**POLITEHNICA UNIVERSITY OF BUCHAREST**

**Doctoral School of Electronics, Telecommunications and Information Technology**

**Decision no. 708 from 16.07.2021**

# PhD THESIS

## - summary -

**Eng. Eugen NEACȘU**

---

# PROTECȚIA INTEGRATĂ A SISTEMELOR INFORMATICE CRITICE

# INTEGRATED PROTECTION OF CRITICAL INFORMATION SYSTEMS

---

**DOCTORAL COMMISSION**

| | |
|---|---|
| **Prof. Eng. Gheorghe BREZEANU, PhD.**<br>Politehnica University of Bucharest | Chairman |
| **Prof. Eng. Paul ȘCHIOPU, PhD.**<br>Politehnica University of Bucharest | PhD supervisor |
| **Prof. Eng. Adrian TULBURE, PhD.**<br>1 Dec. 1918 University of Alba Iulia | Reviewer |
| **Prof. Eng. Ioan BACIVAROV, PhD.**<br>Politehnica University of Bucharest | Reviewer |
| **CSI. Eng. Victor VLĂDĂREANU, PhD.**<br>Institute of Solid Mechanics of the Romanian Academy | Reviewer |

**BUCHAREST 2021**

# Content

# Chapter 1

# Introduction

Creating a robust integrated security system requires rigorous adherence to a solid digital protection process. Only when digital, physical and cyber security work together, an IT system can be considered truly secure. In this context, the first chapter presents an introduction in the field of PhD thesis, highlighting the opportunity of the chosen sector on the protection of critical information systems. The chapter continues with the details of the objectives of the paper, being synthesized with the presentation of the afferent structure.

## 1.1 Presentation of PhD thesis field

The demand for cost-effectiveness and modern system architectures has made system owners turn to interconnected technologies. These technologies give asset owners access to open architectures and enhanced communications technologies that were not previously available. The benefits were immediate and significant, with improved efficiency, operation and analysis, available to help the beneficiary ensure that its infrastructure operated in accordance with security requirements. Of course, with these connection opportunities came increased exposure to risk, attack scenarios and exploitation from external sources.

## 1.2 The purpose of PhD thesis

This paper reveals an incursion of critical IT systems security methods, presenting information flow protection techniques, systems security management methods and an integrated solution for information systems protection.

## 1.3 The content of PhD thesis

The PhD thesis consists of 6 chapters, 8 annexes, the list of tables, the list of figures and the list of abbreviations used. The paper closes with the exposition of the bibliographical references used in the body of the thesis.

Chapter 1 represents the introductory part of the PhD thesis, which sets out the concept of critical information system, the dynamics of current technologies and the major objectives needed to be implemented to ensure increased security of the systems. The chapter continues with the presentation of the main objectives of the thesis and with the exposition of its content.

Chapter 2 clarifies further the concept of information system, presenting the main security foundations that underlie it. At the same time, this chapter presents the most important threats to critical computer systems, types of cyber attacks, both hardware and software, focusing on new technological trends and also preventive measures that can reduce possible damage to the level of managed systems. As an original contribution, I've performed a security analysis on phishing attacks, showing the main technical flaws of the protocols used, methods to improve the usefulness of the service but also solutions to reduce the difficulty of implementing anti-spoofing protocols. Extensive efforts are needed to improve user interfaces for email systems in order to allow users to proactively verify authentication results.

Chapter 3 examines the main methods of securing communications, focusing on those protocols needed to encrypt data traffic. At the same time, efficient solutions were pointed out to improve the utility and reduce the difficulty of implementing the SIP, RTP and IPsec security protocols. Another original contribution, presented at the end of the chapter, is the realization, implementation and development of a VoIP network using the PKI infrastructure, which led to new practical network configuration measures to eliminate potential attacks on the system.

Chapter 4 integrates the main methods of information management of computer systems. The chapter presents, both theoretical and practical aspects of approaching security in a coordinated way. The original contribution is given by the creation of a centralized security model for critical infrastructures, by developing a security plan for a Data Center, with the role of critical infrastructure, in which are concentrated vital tools that ensure the integrity of the services provided.

Chapter 5 presents an optimal solution for managing security at the level of a critical computer system, by developing a standard model for securing access to a database, traffic between used applications and the database and the integrity of private information storage - Integrated Security System (ISS). By setting up this system, I've managed to implement a model of analysis and centralized detection of the main IT events within a critical infrastructure. Custom operating system security policies have also been created to protect data against extended vulnerabilities. An analysis and evaluation of the data flow concluded the formation of a stable security pattern that originally contributes to the limitation of computer events, as well as to the reduction of possible damages.

Chapter 6 is dedicated to the main contributions on the integrated protection of critical information systems, focusing consistently on the security model created, namely, the Integrated Security System. This IT concept represents a step forward in the development of critical infrastructure protection and can be easily modified to allow a quick way to query multiple managed systems. At the same time, the chapter presents the main ideas that formed the basis of this complex scientific research, highlights the original contributions and ends by expressing the directions of further development of the author.

# Chapter 2

# Theoretical landmarks regarding critical information systems

The second chapter focuses on the basic notions of critical information systems, highlighting the fundamentals of security that underlie the development of technological infrastructure. Also, the main types of computer attacks on systems are presented, which are summarised in a case study on new trends in the use of authentication tools for phishing attacks.

## 2.1 The role of information systems

Critical infrastructures, which contain interconnected information systems, are infrastructures with a decisional purpose in protecting the functioning of the systems, but also in the development of information processes. As a rule, these infrastructures on which process safety and stability depend can be included in the special CI category. It is not necessary for any infrastructure that is or may become, at some point, critical, to fall into the same category [4].

## 2.2 Security fundamentals

Security policies are the result of the need to integrate a critical IT system in the new technical, economic and socio-human contexts. By approaching a security policy, decision-makers put into practice the concepts and notions articulated in a unitary way. At the same time, by designing integrated policies, the appropriate protection of the information circulated within the organization is ensured in order not to alter the transmitted data or to illegally access the developed technologies. This concept includes securing the staff, IT and communications networks, storage media and all the spaces in which the organization operates [6].

## 2.3 Cyber attacks

The frequency and extent of cyber attacks continue to increase, and yet, despite the severity of the problem, it remains extremely difficult to differentiate the sources of an attack. Cyber attacks by a number of entities pose a growing threat to the security of states and their citizens.

### 2.3.1 Threat categories

There are three main sources of threats: activists, cybercriminals and state entities, and - based on the evidence - it is sometimes difficult to differentiate them. Indeed, sometimes they can work together when their interests are aligned. Increasing the frequency and severity of attacks makes understanding the source more important than ever. Knowing who planned an attack could make it easier to catch the perpetrators or frame an appropriate response. In addition, there is a risk that a cyber attack will be misjudged or confused with a government attack and trigger a larger cyber or physical war. Alternatively, a government-sponsored hack can be disguised as a case of cyberactivism or cybercrime to avoid a government-to-government response [11].

### 2.3.2 Types of cyber attacks

Security risks are like viruses, and cyber security is the medicine. Both come in different forms. To eliminate security risks, we need to implement the right technology. In other words, we need to know the different types of cyber attacks to come up with the best way to handle them.

