Malicious Software Attack

Session 10

LEARNING OBJECTIVES

On completion of this session you should:

- Understand the threat of malicious software
- Be familiar with different types of malicious software
- Describe how trap door, Trojan horse, logic bomb and Zombie work
- Understand how virus and worm work
- Be familiar with different types of viruses
- Discuss the countermeasures that can be employed to prevent virus and worm attack
- Understand how Distributed Denial of Service (DDoS) attacks are launched and discuss the lines of defence against DDoS

Contents

Reading

Prescribed readings

Reading 1: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 355-359.

Reading 2: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 360-365.

Reading 3: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 365-379.

Reading 4: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 379-384.

10.0 Introduction

Although software programs are intended to increase productivity and efficiency, and to automate activities that would otherwise require human intervention, unfortunately they have been used by people with malicious intensions to exploit the vulnerabilities in the computing system. Over the years numerous incidents of malicious use of software have been reported. Many of us are also victim of virus or worm which are the examples of such programs. Malicious programs can be broadly categorized into two categories: 1) host dependent malicious program that cannot exist independently of some applications or system programs, and 2) self contained program. It can also be categorized as replicating or non-replicating program. A replicating program, when executed, may produce

one or more copies of itself to be activated later. A non-replicating program is activated when the host program is invoked to perform a specific function.

10.1 Types of Malicious Software

Stallings has divided malicious programs into the following types [1]:

- Trap doors
- Logic bomb
- Trojan horses
- Zombie
- Virus
- Worm.

In this study guide, we briefly discuss all of them with particular emphasis on viruses and worms.

10.2 Less Common Types of Threat

First we discuss less common types of attacks. These are: trap doors, logic bombs, Trojan horses and Zombie.

Trap doors (back door): A trap door is a secret entry point into a program that allows someone to gain access without going through security access procedures [1]. These are undocumented entry points written in code for debugging purpose, but hackers can use these points to gain unauthorized access. Usually an application program has an authentication procedure and/or a lengthy setup requiring the user to enter many different values. For debugging purpose, the developer may leave some code that allows him to gain special privilege to bypass authentication or necessary setup. The programmer may also want to ensure a method to activate the program if authentication procedure goes wrong. Trap door recognizes special sequence on inputs triggered by being run from certain user ID. It is difficult to block trap doors by the operating systems. The best practice is to focus on software development and debugging process.

Logic bomb: Malicious code embedded into a program that activates when certain conditions are met, e.g., a particulate date.

Trojan horses: Torjan horses are hidden malicious code in a otherwise good program, but when activated can cause disastrous consequences, e.g., sending data or password to the attacker over the Internet. As named after the Trojan horses, these programs act as a delivery vehicle. It does something undocumented which the programmer intended, but that the user would not approve of if he/she knew about it. There have been many Trojan horse programs reported so far and the new ones come up very often. Most anti-virus programs can't detect new Trojans, but usually once their circulations are reported they can be detected and removed. So, it is important to know and trust the source of any program before running it.

Zombie: Zombies are used to launch DoS attacks. They secretly take over other computers and use them to launch attacks. Since the attack is launched from other computers, it is difficult to trace the zombie creator.

Reading 1:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 355-359.

10.3 Virus Attack

Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer like a biological virus passes from person to person. A virus attaches itself to another program and executes secretly when the host program is running. Any virus is designed to run first when the legitimate program gets executed. The virus loads itself into memory and looks for other programs on the disk to infect. If it finds one, it modifies that to add the virus's code to the unsuspecting program. Then the virus launches the "real program". Sometimes the user has no way to know that the virus ever ran. Now that the virus has reproduced itself, so two programs are infected. This cycle goes on as more and more programs are infected. Virus can infect a big portion of the computer's operating and file system. During its lifetime, a typical virus goes through the following four phases [1]:

- Dormant phase: The virus remains idle waiting to be activated by some events. Not all viruses have this stage.

- Propagation phase: The virus embeds a replicated copy into another program or certain system areas on the disk.
- Triggering phase: The virus is triggered by certain event.
- Execution phase: The virus executes causing harmful or harmless action.

How does virus work?

Most of the viruses generally work in the following ways (see Fig. 10.1 of the textbook):

1. A virus can be prepended or pospended to an executable program. The first line of code is a jump to the main virus program. The second line is a special marker to check whether the potential victim program has already been infected.
2. The infected program is modified so that when the program is invoked, control is immediately transferred to the main virus program. So instead of the proper code running, the virus code runs.
3. The virus code becomes active and takes control of the computer. There are two ways that a virus behaves when it is running: a) direct-action viruses immediately execute, many file-infector viruses are direct-action; b) memory-resident viruses do not do anything immediately; they load themselves into memory and wait for a triggering event. Many file infectors and all boot infectors are memory resident.

What exactly the virus does depends on what the author of the virus wants it to do. In general, viruses search for new targets through replication and spreading. Some viruses are designed to be activated only on a particular day of the year, e.g., the widely spread "Friday the 13th" virus.

Types of Viruses

Virus writers get creative and come up with increasingly more sophisticated viruses everyday. The most significant types of viruses can be categorized as follows [1]:

Parasitic virus: Most common type of virus. It attaches itself to executable files and replicates. When the infected program is executed, it infects other executable files.

Memory resident virus: Resides in the main memory and infects every program that executes.

Boot sector virus: Infects a master boot record or boot record. By putting its code in the boot sector, a virus is guaranteed to be executed. Boot sector viruses can infect the boot sector of any disk inserted in the infected computer, and spread very quickly in an environment where many people share computers.

