IMPROVET

Information and Network Security

Miguel Soriano

Author: Miguel Soriano
Title: Information and Network Security
Published by: Czech Technical University in Prague
Compiled by: Faculty of Electrical Engineering
Contact address: Technicka 2, Prague 6, Czech Republic
Phone Number: +420 2 2435 2084
Print: (only electronic form)
Number of pages: 79
Edition: 1st Edition

ISBN 978-80-01-05297-6

Reviewed by: Gustau Raluy, Santiago Silvestre

Innovative Methodology for Promising VET Areas
http://improvet.cvut.cz

Lifelong Learning Programme

This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

EXPLANATORY NOTES

	Definition
	Interesting
	Note
	Example
	Summary
+	Advantage
–	Disadvantage

ANNOTATION

This module contains some necessary information for the basic orientation of students in the field of information and network security.

OBJECTIVES

This module provides some basic information about information and network security, i.e. how to ensure information and network security, how to protect a personal computer and how to mitigate different types of security threats. It also includes a brief overview of public-key and secret-key cryptography and algorithms. Lastly, some basic information on network security, including secure protocols firewalls and intrusion detection systems, as well as standard solutions for wireless networks security are provided.

LITERATURE

[1] Bruce Schneier: Applied Cryptography. John Kiley & Sons, Inc., New York, 1994

[2] William Stallings: Cryptography and Network Security. Principles and Practices. Prentice Hall, New Jersey, 2003

[3] Vesna Hassler: Security Fundamentals for E-Commerce. Artech House, Boston, 2001

[4] Rolf Oppliger: Internet and Intranet Security. Artech House, Boston, 2002

[5] Michael Sikorski, Andrew Honig: Practical Malware Analysis, The Hands-On Guide to Dissecting Malicious Software. No Starch Press, February 2012

[6] Michael Goodrich, Roberto Tamassia: Introduction to Computer Security, 2010

[7] John R. Vacca: Computer and Information Security Handbook (Morgan Kaufmann Series in Computer Security), 2009

[8] Jason Andress: The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Elsevier, 2011

Index

1 Introduction

1.1 Introduction

Information security is not just about stopping viruses, keeping hackers out and putting a lid on spam email. Information security is also about working with employees and management to make sure that everyone is aware of current threats and how they can protect their information and systems. The terms information security, computer security and network security are frequently used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Computer security is the generic name for the collection of tools designed to protect the processed and stored data and to thwart hackers.

Network security is the generic name for the collection of tools designed to protect data during their transmission.

In connection with the Internet, the term internet security is often used. Moreover, this term involves the concept of perimetric security which is the generic name for the collection of tools designed to protect the resources of a private network from users from other networks.

The differences among information security, computer security and network security lie primarily in the approach to the subject, the methodologies used and the areas of concentration. 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. Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer. Network security focuses on protecting data during their transmission.

1.2 The Causes of Insecurity

The insecurity of computer systems and networks goes much further than the well-known computer viruses, and has now become a priority. In the networked world, the new generation of vandals and data thugs do not need to have physical contact with the victim. Data can be easily copied, transmitted, modified or destroyed. As a result, the scene of crime is a particularly difficult one: there are no traces, identification of the culprits is nearly impossible, apprehension even more so and the legal framework does not make adequate provision for justice in this kind of crime.

The real-time nature of the Internet adds a further dimension to crime: it's instantaneous.

While many causes exist for security problems, at least three types of fundamental weaknesses open the door to security problems.

- Technology weakness
- Policy weakness
- Configuration weakness

Obviously, we could probably add human weakness and some others, but our purpose is to concentrate on those issues that, once recognized, can be managed, monitored, and improved within a security strategy.

Technology Weakness

Every technology has some known or unknown inherent weaknesses, or vulnerabilities that can be exploited by a sufficiently motivated troublemaker. Some weaknesses are publicized widely in the media because they are associated with a well-known product. Don't fall into the faulty logic that because you don't hear about the other products, they must be secure. The fact that no one cares enough to hack a product does not mean that it is necessarily secure.

Among others, we can mention the following weaknesses:

- Internet protocols were not designed for security. Today, security best practices, security services, and an array of products from many vendors work together to reduce the risks inherent in the environment.
- Computer and Network Operating Systems. Regardless of the manufacturer or whether it's an open standard or a proprietary product, every *operating system (OS)* has vulnerabilities that need to be addressed through patches, upgrades, and best practices.

- Network Device Weaknesses. Network devices can have vulnerabilities, often called "holes," that can be exploited. Whenever possible, patches, IOS upgrades, and best practices should be applied to eliminate or mitigate known problems.

Policy Weakness

Policy weakness is a catchall phrase for company policies, or a lack of policies, that inadvertently lead to security threats to the network system. The following examples are some of the policy issues that can negatively impact a business's computer system:

- No written security policy. The lack of a documented and adopted plan means the security efforts evolve and are enforced, if at all, in a best-effort manner.

- Lack of a disaster recover plan. Without a plan, the efforts to fight a network attack – or even a physical emergency such as a fire, flood, or earthquake – are left to the judgment and knowledge of the staff on hand. Even the best-trained and most experienced staff can make foolish decisions when faced with an unexpected catastrophic event.

- No policy for software and hardware additions or changes. Whether motivated by increasing productivity or recreation, any addition or upgrade to software or hardware can introduce unexpected security vulnerabilities. Adding an unauthorized wireless access point to a network can throw open a virtual garage door to the network and the company resources. Similarly, an unauthorized screensaver might also be harvesting passwords, user IDs, and other information for someone else.

- Lack of security monitoring**.** Even if a secure network is developed, failure to monitor logs and processes or weak auditing allow new vulnerabilities and unauthorized use to evolve and proliferate. The worst case would be not recognizing that a serious loss had occurred or was continuing.

- Employment policies**.** Frequent staff turnover, lower than typical compensation, and lack of training opportunities can all impact network security by bringing new untested and underskilled employees into positions of authority and responsibility.

- Internal policies**.** Lax business attitudes and practices often create temptations and a relatively safe environment for the opportunist within to ply their craft. This is the "we are all like family here" syndrome. Unfortunately, even some of the best families have a thief in their midst. Similarly, infighting, backbiting, power struggles, or turf struggles can lead to security issues or divert attention, allowing problems to go undetected.

Configuration Weakness

Many network devices have default settings that emphasize performance or ease of installation without regard for security issues. Installation without adequate attention to correcting these settings could create serious potential problems. Some common configuration issues include the following:

- Ineffective access control lists failing to block intended traffic
- Default, missing, or old passwords
- Unneeded ports or services left active
- User IDs and passwords exchanged in clear text
- Weak or unprotected remote access through the Internet or dial-up services

Monitoring vendor announcements and advisories, combined with industry news services, can identify the most common, best-known vulnerabilities and often include the appropriate mitigation solution.

1.3 Attacks classification

Security attacks can be characterized as the different sorts of systematic activities aimed at decreasing or corrupting the security. From this perspective, an attack can be defined as a systematic threat generated by an entity in an artificial, deliberate and intelligent way.

Computer networks may be vulnerable to many threats along many avenues of attack, including:

- Social engineering, wherein someone tries to gain access through social means (pretending to be a legitimate system user or administrator, tricking people into revealing secrets, etc.)
- War dialing, wherein someone uses computer software and a modem to search for desktop computers equipped with modems that answer, providing a potential path into a corporate network.
- Denial-of-service attacks, including all types of attacks intended to overwhelm a computer or a network in such a way that legitimate users of the computer or network cannot use it.
- Protocol-based attacks, which take advantage of known (or unknown) weaknesses in network services.
- Host attacks, which attack vulnerabilities in certain computer operating systems or in how the system is set up and administered.
- Password guessing; passwords are sequences of symbols, usually associated with a user name, which provide a mechanism for identification and authentication of a particular user. On almost all machines, the users themselves choose the passwords. This places the burden of security on end users who either do not know, or, sometimes do not care about sound security practices. As a general rule, passwords that are simple to remember, are, likewise, easy to guess. Attackers have several venues of guessing passwords and overcoming this obstacle.
- Eavesdropping of all sorts, including stealing e-mail messages, files, passwords, and other information over a network connection by listening in on the connection.

Security attacks may be divided into these two main categories:

- Passive attacks.
- Active attacks.

1.4 Passive attacks

Passive attacks attempt to learn or make use of information from the system but do not affect system resources. A passive attack is one where the attacker only monitors the communication channel. A passive attacker only threatens the confidentiality of data. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

Two types of passive attacks are related to message contents and traffic analysis:

- Eavesdropping**.** In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in the network to "listen in" or interpret (read) the data exchanged over the network. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, the data can be read by others as it traverses the network.

- Traffic analysis**.** It refers to the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.

Figure 1 shows the passive attack model

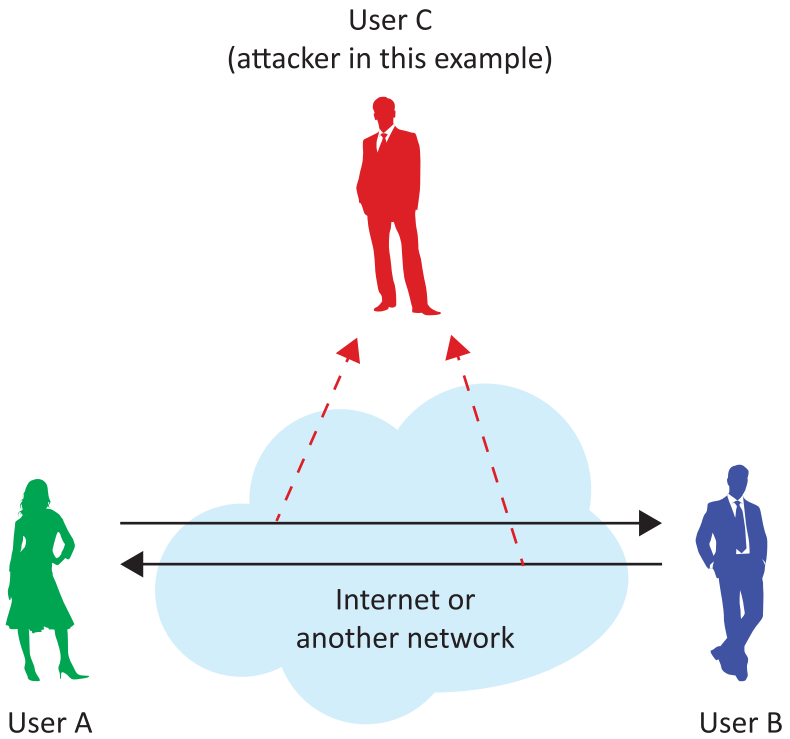

Fig. 1 – Passive attack model

1.5 Active attacks

Active attacks attempt to alter system resources or affect their operation. This type of attack is one where the adversary attempts to delete, add, or in some other way alter the transmission on the channel. An active attacker threatens data integrity and authentication as well as confidentiality.

Active attacks involve some modification of the data stream or the creation of a false stream and can be divided into six categories:

- **Masquerade.** It is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.
- **Replay.** In this kind of attack, a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits them, possibly as part of a masquerade attack.
- **Modification of messages**. The attacker removes a message from the network traffic, alters it, and reinserts it.
- *Man in the Middle* (**MitM**). In this kind of attacks, an intruder intercepts communications between two parties, usually an end user and a website. The attacker can use the information accessed to commit identity theft or other types of fraud.
- *Denial of Service* (**DoS**) and *Distributed Denial of Service* (**DDoS**). A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet [http://searchsecurity.techtarget.com/definition/botnet]) attack a single target.
- *Advanced Persistent Threat* (**APT**). It is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.

Figure 2 shows an example of an active attack (more specifically, a modification attack)

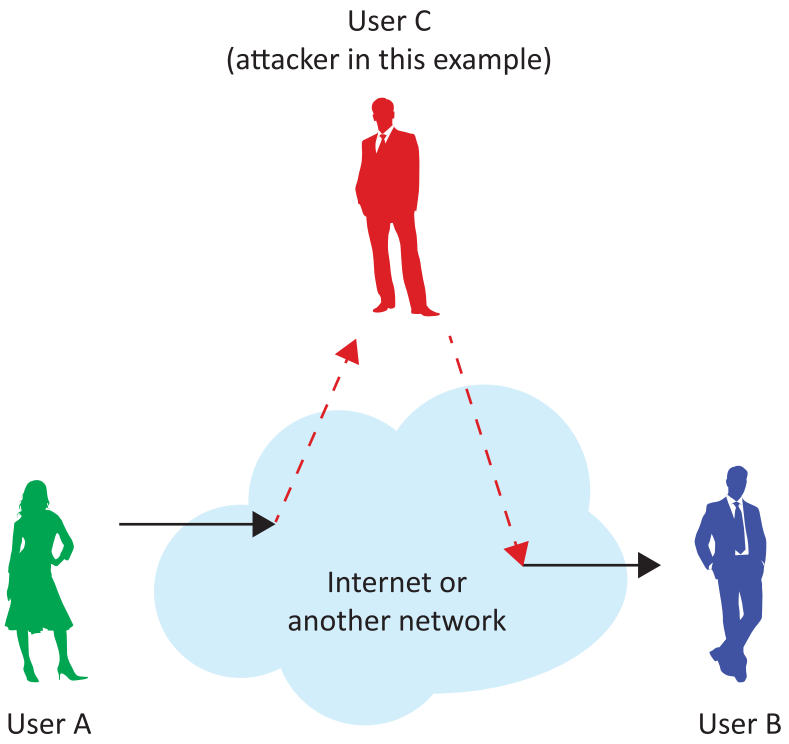

Fig. 2 – Modification active attack

1.6 Attackers: goals and behaviour

An attacker or an intruder is an individual who obtains, or who is trying to obtain, unauthorized rights or unauthorized access to the information system.