The following cyber security threats are the most common types of attacks on computer systems [13]:

a) phishing attack - phishing is a type of fraud in which fake websites, fake emails and text messages are sent through the intrusion of a legal source, such as a bank. Such emails are often sent to obtain the user's password and credit card details. In this form of activity, the user is often asked to update or approve their accounts in order to obtain their personal information. Facebook has become a launching pad for phishing attacks. Infected accounts sent malware links to others via Messenger. We can avoid phishing like this: we do not open unwanted attachments, we do not access unknown links received by e-mail. It is recommended to open the link manually in the browser. We also need to check headers before opening an email from an acquaintance;

b) ransomware attack - ransomware is a form of malware, which, after restricting access to files and computers, forces users to make payment to remove the restrictions. Phishing emails are common examples of ransomware injections. It is basically of two types: ransomware with encryption and ransomware with lock screen. Encrypted ransomware prevents the user from accessing a file on the computer's hard drive by encrypting them, while lock screen ransomware prevents access to the computer by image methods. To gain access to your computer, the ransomware will display a notification or warning on your computer that it has been blocked and ask you to pay to unlock it. We can prevent such attacks by backing up often. It is recommended never to pay the ransom and it is necessary to notify the competent institutions;

c) brute force attack - in this method the hacker uses all possible key combinations to decrypt the encrypted text and convert it into plain text to decipher the

message that is transmitted. This method is becoming increasingly difficult to use with modern cryptographic systems, as the amount of time, money, resources and energy that would be required to crack the code would not normally justify the efforts made in this regard. Sometimes the attacker takes several different pieces of encrypted text that were generated by the same cryptographic system to analyze them for a common pattern that could lead to a clue to breaking them. Even this technique is very difficult with modern computer systems that are designed in such a way as to avoid any attempts at statistical analysis. A similar technique is used in combination with brute force and is known as a meet-in-the-middle attack;

d) Man in the Middle attack - when we assume that we are sending data to a single site, but in reality they are redirected to other sources, this condition is known as Man in the Middle attacks (Man in the Middle). It usually occurs due to inactive malware that has been present on the system for some time. It will seem that we are entering the data into a suitable network, but in reality this is not the case. We can protect ourselves by running updated antivirus programs on all devices, including phones;
e) fragmentation attack - is used as a method of obtaining packets around a packet filtering firewall. In a basic fragmentation attack, the packets are divided into fragments, the first packet containing the complete header data. The remaining packages do not contain header information. Because some routers filter packets based on this header information, packets left without header data are not filtered and go through the firewall.

**Case study: Security analysis of phishing attacks.**

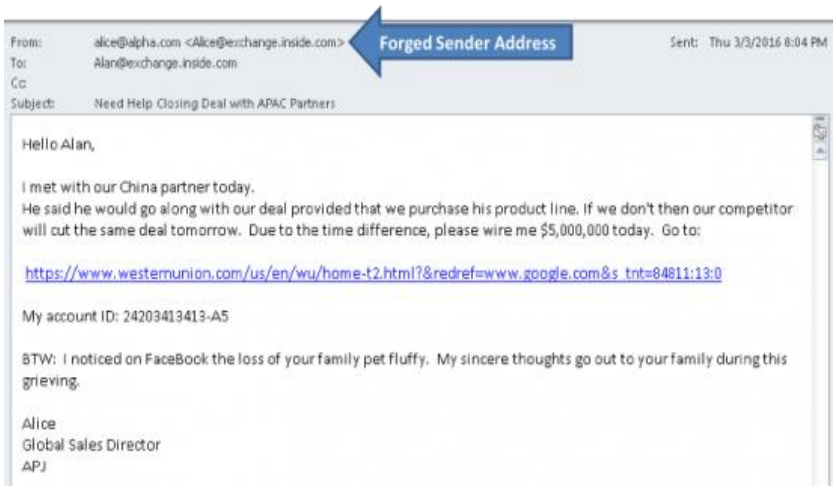


***Figure 2.8*** *Spoofing e-mail [15]*

To perform a phishing attack, attackers can manipulate two key fields to send emails. First, after establishing an SMTP connection to the target mail server, the attacker can use the MAIL FROM command and can set the sender's address to anyone who wants to identify him. After that, the MAIL FROM address is inserted in the header as *Return-Path*. In addition, attackers can change another field called *From* in the email

header. This *From* field specifies the address that will be displayed on the email interface. When a user receives the email, the user will see the address *From* (for example: alice@alpha.com in Figure 2.8). If the user replies to the email, the reply message will go to the *Return-Path* set by MAIL FROM. Keep in mind that the two addresses are not necessarily the same. Email spoofing is a critical step in phishing attacks to gain the victim's trust. Meanwhile, forgery is also a strong signal of attacks. Fake detection results are often used by phishing detection systems [16].

In order to detect and prevent the falsification of e-mails, SMTP extension protocols are proposed: SPF, DKIM and DMARC. All three protocols have been published or standardized by the Internet Engineering Task Force (IETF).

**Technical flaws of the protocols:** first, SPF and DKIM both face the identifier alignment problem. This means that the sender's email address that a user sees may be different from the address actually used for authentication. For SPF, authentication focuses on *Return-Path* and examines whether the sender's IP address is listed in the SPF record of the *Return-Path* domain. An attacker can set the *Return-Path* domain to its own domain and can set the SPF record to pass authentication. However, what the receiving user sees on the e-mail interface is set by the *From* field. DKIM has a similar problem, given that the domain for signing the email with the DKIM key may be different from the domain on the *Return Path*. DMARC helps solve the problem by applying identifier alignment. Second, email forwarding is a problem for SPF. E-mail forwarding means that an e-mail service automatically forwards e-mails to another service. A common scenario is that users often set up their email service to forward all emails to Outlook or Gmail. During email forwarding, email metadata (for example, Return-Path) remains unchanged. SPF will fail after email forwarding because the sender's IP address will not match the original sender's SPF record. Thirdly, mailing lists are a major problem for both SPF and DKIM. When a message is sent to a mailing list, it will forward the message to all subscribers. This is a process similar to forwarding emails. During this process, the IP address of the mailing list will become the IP address of the sender, which is different from the IP address of the original sender. This will lead to SPF failure. Mailing lists will cause DKIM problems, as most mailing lists change the content of the email before sending it to subscribers. The usual change is to add a footer with the name of the mailing list and a link to unsubscribe. Tempering the e-mail content will cause DKIM to fail. DMARC helps solve some of the problems, but not the mailing list problem. For mailing lists, DMARC+SPF will fail for sure - if *Return-Path* is changed, DMARC will fail due to misalignment of identifiers; if *Return-Path* is unchanged, SPF will fail due to IP mismatch. For DMARC+DKIM, it will fail if the mailing list needs to change the content of the email.

### 2.3.3 Preventive measures

Given the range of security elements, we can limit ourselves to 5 objectives that we must implement in order to provide a high level of security at the level of critical information systems:

1. security assessment - it is vital to assess security standards. Hardware and software should be constantly updated to withstand the latest cyber attacks. In addition, it is essential to prioritize server security;
2. centralized control - in any computer system, there are a variety of devices, software and network configurations involved. As such, it is crucial to have a configuration that allows control of all interconnected databases and centralized management in any cybersecurity platform;
3. maintaining security standards - conducting an analysis program to detect unusual activities. This is an effective way to resolve security issues. Each time the system is used, this program must become active. If the system is used from an unknown location, the program may block access and save relevant information. In addition, this program is able to detect any kind of malicious program installation;
4. staff training - hackers often gain access through mobile applications, emails, corrupt links, etc. Most employees are unaware of these dangers, giving hackers access to sensitive information. It is important that staff be trained against these types of vulnerabilities, through specialized courses in the field of INFOSEC, as well as their own procedures for using the systems;
5. compliance with relevant legislation - in order to be aware of the need for security and to ensure that we take appropriate security measures, certain regulatory laws must be applied. For example, the European Union has the GDPR (General Data Protection Regulation) to require companies to comply with security procedures. Failure to comply with these policies will lead to massive fines, thus ensuring that organizations remain safe from potential threats.

