Advanced UAV sensor payloads are acquiring a wealth of data, including full-motion video (FMV) and high-definition (HD) images. Bandwidth is often limited, however, and can prevent the transmission, sharing, and display of mission-critical information. Such network limitations are driving the need for efficient data processing directly on the UAV.

Militaries and technology firms worldwide are focused on the ability to do as much autonomous onboard processing as possible and to reduce the volume of data exchanged between the UAV and ground station and the goal is to exchange processed information instead of a raw data stream.

As the UAV industry continues to reach important milestones, there is clear indication that the UAVs are also implemented into commercial airspace. With this in mind, there needs to be a level of assurance that the unmanned aircrafts in our skies will be operating safely and benefitting many industries, which all starts with the security of their communication links.

REFERENCES

1. Kim Hartmann, Christoph Steup - The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment, 2013 http://www.ccdcoe.org/publications/2013proceedings/d3r2s2_hartmann.pdf
2. Pierluigi Paganini – Hacking drones……..overview of the main threats, 2013 http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/
3. Nils Ole Tippenhauer - On the Requirements for Successful GPS Spoofing Attacks, 2011, http://www.syssec.ethz.ch/research/ccs139-tippenhauer.pdf
4. Alan Kim - Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles, 2012, http://arc.aiaa.org/doi/abs/10.2514/6.2012-2438
5. Mustafa Dinc - Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles, 2013 http://ftp.rta.nato.int/public/PubFullText/RTO/MP/RTO-MP-SCI-202/MP-SCI-202-08.pdf
6. http://www.bbc.com/future/story/20140206-can-drones-be-hacked
7. http://www.online.wsj.com/news/articles
8. http://www.bbc.com/news/technology-18643134
9. http://www.ibtimes.com/drones-which-countries-have-them-surveillance-military-operations-map-1264271
10. http://www.washingtontimes.com/news/2013/nov/10/skys-the-limit-for-wide-wild-world-of-drones/?page=all
11. http://www.militaryaerospace.com/articles/print/volume-24/issue-7/special-report/uav-command-control-communications.html
12. http://theaviationist.com/2013/12/30/unmanned-military-systems-roadmap/
13. http://www.acqnotes.com/News/2013/12/30/uav-integrated-roadmap-2013-2038/
14. http://www.milsatmagazine.com/story.php?number=893938022
15. http://www.wired.com/2011/10/virus-hits-drone-fleet/
16. http://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/
17. http://www.homelandsecuritynewswire.com/dr20140411-hacked-u-s-surveillance-drone-over-crimea-shows-new-face-of-warfare
18. http://www.wired.com/2011/05/double-unmanned-air-force/
19. http://www.milsatmagazine.com/story.php?number=893938022

WIRELESS NETWORK SECURITY

Author:
Mr Mohammad AL-KUWARI

Introduction

This paper will examine wireless network security and why some governments and companies resort to control and surveillance on the internet contents. Wireless security has become urgent necessary for many companies, individuals and countries as well due to increasing of hackers. The Internet has become a growing source of important information over the past years. Statistics say there are over two million new Internet users per month.

In this paper, the issue to be discussed is about the many different ways of wireless network security. These different fields of computer security depend on one another in a way providing for a secured network. For example, in the case of one or more computer security areas are not recognized, so is the whole organization's network. An example of this is in the area of computer virus or worm protection.

In addition, it is important to establish a computer security system because a number of organizations are be damaged by hostile software or attackers, called hackers. Damages or destruction of computer systems may as well include destruction or damage of interior data and, loss of sensitive information to parties of hostile and so on.

Internet is a collection of computer networks in the world connecting users worldwide. Internet protocols are a complex database through hardware and programming established to control the information in the full GPS Internet. IP is the main source network layer protocol used on the Internet, which is responsible for the processing of Internet usage.

Wlan Security

WLANs are best security method that is suitable for home users, small networks, or networks with low security requirements. In coping with developing of wireless networks in business environments and companies, Wlan security is used for implementing security mechanisms that are equivalent to wire-based LANs. This security requirement needs to restrict access to the wireless network only to valid users. Physical access of the WLAN is different than access to a wired LAN. This is because there is existing wired network that

include access points as RJ45 connectors. Such connectors are located inside buildings that might be secured from unauthorized access through the use of such devices as keys and/or badges.

The user shall have physical access to the building with plug a client computer into a network jack. A wireless access point (AP) may be accessed from off the premises if the signal is detectable. Thus, wireless networks need secure access to the access point in a different manner from wired LANs. It is necessary to isolate the Access Point from the internal network particularly until authentication is verified. The device attempting to connect to the access point must be authenticated. Once the device is authenticated then the user of the device can be authenticated. At this point the user may desire a secure channel for communication.

