Cryptography Role in Information Security

Laura Savu
Information Security Department
University of Bucharest
Bucharest, Romania
laura.savu@microsoft.com

Abstract— **The aim of this paper is to provide an overview for information security. Here are discussed the most important properties of security in information like confidentiality, integrity, and availability. The research of protecting information has started in the oldest times and it still is a hot topic today.**

Keywords: security; public key encryption; cipher; concern; cloud.

I. WHAT IS INFORMATION SECURITY

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

II. CRYPTOGRAPHY

Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage. It is the practice of hiding information so that unauthorized persons can't read it. The literal meaning for cryptography is "hidden writing": how to make what you write obscure, unintelligible to everyone except whom you want to communicate with. Cryptography was already used in ancient times, essentially in three kinds of contexts: private communications, art and religion and military and diplomatic use.

A. History

The conceptual foundation of cryptography was laid out around 3000 years ago in India and China. Since the early days of writing, heads of state and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering. The antique cipher of the Greek historian Polibio used a table, with rows and columns, to associate a letter to a pair of numbers. Famous is the Caesar Cipher, based on a three positions' shift, that is, mathematically (considering the English 26 letters alphabet): $y = (x + 3) \bmod 26$. Julius Caesar is credited with the invention of the Caesar cipher ca. 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands. World War II brought about much advancement in information security and marked the beginning of the professional field of information security. The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The Enigma machine was a field unit used in WWII by German field agents to encrypt and decrypt messages and communications. The Enigma machine was one of the first mechanized methods of encrypting text using an iterative cipher. The Enigma machine was used by all branches of the German military as their main device for secure wireless communications until the end of World War 2. Several types of the Enigma machine were developed before and during World War 2, each more complex and harder to code break than its predecessors. The most complex Enigma type was used by the German Navy. In addition to the complexity of the Enigma machine itself, its operating procedures became increasingly complex, as the German military wanted to make Enigma communications harder to code break.

B. Ciphers

Cryptography is built on one overarching premise: the need for a cipher that can reliably, and portably, be used to encrypt text so that, through any means of cryptanalysis — differential, deductive, algebraic — the ciphertext cannot be undone with any available technology. Most modern ciphers can be categorized in several ways

- By whether they work on blocks of symbols usually of a fixed size (block ciphers), or on a continuous stream of symbols (stream ciphers).
- By whether the same key is used for both encryption and decryption (symmetric key algorithms), or if a different key is used for each (asymmetric key algorithms). If the algorithm is symmetric, the key must be known to the recipient and sender and to no one else. If the algorithm is an asymmetric one, the enciphering key is different from, but closely related to, the deciphering key. If one key cannot be deduced from the other, the asymmetric key algorithm has the

ISBN: 978-1-61804-018-3

public/private key property and one of the keys may be made public without loss of confidentiality.

1) The Substitution Cipher

In this method, each letter of the message is replaced with a single character. Because some letters appear more often and certain words appear more often than others, some ciphers are extremely easy to decrypt, and some can be deciphered at a glance by more practiced cryptologists.

2) The Shift Cipher

Also known as the Caesar cipher, the shift cipher is one that anyone can readily understand and remember for decoding. It is a form of the substitution cipher. By shifting the alphabet a few positions in either direction, a simple sentence can become unreadable to casual inspection.

3) The Polyalphabetic Cipher

To make ciphers more difficult to crack, Blaise de Vigenère from the 16th-century court of Henry III of France proposed a polyalphabetic substitution. In this cipher, instead of a one-to-one relationship, there is a one-to-many. A single letter can have multiple substitutes. The Vigenère solution was the first known cipher to use a keyword.

The Kasiski/Kerckhoff Method

In the 19th century, Auguste Kerckhoff said that essentially, a system should be considered secure, even when everyone knows everything about the system (except the password).

C. Modern Cryptography

In the mid-1970s the U.S. government issued a public specification, through its National Bureau of Standards (NBS), called the Data Encryption Standard or, most commonly, DES. The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on a symmetric-key algorithm that uses a 56-bit key. It became the encryption standard of choice until the late 1990s, when it was broken when Deep Crack broke a DES key in 22 hours and 15 minutes. Later that year a new form of DES, called Triple DES, which encrypted the plaintext in three iterations, was published. It remained in effect until 2002, when it was superseded by AES. The release of DES also included the creation and release of Ron Rivest, Adi Shamir, and Leonard Adleman's encryption algorithm (RSA). Rivest, Shamir, and Adleman, publicly described the algorithm in 1977.