## 2.4 Contributions

Network security revolves around the three key principles of confidentiality, integrity and availability. Depending on the application and context, one of these principles may be more important than the others.

The analysis of the concept of information system, section 2.1, involved the detailing of the components, indicators that reflect the security status of the organization, identification elements and criteria underlying the performance of critical information systems.

In section 2.2 I've highlighted the process of implementing the security policies necessary to secure the managed infrastructures, focusing on the two approaches presented: the functional approach and the structural approach of the IT system. Next,

I've defined and exemplified the component elements of IS: the information base, the technical base, the programming system, the scientific and methodological basis, the human resource, the organizational framework. Although the literature does not provide sufficient details on IS interdependencies, I have presented three main issues, managing to identify most approaches to an entire system of interdependent critical infrastructures that interact with each other.

In section 2.3, after the extensive presentation of the main cyber attacks on computer systems, I've made an original contribution by conducting a case study on the security analysis of phishing attacks, resulting in the following aspects:

- ✓ first of all, there is a new perspective on the perceived values and concerns of anti-spoofing protocols from the perspective of e-mail providers. These results show the reasons behind the slow adoption of SPF, DKIM and DMARC, highlighting the main directions of optimization;
- ✓ second, the key implication of the results for protocol designers, e-mail providers and users is presented. We discuss possible user-end solutions to compensate for possible server authentication.

The final part of the chapter presents the main countermeasures we need to implement in order to provide a high level of security at the level of critical information systems.

# Chapter 3

# Protection of critical information systems

The third chapter presents a foray into the security of information systems, presenting the main communication security protocols, methods of implementation and the current needs of large-scale communication systems. At the end of the chapter, the operability of a critical IT system is simulated, through the practical realization of a VoIP network, offering an optimization of the implementation of security policies at the level of communication networks in order to protect confidential data.

## 3.1 General considerations

Currently, the most effective methods of maintaining the integrity and confidentiality of information are given by cryptographic techniques. This paper makes a foray into these information security techniques and proposes solutions, both to the cryptographic community and to specialists in the administration and security of information systems.

Public key infrastructure (PKI) is a general term for everything that is used to establish and manage public key encryption, one of the most common forms of encryption on the Internet. It is included in every web browser used today to provide public traffic, but organizations can also implement it to ensure internal communications and access to connected devices. The most crucial concept involved in PKI is, as its name suggests, the public cryptographic keys that are at its core. These keys are not only part of the encryption process, but help to authenticate the identity of the communicating parties or devices.

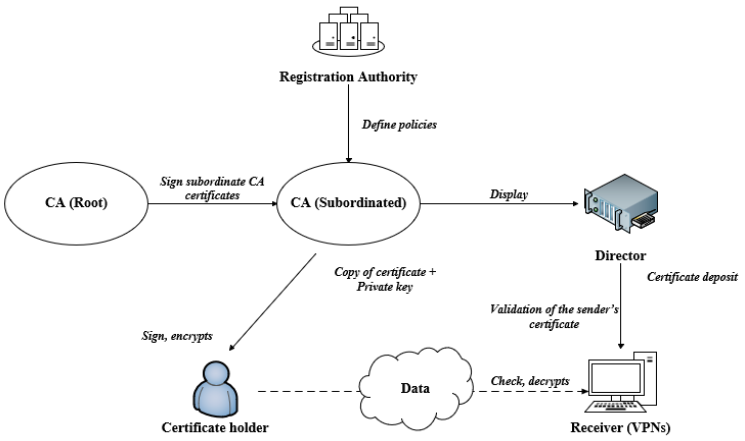


***Figure 3.6** PKI structure [6]*

PKI certificates are documents that act as digital passports, assigned to any entity wishing to participate in a secure PKI conversation. It can include quite a lot of data. One of the most important information that a certificate includes is the public key of the entity. The certificate is the mechanism by which the key is distributed. But there is also the authentication piece. A certificate includes an attestation from a trusted source that the entity claims to be. This trusted source is generally known as the certification authority (CA). PKI is great for securing messaging for the same reason it is great for securing web traffic: data circulating on the public Internet can be easily intercepted and read if not encrypted, and it can be difficult to trust that the sender is who they claim to be if there is no way to authenticate your identity.

## 3.2 Communication security techniques

### 3.2.1 SIP security

The SIP (Session Initiation Protocol) is a protocol developed for the purpose of establishing, modifying and terminating a multimedia session over the Internet, with message delivery capabilities. From the user's point of view, the main advantage of the SIP protocol is the provision of an addressing mode whose format does not require storing IP addresses, the ability to register on a server and to make calls using the same ID from different PCs, or the ability to send calls to others. The signaling protocol functions as a central standard for a communications model and names a VoIP architecture that encompasses different types of communicating entities and their behavior [38].

### 3.2.2 RTP security

RTP is the protocol that provides delivery services for data based on the real-time feature (interactive audio and video messages). RTP uses the UDP protocol. Although it does not ensure the quality of services in IP networks, it does provide the means to detect important events in the context of multimedia broadcasts such as: packet loss, packet arrivals and variable packet delivery delays. The protocol does not correct these problems, leaving them to higher level protocols such as codec or VoIP application [48].

### 3.2.3 IPsec security

IPsec security is based on encryption/authentication algorithms and mathematical functions, in order to ensure the integrity, confidentiality and non-repudiation of the information contained in each IP packet that is sent over the network. IPsec functionality is based on the cryptographic properties of famous algorithms (such as: Diffie-Hellman, RSA, DES, AES). Currently, IPsec is one of the most widely used

technologies used in encrypting Internet transmission. Compared to SSL (Secure Sockets Layer) and TLS (Transport Layer Security), IPsec is at level III of TCP/IP and ISO-OSI stacks, making it possible to secure applications that use this stack [66].

## 3.3 Implementing a VoIP network

To illustrate the large-scale VoIP communications network, I've chosen the Cisco Packet Tracer platform (version 7.1.1). The implementation of this solution requires low resources due to the practical architecture of the platform used. For starters, we will add the following components on the platform: 1 router 2811, 2 PC units, 2 IP Phone and 1 switch 2960 [74].

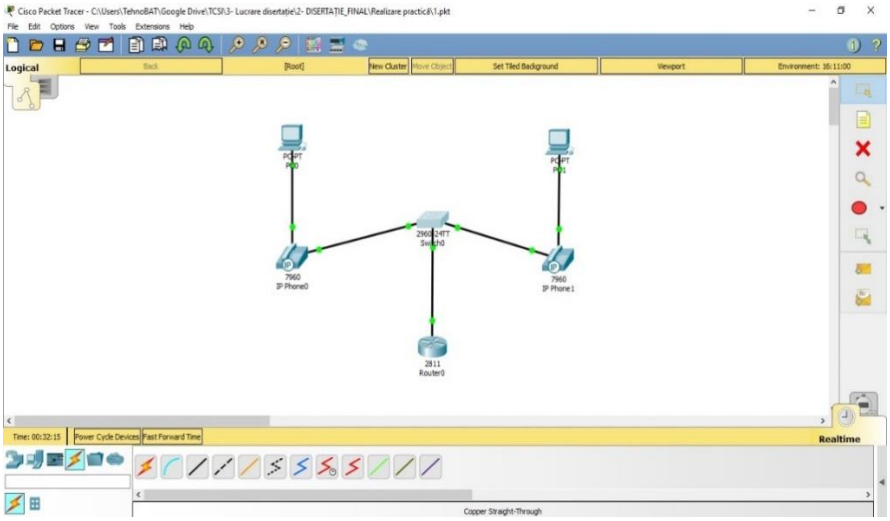

***Figure 3.32*** *Network interconnection*

To demonstrate the functionality of the network we will call from IP Phone 1 (93001) the corresponding number IP Phone 2 (93002).

