REGIONAL DEPARTMENT
OF DEFENSE RESOURCES MANAGEMENT STUDIES

THE 5th EXPLORATORY WORKHOP

"INFORMATION SECURITY MANAGEMENT -

IN THE 21ST CENTURY"

ISSN: 2286 - 2765

ISSN-L: 2286 - 2765

COORDINATOR: Military Professor Ph.D. eng. **DANIEL SORA**

National Defense University "Carol I" Publishing House
Bucharest 2012

THE 5th EXPLORATORY WORKHOP
"INFORMATION SECURITY MANAGEMENT -
IN THE 21ST CENTURY"

WORKSHOP COMMITTEE

LTC Daniel SORA, Military Professor PhD.

LTC Cezar VASILESCU, Senior Lecturer PhD.

Aura CODREANU, Junior Lecturer PhD.

SESSION CHAIRMEN

LTC Daniel SORA, Military Professor PhD.

LTC Cezar VASILESCU, Senior Lecturer PhD.

Aura CODREANU, Junior Lecturer PhD.

THE 5th EXPLORATORY WORKHOP

"INFORMATION SECURITY MANAGEMENT -

IN THE 21ST CENTURY"

21 February 2012

Proceedings of the workshop unfolded during the

Information Security Management Course

Conducted by the
Regional Department
of Defense Resources Management Studies

30 January - 24 February 2012

Braşov
ROMÂNIA

This page is intentionally left blank

CONTENTS

SCADA SYSTEMS VULNERABILITIES AS THREATS TO CRITICAL INFRASTRUCTURE PROTECTION

MAJ PhD eng Claudiu LĂZĂROAIE

I. SCADA systems

I.1 Definition

'Supervisory control and data acquisition' (SCADA) are control systems, initially designed to monitor and control industrial processes using proprietary protocols, and were typically kept isolated from other computer systems. Since these SCADA systems were never designed with security in mind, and are now being connected with business networks and the internet, they are now more than ever at risk.

Supervisory Control and Data Acquisition systems provide automated control and remote human monitoring of real world processes. SCADA systems can be used to improve quality and efficiencies in processes such as beer brewing and snow making for ski resorts, but are traditionally used by utilities and industries in the areas of oil and natural gas, electric power, rail transportation, water and wastewater (all of them defined as **Critical Infrastructures)**. It is estimated that in 2005 there were 3 million SCADA systems in use (SANS Institute 2000 – 2005).

SCADA systems provide near real time monitoring and control with time delays ranging between fractions of seconds to minutes.

Depending on the size and sophistication, SCADA systems can cost from tens of thousands of dollars to tens of millions of dollars.

I.2 SCADA system's components

Typically SCADA systems include the following components:

1. Instruments in the field or in a facility that sense conditions such as pH, temperature, pressure, power level and flow rate.

2. Operating equipment such as pumps, valves, conveyors and substation breakers that can be controlled by energizing actuators or relays.

3. Local processors that communicate with the site's instruments and operating equipment. These local processors can have some or all or the following roles:

a. Collecting instrument data
b. Turning on and off operating equipment based on internal programmed logic or based on remote commands sent by human operators or computers
c. Translating protocols so different controllers, instruments and equipment can communicate, and
d. Identifying alarm conditions

Local processors go by several different names including Programmable Logic Controller (**PLC**), Remote Terminal Unit (**RTU**), Intelligent Electronic Device (**IE**D) and Process Automation Controller (**PAC**). A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment.

4. Short range communications between the local processors and the instruments and operating equipment. These relatively short cables or wireless connections carry analog and discrete signals using electrical characteristics such as voltage and current, or using other established industrial communications protocols.

5. Host computers that act as the central point of monitoring and control. The host computer is where a human operator can supervise the processes, receive alarms, review data and exercise control. In some cases the host computer has logic programmed into it to provide control over the local processors. In other cases it is just an interface between the human operator and the local processors. Other roles for the host computer are storing the database and generating reports.

The host computer may be known as the Master Terminal Unit (**MTU**), the **SCADA Server**, or a personal computer (**PC**) with Human Machine Interface (**HMI**) software. The host computer hardware is often but not necessarily a standard PC.

6. Long range communications between the local processors and host computers. This communication typically covers miles using methods such as leased phone lines, satellite, microwave, cellular packet data, and frame relay.

SCADA systems consist of both hardware and software. Typical hardware includes a Host computer placed at a central location, communications equipment (radio, telephone line or satellite), and one or more RTUs or sensors. The host computer stores and processes the information from RTU inputs and outputs, while the RTU/sensor PLC controls the local function. The communications hardware allows the transfer of information and data back and forth between the CPU and the RTUs and sensor inputs. The software is programmed to tell the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate should the parameters go outside acceptable values. SCADA software is designed to be configured for a user's specific application. Since existing hardware is not

always compatible with the SCADA software, limited-functionality, off-the-shelf RTU hardware packages that have been specifically designed to interface with SCADA software are also available.

The figure 1 shows the setup of a typical SCADA system.

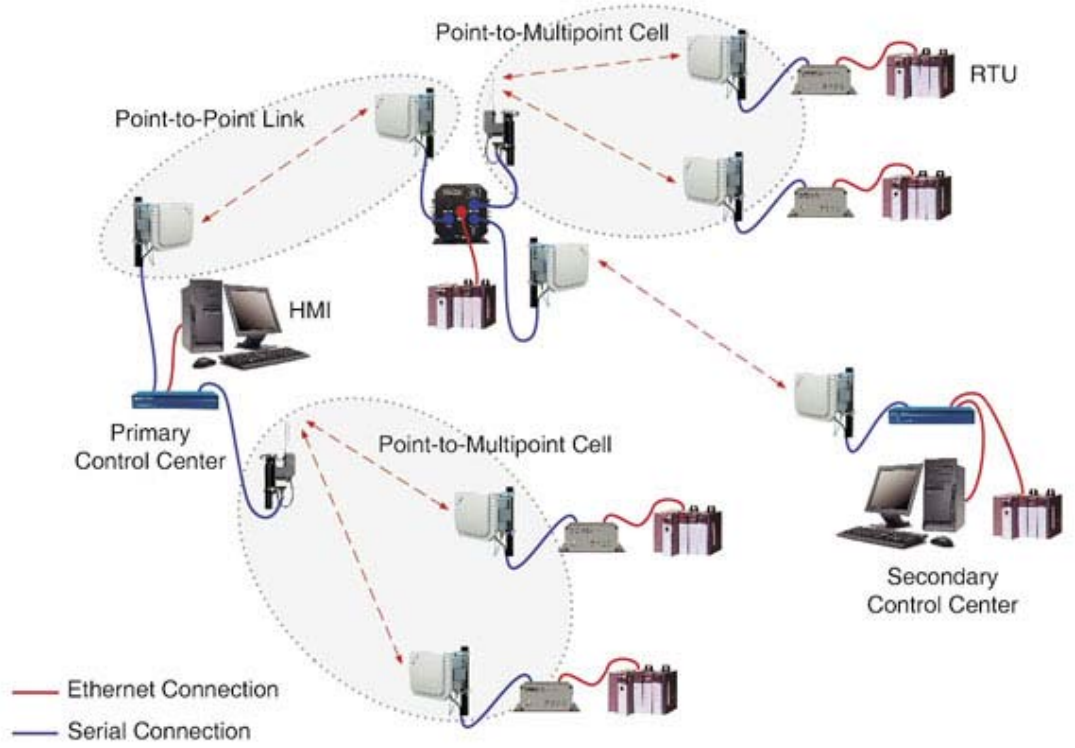


Figure 1 Typical example of SCADA systems,
(http://cfpub.epa.gov/safewater/watersecurity/guide/productguide.cfm?page=scada)

Data, such as the water level in a water tank, are generated by instrumentation (RTUs or sensors) set up at remote sites. In this example, the water level is monitored constantly, and this information is transmitted through a communications network back to a central monitoring station. Once these data are received at the central monitoring location, they can be evaluated by an operator, who can take manual actions regarding the water level, if necessary. If the SCADA system is more advanced, it could provide automatic feedback to the water tank. For example, if the measured water level is below some threshold value, the SCADA system could send a signal back and turn on a pump to fill the tank, etc.

The uniqueness of a SCADA system relative to other process control systems is SCADA's ability to monitor and control remote processes. Other process control equipment, such as Distributed Control Systems (DCSs), which have long been used in factories and in other industrial applications, is designed to control processes within a plant or application that require high processor power for the many analog functions with a given application.

However, with the increased processing power and capabilities now available in programmable logic controllers (PLCs), the outfitting of remote sites or processing equipment with remote telemetry units (RTUs) presents a viable, cost effective solution in industrial automatization. The PLC-based RTU allows communication between the outlying equipment and a central processing unit (CPU), and therefore allows a SCADA system to control both local and remote equipment and processes.

I.3 SCADA and its role to Critical Infrastructure Systems

The term "infrastructure" (according to Rosslin et al., [2]) was defined by The American Heritage Dictionary as: *"The basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, and prisons."*

The US President issued in 1996 an Executive Order (13010) which states that "*certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States*". [7] It is where the term "critical infrastructure" was highlighted. According to E.O. 13010, these critical infrastructures were: telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue) and continuity of government. Figure 2 shows the infrastructures that were commonly pointed out as "critical".

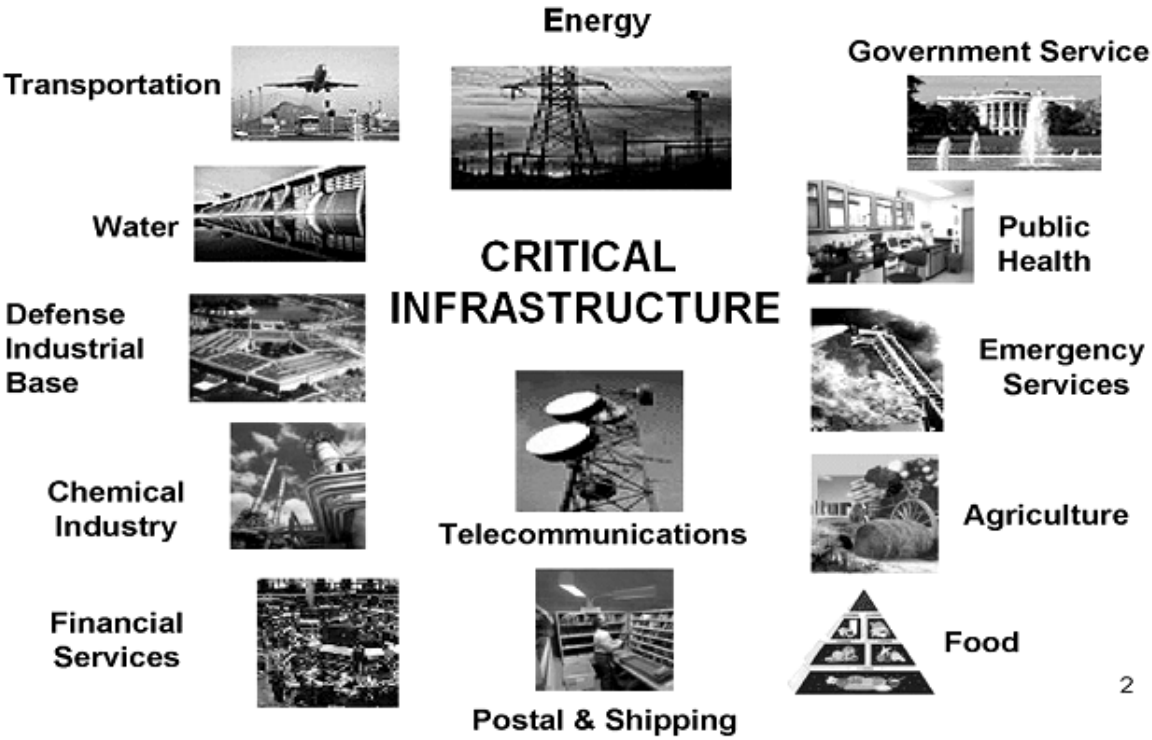


Figure 2 Critical infrastructures identified by EO 13010

(Rosslin John Robles et al., Vulnerabilities in SCADA and Critical Infrastructure Systems, International Journal of Future Generation Communication and Networking)

In the 1997 a report was released by the President's Commission on Critical Infrastructure Protection. It was a very important foundation and the beginning of a series of high profile United States Government documents recognizing the country's reliance on increasingly vulnerable, interconnected physical and cyber infrastructures. Less than a year later, in 1998, The White House acknowledged the work of the Commission and released an important policy document known as the Presidential Decision Directive 63 (PDD63). This directive defined critical infrastructure as "*those physical and cyber-based systems essential to the minimum operations of the economy and government*." It defined critical infrastructure as including: telecommunications, energy, banking and finance, transportation, water systems and emergency services. It had the ambitious goal of protecting the nation's critical infrastructure by 2003.

Significantly, the PDD63 established the principle elements that frame the current efforts to protect critical infrastructure SCADA systems:

· The importance of a public-private partnership for success in reducing vulnerabilities,

· Lead federal agencies that act as liaisons for each infrastructure sector. A partial list of the lead agencies included: the Environmental Protection Agency (EPA) for water supply and wastewater, the Transportation Department for rail and pipelines, and the Energy Department for electric power and oil and gas production,

· Interagency and inter-industry coordination groups including the Critical Infrastructure Coordination Group and the National Infrastructure Assurance Council,

· A warning and information sharing system through the creation of the National Infrastructure Protection Center,

· Industry specific information sharing systems known as Information Sharing and Analysis Centers (ISACs), and

· A requirement for the National Infrastructure Assurance Plan to establish milestones for sector based vulnerability analyses and remedial plans.

Less than two months after the September 11, 2001 attacks the USA Patriot Act was passed. The last section of the law covers critical infrastructure and is known as the **Critical Infrastructure Protection Act of 2001**. It states, as does PDD63, that any disruption of critical infrastructure must be infrequent and "**minimally detrimental**" to the nation. It recognized the existing National Infrastructure Simulation and Analysis Center (NISAC) as the advanced technical resource for research on critical infrastructure protection and provided funding.

In the following year the Homeland Security Act of 2002 created the Department of Homeland Security (DHS) and carried out numerous consolidations. One of these consolidations established the Director of Information Analysis and Infrastructure Protection (IAIP), which became responsible for cyber and critical infrastructure protection.

In 2003, the President released The National Strategy to Secure Cyberspace. This document was addressed to the American public with the intention of expanding the effort and broadening participation. The bulk of the strategy lays out cyberspace security priorities to establish a response system, a threat and vulnerability reduction program, an awareness and training program, and national and international cooperation. Within the threat and vulnerability section it states that, "**Securing DCS/SCADA is a national priority**."

II. SCADA threats and vulnerabilities

II.1 Security threats

SCADA systems have evolved from exotic hardware and software in the 1970's, to systems that can include standard PCs and operating systems, TCP/IP communications and Internet access. The threat exposure has increased further by the common practice of linking SCADA networks to business networks.

Intentional security threats to SCADA systems can be grouped as follows:

1. Malware – Like any IT system, SCADA systems are potentially vulnerable to viruses, worms, trojans and spyware. It could impact the system by corrupting data, overwhelming communications, installing back doors or key stroke loggers.

2. Insider – The disgruntled worker who knows the system can be one of the largest threats. The insider may be motivated to damage or disrupt the SCADA system or the utility's physical system. An insider may also attempt to illicitly gain higher privileges for convenience sake. Bored or inquisitive Operators may inadvertently create problems. (SCADA engineers may make errors that bring down the system)

3. Hacker – Here the individual is an outsider who may be interested in probing, intruding, or controlling a system because of the challenge. Another possibility is modifying data related to rate generation. While not an incident, one example of hacker interest was a presentation at the 2003 Brumcon meeting titled "Water Management Systems Using Packet Radio" The talk apparently discussed radio systems used by the British water utilities, how to monitor un-encrypted traffic and create denial of service attacks.

4. Terrorist – This is the threat that distinguishes critical infrastructure systems from most IT systems. A terrorist is likely to want to either disable the SCADA system to disrupt

monitoring and control capability, take control of the SCADA system to feed false values to the operators or to use the control system to degrade service or possibly damage the physical critical infrastructure system. Based on evidence collected in Afghanistan, Al Qaeda had a "high level of interest" in DCS and SCADA devices. In addition to interest, Al Qaeda presumably has appropriately skilled members, for example it was also reported that Khalid Sheikh Mohammed, their arrested operations chief, was an engineering student in North Carolina who later worked in the water industry in the Middle East.

Fortunately for the critical infrastructure industries that principally use SCADA for their control systems, two of the common threat motivations are not relevant.

One is the lack of economic incentives such as credit cards or financial accounts that inspire many cyber crimes. The other is the absence of proprietary recipes and formulas that can inspire corporate espionage.

II.2 Documented Incidents

There are a number of documented security incidents where critical infrastructure control systems were adversely impacted. The British Columbia Institute of Technology (BCIT) keeps a database of accidental and intentional cyber incidents that affect control systems. As of 2004 they had cataloged 34 incidents. Extrapolating from their 2003 data of 10 incidents and the estimated level of underreporting of traditional business crime, they concluded that there are at least **100 industrial cyber incidents** a year. Records of actual incidents include examples of each of the security threat categories except for the terrorist threat.

