INFORMATION PIRATERY IN THE KNOWLEDGE SOCIETY

Lucian LUCA
”TIBISCUS” UNIVERSITY TIMIŞOARA, FACULTY OF ECONOMICS

Abstract:
This paper intends to notify users of the Internet and databases about potential attacks from hackers, which have become increasingly frequent. Although we live in a "computerized" society, in which reigns the feeling of safety, we must be aware that any system, however complex and well protected it seems, can be "hacked" by various malicious people who want to use their knowledge in computer science for their own purposes. Although in time, there were invented and perfected security systems, there are still problems with hackers worldwide, which, unfortunately, are always a step ahead, the technology.

Key words: *security, information systems, internet, databases, hackers*

JEL classification: *D83*

Information Security

Information Security has become lately one of the major components of the Internet. Analysts have brought this concept a contradiction between the need for communication and connectivity, on the one hand, and the need to ensure confidentiality, integrity and authenticity of information, on the other. The field of information security seeks technical solutions to resolve this apparent contradiction. Speed and efficiency of communication of documents and messages confers numerous advantages of decision making in a modern society based on competitive economy. But the use of email, web, transfer funds, and others, can transform the potential gains arising from rapid access to information in major losses caused by theft of data or the insertion of false or distorted data.

Systems are threatened both from inside and outside. There may be well intended people who make different operating errors, or malicious people who sacrifice time and money to penetrate systems. Among the techniques factors that allow security cracks there can be some errors in the software processing and communication or some defects of computer equipment or communications. Also, the lack of an adequate training manager, operators and users of systems increases the likelihood of security breach. Also, one of the major risk factors of security systems is the misuse of systems (computer piracy).

In recent years, in developed countries, functions of archiving and transmission of information have been taken over by computers and interconnection networks, paper becomes only a way for presenting information. Therefore, solutions had to be found to replace the seals, stamps and handwritten signatures of the classical versions of their digital, based on classical cryptography and public key. Cryptography is the computational method of countering the problems of IT security. Used for a long time only to ensure the confidentiality of diplomatic and military communications, cryptography has undergone in the last two decades, spectacular progress, thanks to its safety data to computers and networks.

Improving security systems should be an important objective of any organization. The measures should discourage unauthorized penetration attempts, to make them more expensive than obtaining legal access to these programs and data. OCED (Organization of Economic Cooperation and Development) is one of the international bodies concerned with the protection of personal data, security systems, ciphering policy and the protection of intellectual property.

As regards the protection of personal data, the OECD has developed, in 1985, "Declaration on trans-frontier flux of data. The fundamental idea was to make, through legal and technical measures, the individual direct control upon personal data and upon their use. Current efforts are directed towards an international framework in terms of life and individual autonomy of individuals (freedom of movement, freedom of association and fundamental human rights).

In the field of information systems, OECD countries have asked in 1988, the OECD Secretariat to prepare a full report on this area, highlighting the technological issues including management, administrative and legal ones. Following this report, member countries have negotiated and adopted in 1992 guidelines on safety systems in the OECD. They provide an international framework of reference for the development and implementation of measures, practices or consistency of IT security in the public and private sectors. OECD Council recommends periodic review of these rules every 5 years.

Security in Internet connections

The Internet is a vast collection of networks, namely a "network of networks" that includes millions of computers that are difficult to control. Therefore we can speak of the vulnerability of networks, shown on various plans. A crucial aspect of Internet communications is security. The need for security appears at all levels of the architecture of the networks. For example, users who use email messages want the messages to arrive from the person who claims to be the sender. Users, especially when acting on behalf of companies they wish to ensure the confidentiality of messages transmitted. In financial transactions, along with the authenticity and confidentiality, an important place has the integrity of messages, meaning the message received was not altered during transmission over the network. In business transactions is very important that, once received, a command to be not only authentic with an unchanged content, but there has to exist the possibility that the sender can recognize it. So doors (gateways) and routers must be between authorized computers and enter. Thus IT security has become one of the major components of the Internet.

