THE FORMS AND DEFENCE POSSIBILITIES OF THE THREATS AGAINST COMPUTER NETWORKS

Valéria Póserné Oláh

Budapest Polytechnic John Von Neumann Faculty of Informatics Institute of Software Technology, PhD student

Dr. Zsolt Haig PhD.

Zrínyi Miklós National Defence University, Information Technology Department

Abstract

In developed countries, the growing danger of attacks against information is one of the major problems of the present age, especially because by now, the Internet has become wide-spread almost everywhere from the civil sphere of the world economy up to the administrations. Illegal offence against any information system can turn out to be critical, be it either bank, financial system, telecommunication, traffic, energy provisions or any military or other defence institutions. Furthermore, a possible attack can damage the state infrastructure seriously. Therefore, the main aim of this article is to introduce the different kinds of computer criminals and their devices as well as map the illegal invasion possibilities and show some modes of prevention.

Introduction

The natural process of the 21st century is the rapid and unstoppable development of the information infrastructures in many countries. At the same time however, the information ally developed countries are also exposed to an increasing danger due to the fact that the Internet is present almost everywhere from the civil sphere of the world economy up to the administrations. The more complex, the more overall and developed the information infrastructure of a country is, the more serious damages can be inflicted upon it by an "invisible enemy". Military institutions, banks, the police, traffic and financial systems, telecommunication and energy provisions all can serve as potential targets along with the possibility of harming the state infrastructure to a significant degree. Moreover, while attacks against any information system maybe critical, violation of defensive, especially military systems with emphasized importance are even more so. It is unthinkable to estimate the damage that an aggressor could cause by illegally invading the military computer network system – since any serious arms' system of the military forces almost totally depends on

intelligence- guiding- navigation- and targeting. Consider how great devastation could be carried out by a “Stealth” type of plane if an aggressor, having accessed the system, gave false codes to the computer on board. For instance, a nuclear rocket, launched according to the false data, would immediately fly onto the target co-ordinates provided by the aggressor. For this reason it is a crucial responsibility to map the attack possibilities and the ways of their prevention. The purpose of this article therefore is to introduce the different kinds of computer and criminals, their devices and the ways to keep information systems, computers and personal data safe.

1. Information operations fundamentals

In the information society, information superiority is a key enabler for victory in future warfare. One of the strategic elements of information superiority is the capacity to collect, process, and disseminate an uninterrupted flow of information. The other crucial component of is the ability to protect one’s own information systems against threats. Therefore, modern warfare information operations (IO) must consist of these basic capabilities. Furthermore, information operations have core capabilities such as electronic warfare, computer network operations, psychological operations, military deception and operations security. These can be used both in offensive and in defensive function. As it is obvious, the computer network operations constitute a fundamental part of the information operations, due to the fact that the modern digital battlefield is constructed by a complex system of computer networks connected to each other.

According to a new theory, in Network Centric Warfare (or Network Enabled Capabilities) these computer networks’ vital role is collect and analyse as well as disseminate information to the shooters.

Computer network operations are the following:

- **Computer network attack (CNA):** It uses the computer networks to disrupt, deny, degrade, or destroy information saved in computers and computer networks, or in a worse scenario, to wreck computers and networks directly.
- **Computer network defence (CND):** This uses computer networks to protect against as well as monitor, analyze, detect and respond to unauthorized activity within computer networks;
- **Computer network exploitation (CNE):** It is the use of computer networks to gather data from the target computer or from adversary computer networks.

Computer network attack can be carried out by state and non-state agents. They have the potential knowledge and resources to invade the defence computer networks. Due to the relative low cost of CNA techniques and technology, recently, several states have shown interest in developing such capabilities.

Fundamentally, the circle of aggressors against information systems can be sorted into four categories as illustrated in Figure 1:

- Unauthorized Users (Insiders, Non-state Agents);
- Terrorists;
- Intelligence Services;
- Military Organizations.