There exist many approaches on how to classify the attackers. The basic features used for the classification of the different types of attackers can be divided into the following three groups:

- The attacker's location with respect to the attacked system.
- How good the performed attack is.
- The aim - why the attack was performed.

From the point of view of the attacker's location, there exist two different kinds of attackers:

- Inside attacker or insider,
- Outside attacker or outsider.

An **Insider** is, in general, a person who has access to the internal computer network, and is therefore a legitimate user, but attempts to obtain unauthorized access to the data, system resources and services or misuses any authorized data.

An **Outsider** is generally a person who does not have authorized access to the internal computer network and wishes to enter into that network by using any vulnerable locations or security holes.

Depending on how good the performed attack is, the attackers can be divided into these two main groups:

- Amateurs.
- Professionals.

The group of amateurs carries out less dangerous attacks than professionals do. These attacks are in keeping with the low level of training and instrumentation of the attackers.

The group of professionals usually consists of top computer specialists, who have access to specialized resources and who are highly trained and skilled. In practice, that means they are able to generate very dangerous attacks with serious consequences for the computer systems and networks.

A very discussed matter when it comes to attackers' classification is the division of the attackers into the following two groups:

- Hackers,

- Crackers.

A **Hacker** is a person with good or excellent IT skills who is often involved in important software projects and whose knowledge and know-how are useful in finding any vulnerabilities and security holes of the designed systems. The hacker's activity is helpful and useful. There are even codexes on hackers which describe their behaviour.

A **Cracker** is someone who has the ability to defeat anti-piracy protections of computer programs and who uses their knowledge in an unethical way. However, there are more definitions of this group of attackers that emphasize the different scope of their activities.

There exist also other groups of attackers, the largest one being called **scriptkiddies**. This group of attackers consists of users with low IT skills. The attacks performed by these attackers exploit the scripts containing the codes aimed at misusing the vulnerabilities of the IS. The attackers apply these scripts to the IS without carrying out a deep analysis, but the harmful effects of this activity usually have serious consequences. These are the most frequent and dangerous attacks.

1.7 How can you protect yourself?

This section recommends the following practices to home users

Use strong passwords

Passwords are often the only protection used on a system. A user ID is only a name and does not verify identification, but the password associated with the user ID works as an identifier. Therefore, passwords are the keys to your network, and you should protect them as such. Firewalls and intrusion detection systems mean nothing if your passwords are compromised.

A strong password is one that cannot be found in any dictionary – English or foreign. It also means a password that is not easily guessed. Longer passwords are harder to guess or crack than short passwords are.

Following is a list that can be used to set strong passwords:

- **Use a nonsensical combination of letters:** The best passwords appear to be sheer nonsense. For example, if we take the phrase, "Don't expect me to behave perfectly and wear that sunny smile" and we use just the first letter of each word, our password would appear to be *demtbpawtss*.

- **Include a mix of upper- and lowercase letters:** The password should include an uppercase letter somewhere other than at the beginning and also include a number.

- **Longer passwords are better:** The password should be at least 8 characters long.

- **The passwords should be changed periodically:** Even the best passwords should be changed regularly (every 60 days or so) to prevent its being used long term if it is cracked. Many operating systems enable you to set this rule for each user. The user will most likely find this practice inconvenient, but it is smart security.

- **Set new passwords instead of reusing the same ones over and over again:** The same password should not be used again by a user within the same year or even 18 months.

- **Do not use a set of characters straight off the keyboard:** The use of passwords like *qwerty, 12345678,* or *asdfghj* must be avoided. Even though they look nonsensical, they follow a distinct pattern of consecutive keys on the keyboard and password crackers will break them in seconds.

- **Treat the passwords as top-secret information:** All passwords should be protected and not shared! Many users write their passwords on sticky notes attached to their computers or put them under their keyboards. That is not fooling anyone!

Root and administrative level passwords are the keys to the kingdom for an intruder. System administrators with *root* privileges – that is, with no access restrictions and the ability to make any sort of changes – should therefore have the hardest passwords and the most stringent rules about changing and reusing them. It is recommended to follow these guidelines:

- Write down all root passwords and store them in a safe: Then, if an administrator is incapacitated for a time or leaves the job suddenly, the password is not lost forever. Password recovery programs are available, but you do not really want to rely on them in an emergency.

- Change ALL user passwords if there is a suspicion that a root password has been compromised**:** It is not possible to guarantee that the all the passwords have not been stolen if an unknown person has a root or administrative level password.

Likewise, if a general user suspects that a password has been stolen or compromised, that user should change the password immediately and notify those in authority at the company.

Always use virus protection software

Anti-virus software is not always 100 percent effective but it is better than no protection at all. Most common viruses are not obvious to the user, so if a user does not have any antivirus, he probably does not know that his computer is infected.

Anti-virus software consists of two parts: the *scanning engine* and the *signature files*. It is necessary to regularly update both the scanning engine and the signature files on a regular basis or the anti-virus software will lose its effectiveness. The software program usually has an *update* command, or can be checked at the vendor's Web site for updates.

The scanning engine tells the software how and where to scan, and the signature files are essentially a database of known viruses and their actions. The scanning engine compares files on your computer to the known viruses in the signature files. The signature file contains the patterns of known viruses. Anti-virus software is prone to false positives, but that is a small inconvenience for the protection it affords you.

When new viruses are found, anti-virus software vendors issue updates to their signature files to include the new strain. Occasionally, the scanning engine itself needs updating, too. If one part of the program is updated and the other part is obsolete, it will simply not work properly.

In order to achieve maximum protection, it is necessary to install the anti-virus software on individual workstations as well as on all the servers and other computers on the network. That is the only way to detect viruses at all entry points. All removable media, such as USB pen drives, CDs, ... should be scanned before used on a system. If the anti-virus software is installed on the Internet gateway servers, the software can catch viruses coming in from outside connections.

Always change default configurations

Installing a system right out of the box and leaving it with the default configuration is probably one of the most common mistakes that people make when setting up a network. Default configurations often have default administrative accounts and passwords that hackers the world over know. This applies to routers, hubs, switches, operating systems, e-mail systems, and other server applications, such as databases and Web servers.

In addition to having known passwords on computers, default configurations contain multiple security holes that should be patched. Before putting any computer online, the default account names and the passwords should be changed and all security patches should be applied. A little bit more time spent on a computer at this point can save a lot of grief later.

Figure 3 shows an example of default passwords in some routers.

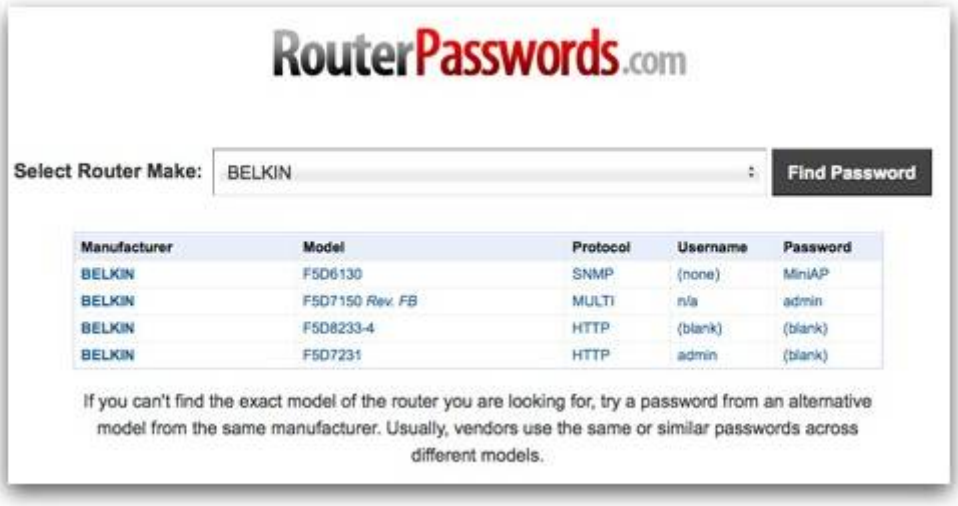

Fig. 3 – Example of default router passwords

Use a firewall

The use of some type of firewall product is strongly recommended. Intruders are constantly scanning home user systems for known vulnerabilities. Network firewalls (whether software or hardware-based) can provide some degree of protection against these attacks. However, no firewall can detect or stop all attacks, so it is not sufficient to install a firewall and then ignore all other security measures.

Do not open unknown email attachments

Before opening any email attachments, you must make sure you know the source of the data. It is not enough that the mail originated from a recognized address. The Melissa virus spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing programs.

When opening an attached file, it is important to observe the following procedure:

1. make sure the virus definitions are up-to-date
2. save the file on the hard disk
3. scan the file using an antivirus software
4. open the file

For additional protection, you can disconnect your computer's network connection before opening the file.

Following these steps will reduce, but not wholly eliminate, the chance that any malicious code contained in the attachment might spread from your computer to others.

Do not run programs of unknown origin

Never run a program unless you know it to be authored by a person or company that you trust. Also, do not send programs of unknown origin to friends or coworkers simply because they are fun – they may contain a Trojan horse program.

Keep all applications, including the operating system, patched

Vendors usually release patches for their software when a vulnerability has been discovered. Most product documentation offers a method to get updates and patches.

Some applications will automatically check for available updates, otherwise it is absolutely necessary to check periodically for updates.

Turn off your computer or disconnect from the network when not in use

Turn off your computer or disconnect its network interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.

Make regular backups of critical data and create boot disk

Keep a copy of important files on removable media. Use software backup tools if available, and store the backup disks somewhere away from the computer. Moreover, to assist in the recovery from a security breach or hard disk failure, it is very convenient to create a boot disk on a CD that will help when recovering a computer after such an event has occurred. Obviously, this CD should be created before you have a security event.

1.8 Summary

In this chapter, we first have introduced some important concepts: information security, computer security and network security, and the differences among these concepts. Secondly, we have presented some causes of insecurity of information and classified security attacks and attackers types according to different criteria. Finally, we have included a section with some of the best practices for home users so as to increase their level of protection.

2 Malicious software and antivirus

2.1 Concept of malicious software (malware)

Malicious software (**malware**) is a generic term to refer to any malicious or annoying software installed in the system which is designed to exploit a computer by carrying out unwanted actions without the user's consent.

The execution of malware can cause the disruption of computer operations and can be also used to gather sensitive information or gain unauthorized access to computer systems. Malware is not the same as defective software, which is software that has a legitimate purpose but contains harmful bugs that were not noticed before release.

In fact, computer viruses are actually a subset within the larger malware family, like other specimens such as worms, Trojan horses, adware, spyware, adware, rootkits, etc...

Nowadays, most of the malware is distributed via the Internet. One of the most common methods is known as the "drive-by download". It downloads and runs the malicious file, for example through the Web or executing an attachment received via email, like a malicious PDF file. In many cases, the user is deceived into believing that a certain program or data is useful for them; for example, for a software to play video. In other instances, the infection is hidden to the user, who just has to visit a Web page that takes advantage of vulnerabilities in the Web browser to download and execute the malware. However, nearly any Internet protocol can be used to distribute malware, for example, P2P or instant messaging. Moreover, it is important to remember that physical storage devices can propagate malware; the distribution through USB pen drives is very common.

2.2 Anti-virus software

Antivirus or anti-virus software is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worms, trojan horses, spyware and adware. In order to be effective, anti-virus software should be regularly updated - otherwise it will fail to give protection against new viruses.

Eradicating a virus is the term used for cleaning out a computer. There are several methods of eradication:

- Removing the code in the infected file which corresponds to the virus;
- Removing the infected file;
- Quarantining the infected file, which involves moving it to a location where it cannot be run.

A variety of strategies are typically employed.

