Information and system security in computerized systems

Rurangwa Elias

Independent Institute of Lay Adventists of Kigali, P O Box 6392 Kigali-Rwanda

Email: rurangwa@gmail.com

Abstract

Security threats have recently become a redoubtable weapon against the dependability of computerized system of individual, organization and countrywide; many methods and mechanism have been proposed but still they are many challenges that current commercial solution and recent researches have not resolved. That is why the viruses, threats and other malwares are widespread. Among different security threats, the attackers who only have to find one security flaw to compromise the whole system are challenging because they don't follow rules; they cheat. They can attack a system using techniques the designers never thought of. The best security protocol ever invented can fall to an easy attack if no one pays attention to the more complex and subtle implementation issues (Bruce Schneier, 2008).

This paper passes through some important information security concepts and their possible threats. Thus, the needs of using downloaded or hard stored free or commercial software is necessary, this paper will propose the combination of digital signature scheme which is embedded in developed software with trusted third part that will ensure the dependability of the new features, therefore different threats coming from un-trusted channel will be eradicated.

Keywords— *Security mechanism, security services, security threats, malwares.*

1) Introduction

A. Background

Computer security is defined as the protection of computing systems against threats to confidentiality, integrity and availability. Thus, we can define security as the practice of ensuring that information is only read, heard, changed, broadcast and otherwise used really by people who have the right to do so. Information systems need to be secure if they are to be reliable. Since many businesses are critically reliant on their information systems for key business processes (e.g. websites, production scheduling, transaction processing), security can be seen to be a very important area for management to get right (Mark Stamp, 2011).

Security threats have recently become a redoubtable weapon against the dependability of computerized system of individual, organization and countrywide; many methods and mechanism have been proposed but still they are many challenges that current commercial solution and recent researches have not resolved. That is why the viruses, threats and other malwares are widespread.

2) Current security state

The day after day, most institutions, companies, and individuals become more and more dependent on software and computers. That arise the problem of securing their information. One known or unknown breach can harm the whole system and cause the catastrophic threat against confidentiality, integrity and availability of the system. It is so easy that hackers don't have to try very hard because most networks are poorly defended (Essam Al Daoud et al.). Eliminating the vulnerabilities exploited by these "easy" hacks will shrink the pool of successful hackers as the less skilled drop out. It will increase the cost for attackers, as they have to put more work into penetrating a target network. The recent studies show the following:

- More than 90% of successful breaches required only the most basic techniques.
- Only 3% of breaches were unavoidable without difficult or expensive actions.
- Outsiders were responsible for most breaches.
- 85% of breaches took months to be discovered; the average time is five months.
- 96% of successful breaches could have been avoided if the victim had put in place simple or intermediate controls.
- 75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching.
- One study found that antivirus software missed as much of 95% of malware in the first few days after its introduction.
- Another study found that 25% of malware is not detected by current techniques.

Hackers can avoid detection by making minor changes to their malware to evade detection, and some use the updates from security companies to see if their exploits can be detected by the latest updates (James A. Lewis, 2013).

The other study found that most of attacks are detected many months after by a third part.

This research attempt to present security issues and propose a new approach of securing a computer system by detecting a malicious software and validating a genuine one during installation process.

3) SECURITY GOALS, Attacks

An easy way to define security is to clearly identify and determine its goals. Confidentiality, integrity and availability are the three gaols of security; therefore we can classify all threats of security as a threat against confidentiality, integrity or availability. Security attacks are classified as either passive attacks, which include unauthorized reading of a message of file and traffic analysis or active attacks, such as modification of messages or files, and denial of service (William Stallings, 2011).

A. *Confidentiality*

Confidentiality deals with preventing unauthorized reading of information. This term covers two related concepts:

- *Data confidentiality*: Assures that private or confidential information is not available or disclosed to unauthorized individuals.
- *Privacy*: assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

A loss of confidentiality is the unauthorized disclosure of information. The attacks against confidentiality are of two types:

- *Snooping:* refers to unauthorized access to or interception of data. This may happen through different means like intercepting Internet communication between two persons or guessing what is written by a user by observing the hand movement or using a keylogger.
- *Traffic analysis*: refers other types of information collected by an intruder by monitoring online traffic.

Notice that snooping and traffic analysis are passive attack, in general the passive attack are difficult to detect, because they do not involves any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the message or observed the traffic pattern. However, it is feasible to prevent the success of these attacks by the means of encryption.