Stealth virus: A stealth virus is explicitly designed to hide itself from detection by antivirus software. It actively hides any change it has made to the hard disk so that it appears that it has not infected the system. The virus takes over system functions that are used in reading files or system sectors. Looking at the system, it appears a clean, virus free system.

Polymorphic virus: A virus that mutates with every infection, making "signature" detection impossible. With every infection its appearance and size change. These viruses are more difficult to detect by scanning, because each copy of the virus looks different from the other copies. To detect this virus more than one method of viral detection should be utilized - good integrity checkers would find viruses of this type when scanners cannot.

Macro virus: This is the newest type of virus that exploits the vulnerability of macro programs, e.g., in Microsoft Office applications. Macro programs allow users to create programs that automate tasks and contain commands that include opening, manipulating, and closing files. Micro viruses are particularly threatening for: (a) they are platform independent, (b) infect documents, delete files, generate emails and edit letters, and (c) can spread easily.

Reading 2:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 360-365.

10.4 Worm Attack

A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another computer that has a specific security hole. It copies itself to the new computer using the security hole, and then starts replicating from there as well. Using a network, a worm can expand from a single copy incredibly

quickly. For example, the Code Red worm replicated itself over 250,000 times in approximately nine hours on July 19, 2001. To replicate itself, a worm needs some sort of networking connectivity including electronic mail, remote execution capability, remote login capability, etc. Since worms use up computer time and network bandwidth, it quickly clogs the system.

Some of the recent big worm attacks are Code Red Worm in July 2001, Nimda in late 2001. The Code Red worm slowed down Internet traffic when it began to replicate itself. Each copy of the worm scanned the Internet for Windows NT or Windows 2000 servers that did not have the Microsoft security patch installed. Each time it found an unsecured server, the worm copied itself to that server. The new copy then scanned for other servers to infect. In the second wave of attack, Code Red infected nearly 360,000 servers in 14 hours.

10.5 Countermeasures

The best solution is to prevent virus get into the system. But this is definitely an extremely difficult task to achieve. The countermeasure approaches consist of the followings [1]:

- Detection: Once infected, detect and locate the virus.
- Identification: Once detected, identify the specific virus that has infected a program.
- Removal: Once identified, remove all traces of virus from the infected program and restore to the original state.

Antivirus software packages are available for cleaning virus infections. Such as Norton, McAfee are popular antivirus software. Antivirus software can be divided into four generations.

- 1st Generation, Scanner: searches files for any of a library of known virus signatures. Checks executable files for length changes.
- 2nd Generation, Heuristic Scanner: looks for more general signs than specific signatures (code segments common to many viruses). Checked files for checksum or hash changes.
- 3rd Generation, Activity Trap: stays resident in memory and looks for certain patterns of software behaviour (e.g., scanning files).
- 4th Generation, Full Featured: combine the best of the techniques above.

Usually an antivirus software program uses some combination of the following three techniques for maximum possibility of detection:

Scanning: scanning depends on prior knowledge of a virus for detection. This is done by recognizing similar signature that represents/resembles to an existing virus or some program characteristic that gives an indication of a virus presence. Its main advantage is that it allows checking programs before execution.

Integrity checking: It reads the disk and creates signature information to determine changes. Advanced integrity checkers incorporate the capability to analyze the nature of the changes, and recognize changes caused by a virus.

Interception: Interceptors monitor OS requests that write to disk or do other things that the program considers threatening (such as installing itself as a resident program). Interceptors are particularly useful for deflecting logic bombs and Trojans.

Advanced antivirus techniques employ two other approaches like **generic decryption and digital immune system**.

Generic decryption technology is capable of detecting the most complex polymorphic viruses. It contains three elements: CPU emulator, virus signature scanner and emulator control module. When a file containing polymorphic virus is executed, the virus must decrypt itself to activate. The emulator intercepts instructions in the target code; if the code includes a decryption routine that decrypts and exposes the virus.

Digital immune system uses a comprehensive approach that combines monitoring programs, administrative machine and virtual analysis machine to automatically capture, analyze, detect and shield an entire organization.

Similar techniques can be used to deal with worms. Once a worm is detected, network activity and usage monitoring can be the basis of worm defence. Worm countermeasure approaches include:

- **Signature-based worm scan filtering**
- **Filter-based worm containment**
- **Payload-classification-based worm containment**
- **Threshold random walk (TRW) scan detection**

- **Rate limiting**
- **Rate holding**

Reading 3:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 365-379.

10.6 Distributed Denial of Service Attacks

Distributed Denial of Service (DDoS) attacks make the target computer systems or network resources inaccessible by flooding servers and networks. DDoS attempts to use a large amount of resources and could be classified in terms of the resources consumed. A simple example of an **internal resource attack** is the SYN flood attack. An example of an **attack that consumes data transmission resources** is using multiple hosts as reflectors.

Another way to classify DDoS attacks is:

- **direct DDoS**
- **reflector DDoS**

DDoS attack infects a number of machines with a zombie software that will ultimate carry out the attack. DDoS countermeasures include three approaches:

- **Attack prevention and pre-emption (before the attack)**
- **Attack detection and filtering (during the attack)**
- **Attack source traceback and identification (during and after the attack)**

Reading 4:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 379-384.

10.7 Conclusion

In a networked environment, virus and worm can spread very quickly. It can cost organizations huge financial loss in restoring the system to the original state and may cause loss of data. Antivirus software packages are available for detection and removal of viruses. Since new viruses and worms emerge at a regular basis, it is very important to update OS and application software patches and antivirus software.

10.8 References

[1] W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011.

[2] J.H. Allen, "The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001.