Signature-based detection involves searching for known patterns of data within executable code. Viruses reproduce by infecting "host applications," meaning that they copy a portion of executable code into an existing program. So to ensure that they work as planned, viruses are programmed to not infect the same file multiple times. To do so, they include a series of bytes in the infected application to check if it has already been infected- this is called a virus signature. Antivirus programs rely on this signature, which is unique to each virus, in order to detect them. This method is called signature based detection, the oldest method used by antivirus software. However, this method cannot detect viruses which have not been archived by the publishers of the antivirus software. What's more, virus programmers have often given them camouflage features, making their signature hard to detect, if not undetectable. To counter such threats, heuristics detection approach can be used.

One type of heuristic approach, generic signatures, can identify new viruses or variants of existing viruses by looking for known malicious code, or slight variations of such code, in files. The heuristic method involves analysing the behaviour of applications in order to detect activity similar to that of a known virus. This kind of antivirus program can therefore detect viruses even when the antivirus database has not been updated. On the other hand, they are prone to triggering false alarms.

No matter how useful antivirus software is, it can sometimes have drawbacks. Antivirus software can impair a computer's performance. Inexperienced users may also have trouble understanding the prompts and decisions that antivirus software presents them with. An incorrect decision may lead to a security breach.

2.3 Categorization of malware

Malware can be classified in different ways according to different criteria: distribution mechanisms, system installation methods, the way they are remotely controlled, etc. Nowadays, malware specimens usually have many features, so they are usually classified according to their main feature. For example, there could be a Trojan horse with rootkit capabilities able to remain hidden from expert users and security solutions. It could also be a boot in a network of infected computers that are remotely controlled. At the same time, it could make advertisements appear and capture keystrokes, so it would also be part of the adware and keylogger families. That is, it would be a Trojan horse-rootkit-bot-adware-keylogger... All in one! In fact, this example is quite common.

A first classification of malware is based on the need of a host file for propagation.

The following four kinds of malicious software correspond to the malicious software needing host files for propagation:

- Trap doors,
- Logic bombs,
- Trojan horses,
- Viruses.

Figure 4 shows the distribution of malware by categories (source: Panda Security)

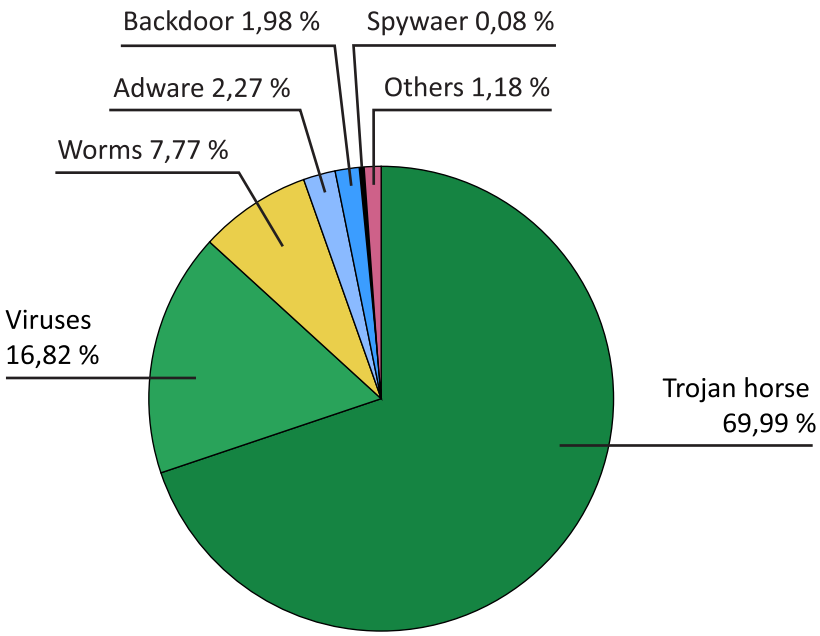

Fig. 4 – Malware distribution by categories

Two kinds of malicious software that do not need a host file for propagation are:

- Worms,
- Zombies.

Trap doors are secret entries into the program which can allow access to the system without going through the security mechanisms. These approaches are used by programmers during the program debugging. The trap doors help avoid the authentication mechanisms during the program debugging and testing and it is then when the programmer can obtain special privileges. These trap doors are searched by malicious software and can be used for the avoidance of the security mechanisms. This results into a serious software threat to the computer system.

Logic bombs are the oldest kind of malicious software, what poses a software threat. This is software integrated into a legitimate program which is activated after the fulfillment of some conditions. One example of these conditions can be the presence or absence of a specific file in a preset day, week or date for the start of a certain application. Logic bomb can cause loss or damage in the IS, for example it can erase some files, stop running computing applications and so on…

Trojan horses are programs or commands that perform useful procedures or processes but at the same time, they conduct malicious activities on the background, such as data erasing. A special example of this kind of malicious software is spyware, which collects passwords entered on the keyboard,

information about visited web pages, the kind of software that is being used on the computer and the information that has been sent through the Internet.

Viruses are programs that attach themselves to other programs or files and can perform unauthorised effects. For their propagation, the hosted file is needed which can be modified by the virus. Viruses can attack other files, propagate themselves and corrupt IS.

A worm can propagate from one computer system to another if the two systems are interconnected by the network. The worm propagation is mainly performed by using e-mail clients or through the services offered by these clients.

A zombie is a malicious software that is propagated through the network. After its successful penetration into a computer system, the infected computer can be remotely controlled and administered. When several computers are infected by the same sort of malicious software, this is known as botnet. The botnet can be controlled from one remote computer and force infected computers to carry out the same orders. This enables **DDoS** *(Distributed Denial of Service)* attack.

2.4 Virus lifecycle

Virus lifecycle consists of four phases:

- Dormant phase,
- Propagation phase,
- Triggering phase,
- Execution phase.

In the dormant phase, the virus remains inactive, so it does not perform any activity at all. It is necessary to note though that not all viruses have this phase in their lifecycle.

In the propagation phase, the virus places an identical copy of itself into another program or into certain areas on the disk. Each infected program contains now a clone of the virus, which is able to propagate itself.

In the triggering phase, the virus is activated. This phase can be initialized by different conditions or states of the infected program.

In the execution phase, the virus performs the activity that was programmed during the virus creation. These are usually destructive activities which can cause the loss and damage of the information contained in the infected computer system.

2.5 Summary

In this chapter, we have introduced the concept of malicious software and classified different types of malware based on various criteria: propagation, installation method, main feature and so on. Moreover, we have explored the phases of the life cycle of a virus. Furthermore, the chapter describes several techniques for cleaning out an infected computer. Since these techniques require the detection of malware, we have introduced different strategies commonly used for detection.

3 Security services and security mechanisms

3.1 Security services

A security service is a service that ensures adequate security of the systems or of data transfers. Security services are implemented by security mechanisms according to security policies.

For over twenty years, information security has held *confidentiality, integrity and availability* (known as the **CIA** triad) to be the core principles of information security.

Later, other elements of information security were added to the three classic security attributes of the CIA triad. These elements are **authentication, acccess control, non-repudiation, and privacy.** Nevertheless, this classification is subject of debate among security professionals.

3.2 Confidentiality

Confidentiality refers to the protection of information from disclosure to unauthorized entities (organizations, people, machines, processes). No one may read the data except for the specific entity (or entities) intended. Information includes data contents, size, existence, communication characteristics, etc.

Confidentiality is a requirement

- When data is stored on a medium (such as a computer hard drive) that can be read by an unauthorized individual.
- When data is backed up onto a device (such as a tape) that can fall into the hands of an unauthorized individual.
- When data is transmitted over unprotected networks.

Furthermore, given the sophistication and power of determined adversaries today, **cryptographic techniques** for providing confidentiality must be employed for all sensitive data. As with data integrity, this requires a common understanding between entities of appropriate algorithms and keys.

3.3 Data integrity

Data integrity is the protection of data against creation, alteration, deletion, duplication or re-ordering by unauthorized entities (organizations, people, machines, processes). Integrity violation is always caused by active attacks. More specifically, integrity refers to the trustworthiness of information resources.

Data integrity is the assurance of non-alteration: the data (either in transit or in storage) has not been undetectably altered whether by accident or deliberately malign activity. Clearly, such assurance is essential in any kind of business or electronic commerce environment, but it is desirable in many other environments as well.

The integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong. In order to thwart deliberate data manipulation by a determined adversary whose goal is to modify the content of the data for his or her own gain, **cryptographic techniques** are required. Thus, appropriate algorithms and keys must be employed and commonly understood between the entity wanting to provide data integrity and the entity wanting to be assured of data integrity.

3.4 Availability

Availability means having timely access to information. For example, a disk crash or denial-of-service attacks both cause a breach of availability. Any delay that exceeds the expected service levels for a system can be described as a breach of availability. An information system that is not available when you need it is at least as bad as none at all. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure.

Availability, like other aspects of security, may be affected by purely technical issues (e.g., a malfunctioning part of a computer or communications device), natural phenomena (e.g., wind or water), or human causes (accidental or deliberate).

While the relative risks associated with these categories depend on the particular context, the general rule is that humans are the weakest link. (That is why each user's ability and willingness to use a data system securely are critical.)

3.5 Authentication

The authentication service is concerned with assuring that the communicating entities are provided with assurance and information of relevant identities of communicating partners (people, machines, processes).

In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purpose of unauthorized transmission or reception.

3.6 Access control

Access control is the protection of information resources or services from access or use by unauthorized entities (organizations, people, machines, processes). That is to say, access control refers to the prevention of unauthorized use of a resource (i.e., this service controls who can have access to certain resources, under what conditions access can occur, and what those accessing the resources are allowed to do).

To achieve this service, each entity trying to gain access must be first identified, or authenticated, so that access rights can be tailored to the individual. In order to better understand access control it is important to define the following concepts:

- Privileges – rights to access or use resources or services
- Principles – entities own access control privileges
- Subjects – entities exercise access control privileges
- Objects / Targets – resources or services accessed/used by subjects
- Delegation – transfer of access control privileges among principals
- Authorization – transfer of access control privileges from principals to subjects

The *Access control lists* (**ACLs**) are the most typical protection mechanism used to offer this service.

3.7 Non-repudiation

Secure communications need to integrate a service in charge of generating digital evidence in order to resolve disputes arisen in case of network errors or entities' misbehaviour when digital information is exchanged between two or more participants.

Non-repudiation is the security service that uses these evidences to provide protection against denial by one of the entities involved in a communication of having participated in all or part of that communication.

Non repudiation is the security service 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.

It includes non-repudiation of origin (i.e. proof that the message was sent by the specific party) and non-repudiation of reception (i.e. proof that the message was received by the specific party).

- **NRO** *(Non-repudiation of origin)* provides evidences to receivers that the message was sent by the claimed sender. This evidence or proof
- **NRR** *(non-repudiation of receipt)* provides evidences to senders that the intended recipient received the message.

The typical protection mechanisms are: notarization, timestamp, digital signatures and confirmation services.

3.8 Data Privacy

Data privacy is the security service that allows an individual to maintain the right to control what information about him is collected, how it is used and who uses it.

In an open network such as the Internet, the increased ability to share information can lead to new ways in which privacy can be breached; new technologies can create new ways to gather information, which may have some negative implications for retaining privacy. The use of data mining and the advent of various search engines has created a capability for data about individuals to be collected and combined from a wide variety of sources very easily.

There is so much information stored in many databases worldwide that an individual has no practical means of knowing of or controlling all of the information about themselves that others may have hold or access. Such information could potentially be sold to others for profit and/or be used for purposes not known to or sanctioned by the individual concerned. The concept of information privacy has become more significant as more systems controlling more information appear.

On the Internet, privacy, a major concern of users, can be divided into these concerns:

- What personal information can be shared with whom.
- Whether messages can be exchanged without anyone else seeing them.
- Whether and how one can send messages anonymously.

Moreover, as location tracking capabilities of mobile devices are increasing, problems related to user privacy arise, since user's position and preferences constitute personal information and improper use of them violates user's privacy.

There are many ways to protect the user's privacy on the Internet. For example, e-mails can be encrypted and browsing of webpages, as well as other online activities, should be done traceless via anonymizers, so called mix nets. These mix nets can be used to prevent the Internet service providers from knowing which sites one visits and with whom one communicates.

3.9 Security mechanisms

Security mechanism is a process that implements security services based on a hardware (technical), software (logical), physical or administrative approach. Security mechanisms support the security services and execute specific activities for the protection against attacks or attack results.

The security mechanisms are divided into those that are implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service.

To the basic mechanisms of enciphering belong:

- Encipherment
- Digital signature
- Access control
- Data integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarization

Encipherment is a mechanism aimed at protecting a message's information content by using mathematical algorithms that transform data into a form that is not readable by unauthorized subjects.