The Davis-Besse nuclear plant in Ohio had been off line for almost a year when the SQL Slammer worm was released in January, 2003 and infected and disabled their Safety Parameter Display System for five hours and their Plant Process Computer for six hours. Both monitoring systems had analog backups that were not affected. The worm reached the systems through a remote contractor link to the corporate network which in turn was connected to the process network.

On August 20, 2003, CSX, the railroad corporation, halted passenger and freight train traffic in response to a worm infection. While the worm did not get into their signal system, it did infect the telecommunications network that supported both their signal system and dispatch system. Service was affected in 23 states.

One of the most commonly cited incidents used to illustrate the vulnerability of critical infrastructure SCADA systems is that of "insider" Vitek Boden who gained access into the controls of the sewer system of Australia's Maroochy Shire Council. The following

information on the incident was described in the documentation of his appeals case. Mr. Boden was convicted of twenty-six counts of unauthorized access to the Council's SCADA system computers and causing intentional damage. Prior to the incident Mr. Boden was the onsite supervisor for a contractor installing a SCADA system for a sewer system with 150 pumping stations. The system included a local processor at each pumping station that could communicate using data radios with other pumping stations and a central host computer. After two years of working on the project, the job was basically done. Mr. Boden resigned from his firm and asked the client about employment. He was told he would not be hired. Later that month the Council's sewer pumping stations began experiencing apparent malfunctions. Over time it became clear that the problem was not system failures but rather intentional disruptions. Problems included alarms being turned off, loss of communications, pumps not activating at appropriate times and the release of raw sewage. Mr. Boden did this from his car using a laptop computer, a data radio from his former employer and one of their local processors. He received a prison sentence of two years. It was estimated that he released nearly 264,000 gallons of sewerage.

In the spring of 2001 the California Independent System Operator, the organization that manages the electric grid in California, was remotely hacked. While the hackers did not gain access to the active SCADA system, they did have access to the network for 17 days. The intent of the hackers and whether they were in fact merely hackers was not known.

II.3 Vulnerabilities of SCADA systems

Opinions vary on how difficult it is for an outsider to access control systems. Some articles describe it as "extremely difficult", while others say it "requires very little knowledge". In the same way that critical infrastructure SCADA systems have common and unique threats compared with traditional IT systems, they also have shared and additional vulnerabilities, with some extra peculiarities:

1. Staff Experience – SCADA system staff are familiar with keeping control systems running. The normal goals of reliability and availability can initially feel in conflict with security efforts. With a bent for engineering and technical solutions to problems, the important role of developing security policies can be a foreign concept to typical SCADA staff. Furthermore SCADA staff may not be receptive to IT staff recommendations.

2. Operating System Vulnerabilities – The whole host of normal IT operating system vulnerabilities are present in SCADA systems. The difference from an IT shop is that patching may be performed less rigorously. The SCADA system operator has a running system that is expect to perform without interruptions. A test bed is unusual and reports of

patch induced problems that cause systems to crash or take severe performance hits creates reluctance.

3. Authentication – It is not uncommon for SCADA systems to have shared passwords. This creates convenience for the staff but eliminates any sense of authentication and accountability. In some cases moving to two-factor authentication is limited by work conditions that may impede iris scans or fingerprint scans because of dirty hands or the wearing of safety goggles. Confidentiality of authentication is often compromised by the use of clear text transmissions.

4. Remote access – Because of the economics of staffing control centers around the clock it is not uncommon for SCADA systems to be configured with remote access. This can include dial-up access or VPN access over the Internet. In one interview of 50 water utilities in 1997 and 1998, a total of 60% reported that they could control their systems from a dial-up line.

5. Interconnections – The more connections the more exposure and vulnerability a SCADA system has. The deregulation of the electric power industry has increased interconnections between systems. Economic and enterprise pressures often result in internal connections between the SCADA network and the business network. As recently as 2003, a security conscious SCADA consultant publicly promoted combining networks for the sake of simplifying network administration and enhancing security.

6. Monitoring and Defenses – The use of Intrusion Detection Software (IDS) is not common. Firewalls and antivirus software is not universal. Given staff cut backs and drives for higher efficiency there is often little time to review logs. The potential for zero-day worms is always present.

7. Wireless – SCADA systems often use microwave, data radios and cellular packet services for communications. Depending on the implementation, these forms of communication can be vulnerable to certain types of attacks. Recently at least one utility adopted 802.11 wireless for their control system. Their consultant acknowledged that the implemented security measures would not stop a determined hacker.

8. Remote Processors – Certain classes of remote processors have recognized security vulnerabilities. Here the difficulty is two fold. First the computation power and memory resources of the processors are modest and not suitable for security upgrades. Secondly, once they are installed they typically stay in place for ten years or more. The result is vulnerable equipment that stays vulnerable for a long time.

9. SCADA Software – The SCADA application software has modest security features and other design weaknesses.

10. Public Information – It is not unusual for SCADA system owners to have published papers on the design of their system at a time when security was not a priority. This can expose system vulnerabilities. It is also fairly common for consultants or contractors to advertise their experience and reveal information about past clients. The availability of information data was demonstrated in 2003 by a George Mason University graduate student who, in his dissertation, reportedly mapped every business and industrial sector in the American economy to the fiber-optic network that connects them, using material that was available publicly on the Internet—and not classified.

11. Physical security – SCADA systems are usually distributed over large distances with multiple unstaffed locations. The physical protection of SCADA devices becomes important. But because pin tumbler locks, master keys and cylinder locks all have reported weaknesses it is important to be realistic about the level of protection they provide. In some cases economics and vendor promotion have brought closed circuit TV and intrusion contacts into the SCADA system. While convenient and cost effective, this weakens the reinforcing nature of separate physical security and SCADA systems.

II.4 SCADA Security Initiatives

Numerous SCADA security initiatives have been undertaken to address the vulnerable nature of SCADA systems. Valuable contributions have been made by all of the stakeholders in improving SCADA security: system owners, vendors, consultants, academic institutions, National Labs, independent associations and bodies, and government organizations.

SCADA system owners bear the ultimate responsibility for protecting what they manage. They have participated in **vulnerability assessments**, have made improvements and continue to do so. Through vulnerability assessments and responding to research questions, they also provide the information that gives direction for other stakeholders.

The vendors in the SCADA world are working on **securing their products**. They are aware of the market value and competitive advantage of secure products. If they do a good job and produce products that are demonstrated, through independent testing, to be secure and that are easy to upgrade to, they may even shorten the typical SCADA system lifecycle and reap extra gains. On the down side, in theory, they could face legal suits for providing knowingly insecure products, should their component be the primary factor contributing to a severe SCADA attack. Of the industrial cyber incidents documented by BCIT, five were self-reported to have cost over $1 million.

SCADA consultants are also driven by economics and an interest in helping solving an important problem. They contribute to the security cause by **providing expert services** to

clients, publishing papers and making presentations that educate and heighten awareness of system owners, and conducting funded research that advances the state of the art. The sophistication of consultant advice is variable so hopefully firms with less knowledge will partner with IT security firms to provide rigorous recommendations and designs. Consultants are also acting as instructors in the handful of SCADA security classes that are being offered.

Academic institutions are similar to the consultants in that they **raise awareness** and advance the field of SCADA security. They also play the unique role of educating students who may become the future experts in the field.

The Department of Energy's National Laboratories in the United States were created for nuclear energy and related research and development. Some of these labs now support **advanced research on SCADA security**. The Idaho National Laboratory in conjunction with the Sandia National Laboratory have created the **National SCADA Test Bed** in a setting that includes a functioning power grid and synergistic cyber and wireless test beds. The Sandia National Laboratory has The Center for SCADA Security, where they participate in research, training, red teams and standards development. One of their past projects was the development of the Risk Assessment Methodology for water utilities (RAM-W). A current project is the creation of a SCADA security guide book for the SCADA user.

There are many independent associations and organizations engaged in SCADA and PCs security work. They are both industry specific and broad based in interest. They can be grouped into two populations, Information Sharing and Analysis Centers (ISACs) and Standards Bodies.

ISACs were encouraged under PDD63 and have been established for the Electricity Sector, Energy (oil & gas), Surface Transportation (rail) and Water (water and wastewater). They are independent organizations with members from their industrial sector. They maintain confidential information and provide early warning and analysis of threats and vulnerabilities.

The other class of independent organizations can be loosely called Standards Bodies. Examples of these include:

- the Instrumentation, Systems and Automation Society (ISA),
- the American Gas Association (AGA),
- the National Institute of Standards and Technology (NIST) and
- the North American Electric Reliability Council (NERC).

The ISA, through its SP99 standards committee has published two technical reports that are directed to **cyber security of** manufacturing and **control systems**. The first document, "Security Technologies for Manufacturing and Control Systems", acts as a primer on computer security technology. It examines different topics such as biometric authentication,

host-based firewalls and virtual private networks and describes the vulnerability that the technology addresses, the typical deployment, known weaknesses, how it fits into the control systems environment, future directions and recommendations. The second technical report, "Integrating Electronic Security into the Manufacturing and Control Systems Environment" gives guidance on developing a security program.

The AGA has focused on communications encryption. The first document in a future series, "Cryptographic Protection of SCADA Communications, Part 1: Background, Polices and Test Plan", provides background on the need to protect SCADA communications, a guide to defining security goals, and cryptographic requirements.

NERC has established cyber security standards that it holds it members to. "Urgent Action Standard 1200 – Cyber Security" lays out security requirements, measures for compliance, compliance monitoring through self-certification, levels of non-compliance and sanctions. Depending on the level of noncompliance, financial penalties are established.

Government organizations represent the public part of the public-private partnership. They have established critical infrastructure protection centers, provided research funding, overseen industry groups as regulators and most recently attempted an overall coordination of process control security.

In the United States there is the Directorate of Information Analysis and Infrastructure Protection (IAIP) within the DHS. The IAIP took over and consolidated the National Infrastructure Protection Center and the National Infrastructure Assurance Office, both of which were created by PDD63.

In England there is the National Infrastructure Security Co-ordination Centre that aims to "minimize the risk to the CNI (Critical National Infrastructure) from electronic attack".

In February 2005, the Canadian government announced the formation of the Canadian Cyber Incident Response Centre with a focus on critical infrastructure.

New York State even has its own Office of Cyber Security & Critical Infrastructure Coordination.

Given the relatively primitive state of SCADA hardware and software security, research funding is needed to help move SCADA security. In 2004, DHS provided grants of up to $100K to 11 small businesses to do research projects involving SCADA security. Several of the topics involved IDS and encryption.

The EPA has also supported research. In the fall of 2004 the EPA granted the Water Environment Research Foundation $250K towards work on "Security Measures for Computerized and Automated Systems", which WERF subsequently awarded along with some of their own funds to a consultant.

The Interagency Technical Support Working Group has provided $87K of funding to a university to test SCADA communication protocol vulnerabilities and $881K to an institute to develop a retrofit table encryption module.

Finally, the National Center for Advanced Secure Systems Research has funded a university to develop a way of authenticating data signals without full encryption.

Research work has paid off in the development of Modbus / TCP and DNP 3.0 attack signatures for the Intrusion Detection Software (IDS), Snort. Another useful tool, the protocol analyzer, Ethereal, supports the following SCADA and PCS protocols: BACnet Virtual Link Control, Common Industrial Protocol, EtherNet / IP (Industrial Protocol), Modbus / TCP, PROFINET and Distributed Network Protocol 3.0. While not complete, work has also begun on creating a SCADA Honey Pot to simulate a SCADA or DCS network.

The Department of Homeland Security has recently sponsored the creation of a new group called the Process Control Systems Forum (PCSF). It has the ambitious aim of facilitating and coordinating all work in the field of process control security. Its focus is on the future and to "accelerate the implementation of more secure Process Control System (PCS) and Supervisory Control and Data Acquisition (SCADA) systems."

III. Conclusion

Critical Infrastructures are vital and very important to the society. Most Critical Infrastructures are controlled by Control Systems like SCADA. As presented in this paper, SCADA has some vulnerability that needs attention. If these vulnerabilities will not be attended, it will cause great effect to the society. As it is well-known, SCADA was designed not focusing on security so ways to keep it from emerging vulnerabilities should be performed.

Government, academia, and private industry have independently initiated multiple efforts and programs focused on some of the key areas that should be addressed to strengthen the cybersecurity of SCADA systems. Both federal and nonfederal entities have initiated efforts to develop encryption methods for securing communications on SCADA system.

Several entities are working to develop standards that increase the security of SCADA systems.

References

1. *** - *A Review of the EPA Water Security Research and Technical Support Action Plan*, issued by The Panel on Water Systems Security Research, Water Science and Technology Board, Division on Earth and Life Studies, National Research Council of The National Academies, ISBN 0-309-52628-0, 2004;
2. Rosslin John Robles, Min-kyu Choi, Eun-suk Cho, Seok-soo Kim, Gil-cheol Park, Sang-Soo Yeo - *Vulnerabilities in SCADA and Critical Infrastructure Systems*, International Journal of Future Generation Communication and Networking, Vol. 1, No. 1, December 2008, pp.99-104, ISSN: 1738-995x;
3. *** - *EPA Needs to Determine What Barriers Prevent Water Systems from Securing Known Supervisory Control and Data Acquisition (SCADA) Vulnerabilities*, Environmental Protection Agency (EPA) Report No. 2005-P-00002, 2005;
4. Andrew Hildick-Smith - *Security for Critical Infrastructure SCADA Systems*, SANS Institute InfoSec Reading Room, 2005;
5. Robert F. Dacey - *CRITICAL INFRASTRUCTURE PROTECTION. Challenges and Efforts to Secure Control Systems*, Testimony of Robert F. Dacey, Director, Information Security Issues from United States General Accounting Office before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, 2004 (http://www.iwar.org.uk/cip/resources/gao/d04628t.pdf);
6. *** - *Securing the move to IP-based SCADA/PLC networks*, Centre for the Protection of National Infrastructure, 2011 (http://www.cpni.gov.uk/documents/publications/2011/2011034-scada-securing_the_move_to_ipbased_scada_plc_networks.pdf?epslanguage=en-gb);
7. *** - *Supervisory Control and Data Acquisition (SCADA) Systems*, Technical Information Bulletin 04-1, US National Communications System, 2004;
8. *** - http://en.wikipedia.org/wiki/SCADA
9. *** - http://cfpub.epa.gov/safewater/watersecurity/guide/productguide.cfm?page=scada
10. *** - http://www.exida.com/images/uploads/The_7_Things_Every_Plant_Manager_Should_Know_About_Control_System_Security.pdf

COMPUTER NETWORK MANAGEMENT, SECURITY TECHNIQUES

1st LT Andrei DUDNIC

Introduction

Introduction to network management

The management telecommunications networks means coordinating all the resources required to design, planning, control, simulation, generation, implementation, analysis, monitoring, measuring and testing telecommunications networks, in order to guarantee the end user a degree of services with optimum cost through optimal distribution capacity. Network management can be seen as a process of monitoring (surveillance) and distributed control systems for large, medium and small errors or defects that normally occur. We can say that network management can have the following components:

- Network control;
- Monitoring networks;
- Maintenance of networks;
- Operating;

In terms of the OSI reference model, network management provides a way to maintain network operation and function of the parameters set. It also provides command and control facilities. Network management can be divided into the following components:

- Fault management - all equipment can be damaged at a time and can stop connections and interfaces. All this together can cause some erroneous information network. Events can be considered as defects, indicating that they do not necessarily mean that something has failed in the network. Events are to inform management system about possible things in the system.
- Configuration management - all trying to get some equipment configurations or settings

Configuration settings can be read or written in equipment.

- Financial management - billing for services offered is an important component in the management system. This will be used for charging resource utilization by each department, user, etc. and also verify the correct charge sent by the service provider.
- Performance management - as the number of users and the need for bandwidth increases, it is essential to performance can be measured, especially for performing any SLA (Service Level Agreement). Verification performance can be used to prediction possible congestion.

- Security management - network attacks include unauthorized access, modification or theft of data, etc.. Security is required to ensure that both data and network itself are protected. All these categories actually describe what is considered in terms of the OSI model as network management functional areas. An acronym that identifies the components of a management system is FCAPS (Fault, Configuration, Accounting, Performance, and Security).

Chapter 1

1.1 Management architectures

Management architecture is a collection of managed equipment, monitoring equipment and ways to transfer information between them. When talking about management architecture is important to understand that it is linked to management technology chosen.

