"Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XX – 2017 – Issue 1
The journal is indexed in: PROQUEST / DOAJ / Crossref / EBSCOhost / INDEX COPERNICUS / DRJI / OAJI / JOURNAL INDEX / I2OR / SCIENCE LIBRARY INDEX / Google Scholar / Academic Keys/ ROAD Open Access / Academic Resources / Scientific Indexing Services / SCIPIO / JIFACTOR

CRYPTOLOGY AND INFORMATION SECURITY

Claudiu ARAMĂ[1]
Eduard Eusebiu EMANDII[2]
[1] Head Office, Romanian Air Force, Romania
[2] Head Office, Information Technology Center, Naval Academy "Mircea cel Bătrân", Romania, eduard.emandii@anmb.ro

Abstract: *Cryptography has emerged as a security guarantee, because the risk of security, like any other risks otherwise need to be covered. When the object is manipulated information only, cryptography is one of the few guarantees demonstrable. So its role is to provide security guarantees to the risks of information.*
In an era where information is essential, its security has become a primary concern. This is because the information is worthless as long as its security attributes are not insured. In high, security means protection against a potential threats and threats in relation to information can range from simple alteration to its inadvertent access by unauthorized persons or destroy them .
Security is not a product that can be bought to ensure total protection. Security is an accumulation of points for updates constantly, whether we're talking about software or human component. At the same time safety culture will always play the leading role.
It should be understood that cryptography is an essential piece in security but not the only one.
Keywords: *cryptography, information, security, risk*

- **Cryptography and its role.**

Cryptography[1] is a component of a much broader field called security information.
Cryptography is the study of mathematical methods related to information security, capable of ensuring confidentiality, authentication and non-repudiation of messages and data integrity circulated.
Cryptography has emerged as a guarantee of security, because security risks like any other risks be covered. When the manipulated object is information only, cryptography is one of the few guarantees demonstrable. So its role is to provide security guarantees to the risks of information.
Cryptography is commonly used in a wide range of applications in the area: health care institutions, public, private banking and even in the most common applications you use every day: mobile telephony, email, document editor, and so on..
Cryptography[2] is defined as the study of mathematical techniques related to information security issues such as confidentiality, integrity, authentication entities, data origin authentication.
A definition of cryptography is never complete. One hand because it is not entirely mathematical cryptography (even if her great part is), for example quantum cryptography does more than appeal to the knowledge of physics and mathematics of cryptography implementation is more about mathematics than computer science. Ron Rivest made a remark as simple as it is profound in terms cryptography and this remark may be considered an excellent definition of cryptography: *Cryptography communication means communication in the presence of opponents.*
Cryptography has been defined as a secret writing by a code of conventional signs, but this description was available until a few centuries ago.
Cryptography is dealing with construction of cryptographic functions.
We can define a cryptographic function as a function that depends on a parameter called **the key** and applies a **message** ("plaintext") to obtain an encrypted message called **criptotext** ("ciphertext"). At the same time the objective of cryptography is to build reverse this function with which the criptotext alongside key can recover the original message - this is what we call the decryption function.
Not all cryptographic functions have key, and more, not all cryptographic functions allowed a reverse.
The field aims to recover from criptotext the message and the key is called **cryptanalysis** and the common language is what we call breaking cryptographic functions intuitively that legally can be seen as reversing them. Generally break a cryptographic function involves actions much simpler than reversing its image created again having only intuitive value. Cryptography and cryptanalysis are the two branches of domain called **cryptology.**

[1] The word is formed from the Greek words Crypt - hidden script - writing
[2] A.J. Menezes, P.C. Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press,1996

DOI: 10.21279/1454-864X-17-I1-067

- **Cryptography – short history**

The evolution of cryptography can be systematized in four etape[3]:

i. During antiquity,

ii. the medieval period,

iii. the period before World War until after the Second World War,

iv. Modern cryptography period beginning after the Second World War (perhaps more precisely around 70 years).

The first, antiquity, is characterized by mathematical foundations cryaptographic systems without any automatism or by he desire of any automatism(is a procedure to create a automatically model, for example mechanical encryption). From this period dates Caesar code (a simple permutation of letters) and Greek SkyTeam cylinder which was wrapped a strip of paper on which was written the text (decryption requires winding course on a cylinder similar diameter). Indeed, these techniques are remotely related to modern cryptography.