Digital signature is the mechanism that uses the cryptographic transformation of a data unit to prove the source and integrity of the data unit and protect against forgery.

Access control covers a variety of mechanisms that enforce access rights to resources. This mechanism involves authorization to access some resources.

Data integrity covers a variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication exchange is a mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic padding is a mechanism that inserts bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing control enables selection of particular physically secure routes for certain data and allows routing changes, especially when a security breach is suspected. This mechanism also involves perimeter security.

Notarization is a mechanism that uses a trusted third party to assure certain properties of a data exchange.

Perimeter security is a mechanism that allows accepting or denying data from or to a particular address or service located outside of the local network. Security service – security mechanism mapping.

3.10 Security Service – Mechanism mapping

Single security services may need to be implemented by multiple and different security mechanisms. The following illustrates the relationship between security services and security mechanisms.

	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Authentication	√	√			√			
Access control			√					
Confidentiality	√					√	√	
Data integrity	√	√		√				
Nonrepudiation		√		√				√
Availability			√	√				
Privacy	√					√	√	

Fig. 5 – Security services and mechanisms

3.11 Summary

Communications require the integration of different services in order to ensure adequate security of data transfers. In this chapter, we have presented the most important security services (confidentiality, integrity, availability, authentication, access control, non-repudiation and privacy) and introduced the security mechanisms needed to provide such services. Basically, these security mechanisms are: encryption, digital signatures, access control, data integrity, authentication exchange, traffic padding, routing control and notarization. Finally, we have established a connection between security services and mechanisms.

4 Basics of cryptography

4.1 Introduction

Cryptography is a mathematical study dealing with methods of secretion of messages into forms which prevent unauthorized entities from understanding of the meaning. . Many security applications are, in fact, based on the use of cryptographical algorithms to encrypt and decrypt data.

Encryption is a process (transformation) of changing data so that if an unauthorized person accesses the encrypted data, this data will be unrecognizable and useless. Decryption is converting data back to its original form.

Cryptographic system (comprising encryption, decryption and key) enables to store sensitive information or transmit it across insecure environments (like the Internet) so that it cannot be read by anyone except the intended recipient. Cryptography has now become an industry standard for providing information security, trust, controlling access to resources, and electronic transactions.

This technique is used in everyday actions, such as making or receiving a call from a mobile phone, paying with a credit or debit card, withdrawing money from an ATM or logging on to a computer with a password.

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with one or several keys – a word, number, or phrase – to encrypt plaintext. The same plaintext encrypts to different ciphertext when different keys are used. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

A strong cryptographic algorithm needs to fulfill the following criteria:

- There must be no way to find the plaintext (clear data) if the key is unknown, except brute force, i.e. by trying all possible keys until the right one is found.
- The number of possible keys must be so large that it is computationally infeasible to actually stage a successful brute force attack a reasonable length of time.
- Anything done by encryption must be undone during decryption using the same key.
  In this book, we will examine **what encryption does**. We will introduce the basic concepts in encryption and study the encryption model. However, it is **out of the scope** of this document:
  - **how encryption works**, basic principles to design encryption algorithms.
  - **how encryption can fail**, how encryption algorithms can be broken using cryptanalysis.

4.2 Classification of cryptographic algorithms

Cryptographic algorithms can be classified as:

Symmetric key or secret key algorithms where only one key is used for both encryption and decryption. The *Advanced Encryption Standard* (**AES**) is an example of a conventional cryptosystem widely employed.

Public key or asymmetric key algorithms where a pair of keys is used: a public key, which encrypts data, and a corresponding private, or secret, key for decryption. Although the two keys of the same pair are mathematically linked, it is computationally infeasible to derive the private key from the public key. A user or *entity* publishes their public key to the world while keeping their private key secret. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.

The primary benefit of public key cryptography, cryptographical systems (cryptosystems) based on asymmetric key algorithms, is that it allows entities (for instance, people), which (who) had no preexisting security arrangement, to exchange messages securely. The sender and the receiver do not need to share any secret keys via secure channels; all communications involve only public keys, and no private key is ever transmitted or shared.

4.3 Terminology

Plaintext is the message that has to be transmitted to the recipient. It is also commonly referred to as *cleartext*.

Ciphertext is the output that is generated after encrypting the plaintext.

Encryption is the process of changing the content of a plaintext in such a manner that it hides the actual message.

Decryption is the reverse of encryption; it is the process of retrieving the plaintext message from its encrypted form (ciphertext). This process converts ciphertext to plaintext.

Key is a word, number, or string that is used to encrypt the plaintext or to decrypt the ciphertext.

Cryptanalysis is the science of breaking codes and ciphers.

Hash algorithm is an algorithm that converts a text string of arbitrary length into a string of fixed length.

Cipher is a cryptographic algorithm, i.e. a mathematical function used for encryption and decryption.

Decipher converts enciphered text to the equivalent plain text by means of a cipher system.

Key Management - Process by which key is generated, stored, protected, transferred, loaded, used, and destroyed.

4.4 Symmetric Key Cryptography

The process of encryption and decryption of information by using a single key is known as secret key cryptography or symmetric key cryptography. In cryptographic systems based on symmetric key, the keys used to encrypt the plaintext and to decrypt the ciphertext may be identical (usual situation) or there may be a simple transformation to go between the two keys. The main problem with symmetric key algorithms is that the sender and the receiver have to agree on a common key. A secure channel is also required between the sender and the receiver to exchange the secret key.

4.5 How Does the Secret Key Cryptography Work?

The process of using symmetric key cryptography is as follows: User A wants to send a message to User B and wants to ensure that only User B is able to read the message. To secure the transmission, User A generates a secret key, encrypts the message with this key, and sends the message to User B. User B needs that secret key to read the encrypted message. User A can give the secret key to User B by using any means available. After User B receives the secret key, he or she can decrypt the message to retrieve the original message.

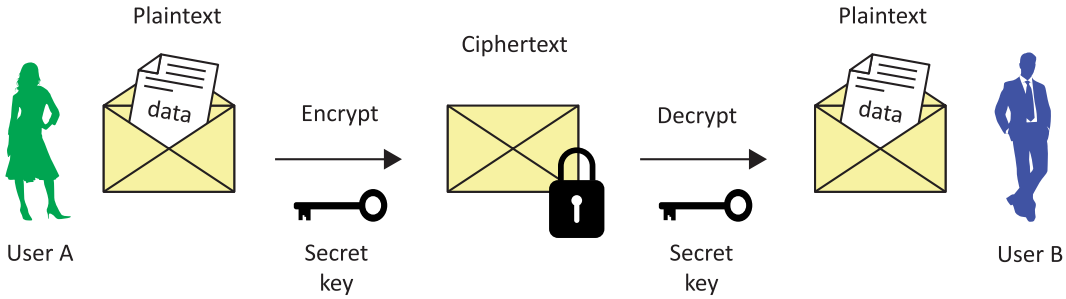

Fig. 6 – Symmetric key encryption model

The properties that a cipher algorithm must fulfill are the following:

- **Diffusion:** each bit of the plaintext influence many ciphertext bits and each ciphertext bit is affected by many plaintext bits,
- **Confusion:** it is necessary to avoid structured relationships (especially linearity) between plaintext and ciphertext/key that are exploited in known attacks.
- Ciphertext should be random-looking and have good statistical properties.
- **Simplicity.**
- **Efficiency:** extremely fast in hardware & software on wide variety of platforms.

The most widely used secret key algorithms include:

- *Data Encryption Standard* (**DES**)
- *Advanced Encryption Standard* (**AES**)

The major problem with symmetric cryptography is that the process of transferring keys to the recipient is prone to security risks. Establishment of a *secure channel* is not a trivial operation as sending the key via Internet in an e-mail is not secure, verbally communicating the key over a phone line runs the risk of eavesdropping. Similarly, snail mail runs the risk of possible interception.

The security risks that are involved in secret key cryptography have been overcome to a large extent by using public key cryptography. Secret key cryptography is often used to encrypt data on hard drives. The person encrypting the data holds the key privately and there is no problem with key distribution.

4.6 Public Key Cryptography

The cryptographic systems based on public key evolved to address the security issues posed by symmetric cryptosystems. This method solves the problem of secret key cryptography by using **two keys** instead of a single key. Public key cryptography uses a pair of keys. In this process, one key is used for encryption, and the other key is used for decryption.

This process is known as public key cryptosystem (also denoted as cryptography) or asymmetric cryptosystem because both the keys are required to complete the process. These two keys are collectively known as the **key pair**. In asymmetric cryptography, one of the keys is freely distributable. This key is called the **public key** and is used for encryption. Hence, this method of encryption is also called public key encryption. The second key is the **secret or private key** and is used for decryption. The private key is not distributable. This key, like its name suggests, is private for every communicating entity. It is important to point out that the public and private keys are related, but it is virtually impossible to deduce the private key if you know the public key.

The most common public key algorithm is **RSA**, which name is created as an abbreviation of the first letters of its authors' surnames; *Rivest, Shamir, Adleman.*

4.7 How Does the Public Key Cryptography Work?

Using public key encryption to provide confidentiality

Let us take an example where User_B wants to send a message to User_A. User_B encrypts the message with User_A's public key, and User_A decrypts the message using his or her private key. Since the key pairs are complementary, only User_A's private key can decrypt this file. If someone else intercepts the ciphertext, they will be unable to decrypt it, because only User_A's private key can be used for decryption. This method does not provide any authentication that the message is coming from User_B, because User_A's public key is known to the world. However, it does provide confidentiality to the message, as only User_A can decrypt the message.

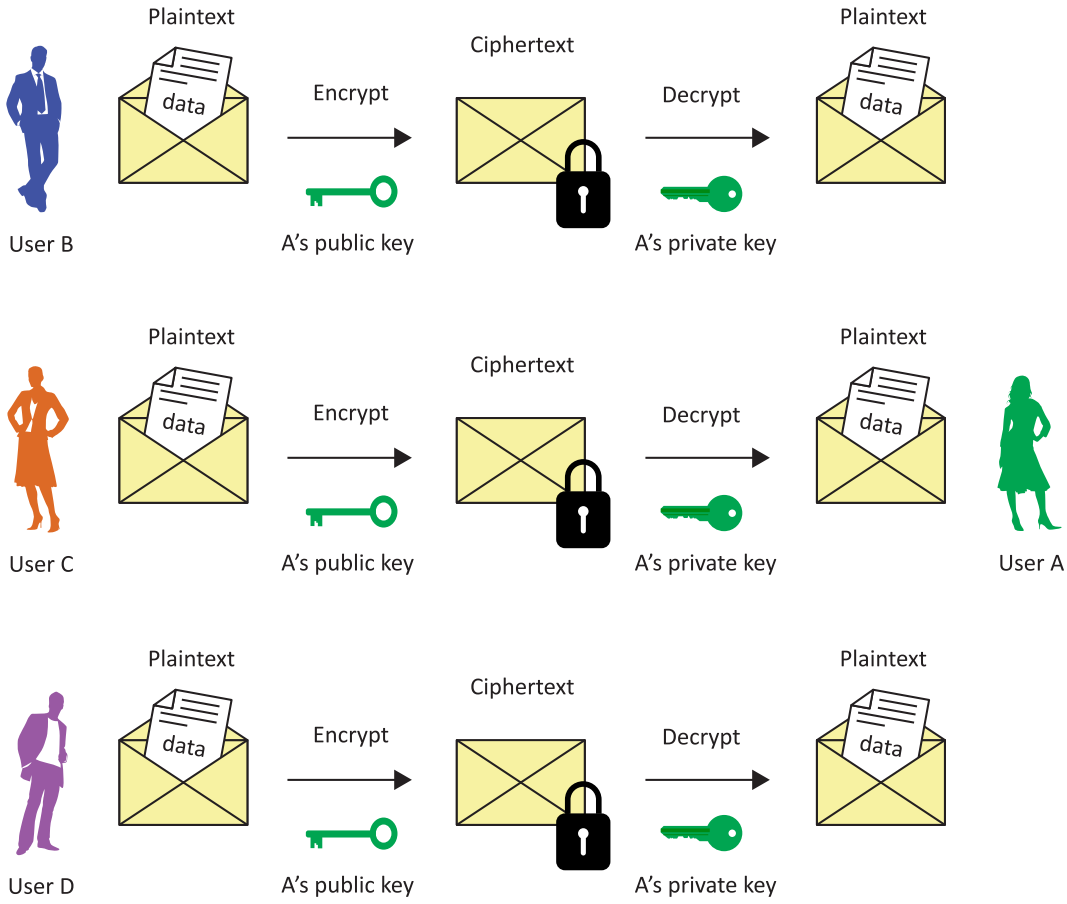

Fig. 7 – Public-key encryption model (to provide confidentiality)

This method very clearly indicates that the data you send to a user can only be encrypted by the public key of the recipient if confidentiality is required. Similarly, the decryption can be done only by the private key, which is supplied by the recipient of the data. Therefore, messages can be exchanged securely. The sender and receiver do not need to share a key, as required for symmetric

encryption. All communications involve only public keys, and no private key is ever transmitted or shared.