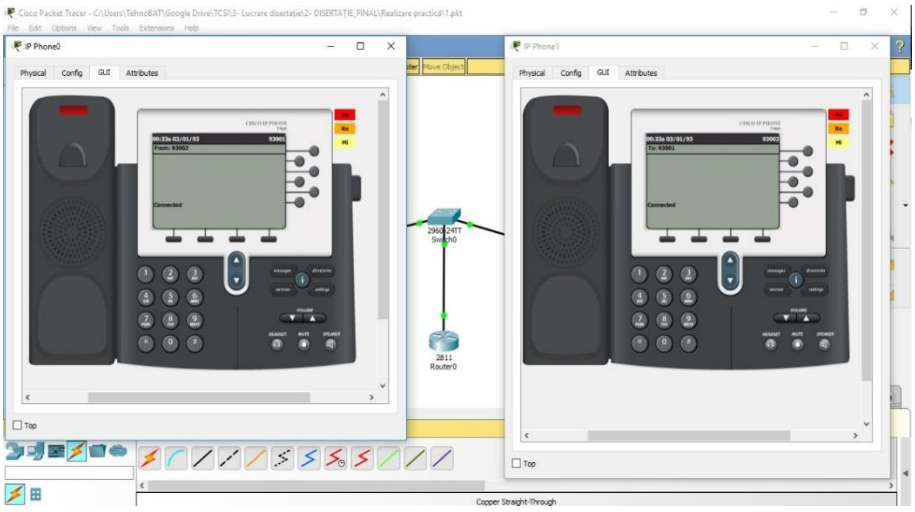

***Figure 3.34*** *VoIP connection*

From figure 3.34 it can be seen that the VoIP network created is functional, and the connection between the two IP Phones is successful.

If the VoIP traffic has no security method, it is very easy for an attacker to intercept the network traffic, it can even reconstruct the entire call. For this reason, it is useful to protect the network as much as possible and to pay attention to the vulnerabilities that exist at the level of communication systems.

**Case study: VoIP network security analysis.**
The attack on VoIP traffic does not differ from that on a regular network, instead the connection to a VoIP network differs from that on a regular network. While mail servers, DHCP, DNS are accessible through certain VLANs, VoIP networks are in separate VLANs. Attackers who are not connected to the correct network segment will not be able to initiate the attack. Separation of services into VLANs is an important measure to prevent attacks. A VLAN can be used for many purposes, including security, QoS, segmentation, priority levels. VoIP packets should have a higher priority over packet data as people using VoIP phones should not be bothered about the audio quality of the data transfer process initiated by someone else.

# 3.4 Contributions

Chapter 3 presents a detailed analysis of the main methods of protection of information systems, starting from the key element (information) to the encryption of large-scale communications, addressing the related security issues.

Section 3.1 presents key communications considerations, being complementary to the protection of information systems, addressing key technological attributes of public key infrastructure (PKI). It offers the possibility to meet the minimum security requirements by generating certificates, verifying the construction generated by public keys, validating electronic signatures, storing and accessing CRLs, but also defining group policies in accordance with the principles of using cryptography. At the same time, the PKI infrastructure is essential for the implementation of cryptography in applications that require secure communication sessions. The main benefits are found in: the possibility of protecting INTRANET/EXTRANET applications (the risk being reduced by the use of security protocols), ensuring the integrity of data transmitted over the network using strong cryptographic algorithms (AES, RSA, etc.), authentication at the operating system level, but also the secure storage of the associated keys. An original contribution in this subchapter is represented by the comparative analysis of the algorithms with public key/private key, highlighting the advantages and the characteristics specific to each one.

Section 3.2 discusses the main communication security techniques, using the SIP, RTP and IPsec protocols. The SIP protocol has the advantage of procuring an addressing mode that does not require the maintenance of IP addresses, the same ID being used for registration on the server and for making calls. RTP provides a way to detect major events in multimedia data transmissions (packet loss/arrival/delay), using

delivery services for information that is based on the real-time feature (audio, video). IPsec is a security method spread in LAN (client-server) environments, based on encryption algorithms and mathematical functions, its use ensuring the main security mechanisms (ESP, AH, IKE). Another original contribution is the analysis of the data packets related to each protocol, providing vital information about security vulnerabilities in their use.

The main contribution in this chapter was the implementation and encryption of VoIP and videoconferencing connections using the PKI infrastructure, also performing a security analysis of the main vulnerabilities, resulting in the following (section 3.3):

- ✓ flexibility in implementation. In this way, the maintenance of a complex infrastructure of VPN tunnels is avoided, in the conditions in which there is a PKI infrastructure that provides the certificates and keys;
- ✓ the problems posed by the IPsec protocol in the case of a NAT infrastructure, are avoided;
- ✓ the additional loading of data packets due to the added headers when using SRTP is considerably lower than IPsec, offering an advantage in case of low bandwidth connections;
- ✓ the transmission of the media stream (voice and video) in the case of SRTP is done through the UDP protocol, which is a protocol without confirmation. It is less susceptible to delays than the TCP protocol in the case of IPsec. Restoring the call in case of lost packets falls to the codecs used;
- ✓ the adoption of the PKI infrastructure in order to implement the TLS protocol is absolutely necessary to protect the connection, which offers the advantage that critical information that may affect the security of communications transmitted over SRTP is inaccessible to potential interceptions.

# Chapter 4

# Information security management

Information security management is a proactive measure that allows companies to accurately identify and immediately strengthen the defense, thus being one step ahead of cybercriminals. The chapter presents both theoretical and practical aspects of security management at the level of a critical infrastructure, a security plan of a Data Center being developed, that highlights a coordinated approach to information systems security that integrates all available resources to ensure critical infrastructure protection.

## 4.1 Centralized security administration

A centralized model would seem like the right choice. By directing and managing security within a central body, better oversight of possible security breaches is provided. Centralized management is generally the most efficient, as resources can be managed cost-effectively across infrastructure, thus limiting duplication of effort and making better use of human resources and IT tools. There is also some sustainability, because in the event of an incident, it can be treated in a uniform way as soon as possible.

## 4.2 Security plan

The security plan helps to identify the existing security solutions or those that are implemented for the protection of critical infrastructure elements. All data in this plan is fictitious, without containing sensitive information. A critical infrastructure (Data Center) called DATANET SYSTEMS [79] will be chosen.

### 4.2.1 Organizational description

The DATANET SYSTEM Data Center has a number of 50 employees (security staff: 25, administrative staff: 5, security staff: 15, management staff: 5).

### 4.2.2 Security environment analysis

The security risk analysis is based on the threat scenarios, the identification of the vulnerable points of each element of the CD and its impact in case of an unwanted event (in case of exploitation of a vulnerability by a threat).

### 4.2.3 OSP management

The services within the INFOSEC Department with responsibilities in the field of critical infrastructure security are directly subordinated to the director.

### 4.2.4 Risk management

Risk prevention, control and mitigation measures derive from the risk assessment performed. Identify, select and prioritize countermeasures and procedures, distinguishing between permanent measures - permanent security measures (of a technical nature), which identify the necessary security investments and non-permanent security measures (of an organizational nature), which they can be activated gradually according to the different levels of risks and threats identified [79].