If the Internet, addresses of various nodes and services can be determined easily. Any owner of a PC with a modem, with knowledge of operating environments, may try to penetrate networks or services, such as connecting to remote (telnet), file transfer (FTP) or electronic mail (e-mail). There are people willing to spend resources, money and time to penetrate the various security systems. Some are true "masters" in the field: He penetrates the computer A, and with its help in the computer B, used further for accessing to computer C and so on.

Network Vulnerability

A network of computers is an open structure which can connect new types of equipment. This leads to an uncontrolled expansion of the circle of users with direct access to network resources.

The vulnerability of networks is on two plans:

- the possibility of changing or destruction of information, namely the attack on the integrity of its physical possibility;
- the possibility of unauthorized use information that is leaking from the circle of users.

We have to considered, with priority, two aspects of computer security:

- integrity of a network's resources, irrespective of their functional defects, hard or soft, the attempts of illegal information theft and attempts to change information;
- the private character, meaning the individual right to control what information, regarding a person, can be stored in databases and who has access to these data.

A secure network is one, in the components of which (resources and operations) that you can have confidence in, that provides quality and fair services. Since a network consists of different components it is a convenient area for different attacks or illegal operations, which leads to the conclusion that protection has become one of the key operational aspects of a network.

Security and in particular the private character must be examined closely in networks. Networks are complex sets of computers. It is very difficult to obtain a complete schedule of all existing entities and operations at a time, so that networks are vulnerable to various types of attacks or abuse. Complexity is caused by geographical dispersion, sometimes international of the components (nodes) network, involving several organizations in the administration of a single network, the existence of different types of computers and operating systems, the existence of a large number of entities. In the immediate future, computer networks will become an essential part of individual and social life. For their proper functioning depends on government, commercial, industrial and even personal businesses. As personal computers can be connected to home networks, a number of activities can be made by individuals. There should be taken into account the types of data that people can read, which are the other people who they can communicate, on what programs do they have access. More and more information stored in files are becoming linked through the network. The combination of files on individuals may have damaging consequences upon the private individual. Information is vulnerable to attack at any point of a network, from its introduction to its final destination. In particular, information is more likely to attack when you pass through the lines of communication. The strong control of access based on password protection schemes operating systems attacks are more attractive than the lines on the network host computers.

Types of attacks on networks

Security threats to computer networks may have the following origins: natural calamities or disasters, equipment failures, human errors in operation or manipulation, fraud. Several security studies of computers estimates that half of the costs of incidents are due to intentional destructive actions, accidental disasters fourth quarter and human errors. Respective the threats from intentional actions, there are two main categories of attacks: passive and active.

Passive attacks - are attacks in which the intruder observes information through the "channel", but he doesn't interfere with the flow or content of messages. It only makes traffic analysis, by reading the identity of parties communicating and "learning" the frequency and length of messages circulating on a logical channel, even if the content is obscurely. Passive attacks have the following common characteristics:

- do not cause damage (do not delete or change data);
- violates privacy laws;
- the objective is to observe and analyze the data exchanged over the network;
- can be achieved through a variety of methods, such as supervision telephone or radio links, exploitation of electromagnetic radiation emitted, routing data through additional nodes less protected.

Active attacks – are those in which the intruder commits either theft messages or alteration, or resumption of inserting false messages. This means that it can delete, modify or delay messages, may insert false or old messages can change the order of message or a direction or both directions of a logical channel. These attacks are serious because they change the state of calculation and data communications systems. There are the following types of active threats:

- pageant - a type of attack in which an entity claims to be another entity. For example, a user attempts to substitute another, or a service claims to be another service, with the intention of taking secret information (credit card number, password or key encryption algorithm). A "farce" is accompanied usually by an active threat, such as replacement or modification of messages;
- repeating - it takes place especially when a message or a part thereof is repeated, the intention to produce an unauthorized effect. For example it is possible to reuse the authentication information of a previous message. In banking, the resumption of units involves duplication of data and / or other changes in the value of accounts unreal;
- changing messages - makes the data message to be altered by modification, insertion or deletion. It can be used to change the beneficiary of a loan. Another use may be changing field receiver / sender of the mail;
- service refusal - occurs when an entity does not accomplishes its own function, or when it acts in order to prevent another entity from fulfilling its functions;
- service repudiation - occurs when an entity refuses to recognize a run. It is clear that applications transfer of funds is important to avoid service repudiation both by transmitter and the receiver.