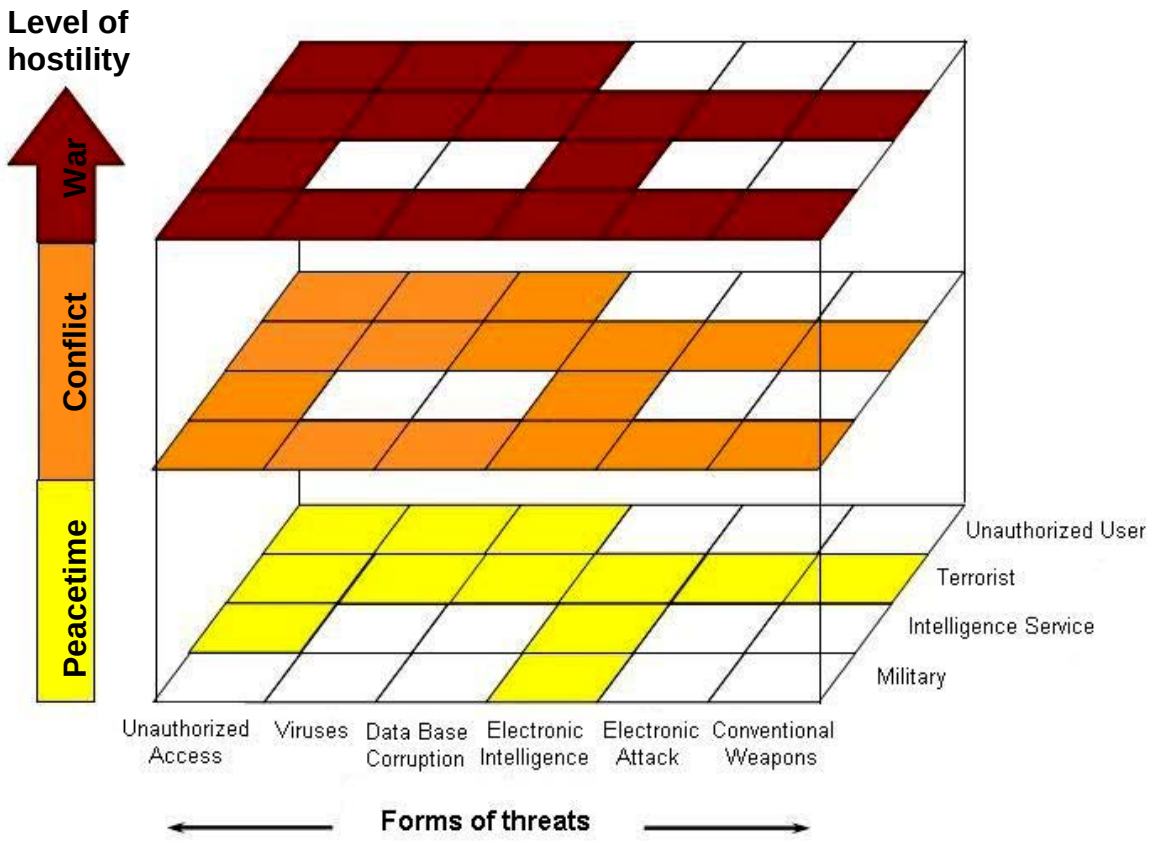

Figure 1. The forms of the threats against military information systems [1]

Out of the above four, this article aims to deal with the first item in detail. This is all the more important since unauthorized users can become potential threats to defence systems. For instance, many terrorist organizations use unauthorized personnel (hackers, crackers) to log in an adversary computer network, and disrupt, deny, degrade, or destroy their databases.

For this reason, first the meaning of "unauthorized user" will be clarified, which is followed by the development and transformation of such agents.

The informal names for unauthorized users are "hackers" or "crackers". These two notions nowadays have come to be perceived as the same thing partly the media. There has been a common culture of excellent programmers and net magicians since the time of the very first Arpanet experiments. During this period of time the expression of "hacker" practically has become a household word. Besides developing the operation system, they also run news centres and keep the WorldNet under their control. [2]

2. Some language analysis

Hacker, cracker: the two words are synonyms; their meanings are a "breaker" or "cracker" of codes and "an illegal invader" of secret Network systems. In the English language the verb "hack" means "break", "smash" and "crack". It is also sound imitating word meaning "break", "break in" and "break up". According to the original meaning the differences appear to be minor, but in fact, in function the dissimilarity of the two words becomes evident.