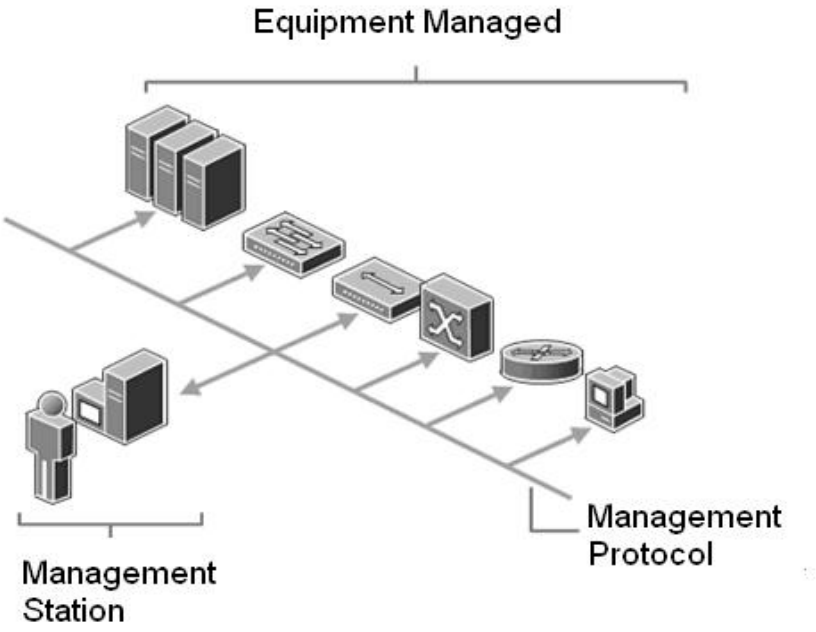


Figure 1.1 General architecture of a management system

1.2 Managers

Managers (or NMS - Network Management Station) is probably the most important element of management infrastructure that collects data about network status and send messages to configure network elements. The main functions of a manager are to receive alarms sent by managed devices, request information from the equipment and send the configuration parameters. A manager should give the possibility to configure certain parameters, number of retry to obtain the information, answer the waiting time (timeout) or

range of query parameters that can be used to determine if a device does not respond to commands. Managers must know the structure and format of management information used by managed devices, regardless of protocol or technology.

1.3 Agent

Agents are pieces of software or hardware that implements various functions and running within the monitored equipment. First and most important task of an agent is to respond to requests sent by managers. Agencies usually require minimal configuration before use (system information, positioning, and system administrator access rights). Such information (access rights) can help management system to meet management only messages coming from a trusted management station.

1.4 Topology management

Currently the trend is moving toward a centralized system that can be achieved a relatively simple way by using a single management system that supervises entire business. The disadvantage is that this mode of network resources consumed by need to add such additional signaling networks. The major disadvantage remains that if the network infrastructure greatly increases a simple management can not cope. Decentralized management architecture was the first approach in implementing existing management functions. Has the advantage that offers flexibility and is designed to meet all types of traffic in the area it covers. Problems that virtually every such area is isolated, is because that the efforts to set up and support is higher and if the network is very difficult to have an overview of its behavior.

1.5 Communication Manager – Agent

An important thing to be added to the above is related to the communication between manager and agent. Using this process agent sends information to the manager. Communication is usually based on transport support offered by a particular management protocol that is generally specific technology used. In terms of mode of transmission there are two broad categories:

- Communication based on query
- Communication based on events

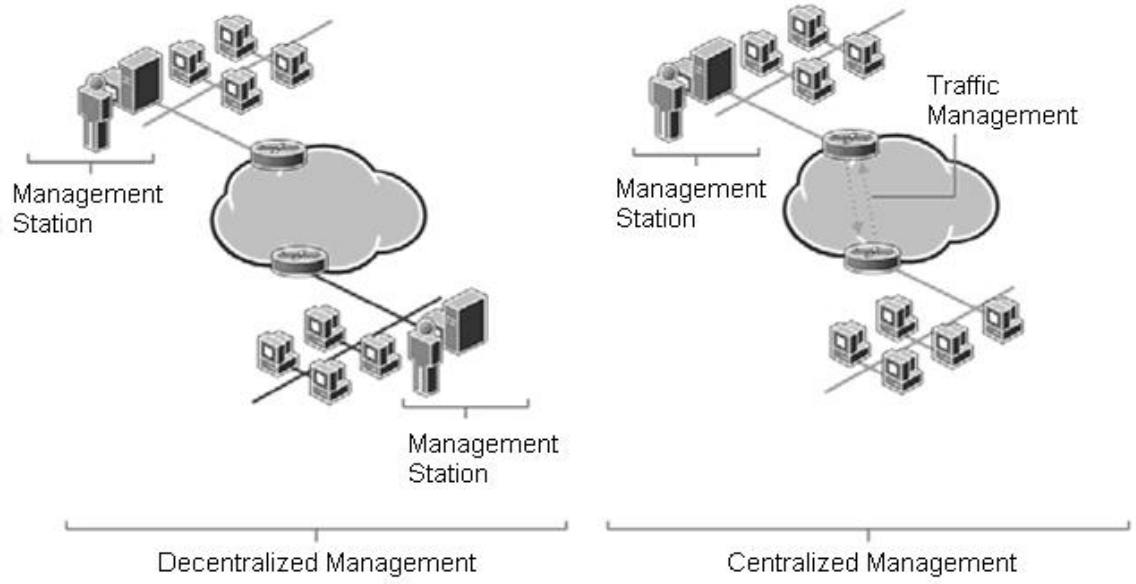


Figure 1.2 Centralized or Decentralized

The method used is actually a combination of the two above. In this event messages will be sent based on events in exceptional cases, while the query mechanism will be used to query larger intervals. Sometimes you a message generated by the agent for an event to lead to the generation of messages query to get more information.

CHAPTER 2

2.1 The definition of a network

A computer network is a complex computer system, computer equipment consists of several individual, homogeneous or heterogeneous, interconnected through a communication channel, so you may share certain hardware and software. These resources may be disk drives, files, databases, printers, communication equipment or other peripherals. Networked computers are called nodes.

Technical infrastructure network is the hardware, the medium and software components. The content network is the information available on the network. Reported to resources, a computer network is a set of physical resources (Communications equipment, transmission media), logic (operating systems, applications) and information (bit data) that communicate. Components of the computer network, a computer network can be divided into the following components:

- physical component;

- logical component;
- component information.

Physical components (hardware) comprise nodes (computers), communication equipment (gates, bridges, etc.) and links (transmission media). Component logical (software) includes operating systems, applications and services. Component comprises information bits (data) that travels over the network. An important aspect is the management of these network components, having as a target of increasing performance management of these components for the network to function optimally. This is the purpose and objective is to analyze factors influencing the performance of the Network as a whole. Network management structure work according to three components in managing physical and logical management of network management information.

2.2 Stages of the network

In establishing a network you must adhere to the following stages: design, equipment selection physical and logical components, the actual realization and final functional testing. Once these steps are completed you can move forward to network monitoring and maintenance. Ever since the network design should be approached in the network management chapter. Correct design and construction of a network depends heavily on its future functionality. Choosing the physical equipment (means of communication, transmission and switching equipment) is made after a thorough physical characteristic that match the well the network is designed. This step is related to physical network management and transmission network design plan. Choosing logical components (operating system, applications) is made after careful consideration of the logical characteristics that fit best with that network designs. This step is related to logical network administration. Practical realization requires cabling, connection, installation of operating systems and applications, setting physical equipment, etc.., citing personnel. Testing the network has link with management information network designed and built. The total time spent making a network project 1/3 will be used for planning, 1/6 for installation and programming, 1/4 for testing modules and 1/4 to test the entire network.

2.3 Network design

To achieve a network to function optimally design is required. Network design is usually determined by the cost of investing in technology switching and transmission. Price is a crucial aspect in the choice of technology for design and establishing a network. In recent

years due to flat networks number switching nodes and thus low switching costs have decreased. When designing a network administrator must consider the following plans:

- technology plan;
- development plan;
- investment plan.

Of these plans is the most important first, because it refers to internal characteristics of the network, the other two plans are derived from the foreground and can be made only after there are basically a network. All these plans are constantly adapting and updating. Technology plan includes fundamental technical plans related to physical and logical network component. Technology plan should take account of dependence equipment required services and applications to be used determine network technology (hardware and software) to achieve.

Development plan should consider:

- demand for new services by users;
- the extent to which new services meet users;
- if the requirements are urgent, and when can be satisfied;
- if new technologies can be integrated into existing network.

Scorecard for inclusion in development plan is made by:

- Volume: the number of people using the service;
- Efficiency: the extent of costs and resources required to provide service;
- Service quality: how well a service performed work required;
- Utility service: what percentage of the service users interested in a particular type.

The investment plan should be directed to:

- financial analysis of investments;
- calculation of return on investment for the network;
- if the application development services is justified.

2.4 Network Management

According to that defined network management, it is the act of design, configuration, monitoring, modification and maintenance of the primary functions of the network, network access, information exchange, etc. Once the physical network was designed and built, it should administrator, in the sense configuration and performance monitoring, detection and location of faults and fault operation and protection system. Therefore, these issues have been divided into management areas for the physical component, logic and data. All network

management provides a basis for analysis of trends in the use of network components and to analyze the quality of services it offers.

2.5 The need for network management

Any network regardless of its size needs management. Network management is necessary to control and optimize network performance, but also respond to changes requested by users. Network management usually involves high costs and specialized people (network administrators) and a mature management must analyze the main factors affecting network performance. These factors are the subject of the thesis. Comprehensive network management means taking part physical, part logic and part information network.

2.6 Types of management

Network management can be performed automatically, implicitly module dedicated hardware and software, and manually clear the human component, the operating system commands. This paper presents the latter method of administration. If management hardware and software modules can be distributed network systems, in exchange for explicit management of this can be achieved from a limited number of remote locations, which sometimes can be a disadvantage. Taking explicit advantage is that it is necessary to work out all management functions. The two modes of administration can be combined. All network management can be done centrally or distributed. For centralized management system is central to the decision-making.

For centralized administration a large number of managed systems can be controlled by a single management system. Agents and protocols are needed for administration. Centralized management can be performed both implicitly and explicitly. For managing distributed systems management take their own decisions. Distributed administration must be made by default. The types of monitoring networks, based on the location of where this activity can be done:

- Simple monitoring network;
- Remote network monitoring;
- Advanced network monitoring.

2.7 Standards used in the management

Some standards are used in network management: SNMP, CMIP, CORBA, NMS. SNMP (Simple Network Management Protocol) is a standard for managing Internet. CMIP (Common Management Interface Protocol) is the vision OSI network management, very

elegant and sophisticated and is based on a connection oriented transport protocol (TP4/CLNP) agents to carry commands and responses back to the manager. CORBA (Common Object Request Broker Architecture) provides a framework for object-oriented applications. Access to information is transparent, without knowing where information is located on the network.

It was adopted for Web browsers using IIOP and Java (the language Interface Definition Language). NMS (Network Management System) developed by Ericsson is used to manage wireless networks. NMS includes all areas of management networks connected by wires. NMS is built over TMIP (Telecommunications Management Information Platform) work on the Compaq. OSI management areas Network management is divided into five functional areas of management, according to OSI management framework:

- management of operational problems;
- administering the accounts;
- configuration management;
- performance management;
- security management.

Of these areas to tackle first three depend on each network in part (configuration, the umber of users, resources), the latter two can be addressed in general on measures to be followed to have an administration as well. For configuration management, accounts and operating problems administrator must work with end users because they actually work with the network and can report and inform these issues. A part of configuration management, accounts and operating problems in the administration is both physical and logical management information in the network.

In this paper we will discuss in particular performance management because it falls strictly on the task of the network, which has the responsibility to monitor, analyze and control the optimal network and is an area that has influence in other areas of administration. Telecommunication Management Network (TMN - Telecommunications Management Network) covers the same areas of administration, including many ideas of OSI systems management, but there are many differences.

2.8 Administration errors

Normal operation is affected by damage to equipment and software problems. Administration allows an identification, detection, reporting, isolation and correction of operational defects and abnormal operations. Possible causes of abnormal operations are: design and implementation errors, external disturbances, and operating period. Also included

in this management and diagnostic tests. Keeping in conditions of failure or error is determined by:

- project quality network equipment and applications used;
- how the fault or error is detected;
- time of diagnosis of the malfunction or error;
- time to correct the malfunction or error.

2.9 Management accounts

Allows management of users, resources and services, collecting information about accounts, setting load, identify the costs of resource use. These resources can be:

- network service providers that are responsible for transferring user data;
- network applications (directory services).

Management accounts can:

- inform users about the costs (expenses);
- inform users that will be future costs;
- set limits costs (to disable certain connections to different addresses);
- combines expenditures for each individual connection or for international connections to cross country.

2.10 Configuration management

To identify network components, installation of network equipment, setting configuration parameters (routing tables), recording and maintaining the current configuration or changes in configuration, updating configuration parameters. Configuration management and administration is called names.

2.11 Performance management

Allows collection, saving and interpreting the statistics, network optimization with available resources, detect changes in performance, quality of service. Detects changes in network performance through statistics (timers and counters) offering safety and quality in the network. Performance may be useful for management faults (to detect errors), for administration accounts (to accommodate cost) and configuration management (the change is necessary for optimal configuration).

2.12 Network development plan

Network development plan must take into account in addition to the physical component of the network by (sub architecture) network comprising:

- access to the network;
- switching;
- transport information;
- connections between networks;
- services;
- Network Management;
- increase network performance work.

Planning to use the access network nodes access different traffic types (interfaces for ISDN, B-ISDN, PSTN, PCS band base station based on radio transmissions). Fiber rings or buses can be used to interconnect access nodes. Access nodes will be located close to end users. Nodes can access multiplexers and concentrators. Video on demand networks and simulation services introduce a new aspect in the planning process, because these networks require a much higher bandwidth than traditional networks.

Access network generally uses ~ 50% of total investment and switching nodes and the transmission is another great investment. Once access and switching nodes for different network applications have be en positioned and sized, public and private virtual traffic flow can be calculated. Flow total traffic is obtained when leased lines are added. Different nodes can be planned and designed taking into account the transport network. Transport network is the heart "of telecommunications infrastructure and transport is pure function and control of flexible connections to allow allocation of transmission resources. Switching equipment located in the transmission network will serve different transfer modes: circuit switched mode, a cell, a package, release framework. In future, there will be remotely located nodes, for different basic services.

2.13 Investment Plan

For continuous increase network performance has to answer the questions: "We can improve network performance using the same resources and have made new investments? What are the costs and benefits? The answer to these questions is related to all network components. The investment plan is for the financial managers, who must collaborate with IT (information technology) and network administrators to properly estimate the financial resources. The first attention should be focused on factors affecting long-term investments

(traffic transport network architecture, technology used, network administration). Then, it will examine:

- available capacity of existing network and its resources;
- degree of functionality of existing network;
- the degree of exploitation of available resources.

The conclusions will determine whether the investments are profitable. Characterized power capacity network service and user demand is the amount of work that can be performed in a unit time.

2.14 Network Cost Analysis

Network cost is the sum of cost components. The categories of costs for typical IT department include:

- network design;
- server hardware;
- computer hardware;
- hardware for the medium;
- network cabling;
- licensed software;
- software installation;
- training and education of users;
- facilities update (upgrade) and maintenance (servicing);
- Network services and development;
- Network management and accounts;
- Internet connection (for session ftp, telnet, http)

These costs plus the total amount of money spent (annually) by an institution for refurbishment. You can extend the user cost analysis and cost for network use, but this data is needed on the number of users. Users can as network users, defined as the number of users that have access to the network and active network users, defined as the number of users connected to the network in a specified period of time. Network users can be divided into categories depending on the department where he works. Moreover, an analysis can be done monthly during a calendar year. This determines peak of network activity.

Chapter 3

3.1 Classification of information according to their importance

The data are classified into four levels, namely:

- Public data (unclassified information);
- Confidential data;
- Internal data;
- Secret information ("top secret").

In the data classification takes into account not only the content data and information in the system but a number of other issues. In addition, if a system contains data belonging to several levels of security will be classified according to the requirements of the data most sensitive managed system.

Security needs of the system should focus on availability, confidentiality and / or integrity.

3.2 Public data (unclassified information)

- Installation of SNIF (software or device that captures data packets transmitted on a network)
- Virus Scan
- Open only to persons authorized accounts, accounts with password access is mandatory.
- Write access to system files should be restricted to groups of users or machines (PCs).
- Communication software (NFS - Network File System, LAN Manager, RAS - Remote
- Access Service, UUCP - Unix-to-Unix Copy, Workgroups) is correctly installed, with security features

3.3 Internal data

Internal data is data processed in the system in the various functional departments direct access, unauthorized should be prevented. For this category of data protection recommendations focused on the following means:

- Documentation: testing, developing a philosophy of security, a user's guide with security features (describing their security mechanisms, in terms of user security administration guide).
- Safety: System Architecture: Check if it runs in protected mode. There should be functions to verify hardware and software integrity. Check that has been successfully tested security mechanisms.
- Identify and authorize users and protect information regarding permits.

- Quality control of access: Access is controlled between users specify or specified objects.

3.4 Confidential Information

Data from this class are confidential within the organization and protected from external access. Confidentiality of such data damage due to unauthorized access can affect the organization's operational efficiency, financial losses can generate and give competitors an advantage or a significant decrease in consumer confidence. This time, data integrity is vital.

Controlled access protection (Controlled Access Protection) requires user responsibility: Users are responsible for their actions. Therefore it must be possible with audit trail monitoring and alert functions. Audit logs (audit logs) should be protected.

Reusing objects: objects used by a person must be reset before being used by another person. Secure data transmission: the transmission of messages other use of programs that communicate with each other have maintained confidentiality and integrity.

3.5 Secret Information

Internal or external unauthorized access to data is critical. Data integrity is vital. Number of users eligible to access these data is very limited and these data are set very stringent rules on access security. Labeled (Security Protection by labeling):
Additional requirements for identification and authentication (maintaining information security department), reliable facilities manual, manual design (description of the security model and mechanisms) and insurance (system architecture: isolation process, check the integrity, security testing and penetration attacks simulating audit log security levels of objects).