Wireless Physical Transport

The wireless signal that carries the data may be transmitted using electromagnetic waves in the either radio frequency (RF) or infrared frequency (IR) portion of the electromagnetic wave spectrum. If radio frequency Transport is used then the *Spread Spectrum* method is employed to generate the signal. The spread spectrum method expands the initial bandwidth and "spreads it out" in order to use a portion of the expanded bandwidth for portion of the message. Two common variations of the spread spectrum technique are the Frequency Hopping Spread Spectrum (FHHS) and the Direct Sequence Spread Spectrum (DSSS).

When the FHSS variation of the spread spectrum is used, non-consecutive portions of the spread spectrum are used to transmit consecutive portions of the message. The transmitted message will be received out of order unless the receiver knows which portion of the spread frequency to tune to and how long to listen before hopping to the next frequency for a specific time period.

An analogy would be listening to a song on the radio where the consecutive portions of the song are broadcast sequentially but on different stations. To hear the song correctly the listener would need to tune the stations in the correct sequence. The purpose of using FHSS is security and to reduce signal interference. Radio frequency is most commonly used of the two physical transport methods. In particular, the 802.11 standard employs the Industrial, Scientific, and Medical (ISM) RF band of the electromagnetic spectrum. This ISM band is specified as:

• the I-Band from 902 MHz to 928 MHz,

• the S-Band from 2.4GHz to 2.48GHz, and

• the M-Band from 5.725GHz to 5.85GHz.

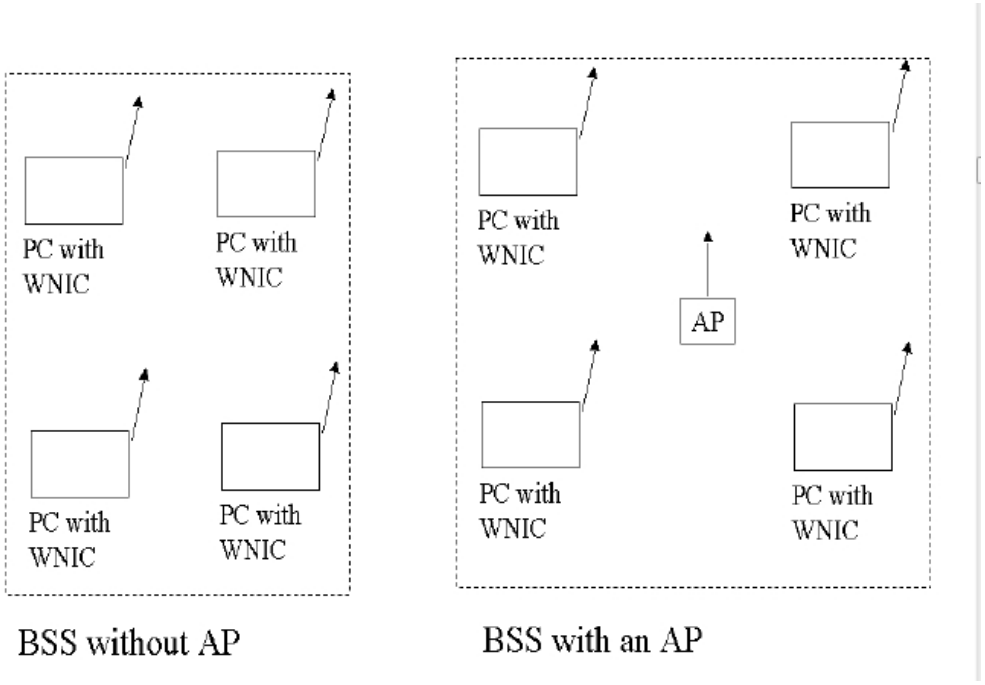
These bands are unregulated since they are used with low power. However, operating at low power limits the distance at which these signals can be detected. For example, depending on circumstances, using the S-band with a bandwidth of 1Mbps the distance varies anywhere from 300 feet indoors to 1500 feet outdoors.

Wlan Architecture

A WLAN architecture is built from stations and an access point (AP). The basic structure of a WLAN is the Basic Service Set (BSS). A BSS may either an independent BSS or an infrastructure Basic Service Set. In an independent Basic Service Set, the stations communicate with one another directly if they are within

range of each other. These are sometimes referred to as *ad hoc* networks and generally last for a short time. These ad hoc WLANs are typically used for meetings and allow the participants to share data with one another. To participate in an ad hoc WLAN, the participants place the wireless network interface card (WNIC) of their devices into "ad hoc" mode. This mode allows a station to establish a connection with any other station in its proximity.