In the case of active attacks there can be included some of the programs created with the destructive and affecting, sometimes essential, computer security. There is a terminology that can be used to show different possibilities of attacks on a system. This vocabulary is well popularized by the "stories" about "hackers". The attacks involve, in general, either unauthorized reading of information, either partial or total destruction of data or even computers. What is worse is the potential possibility of infestation by the network or even copies of disks, of a large number of machines. From these destructive programs we can mention the following:

- viruses - are inserted into software applications that multiply themselves in other programs in the resident memory, or on disks. Then, they either completely saturate the memory / disk system and block the system, either after a fixed number of multiplications they become active and enter in a destructive phase (which is usually exponential);
- software bomb - is part of the procedure or code included in a "normal" application, which is activated by a predefined event. The author of the bomb schedules it, and then leaves it to "explode", in order to initiate actions to destroy the system of calculation;
- worms - have similar effects to those of the bombs and viruses. The main difference is that it does not remain at a fixed location and does not own rejoinder. They are constantly moving which makes them difficult to detect. The most famous example is the Internet worm; the first worm ever created that has paralyzed the Internet for a few hours in 1988.
- hatches - represent a special access to the system, which are normally reserved for procedures for remote loading, or maintenance for developers of applications. But they allow access, eluding the usual identification procedures;
- Trojan horse - is an application that has a very popular use function, which in a hidden manner fulfills another function. Do not create copies. For example, a hacker can replace the code of a normal control "login" with another code, which is the

same, but makes additional copies in the form of a file name and password that the user types in the process of authentication. Subsequently, using this file, the hacker will easily penetrate the system.

Hackers

Hackers are passionate of Informatics, which usually have as purpose "breaking" some code, databases, web sites, and other. Real hackers do not pay attention to the "harmless" pages, such as personal pages. The usual targets of hacker's are informational systems, which have advanced protection and contain top secret information, such as databases of banks, the Pentagon or NASA. Once obtained, these files (information) are either published throughout the Internet to be viewed or they are used by several people, or are used for their own purpose. Any real hacker must know and respect a "Code of lows of hackers", which is well established.

There are hackers who attack random targets, wherever and whenever they have the occasion. They are known as "amateur hackers". For example, more frequent attacks on Yahoo and Hotmail have blocked search engines and email accounts for those few days, and prejudiced million. Behind these attacks (which are a pretty serious breach of the "Code of Laws of hackers) are usually people who "were just curious to see what happens" or "wanted to have fun". This virtual hackers are not real hackers, because they don't write their own programs through which they attack, getting them from the Internet or from other sources. These hackers are amateurs who are brought in front of the justice. Why? Because those hackers, who can really write their own programs with which they attack, are usually smart enough to make certain systems to mislead everyone who would try to determine the source of the attack.

Another category of hackers are crackerii. They represent a style of some hacker who specialize in "cracking" or shareware programs that require a serial code. The only ones who are affected by this category of hackers are the ones who write programs and design "cracked" programms. The protection of the applications may be "cracked" by two methods:

- introducing the code, that can be found on the Internet or using a special program.
- patches used for protection systems more advanced, requiring hardware keys (to be installed on the computer's parallel port and send a coded signal of whenever it is required by the software). These programs are made specifically for certain software, which, once launched, modify the executable code, restricting instructions that require the hardware key. Patches and serial code libraries are the most often used ones on the Internet. They are made by certain people (who are sometimes former employees of companies that wrote the software in question) that only want to bring damages to the company designed.

Although it seems strange, cracking is considered the "Computer piracy" and it is a serious offense. However, we rarely found those who place patches and serial codes on the Internet.

Real hackers are those who write their own software that they need. Many of these programs after they are tested are published on the Internet. Of course, the more advanced and more dangerous they are, for "breaking" servers at the Pentagon or decoding files encoded 64-bit, they will not be found so easily on the Internet and they are kept secret by the ones who design them.