The second period, medieval, is distinct by using alternative techniques polyalphabetical. In this one letter is substituted with any other letter without obvious repetition, not just one as in simple substitutes, eg permutation of the Caesar code. Polyalphabetical cryptosystem was first discovered by Leon Battista Alberti (1404-1472) and is called Alberti's code, it is considered the first major breakthrough in cryptography after the time of Caesar. The most striking example is Vigenère after the name of the Vigenère Blaise (1523-1596) although it was first described by Giovan Battista Bellaso Italian cryptographer (1505-?) in 1553 while Vigenère publishing it in 1586. Bellaso is also known as the encryption table the table of Giambattista della Porta Porta published (1535? -1615) 1563 without giving credit to Bellaso. In the same period engaged in cryptography and Gerolamo (Geronimo) Cardano (1501-1576) whose name is known in mathematical formulas for solving quadratic equations, cubic and quartz; it introduces an encryption system called Cardano's grid in 1550.

The third period, the world wars and the period before wars is remarkable for the appearance of principles, like the laws of Auguste Kerckhoffs (1835 - 1903) which are present even today and more than that of cryptosystems like cod Gilbert Sandford Vernam (1890 - 1960) which to this day remains the only code with unconditional security (known as Vernam code, and slightly modified version of the one-time pad).

The first goals in building a cryptographic algorithm was set by Kerckhoffs in the nineteenth century, with historic goals, these heaving relevance even nowadays:

i) the system must be, if not theoretically unbreakable, unbreakable in practice then.

ii) details of the compromise of cryptographic system should not create problems to the correspondents.

iii) the key should be memorable without being noted and to be easily changed.

iv) cipher (encrypted message) to be easily transmitted by telegraph.

v) the device encryption should be wearable and operable by one person.

vi) the system must be simple, without requiring knowledge of a long list of rules or intellectual stress.

In the run of the Second World War Enigma machine appears a cryptosystem which can be said to have played a decisive role in one of the most important events in human history: the Second World War. This period includes contributions from Alan Mathison Turing's fundamental (1912 -1954) of the machine builder who broke the Enigma (not to be confused with the Turing machine, a fundamental discovery which is perhaps its first abstraction of modern computing machines). Alan Turing remains recognized as the father of computer science and artificial intelligence.

In some historical presentations is a separation between the pre-war period (Kerckhoffs and Vernam's period) and the period of the Second World War. No wonder that the Second World War led to the development of cryptography, because the basic role in the fate of the war was played by submarines and aircraft, two weapons that depend on wireless communication, communication easy to do (without requiring a infrastructure for the transmission medium, there is no cable, only air) but is exposed enemies (whoever hears what is said). Wireless environment is one of the main drivers for the development of security, obviously because of the fragile environment in the face of opposition.

Modern cryptography begins in the opinion of many peoplewith Claude Elwood Shannon (1916 - 2001) parent for the domain of information theory and cryptography ushers in the era of mathematical cryptography. Maybe another beginning of modern cryptography could be seen in the code of Horst Feistel and the birth of public key cryptography due to Diffie-Hellman-Merkle's. With the discovery of cryptography public key cryptography move from a predominantly military area in an academic field, universities and research groups.

[3] Bogdan Groza, Introducere în Criptografie-Funcţii criptografice, Fundamente matematice şi computaţionale, Publisher Politehnica, 2012, p.27

DOI: 10.21279/1454-864X-17-I1-067

- **Information security. General information.**

In an era where information is essential, its security has become a primary concern. This is because the information is worthless as long as its security attributes are not insured. In high security means protection against a potential threats and threats in relation to information can range from simple alteration to its inadvertent access by unauthorized persons or destruction.

Information security is the field that deals with the study of mechanisms of information protection in order to ensure a level of trust in information and is fair to say that the level of trust in the information depends on the security mechanisms that guarantee protection against risks appear on its security. Techniques for security of information gives information of whatever nature and it is important to note that the information has value especially when is the subject of the exchange and processing, so just when vulnerable parts that can not be considered reliable. Thus,without excluding the value of the information stored ,value of information increases evident in the action of exchange or processing and it is obvious that an information completely isolated not lead to very high security risks yet neither can bring many benefits if is having a low value.