Figure 1 Basic Service Sets With And Without Access Point



Source: Boncella, R. 2002. Wireless Security: An Overview. Communications of the Association for Information Systems Volume 9. P.p 269-282.

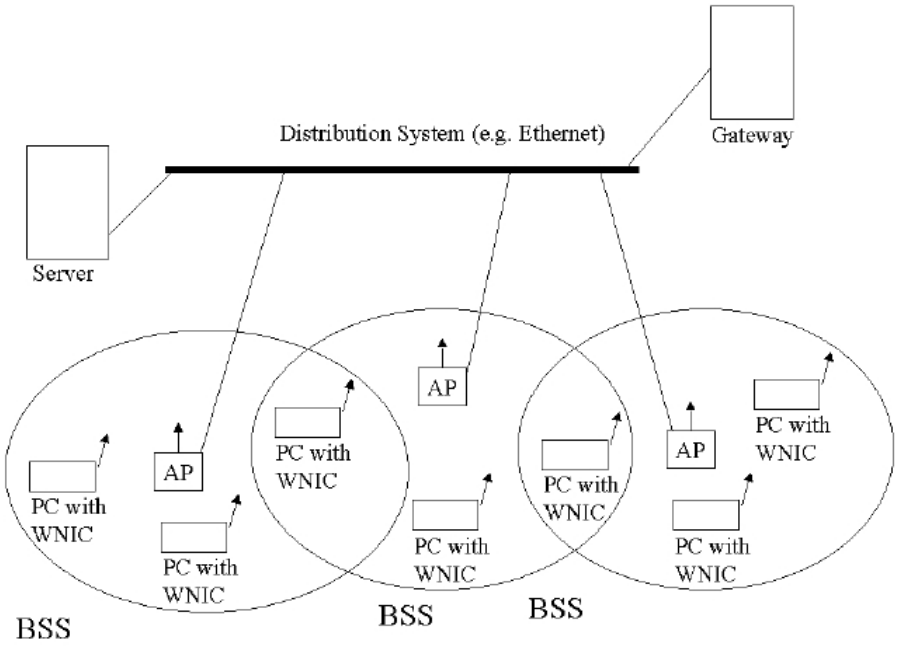
An infrastructure Basic Service Set requires the use of an access point (AP). The AP is used for all communications between stations. If one station wishes to send a transmission to another, the sending station sends its transmission to the access point. The access point then

relays this transmission to the receiving station. This transmission requires two hops and will slow the WLAN. However the distance covered by the WLAN is increased by using the access point as a relay device. An important feature of the infrastructure Basic Service Set is the need for stations to *associate* to an access point. This feature can be used to set up a WLAN that has a form of restricted access.

Insertion Attacks

An insertion attack occurs when an unauthorized wireless client joins a BSS with the intent of accessing the distribution system associated with the ESS that contains the BSS. The intent is to gain access to the Internet at no cost.

Figure 2 Extended Service Set – ESS



Source: Boncella, R. 2002. Wireless Security: An Overview. Communications of the Association for Information Systems Volume 9. P.p 269-282.

Wireless LANs

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

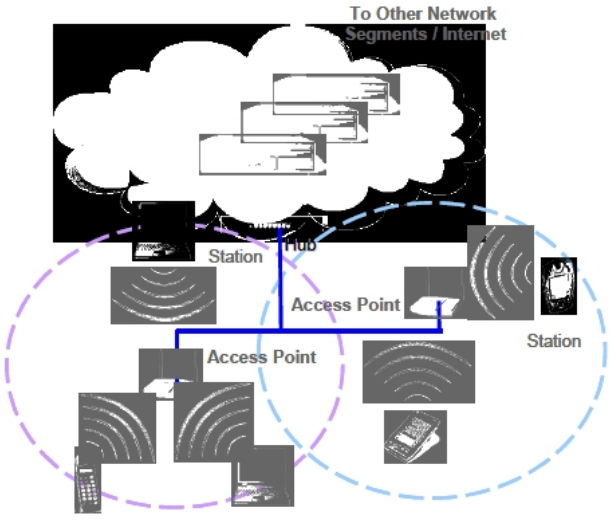
Table 1: characteristics of 802.11 Wireless LAN.