RSA is the first encryption standard to introduce (to public knowledge) the new concept of digital signing. In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography.[1] It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

AES represents one of the latest chapters in the history of cryptography. It is currently one of the most popular of encryption standards. In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard adopted by the U.S. government. AES was announced by National Institute of Standards and Technology (NIST) on November 26, 2001 after a 5-year standardization process in which fifteen competing designs were presented and evaluated before Rijndael was selected as the most suitable (see Advanced Encryption Standard process for more details). It became effective as a Federal government standard on May 26, 2002 after approval by the Secretary of Commerce. It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the NSA for top secret information

The core principles of information security are confidentiality, integrity, authentication and nonrepudiation.

1) Authentication

Authentication is any process by which you verify that someone is who he claims he is. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints.

2) Confidentiality

Confidentiality means that only people with the right permission can access and use information. It also means protecting it from unauthorized access at all stages of its life cycle. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds. Encryption is one way to make sure that information remains confidential while it's stored and transmitted. Encryption converts information into code that makes it unreadable. Only people authorized to view the information can decode and use it.

3) Integrity

Integrity means that information systems and their data are accurate. Integrity ensures that changes can't be made to data without appropriate permission. If a system has integrity, it means that the data in the system is moved and processed in predictable ways. The data doesn't change when it's processed.

4) Non-repudiation

Nonrepudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Nonrepudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

ISBN: 978-1-61804-018-3

5) Availability

Availability is the security goal of making sure information systems are reliable. It makes sure data is accessible. It also helps to ensure that individuals with proper permission can use systems and retrieve data in a dependable and timely manner.

III. PUBLIC KEY ENCRYPTION

Public key encryption refers to a type of cypher architecture known as public key cryptography that utilizes two keys, or a key pair, to encrypt and decrypt data. One of the two keys is a public key, which anyone can use to encrypt a message for the owner of that key. The encrypted message is sent and the recipient uses the private key to decrypt it. Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. For this reason, it is sometime called *Diffie-Hellman encryption*. It is also called *asymmetric encryption* because it uses two keys instead of one key (*symmetric encryption*). The latest research focus is on the cryptographic primitive named Signcryption. This represents the combination of the digital signature and the public key encryption in a single logical step. The most important advantage of this new method is the cost which is less than the sum for the cost of digital signature and the cost for encryption. This new encryption schema has been invented by Yuliang Zheng 1997 [5].

Public key cryptography is used to solve various problems that symmetric key algorithms cannot. In particular, it can be used to provide privacy, and nonrepudiation. Privacy is usually provided through key distribution, and a symmetric key cipher. This is known as hybrid encryption. Nonrepudiation is usually provided through digital signatures, and a hash function [6].

A. Rivest–Shamir–Adelman

The Rivest–Shamir–Adelman (RSA) cryptosystem is a public key system. Based on an underlying hard problem and named after its three inventors, this algorithm was introduced in 1978 and to date remains secure. RSA has been the subject of extensive cryptanalysis, and no serious flaws have yet been found. The encryption algorithm is based on the underlying problem of factoring large numbers. So far, nobody has found a shortcut or easy way to factor large numbers in a finite set called a field. In a highly technical but excellent paper, Boneh reviews all the known cryptanalytic attacks on RSA and concludes that none is significant. Because the factorization problem has been open for many years, most cryptographers consider this problem a solid basis for a secure cryptosystem [1].

B. Cryptographic Hash Functions

The most widely used cryptographic hash functions are MD4, MD5 (where MD stands for Message Digest), and SHA/SHS (Secure Hash Algorithm or Standard). The MD4/5 algorithms were invented by Ron Rivest and RSA Laboratories. MD5 is an improved version of MD4. Both condense a message of any size to a 128-bit digest. SHA/SHS is similar to both MD4 and MD5; it produces a 160-bit digest. Wang et al. [WAN05] have announced cryptanalysis attacks on SHA, MD4, and MD5. For SHA, the attack is able to find two plaintexts that produce the same hash digest in approximately 263 steps, far short of the 280 steps that would be expected of a 1 60 bit hash function, and very feasible for a moderately well financed attacker [2].

C. Digital Signature

A digital signature is a protocol that produces the same effect as a real signature: It is a mark that only the sender can make, but other people can easily recognize as belonging to the sender. Just like a real signature, a digital signature is used to confirm agreement to a message. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature assures the receiver that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering [3].

D. Certificates

A public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. The most common use of certificates is for HTTPS-based web sites. A web browser validates that an SSL (Transport Layer Security) web server is authentic, so that the user can feel secure that their interaction with the web site has no eavesdroppers and that the web site is who it claims to be. This security is important for electronic commerce. In practice, a web site operator obtains a certificate by applying to a certificate provider with a certificate signing request. Contents of a typical digital certificate:

- Serial Number - used to uniquely identify the certificate.
- Subject - the person or entity identified.
- Signature Algorithm - the algorithm used to create the signature.
- Issuer - The entity that verified the information and issued the certificate.
- Valid-From - The date the certificate is first valid from.
- Valid-To - The expiration date.
- Key-Usage - Purpose of the public key (e.g. encipherment, signature, certificate signing...).