The notion **"hacker"** originally carried the meaning of a "computer addict" who considers it to be a challenge to solve different kinds of computer problems, as well as explore and eliminate the security gaps within the information systems. They learn the programming language very quickly and absorb the existing knowledge in no time. Characteristically a hacker's actions are governed by goodwill, and since he has got serious principles he is always true to his colours at whatever cost. When he breaks into different systems, he does it for the sake of challenge without intending to cause any damage. By doing this he in fact aims to draw the attention of the system administrator to the gaps and errors of the system, well before a "cracker" could also find the same entry. Moreover, he shares the acquired information with other hackers too so that the arising problems can be dealt with more effectively. [3]

"Crackers" on the other hand are criminals, who break into databases and gain information by double-crossing the security systems of the particular software – protected by law –, causing severe problems to programmers and alike. They in fact deliberately inflict damages on different systems. The following excerpt is from a correspondence forum. It describes vividly the distinction between hackers and crackers. *"If, in the morning, you get to your car and notice that its door is open, but at the same time somebody repaired the radio and the CD player that has been out of order for weeks, works again, you can be sure you were visited by a hackers. But! If you notice that the back windows of your car were broken*

out by a half brick and they pulled out the radio and all the valuable built-in electronics than your visitor was a cracker."

In summary, the basic difference between them is that hackers build up while crackers tear down.

3. The hacker society today

Real hackers: They constitute the top of the hacker society. The original meaning of "hacker" actually refers to them. They in fact are the best system administrators and organizers. They keep an eye on security systems of multinational companies thus, when a gap occurs they ward off the attack, correct errors and improve the system.

Light hackers are those who crack different kinds of websites. Their number is very large. For example in the USA, some undergraduate have become notoriously famous by changing the homepage of the FBI to a porn website. Or, for instance in Hungary, a hacker, who calls himself "The Phantom", put destructive captions on one of the largest service provider's homepage. Light hackers therefore bear very little resemblance to real "hackers".

Dark hackers i. e. "evil" hackers: They are in fact the actual "bad boys". Their activity is controlled by their eagerness for gain and/or revenge. They may release different data acquired illegally, may obtain money from bank accounts or may create internet viruses and format the hard disk of the user's computer. They are simply criminals.

Phreaks: They are the experts of computer-controlled telephone exchanges, experts of telecommunication in general so they can use non-contributory telecommunication network. Phreaks have sufficient knowledge and have the appropriate devices to reprogram and monitor the flow of the internal data of mobile telephone networks. As a result, they and those to whom they pass on the illegally obtained information can make phone calls at the expense of others. For this reason they also belong to the "criminals" category.

Wannabe-hacker: As their name shows, they are those who are aspiring to become real hackers. However, they are not able to write their own program, thus, they use hack-programs prepared by somebody else. Thanks to this they are more or less successful.

Troll: These are comprised by the youngest generation. They are usually very enthusiastic but are not exactly experts in the field of computer technology. They are similar to wannabe-hackers in terms of using programs made by others, especially light hackers. The difference however is that they do not have the faintest idea about what they really do. (These in fact the first attempts of hacking of the youngest computer generation).

Difter is someone who by browsing on the internet happens upon something of interest on someone else's computer which he copies it for himself. His activity usually remains unnoticed. The only sign that points to the presence of a difter is the flashing of the TRANSMIT LED on one's modem without any apparent reason. [2]

Several groups, including 15 to 25 year-olds, have come into existence both in the USA and in Western Europe and are well-known all over the world. The Legion of Doom (LoD), the Masters of Deception (MoD), the Cult of the Dead Cow (cDc) or the Dutch Hack-tic are just a few examples of them. Within a group, there is a strict division of labour since each member is highly specialized in one particular area of information technology. For instance, one may explore the discarded materials in one's recycle bin searching for login names and/or passwords, thus, the most essential defence against such invaders is to store any user name and password securely. One may operate the so called "war dialler" that is capable of dialling thousands of telephone numbers expecting to tumble on a modem. The list of the numbers found in this fashion is saved in their own insider network. This way these numbers not only turn into potential targets but also become available to all inside such network. Finally, one may examine the operation of the postal services. Through that, they provide the exact descriptions how to set up different coloured boxes (such as blue box, red box, etc.) to outwit telephone companies. By using these boxes they can make telephone calls at a reduced rate. In addition, all this information is published on BBS, on different servers, on the lists of the News groups, and in temporary issues. [4]