3.6 Control security systems

Each organization should have a security policy and a security plan to ensure implementation of this policy. Audit security system is a very complex approach that starts from the evaluation policy and security plan, continuing to analyze security architecture, network architecture, hardware and software configurations, penetration testing etc. these are only some of the activities involved. Safety audit carried out an objective evaluation system that will indicate:

- Risks faced by the organization values (hardware, software, information, etc.);
- Exposure organization if appropriate measures are taken to limit risks identified;

- Efficiency and effectiveness of overall security and effectiveness of each component thereof.

Processes to ensure systems meet security function to protect systems against the use, publication or unauthorized modification, destruction or loss of stored information. Information systems security is achieved by logical access controls that provide access to systems, programs and data only to authorized users. Controls logical security systems are:

- Data confidentiality requirements;
- Control authorization, authentication and access;
- User identification and authorization profiles;
- Determining the information required for each user profile;
- Control of encryption keys;
- Incident management, reporting and follow-up;
- Protection against virus attack and prevention;
- Centralized management of security systems;
- Training for the users;
- Methods for monitoring IT compliance procedures, intrusion testing and reporting.

From the above results that the system risks are relating to:

- Loss, misuse and / or modification of system data and information
- Unauthorized access to computer system
- Damage or interruption of data processing.

Depending on the vulnerabilities it generates risks are classified as:

- Environmental risks
- Environmental Risks

Risks system must:

- Assessed in terms of severity of their effects
- Assessed in terms of probability of their occurrence
- Financial estimates for each occurrence of a risk and overall risk.

IT systems have several features to be considered in risk assessment:

- Organizational Structure
- The nature of data processing
- Procedural Issues

3.7 Risks and accidents triggered

The concept of system risk appearance expresses the possibility of a loss to harm the information resources, financial and functioning. The main risks and accidents that can result are:

- Operating Error
- Malfunctioning hardware
- Malfunctioning software
- Undetected erroneous Data System
- Risks associated with nanoscale components

The greatest risks in information system of organizations and the financial losses caused by unintentional errors and omissions. The existence of these risks requires the definition and implementation of control mechanisms to mitigate and even the elimination of these vulnerabilities. These controls are represented by checks classified in:

- Restrictive controls
- Preventive controls
- Detective controls
- Corrective controls

These controls are contained in the security strategy established risk management process. This highlights the first steps to be completed to establish and implement internal controls system and the fact that the process of identifying vulnerabilities and establishing controls is iterative due to system development by implementing new technologies, continuous change environment IT work, modifying applications and procedures used which means new threats.

The steps are:

- Identify threats
- Determination of risk (probability) for each vulnerability identified
- Estimation of exposure or potential loss for each threat
- Identify the set of controls to be implemented for each threat and if it evaluates the cost-benefits of implementing security solutions, they are added and implement the set of controls.

3.8 Methods for minimizing the risks

Risk minimization methods must meet the following imperatives:

- Create a system right from the start;

- Prepare users for security procedures;
- Once the system turned to maintain physical security;
- Physical security provided, prevents unauthorized access;
- With access control, ensure that the resumption of proceedings to be fair;
- Even if there are control procedures, looking for ways to improve them;
- Even if the system seems secure, it must be audited in order to identify new possible security problems;
- Even if you are very vigilant, get ready for disaster;

Minimizing risk can be achieved in the following ways:

- Development and change control system;
- Verification and approval of any changes in software;
- Update documentation to date;
- Providing specialized antivirus software daily;.
- Training staff to reduce risk;
- Frequency of training;
- Selection of staff;.
- Maintain physical security;
- Physical access restricted;

Control access to data, hardware and networks:

- Control of formal operations;
- Exact definition of privileged access;

Eliminate intrusion by using:

- Passwords;
- ID cards;
- Hardware keys;
- Control - retinal scan, fingerprints, palm prints, voice recognition etc;
- Encrypt and decrypt data;
- Control Transaction;
- Segregation of duties;
- Validation of data;
- Correction of errors;
- Backup;

3.9 Security management

A computer network is an open structure that can connect new types of equipment (terminals, PCs, modems, etc..), Which leads to a widening circle of users not always controlled direct access to network resources (programs, files, databases, traffic, etc..). Security Administration allows the administrator to initialize and modify functions that protect the network from unauthorized access. Important parts of safety management are:

- protection against all threats to resources, services and data network;
- providing authorization, authentication, privacy and control access rights of users;
- management of encryption keys;
- maintenance of protective walls;
- creating secure connection.

Network vulnerability is manifested on two levels: physical attack on her integrity and on the other hand use or unauthorized modification of information and network resources (leak limited circle of users established that abuse of network resources by unauthorized persons). Among the technical factors that allow security flaws can be certain defects of computing or communications equipment or software errors in processing and communication. Also, lack of appropriate training of managers, operators and users of systems increases the likelihood of security breaches. Misuse of systems (hacking) is also one of the major risk factors of security systems. In the present security management is divided into physical security equipment

3.10 Security policies

Security policy consists of a set of measures, supported by management, providing clear rules, but flexible standard for determining the necessary operations and security technologies.

A security policy is a document that highlights the main requirements or rules to be known and applied for security. A security policy will contain security requirements of an organization and describes steps to take to ensure security. It aims to protect the following:

- Memoirs of assets;
- Files or data stored on auxiliary support;
- programs (executables) from memory;
- The structure of directories / folders;
- Some electronic devices;
- data structures;
- The operating system;

- operational instructions;
- User names and passwords;
- protection system as such.

Should be made, however, from the outset, a distinction between certain terms, much literature circulated dedicated security information systems, such as: standard, guidance and policy. A standard set consists of a system or procedural requirements that must be known and implemented. A standard will describe, for example, how to enhance the security of Windows Server 2008 SP2 that will be placed in an unprotected area of applications. Guidelines are a set of suggestions for system or procedural specific need for a practical implementation more efficient. They are not required to know, but are strongly recommended, in general. Effective security policies make frequent references to standards and guidelines that must be found within each organizational structure (economic, educational, etc.).

3.11 Security models

Security models are important in determining the organization's security policy at information system. Study abstract security models can be crucial in understanding the security mechanisms to be applied in certain cases, concrete. A security model describes a mechanism that implements a particular logical security policy already established. The main features of a security model are:

- the model is precise and unambiguous
- is easily understood and implemented
- focuses only on security issues and does not restrict the system functions.

The essential elements of an information security model are the resources and users (often called subjects). Resources are mentioned in the literature, generic objects. This category includes compilers, link editors, modules and software libraries, databases, documentation, etc. resources.

Over resources and users, viewed as sets are defined relationships. Security models describe a set of relationships between users and resources. Best-known security models are:

- Monitor
- Graham-Denning,
- Bell LaPadula,
- Harrison-Ruzo-Ullman
- Biba,
- Clark-Wilson

- Lattice,
- Chinese Wall

Resources in information systems security

The Monitor. This model represents the simplest model of access control. This model itself is a gateway between users and objects. The use of resources is often the users, this model is describable by a sequence of steps. Stages to be completed are:

- The subject application launches;
- The system records request subject;
- The system queries the database, access control, to determine the access rights of the subject;
- The granted subject access rights under it (of course, can be denied access, possibly). This model is generally easy to achieve and implement. As disadvantages of this model system can enumerate frequent jams that model operates exclusively on direct access control on resources.

The Graham-Denning. This is a security model that shows how it should be created and deleted threads and objects in a system and the assignment of specific rights in the system. The focus on security issues associated with how to define the set of fundamental rights on objects. Considered ways in which certain subjects can perform security functions on a specific object.

Bell-LaPadula model. The model provides a formal description of the means of access to information from a system considered as safe in terms of security engineering. This model is considered in most works of literature in the field, as a milestone in the development of information systems security techniques. It was introduced for the first time, the general security model, multi-level. This model is used as the basic model for designing distributed systems that handle data at multiple levels. Designed by David Elliott Bell and Len LaPadula in the seventh decade of last century, the model is used, especially for secrecy and data protection.

The model was introduced as a formalization of multilevel security policy of the U.S. defense department. Bell-LaPadula model makes no distinction between protection and security at an information system. This model covers mainly information privacy and access to the classified U.S. military information systems of those years. Bell-LaPadula model has some limitations:

- focuses only on the treatment of confidentiality;

- is static can only apply to systems that have provided a static security. The policy does not have access or change the rules for creating or deleting subjects or objects;
- allows, however, that a point on a lower security level to detect the existence of an object on a higher security level. In some cases, the current information systems, is necessary not only to hide the contents of an object, but even hide the existence of the object.

The Harrison-Ruzo-Ullman. It is a model that is meant to be a general model capable of Bell-LaPadula model cover limitations. This model introduces the authorization..

The Biba model. Is a model Bell-LaPadula model dual. This model assumes a multi-level security classification, only this time domain function as subjects must interpreted integrity (or the confidence to produce and modify the information). The concept of integrity of certain data is used instead of actual security, because secrecy is completely separate certain data against that data integrity, until the moment you check this property.

The Clark-Wilson. This model was published in 1987, a work of researchers belonging to David D. Clark and David D. Wilson. This paper develops the model as a way of formalizing the notion of integrity of information in the context of multi-level security systems. The two authors show that models integrity, such as Bell-LaPadula and Biba prove to be closer to strengthening confidentiality information than integrity. It is estimated that the Bell-LaPadula and Biba models are very useful, for the reason stated, military systems.

The model proposed by the two authors, the environment of astonishing natural to previously developed models, appears to be more suitable and applicable business and industrial processes. This is because the target application area (business and industrial processes), integrity of information is most important at any level of its classification. The security it seeks to include security requirements of commercial applications, with emphasis on internal and external consistency of data. Model restrictions and certification rules define specific categories of data and processes that form the basis of political integrity. This model consists of a set of fundamental building representing both data and processes that operate on data. The core approach is based on transactions.

Clark-Wilson model uses two mechanisms to maintain the integrity of information:

- secure transactions;
- separation of duties.

A well-formed transaction consists of a sequence of operations that transit system in a consistent state to another consistent state. Information integrity policy in this particular model, aimed at the integrity of transactions, in fact. And the principle of separation of duties requires that the certifier and implementer of a transaction to be separate entities. Links

between subjects and objects, unlike previous models, are produced by programs, which constitute a new entity arising from the first two. Access control is achieved by two ways:

- defining access operations to be applied for each type of data to be accessed;
- define the operations performed by each subject and defining access rules.

Security properties are provided in part by:

- certification rules;
- restriction rules.

Clark-Wilson model is less formalized Bell-LaPadula model theory only, but measured by pragmatic, is more than a model of security and integrity control.

The Chinese wall. The model proposed by David FC Brewer and Michael J. Nash. This model treats the situation where an employee of a financial institution (financial advisor) who has professional relationships with several customers, may enter into a conflict of interest. Working model components are:

- Subject: financial consultant;
- Subject: data from a single client;
- Institution data: data represented by all customers;
- Class Conflict of interest: companies that are competing;
- Label: Data institution collaborate class conflicts of interest;
- filtered information: unrestricted access.

3.12 Data security issues in network

Addressing data security in a network means we are identifying operational requirements for the network, and then identify all possible threats against which protection is needed. This analysis consists mainly of three sub-stages:

- Vulnerability analysis: identification of potential weaknesses of the network;
- Threat assessment: determining problems that occur due weaknesses of network elements and how these problems interfere with operational requirements;
- Risk analysis: possible consequences that can create problems.

The next step is to define security policy, which means to decide:

- the threat must be eliminated and can tolerate;
- that resources should be protected and at what level;
- what security means can be implemented
- what is the price (financial, human, social, etc.) security measures that can be accepted.

Once established security policy objectives, the next step are the selection of security services, that individual features that enhance network security. Each service can be implemented by methods (security mechanisms) varied for the implementation of which requires so-called security management functions. Security management is a network control and distribution of information to all systems that make the network open for use by security services and mechanisms, and reporting of security events that may occur by the network.

3.13 The system security

The security system (a computer or computer network) can be seen as having multiple layers of security levels that are surrounding the subject to be protected. Each layer isolates the subject and makes it more difficult to access otherwise than it was designed.

Physical security is outside the security model and is generally locked in protection of computer equipment in an office or another site and ensure the security and access control. The physical security deserves special consideration. All physical security issue is the safety of storage racks save (backup) data and programs. Local networks, in this case, very helpful, backups may be submitted over the network on one machine can be easily secured. Another important issue in the physical security of a system is simply a misuse of equipment. In addition, other logical security measures (passwords, etc.) Become insignificant if unauthorized physical access to equipment.

In a system in which processing is distributed, the first measure of physical security to be considered is preventing access to equipment.

Logical security of those methods is logical (software) that provides access control system resources and services. It has, in turn, several large groups split into two levels: levels of access security and security levels of service.

Access security includes:

- access, which is responsible for determining if and when network is accessible to users and in what circumstances.
- access to a valid account name and password;
- access rights to files, services, resources, user or group.

Security services, which is under security access controls access to system services such as threads waiting on disk and server management. From this level are:

- control services and report warns state services, enables or disables mains services;
- the rights to how to use a service point. Access a perfect security system must be made by the security levels, from top to bottom. Data communication networks provide better management capabilities errors, so that their costs exceed the benefits of these networks.

By the means of network management are achieved the following objectives:

• resource management and network services;

This management includes: control, monitoring, updating, reporting network status, configure network devices and services.

• simplifying network management complexity;

Network management systems have the task to extrapolate information on network administration in a human manageable form.

• secure services;

The network must provide high quality services, while minimizing the network failure.

• knowledge of costs.

Network Management costs vary depending on the connection used by area. All resources and services used in the network, should be monitored and reported. For these objectives achieved by administering a network administration utility network shows.

3.14 Security incidents and their elimination

Security systems and communications networks are a topic that comes ever more frequently on issues facing organizations. Offenses reported within the state institutions and private sector, are growing:

- unauthorized access and data with varying degrees of confidentiality;
- modification, deletion or corruption of data;
- disruption of information systems;
- the production, sale, procurement for use and distribution without the right of devices can seriously disrupt computer systems;
- interception of passwords and access codes to sabotage computer systems and networks;
- falsification of data intended to be used later as authentic data;
- deception or fraud committed using computers;
- unauthorized use of software protected by copyright;

Therefore, today's business environments dependent on information technology require that employees know the importance of protecting company resources. And yet, when we talk about IT security in many organizations there is a gap between security awareness and compliance needs security measures. This is explained by the very misconceptions about information security process that may result in inefficient implementation of solutions. The most common "myths" about informational security are:

- "Myth: Hackers cause the most serious security incidents"

  In fact, statistics show that 75% of cases, incidents are produced within organizations.

- "Myth: encryption allows data confidentiality and integrity"

In fact, encryption is only a technique to protect data. Informational security involves a complex series of mixed media: media organization combined with the technical.

- "Myth: The firewall is a reliable data protection and information infrastructure of the organization."

In fact, 40% of the attacks made on the Web, have been made even despite the fact that the firewall was present. To implement an effective solution to protect data really will be necessary first of all to carry out an effective risk management procedure. The often neglected but organizations need to determine the risk of creating formal procedures for preventing, detecting and removing security incidents. In addition, those decision makers often interpret the absence of large gaps in safety assurance system as a confirmation that IT security is adequate - but it is a dangerous assumption. Experience has shown that most organizations do not know how to answer an information security incident until they were significantly affected by such an incident. Many of them have a priori assessed business risk associated lack of a well set detection and response to security incidents. Most times, the organizations receive reports that are informed by their involvement in security incidents which usually originate elsewhere without identifying themselves involved in the incident. This approach may be called as well and approach "fatal attempt".

The problem stems from lack of recognition by many organizations a pressing need for a comprehensive security system infrastructure. Usually business impact and risk of lack of such a system is found only after a serious incident. Management may often view as network and information system security is a concern for network administrators and system as part of their daily activities. They also may think that security is provided by the organization's firewall.

Usually, though, this perception is often inaccurate in all respects. Information system administrators priorities are largely focused on maintaining and managing existing computer equipment. Firewalls can prevent some attacks, but certainly not all attack, and if not monitored properly configured and then they can leave the organization vulnerable to a range of many other attacks. This approach can result in serious problems such as:

- Not knowing if the system has been compromised, or if it was for how long.
- Lack of information on which systems are at risk, or on what information was taken, or modified by intruders.
- Lack of methods used by attackers to gain access to systems.
- Lack of measures to be taken to stop the attacks and secure systems and networks.

- failure to identify early adverse effects caused by an incident on the company's ability to operate under normal conditions.
- Lack of a person responsible for making decisions to halt work, contact the relevant bodies, etc.
- delays for identifying and contacting appropriate persons on the event produced (both internally and externally).
- Lack of reporting contacts in the organization known by external or internal parts.

In spite of good intentions technical experts or other members of the organizations, the only effective approach for incident detection and prompt response in addressing them is to involve management and senior management of the organization in designing and implementing risk management procedures, the creation a group responsible for identifying and solving security incidents, all based on the highest management level. The design, either through a centralized or geographically distributed team of employees, or resorting to specialized services is not as important as the effort itself. In addition to supporting the management group empowered with such tasks must be recognized internally and externally, to prove the effectiveness and management credibility. Authority is the success and recognition. But an efficient detection and response will require trust and credibility of management and others with whom you interact.

Teams set for the detection and response to security incidents in an organization known as the Incident Response Teams related to computer security. However, if such a team is built and properly empowered in an organization, it can also address problems in a very constructive and can earn respect and credibility for its normal functioning. Response teams vary in structure, personnel involved and the range of services we can provide depending on the situation or need that will meet her at the moment. Thus, it should be considered very carefully the need for such a team within the organization, whether for the entire company or just one department.