B. *Integrity*

Integrity deals with preventing, or at least detecting, unauthorized "writing" (i.e., changes to data).A loss of integrity is the unauthorized modification or destruction of information. The term integrity covers two related concepts:

- *Data integrity:* Assures that information and programs are changed only in a specified and authorized manner.
- *System integrity:* Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

The attacks against confidentiality are active attacks. They involve some modification of the data stream or the creation of a false stream. The following are the attacks against integrity:

- *Masquerading:* This kind of attack that takes place when one entity pretends to be a different entity. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. This can happen also when a user of IP protocol A sends a message that contains the destination IP Address of another user B. Here we pretend that the user A has spoofed the IP address of user B.
- *Replaying:* involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- *Modification of a message:* Means that some portion of a legitimate message is altered or that messages are delayed or reordered, to produce an unauthorized effect.
- *Repudiation:* Means that the sender of a message can deny it.

C. *Availability*

Availability deals with preventing denial of service to authorized users of the system. A loss of availability is the disruption of access to or use of information or an information system. The attack against availability is denial of service that prevents or inhibits the normal use or management of communication facilities.

4) SECURITY SERVICES

RFC2828 defines a security service as a processing or communication service that is provided by a system to give a specific kind of protection to system resource; security services implement security policies and are implemented by security mechanisms.X.800 divides these services into five categories .

D. *Authentication*

The authentication service is concerned by assuring that the communicating entity is the one that it claims to be. The mechanisms that put in place verify the identity of the user or computer system (William Stallings, 2011).

E. *Access control*

Access control concerns with being able to tell who can do what with which resource. In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications link. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual (William Stallings, 2011).

F. *Data confidentiality*

To keep a message secret to those that are not authorized to read it. Confidentiality is the protection of transmitted data from passive attacks.

G. *Data integrity*

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

H. *Nonrepudiation*

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

5) Information security Issues

I. *Problems*

In general, data and information in any information system is at risk from:

- *Human error:* e.g. entering incorrect transactions; failing to spot and correct errors; processing the wrong information; accidentally deleting data.
- *Technical errors*: e.g. hardware that fails or software that crashes during transaction processing.
- *Accidents and disasters:* e.g. floods, fire.
- *Fraud:* deliberate attempts to corrupt or amend previously legitimate data and information.
- *Commercial espionage:* e.g. competitors deliberately gaining access to commercially-sensitive data (e.g. customer details; pricing and profit margin data, designs).
- *Malicious damage*: where an employee or other person deliberately sets out to destroy or damage data and systems (e.g. hackers, creators of viruses and other malwares).

J. *Secure system*

There is no such thing as failsafe security for information systems. When designing security controls, a business needs to address the following factors;

- *Prevention:* What can be done to prevent security accidents, errors and breaches? Physical security controls are a key part of prevention techniques, as are controls designing to ensure the integrity of data.

- *Detection:* Spotting when things have gone wrong is crucial; detection needs to be done as soon as possible - particularly if the information is commercially sensitive. Detection controls are often combined with prevention controls (e.g. a log of all attempts to achieve unauthorized access to a network).
- *Deterrence*: deterrence controls are about discouraging potential security breaches.
- *Data recovery* - If something goes wrong (e.g. data is corrupted or hardware breaks down) it is important to be able to recover lost data and information.

K. *Business benefits of good information security*

Managing information security is often viewed as a headache by management. It is often perceived as adding costs to a business by focusing on "negatives" - i.e what might go wrong. However, there are many potential business benefits from getting information system security right: for example:

- If systems are more up-to-date and secure - they are also more likely to be accurate and efficient
- Security can be used to "differentiate" a business – it helps build confidence with customers and suppliers
- Better information systems can increase the capacity of a business. For example, adding secure online ordering to a web site can boost sales enabling customers to buy 24 hours a day, 7 days a week.
- By managing risk more effectively – a business can cut down on losses and potential legal liabilities

6) *Secure installation*

The softwares in their different forms are acquired in different manner, some are downloaded online and others are bound in different memory media. Because of their different origin, it is hard to grant their genuine and free from malwares like Trojan horse, worms, viruses or spyware. The use of public key cryptography can solve the computer malware problem. In this case all the developers must embed their digital signature within their software and they must prepare a certificate that is signed by a well known certificate authority as shown by the following figure. The developers of operating systems must offer a new procedure to copy, download and install the new software.