4. Devices, which can be used for the purpose of offence

The emergence of the hacker subculture produced unprecedented in past Revolutions in Military Affairs, namely a glimpse of how the future may look. Even in a best-case scenario, where the compromised system could be restored from backups, have its security holes plugged, and be reconnected, the attacker has managed to deprive users of its services for several hours at least. Just like the delays communications jamming can cause to command and control, this effect could be useful to an attacker. So even if the Digital Pearl-Harbour itself does not occur, successful espionage and harassment carried out through CNA might enable an adversary to carry out a real Pearl-Harbour-like surprise attack. [5]

With the help of the following programmes computer networks, both civil and defence, can become vulnerable. This is in spite of the fact that cracking a military system is far more difficult than entering into a civil system due to the enormous difference between the

technologies and the strategic systems' development of the two.

Cracker – password hacker: This programme either needs to be written or to be downloaded from the Internet. Naturally, the first option is the more difficult because one has to be familiar with not only the algorithm of constructing passwords – that conceal the operation system of the target computer – but also with the programming language.

Sniffer – an analyser and interpreter programme: Sniffers are programs or hardware that help one to listen into the computer network's flow. This is possible on networks where several computers are connected and share a physical line, thus, the information on the line is becomes available for anybody. The Ethernet is the perfect example of such activity. There are many sniffers in circulation; they can be purchased as a part of some network-control device, and for this reason they are actually quite expensive. In connection with them, it is vital to know that they can not be detected from the outside, therefore beginner offenders freely use them without running the risk to be revealed by the system administrator.

Backdoor – back entrance: This is usually an error in the target operation system that makes it possible for somebody to get permission without being noticed by anyone, not even by the operation system. One classical example of the Backdoor was the Gatedmine.exe – that was neutralized by a patch some time ago. This program enabled a simple user to have access to the group of administrators, by exploiting the error of the Windows NT API call. Furthermore, Backdoor is also a user name and with its help the invader can enter the system again and again.

Fake login: This program can be written by the invader in most cases. The point is that a fake login interface – identical with the real – starts before the original one. The victim may think that it is the real login window and provides the password, which in turn is saved by the invader's program. After some error message the user might encounter with the real login interface. However, in case of a successful operation the deception is in fact impossible to be noticed.

OpenPass: They are tiny programs that are available anywhere on the Internet and are used to discover passwords. Nowadays they are not utilized so often since the most recent programs are immune to their operation.

Portscanners: A portscanner is a device that recognizes the open ports of another computer. A PC for instance can have 65536 different (TCP) ports altogether, but only some

of them are open and through them one can establish a connection to a computer. There are several different kinds of portscanners in existence. They help find a given IP-area, or a given point-area, to store and send a message (that can be set up to the ports that are opened), to take a message, to measure the opening hours of the closed ports, to setup the opening time between openings of ports…etc.

Trojan – the Trojan horse: This program seems to be harmless but when it runs, it does not do what it should do. These programmes have two parts. The smaller part is the "server" while the bigger is called the "client". To get unlimited control over other computers the server needs to reach the victim. The general and the simplest way to achieve this is to send an e-mail to someone with a name that inspires confidence, such as "brietnyspears.exe", and trust that the victim opens it. After that the IP numbers can be retrieved. This way the aggressor gains unlimited access to the victim's computer.

Keylogger: As the name suggests it stores data given by the keyboard. There are different kinds of keyloggers, however they are not viruses unlike the Trojans. This in fact has to be put on the victim's computer by the aggressor directly. (There are some Trojan programs that contain this function also). Keyloggers register every starting of operation system and they save the date if we want it.

WinGate servers: WinGate server helps an IP address become unnoticeable. For example, if one connects one computer to another, it can either serve as an intermediate computer or it may function as a firewall.

E-mail bomber: They swamp the mailbox of the victim with a large number of junk anonymous email. Once the inbox is full, it can not receive new messages. In addition, it usually takes quite some time to download and to delete such messages. Email bombers are for example, the newest versions of Avalanche and Kaboom programs. They are quick and contain the functions of WinGate usage, bombing with error messages, and built-in insulting programs (English version).

Buffer overrun: Here the purpose of the aggressor is to find programming errors in the operation system of the target computer and take advantage of them. Thus the required program does not do what it is supposed to – even if the parameters are correct –, but runs according to the codes provided by the aggressor.