CONCLUSIONS

As organizations become increasingly dependent on proper functioning of information systems security issue these systems becomes increasingly important. Security by investing in "head to toe" we can have secured IT systems. Often we find that the benefits will be higher, and investment and efforts will be less if we have an overall approach, unless we address the point, or worse, we will work to reverse the effects only after production a security incident.

Whatever you are called, respectively the executive or management information systems for strategic decision-assist systems, decision support systems, management

information systems, etc., all represent a category of information systems designed to support and improve decision-making process to achieve control as efficiently and as good.

REFERENCES

1. http://www.terena.nl/tech/task-forces/tf-csirt/
2. http://www.theiia.org/itaudit/?fuseaction=reflibhome
3. http://www.scribd.com/doc/55573866/36/Infrastructura-cheilor-publice-PKI
4. http://www.securitatea-informatiilor.ro
5. Ioan RADU – *Informatica manageriala*, Editura Economica 1996

THE IDEAL LOCAL AREA NETWORK (LAN)

HOSTING FACILITY

Physical Security perspective

LTC Florentin MOTOACĂ

Introduction

The purpose of this paper is to provide a comprehensive look at Physical Security by means of building an ideal LAN hosting facility. By viewing this design and construction process from a Physical Security perspective, we will identify and describe the measures needed to make our facility fully secure. Along with this we should, as an end product, have a comprehensive Physical Security Primer that can be used in many types of facilities and circumstances.

First, it would be best to define Physical Security. Physical Security is not something that can be easily and strictly defined, and their definition demonstrates this well.

"Physical Security is almost everything that happens before you (or an attacker) start typing commands on the keyboard. It's the alarm system that calls the police department when a late-night thief tries to break into your building. It's the key lock on the computer's power supply that makes it harder for unauthorized people to turn the machine off. And it's the surge protector that keeps a computer from being damaged by power surges."

With that wide-open definition in mind, we'll begin our journey through the design and construction of our facility. Along with identifying the pertinent Physical Security requirements at each step, we'll also look at some of the commercially available products that'll fit our evolving physical security specifications. Finally, with our ideal LAN hosting facility completed, we'll discuss some real world Physical Security implementations, focusing on where and why they fell short as compared to our ideal.

I. Choosing a Site

The first Physical Security consideration is the building site. Long before any concrete is poured, we must have ensured that our site meets all Physical Security specifications. Any proposed site must meet the following minimum requirements:

- Conveniently Available Utilities (Electricity, Water, Sewer, Gas, Telephone, Fiber).
- The facility must not be located in a flood, earthquake, hurricane, or tornado prone area.
- Interstate Highways, Railroads, Landfills, Feedlots, & Lakes must be at least two miles away.
- It must be built as a freestanding building on a lot sized to provide adequate buffer space between it and any outlying buildings or roads.
- Any Nuclear Plants must be a minimum of ten miles away (preferably 50 miles away).
- Military Bases, Munitions, Embassies, & Research Labs must be at least five miles away.
- Gas Stations, Self-Storage Facilities, Water Towers, & Substations must be a minimum of one mile away.
- Emergency Services must be within five miles (Police, Fire, Medical, Etc.).
- No Subsurface Soil Contamination.
- Limited Fire Hazards (No Dry Forest/Grass Lands or Periodic Hot, Dry Winds) and no Other Limited Hazard Exposures (No Nearby Wetlands, Protected Habitats, Etc).
- Moderate Temperature/Climatic Extremes (20-95 F, < 4 Days/Yr Freezing Rain)
- Only when our site has met all of these requirements, can we move on to the Design and Construction phase.

II. Building Design and Construction

The building design as well as the required construction materials must be chosen with Physical Security as a prime requirement, particularly as regards the walls, roof, windows, and entrances.

Form must follow function — the building's appearance must be secondary to its security requirements. Indeed, the less the building calls attention to itself, the better.

Some of the design elements we must include in our Design and Construction considerations are:

- Full-Height, One-Hour Fire-Rated Walls Around Complete Perimeter
- Penetration Resistant Perimeter Wall Construction

- Windowless Perimeter or Interior Barriers at External Windows
- RFI/EMI Shielding (TEMPEST)
- Anti-Concealment Landscaping and Architecture
- Physical Barriers for Site Perimeter and External Facility Environmental Equipment

The design must provide the maximum protection to the server farms. To this end, we will use a building within a building design where in the server farms are placed at the center of the building, with office or utility areas surrounding them on all sides. The server farms will be built in a bunker style, with reinforced, lead filled concrete walls, which will prevent any computer electrical signals from getting outside of the building. All doorways will be constructed with concrete block above and below. In any areas where concrete block isn't feasible, hardened steel installed at regular intervals under the raised floors and in the space between the server farm ceiling and the building roof. The server farm ceiling will be made of the same material as the roof and there will be nothing intervening between the ceiling and floor. As mentioned earlier, the utility areas will form one of buffers surrounding the server farms.

Here is we'll find our main electrical systems, diesel generators and plumbing. Additionally, utility shafts will also be located between each server farm to house the fire suppression and environmental equipment. This points up another basic Physical Security design principle – to completely segregate any ancillary equipment from the server farms. Electricians, plumbers, and other utility technicians will access their equipment without ever entering the server farm. The only exceptions to this are the Power Distribution Units, which by design, must be located inside the server farm with the computer equipment.

Another value of this design is that we can sandwich the server farms with redundant environmental and fire suppression equipment within the utility shafts. Should one shaft become disabled, the other side will continue providing an N + 1 level of protection.

Finally, within the utility area we will build two loading areas. This will allow a separate area for those vendors with clearance and another for those without it. The security arrangements for these areas will be discussed in more detail in the Internal Physical and Environmental Security section. The remainder of our buffer area will be provided by office space for the engineers.

III. External Security

We've got our facility built, but now we need to turn our attention to its defenses. We'll begin with our external security requirements. We want to create multiple layers of

security. An alarm will be sounded if a force of 88 pounds or more is applied to the fence; or if a gap of 8.7 inches or more is created between any of the vertical bars.

An intrusion detection system will provide our next barrier. A camera system covering the entire exterior of the facility and, in particular, recording all license plate numbers of vehicles entering the facility, is also required.

Only delivery and security vehicles will be allowed within the security perimeter. Staff and visitors will have a separate parking area located outside of the fence.

All entrances must be secured. This can best be done using a combination of smart cards, biometric devices, and man-traps. Each employee is issued an ID card and a Personal Identification Number (PIN). The first entry level then requires that you swipe your card through the reader and then enter your PIN, generally within a proscribed length of time. These systems will also provide an audit trail of all entering and will allow a limited number of failed attempts before locking the card out.

As this method is prone to the unauthorized use of cards, the next level uses biometrics for authentication. These offer a choice of fingerprint readers, palm readers, retinal scans, and voice identification. As fingerprints alone can be copied, my preference is either a palm reader or retinal scanner. The palm reader needs a live hand to provide the necessary amount of pressure for authentication and the retinal scanner requires the correct eye to be scanned. While both can be hoaxed, the degree of difficulty is quite high.

There is still one major gap in our entrance security. Neither of the previous methods will stop an unauthorized person from piggybacking in with or without the cooperation of an employee. A man-trap, an arrangement of two locked doors with only enough space between for one person, will close this gap nicely. A card reader and a biometric device will be used at both the entrance and the exit to the man-trap along with constant camera observation. Additional sensors may be considered to detect an extra set of feet, the presence of metal or explosives, etc.

If the building is small enough, only one entrance should be available for employees and visitors alike, manned by a permanent guard station. If there are additional entrances, the combination of card reader, biometric device, and man-trap should be used, but, if the entrance is in a low security zone, a card reader alone may suffice. Our final barrier, which should never be underestimated, is that essential human touch – roving guards along with permanently manned stations.

IV. Internal Security

Many of the same external security techniques are used as well for internal security. A camera surveillance system will be installed throughout the facility along with roving guards and a permanent guard station at the main entrance. A combination of card readers and biometric devices will handle authentication and where required man-traps will be installed.

The building will be partitioned into different security levels. Low security areas may only require a card reader for access, while the highest security areas will have a combination of card readers, biometrics, and man-traps. At the least, the server farms and utility areas will be classified at the highest level of security. Both the entrances and exits of the server farms will require auditing and authentication of all who pass through. The exit devices in the server farms will be programmed to reject any card and PIN that was not used to enter the center. This will require that every person in a group authenticate themselves one at a time. Use of man-traps at all doorways will make this requirement unavoidable.

In the case of extremely secure rooms or centers, it may be necessary to require authentication and auditing of the server cabinets. Additionally, this type of room will require a permanently manned guard station and manual logging of all entries and exits.

Temperature, Smoke and Humidity sensors will be installed throughout the facility, in various zones. In particular, there will be separate fire zones below the floor and above the ceiling. The gas will be stored in the utility shafts with air-sampling sensors inside the center used to release the gas. Air-charged, dry pipe sprinkler systems will also be installed.

The farms will be kept at 68 degrees Fahrenheit and 50% humidity. Water-cooling systems (aka chillers) will be located within the utility shafts.

V. Personnel

Access is the key issue with personnel security. All staff will be issued a Photo ID and PIN. These will be keyed to the different access levels discussed in the previous section. Only those who can demonstrate a need for access to a high security area will have it granted and that access must be held only as long as needed. The security team will maintain a record of all personnel with the highest access and will run regular audits to ensure that all IDs are accounted for and that justifications for high security access remain valid.

Requirements for this level of access should include at a minimum a background check, and very likely periodic drug and polygraph tests. As discussed in Building Construction and Design, our facility is designed correctly, it’ll allow repairmen to do their

work without entering a farm repairmen, custodians, etc. are denied access to any of farms. This goes back to the building design. There is no way to justify having custodial workers in such areas, which means the engineers will have to be responsible for maintaining a clean environment.

Vendor support engineers will have to be accompanied at all times by a staff engineer with the proper clearance. It is possible that vendor engineers may wish to go through the clearance process as well, which would then negate the need for anyone to accompany them.

All staff must sign a statement that they have been informed of the security policy, which will cover such areas as laptop security, maintenance and disposal of sensitive documents, and access levels. All must be held strictly accountable for any security breaches with misuse of one's access rights being grounds for dismissal. This policy must be supported and vigorously endorsed from the executive staff down if it is to be taken seriously.

The guards will be instructed to sweep work areas as they patrol and confiscate and report any unsecured equipment or sensitive documents.

VI. Tempest Needed

What kind electronic means would somebody use to spy on a computer that location would actually play a role in? If they cannot get in over the network, and cannot access the computer directly, then they cannot monitor anything about it, one would think. There are however always emanations from electronic equipment known as Electro Magnetic Radiation. Everything that carries a current of some sort produces this- everything from power lines and extension cords, to monitors and CPUs. These emanations are known as TEMPEST emissions. From this radiation it is possible from this radiation to do everything from see what is on people's CRT monitors, to actually monitoring what a computer does remotely. The biggest concern with TEMPEST lies in the fact that because of how the emanations occur, they are usually plain text and therefore once monitored, perfectly legible. This can be a huge concern as it could be extremely detrimental if somebody with the correct equipment, training, and motivation were to start monitoring for TEMPEST emanations. There are a couple of methods for combating TEMPEST emissions however. Just as you can shield against EMR coming in (solar flares and nuclear explosions are common sources), you can shield against that sort of energy being broadcast.

The most thorough methods of shielding involve building with copper foil in the walls to make a continuous cocoon around the room. All seams must be soldered together, and doors have to have the same shielding. Door edges need to have special seams to ensure

adequate conduction of current can occur, and the floor has to have a layer of steel in it to prevent any signal leakage occurring there. Everything that needs to enter or exit the room (wires, heating/cooling systems, etc.) have to run through special filters to help make sure that only clean signals that are intended to be leaving the facility are. Shielding a whole building for TEMPEST is usually prohibitively expensive. It is far more economical to merely shield a portion of the building- the server room. There is actually an advantage to this as well. As long as all the important information is processed in the server-room and the TEMPEST shielding is doing its job properly, then all the exposed computers and equipment outside the shielding act as an additional barrier to prevent people from monitoring EMI emissions. It would be similar to holding a whispered conversation in a football stadium when the home team just scored a touchdown. You can hear each other, but all anybody else hears is the roar of the crowd, which contains no meaningful information (Department). What if you could read lips though?

That brings us to another form of TEMPEST, Optical TEMPEST. A recent development has shown that the nice LEDs that are in everything from our desktop PCs, to our Servers, to our switches and router can be monitored for the flickering of network traffic and actually decode when things are being sent and received. Of course, if we observe the previous building/locational criteria, there are no windows or other openings for criminals to spy on the LEDs, and hence renders that method of observation useless (Loughry). Another method of Optical TEMPEST utilizes the light given off from monitors and recreating the image displayed from that. Obviously if one can look directly at a monitor, the recreation process is fairly straightforward, however new research shows that even light that has reflected off of walls can be used to recreate monitor displays. While there are some things that cannot be avoided, placing monitors with their displays facing windows is something that is an obvious security measure that is easy to remedy. Ensuring that the displays of monitors face perpendicular to windows would be most beneficial, as it prevents the monitor from shining off the wall directly opposite a window, in addition it should cut down on glare reducing eye strain.

The final option for TEMPEST security is white noise jamming. The theory is that if you make enough noise, even an unshielded system is safer because of the amount of noise surrounding it. It takes the idea of placing the server-room in the center to help mask the TEMPEST emissions one step further. Instead of just letting other equipment make noise, you generate the noise intentionally, and “louder” to drown out any emissions that your equipment might really be making. Obviously, a combination of all of the above would be the most

effective method of TEMPEST protection, however as stated earlier, this can be incredibly expensive, especially for entire buildings.

TEMPEST shielded buildings protect against unintentional emissions, what about signals that were intended as broadcast signals that are therefore inherently a vulnerability? Wireless networks, while incredibly convenient to install can be a severe liability in terms of security. In an office situation, there is no reason that, with proper planning and implementation, a completely wired office would not yield the same mobility that a wireless network does. It may be slightly less convenient due to the requisite plugging and unplugging of cables, but it is almost ten times faster, and there are no broadcast signals to be monitored by people who just happen to wander by with a laptop and a wireless network card surrounding it. It takes the idea of placing the server-room in the center to help mask the TEMPEST emissions one step further. Instead of just letting other equipment make noise, you generate the noise intentionally, and "louder" to drown out any emissions that your equipment might really be making. Obviously, a combination of all of the above would be the most effective method of TEMPEST protection, however as stated earlier, this can be incredibly expensive, especially for entire buildings.

TEMPEST shielded buildings protect against unintentional emissions, what about signals that were intended as broadcast signals that are therefore inherently a vulnerability? Wireless networks, while incredibly convenient to install can be a severe liability in terms of security. In an office situation, there is no reason that, with proper planning and implementation, a completely wired office would not yield the same mobility that a wireless network does. It may be slightly less convenient due to the requisite plugging and unplugging of cables, but it is almost ten times faster, and there are no broadcast signals to be monitored by people who just happen to wander by with a laptop and a wireless network card.

VII. Disaster Recovery

Now we need to address the possibility of things going wrong..

To counter the loss of electricity to any of the server farms we have Uninterruptible Power Supplies (UPS). We will again double the standard N + 1 redundancy rule and as a further precaution will separate the UPS in two rooms. If we lose power from one grid, we have the second power grid to fall back on. If this is out as well, we will have diesel generators ready to supply power.

To keep the generators running, we will contract with a minimum of two vendors and will have storage capacity on-hand sufficient to run the facility for several days. At least once

per month we will test the generators by switching the facility off of the grids, using the diesel generators as the sole source of power.

Our extensive Physical Security measures would be for naught should we lose the very function the facility is meant to provide— LAN hosting, which means we must have multiple Internet connections provided by at least two different vendors.

All servers will have their data backed up through a central backup system. This system will follow a standard rotation of full and differential backups. The backup logs will be audited on a daily basis to ensure that all systems were completely backed up. Tapes will be duplicated, with one copy being sent offsite for secure storage. Random test restores will occur on a weekly basis to ensure the integrity of the tapes.

Finally, to protect the data even if the facility is destroyed, fail-over sites will be maintained for those clients with no downtime tolerance. These will be tested on a monthly basis.

Conclusion: The Ideal vs. the Real

To build a facility that meets all of these requirements is an expensive intention. For a LAN Hosting Company, it's a question of how much of this cost they can pass on to their clients.

With a corporate data center, it's more about convincing senior management that all of this is necessary. Physical Security implementations in the real world generally fall well short of the ideal.

From the start, your attempts to promote this high a standard of security will be compromised, with the site of the facility the first of many more compromises to come. In the ideal scenario, our facility is built where we want it and how we want it. In reality, the budget may only allow you to use an existing building, or the location may be too close to streets or railways. The ripple effect begins.

If you're in an existing building and particularly if your data center is on the tenth floor, fencing, as well as some of the other external measures are out of the question. You will have to live with the exterior walls that are highly unlikely to meet standards.

You likely will have no control on the choice of neighbours and no buffer to offer you some protection. Biometric devices are, you discover, quite expensive, as are man-traps. How will you ever convince your senior management that these are necessities and not luxuries? Perhaps you'll even end up convincing yourself that security won't suffer if you only use

smart cards and standard doors. It can get even worse; you may not even be able to control the number of people with access to the server farm.

