METHODS OF OPERATION RELATED TO THE OFFENSE OF UNAUTHORIZED ACCESS TO A COMPUTER SYSTEM

Ionuț Andrei BARBU*
„Alexandru Ioan Cuza” Police Academy, Bucharest, Romania**

Cristina PIELMUȘ
„Alexandru Ioan Cuza” Police Academy, Bucharest, Romania***

Abstract
This study presents some methods of operation related to the offense consisting in the unauthorized access to a computer system, which is stipulated in article 360 of New Romanian Criminal Code (Law no. 286/2009). Since the material element of the offense is represented by the unauthorized access to a computer system, there are several methods to achieve this access that can be analyzed, such as password attack, trusted access attack, exploitation of technological weaknesses, shared library attack, IP attack or TCP hijacking attack.

Keywords: unauthorized access, computer system, methods of operation, password, IP, TCP attacks.

According to the provisions of article 360 of New Romanian Criminal Code1
(1) The unauthorized access to a computer system constitutes a criminal offense, which is punishable by imprisonment from 3 months to 3 years or a fine.
(2) As stipulated in paragraph (1), the act committed for the purpose of obtaining computer data is punishable by imprisonment from 6 months to 5 years.
(3) If the offense referred to in paragraphs (1) is committed regarding to a computer system that, through some procedures, devices or specialized programs, the access is restricted or forbidden for some categories of users, the punishment is imprisonment from 2 to 7 years.

The generic legal object of the offense, which is in fact common to all types of computer crimes, consists in the social value called computer system and in the social relations that arise in connection with the use of computer systems2.

---

1 Email: ia_barbu@yahoo.com.
The specific legal object consists in the interest of the owner, the holder or user of the legally protected computer system, but also of the legal owner, holder or user of the computer data stored or disseminated in that system.

As a result of the criminalization provisions, computer crimes have two or more specific legal objects, as they affect two or several social values. One of these legal objects is primary, whereas the other/other is/are adjacent or secondary. For example, the unauthorized access to a computer system connected to a state’s national security endangers both the national security and the accessed information.

The material object of the offense is represented by the material entities that make up computer systems (computers, networks, hardware - peripheral equipment, wires, plates, servers and so on).

The subject of the offense

The active subject can be any criminally liable natural or legal person and it is not circumstantiated in any way. Judicial practice has shown that perpetrators are usually people who possess solid knowledge of information technology. Actually, many of these offenders are experts in computer systems and computer networks and are skilled in “breaking” the protection systems of these information networks. Participation is possible in all its forms: co-participation, solicitation, conspiracy.

The passive subject is the natural or legal entity owning or legally possessing the computer system or computer data accessed without authorization. When the computer data targeted by the illegal access refers to a natural or legal person other than the rightful owner or holder of the information system, then we can speak of a secondary passive subject. The literature exemplifies the illegal access to an integrated computerized record of individuals and the access to the personal data of an individual.

The objective element of the crime

The material element is achieved by the unauthorized access to a computer system. The access involves entering the entire system or only part of it. But the access method is rather irrelevant. In its simplest form, the unauthorized access to a computer system consists in the perpetrator’s interaction with the information technology via devices or components of the targeted computer

---


4 The indictment of the Prosecutor’s Office of Iași Appeals Court served to determine that the defendant, C.D., had to be sent to trial for committing the offenses stipulated by and punishable according to article 46, paragraph (2) of the Romanian Law no. 161/2003. According to the indictment, the defendant had developed a new version of the MS Blast computer virus, called Blaster, which he illegally possessed and distributed, thus infecting a series of 27 computer systems. The defendant, C.D., was working as network administrator of the a certain company in Iași and was great on IT and interested in issues related to computer system security. In M. Zainea & R. Simion, 2009, *Computer crimes. Reports of judicial practice*, Bucharest: C.H. Beck Publishing House, pp. 29-32.

5 M.A. Hotca & M. Dobrinoiu, p. 577.
system (power supply, power button, keyboard, and so on). The illegal access in its simplest form can be achieved by intruders who are able to remotely manipulate their own peripherals, to find and use an external way of access a certain computer system. A classical example is the access to another computer in the same network. Pursuing the unauthorized access, the perpetrators will try a variety of technical procedures such as the password attack, trusted access attack, the exploitation of technological weaknesses etc.

According to the legislation, the perpetrator should have acted without authorization so as the attack may be considered an offense. This signifies that the offender was not authorized by virtue of the law or any other contractual relationship to have access to the computer system or information.

As previously mentioned, to gain access to a computer system the perpetrator will try a variety of techniques such as password attack, trusted access attack, the exploitation of technological weaknesses, shared library attack, IP attack or attack by TCP hijacking.