Denial of Service: In this case the aim of the aggressor is to break down the victim's computer system. Thus the victim unsuspectingly restarts the PC in the belief that the earlier installed program will start once the computer is rebooted.

Replay: The ways to login to the Windows operation system are all replay resistant, thus this method is restricted to the replay of the flow after logging in. This however might be the repetition of SQL polling.

Hijack - diversion: It usually refers to the diversion of TCP channel, in such a way for example, that a complete, built-up, identified and certified TCP channel is simply taken out of the control of the legal user by the aggressor. The aggressor then sends requests to the server which responds automatically. This requires a complex operation range. On the one hand, the information link has to be collected together with the Sniffer in order to enter in the TCP channel. On the other, the original user has to be muzzled by the Denial of Service. The chance to accomplish this with precise timing and without error is not very high. The Hijack offence is so called "Man in the middle", wherein the aggressor communicates with two computers at the same time. As a result, both command and answer flow passes through the aggressor's system, who in turn can falsify the data.

Viruses: Another damaging area of the information technology is viruses. These are usually constructed by hackers and can cause inestimable damage. However, creating a more serious virus requires high level of competence.

Hoaxes (computer false reports, deceptions, rumours): Computer hoaxes can mingle with real virus threats that is being spread on the Internet and with messages that warn of the danger. Although, they do not infect whole computer systems nevertheless they waste time and money by getting users to spread false information (for example: unnecessary load of networks).These kinds of warnings either should not be sent further or before forwarding it to others one should ask an expert's opinion. [6]

5. Computer defence

It is important to protect one's computer, no matter if it is a defensive system, or a private PC. For this reason, the experts of AvantGarde Company examined how long a computer is able to run without a virus remover, a firewall or other security programs. They connected six computers to the Internet for two weeks, using different operation systems on each computer. The result presented in Table 1 below is not surprising. During the two weeks the six computers were attacked 305 922 times by different harmful and malicious programs.

Configuration	number of offences	per cents
Windows SBS 2003	25222	8.24
Widows XP SP1	139024	45.44
Windows XP SP1 with ZoneAlarm 5.1 (Free)	848	0.28
Widows XP SP2	1386	0.45
Ac OS X 10.3.5	138647	45.32
LinSpire (Linux)	795	0.26

Table 1. The survey of AvantGarde Company [7]

The most often attacked PC was the one running the operation system Windows XP with No. 1 service pack. For the first violation the experts had to wait for only four minutes. During the tests, Linspire, running No 1 service pack, Windows XP, provided with the copy of Zone Alarm firewall programme and Windows XP – completed with No 2 service pack performed the best. These three PCs and operation systems accounted for 0.3-0.4 percent of the total attacks only.

In the case of the computer running Mac OS X 10.3.5 operation system, the situation came to be very interesting. Although, 45 percent of the harmful action aimed at this computer, the worms, to which the Windows operating system and its security gaps have been immune to, could not cause harm to Mac either.

Aggressors usually eagerly take advantage of any possibilities when a defence system is protected by weak passwords or a security gap appears in the software. It is important to emphasize that there is no perfect defence for any computer against harmful invasion. Nevertheless any user must make sure to have safe passwords and a regularly refreshed virus remover program along with a firewall.

6. Computer network defence possibilities [5]

The computer network defence can be passive and active. The passive defence systems are well-known to most users and are utilized by every computer network. The active defence measurements and processes are generally employed by military organizations, and intelligence services.

The passive defence covers:

- **Firewalls**: They are either a combination of software and hardware, such as the PIX Firewall 4.1 supplied by Cisco to work with its routers, or a software application by itself, such as Norton Personal Firewall that continuously monitors the data-flow. In the case of a suspect entry, they interrupt the connection, alarm the system and immediately

check the existing files. It is however important to note that these programs are also breakable, therefore using the software application of the firewalls on their own may not provide adequate protection.