### 4.2.5 Alert levels

Alert levels are set for the implementation of security measures at the time of an event with an impact on the DC. Preventive measures are taken to maintain an acceptable level of DC security, as well as to allow the continued provision of specific services. The dissemination of the information regarding the alert level is done hierarchically, according to the organizational chart of the Center, through the normal means of communication [79].

## 4.3 Contributions

The complexity of threats to critical IT systems - part of national infrastructures, increasingly interconnected, make it necessary to establish and function the security conditions of managed systems. The integrated protection of critical infrastructures on the national territory starts from the principle of confidentiality, which implies the reduction of security vulnerabilities through the flexibility of adaptation to national interests; it is also essential for the protection of citizens, the security of the services provided, but also for the territorial integrity of Romania.

In this context, the chapter begins with section 4.1 which plays a key role in the good governance of a critical infrastructure, namely security management. It is

absolutely necessary for this administration to be centralized because, by providing all events at the NOC level, you can get a much shorter response time for responding to security events/incidents. At the same time, the results of the events within the organization must be well known within the INFOSEC department that manages everything related to systems, being beneficial to develop a rapid reaction procedure for each known type of attack. The most difficult situations to eliminate possible sources of risk is the human resource, because it can be lured in order to penetrate from inside the communication rooms that have stand-alone information systems and contain the main credentials necessary for the management of the entire critical infrastructure. Staff must be trained, specialized and regularly checked.

The following sections (4.2.1÷4.2.5) provides original contributions by creating a complete security mode (physical, personal, procedural protection, INFOSEC), starting from the establishment of a functional organization of a critical infrastructure, to the realization of security management. Potential threats can materialize in a very wide spectrum, such as proliferation, international terrorism, the spread of organized crime or pandemics (COVID-19). In addition, globalization is putting even more pressure on existing threats with direct consequences exacerbated by energy demand, climate change, urbanization, the current economic crisis, and population growth and its socio-economic consequences. All of these potential threats pose a security risk to our critical infrastructure, which is vulnerable to the effects of an attack. Cyber resilience also illustrates the importance of interfaces and database connections. The importance of interaction and dependencies is obvious: they are essential elements for assessing the sensitivity of the system as a whole. Not only are the different sectors or subsectors critical, but their mutual dependence is crucial for scenarios where cascading effects will prevail. Research is underway in this area for all possible attack scenarios.

The fast exchange of information on potential threats and vulnerabilities plays a crucial role. As such, a specific network has become necessary: CIWIN (Critical Infrastructure Warning Information Network). This network fulfills two functions: it is the first and most important electronic forum for the exchange of information related to CIP (Critical Infrastructure Protection); moreover, it serves as a rapid alert functionality between Member States to inform the responsible authorities about common risks and threats. All Member States have signed a memorandum of understanding to contribute to operational network participation. The way in which this information needs to be provided is still under development. If we are talking about European critical infrastructures, they are designated according to the greatest importance for the community and which, if disturbed or destroyed, would cause dysfunctions in several Member States. This includes cross-border effects resulting from the interdependencies between interconnected infrastructures in different sectors.

The main contribution of this chapter is the realization of a complete security plan of a Data Center operator (analysis of security environments, centralized security management, risk analysis of critical IT systems, risk management). Practically, this tool represents the integration of all security policies presented at the level of a critical infrastructure consisting of a Data Center with critical information systems in management, risk data, threats and vulnerabilities of the infrastructure, measures to

prevent security incidents, but also an alert system on priority levels. The security plan was implemented through the methodological guidance of organizations with critical infrastructure.

# Chapter 5

# Contributions regarding the implementation of an Integrated Security System

An Integrated Security System (ISS) is designed in this chapter to secure databases. Information is a valuable entity that must be treated and managed firmly, as in the case of any economic resource. Therefore, some or all of the data may be of tactical importance to that organization and must therefore be kept protected and confidential. The documentation produced is the result of the entire study on the protection of critical information systems.

## 5.1 Defining security objectives and requirements

Database audit is the activity of monitoring and recording configuration actions from database users and nondatabase users, to ensure the security of databases. There are five main objectives for developing an audit trail:

1) standard audit of applications;
2) audit trail at application level;
3) auditing database events;
4) audit of the database trigger;
5) external audit.

## 5.2 Integrated Security System (ISS)

In order to effectively protect stored information, security management requires appropriate controls, which are distinct in a mission, as well as a specific purpose for the system. **ISS** combines multi-level security systems and integrates them into a single solution. The requirement for adequate protection, although often neglected or overlooked, is now increasingly pressing.

### 5.2.1 Implementation stage

**ISS** contains several available mechanisms that must exist when securing databases:

- ✓ timely writing of sensitive data in the results of the SQL query, before displaying the application, so that unauthorized users can not view sensitive

data. Allows consistent writing of database columns between application modules that access the same information about the database. Data editing minimizes application changes because it does not change the actual data in internal database storage and retains the original data type and formatting when the transformed data is returned to the application. Writing information has no impact on the operational activities of the database, such as backup and restore, updating and correction, as well as on high-availability clusters;

- ✓ data masking covers sensitive data by replacing it with other data - usually characters that will meet the requirements of a system designed to test or continue working with masked results. Masking ensures that vital parts of personally identifiable information (PII) - such as the first six digits of a personal numeric code - are hidden or otherwise misidentified;
- ✓ data encryption is achieved by converting and transforming data into encrypted text, using mathematical calculations and illegible algorithms. Restoring the message requires a proper decryption algorithm and the original encryption key.

**ISS** is a standard model for hardening (securing) access to a database, traffic between the application and the database, and storing information in a database. At the same time, by integrating this system, a model of centralized analysis and detection of this setup is implemented, which can be considered a standard in a Data Center. Centralized detection can be performed using APEX technology for PL/SQL development that allows a quick and easy way to query multiple databases managed simultaneously. The standard setup also includes an area within the database, for encrypted data storage, which will be easily demonstrated by analyzing the files that host the data. This feature is useful for those organizations that have multiple critical information systems.

**Database traffic encryption.** Oracle supports network-level encryption through both Secure Sockets Layer (SSL), using X.509v3 signed certificates, and native encryption without certificates. The solution with network-level encryption is not only that sensitive data in transit is protected when encryption is used, but also that the SID is protected. Without encryption, SID can be easily listed by Man-in-the-middle attacks.

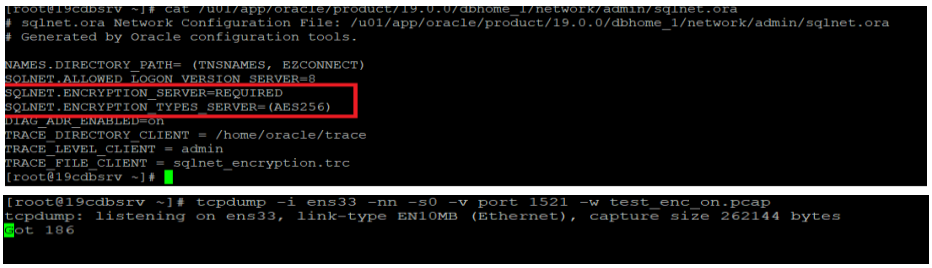


***Figure 5.15*** *Package collection on the network board*

**Data integrity.** Advanced integrity functionality for data security is separate from network encryption. The configuration is similar to network encryption, using the following parameters in the server and/or client *sqlnet.ora* files:

We check the encryption keys:

```
SQL> col KEY_ID format a55
col ACTIVATING_PDBNAME format a15
select KEY_ID,ACTIVATING_PDBNAME,ACTIVATION_TIME from v$encryption_keys;
```