Considering how processing and storing information nowadays is made attention should be paid to Information Systems Security (INFOSEC - Security Information System) which is defined as follows:

Systems Security Informatice[4] (INFOSEC) means protecting computer systems from unauthorized access or modification of information, whether stored, processed or in transit, and against the denial of service to authorized users or the provision of services by unauthorized users, including those methods necessary to detect, documentation and rejection of these threats.

Designing a potential security solutions can be made by generating solutions to the following[5]:

- How does the opponent rich to the system?
- What are the objectives of security that must be provided in the system?
- What is the security level to witch a system needs to respond?

These three questions can be set by others such as[6]:

- What should be protected?
- What are the threats and vulnerabilities?
- What are the implications in the destruction or loss of equipment?
- What is the value of the equipment for the organization?
- What can be done to minimize exposure to hazards?

It should be considered that to ensure information security means to ensure information itself, but also ensure environment which it is stored. At the same time answering the first question we can distinguish two situations: where your opponent personally reach into the system and the situation when zou opponent get inside the szstem using electronicall metods . For the first situation treatment solutions fall into the category of physical security solutions. For the second situation we speak of electronic security, cryptographic techniques play a fundamental role in this context. These two distinct security solutions can often merge into a physical security device authentication based on cryptographic techniques, such as for example a smart card.

- **Incident - Motivation For Security**

Adoption of best security practices (and developing cryptographic techniques in general) is generally motivated by incidents, most often with negative consequences .

If during the period 1982-2000 there was a balance between security incidents sources, they basically coming from three distinct directions: external, internal, accidental; in 2001-2003 in addition to the fact that the number of attacks increased significantly this balance is lost, most security problems ar related to external factors.

The reason for this comes from the natural opening to the public use for networks and systems using standard components required by the market. Opening system (opponent has access to the system) is due to the fact that there is no sense of isolation perimeters for secured computer. Even disconnecting from the Internet does not guarantee this because once inserted a USB device infected can infect isolated system.

Of course, it should be taken into account that the cryptographic security vulnerabilities could be exploited by adversaries such extremist movements for example, to cause damage. The vulnerability in the sectors of electricity and gas distribution is routinely recognized especially in the United States.

Lately we witness an avalanche of attacks against companies with high visibility in the landscape of international business, such as Ubisoft, Google,

[4] Bogdan Groza, Introducere în Criptografie-Funcţii criptografice, Fundamente matematice şi computaţionale ,Publisher Politehnica, 2012, p.10

[5] D. Dzung, M. Naedele, T.P. Hoff, M. Crevatin, *Security for Industrial Communication Systems*, Proceedings of the IEEE, vol. 93, no. 6., 2005

[6] J. Bayne, *An Overview of Threath and Risk Assesment*, SANS Institute, 2002

DOI: 10.21279/1454-864X-17-I1-067

Facebook or Twitter, and on some state institutions such as NASA or FBI, with worrying results to security data and reputation.

While malware attacks is producing greatest losses for companies , approximately 70% of security breaches are the result of human error and various system problems and IT implementation.

Besides the interests of attackers targeting corporate data, private information of customers, employees or business partners who may be exposed on the net and subsequently used in other complex attacks against targets.

Companies, whether large, small or medium should know that these dangers can be avoided or controlled if you take into account some simple rules, but essential for security[7]:

- Evaluation of information that you own. It is important to know precisely and in advance what may be lost in the event of security breaches. What kind of information you have, whether or not confidential, how important for the company, customers or employees and what are the risk of losing control of such dates. Once you know what you are protecting, you'll also know how to protect.

- Do not limit yourself to one extent or data protection product.Is capital to use different security methods. In case one fails or turns out to be vulnerable, others remain.

- Limiting physical work space to all unauthorized persons. Someone may steal from you company a server, a laptop or a hard drive with important data. Secret information can be stored in different locations and you can protect the system by limitating the number of people allowed into the system.

- Setting up the network architecture should be such that it can intervene quickly to isolate an infection, say, in a single subnet, thereby preventing the spread of infection throughout the department or the company network.