ISBN: 978-1-61804-018-3

- Public Key - the purpose of SSL when used with HTTP is not just to encrypt the traffic, but also to authenticate who the owner of the website is, and that someone's been willing to invest time and money into proving the authenticity and ownership of their domain.
- Thumbprint Algorithm - The algorithm used to hash the certificate.
- Thumbprint - The hash itself to ensure that the certificate has not been tampered with.

IV. Information Security Concerns

- Shoulder Surfing

Shoulder surfing occurs when an attacker looks over the shoulder of another person at a computer to discover sensitive information.

- Social Engineering

Social engineering describes an attack that relies heavily on human relations. It's not a technical attack. This type of attack involves tricking other people to break normal security procedures to gain sensitive information. These attackers take advantage of human nature.

- Phishing and Targeted Phishing Scams

Phishing is a form of Internet fraud where attackers attempt to steal valuable information from their victims. Phishing attacks take place in electronic communications. These attacks can take place via e-mail or instant messages. Phishing attacks also can take place in Internet chat rooms.

- Malware

Malware is a general term that refers to any type of software that performs some sort of harmful, unauthorized, or unknown activity. Malware includes computer viruses, worms, and Trojan horses. The term malware is a combination of the words malicious and software.

- Logic Bombs

A logic bomb is harmful code intentionally left on a computer system. It lies dormant for a certain period. When specific conditions are met, it "explodes" and carries out its malicious function. Conditions that cause the logic bomb to explode vary. Programmers can create logic bombs that explode on a certain day or when a specific event occurs.

- Backdoors

A backdoor, also called a "trap door," is a way to access a computer program or system that bypasses normal mechanisms. Programmers sometimes install a backdoor to access a program quickly during development to troubleshoot problems.

V. INFORMATION SECURITY IN CLOUDING

Design Principles for Information Security in Clouding

- Least privilege

The principle of least privilege maintains that an individual, process, or other type of entity should be given the minimum privileges and resources for the minimum period of time required to complete a task. This approach reduces the opportunity for unauthorized access to sensitive information. Only the minimum necessary rights should be assigned to a subject that requests access to a resource and should be in effect for the shortest duration necessary. Granting permissions to a user beyond the scope of the necessary rights of an action can allow that user to obtain or change information in unwanted ways. Therefore, careful delegation of access rights can limit attackers from damaging a system. This principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur. Thus, if a question arises related to misuse of a privilege, the number of programs that must be audited is minimized.

- Separation of duties

Separation of duties requires that completion of a specified sensitive activity or access to sensitive objects is dependent on the satisfaction of a plurality of conditions. Separation of duties (SoD) is the concept of having more than one person required to complete a task. It is alternatively called segregation of duties or, in the political realm, separation of powers [10].

- Defense in depth

Defense in depth is the application of multiple layers of protection wherein a subsequent layer will provide protection if a previous layer is breached. Defense in depth is an information assurance (IA) strategy in which multiple layers of defense are placed throughout an information technology (IT) system. It addresses security vulnerabilities in personnel, technology and operations for the duration of the system's life cycle. Defense in depth is originally a military strategy that seeks to delay, rather than prevent, the advance of an attacker by yielding space in order to buy time. The placement of protection mechanisms, procedures and policies is intended to increase the dependability of an IT system where multiple layers of defense prevent espionage and direct attacks against critical systems. In terms of computer network defense, defense in depth measures should not only prevent security breaches, but buys an organization time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach [11].

ISBN: 978-1-61804-018-3

- Fail safe

Fail safe means that if a cloud system fails it should fail to a state in which the security of the system and its data are not compromised. One implementation of this philosophy would be to make a system default to a state in which a user or process is denied access to the system. A fail-safe or fail-secure device is one that, in the event of failure, responds in a way that will cause no harm, or at least a minimum of harm, to other devices or danger to personnel.

- Economy of mechanism

Economy of mechanism promotes simple and comprehensible design and implementation of protection mechanisms, so that unintended access paths do not exist or can be readily identified and eliminated. One factor in evaluating a system's security is its complexity. If the design, implementation, or security mechanisms are highly complex, then the likelihood of security vulnerabilities increases. Subtle problems in complex systems may be difficult to find, especially in copious amounts of code. For instance, analyzing the source code that is responsible for the normal execution of a functionality can be a difficult task, but checking for alternate behaviors in the remaining code that can achieve the same functionality can be even more difficult. One strategy for simplifying code is the use of choke points, where shared functionality reduces the amount of source code required for an operation. Simplifying design or code is not always easy, but developers should strive for implementing simpler systems when possible.