- **Antivirus software**: They are the most basic protection forms; an effective antivirus software can be the crucial second line of defence for a particular network. The virus protection programs search and remove viruses, worms and Trojans automatically, without any interruption to the user. They are capable of recognizing spy-software and are able to offer protection against potentially damaging programs on the user's computer – these would spy the users data or watch the system's Internet connection. Therefore the regular updates of software and of the virus signature lists are crucial as well as scanning the system regularly. The computer can be easily adjusted to automatic downloads and installation of updated virus signatures, and to scheduling automatic virus scans on each PC of the network. The heuristic antivirus software operates differently from the above outlined system. It does not have a virus database, but instead, it observes the different programs' behavior, and if it is necessary, it prevents them from running.
- **Access control**: Users are assigned to different levels of permission that determine which directories and files they may or may not access. One of the levels is the "root" access that is the most powerful since it has permission to reach and alter any directory or file in the network. The other level of permission is the so-called "user" access that has the least permissions. Users have a private directory where they can store files and create directories. Also an intermediate level may exist, such as the "superuser" that allows the system administrator to delegate specific routine tasks. Access to an account at this level is, typically, protected by a password. It is important that passwords must be chosen carefully, to be remembered easily yet it must be safe nevertheless they need to be changed time to time.
- **Intrusion detection and adaptive response tools:** The former scans the application logs and processes looking for abnormal activity configured by the system administrator. In case it finds such, it alerts the system administrator immediately. Adaptive response tools are intrusion detection softwares with automated responses, allowing a network to "defend itself" against any attack. They are the most recent developments.

The active defence includes:

- **Preemptive attacks:** One has to know the structure of the computer network of the adversary to execute this operation. For instance one has to be familiar with the defensive solutions that are used and with the means and skill of attack. This operation is in fact a reconnaissance of the adverse computer network. Before taking any action, one needs to chart how these networks' infrastructure can be attacked most effectively.
- **Counterattacks:** In case of the failure of the preemptive attack this method should be applied. In order to launch a suitable and effective counterattack however, one needs to determine the source of attacks and has to chart the network structure of the aggressor by means of reconnaissance.
- **Active deception:** In this case a virtual network is operated, which has a real database in order to deceive the adversary. To this network the access is purposefully made easy in order to "invite" the adversary's attack. During the offence the adversary's methods and techniques are detected. This enables one to prepare adequately for a system invasion.

The dangers to network systems have been spreading quickly and significantly, while at the same time, they are becoming more and more complicated. Therefore it is inevitable for both civil and military systems to develop a fundamental defensive solution that are able to deal with the more and more serious threats.

Summary

Since the war in Kosovo, it has become apparent that the Internet can serve as a basis for disasters in any state or country. Since conflicts may happen on the Internet as well, thus the possible damages are not limited to physical war activities anymore. A political/state system can become destabilized or even destroyed completely in the shortest time period in case of an inclusive information attack on more than one stage at the same time.

Hackers nowadays are those youngsters, who are experimenting with the computer technology merely out of curiosity and for the sake of adventure. They can find all the necessary hacking programs on the Internet together with their explanations, so no wonder that it becomes hard to resist temptation. No doubt, this age is the golden era of computer crimes and, unfortunately, this situation will not likely to change, despite the fact that the devices continually improve. Nevertheless the task at hand is to try to protect the computer systems against illegal invasion and make sure that all data is safe either in the case of civil or

military information systems. Still, it must be kept in mind that so far there NO PERFECT defence system exists.

References

[1] Dr. Haig Zsolt-Dr. Várhegyi István: Információs műveletek I., egyetemi jegyzet, ZMNE Budapest, 2004.

[2] ERIC S. RAYMOND: How To Become A Hacker? http://www.catb.org/~esr/faqs/hacker-howto.html 2005.05.24.

[3] CS. PLÉH: Számítógép és személyiség. Replika, 30. 1998. június.

[4] Kik ezek: hacker, cracker és phreak? http://x3.hu/freeweb/frameset.x3?user=/thewarenavigator&page=/hackcrackphrek.html

[5] ERIC J. HOLDAWAY: Active Computer Network Defense: An Assessment. Maxwell Air Force Base, Alabama, April 2001. www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2001/01-055.pdf 2006.06.15

[6] www.warforge.com 2006.05.24.

[7] Berta Sándor: Négy perc jut egy Windows XP-t futtató védtelen PC-nek http://www.sg.hu/cikkek/34787/negy_perc_jut_egy_windows_xp_t_futtato_vedtelen_pc_nek 2005.05.24.