This minimizes the impact that an attack may have ;an attack that managed to penetrate the first line of defense. A well configured firewall can do wonders. Make sure that the person who is configuraing you the firewall knows what he does.

- Access points (hot spots) unauthorized must be completely denied within the company networks, and a device that must first login to the WiFi authoriyed by the company must allow only login-based with digital certificates.

- The access must be restricted to persons in contact with company resources with an username and password that needs to be changed regularly and have a high degree of difficulty. The moment an employee or collaborator completed its work in the company, its authentication data must be immediately canceled.

- A competitive antivirus technology based anti-spam, anti-phishing and anti-malware who starts even from gateway is vital to run against phishing attacks or exploits.

- Security courses held regularly for employees. Each must know how to recognize a phishing message, to know how to handle attachments in e-mails, to scan and, very importantly, to report to the departametului IT any incident or situation that they found it suspicious.

- Use different passwords for different accounts .Avoiding connecting to corporate resources using personal accounts. Avoiding publication on personal accounts in various social networking information concerning the employer company. Sometimes inadvertently, an employee can provide data that helps an attacker to break into a corporate network.

- An reserved attitude towards BYOD (bring your own device) .Angajaţii that bring to the company and use their own devices to work, should be aware that the smart phone, tablet, laptop can be a big challenge for the IT department company's. It is important that each device running a different operating system to have updates made for security and need to be included in the company's secure network when are running inside the company. That's not totally eliminates the risk of an unpleasant incident security, as long as it connects the phone to the Internet through Wi-Fi networks in cafes or airports where they can become infected with a virus, to bring then in the firm and compromise the entire network the company. Equally serious is if an employee loses phone or tablet that maintains information related to service that reached into the wrong hands can have devastating impact on business.

- Whitelisting site is performing better than blacklisting site. Companies can configure the network so that employees can only access websites that have been previously checked by qualified and approved as safe and without risk as attack. Considered hazardous sites can be blocked so the company firewall and nobody can connect to this web location even if, for example, someone clicked on a dangerous link or open an attachment studs. Often employees can infect through social networks like Facebook. You can either restrict access to those resources or can provide security training to use social networks.

[7] http://www.securitatea-informatiilor.ro/solutii-de-securitate-it/mic-ghid-de-securitate-a-datelor-pentru-companii-mici-si-mijlocii/#more-1612, visited 11.01.2017

DOI: 10.21279/1454-864X-17-I1-067

All these security measures must cope habits of users less secure. The loss or destruction of all or part of the data can have disastrous effects on the security and integrity of a company.
Thus, unless you want to help a stranger to harm you or your company for which you work, use discretion when updating your social network account with informations pertaining to private or professional life.

- **Relationship Vulnerability - Opponent - Security risk**

The existence of a vulnerability and a potential adversary involves a security risk. It is an unwritten law of information security that can be written as follows:

Hazard + Vulnerability = Security Risk[8]

In addition to sending and receiving distinguished presence of an opponent, which closes insecure communication channels (through understanding these public channels that can be accessed by opponents). The list of potential adversaries can be a starting point in assessing risks. They care about some coordinates such as computing resources, financial resources, intellectual resources, motivation, scale and nature of the damage they can cause. When we speak of opponents,we have to consider the followin:

- Hackers have financil resources and computing systems generally low and attack only motivated by the desire to defy or for fun.
- A network customers have limited computing power and are motivated by economic interests, eg fraud envolving network thermo-electric etc.
- Traders have modest computing power and financial resources with considerable interest in finding or handling secrets for gaining financial benefits.
- Organized crime has modest computing power and financial strength with high interest in altering the operating parameters of systems for gaining financial advantage.
- Terrorists have high computing power and financial reasons motivated by political-religious order to spread financial panic and damage.
- State governments adversaries have computing power and high financial, and more skilled and trained operators with experience. Their purpose is generally to affect infrastructures in complex attacks physical or electronic.
- People from the system are persons who have detailed information and have access to operational key , are generally motivated by interests or grievances order salary / financial.
- A combination of the above is the most dangerous kind of opponent; in practice any combination is possible and it has the greatest chance of success in an attack.

- **Objectives of security**

Regarding cryptography we generally distinguish four major security objectives that are recognized by any author in the field: confidentiality, integrity, authenticity and non-repudiation.