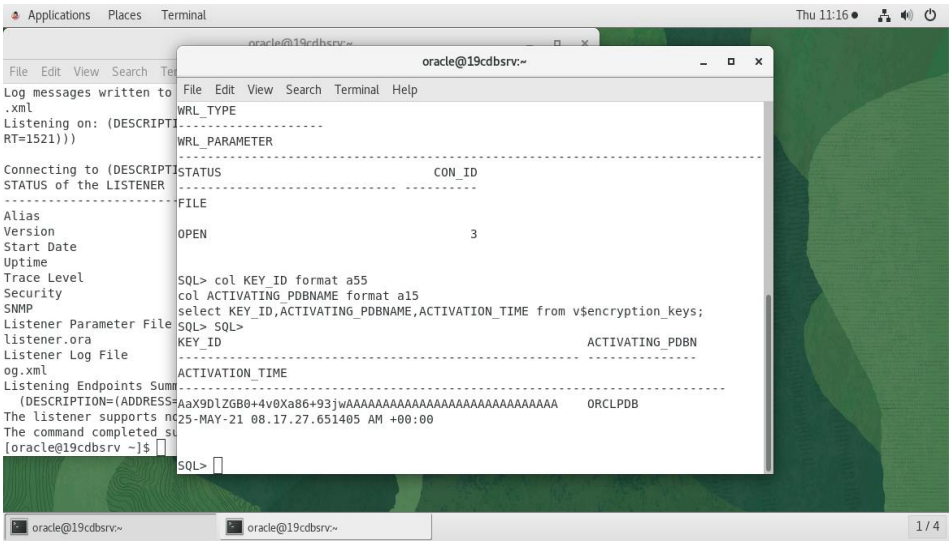


***Figure 5.20*** *Check encryption keys*

We read the data files and we will see that in the unencrypted file the data can be read, but in the encrypted one it is impossible to read:

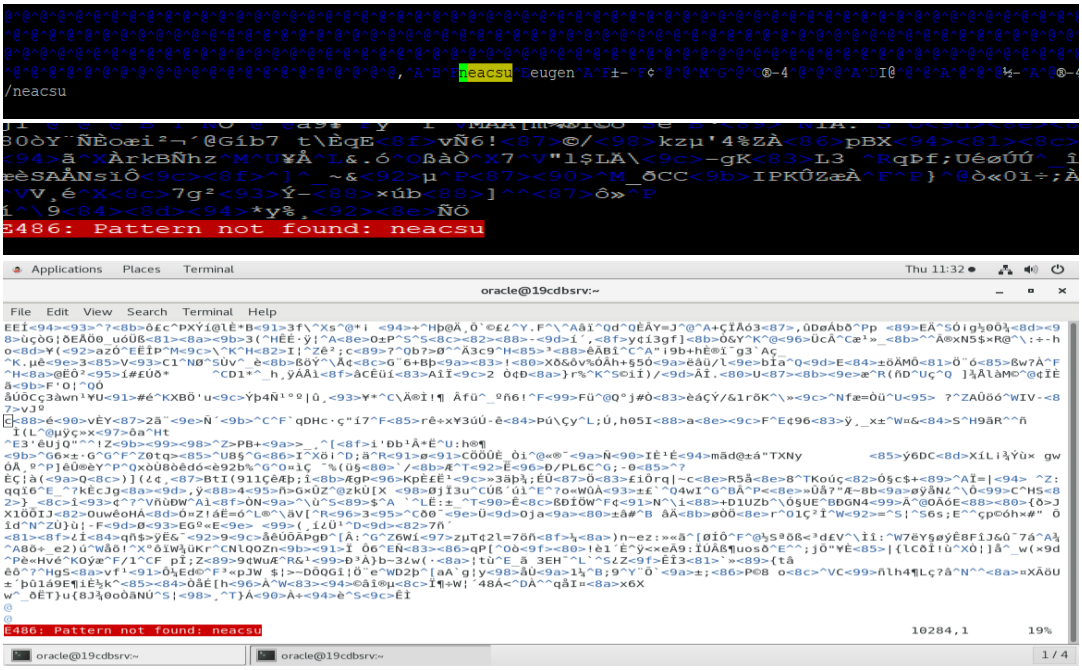


***Figure 5.21*** *Data integrity check*

The principle of minimum privilege is that users will be granted only those privileges that are actually necessary to perform their tasks effectively. In order to concretely implement this principle, the **Integrated Security System** restricts the following:

- ➔ the number of *SYSTEM* and *OBJECT* privileges granted to database users;
- ➔ the number of people who are allowed to make privileged SYS connections to the database;
- ➔ the number of users who are granted any privileges, such as the *DROP ANY TABLE*. In general, we do not need to grant *CREATE ANY TABLE* privileges to a user without DBA privileges;
- ➔ the number of users who are allowed to perform actions that create, modify or delete objects from the database, such as the instructions *TRUNCATE TABLE, DELETE TABLE, DROP TABLE*;
- ➔ the privileges *CREATE ANY JOB, BECOME USER, EXP_FULL_ DATABASE* and *IMP_FULL_DATABASE*;
- ➔ library privileges only for trusted users;
- ➔ non-administrative access of users to objects owned by SYS;
- ➔ permissions for running facilities;
- ➔ default (predefined) user accounts are blocked;
- ➔ the granting of the privileges *ALTER SYSTEM, AUDIT SYSTEM* and *CREATE EXTERNAL JOB* is monitored only to the users and roles that have the need to know;
- ➔ the privileges of the proxy account (for authorization) are limited only to *CREATE SESSION*;
- ➔ secure application roles are used to protect roles that are enabled by the application code.

### 5.2.2 Security policies development

Although the most common type of policy breach are unintentional attempts by users to access, such as browsing restricted directories, such breaches are usually the least significant, as access restrictions and well-designed rights policies address this issue. Violations of administrative policy are the most significant type of events, whether deliberate or accidental, due to the nature of administrative rights. The privileges of the administrator account grant a significant degree of access to the systems, for the persons requesting to fulfill their specific tasks. However, this does not imply authorization to use those system rights outside the authorized domain or process. The ability of administrator accounts to allow user account creation, account modification, restricted data viewing and data access rights changes requires a careful analysis of how to mitigate the risks associated with such strong capabilities.

### 5.2.3 Analysis step

In order to implement a security monitoring and attack detection system based on the recording of security events, the following issues need to be addressed [95]:

- ➔ managing large volumes of security events;
- ➔ storing and managing event information in a central node;
- ➔ identification and reaction to attacks;
- ➔ restricting staff to bypass security audit controls.

### 5.2.4 Security evaluation of the system

The main purpose of a security monitoring and attack detection system is to help identify suspicious events in a network that may indicate malicious activity or procedural errors [98]. The **Integrated Security System** (ISS) contributes to solving the need for security in critical IT systems. It offers a security monitoring solution, a continuous process of planning, implementation, management and testing, because this is the very nature of security monitoring. As threats to computer networks are constantly changing, so must the security monitoring system. Applying this process to security management involved:

- identifying ways to reduce the risk to acceptable levels;
- mitigation of security risks;
- identification of the main objectives to be secured;
- assessment of efficacy and safety requirements.

## 5.3 Results. Conclusions

Data is a very crucial resource for any organization due to its protection. Regular audit of the managed database should never be left to chance or patchwork solutions. During the audit period, stakeholders should identify that a system is configured to the standard that ensures risk mitigation.

The number of threats and incidents that have dominated media reporting for years has raised awareness and stimulated most organizations to invest time and resources in defending against this predominant security issue. However, the biggest threat to IT infrastructure may not be in the form of an external attack, such as a virus, but may reside within the internal network.