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data Rates	1 Mbps, 2 Mbps, 5.5 Mbps (11b), 11 Mbps (11b), 54 Mbps (11a)
Data and Network Security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management. (AES is being considered for 802.11i.)
Operating Range	Up to 150 feet indoors and 1500 feet outdoors.[9]
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

802.11 Architecture

The IEEE 802.11 standard permits devices to establish either peer-to-peer (P2P) networks or networks based on fixed access points (AP) with which mobile nodes can communicate. Hence, the standard defines two basic network topologies: the infrastructure network and the ad hoc network. The infrastructure network is meant to extend the range of the wired LAN to wireless cells. A laptop or other mobile device may move from cell to cell (from AP to AP) while maintaining access to the resources of the LAN. A cell is the area covered by an AP and is called a "basic service set" (BSS). The collection of all cells of an infrastructure network is called an extended service set (ESS). This first topology is useful for providing wireless coverage of building or campus areas. By deploying multiple APs with overlapping coverage areas, organizations can achieve broad network coverage. WLAN technology can be used to replace wired LANs totally and to extend LAN infrastructure.

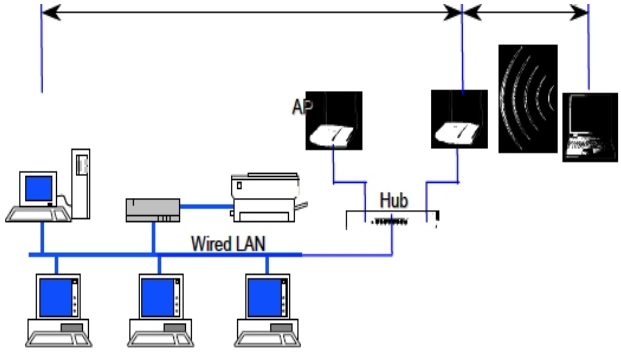
Figure 3: **Fundamental 802.11 Wireless LAN Topology**



Security of 802.11 Wireless LANs

This section discusses the built-in security features of 802.11. It provides an overview of the inherent security features to better illustrate its limitations and provide a motivation for some of the recommendations for enhanced security. The IEEE 802.11 specification identified several services to provide a secure operating environment. The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, but only for the wireless portion of the connection as shown in Figure 4

Figure 4: **Wireless Security of 802.11 in Typical Network**



Problems of 802.11 Wireless LAN Security

There are some problems related to wireless LAN security as provided and summed in the following table number 2.

Table 2: Key Problems with Existing 802.11 Wireless LAN Security

Security Issue or Vulnerability	Remarks
1. Security features in vendor products are frequently not enabled.	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. IVs are short (or static).	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. Cryptographic keys are short.	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4. Cryptographic keys are shared.	Keys that are shared can compromise a system. As the number of people sharing the key grows, the security risks also grow. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. Cryptographic keys cannot be updated automatically and frequently.	Cryptographic keys should be changed often to prevent brute-force attacks.
6. RC4 has a weak key schedule and is inappropriately used in WEP.	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 key stream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. Packet integrity is poor.	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8. No user authentication occurs.	Only the device is authenticated. A device that is stolen can access the network.
9. Authentication is not enabled; only simple SSID identification occurs.	Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.
10. Device authentication is simple shared-key challenge-response.	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

Security Threats and Risks

Presently, most of populations of the worldwide use computers in their works and deals as well as communication. Currently, computers are used in anywhere companies, banks, shops, clubs and etc……, consequently it's necessary to protect our computers from any damage or types of viruses. So that there are some procedures and steps are used to protect the computers.

History of Computer Viruses

In the mid- 1980s, two brothers in Pakistan found out that people were pirating their software. They responded by writing the first computer virus, a program that would put a copy of itself and copyright message on any floppy disk copies their customers made. This is considered simple beginning; an entire virus counter- culture has emerged. In 1987**,** Franz Swoboda found Charlie virus; and 1989 virus hit the media whereas many international mass

media talked about viruses, American called it as " Columbus Day virus" and point to "Norwegian terrorists.

In 1999, the Melissa virus was discovered. It used Microsoft Word to infect computers and was passed to others through Microsoft Outlook and Outlook Express email programs. In 2000, a new virus was found under title " "I love you" that was transmitted by email and when opened. It can be automatically sent to everyone in the user's address book.

Presently, there are new viruses sweep the planet in minutes and can corrupt data, slow networks down, or harm person's reputation. A virus was found in many organization or firm under name wild virus. Presently, there are 250 viruses exist in the wild either the virus is new or old. The present census refers to there are about 42.000 + zoo viruses. Viruses have many shapes and forms, when they carry out, it will infect other programmes.