Backups are another area needed in companies When web hosting, you've got to check that this is included. Otherwise it's your responsibility. Often, though, backups are not even being done or tapes being sent off-site. Many LAN -hosting companies and IT departments just go along hoping that no one will ask for any data to be restored. Finally, fail-over sites are still a luxury for all but a relative few. This is definitely an expensive service and most companies never consider the cost of losing not only their data, but their workplace as well. If they did the math, the cost of a fail-over site might seem a lot more reasonable.

Physical Security isn't rocket science. The standards exist and there're many good checklists and examples for other companies to follow. The reason Physical Security is an often ignored or under-implemented piece of Information Security is quite simply the cost. There're simply is no cheap or easy ways to good physical security. Natural or man-made disasters can always be counted on to bring Physical Security to the forefront of everyone's minds, and it is to be hoped that many companies will then begin the process of reviewing, creating and implementing better Physical Security standards. Past history, however, has shown that once the initial event recedes further into the past, companies tend to go back to their old ways, forgetting these hard-learned lessons. Perhaps now, with the recent effects and threats of global terrorism all too obvious, this will change and a complete physical security implementation will become as commonplace as firewalls.

References

1. Ellerbe Becket Physical Security Primer, http://www.eb-datacenters.com/tech/sec1198.html
2. Ellerbe Becket Physical Security Check List, © 1998, 1999 Ellerbe Becket, http://www.ebdatacenters.com/tech/sec1198-list.html
3. Digex SmartCentersSM, © 2001 Digex Inc., http://www.digex.com/leverage/smartcenters04.htm#dc
4. Premier Data Centers, Copyright © 1996-2001 Verio Inc., http://home.verio.com/products/datacenter/premier.cfm
5. Shelter From the Storm, By: G. Beato Business 2.0, Issue: June 2000, Copyright © 2001 Business 2.0 Inc., http://www.business2.com/articles/mag/print/0,1643,13782,00.html
6. Internet Data Centers, © 1999-2001 Exodus Communications, Inc., http://www.exodus.net/idc/idc_diagram.html
7. FM-200 Fire Protection Systems, http://www.reliablefire.com/fm200/fm200.html

8. CSU3000, Constant Protection For Water-Cooled Medical & Industrial Equipment, Copyright © 2001 Liebert Corporation, http://www.liebert.com/products/english/products/env/csu3000/60Hz/bro_4pg/html/SL_11730.asp
9. Generator Packages, Power Solutions & Sizing Your System, http://www.caterpillar.com/industry_solutions/shared/electric_power/products/products.html

SECURITY POLICIES AND NEW TRENDS OF INFORMATION ASSURANCE IN A UNIVERSITY

Capt. Călin LUP

I. INTRODUCTION

As the time passes the importance of the physical things accumulations is paler opposing to the value of the amount of information that someone posses. The increased development of the information management and the use of the personal computers became very fast a condition "sine qua non" of a person/organization level of performance. There were a lot of managers who did not pay attention to this point of view and paid a lot for that. As soon as they realized the importance of personal computers and the connections between them, they were with a step in front of their competitors. Of course there were great windfalls profits obtained by those who discovered these things first, but there were too terrible scenarios of giant organizations which went bankrupt due to their indifference, lack of knowledge or fear towards the computers.

A proper understanding of the computers role reflected in economical advantage and it was very clear that in order to stay up to date with them we must use the proper applications installed on them. On a personal computer from home is easier, but when we involve here organizations the problems begin to arise. The fact that the data must be stored and used by different people represented an issue. Another problem is that the individuals who use the applications don't have the same rights. From this point forward it was clear for everybody that at the organizational level something must be done in order to solve these problems. A proper scheme is needed in order to see who must have access to what kind of information; an authority over the information management must be named and so on.

For example, in a university there are a lot of computers networked in different places and which are accessed by several people. The teachers must have some specific rights in order to trace the students' presence in classes, to put grades or to modify those grades. The students, on the other hand must have only the permission to consult the grades or the class schedules without the possibility to modify them. The access to internet must be permitted to everybody in order to access data they need, but the traffic must be somehow analysed in

order to restrict the extracurricular use of the bandwidth (social networks, messaging, etc.) If we are talking about a military university the problem is a little bit more complicated, and there are other issues that arise from the classification levels of the information which are trafficked.

Strong security policies are the answer to all that we need in order to ensure that the information possessed is protected. The security policy is basically a plan, outlining what the organization's critical assets are, and how they must (and can) be protected. Its main purpose is to provide staff with a brief overview of the "acceptable use" of any of the Information Assets, as well as to explain what is deemed as allowable and what is not, thus engaging them in securing the organization's critical systems.[1]

II. INFORMATION SECURITY POLICIES

Acceptable Encryption Policy

This policy resigns from the need of having a proper control of the data which is encrypted. In order to encrypt something one must be aware of the fact that the encryption algorithm that he/she uses has a substantial public review and it works effectively in order not to loose the information.

The subject of the encryption is usually sensitive data, which must be publicized on an available database, and which must be encrypted in accord with the standards from the below paragraph. All the subjects who use information technology resources involved in the development, transfer, or sharing of the encryption technology must be aware of the fact that these activities may be controlled by the national laws.

On the military universities the encryption must be used on the operative work, usually when the operational readiness is tested. During field training exercises the students must be encouraged to do rehearsals in order to be ready anytime to use encryption equipments to their communication terminals. The proper use of the encryption terminals must be supervised very carefully in order not to loose them, our days are very small pieces of equipment, or to make possible for the encryption keys to be stolen or intercepted by someone who is not allowed to work with them.

Antivirus Software Policy

All the computer machines from a university network must have an antivirus /antispyware software installed and updated with the latest definitions. It is necessary that a

[1] http://www.windowsecurity.com/pages/security-policy.pdf

list of the antivirus/antispyware acceptable programs to be publicized in order for the students to know exactly which the lowest level of protection is requested. All the machines which are owned by university must have access to a particular file from where to install the latest updates of their antivirus/antispyware software.

Audit Policy

The audit policy from a site must be known by all the users in order to advise the security scan procedures and precautions used by the IT department to audit their network and systems. Other persons or entities are prohibited from performing any such tasks, unless they are authorized (some kind of higher audit agencies or organizations).

Audits are made in order to:

- Ensure integrity, confidentiality, and availability of information and resources;
- Investigate possible security incidents to ensure conformance to the university's Information Technology policies;
- Monitor user or system activity where appropriate.

The IT department utilizes auditing software to perform electronic scans of their networks, servers, switches, routers, firewalls, and/or any other systems from university. This also includes scans of any electronic communication and e-mails regardless of by or to whom the communications are sent.

These tests may include:

- User and/or system level access to any computing or communications device;
- Access to information that may be produced, transmitted or stored on university equipment;
- Access to work areas (labs, offices, etc.);
- Access to interactively monitor and log traffic on university networks;
- Penetration testing;
- Password Auditing;
- Scanning for Personally Identifiable Information.

Data Sanitation Policy

This policy shows the procedure by which data is permanently removed from a computer, server, removable media, etc. in such a way that the data is deliberately made non-recoverable. A record retention policy must be consulted by the users prior to delete any data.

In order to avoid the risk of multiple information storage a secure deletion of files is required in some situations. These situations are:

Transfers within a module: it is the situation when a change of position occurs in a department and a laptop, computer, etc. must be transferred from one person to another. The data sanitation is not necessary all the time because usually the tasks of specific position remain the same, but there are situations when the one who is promoted doesn't have appropriate rights to the information contain on a specific device. If the information must be deleted than the required steps must be followed to ensure that the device is sanitized.

Transfer to another module: when devices are moved between compartments, the entire data specific to the old compartments must be deleted. There are special cases when the data can be kept, but with an agreement between managers/chiefs and the approval of the security department.

Device disposed outside the university: it is the case when a computer, laptop, removable media, etc is removed from the university's inventory and all the data should be removed before that.

It is the administrators and/or the device owner responsibility to ensure that the device is properly sanitized. The method used to sanitize the device will depend on the level of confidentiality of the data which were stored. Any problems which are observed and which doesn't match the data sanitation standards must be reported as soon as possible to the security department.

The data sanitation in military university from the point of view of the devices which are throwing away is very simple, physical destruction. There are a lot of computers from libraries or study rooms which in my opinion can be traded or donated to some organizations; usually the level of confidentiality of the data from these machines is unclassified.

E-mail Policy

A modern policy regarding the e-mail use must be focused not to impose restrictions but to encourage the culture of openness, trust and integrity, in order to outline the appropriate use of the e-mail as a main mean of communication. This open minded approach must be doubled with some rigorous checks and the users must be aware of the fact that they can be monitored without prior notification. These regulations must be applied both to the sent and received messages.

Users are strictly prohibited from:

- Sending unsolicited email messages such as chain mail or spam;
- Forging or attempting to forge email messages, or disguising or attempting to disguise the identity when sending mail;
- Giving out a password for any type of university account via email.

Users are strictly required to delete spam, chain, and other junk email without forwarding.

Subject to the e-mail transmission is only unclassified information; any sensitive data which must be transmitted outside must be encrypted by following the level of classification in which it is part.

In addition, users are reminded that they will be held responsible for the content of e-mail the same as with any other communication. An e-mail which is defamatory may lead to the user being sued by the defamed individual. The sexual harassing or any kind of threat messages doesn't isolate users from the responsibilities which exist according the law.

E-mail may be used as an official mean of communication, with some exceptions, which will be clearly stated and which regard the situation of the parts to be face to face. The personal e-mail may be used by the students, teachers and staff without affecting the productivity or the mission of the university.

In military universities there are some kind of formatted messaging which is used in order to transmit all kinds of reports but it will be discussed in the third chapter. The computers which are connected to the Internet and can be used in order to send or receive e-mails must be very carefully verified in order for the data which is transmitted to be unclassified. Any kind of classified information must be transmitted thru the secured connections.

Incident Response Policy

This policy defines the actions that should be taken if the university's system is compromised. The IT department is authorized to take any immediate and appropriate measures to ensure that the breach which occurred doesn't produce any further damages.

The security structure chief must be informed immediately about any breach of security which is observed. Everything that has been observed must be noted in the Incident Report, and presented to the security structure. The Incident Report must be clear and concise. A model of Incident Report is presented in *Annex A*.

In order to solve the problem will be used communications which have nothing to do with the compromised system or network. The Security Structure Chief will ensure that all the organizations which were connected to that system/network are informed about the incident in order to be able to take the necessary steps in order to respond to a possible intrusion. The log of all the contacts and the information exchanged must be very accurate and detailed analysed.

The violation of this policy must be very precisely sanctioned with a prohibition of the access to the IT resources (temporary or total) or termination of employment.

Information Sensitivity Policy

The information covered in this policy includes electronic information stored on computers, e-mails, information on computer screens, and information shared (oral or visual). At the security structure chief must be a list of the categories of information which is considered sensitive and any questions about the proper classification of a specific piece of information must be addressed to him or her.

The type of information which is handled, the legal requirements regarding that information, the level of sensitivity attached to it and the ways for protection is the responsibility of every single employee who handles electronic information.

The levels of sensitive information from a military university must obey the military regulations with few exceptions. The exceptions regard the fact that not all the students after graduation will continue in the military. This is the reason why the students access in allowed only to the unclassified information in electronic mode. The use of classified information will be under a very strict control of the platoon leaders. At platoon level must be a register with all the students who consulted classified information and the reason why he or she needed that information. The details regarding electronic distribution, encryption, storage and destruction are the same like those from the military.

Mobile Device Policy

Portable computing devices, but not only Personal Data Assistants (PDA), Blackberry devices, iPhones, laptop/tablet computers, etc. is subject to this policy. The portability offered by these devices increase the risk that the data which are stored in them can be spread without a proper control. The poor security of the devices represents another important issue of their management. In order to deal with them there are a set of rules which must be followed to preserve the confidentiality, integrity and availability of these devices.

A minimum set of rules to follow when use these devices are:

- Sensitive data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive data must be encrypted using approved encryption techniques and password protected;
- Sensitive data must not be transmitted via wireless communication to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized;

- All remote access to university information resources must use a university approved communication channel (e.g., Virtual Private Network (VPN), and web-based access to resources provided using the web, etc.);
- Computer systems not owned by university that require network connectivity must conform to university's information security policies and procedures;
- All mobile computing devices must have approved virus and spyware detection/protection software along with personal firewall protection (where applicable);
- Unattended portable computing devices must be physically secured.

Password Policy

The passwords represent a major aspect and they are the front line of the protections of the user accounts. The people from university who have a password must be aware that a strong one will ensure the security of their data, and of course they have to take the appropriate steps to select and secure their passwords. The protection and frequent change of the passwords is another important step in information assurance.

The particularities of the passwords from a military higher education institution must be focused on the fact that students deal only with unclassified information. At all the other modules from the university the military standard of password management must be followed.

Strong passwords have the following characteristics which will be followed regardless of system imposed restrictions:

- Are at least eight alphanumeric characters long;
- Are not words in any language, slang, dialect, jargon, etc;
- Contain both upper and lower case characters;
- Have digits and punctuation characters as well as letters;
- Are not the same with those used in other occasions (social networks, etc.);
- Are not based on personal information.

The password cracking is subject to IT office mandatory activity and if the password is cracked the user will be informed in order to be changed.

A more powerful method to protect a user account is to use passphrases which are encouraged to be used in order to defend against “dictionary attacks”.

Removable Media Policy

The removable media represents a well-known source of malware infection, and a possible threat of the sensitive data. In order to have a highly protected system/network the removable devices must be very careful handled.

In military universities the use of removable media is allowed only on personal computers which are not connected to any classified network. For the machines connected in the classified networks the use of removable devices are monitored by the communication module. In this direction at the communication compartment exists distinct registers for all levels of classification. After their use, the removable devices must be erased in order to prevent the security of the information. All the removable media which are assigned to be used in classified networks must be registered and carefully handled. For the external use of these devices a commander approval must be obtained.

Wireless Communication Policy

The use of wireless connectivity is a normal development of the communication systems, but in the same time represents a potential source of insecurity. The tremendous rate of development blinded the producers from the IT sector and the attention paid to the security of the information lowered from a generation of devices to another.

The wireless infrastructure which resides or is connected to a university network must meet the following requirements:

- Be installed, supported, and maintained by communication module;
- Use university approved authentication protocols and infrastructure;
- Use university approved encryption protocols;
- Maintain a MAC address that can be registered and tracked;
- Not interfere with other wireless access deployments.

The isolated wireless devices must meet the following requirements:

- Be approved by communication module;
- Not interfere with the other wireless access deployments.

Any rogue access point discovered in university may be confiscated.

III. POLICY BREACHES

Policy Breach Plan

Despite the security measures that are taken in order to protect the sanity of the machines and system there are always problems that occur and which must be handled very

carefully. The problems may arise from a theft, a deliberate attack on your systems, from the unauthorized use of personal data by a member of staff, or from accidental loss or equipment failure. However the breach occurs, you must respond to and manage the incident appropriately. Having a policy on dealing with information security breaches is another example of an organizational security measure.

A possible definition of "security breach" is the following one: an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach.[2]

There are four main steps contained in any breaches management plan[3]:

1. Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.

2. Assessing the risks – you should assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

3. Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. You should be clear about who needs to be notified and why. You should, for example, consider notifying the individuals concerned; the security structure chief; other regulatory bodies; other third parties such as the police and the banks; or the media.

4. Evaluation and response – it is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. If necessary, you should then update your policies and procedures accordingly.

Information Security Education

The goal of keeping the information protected can be achieve thru a lot of measures but one of the most important is a proper education provided to the people that work with

[2] http://policy.uncg.edu/security_breach_notification/
[3] http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx

those data. Below are some new methods of education which can make the IT briefings on information assurance more interesting.

1. **Security Newsletter** sent thru e-mail is an interesting and valuable way to reach and educate your staff. You could also give staff the additional option of having the newsletter sent to their private e-mail address as well, so even if they do not have the time to read it at work, they will have the opportunity to do so later, from home. The main idea behind the creation of a security newsletter is to provide users with an interesting, and engaging way of understanding the points outlined in the security policy.

2. An Information Security Web Site is recommended to be created in order to act as a central starting point for everyone interested in IT security. If successfully implemented, this venture will also create a community feeling in the long term, which is an invaluable asset for company security in general.

The site must be clear, easy to browse, and easy to navigate; do not overload it with a lot of files and technical papers, most of which probably contain words not known to staff members. Provide them with interesting and comprehensive FAQ's (Frequently Asked Questions) on specific topics; if you cannot find suitable content for your needs, write new ones and distribute them among staff using the security web site as a distribution medium.

3. The 'We need YOU' Technique is a must-use technique, as far as changing the employees attitude towards their role in company security is concerned. Basically it provides all involved with the opportunity to actively contribute to the educational process with their very own advice, ideas, personal experiences, recommendations, and if the contribution is good enough the employee will get the opportunity to present the topic personally at one of the lectures or discussions.

This method will motivate more or less everyone to participate in the security awareness program, while on the other hand creating a friendlier, more informal atmosphere. As an added bonus they will also learn how to protect their own personal PC's at home and pick up valuable tips and tricks on the way.

4. Educational Contests which are organized from time to time not only helps measuring the security awareness level of staff, but also varies and innovates the educational process.