Using public key encryption to provide authentication

To provide authentication, User_A must encrypt the message with his or her private key and User_B will decrypt the message with User_A's public key. This method will provide authentication that the message is coming from User_A but it does not provide confidentiality, because User_A's public key is known to all. Hence, anybody possessing User_A's public key could decrypt the message.

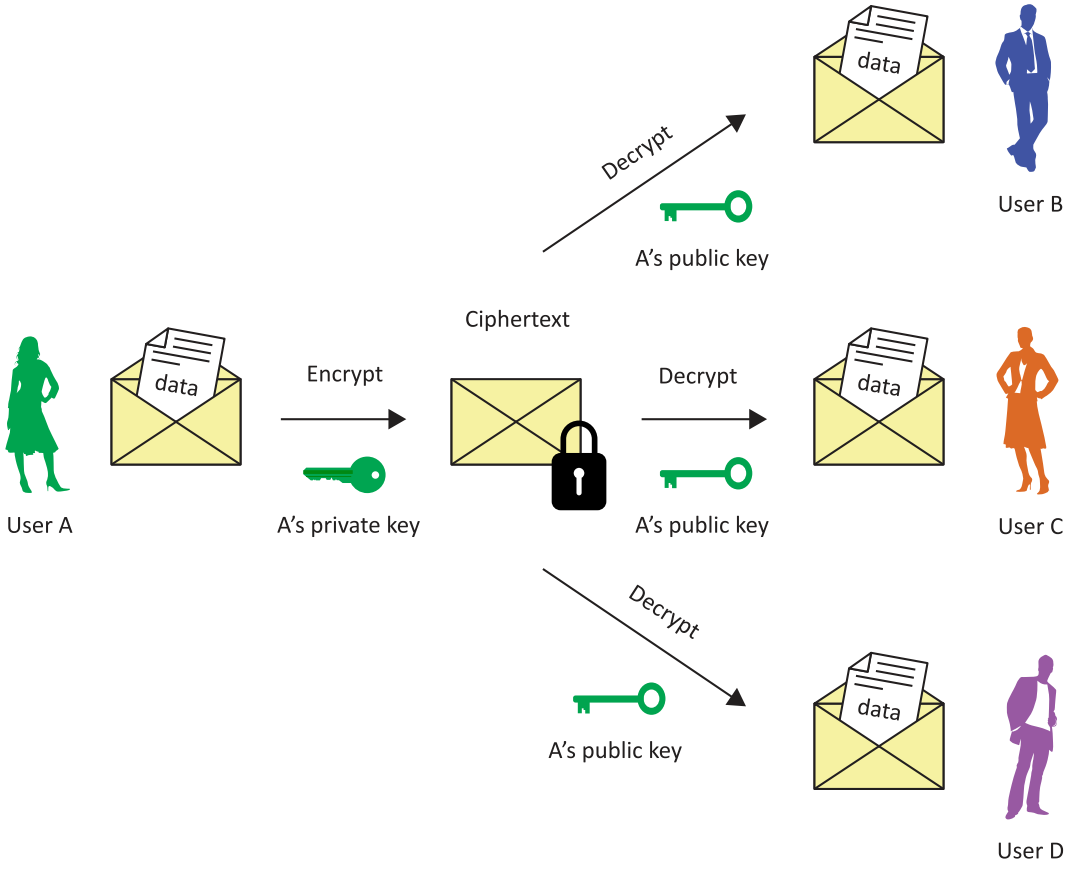

Fig. 8 – Public-key encryption model (to provide authentication)

Using public key encryption to provide authentication and confidentiality

To provide both confidentiality and authentication, User_B will need to encrypt the plaintext first with his or her private key, which will provide authenticity. Then, User_B will use User_A's public key to encrypt the message, which will provide confidentiality.

The disadvantage of the system is that it will be very time consuming and complex as public key encryption and decryption has to be done four times, and the key length of the public key is large (1024 bits to 4096 bits).

4.8 Hybrid System: Combining Symmetric and Asymmetric Encryption

The disadvantage of using **public key encryption** is that it is **quite a slow process**, as key lengths are large (1024 bits to 4096 bits). When both processes are compared, **symmetric key encryption** is significantly **faster**, as the key length is smaller (40 bits to 256 bits). On the other hand, there is a problem in transferring the key in secret key encryption. Both these techniques can be used together to provide a better method of encryption. This way one can make use of the combined advantages and overcome the disadvantages.

Specifically, the hybrid system uses a public key algorithm in order to safely share the symmetric encryption system's secret key. The real message is then encrypted using this key and then sent to the recipient. Since the key sharing method is secure, the symmetric key used for the encryption changes for each message sent. For this reason it is sometimes called the session key. This means that if the session key was intercepted, the interceptor would only be able to read the message encrypted with that key. In order to decrypt other messages the interceptor would have to intercept other session keys.

The session key, encrypted using the public key algorithm, and the message being sent, encrypted with the symmetric algorithm, are automatically combined into a single package. The recipient uses his or her private key to decrypt the session key and then uses the session key to decrypt the message. Many applications use this system.

The steps in data transaction within a combined technique are:

1. Encrypt the plaintext using a symmetric encryption and a random key.
2. Encrypt only this random key with the recipient’s public key using asymmetric encryption. Now send the encrypted random key to the recipient. The recipient, at his or her end, can now decrypt the random key using his/her private key.
3. Next, send the actual encrypted data. The encrypted data can be decrypted using the key that was encrypted by using the public key from the asymmetric key pair.

The next figure illustrates the process.

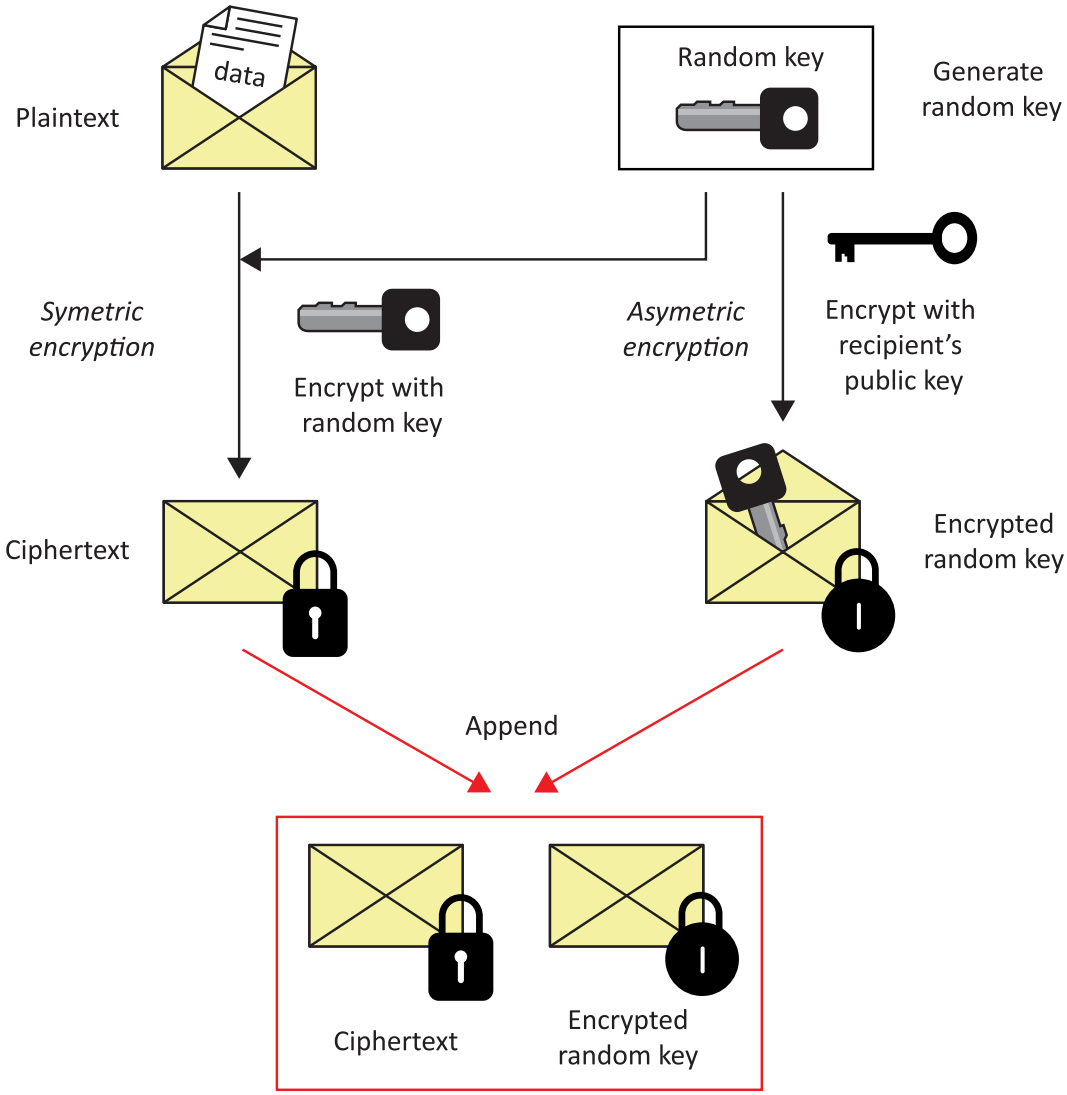

Fig. 9 – Hybrid encryption model (to provide confidentiality)

The combined technique of encryption is widely used. For instance, it is used in *Secure Shell* (**SSH**) to secure communications between the client and the server and in **PGP** (*Pretty Good Privacy*) for sending messages. Above all, it is the heart of *Transport Layer Security* (**TLS**), which is widely used by Web browsers and Web servers to maintain a secure communication channel with each other.

4.9 Hash functions

A hash function is a transformation that takes a variable-size input data *m* and returns a fixed-size string, which is called the hash value h (that is, $h = H(m)$). Any change to the input data will (with very high probability) change the hash value. Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties.

The basic requirements for a cryptographic hash function are:

- the input can be of any length,
- the output has a fixed length,
- it is easy to compute the hash value for any given message,
- hash functions are one-way, that is to say, it is computationally infeasible to generate a message that has a given hash,
- it is infeasible to modify a message without changing the hash,
- Collision-free, that is to say, it is computationally infeasible to find two different messages (x, y), such that H(x) = H(y).

The hash value represents concisely the longer message or document from which it was computed. One can think of a message digest as a "digital fingerprint" of the larger document.

The main role of a cryptographic hash function is in the provision of *digital signatures*. Additionally, a digest can be made public without revealing the contents of the document from which it is derived.

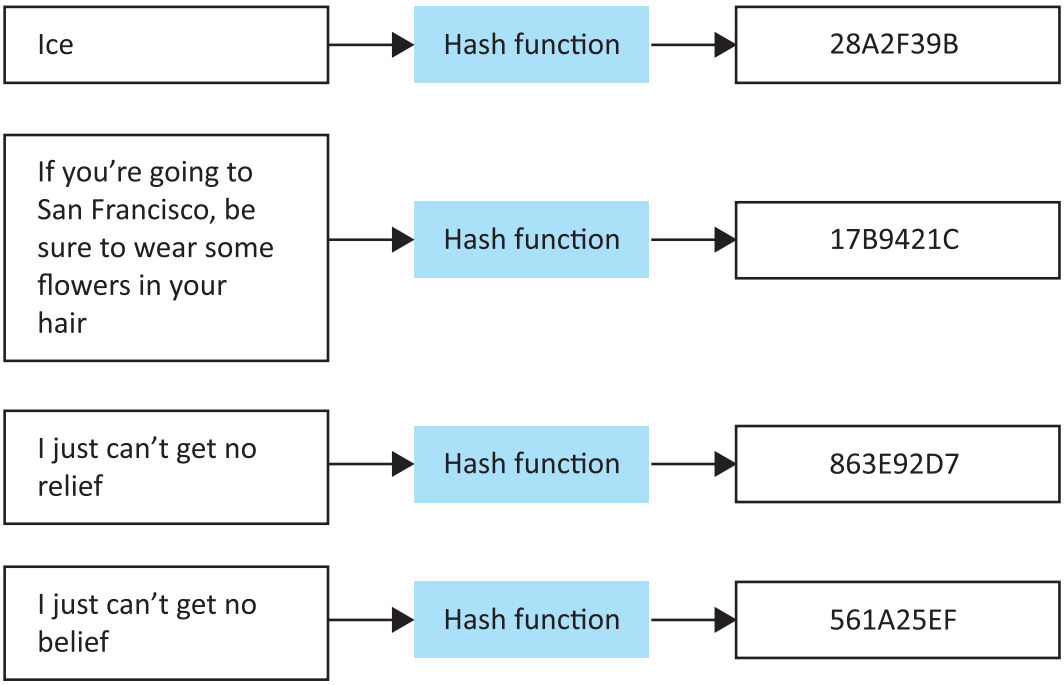

Fig. 10 – Hash function

4.10 Digital signature

Digital signatures are the most important development from the work on public-key cryptography, and provide a set of security capabilities that would be difficult to implement in any other way.