- Complete mediation

In complete meditation, every request by a subject to access an object in a computer system must undergo a valid and effective authorization procedure. A software system that requires access checks to an object each time a subject requests access, especially for security-critical objects, decreases the chances of mistakenly giving elevated permissions to that subject. A system that checks the subject's permissions to an object only once can invite attackers to exploit that system. If the access control rights of a subject are decreased after the first time the rights are granted and the system does not check the next access to that object, then a permissions violation can occur.

- Open design

An open-access cloud system design that has been evaluated and tested by a myriad of experts provides a more secure authentication method than one that has not been widely assessed. Security of such mechanisms depends on protecting passwords or keys. The principles of open design are derived from the Free Software and Open Source movements.

- Least common mechanism

This principle states that a minimum number of protection mechanisms should be common to multiple users, as shared access paths can be sources of unauthorized information exchange. Avoid having multiple subjects sharing mechanisms to grant access to a resource. For example, serving an application on the Internet allows both attackers and users to gain access to the application. Sensitive information can potentially be shared between the subjects via the mechanism. A different mechanism (or instantiation of a mechanism) for each subject or class of subjects can provide flexibility of access control among various users and prevent potential security violations that would otherwise occur if only one mechanism was implemented.

- Psychological acceptability

Psychological acceptability refers to the ease of use and intuitiveness of the user interface that controls and interacts with the cloud access control mechanisms. Accessibility to resources should not be inhibited by security mechanisms. If security mechanisms hinder the usability or accessibility of resources, then users may opt to turn off those mechanisms. Where possible, security mechanisms should be transparent to the users of the system or at most introduce minimal obstruction. Security mechanisms should be user friendly to facilitate their use and understanding in a software application.

- Weakest link

The security of a cloud system is only as good as its weakest component. Thus, it is important to identify the weakest mechanisms in the security chain and layers of defense, and improve them so that risks to the system are mitigated to an acceptable level.

VI. RESEARCH CHALLENGES

Encryption and signature schemes are fundamental cryptographic tools for providing privacy and authenticity, respectively, in the public-key setting. Traditionally, these two important building-blocks of public-key cryptography have been considered as distinct entities that may be composed in various ways to ensure simultaneous message privacy and authentication [8]. Julian Zheng proposed a new cryptographic primitive named “signcryption" which simultaneously fulfills both the functions of digital signature and public key encryption in a logically single step, and with a cost significantly smaller than that required by signature followed by encryption. Signcryption is a cryptographic primitive which offers authentication and confidentiality simultaneously with a cost lower than signing and encrypting the message independently. Starting from signcryption, it has been developed extended schemas like ring signcryption. Ring signcryption enables a user to signcrypt a message along with the identities of a set of potential senders (that includes him) without revealing which user in the set has actually produced the signcryption. Thus a ring signcrypted message has anonymity in addition to authentication and confidentiality.
Ring signcryption schemes have no group managers, no setup procedures, no revocation procedures and no coordination: any user can choose any set of users (ring), that includes himself and signcrypt any message by using his private and

public key as well as other users (in the ring) public keys, without getting any approval or assistance from them. Ring Signcryption is useful for leaking trustworthy secrets in an anonymous, authenticated and confidential way [9].

Research along signcryption lines is open-ended.

ACKNOWLEDGMENT

Information security is the study and practice of protecting information. It's important because information is valuable. Organizations need data to conduct business. Governments need information to protect their citizens. Individuals need information to interact with businesses and government agencies. They also stay in touch with friends and family over the Web. Information is a critical resource that must be protected. The main goals of information security are to protect the confidentiality, integrity, and availability of information.

REFERENCES

[1] John Vacca, "Computer and Information Security Handbook", Publisher: Morgan Kaufmann

[2] Joanna Lyn Grama, "Legal Issues in Information Security", Publisher: Jones & Bartlett Learning

[3] Andy Oram; John Viega, "Beautiful Security", Publisher: O'Reilly Media, Inc.

[4] http://searchsecurity.techtarget.com/

[5] Yuliang Zheng, "Digital signcryption or how to achieve cost(signature & encryption) _ cost(signature) + cost(encryption)". In B.S. Kaliski Jr., editor, Proc. of Crypto '97,Springer-Verlag,1997.

[6] Nick Moldovyan; Alex Moldovyan "Innovative Cryptography", Publisher**:** Course Technology PTR.

[7] Tom St Denis "Cryptography for Developers", Publisher**:** Syngress.

[8] Yevgeniy Dodis, "Signcryption (Short Survey)", March 2005.

[9] S. Sharmila Deva Selvi, S. Sree Vivek?, C. Pandu Rangan , "On the security of Identity Based Ring Signcryption Schemes"

[10] http://en.wikipedia.org/wiki/Separation_of_duties

[11] http://en.wikipedia.org/wiki/Defense_in_depth_(computing)