Password cracking contests are a good example; they contestants are faced with the challenge of cracking a file that has been protected by a password chosen by a fellow contestant, with the idea of finding/eradicating weak passwords. Most staff is usually interested in such activities, and most of them will do their best to use hard to crack passwords following the recommendations on the process of creating strong passwords.

Of course these are just some of the methods from an entire arsenal which a bright security structure chief has in order to increase the level of data protection within the organization where he or she is hired.

IV. NEW TRENDS

Cloud computing

Universities, due to their research work, in special, and to their mission to teach, in general, must provide technology services to a high level. In some of them, the technical ones, the need of special services is high, as long as in the other ones the need is just to be available.

By offering a wide range of services over the Internet, cloud computing is a useful tool in order for the universities to use their resources in a proper manner. The cloud environment is somehow a new way of seeing things from the IT department point of view. If their technical skills were very important in order to do their job, from now on they have to enlarge their horizons and study more on management, in order to sign contracts with the cloud computing providers; on finance, in order to stay on a particular budget and last but not least on decision making, because they will have to decide between in-sourced and outsourced services. Another advantage of cloud computing relates to the possibility of a university which has its faculties spread in different areas to access their resources without any concern. From this point of view the collaboration between higher education institutions, and not only them, is encouraged.

Of course there are some question marks when we talk about cloud computing. The wide spread of the cloud computing is pulled down by the security, availability and third-party control issues. The defenders of the cloud computing argued that their security measures and processes are by far more reliable by those used at the average level; the availability is solved by multiple back-ups and the references to the third-party control were combated with the private clouds, which of course have a lot of limitations towards the public cloud. Another measures used in order to trust the cloud is by encrypt the data which are handed over the cloud.

In conclusion, by taking into account the positive and negative parts regarding the cloud computing, there are IT specialists who decided that at the campus level the cloud computing represents a viable option which is safer and more proper regarding the complexity of the IT system at this level.

C2 and Messaging Software

Due to the increased evolution of the modern warfare the classical way of approaching military conflicts is obsolete. A new generation of conflict is under way in operation theatres and it is based on asymmetry. This is the reason why the military leaders underline the importance of information and there are voices who claim that without a reliable flow of the data the brute military force is useless.

In order to educate the future leaders to easily master the quantity and quality of information they posses, the software developers came with solutions which help military system to adjust their needs to our days technology.

Command and control software SitaWare, developed by Systematic, represents a reliable, cost-effective off-the-shelf C2 solution designed to put information where military leaders need it most. SitaWare solutions provide consistent, scalable frameworks for information management systems for military organisations. Using the same core at all levels ensures seamless integration right from HQ to the individual vehicle and soldier, providing complete command and control.

The critical importance of this system represents the real time image of the battlefield from soldier to general. By using this software the soldier who is on the battlefield is able to enter data on map in order to help his superiors to make the proper decisions from their headquarter location. Thus, the decision making process reaches at the platoon or even squad level in real time.

Another very important software application, IRIS, places the information within data structures that help recipients understand the contents clearly, so they can take the right action. This military messaging application is designed to enhance Outlook with the possibility to send/receive military formatted reports.

Bottom line, SitaWare and IRIS represents a cutting edge technology which enables military organisations to rapidly analyse and respond to threatens provided by the asymmetric conflicts in a secure environment. The classification levels of the data which are transmitted require undoubtedly some specific software focused to provide the ultimate protection.

V. CONCLUSIONS

The security policies which were named here are those who regard the non IT members of a university, there are some others like server or VPN policy which regard them. The content of the policies must be a subject of continuous modification because they regard electronic equipments that have an exponential development. The problems which arise must

be immediately transformed in lessons learned and implemented in order to maintain a functional system. A key factor of the policies is represented by the means with which they are delivered to the users of the computers / networks, because without their active participation the efforts made by the specialists are useless.

Regarding the new trends from the domain there are a lot of other interesting things that must be said. Cloud computing and military software are just the two ones which I referred here. By analysing them we have to be very careful on the level of security provided by the first one and on the lack of control over the software provider of the last one. Without a proper checking and rechecking of these new trends, a blind implementation in sensitive sectors may lead to serious security problems.

Annex A - Incident Report

1. General Information
1.1 Incident Number:
1.2 Reporting Site Information
1.2.1 Date/Time of Report
1.2.2 Name
1.2.3 Department Name
1.2.4 Title
1.2.5 Telephone Number
1.2.6 Fax Number
1.2.7 E-mail Address
1.2.8 Office Address
1.2.9 Domain Name
1.2.10 Other Contact Info

2. Incident Information
2.1 System Information
2.1.2 Physical Location of system(s)
2.1.3 Type of device
2.1.4 Machine name
2.1.5 Purpose of system(s)
2.1.6 Current Status
2.1.7 Operating system(s) of device(s)

2.1.8 Security in place (i.e., Firewall)

2.1.9 Can you provide logs? _

2.2 Intrusion/Attack Information

2.2.1 Date/Time of Incident?

2.2.2 Duration of Incident?

2.2.3 Nature of Problem?

2.2.4 Attack Type (i.e., Trojan)?

2.2.5 Extent of compromise?

2.2.6 Damage or loss of information?

2.2.7 Source address of the attack? (IP, MAC, etc.)

3. Other Information

3.1 What actions or technical measures have been taken?

3.2 Have you notified law enforcement or another agency?

3.3 If known, please list stakeholders of the compromised system.

REFERENCES

1. https://sites.google.com/a/murraystate.edu/information-security/policy;
2. Dancho Dancev – Building and Implementing a Successful Information Security Policy, WindowsSecurity.com, pag. 19-22;
3. Institute of Education University of London - Computer Security Policy;
4. http://www.hampshire.edu/computing/17436.htm;
5. http://www.nist.gov/itl/cloud/index.cfm;
6. http://www.nist.gov/itl/computer_security.cfm;
7. http://www.systematic.com/defence+website/defence;
8. http://policy.uncg.edu/security_breach_notification/;
9. http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.asp x

All websites listed above were accessed from 11 to 19 February 2012.

CURRENT METHODS AND TECHNIQUES USED IN CRYPTOGRAPHY

MAJ. George NICOLA

Introduction

1. Basic Concepts of Cryptography

I chose this theme because information security, cryptography is a fundamental science to secrecy of communications between users on different platforms developed.

The meaning of the word cryptography (the primary meaning: secret writing) comes from the Greek "kryptos" which means *obscure, hidden, secret*, and "graphy" which is the Greek word for *writing*.

Yaman Akdeniz in his article "Cryptography and Encryption" gives the following definition of the term: "Cryptography, defined as <the science that deals with the study of secret writing>, treating the means through which communication and data can be encrypted to prevent their discovery by interception, codes usage, ciphers and other means, so that only certain people can view the original message."

The first mention about cryptography appeared more than 4,000 years ago, in ancient Egypt.

Cryptography provides the methods for hiding the meaning of messages so that only certain people may understand them, and also the methods to ensure that the content of the message remains unaltered[4].

Cryptography studies encryption, classification, and coding systems of information and also the procedures for storage, processing and transmission of resulted cryptograms, solving categories of security issues: the secrecy and authentication of the information.

The methods, procedures and covering techniques are ensured by the **secrecy** and the measures to prevent the injection of unauthorized messages in the channels used for sending the messages and the insurance of the target recipient are managed by the **authentication**. The domain of cryptology which studies the principles, methods, procedures and the systems of "attack" on information deposits and the processing resources is the **cryptanalysis**.

[4] Constantin Popescu, *Introducere in criptografie*, Ed. Universitatii din Oradea,2011.

The **encrypted writings** are composed of sets of signs, figures or texts which have a clear aspect of a secret language, remaining incomprehensible for those who do not know the agreement (cipher) established for their understanding.

The **cipher** is a set (a lot) of bi-univocal transformation agreements together with their rules of use, through which we obtain from a plain text an encrypted one, called cryptogram. This method is necessarily a reversed method.

2. Brief History of the Encryption Systems

2.1 The ancient system Skitala

Skitala (in Greek "stick") was a device used to obtain a permutation encryption system. It had a cylindrical form and around it a strip of paper was wrapped. The message was written clearly on the tape and then, the paper was unwrapped. Upon receipt they used a similar cylinder on which there was wrapped the strip of paper and the message became intelligible again[5].

The Spartans used this mode of communication during military campaigns. The system was fast and there were no transmission errors. A major drawback was that it was easy to break.

Skitala

2.2 The Jefferson Cylinder

Thomas Jefferson invented a mechanical encryption device called "encryption wheel" used for the security of diplomatic correspondence.

The Jefferson cylinder is in the form of *n* disks having an equal size (initial $n = 26$ or $n = 36$, the value is irrelevant for the system) placed on an axle.

The disks could rotate independently on the axle, and on the edge of each disk the 26 letters of the alphabet were written in a random order (different for each disk).

[5] http://ro.wikipedia.org/wiki/Criptografie

During encryption, the plain text was divided into blocks of *n* characters. Each block is written on one row (generator) of the cylinder, turning each disk in order to bring on the line the letter which was sought. The block of ciphered text consisted of either one of the other 25 rows.

In order to decrypt, they used an identical cylinder on which it was written on one row the encrypted text (*n* characters) and then they searched among the remaining 25 rows a text having a semantic significance. The likelihood of having a single text like this increased with the number of disks used from the cylinder.

2.3 Machine C – 36

The C - 36 machine (known as M-209) was created by the Swedish engineer Boris Hagelin, based on a model created by Hagelin in Sweden in 1937. After some changes they started to produce it in 1940 and gradually replaced the encryption machine M - 94. During the Second World War there were produced about 140,000 C - 36 encryption machines.

There were not taken special security measures since the C – 36 machine was intended for tactical military areas, which needed only a few hours of safety for a possible cryptanalysis[6].

2.4 Colossus machine

The world's first computer (equipped with electric lamps) an electronic giant (the size of the interior of a cathedral), was called Colossus and was built in 1942.

Another character was added to the binary representation of each character. For example, by adding H (00101) to F (10110) we obtained B (10011).

The Colossus had a 25-bit RAM memory, and the programming was obtained by connecting cables among the various connections on a panel, but with a conditional instruction (e.g. IF THEN ELSE). It was very reliable, producing an error at every 100 billion calculations.

2.5 Encryption machine ENIGMA

Enigma (the German encryption machine having different models for the armed forces) was a combination of mechanical and electrical systems.

The main subsystems consist of a keyboard, a set of rotating disks called rotors and a movable mechanism for moving one or more disks during the pressing of keys. There were

[6] http://webhost.uoradea.ro/cpopescu/cryptography/Cursul1.pdf

several mechanisms, but the most common is the one for which the rotor on the right moves for each keystroke and occasionally triggered the motion of the adjacent rotors[7].

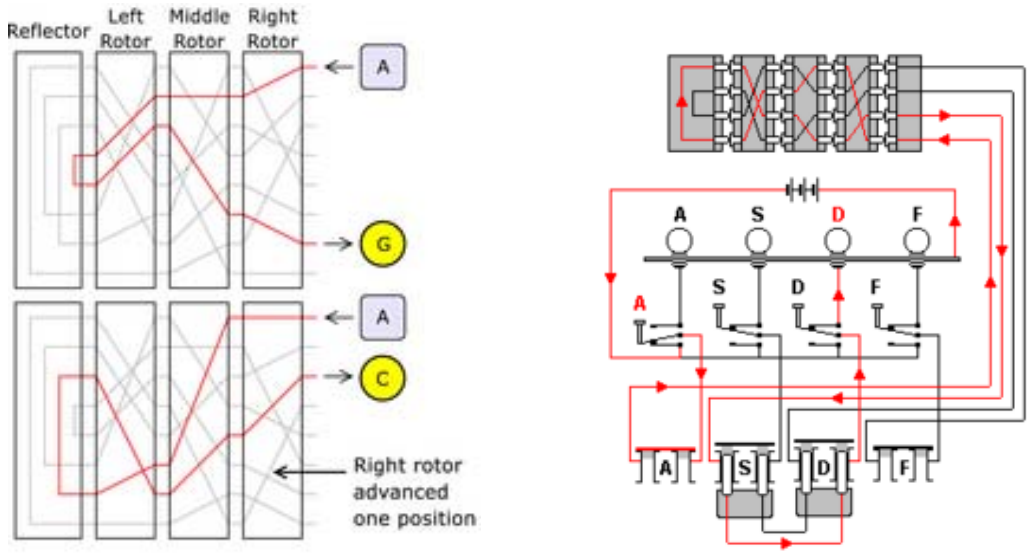
Continuously moving rotors induce a different cryptographic transformation after each keystroke.

The mechanical parts act so as to form a different electric circuit. The encryption of a letter was done electrically. When a key was pressed, the circuit closed, the current flew through the components of the subsystems, lighting one of the lamps and indicating the output letter.

At the beginning of a message encryption, the operator (for example) can first press button B and Y lamp is lit so, this would be the first letter of the ciphertext. The encryption will continue the same way throughout the operation. The electricity started from a source through a bipolar switch controlled by the pressed key. The panel with sockets (if any) mediated the connection between the keyboard and the fixed “input disk", the configuration could be easily rebuilt by any operator. From the panel with sockets the electricity reached the fixed” input disk ".

From this point the current passed into the set of rotors, each rotor causing the voltage to go through circuits with a variable configuration from a rotor to another. After passing through all the rotors, the flow went through the "reflector", which redirected again the signal through the rotors towards the “input disk" (using another way of transmission) then through the panel of sockets, through the bipolar switch of the target letter, finally lighting the appropriate lamp.

[7] http://www.apprendre-enigne.net/crypto/bibliotheque/PDF/KruhDeavours.pdf



Full diagram of the rotation

Chapter 1

1. Encryption Equipment for Voice - Data Communication Protection

In this chapter I will present some of the modern cryptographic means. About 40 companies in over 20 countries, such as Marconi Italiana, Italy, Alcatel Bell-SDT, Belgium, Motorola Inc., USA, Philips Crypto BV, Netherlands, Ericsson Radio Sytems, Sweden, etc. are interested in the domain of the cryptographic equipment.

2. DSP 9000 HS - Speech encryption equipment

The equipment consists of a module incorporated into the panel of the radio station DSP 9000 RB, both produced by the Communications Corporation (TCC), USA. It provides high protection for HF, VHF and UHF radio communications. The encryption algorithm consists of the numerical processing, controlled by a non-linear generator of the audio spectrum[8].

The key management implies the existence of three levels of keys:

- network keys with a diversity of 6,55 x 10^4;
- system keys with a diversity of 8,39 x 10^{79};
- local keys with a variety of 7,2 x 10^{16}.

[8] www.tccsecure.com/.../DSP9000-detail-HS

DSP 9000 HS

The equipment can record a number of 200 local keys introduced from the keyboard or from an external module of transport and key loading, which are divided into two groups of 100 keys.

Some important features of the device:

- the protection of the equipment against unauthorized access is done by using a password;
- the change of the keys can be done manually or automatically by indexing 1,12,24,48 or 120 hours by indexing from 001 to 100 and in both cases the current number of new local key is sent through radio to the receiving equipment DSP 9000 HS;
- after working, in a secret mode, you can return automatically to plain text to allow plain and encrypted reception;
- the delay due to the signal processing for encryption may be of 524 ms/262 ms depending on the quality of the channel (HF / VHF and UHF).

3. CRYPTOVOX HC-3300 - voice, fax and data encryption equipment

The device is manufactured by Crypto AG from Switzerland.

The encryption algorithm based on a numerical flow generated pseudo randomly, relies on the usage of the analog-digital voice signal.

An internal modem provides the interface with the phone line that enables[9]:

- classified telephone calls duplex encrypted at the speeds of 9600/4800/2400 bps and semi duplex encrypted at the speeds of 4800/2400 bps;
- duplex encrypted data transmission at the speeds of 9600/4800/2400 bps;
- facsimile connections.

Key management is done using several types of keys, namely:

- communication keys (33 keys of which 3 of them are for multipoint connections);

[9] www.cryptomuseum.com/.../hc3300/index

- structure key (one);
- key for keys transport.

CRYPTOVOX HC-3300

The communication keys are stored in the equipment, also encrypted, having a length of 128 bits and a diversity of 10^{38}. Total diversity of the key is of 10^{77}.

Using manipulation and key management equipment there can be done an on-line key manipulation where CRYPTOVOX-3300 equipment is spread over a large area. To protect the communication keys for loading and distribution we use an electronic card, KDC-3300 (2kb memory type EEPROM).

4. CRYPTOFAX 4750 - military fax machine having an encryption device

The device is manufactured by Crypto AG in Switzerland. Basically it uses two communication protocols that can create classical connections with other fax machines and facsimile connections through radio channels using a digital protocol[10].

Key management is done by:

- 32 sets of 3 keys of communication (active, replacement and expired), expandable (optional) to 256 sets of 3 keys with a variety of 10^{38};
-a structure key, saved in EPROM, with a diversity of 10^{38};

The communication keys are inserted manually from the keyboard or using the electronic card or from the management center, using the connecting channel.

The 3 communication keys (active, replacement or expired) allow the changing of keys to be executed at any moment of the time interval for which this set is used (non-

[10] www.scribd.com/doc/44693432/20/Introducere în criptografie

sensitive information about the key which is active on transmission is sent in the connection protocol).

The information received at reception makes possible the use of the appropriate key (active if set of keys is the same in both correspondents, replacement key if in transmission the set of keys has already been changed, or expired if in transmission the set of keys has not been changed in transmission but it has been changed at the reception).