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure the integrity of the message.

Digital signatures are easily transportable and cannot be imitated by someone else. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

Digital signatures are based on handwritten signatures, which are used for ownership rights or message content confirmation. Handwritten signatures should have the following properties:

- The signature is secure – the signature should not be imitated and any potential attempt at signature forgery should be detected easily.
- The signature facilitates authentication – the signature identifies uniquely the signature keeper, who signed the document without restraint and wittingly.
- The signature is untransferable – the signature is part of the document and an unauthorized subject is unable to transfer the signature to another document.
- The signed document is unchangeable – the document cannot be changed and modified after the signature.
- The signature is undeniable – the keeper of the signature cannot deny the subscription of the signed document.

In practice, none of these features is consistently fulfilled in handwritten signatures and can be discredited or corrupted. All these features should have digital signatures too.

However, there are some problems associated to the practical realization of digital signatures. Digital files can be easily copied and part of a document can be transmitted to another document and the signed document can be easily modified. Therefore, additional requirements must be formulated for a digital signature:

- The signature must be a bit pattern that depends on the message being signed.
- The signature must use some information unique to the sender, to prevent both forgery and denial.
- The realization and implementation of the digital signature must be relatively easy.

- The forgery of the digital signature must be computationally infeasible, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

A digital signature can be used with any kind of message, whether encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact.

There are several possible schemes for digital signatures. Among others, one of the most accepted schemes is based on hash functions. In this case, if a user wants to digitally sign a document, the steps that he/she has to follow are:

- Evaluate the hash of the document to be signed.
- Using asymmetric encryption, encrypt the hash with the sender's private key to obtain the digital signature.
- Append the digital signature to the document.

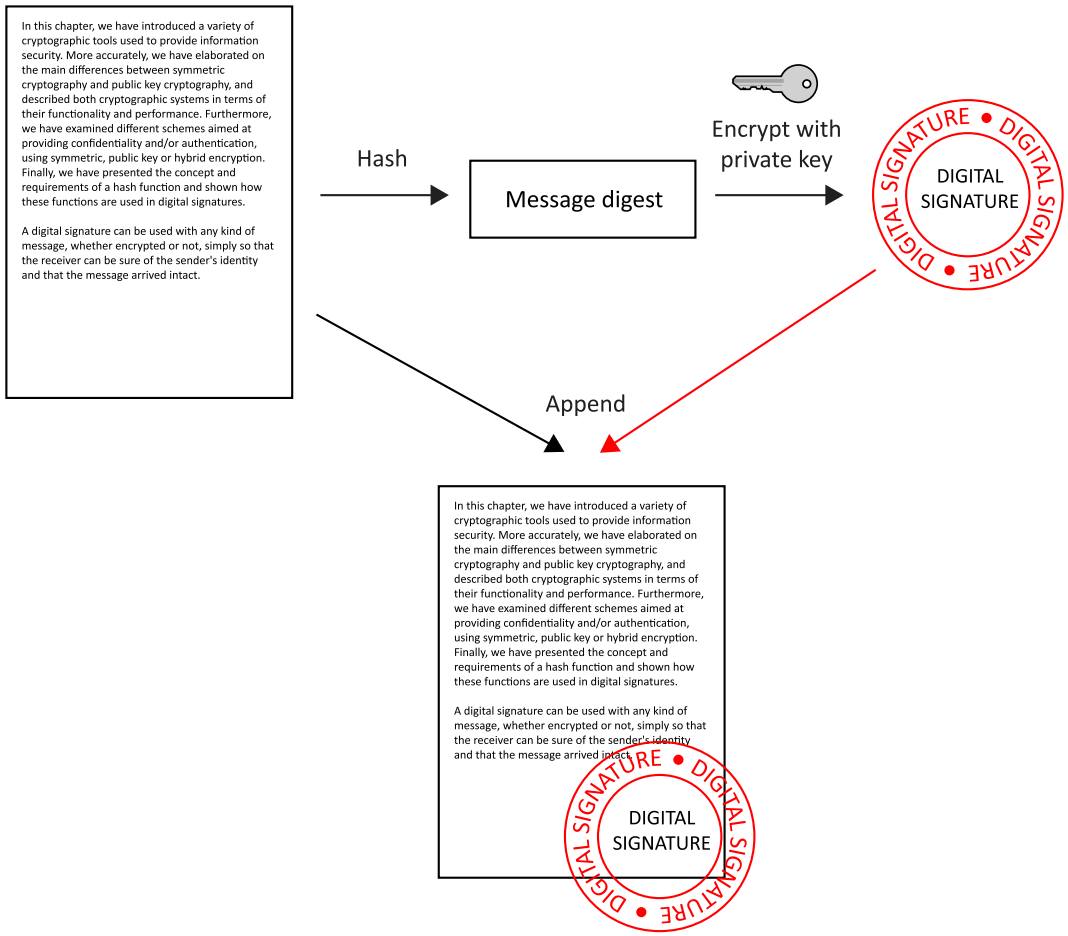

Fig. 11 – Hash based digital signature model

The receiver can verify the authenticity of this digital signature following the steps below:

- Evaluate the hash of the document (excluding the digital signature).
- Using asymmetric encryption, decrypt the digital signature with the sender's public key to obtain a message digest.
- Compare the results obtained in the two previous steps

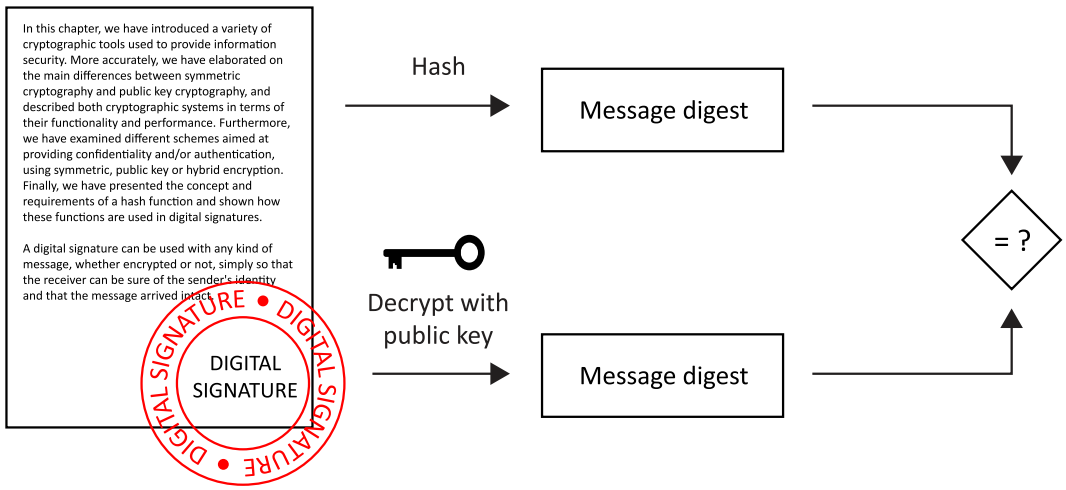

Fig. 12 – Verification process of a hash-based digital signature

If the message digests obtained in the two steps are the same, the recipient will know that the signed data has not been changed.

4.11 Summary

In this chapter, we have introduced a variety of cryptographic tools used to provide information security. More accurately, we have elaborated on the main differences between symmetric cryptography and public key cryptography, and described both cryptographic systems in terms of their functionality and performance. Furthermore, we have examined different schemes aimed at providing confidentiality and/or authentication, using symmetric, public key or hybrid encryption. Finally, we have presented the concept and requirements of a hash function and shown how these functions are used in digital signatures.

5 Digital certificates and key management

5.1 Public-key distribution

Digital signatures represent one of the primary uses of public-key cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. In many aspects, digital signatures are equivalent to traditional handwritten signatures, but properly implemented digital signatures are more difficult to forge than the handwritten type. In order to verify a digital signature, the sender's knowledge of the public key is required. Therefore, a key distribution mechanism is totally needed.

The most accepted approach is based on the usage of digital certificates, which enables the realization of the key exchange.

5.2 Concept of digital certificate

Digital certificate is an electronic document which incorporates 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. A digital certificate is a data structure which contains the public key of a subject or certificate holder, as well as the identification data of the certificate holder, a time stamp related to the certificate validity and other data from the certification authority. This structure is signed with the private key of a *certification authority* (**CA**) and every user is able to check the authenticity of the certificate content by using the public key of the certification authority.

The next figure shows the structure of a digital certificate:

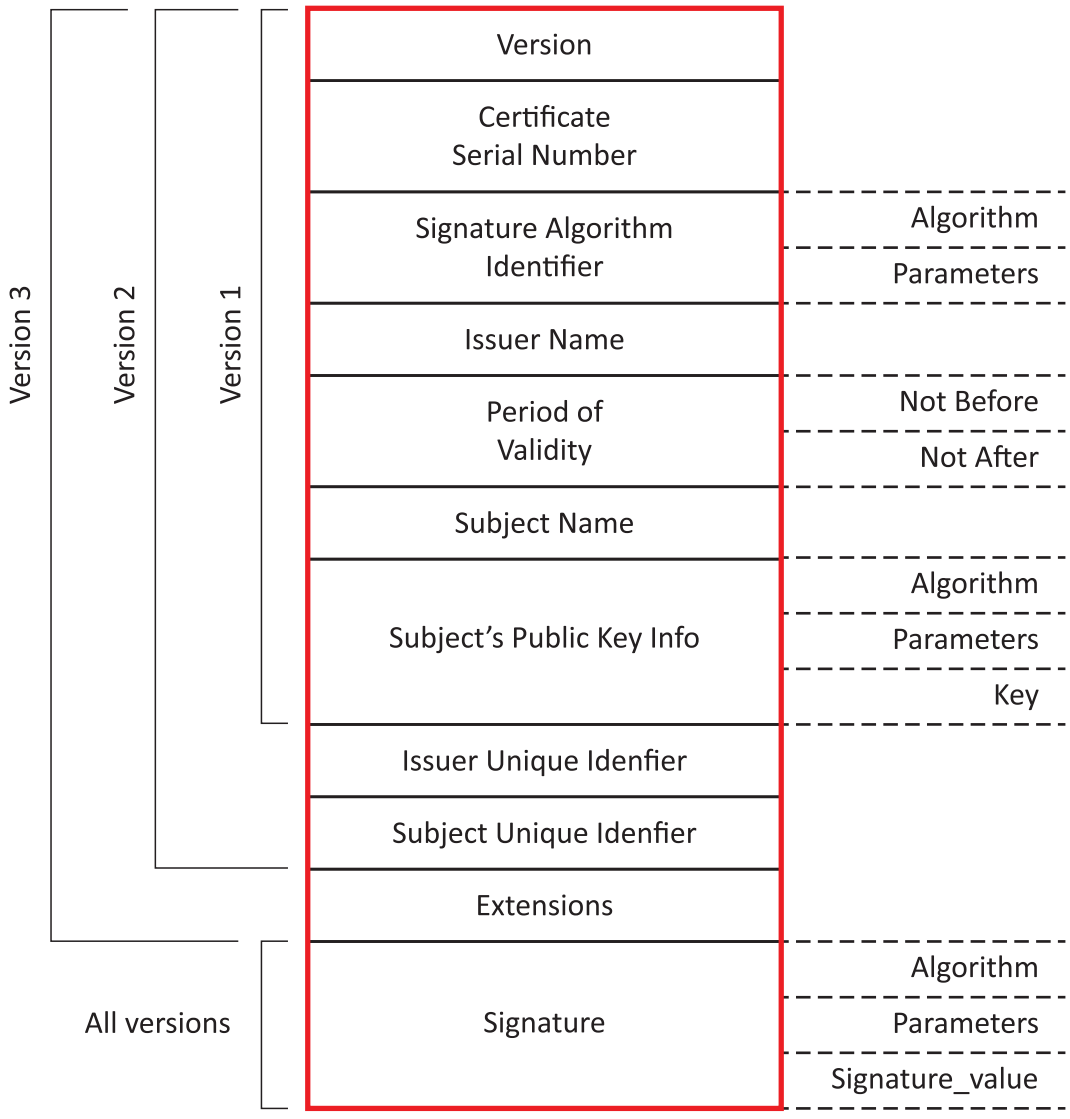

Fig. 13 – Digital certificate structure

5.3 Certificate revocation mechanisms

A digital certificate can be revoked if, for example, the user is no longer in sole possession of the private key (for example, the token that contains the private key has been lost or stolen) and theferore the private-key is thought to have been compromised. Certificates may also be revoked if it is discovered that the *certification authority* (**CA**) has improperly issued a certificate, without complying with the requirements of security policy.