**Password attacks. Cracking network passwords.** To understand the hackers’ methods of operation in network password attacks we can refer to Windows operating systems.

To retrieve passwords from a Windows NT network, a hacker must have access to at least one username to implement MD4 algorithm. Once the database is copied (the only place where the user name and MD4 function can be found), the hacker can perform an hostile overtake or a dictionary attack against the password file.

Because only the system administrators can access the location of the Windows NT in the database, the only way the hackers may find the database is either the console or a backup of the database. In other words, to get to the database, the hacker must have physical access to the console or to the copy of

---

6 *Internet Protocol* identifies various network devices finding out what networks these are located on and what are the elements that describe the IP address. It represents a unique string of numbers that identify a computer from the Internet environment. As a rule, such numbers are grouped in series separated by dots, for instance: 134.137.23.69. Everything that “moves” on the Internet has an IP. It is also an identifier for a computer or device on a TCP/IP network. In S.A. Vasile, 2008, *Dictionary of Applied Informatics and Information Technology*, Craiova: Sitech Publishing House, p. 143.


8 *Transmission Control Protocol* is a full-duplex connection and it deals with the detection and correction of transmission errors. It receives data blocks and divides them to later be numbered. At the destination it will be able to put together the data received from the “emitter”. A data communication protocol developed by the USA Ministry of Defense underlying the creation of the Arpanet networks and then the Internet TCP is a protocol that ensures the safe transfer of a datagram from the emitter to the receptor without guaranteeing a time limit of the transfer.

9 Operating systems created by Microsoft Corporation.

10 *Make directory.*

11 Maxim Dobrinoiu, p. 149.

12 Backup of a file or set of files created regularly to ensure recovery of data in case of accidental loss.

13 Located, for instance, on a repair disk.
the database. If the server and the backup copies are physically secure, the risk of an attack via the password database is significantly reduced.

**Trusted access attacks.** Trusted access attacks frequently occur in networks that use an operating system (including *Unix*, *VMS* or *Windows NT*), which incorporates free access mechanisms. These mechanisms are a very weak point of the systems. For instance, in the *Unix* operating system users can create trusted host files that include hostnames or addresses a user can employ to access the system without a password. When connected in such a system, the user must use only the *login* command or any other similar command. Thus, a hacker can get an extended control of the system if he/she guesses the name of a trusted access system or a combination *host* - *username*. And worse, most hackers know that many *Unix* system administrators configure *.rhost* files in the root directory so that users can quickly move from one *host* to another using the privileges of the so-called „superuser”. Several *Unix* system administrators begin to realize that the use of *.rhost* files can be an expensive facility. These files allow a skilled hacker to easily gain unauthorized access to the root directory.\(^\text{14}\)

**Exploitation of technological weaknesses.** Attacks exploiting technological weaknesses include the trusted access attack discussed above, and many others. Every major operating system has its weaknesses. Some are easier to access than others. However, it is less likely that a hacker can detect such weaknesses. For instance, a recent version of *Microsoft Internet Information Server*\(^\text{15}\) contained an error that could potentially damage the system. System would have given in if the hacker had inserted in his *browser*\(^\text{16}\) a unique *URL*\(^\text{17}\) with several numbers when accessing that site. The *URL* is very long and unique to each system. Yet, the likelihood that hackers exploit this flaw is very small.

**Shared library attacks.** These attacks exploit shared libraries most frequently used in *Unix*. A shared library is a set of common software functions, which are loaded into a *RAM*\(^\text{18}\) file by the operating system at the request of each program.

---

\(^{14}\) Maxim Dobrinoiu, p. 153.

\(^{15}\) Auxiliary product for *Windows NT*

\(^{16}\) Web navigation software, which is the interface with the web environment and it has hypertext file interpretation and can navigate through Internet nods. It is used to navigate the Internet, to access the information available on the Internet displayed as web pages, but also to use most of the available Internet services. In S.A. Vasile, p. 49.

\(^{17}\) *Uniform Resource Locator* is the Internet equivalent of the actual address and operates similarly to other types of addresses by shifting from generic to specific data. Generally, it is the address of an Internet document. It contains both the file name and the information about the exact location of this file. In S.A. Vasile, p. 259.

\(^{18}\) *Random Access Memory* is the memory that can be randomly read or written and a single memory cell can be accessed without the use of other cells. Practically, it is the computer’s work memory and it is used in the temporary processing of data, which must be stored (saved) on a device that is not directly linked to a power source to preserve the information. The software data and instructions are stored so as the CPU (Central Processing Unit) can directly access them via the CPU high speed data bus. In S.A. Vasile, p. 222.
The hacker often replaces the shared libraries programs with new programs that serve his/her purpose, such as privileged access permission.