Public key certificates software authorization

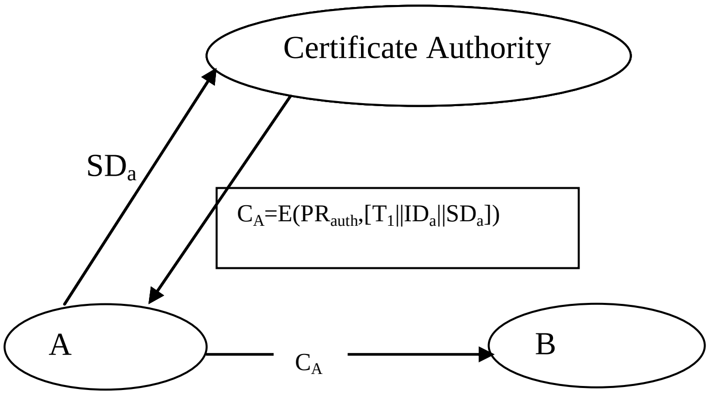
A certificate may consist of software digest generated by hash function ensures that the software cannot be modified and an identifier of the software owner, and the whole block signed by a trusted third party. Typically, the third party is certificate authority, such as a government agency or a financial institution; that is trusted by the user community. A user can present his or her public key to the authority in a secure manner and obtain a certificate. The certificate can be embedded in software and anyone can use or install the software after the system has verified that the certificate was created by the authority. The following are the requirements:

L. Any user can read a certificate to determine the name and software digest of the certificate's owner.

M. Any user can verify that the certificate originated from the certificate authority and is not counterfeit.

N. Only the certificate authority can create and update certificates.

O. Any participant can verify the currency of the certificate.



Application must be in person or by some form of secure authenticated communication. For participant A, the authority provides a certificate of the form

$$C_A=E(PR_{auth},[T_1||ID_a||SD_a])$$

Where $\boldsymbol{PR_{auth}}$ is the private key used by the authority and T is a timestamp. A may then pass this certificate on to any other participant, who reads and verifies the certificate as follows:

$$D(PR_{auth,}C_A)=D(PU_{auth,}E(PR_{auth},[T_1||ID_A||SD_a]))=(T||ID_A||SD_a)$$

The recipient uses the authority's public key, $PU_{auth,}$ to decrypt the certificate. Because the certificate is readable only using the authority's public key, this verifies that the certificate came from the certificate authority. The elements ID_A and SD_a provide the recipient with the name and software digest of the certificate's holder. The timestamp T validates the currency of the certificate.

B can be considered as the final user. B must compute a new digest of the owned software and verify if the computed digest is the same as the one comes with a certificate.

CONCLUSION

All security issues can be explained by using the concepts of confidentiality, integrity and availability. Some may require to combining two or three of them. The security threats are also classified as a threat against confidentiality, integrity or availability. Some of threats are the malwares that are sometimes embedded in softwares and are difficult to detect. The use of certificates and public key cryptography can solve the computer malwares problem because nothing will be installed without proving its genuine.

Are the developers able to certify their software system before releasing them?

REFERENCES

- Bruce Schneier,Why cryptography is harder than it looks,2008.
- Essam Al Daoud, Iqbal H. Jebril and Belal Zaqaibeh, Computer Virus Strategies and Detection Methods, 2008
- Srinivas Mukkamala, Andrew Sung and Ajith Abraham, Designing Intrusion Detection Systems: Architectures, Challenges and Perspectives
- James A. Lewis, Raising the Bar for Cybersecurity, 2013
- Mahbod Tavallaee, Natalia Stakhanova, and Ali Akbar Ghorbani, Toward Credible Evaluation of Anomaly-Based Intrusion-Detection Methods,2010
- Computer Virus Strategies and Detection Methods, Essam Al Daoud, Iqbal H. Jebril and Belal Zaqaibeh, 2008
- Mark Stamp, INFORMATION SECURITY Principles and Practice, Second Edition, 2011.
- William Stallings, Cryptography and Network Security, principles and practice, Fifth Edition,Pearson,2011
- R. Shirey, Internet Security Glossary, Request for Comments 2828, 2000
- ITU, International telecommunication union, x.800
- Yves Deswarte et Ludovic Me, Securite des reseaux et system repartis, 2003