The most common mechanism to verify whether a certificate has been revoked is based on the use of a *certificate revocation list* (**CRL**). The CRL is a list of certificates (or, more specifically, a list of serial numbers for certificates) that have been revoked, and therefore should not be relied upon. The CRL is always issued by the CA which issues the corresponding certificates and is generated and published periodically, often at a defined interval. Every CA therefore needs a CRL.

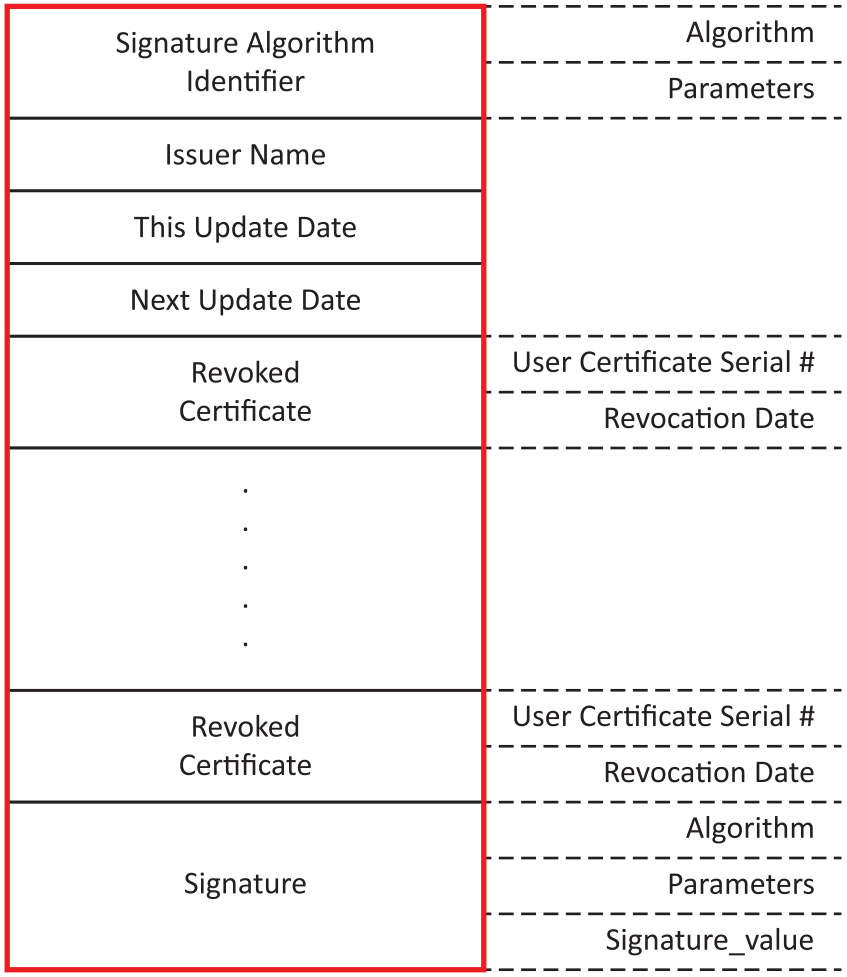

Fig. 14 – Certificate Revocation List structure

5.4 Summary

In this chapter, we have presented the problem of public key distribution and the use of digital certificates as the most accepted method to get around this issue. In addition, we have illustrated the problem of certificate revocation, and given details of the CRL-based mechanism.

6 Security of network services

6.1 TLS

Transport Layer Security (**TLS**) is an Internet standard protocol that provides communication security over the Internet. The primary goal of this protocol is to provide confidentiality and data integrity between two communicating applications. A prominent use of TLS is for securing World Wide Web traffic carried by HTTP to form HTTPS, allowing secure electronic commerce transactions. Increasingly, the *Simple Mail Transfer Protocol* (**SMTP**) is also protected by TLS.

TLS is in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and *voice-over-IP* (**VoIP**).

TLS is based on the earlier *Secure Sockets Layer* (**SSL**) specifications developed by Netscape Communications. Both protocols (TLS and SSL) use cryptographic algorithms and public key certificates to verify the identity of end points and for key exchange. This authentication can be made optional, but is generally required for at least one of the two communicating entities.

They also use symmetric encryption for confidentiality, and message authentication codes for message integrity. Symmetric cryptography is used for data encryption. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret previously negotiated. The negotiation of this shared key is secure and reliable: the negotiated key is unavailable to eavesdroppers, and for any authenticated connection the key cannot be obtained, even by an attacker who can place himself in the middle of the connection (Man in the Middle attack). Moreover, no attacker can modify the negotiation communication without being detected by the parties to the communication.

Figure 15 shows in a simplified way, how the TLS session is established

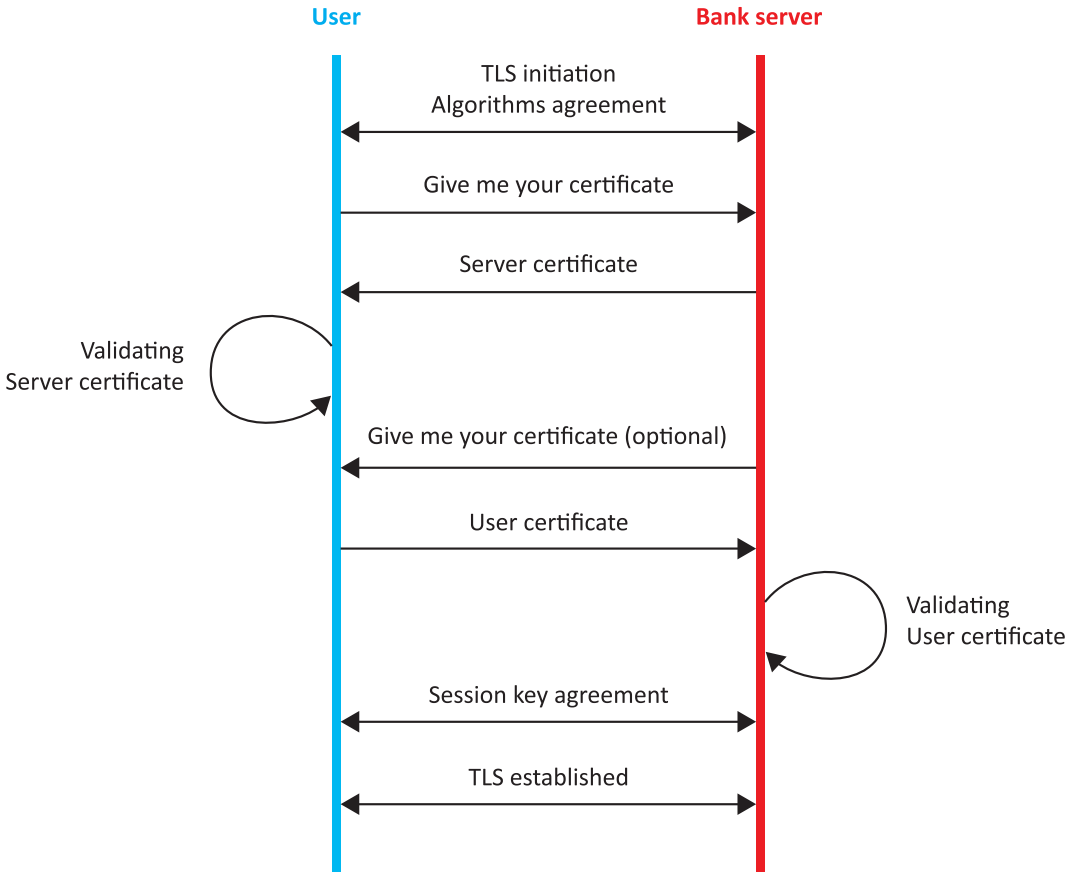

Fig. 15 – TLS session establishment

6.2 E-mail security

Usually, when an email is sent, its contents are open for anybody to read. Email is like sending a postcard: everybody who gets it in their hands can read it. To keep data sent via email confidential and/or authentic, it is necessary to encrypt it. In the case of confidentiality, only the intended recipient will be able to decipher the message while anybody else sees but gibberish.

The most accepted mechanisms to provide e-mail security are **S/MIME** and **PGP**.

S/MIME is a standard that provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures) and data confidentiality (using encryption). The use of **S/MIME** requires digital certificates

Figure 16 shows how S/MIME is applied in order to provide confidentiality.

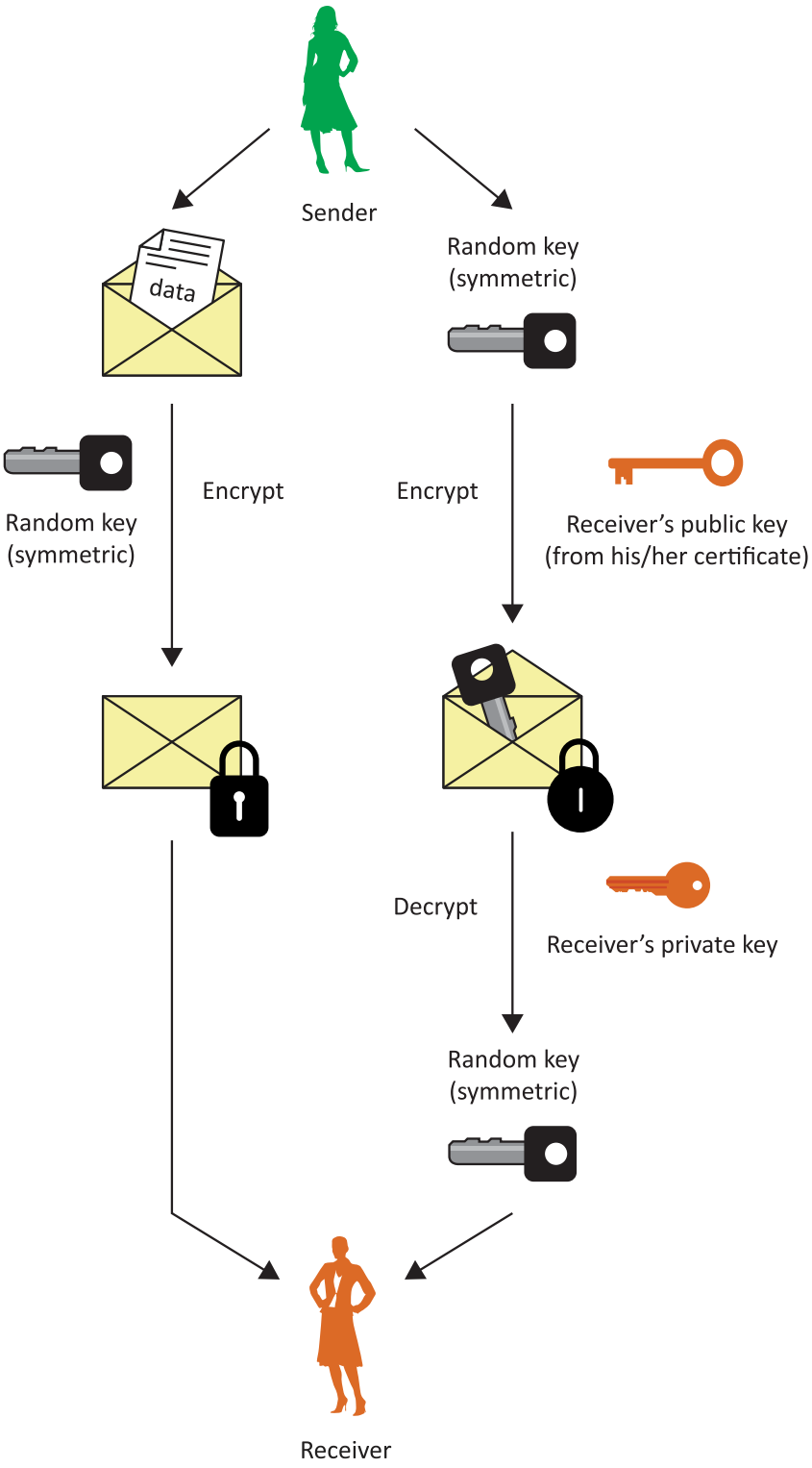

Fig. 16 – S/MIME confidentiality scheme

6.3 Summary

In this chapter, we have briefly introduced two secure protocols (TLS and S/MIME) that use a combination of public key and symmetric cryptography. In both cases, authentication is provided through the use of digital certificates, and encryption of user data is performed by means of symmetric cryptography.