The **Integrated Security System** (ISS) is a complete protection solution that can easily achieve the following:

- ✓ access and authentication audit;
- ✓ user audit;
- ✓ administrator audit;
- ✓ audit of suspicious activity;
- ✓ auditing vulnerabilities and threats;

- ✓ policy implementation on managed systems;
- ✓ encryption of information flow.

Without a comprehensive audit solution, organizations jeopardize valuable information. Corrupt, inaccurate or compromised data represent lost revenue, lost time and compromised relationships. Auditing is an ongoing process, no matter what system or vendor is used. Even the basics should be reviewed regularly to avoid a false sense of security. The database is a sensitive component in critical infrastructures so it is important that it is configured correctly to ensure integrated information security..

Correlating information about security events involves collecting security events from multiple systems and placing this data in a secure central location. When security information has been correlated, the security engineer can analyze this central node to identify violations or external attacks. This node is important not only for cyberint analysis, but also as a tool for detecting attacks and addressing vulnerabilities. Planning to use cyber analysis differs from approaches to other solutions, because it involves investigating incidents after they have occurred, rather than a real-time analysis of incidents. Therefore, a detailed history of events in several systems must be maintained for a longer period of time (preferably 6 months). Because of this additional need, an effective security system should be centralized and have a significant amount of storage capacity to store a large number of records in an appropriate database structure.

The security of cyberint data analysis must also be taken into account, as access to this information should be rarely necessary. However, if access is required, it should only be provided to a few trusted people in the security level of the managed infrastructure. The administrator's access to this information should be strictly regulated in an established change control process – which has additional oversight. No one else should have the ability to access, interrupt or change this information.

# Chapter 6

# Conclusions

The paper entitled *INTEGRATED PROTECTION OF CRITICAL INFORMATION SYSTEMS* addresses an indispensable topic for this period, in which information is power in the current geopolitical context. Data protection is a permanent concern of all entities dealing with the management of critical systems, regardless of the economic situation of the organizations component. The security of critical IT systems requires specialized assistance and a commitment to the standards of the best competencies. In this paper, there were presented the best practices based on proven technologies and processes, that will help you protect your infrastructure and organization. You have learned the main methods of protecting critical information systems, starting from the development of the network, till encryption operations and optimization of information flow. You need to take a proactive approach to security, an approach that starts with an assessment to identify and classify your risks at the communications network level. In addition, you need to understand the technical security details related to the security policy and incident response procedures. This paper covered many good practices that will help you orchestrate a long-term strategy for the infrastructure you manage.

## 6.1 Obtained results

Chapter 2 clarifies the basic elements of information systems, focusing on the concept of *integrated protection*. It was presented the terminology used in this field, but also the mathematical foundations necessary to understand modern security concepts: confidentiality, integrity, authentication and non-repudiation.

In the process of defining the CIS, the following results were identified and proposed:

- ✓ basic SI criteria necessary to identify the performance of the system;
- ✓ ways to interconnect CIS;
- ✓ techniques of structural and functional analysis of an information system;
- ✓ interdependencies between infrastructures due to the complexity of the services provided;
- ✓ methods for assessing IS vulnerabilities;
- ✓ identification and analysis of the main sources of threats within a critical infrastructure;
- ✓ providing the main procedures to improve the utility of the systems;
- ✓ analysis of the issue regarding the difficulty of implementing security (from the point of view of a system administrator);
- ✓ elaboration of own prevention measures in front of external intrusions (having in composition 5 objectives: security assessment, centralized control,

maintenance of security standards, staff training, compliance with the law).

Chapter 3 presents the best cryptographic techniques currently used in computer and communication systems, necessary for the protection of managed data. I started from the main methods of information protection, specific to contemporary technology and I came to these results:

- ✓ identifying the most common techniques for hiding information: determining certain forms in encrypted messages, weaknesses and measures to prevent message interception;
- ✓ presentation of current cryptographic techniques and notions of cryptographic key management;
- ✓ explaining the methods necessary to implement an integrated protection at the communications node level;
- ✓ security analysis of the main cryptographic algorithms used for information secrecy;
- ✓ integration and documentation of an infrastructure with public keys, being part of the encryption process;
- ✓ identification and security analysis of the most important techniques for securing large-scale communications (SIP, RTP, IPsec);
- ✓ justification of the data packets from the structure of the messages transmitted in the network;
- ✓ ensuring the flexibility in the implementation of the protocols is achieved by avoiding the maintenance of a complex infrastructure of VPN tunnels in the conditions in which we have a PKI infrastructure that provides the certificates and encryption keys;
- ✓ understanding the technological considerations regarding the adoption of PKI in order to implement the TLS protocol for the protection of connections, critical informations that may affect the security of communications transmitted via SRTP are inaccessible in the face of potential interceptions.

The main benefit of information security is the possibility to ensure the integrity of sensitive data, which can provide a high degree of protection at the network level.

Chapter 4 is dedicated to the centralized security management of critical infrastructures managed at organizational level, providing the necessary tools to accurately identify security risks, but also to strengthen institutional protection. Practical aspects are presented that reveal a coordinated approach to systems administration that integrates all available resources to ensure the necessary security. The conclusions presented in this chapter require a complete refurbishment of telecommunications equipment within critical infrastructures, massive investments in IT resources, the recruitment and improvement of security engineers who manage these systems, but also the development of timely response to intrusions software programs.

Potential threats can materialize over a very wide horizon, such as: international terrorism, proliferation, organized crime or pandemics (COVID-19). Globalization puts pressure on existing threats, with direct consequences for people. It is absolutely

necessary to develop at national level the concept of cyber resilience that clearly illustrates the importance of interfaces and database connections.

Chapter 5 presents the main steps taken in the design, implementation and configuration of an **Integrated Security System** (ISS) in order to secure databases that are a valuable entity that may have tactical importance for the entities concerned. A first step was to define security objectives and requirements (standard audit, application-level audit trail, audit of BD events, database trigger audit, external audit). Database auditing is required to track certain events that may penetrate configured security measures. Next, I went through the implementation stage which consisted of: creating the **ISS** framework, changing the database structure, configuring BD triggers, modifying scripts at the operating system level, configuring packages at the BD level, configuring profile settings at the application level and implementing the integrity functionality of stored information by encrypting database traffic. The next step was to develop local security policies for the operating system, necessary to secure the data in the face of widespread vulnerabilities. The integration of these stable, monitored and revised measures ensures the security objectives of the study. **ISS** is basically a model for securing access to data traffic between the applications used and the database in the central node. By designing this system, I developed a model of centralized analysis and detection that can be considered a standard in a critical infrastructure (for example, in a Data Center). This system contains a risk analysis of possible vulnerabilities in the system and a complete security assessment to help improve and develop the security monitoring practices of computer systems.