5. Crypton HC 7200 - Equipment for data transmission encryption

It is designed to protect data traffic between a server and its detached peripherals which use for communications public telephone lines and private networks.

The equipment can be mounted in rack or on the desk. The line speed is between 0.6 and 14.4 Kbps.

Key management is performed by using:

- communication keys calculated individually for each work session based on non-sensitive data transmitted to the correspondent with a variety of 10^{38};
- specific connection keys, the variety of 10^{38}.

The device can store a set of specific connection keys (active, replaceable, expired) the standard version or optionally, a number of 128 sets.

The keys can be introduced using:

- the key management center, from where the necessary data can be transmitted using the communication channel to the equipment;
-the electronic card for the distribution and introduction of the key;

. For protection against unauthorized access there were used:

- the password to enter the keys;
- the password to enter the parameters;
- mechanical key lock.

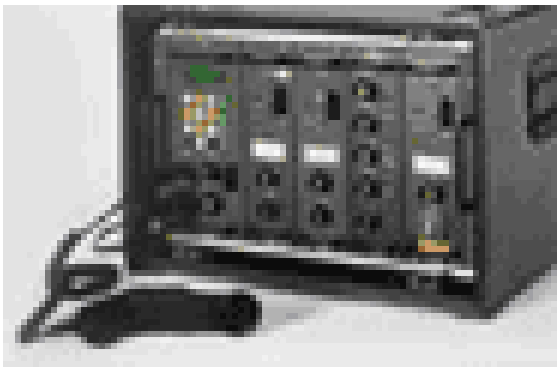
6. OMNISEC 600 - Equipment for data transmission encryption

The device (created by OMNISEC company - Switzerland) is used for all data transmissions done by telephone line, satellite, optical or coaxial cable).

The equipment is connected between the data terminal equipment and data communication equipment.

For the key management there are used two types of keys:

- session keys, which are produced by each device, based on the master keys and a key authentication procedure that involves the transmission of non-sensitive mathematical variables using an unencrypted channel, in a protocol, total diversity of the keys is 10^{76}.
- primary and secondary master keys, keys which have a longer usage time span, bilateral.



OMNISEC 600

The security module allows[11]:

- authentication of the equipment in order to authenticate the session key;
- storing the primary and secondary master keys and the data necessary for the authentication procedure of the session key;
- identification of the equipment for system access;
- total protection of the stored data.

The session key is destroyed immediately after use, causing the information once encrypted, not be decrypted by someone unauthorized who intercepted or captured this information even if they captured an equipment with security module

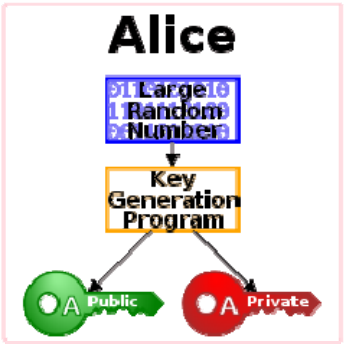
Chapter 2

1. Public key infrastructure

In the electronic data system, a basic attribute, confidentiality, is ensured by encrypting the message with a secret key and a decryption algorithm unique to each message. The recipient can read and understand the message only if they possess the secret key and the decryption algorithm. The central problem of most cryptography applications is to keep the keys secret. PKI (public key cryptography) ensures the secrecy of the encryption keys by replacing the secret key with a pair of keys: one private and one public key.

[11] http://articles.janes.com/articles/Janes-Military-Communications/Omnisec-621-field-wire-encrypter-Switzerland.html

P.K.I. is a platform for software and hardware products, which are provided by specific procedures for confidential communications. The digital certificates (one for each system user) identify and make the connection of the user's digital signature with their public key.



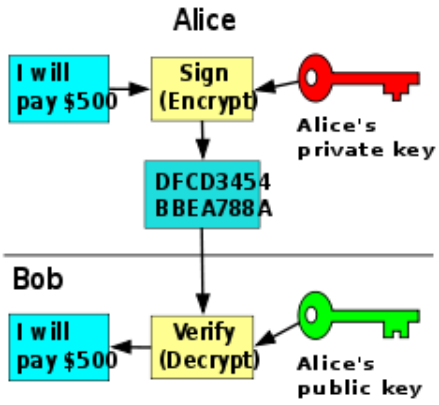
PKI infrastructure, establishes through operational standards the main attributes for the encrypted data flow, between two or more users:

-Keeping the information private - confidentiality;

-Ensuring against possible information fraud - integrity;

-Verifying the identity of the sender - authentication;

-Ensuring the paternity of the message sender - non-repudiation.



The encryption algorithm is done using symmetric keys (using a unique key for encryption and decryption) or asymmetric keys (using different keys).

The encryption can be done with symmetric or asymmetric keys. The first one is done with the same key for encryption and decryption, and the other with different keys.

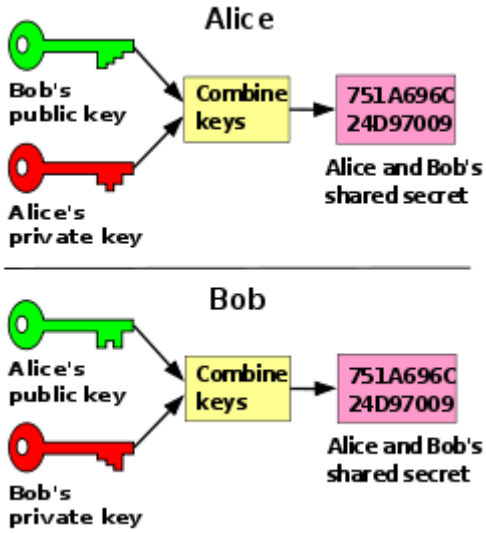
In the case of asymmetric encryption one of the keys (that one used for encryption) can be made public, it can be sent to anybody. The decryption key that is held by the sender, is called private key. The asymmetric keys provide an effective user ID.

The digital signature, is founded on the following example: if a person A encrypts a message with a private key and sends it to a person B, and B can decrypt it using a public key, we can say that B has the certainty that the message comes from A[12].

For the symmetric encryption, the main advantage is the speed, the encryption algorithm being effective for the local files.

The integrity and authentication (basic attributes of PKI), are ensured by the digital signature using the hashing function.

These, perform only the data encryption and the original message will never be recovered (the message has necessarily the same value after applying function being absolutely impossible that any two messages should generate the same value).



2. THE DIGITAL CERTIFICATE

The certification authority (CA - Certification Authority), though the digital certificate, generates a public key which includes the entire user's personal data, which is packaged and signed.

The digital certificate contains:

- the digital signature;
- the information that connects the public key to the user;
- the information to validate the certificate;
- the public key.

Non-repudiation ensures that the sender can not deny later having sent the message.

The digital certificate based on public key infrastructure (PKI), provides the basics of the message integrity: integrity, confidentiality and non - repudiation

[12] A. Salomaa, *Criptografie cu chei publice*, Ed. Militară, 1996

The main components of the PKI platform are:

- Certificate holders (users)
- Customers: validate the digital signature and the certification from a CA.
- Certification authority (CA): generates and revokes certificates
- Registration Authority (RA): checks the public keys and user identities.
- Deposits: store and make available the certificates and Certificates Revocation Lists - (Certificate Revocation Lists CRLs)
- Specific policies to secure the encrypted messages.

Some of the benefits of using PKI:

- Securing the e-mail system;
- Securing the applications from the Intranet and Extranet networks;
- Encrypting data and documents;
- Authentication at the operating system and applications level.

Chapter 3

1. Encryption Management in the Modern Telecommunication Networks

Data encryption management can be defined as the generation, storage, allocation, distribution, use and destruction of the keys and passwords necessary for the specific devices performing encryption of voice and data communications from a network.

The keys protection for an encryption system in a telecommunications network is a fundamental imperative. The keys control the way the message is transformed by encryption algorithms, locking or unlocking the data protection mechanisms.

To prevent the discovery of the keys, they must be issued randomly.

The keys are allocated according to the type of encryption connections made between the encryption equipment and the topology of the subnetworks made within the encryption system.

The key storage is done on devices such as printed lists, punch cards, punch tape, magnetic storage devices (tapes / disks) electronic cards (with EEPROM RAM memory type) etc..

The key distribution is done by mail, courier or other public or private channels, electronic means (the keys are encrypted using a key encryption key, the resulting information being transmitted through connecting channels that are already protected) or they are

presented publicly (public key systems)[13]. The keys usage requires their use in the process of data or keys encryption-decryption.

The key destruction, at the end of the communication for which it has been used, represents a basic principle in cryptography.

In the context presented above, we can define the following types of management:

- *Manual management* - is achieved through key distribution, as printed lists, and it is done through public channels (if the keys are encrypted) or private (high security level), and introducing the auxiliary key in the equipment and it is done using its keypad.
- *Off-line management*, in this case, the key distribution can be done either through: public or private channels and couriers, being used in any physical support of the keys. The keys are entered by direct transfer of information from physical support.
- *Online management* – the key change is done based on the information exchanged between equipments, within a connection protocol, for subscriber encryption equipment, or a management protocol for group encryption equipment which are initialized when they are activated.
- *Electronic key distribution management* - using protected transmission channels from the network.
- *Centralized management* – it is achieved through centralized key generation by a single administrator.
- *Decentralized management* - key generation means in several network nodes, for group encryption equipment (through short links, point to point).

2. Practical Application - The Enigma Emulator

Next we present an application that emulates how a machine with the rotors used for encryption / decryption operates.

The software project presented is a simplified version of Enigma used by the German armed forces. Like the Enigma version used by the German armed forces, the application uses three moving rotors. Each rotor can be rotated manually to set the initial position to start a session of encryption or decryption. The reflector is fixed, it can not be rotated manually, unlike the original version. Also, there is no emulation of the socket panel, for simplicity. "Keys" mappings are 1 to 1, i.e. A → A, B → B, etc.

The application has a stock of five rotors, which have the same mappings as the physical ones, numbered using with Roman numerals I, II, III, IV and V. Also, there is a total

[13] www.scribd.com/doc/44693432/20/Introducere în criptografie

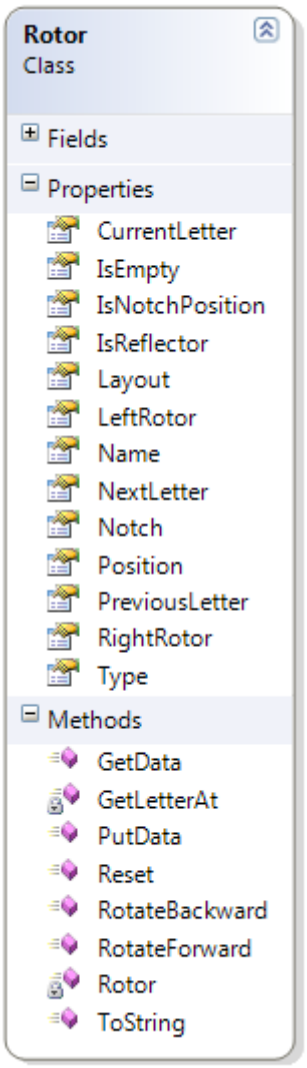
stock of 3 reflectors, physical replicas of the numbered A, B and C. For operation there should be installed: a reflector of your choice (on the left slot) and three rotors to choose from the 5 rotors, for the three slots assigned for the moving rotors.

It should be noted also that there was no adjustment of the ring, also for simplicity. The relative position between the letters and the wiring is fixed.

From there were extracted the rotor wiring tables to be used in application, as follows:

Rotor #	ABCDEFGHIJKLMNOPQRSTUVWXYZ	Notch position
Rotor I	EKMFLGDQVZNTOWYHXUSPAIBRCJ	Q
Rotor II	AJDKSIRUXBLHWTMCQGZNPYFVOE	E
Rotor III	BDFHJLCPRTXVZNYEIWGAKMUSQO	V
Rotor IV	ESOVPZJAYQUIRHXLNFTGKDCMWB	J
Rotor V	VZBRGITYUPSDNHLXAWMJQOFECK	Z
Reflector A	EJMZALYXVBWFCRQUONTSPIKHGD	
Reflector B	YRUHQSLDPXNGOKMIEBFZCWVJAT	
Reflector C	FVPJIAOYEDRZXWGCTKUQSBNMHL	

This table should be read as follows (for example for rotor I in the initial position - A): on the entrance disk appears a signal from key A. Through the wiring of the rotor, the signal is routed to the right from the input disk and goes out to the left through pin E, where it enters in the next wheel. After coming back from the reflector, the signal enters, say, through pin T on the left. This time the route is from left to right, so T is wired to L. From L the electric impulse goes through the entrance wheel and follows the same route that was described in this paper.



The application was done in MS Visual Studio 10 using C # programming language. The core of the application is Rotor class that emulates the mapping configured by wiring.

As shown in the class diagram, a series of properties (attributes in UML language) identifies the rotor by:

• Layout (indicating the cabling configuration),

• LeftRotor, RightRotor (adjacent devices),

• CurrentLetter (the letter seen through the window),

• Notch (notch position to drive the left rotor)

• Position (indicates the offset from the initial position)

Conclusions

Trends and Perspectives In Cryptography

The evolution of data encryption algorithms is a natural consequence of the Internet development and the transformation of the environment in the main communicational infrastructure of mankind.

Classical methods of encryption, based on mathematical modeling of public and private keys patterns, can be neutralized by large computing resources.

As computer systems evolve and the capacity of computing power increases, the vulnerability of the classical encryption systems increases proportionally.

A solution to this constraint is considered the quantum cryptography (QKD – Quantum Key Distribution).

In essence, QKD technology means that when trying to intercept a message, both the transmitter and receiver should be notified of the attempt. In this case the encryption key can be immediately changed by mutual agreement[14].

The specialists who develop the platform say that the information security degree can reach 100%.

The process consists in the production of two polarized photons (by laser), but quantum-correlated, which then are sent to the two users who want to communicate. Along the channel of transmission the photons keep their quantum state, but this is destroyed when the transmitter measures the photon it receives. This way it can measure either of the two possible photon polarizations of the received photon and which represents classical bits 1 and 0.

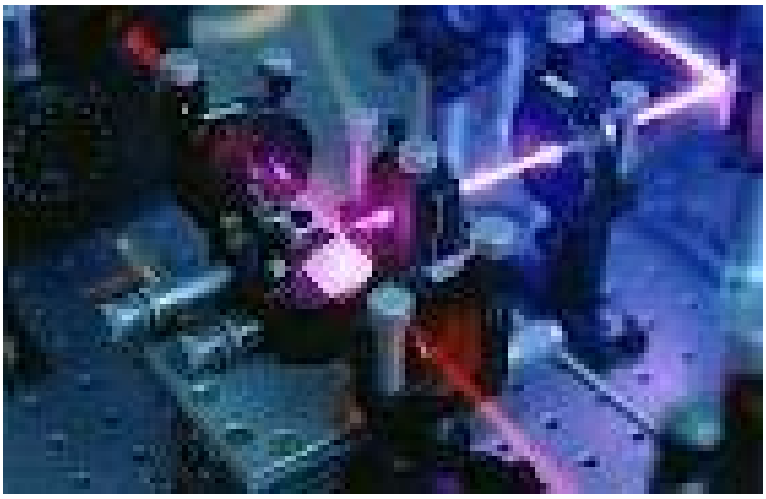
Taking into account the correlation of the two photons, the second will be assigned the opposite polarization (1 or 0) to that measured at the "sender".

The transmitter, by measuring the polarization state of the first photon, knows with certainty that the receiver measured the opposite polarization because the photons are correlated.

For example, if the sender wishes to send the number 1, there must be done a set of measurements, and then wait until it measures 0 (at that moment the receiver will be measured but then, they write down the time when they measured, time that is sent to the receiver in a document (a classical transmission channel). When reading the document, the

[14] http://www.securitatea-informatica.ro/securitatea-informatica/securitatea-datelor/criptarea-cuantica-istorie-abordari-si-perspective/

receiver sees the time of the measurement which represents the bit that the transmitter wanted to send, they look to see what was measured then and finds the correct bit.



Transmission on channel - laser

This concept appeared in the 1950s, once physicists began to question the foundations of quantum physics. The concept remained on stand by until the 1980s', when the first lasers and the special nonlinear crystals allowed these measurements. It is obvious that once the advantage of securing the communication networks became a certainty, many companies began to invest money in this technology, which led to an even faster progress QKD platform.

What could the science of cryptography offer for the future? Perhaps the biggest dream of cryptology: an algorithm for the encryption of messages that can not be decoded.

References

1.Constantin Popescu, *Introducere in criptografie*, Ed. Universitatii din Oradea,2011.

2. http://ro.wikipedia.org/wiki/Criptografie

3. http://webhost.uoradea.ro/cpopescu/cryptography/Cursul1.pdf

4. http://www.apprendre-enigne.net/crypto/bibliotheque/PDF/KruhDeavours.pdf

5. www.tccsecure.com/.../DSP9000-detail-HS

6. www.cryptomuseum.com/.../hc3300/index

7. www.scribd.com/doc/44693432/20/Introducere în criptografie

8. http://articles.janes.com/articles/Janes-Military-Communications/Omnisec-621-field-wire-encrypter-Switzerland.html

9. A. Salomaa, *Criptografie cu chei publice*, Ed. Militară, 1996

10. http://www.securitatea-informatica.ro/securitatea-informatica/securitatea-datelor/criptarea-cuantica-istorie-abordari-si-perspective/