7 Perimeter security

7.1 Firewalls introduction

One of the most widely deployed and publicized security measures in use on the Internet is a "firewall". Firewalls have been given the reputation of a general panacea for many, if not all, of the Internet security issues. They are not. Firewalls are just another tool in the quest for system security. The level of security that a firewall provides can vary as much as the level of security on a particular machine. There are the traditional trade-offs between security, ease of use, cost, complexity, etc.

A firewall is a device, which is used to manage and secure network traffic between networks with different level of trustworthiness and security using predefined rules for communication between networks, which it separates. Formerly, these rules consisted only of source and destination identification (source and destination address of a network/device) and source and network port. Nowadays, modern firewalls operate with session state information and with knowledge of monitored protocols.

Before we can install a firewall, the organization, which is to be protected, is adviced to define a set of rules to ensure the protection of its assets, computer systems, personal information and other sensitive data. This set of rules is denoted as the *security policy*.. Such document ensures, that in the whole company's network will abide by the same and unified rules, which will the device administrators follow.

A firewall can do two things. It can either block communication or permit it. I tis important to realize, that to prevent the illegal network activities to spread, it is always advantageous to monitor the incomming traffic as well as the outgoing traffic leaving the specific network.

Firewalls can be cathegorized as follows:

- Packet filters
- Application gateways
- Stateful packet filters
- Stateful packet filters with protocol inspection

Packet filters are the spiplest and oldest form of traffic security. They work with source and destination address and port information only, i.e. at the third (network) and fourth (transport) layer of ISO/OSI model. Because their advantage is the processing speed, this security principle is used till now.

Application gateways or *Proxy servers* are used to monitor sessions initiated by client applications. The gateway acts as a mediator between the client and the

destination server, thus the original session is divided into two: client–gateway and gateway–server. This enables to filter requests targeting specific destination devices. The inspection is done at the seventh (application) layer of the ISO/OSI model.

Statefull packet filters, compared to the classical (stateless) packet filters, store information about already allowed sessions, which use for further evaluation of further packets, whcih are related to the already allowed packet (resp. session). This is not only faster, but also makes the configuration efficient, as i tis sufficient tot set up only one direction and the returning reply packets will be automatically allowed.

Statefull packet filters with protocol inspection are modern stateful filters, which, beside the session information and ability to dynamically open ports for control and data sessions of known complex protocols, enable to monitor (inspect) the sessions up to the application layer data of known protocols. Therefore, it enables to reveal attempts to establish a hypertext protocol session (HTTP), while it is not a valid WWW server request, but it is a tunneling of a completely different protocol (a different application trying to communication on the same port).

7.2 Intrusion Detection Systems

The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less technical ability is required for the novice attacker, as proven past methods are easily accessed through the Web. So, *Intrusion detection systems* (**IDS**) are being developed in response to the increasing number of attacks on major sites and networks.

Intrusion detection systems monitor the network traffic, work with signature databases and by using a heuristic analysis reveal suspicious patters in seemingly not related attempts for connection establishment (e.g. address range scanning, port range, signatures of known attacks ecapsulated withing the allowed connections etc.) The aim of IDSs is to detect unusual activities, which can lead to security violence in an operating systém or a computer network, and also a possible couterstrike against them.

IDS uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- monitoring and analyzing both user and system activities,
- analyzing system configurations and vulnerabilities,
- assessing system and file integrity,
- ability to recognize patterns typical of attacks,
- analysis of abnormal activity patterns,
- tracking user policy violations.

An *intrusion detection system* (**IDS**) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

There are several ways to categorize an IDS:

Misuse detection vs. Anomaly detection

- **Misuse detection:** the IDS analyzes the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. The intrusion detection technique based on attack signature consists in looking for “signatures” (a typical character sequence of an attack) in all communications going through the network. It can detect application level attacks, even if they conform to inter-application protocol standards; as such, it complements inter-application protocol decoding. Like a virus detection system, misuse detection software is

only as good as the database of attack signatures that it uses to compare packets against, so it implies the maintaining and updating of the attack signatures database; the frequent update of this database on equipment using this technology is of utmost importance for the relevance of this technique.

- **Anomaly detection:** the system administrator defines the baseline or normal state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

Network-based vs. Host-based systems

- *Network-based system, or NIDS*: the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules.

- *Host-based system, or HIDS*: the IDS examines all the activity on each individual computer or host.

Passive system vs. Reactive system

- *Passive system*: the IDS detects a potential security breach, logs the information and signals an alert. The advantage is, that the device is not located inline, but the network traffic is copied towards it (mirrored). In case of suspicion, it performs only a correponding announcment (an e-mail, a SNMP trap message, etc.)

- *Reactive system*: the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source. Active IDS, usually danoted as a *Intrusion Prevention System (IPS)*, responds to a suspicious activity, beside the passive announcment (the same as the passive IDS does) proactively, for instance, by logging a user out of a system or reprogramming a corresponding network device (typically a firewall) to block the network traffic from a suspicious (and potentially harmful) source. The IPS device is always located inline with the data traffic to be able to actively prevent the malicious packets to spread throughout the network. However, this brings a potential risk in the terms of data throughput (a bottleneck), and contributes to the total transmission delay of the messages. On the onther hand, the moderm IPSs are designed to minimize the processing delay of packets while being inspected (approximately, units or tens of microseconds).

Figure 17 shows a diagram of a network including a firewall and an IPS

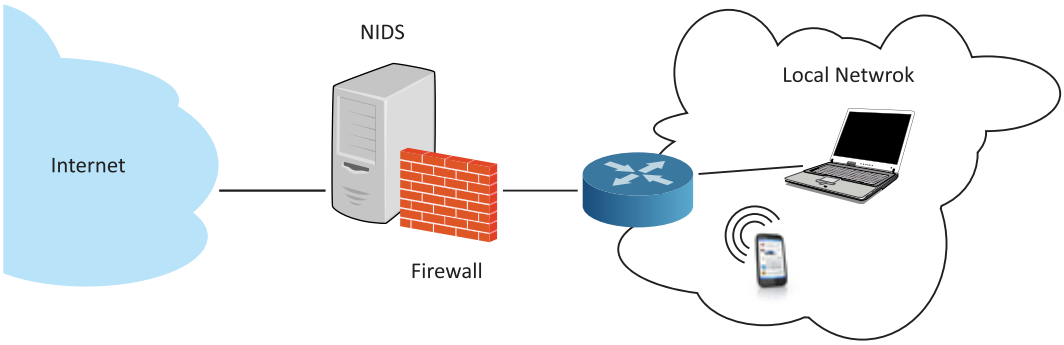

Fig. 17 – Diagram of a NIPS (active NIDS) with firewall

An IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.

7.3 Summary

In this chapter, we have discussed the typical solutions adopted to provide perimeter security. Perimeter security is a set of hardware, software and programmatic security policies that provide levels of protection against remote malicious activity. In addition, we have described the main features of firewalls and intrusion detection systems, and classify these systems according to different criteria.

8 Wireless Security

8.1 Wireless networks

Wireless networks (**WLAN**) are very popular nowdays, as they allow mobility within wireless network range and wireless connection of end devices. That offers the possibility to make use of network services and Internet almost everywhere and to exploit data and voice communication.

Advantages of wireless communication present also high security risks resulting from the accessibility to radio signal within wireless network range. For this reason, the security of wireless connection is an actual topic.

WLAN security involves these important tasks:

- *ensuring confidentiality* or communication content encryption,
- *user authentication* or network access control.

It is necessary to notice that almost all types of attacks in WLAN networks are performed from the internal network.

8.2 Wireless security

Wireless network security involves these main fields:

- **authentication,**
- **confidentiality,**
- **key management.**

Authentication is the process whereby the user associates to the WLAN network; the result is a successful or unsuccessful user association.

Confidentiality in WLAN networks is realized by encryption. The most used encryption algorithms are **RC4** (**WEP**) and **AES** (**WPA2**).

Key management involves distribution and key generation.

8.3 The WEP Protocol

WEP protocol (*Wired Equivalent Privacy*) is used as an optional supplement to the IEEE standard 802.11a/g/b and is designed for WLAN access control to ensure confidentiality of transferred data.

It involves the authentication and confidentiality services:

- **WEP authentication**
  WEP authentication can be done in two ways, which are:
  - open authentication,
  - shared key.

Open system authentication uses only SSID network identificator. SSID is not a password; it is only a wireless network identificator. *Wireless access point* (**WAP**) broadcasts this identificator in intervals of a few seconds.

In open authentication mode, the user sends an 802.11 authentication frame, which contains identification data of the user. WAP checks the user ID and a frame confirming or denying access to the WLAN is sent back to the user.

Shared WEP key authentication uses a 40 bits secret shared key, which is the same for all WLAN users and is distributed to all of them in a secret way. Authentication verifies the identity of the end device network card.

- **WEP encryption**

WEP Protocol uses symmetric RC4 encryption, which in turn uses a 64 or 128 bits key to encrypt the data. The key consists of a secret 40 or 104-bit key and a 24-bit *initialization vector* (**IV**).

WEP Protocol is vulnerable to known attacks (activity monitoring, brute force attack, repetition attack, and so on…) and RC4 cipher was broken in 1996.

8.4 The WPA Protocol

WPA Protocol (*Wi-Fi Protected Access*) was accepted in 2002 to eliminate vulnerabilities of the WEP protocol. This protocol was accepted as a temporary solution because in that moment of time, the work on the new standard IEEE 802.11i (accepted in 2004) had already begun. WPA Protocol is a subset of 802.11i standard features, so implementation of 802.11i does not require any changes in technical devices. Changes are only necessary in software or firmware.

As WEP protocol does, WPA protocol uses also RC4 cipher, but involves new security mechanisms. Main parts of WPA protocol are:

- *Temporary Key Integrity Protocol* (**TKIP**),
- *Message Integrity Check* (**MIC**),
- Access control based on the 802.1x standard with **EAP protocol** (*Extensible Authentication Protocol*).

8.5 802.11i (WPA2) Protocol

802.11i standard, also referred to as WPA2, combines the mechanisms of 802.1x and TKIP. This standard uses a 128-bit AES block cipher.

From the structural point of view, the 802.11i standard has a similar structure to WPA and comes with new features, such as the CCMP protocol and selectable preauthentication, which ensures fast and secure roaming between access points.

Main mechanisms and security services of the 802.11i standard are:

- authentication,
- encryption,
- integrity.

8.6 Summary

In this chapter, we have presented the security risks associated with the use of wireless communication networks. In the case of wireless LAN, different security solutions have been adopted, although some of them, e.g., the WEP protocol, are vulnerable to a range of attacks. The most accepted solution to ensure the different security requirements in this scenario consists in using the 802.11i standard, also known as WPA2.

9 Summary

This document contains an overview of the various aspects related to the information and network security. It is divided into eight parts.

The first is an introduction that tries to motivate the reader about the need to protect data and the network communications. Some causes of data and network insecurity are presented along with different basic mechanisms that users should consider in order to protect themselves. Moreover, a basic classification of the types of attacks is included.

The second part is devoted to malicious software and antivirus. Basically, the concept of malicious software is introduced and classified according to several criteria: propagation, installation method, main feature and so on. Furthermore, the chapter describes various techniques for cleaning out an infected computer. Since these techniques require the detection of malware, different strategies commonly used for detection are introduced. Moreover, the document contains basic information on antivirus software, emphasizing the need to keep it updated.

The third part is focused to the security services and mechanisms. The most important security services (confidentiality, integrity, availability, authentication, access control, non-repudiation and privacy) are introduced along with the security mechanisms needed to provide such services. Furthermore, a connection between security services and mechanisms is included.

The fourth part contains basic information about a variety of cryptographic tools used to provide information security. The chapter presents the main differences between symmetric cryptography and public key cryptography, and describes both types of algorithms according to their functionality and performance. Finally, the concept and requirements of a hash function are shown and also it is indicated how these functions are used in digital signatures.

The fifth part is focused to the problem of public key distribution. The concept of digital certificates is introduced as it is the most accepted method to get around this issue. In addition, the problem of certificate revocation is shortly illustrated.

The sixth part includes a short description of two secure protocols (TLS and S/MIME). Both schemes use a combination of public key and symmetric cryptography, and require through the use of digital certificates.

The seventh chapter deals with the perimeter security. The basic components (firewalls and intrusion detection systems) are presented. Moreover, the IDS are classified according to different criteria.

Finally, the eigth part is devoted to the security risks associated with the use of wireless communication networks. Different security solutions have been adopted, although some of them, e.g., the WEP protocol, are vulnerable to a range of attacks. The most accepted solution to ensure the different security requirements in this scenario consists in using the 802.11i standard, also known as WPA2.