## 6.2 Original contributions

In achieving this work, the following original contributions were made to the security of critical information systems:

1. a brief analysis of the components, indicators and criteria reflecting the security status of the IS (section 2.1);
2. the following were defined and exemplified: the information base, the technical base, the operating system, the scientific basis and the organizational – presenting the main issues of IS interdependencies in order to identify approaches to a whole system of critical infrastructures that interact with each other (section 2.2);
3. security analysis of the main cyber attacks on IS (section 2.3.1);
4. conducting a case study on the analysis of phishing attacks, providing important security aspects (section 2.3.2);
5. the elaboration of countermeasures necessary to be implemented to combat cyber aggression, which led to the provision of a high level of security of IS (section 2.3.3);
6. comparative analysis of public key/private key algorithms (section 3.1);
7. comparative analysis of data packets transmitted over a large network (section 3.2);

8. implementing and encrypting VoIP network connections using the PKI infrastructure (section 3.3);
9. conducting a case study on the security analysis of a VoIP network, identifying the main vulnerabilities of the network and creating preventive measures (section 3.3);
10. developing practical network configuration measures to eliminate potential infrastructure attacks;
11. setting up the centralized security management process (section 4.1);
12. development of an information risk management model (severity – impact);
13. implementation of an integrated security plan of a Data Center (analysis of security environments, centralized security management, risk analysis against CIS, risk management), tool that provides a clear picture of the threats and vulnerabilities of the critical infrastructure, measures to prevent security incidents, but also an alert system on priority levels (section 4.2);
14. development of two scenarios for the analysis of security risks: terrorist attack and earthquake (grading the severity of the impact, strengthening the capacity to react);
15. designing, implementation and development of an Integrated Security System (Chapter 5);
16. creation of a guide on data protection in the virtual environment, in order to strengthen the effective protection of personal data (Annex 7);
17. creation of a test in the field of INFOSEC, designed to assess the knowledge required of security engineers managing critical information systems (Annex 8).

## 6.3 List of the original works

### A. Scientific articles in ISI Web of Science indexed publications

**[A1] E. NEACȘU**, P. ȘCHIOPU, *An Analysis of Security Threats in VoIP Communication Systems*, International Conference on Electronics, Computers and Artificial Intelligence ECAI, ISBN: 978-1-7281-6843-2 IEEE Xplore, doi: 10.1109/ECAI50035.2020.9223162, ISSN 2378-7147, WOS: 000627393500042, 2020.

**[A2] E. NEACȘU**, P. ȘCHIOPU, *Proposed Pattern for Data Confidentiality in Wireless Communications*, Proc. SPIE 11718, Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X, 1171836, ISBN: 978-1-5106-4272-0, doi: 10.1117/12.2573269, ISSN 0277-786X, WOS: 000641147900113, 2020.

**[A3] E. NEACȘU**, P. ȘCHIOPU, *A Security Analysis of Public Key Cryptographic Systems Used for Electronic Signature*, University Politehnica of Bucharest, Scientific Bulletin, Series C Electrical Engineering and Computer Science, ISSN 2286-3540, WOS: 000628640200011, 2021.

**B. Scientific articles in BDI indexed publications**

**[B1] E. NEACȘU**, *Data Protection System Based on Digital Signature*, Bulletin of the University of Pitesti, Series: Electronics and Computers Science, ISSN 2344-2158, 2020.

**[B2] E. NEACȘU**, *The Effectiveness of the Statistical Testing of Randomness in a Complete Cryptographic System*, Bulletin of the Polytechnic Institute of Iași, Section of Electrical Engineering, Power Engineering and Electronics, ISSN 1223-8139, 2020.

**C. Scientific articles in publications with a recognition point**

**[C1] E. NEACȘU**, *VoIP and Video Conferencing Security Methods. IPsec Security*, Student Scientific Communications Session SCSS 2, Department of Mathematical Methods and Models, Section 13 - 3, Polytechnic University of Bucharest, 2017.

**[C2] E. NEACȘU**, *Encryption of the RTP Session (Real-time Transport Protocol)*, Student Scientific Communications Session SCSS 2, Department of Mathematical Methods and Models, Section 13 - 2, Polytechnic University of Bucharest, 2018.

**[C3] E. NEACȘU**, *Providing Secure End-to-End Networks*, Workshop on Innovative Techniques, Diversity & Connectivity WITDC-19, Center for Research and Training in Innovative Techniques of Applied Mathematics in Engineering Traian Lalescu (CiTi), București, 2019.

**D. Research project**

**[D1] E. NEACȘU**, *Operator Security Plan*, Information and Communications Technology Sector, Information Security Infrastructures Subsector, Carol I National Defense University, Faculty of Command and General Staff, Critical Infrastructure Protection CIP, Bucharest, 2020.

**E. Reports of scientific activity within the PhD program**

**[E1]** Scientific report no. 1/2019, *Dynamics of the Security Environment and The Role of Information Systems*.

**[E2]** Scientific report no. 2/2019, *Identifying and Counteracting Cyber Attacks*.

**[E3]** Scientific report no. 3/2020, *Securing Communications of Great Extent (VoIP)*.

**[E4]** Scientific report no. 4/2020, *Vulnerabilities, Risks and Protection Measures against Attacks on Communication Systems (VoIP)*.

# 6.4 Prospects for further development

The paper proposes a new system for securing sensitive data in critical infrastructures. Demonstrating performance and security, recommends this Integrated Security System (ISS) as a new solution for protecting sensitive data in computer systems.

As a perspective for further development, I want to develop an application for centralized detection at the communications node level, using APEX technology PL/SQL development, which will allow me to outline an easier way to configure and query multiple managed databases simultaneously. Personally, I believe that cyber security is a decisive factor in the technological development of any state, and the practices that ensure the security of information systems must be adapted to the new challenges that threaten the integrity of communications infrastructures.

# Bibliography

[4] C. Răcuciu, D. Grecu, *Cryptography and Information Security*, Renaissance Publishing House, Bucharest, ISBN 978-606-8321-89-9, 2010.

[6] **E. NEACȘU**, P. ȘCHIOPU, *Proposed Pattern for Data Confidentiality in Wireless Communications*, Proc. SPIE 11718, Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X, 1171836, ISBN: 978-1-5106-4272-0, doi: 10.1117/12.2573269, ISSN 0277-786X, WOS: 000641147900113, 2020.

[11] Cyber Security Guide, https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf

[13] **E. NEACȘU**, P. ȘCHIOPU, *A Security Analysis of Public Key Cryptographic Systems Used for Electronic Signature*, University Politehnica of Bucharest, Scientific Bulletin, Series C Electrical Engineering and Computer Science, ISSN 2286-3540, WOS: 000628640200011, 2021.

[15] Email Spoofing, https://blogs.cisco.com/security/what-is-email-spoofing-and-how-to-detect-it

[16] B. Robisson, P. Manet, *Differential Behavioral Analysis*. Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Computer Science, vol. 4727, pp. 413-426. Springer Berlin/Heidelberg, 2007.

[38] P. C. Pfleeger, *Security in Computing*. Prentice Hall, Inc., 1989.

[48] **E. NEACȘU**, *Encryption of the RTP Session (Real-time Transport Protocol)*, Student Scientific Communications Session SCSS 2, Department of Mathematical Methods and Models, Section 13 - 2, Polytechnic University of Bucharest, 2018.

[66] **E. NEACȘU**, *VoIP and Video Conferencing Security Methods. IPsec Security*, Student Scientific Communications Session SCSS 2, Department of Mathematical Methods and Models, Section 13 - 3, Polytechnic University of Bucharest, 2017.

[74] **E. NEACȘU**, P. ȘCHIOPU, *An Analysis of Security Threats in VoIP Communication Systems*, International Conference on Electronics, Computers and Artificial Intelligence ECAI, ISBN: 978-1-7281-6843-2 IEEE Xplore, doi: 10.1109/ECAI50035.2020.9223162, ISSN 2378-7147, WOS: 000627393500042, 2020.

[79] **E. NEACȘU**, *Operator Security Plan*, Information and Communications Technology Sector, Information Security Infrastructures Subsector, Carol I National Defense University, Faculty of Command and General Staff, Critical Infrastructure Protection CIP, Bucharest, 2020.

[95] Cilluffo, J. Frank. *A Global Perspective on Cyber Threats*. Center for Cyber and Homeland Security. June 16, 2015.

[98] Feakin, Tobias. *Developing a Proportionate Response to a Cyber Incident*. Council on Foreign Relations Press. August 2015.