TCP hijacking attacks. Perhaps the most dangerous threat to the servers connected to the Internet is TCP hijacking. Although sequence numbers TCP prediction and TCP hijacking have many common elements, the latter is different because the hacker has access to the network by forcing it to your own IP address as a credible network address, and not by repeated attempts to test multiple IP addresses until the right one is found. The essential idea underlying TCP hijacking attack is that the hacker gains control of a computer connected to the target network, and then disconnects the computer from the network and make the server believe that the hacker has replaced actual host\textsuperscript{19}.

After he successfully hijacks a credible computer, the hacker will replace the target computer's IP address in each packet with its own address and will simulate the target sequence numbers. Security specialists call this process "IP simulation". A hacker simulates a credible IP address on their own computer system using IP simulation. After simulating the target computer, the hacker will use an intelligent simulation of the sequence numbers to become the server’s target.

To illustrate the context and the modes of unauthorized access to a computer system, we shall refer to case investigated by the General Directorate for Combating Organized Crime and Drug Trafficking within the Romanian General Police Inspectorate\textsuperscript{20}. In April 2003, the FBI liaison officer in Bucharest informed General Directorate for Combating Organized Crime and Drug Trafficking that the servers of four U.S. companies offering various Internet services were accessed without authorization and confidential information about customers was stolen. According to the clues the investigators had at that moment the criminal activity was initiated in Sibiu, Romania.

Subsequently, the individuals who had accessed the databases and stolen secret information threatened the victims demanding each of them approximately $ 50,000 so as not to publish the stolen information. To identify and prove their criminal activity a series of specific activities were carried out such as conducting in collaboration with FBI officers two controlled deliveries of money. Thus, as a result of these activities several persons were identified: O.Ş.A., aged 21, a student who had intruded the U.S. companies’ servers and threatened the customers with the publication of confidential data, M.E., aged 25, a student, and Ş.C.V., aged 25, an Internet Café administrator, who had conspired to intrude the U.S. companies’ servers; Z.S.N., aged 25, unemployed, and L.F.I., aged 19, a student, who had to receive the money gained from the illegal activities, and N.R.L., aged 18, unemployed, on whose behalf a credit card

\textsuperscript{19} L. Klander, pp. 430-431.
\textsuperscript{20} File no. 122/D/P/23.09.2003.
account had been opened in order to be used to collect the money. On June 2, 2003, O.S.A. and Z.S.N. withdrew U.S. $1,500 from several ATMs in Sibiu, money which had been transferred to N.R.L.’s credit card account by one of the blackmailed U.S. companies.

Being conducted by a prosecutor of the Prosecutor’s Office of the Supreme Court of Justice, the Directorate for Combating Organized Crime and Drug Trafficking organized several raids at the suspects’ homes and at the Internet Café, when police officers found 1,500 USD in cash, the credit card, the computers containing the stolen information and other evidence. O.S.A. and Z.S.N. were arrested for committing the crime of unauthorized access to a computer system and illegal transfer of data, and the others were under investigation without being taken into custody.

The immediate consequence consists in the change that the criminalized act produced in outer reality. This change can be the alteration of a situation or condition, a material transformation of the object of crime. Practically, the consequence of a simple unauthorized access to a computer system is a state of insecurity of that system.

If the goal of the intrusion was to gain unauthorized access to computer data, then the computer system’s insecurity is doubled by that of the data stored in or processed by that system.

Legally speaking, in terms of the consequences generated by the criminalized act on the social value that is the object of the offense, the result is a state of danger or threat to the computer’s IP address or address space.

The perpetrator’s action and the consequence of his action have to be causally linked. The causal link is an ex re result, that is the consequence of the action’s materiality if the unauthorized access to a computer system is a simple offense (the basic form of the offense). Secondly, if an unauthorized access has taken place, the violation of the security measures has to be proven.

The subjective element of the offense. The offense of unauthorized access is committed with direct or indirect intent. When obtaining computer data (paragraph 2), the intention is qualified by purpose.

Forms and methods

Although possible, preparatory acts are not criminalized. The attempt is punishable under article 366 of the same law. The perpetration of the offense referred to in paragraph (1) is considered to have taken place when the offender directly or remotely intrudes the computer system resources. The offense referred to in paragraph (2) is considered to have been committed when the intruder attacks the security measures, whether he has been successful or not in neutralizing or removing them.

21 Maxim Dobrinoiu, p. 149.
The offense in question has only one normative form expressed by its material element, that is by the unauthorized access to a computer system. This normative form can be matched to various factual forms. The law also stipulates two aggravated forms. The act is worse (paragraph 2) if committed for the purpose of obtaining computer data or by breach or removal of security measures (paragraph 3).

References