Damages of Computer Viruses

It's known that computer viruses are one of programs that have ability to penetrate and invade the computer systems, whereas they perform with some serious actions including variety of functions such as popping up messages as a joke along with dangerous actions including delete files or even destroy the hard disk. Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation.

Viruses have badly affected systems of computer due to damages resulting from them. Such damages vary from shape to another and they can range from displaying irritating messages to stealing data or giving other users control to over the computers. There are many types of computer viruses such as Resident viruses, direct action viruses, overwrite viruses, worms, virus hoax and Trojans or Trojans horses. There are some viruses infect other programmes many times, while there are viruses infect only one. As well as there are some viruses are so selective. There are many types of viruses such as Multi- Partie Viruses, Polymorphic Viruses, Stealth viruses and Retro viruses.

Methods of protection

There are many methods of protection of wireless network including as provided in this part.

Install firewall

A firewall is a software piece of hardware that closes hackers from entering into the computers. Hackers search for the internet about the method some telemarketers dial random phone automatically. They transmit calls to thousands of computers as well as waiting the responses. So that firewalls prevent the computers from responding to such calls and blocks communications from and to sources.

Use anti- virus software

It's known that uses of anti-viruses software are so important to the computer systems to protect the computer form any penetrating. Anti-virus software can protect the computer form the viruses that destroy and corrupt the data, or even crash the computer. You shall pay attention that anti-virus software shall be updated. Most of anti-virus software includes a feature to download updates automatically in the case of connecting to the internet.

Antivirus software

In fact, there some programs can be used to protect the computer systems including anti-virus software that is considered main element and factor to fight viruses. There are some common anti-virus programs that are connected to web page. Such anti-virus may offer free or trail software. Among of these anti-viruses are ALADDIN ESAFF, MACFEE VIRUSSCAN and SYMANTEC NORTON ANTIVIRUS. Such anti-viruses offer protection from all several types of viruses, spam email and other related options as well as internet and download. Moreover, the program also notifies and alerts the user to suspicious activity on his computer.

Virus scanners

Another method to protect the computer systems are using of virus scanners. Virus scanners can detect and often disinfect due to the viruses are became to the scanners. Scanners are the most well known than anti- viruses software but they required to be updated in regular manner to recognize the viruses. On-Access scanners remain active on the computer to when are used by the users. They check files automatically and can prevent the users from using of infect files.

Use strong password and Secure wireless network

The user shall use strong passwords with eight characters at the least that are combined between letters and numbers as well as special character for example HMC@23H. the user shall protect the password itself that keep it to himself. Another way to protect the computer systems is secure wireless network. When the user uses wireless in the home, he should take all precautions to secure it against hackers. He should wireless router with an encryption feature and turn it on. It's know that encryption of WPA is stronger than the WEP.

CONCLUSION

Finally, I can conclude that computers are venerable to many damages and risks that may affect badly their systems. Such damages and risk are resulted from viruses that can destroy and damage data and information, delete files, steal data and confidential information. Such viruses are considered fatal danger threat our computer systems. Whereas viruses are harmful on computer systems because it can corrupt data destroy hardware itself along with other related matters. There are many types of viruses including but not limited Trojan horses, Worms and Virus hoaxes. So that the users shall take precautionary for protecting their computer systems from such viruses, there are many steps and processes to make the computer in safe condition.

From this point, wireless network security has become urgent necessary. It should be regarded by all users to protect their networks from any damages. In the same time, much attention mainly concerned on the security aspects or wireless network, due to the rapid growth and deployment of such systems into a wide range of networks. This paper discussed some of methods of the network security and providing protection ways for maintaining wireless networks from any damages or risks.

REFERENCES

1. Banerjee, R. 2008.*Computer Networks Foundation Concepts-IV*. Birla Institute of Technology & Science. India
2. Boncella, R. 2002. *Wireless Security: An Overview*. Communications of the Association for Information Systems Volume 9. P.p 269-282.
3. Government of the Hong Kong. 2010. *Wireless Networking Security*. Hong Kong.
4. Joseph, H. 1997. *Computers and Security*. A History Of Computer Viruses –The Famous 'Trio'. *Vol. 16, No. 5* Elsevier Science Ltd
5. Karygiannis, T. and Owens, L. 2002. *Wireless Network Security 802.11, Bluetooth and Handheld Devices*. National Institute of Standards and Technology. U.S. Department of Commerce.
6. Oldfield, P. 2001. *Computer Viruses Demystified*. Sophos Plc. USA.
7. Pascual, A. E. (2006). *History of Computer Viruses. Securing the Infrastructure and Services*. Italy.