Confidentiality[9] means ensuring that information remains accessible only to authorized parties. It is the oldest object of cryptology. Among who do not know is still widespread opinion that the concept of cryptography is synonymous with that of privacy. Sure the view is flawed because cryptography deals and ensure objectives are listed below and who have no connection with keeping information secret.
Regarding this objective by providing cryptographic techniques, he is done by using encryption functions. Overall efficiency due to use features symmetric (secret key), but practical scenarios generally lead to orchestrate their functions asymmetric (public key).
Integrity refers to ensuring that information has not been altered during transmission or by a possible opponent. Cryptographic functions used for this purpose are hash functions that make modifying a single bit of information can be detected. We note that in principle it is wrong to use symmetrical and asymmetrical encryption functions for this purpose, the instrument is dedicated cryptographic hash functions (MAC codes or digital signatures in the broader context of authentication).
Of course there are symmetrical and asymmetrical encryption function that can ensure integrity for this purpose but their choice should be made with caution.
Authentication has two distinct coordinated entities authentication and authentication information. Authentication entities refers to the existence of a guarantee of the identity of a particular entity. Authentication information is for determining the source of the information - by default this guarantees the integrity of the information because if the information does not have integrity, so a potential adversary altered it, then neither its source of origin is not the same.
But only the integrity of information is not guarantee the authenticity of information. Authentication is generally achieved through

[8] Bogdan Groza, Introducere în Criptografie-Funcţii criptografice, Fundamente matematice şi computaţionale, Publisher Politehnica, 2012, p.13

[9] Bogdan Groza, Introducere în Criptografie-Funcţii criptografice, Fundamente matematice şi computaţionale, Publisher Politehnica, 2012, p.15

DOI: 10.21279/1454-864X-17-I1-067

protocols that may stem from whole arsenal of cryptographic functions: hash functions, MAC, symmetrical and asymmetrical encryption, digital signatures. Authentication includes most often a temporal factor involving a guarantee on the time the entity to which it is linked deposited it (because in the absence of a guarantee temporal information can be replicated and made by any other entity thus losing a valence authentication).

Non-repudiation (or unrepudiation) prevents an entity from denying an action taken (action materialized of course in the transmission of information). This means that if at one time an entity denies that certain information would be issued, the entity receiving the information that a neutral party can demonstrate that the information is really coming from the entity. Non-repudiation is achieved using digital signatures.

Other objective, something more specific but equally relevant are:

News information relates to ensuring that information received is present (fresh). This can be interpreted in two ways: on the one hand refers to the fact that the information can expire after a certain period of time, on the other hand refers to the fact that a possible adversary could change the order in which packets of information get destination (various scenarios can be imagined).It is generally achieved by using time-varying parameters: fingerprints temporal (time stamps), random number (nonce), counters (counter), etc.

Anonymity means preventing identity identifying an entity that requested the service. For example, it can be extremely helpful in banking when there is no desire to identify the person who makes a payment, or e-mail services for maintaining anonymity of the sender, etc. Is achieved either through agreements or by cryptographic functions adapted for this purpose.For example there is a strong research area in the functions of encryption denial (deniable encryption), which can encrypt information whose content can be changed to decrypt, making disown any information encrypted (there is for this effective solutions to present).

The authorization shall cover access control to prevent unauthorized entry into the system agents. The relationship between objective authentication and access control entities is that the latter objective in general is built first (it is normal to require a method to authenticate the entity before it allows access) but the goals are still distinct. This is because authorization means using authentication mechanisms and security policy to decide the right of access to the resources of entities.

Availability refers to ensure that a service is accessible when a legitimate user requests it.Ensuring this objective requires that an entity can not block unauthorized access to services of the authorized entity. But in this case no question of authorizing access issues previously mentioned, but the availability of the resource itself. This implies to avoid problems of resource depletion system because their misuse. Attacks on this are the Denial of Services (DoS) and causing economic damage as well as reliability.

Protection of third parties relate to avoid spreading danger on the parties that there is a connection. For example the attack on a particular component will not damage IT and other component or economically: the fall of a component due to an error handling will not result in discrediting manufacturer, etc.

Revocation refers to the possibility of revoking the right offer. Perhaps the most relevant example in connection with cryptography is the ability to revoke a public key certificate of the entity that issued it.