Spammers

Spammers are those hackers that send huge quantities of e-mail (or other information), containing false information or offer random transmitted information to block certain servers. Most important sites such as Yahoo, Google or Hotmail have some filtering systems that should protect those servers from attacks with enormous amounts of information. These pitfalls are easily avoided. The last time servers specified above and many others have been subject to strong "information attacks", which could not cope. They sent messages to a capacity of about 1 MB per second, while servers that support a normal traffic of up to 1 - 1.5 GB Weekly. Spammers through their damaging attacks prejudice with hundreds of millions of dollars the target servers. At the same time, users of those certain servers are affected when the traffic is completely blocked, sending or receiving messages or using other similar services being completely impossible.

How are sending large quantities of information at amazing speed, without locating those hackers. It is relatively simple for them: they send messages from about 50 email addresses, and then departs the information transmitted through several points in the world (different servers). It is very difficult to be detected; the teams of specialists from the FBI worked weeks (even months) to catch the whole virtual offender, often not reaching to any result. The only problem (of hackers) that appears in such deviations of successive information is that through one of the servers in which the information "pass" on his way to its "target" may be the final block. Information will not go entirely to the destination, substantially reducing the power of the attack.

Such cases can be considered the recent attacks, the servers were not affected by the hackers targeted.

Protection against hackers

These issues are important for many computer users who regularly use the Internet. There is protection against hackers. The only problem is that no matter how complex and apparently reliable the security systems is, they it can be avoided and "broken". There are certain methods which, so far, could make life a little hard for hackers, and especially for their spammers (this being the most recently used). These should be primarily applied by the Internet providers (ISP): there will have to be removed all files from unknown servers (which would facilitate hacker's attack), so that there will be kept strict evidence, disposing packages that have another header than the owned IP address. They can be used by some people under the pretext of anonymity necessity.

But there are other methods to maintain your anonymity, using systems of encryption and specialized servers. The best encryption systems are those that use hardware, but they are very expensive. The most commonly used DES encryption and are CCEP, the last being a newer standard, created by the NSA, and used by government organizations.

Conclusions

A good way to keep hackers away is using a firewall. This is a screen, which can keep off the Internet traffic, bad intentions, such as hackers, worms and some types of viruses before they can cause problems. In addition, it can prevent the computer from an attack against others without your knowledge. Using a firewall is especially important if you are permanently connected to the Internet.

A firewall is an application or a hardware device that monitors and filters permanent data transmission achieved between PC and local network, or the Internet, in order to implement a "policy" filter. This policy could mean:

- protection of network resources from the rest of the users of other similar networks - Internet → the potential unwanted "guests" are identified, as well as attacks on their PC or local network and they could be stopped.

- control resources that could be accessed by local users.

A firewall can:

- monitor routes of penetration into the private network, thus allowing better monitoring of traffic and therefore its easier to detect infiltration attempts;
- traffic blockage at a certain time from and towards the Internet;
- selecting access on the private information contained in packages.
- permitting or prohibiting access to the public on certain specified stations;
- and last but not least it can isolate the private and the public space and can realize the interface between the two.

Also, a firewall application can not:

- prohibit importation / exportation of harmful information circulating as a result of the mean action of users from private space (ex. the inbox and attachments);
- prohibit leaking information on other ways that bypass the firewall (access via dial-up which not pass through the router)
- protect private network from users using natural systems for the introduction of mobile data network (USB Stick, floppy, CD, and others)
- prevent the emergence of design projecting errors of applications that realizes various services, as well as weaknesses points which arising from the exploitation of these mistakes.

At present time, Firewall can provide very good protection, but as complex as these applications are, there will always be hackers who in one way or another will pass these firewall protections.

REFERENCES

1. Gabriel Mircea – Introducere în informatica economică, editura Mirton, 2004
2. Ioan Bandu – Introducere în informatica economică, editura Mirton, 2004
3. Ioana Vasiu – Totul despre hackeri, editura Nemira, 2001
4. www.wikipedia.org
5. www.yahoo.com