Traceability and tracking system refers to the ability to reconstruct the history of system operation based on records, eg registration of relevant controls, persons who have released etc. The objective is relevant in determining possible causes operating problems, so it is used in diagnosis.

List of can vary according to what is important to each holder of information.

- **Vulnerabilities**

The vulnerability is a weakness of a system which can be exploited by a potential adversary. Related to vulnerabilities we have to retaine joint rule embodied in the Charter of security that a system is safer than most vulnerable part of his.

A computer system vulnerabilities can be classified into[10]:

• design vulnerabilities (eg wrong design a communication protocol)

• vulnerabilities of implementation (eg overflow) fundamental vulnerabilities (eg choosing weak passwords), for example, the vulnerability of a primitive cryptographic can be enhanced by the security protocol (it is important to note that many cryptographic functions have vulnerabilities hidden and on the other hand, even using the most robust cryptographic function improperly can lead to total loss of security), assuming some security guarantees that are over-specified or misunderstood (perhaps the most common type of error is the use of functions encryption and the presumption that it will also ensure that data will not be altered), lack of attention in the application of general principles applicable to a wider class of primitive (eg

[10] D. Dzung, M. Naedele, T.P. Hoff, M. Crevatin, *Security for Industrial Communication Systems*, Proceedings of the IEEE, vol. 93, no. 6., 2005

DOI: 10.21279/1454-864X-17-I1-067

encryption using a device public key of information of low entropy can be easily located with an attack forward-search).

- **Attacks**

An attack is an assault on a security objective. There is a wide range of attacks and their various classifications according to various criteria. For example in they are classified into: attacks untargeted consisting of infiltrations in the system in order to exploit any vulnerabilities found and targeted attacks that have a specific purpose which is the operation of a part of the system (eg extraction of certain information, stealing passwords, etc.). A little more classic attacks classification is: passive attacks and active attacks.

Passive attacks are reading messages and traffic analysis. The difference between the two attacks is that the traffic analysis is not necessary to read the actual messages sent only to see patterns in communication, eg what nature has information sent, it's a download for a movie, a phone call over the Internet, and so on .It is important to note that these attacks are violations of privacy shared goal.

Active attacks are : changing information conveyed between two entities which involves altering detectable or not of the information, imposture (impersonation or mascaradarea) which is to claim another identity than the actual retransmission means to convey information that was previously transmitted a participant and closed the connection that effectively means cutting the communication channel (Denial of Services - DoS).

It is important to note, in terms of security objectives, the first three attacks are an assault for the lens of authenticity and the last an aggression for availability.

All these attacks are also called attacks on the communication channel and to combat their successful use cryptographic techniques in practice.

Conclusion

Security is not a product that can be bought to ensure total protection. Security is an accumulation of points for updates constantly, whether we're talking about software or human component. At the same time safety culture will always play the leading role. Users can be taught to use password complexity increased, but they can also give their passwords. Such security must be seen as a process, as an overall system, in which each component plays a role. It should be understood that cryptography is an essential piece in security but not the only one[11]. "Security is a process, not a product" is a common statement in information security.

Bibliography

Romanian and foreign authors

[1] Bogdan Groza, Introducere în Criptografia cu cheie public, Publisher Politehnica, 2007.

[2] Bogdan Groza, Introducere în Criptografie-Funcţii criptografice, Fundamente matematice şi computaţionale, Publisher Politehnica, 2012.

[3] A.J. Menezes, P.C. Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press,1996.

[4] D. Dzung, M. Naedele, T.P. Hoff, M. Crevatin, *Security for Industrial Communication Systems*, Proceedings of the IEEE, vol. 93, no. 6., 2005.

[5] J. Bayne, *An Overview of Threath and Risk Assesment*, SANS Institute, 2002

Infographic

[1] http://www.securitatea-informatiilor.ro/solutii-de-securitate-it/mic-ghid-de-securitate-a-datelor-pentru-companii-mici-si-mijlocii/#more-1612, visited 11.01.2017.

[11] Bogdan Groza, Introducere în Criptografia cu cheie public, Publisher Politehnica, 2007, p.147

DOI: 10.21279/1454-864X-17-I1-067