**Chapter 18**

**Computer Security**

*Lesson 18.1:* Computer Security Issues

*Lesson 18.2:* Protective Measures

****

***Lesson 18.1***

***Computer Security Issues***

**18.1.0 Objectives**

*On completion of this lesson you will know:*

* *About the basic of computer security*
* *About computer virus*
* *About the network attacks*

**18.1.1 Computer Security**

In computing, computer security refers to techniques by which valuable information and services of a computer network are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

The objective of computer security includes protection of information and allows the information to remain accessible and productive to its intended users. Basic security issues of different information systems are described below:

**Software Security:** The security of software is the idea of engineering software so that it continues to function correctly under malicious attack. It is threatened at various points throughout its life cycle, both by unintentional and intentional choices and actions taken by insiders and outsiders. The software’s security can be threatened by different ways as outlined below:

* **During its development:** A developer may corrupt the software—intentionally or unintentionally— during its development. It compromises the software’s dependability and trustworthiness when it is operational.
* **During its deployment (distribution and installation):** If a software’s distributor fails to tamperproof the software before shipping or uploading, or transmit it over easily intercepted communications channels, the software may be vulnerable to intentional or unintentional corruption. Similarly, if the software’s installer fails to “lock down” the host platform, or configures the software insecurely, the software is left vulnerable to access by attackers.
* **During its operation:** Vulnerabilities may be discovered and publicized with the use of open source software (OSS); unless security patches and updates are applied. Non-commercial software may also be vulnerable, especially as it may manifest untrustworthy behaviors due to changes in its environment. Any software system that runs on a network-connected platform has its vulnerabilities exposed during its operation.
* **During its sustainment:** If those responsible for addressing discovered vulnerabilities in released software fail to issue patches or updates in a timely manner, or fail to seek out and eliminate the root causes of the vulnerabilities to prevent their perpetuation in future releases of the software, the software will become increasingly vulnerable to threats over time.

**Data Security:** Data Security is a process of protecting a database from destructive forces or unauthorized access. Few data security techniques are discussed below:

* ***Disk Encryption:*** Disk Encryption encrypts data on a hard disk drive and then prevents data from being stolen. Disk encryption typically takes form in either software or hardware.
* ***Hardware based Mechanisms for Protecting Data*:** Hardware-based security solutions can prevent read and write access to data and hence offers very strong protection against tampering and unauthorized access. A hardware device allows a user to login, logout and to set different privilege levels by doing manual actions. The device uses biometric technology to prevent malicious users from logging in, logging out, and changing privilege levels. Hardware based access control is more secure than protection provided by the operating systems as operating systems are vulnerable to malicious attacks by viruses and hackers.
* ***Data Masking***: Data masking of structured data is the process of obscuring or masking specific data within a database table or cell to ensure that data security is maintained and sensitive information is not exposed to unauthorized personnel.
* ***Data Erasure***: Data erasure is a software-based overwriting that completely destroys all electronic data residing on a hard drive or other digital media.

**18.1.2 Computer Virus:**

# A virus is a computer program or piece of [code](http://www.webopedia.com/TERM/C/code.html) that is loaded onto a computer and run without the knowledge of the user. Viruses can also replicate themselves. A simple virus that can make a [copy](http://www.webopedia.com/TERM/C/copy.html) of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available [memory](http://www.webopedia.com/TERM/M/memory.html) and bring the [system](http://www.webopedia.com/TERM/S/system.html) to a halt. An even more dangerous type of virus is one capable of transmitting itself across [networks](http://www.webopedia.com/TERM/N/network.html)  bypassing [security](http://www.webopedia.com/TERM/S/security.html) systems. There are many types of computer virus, these are:

# *Cluster virus:* A virus that associates itself with the execution of programs by modifying directory table entries to ensure the virus itself will start when any program on the computer system is started is called cluster virus.  If a computer is infected with a cluster virus, it will appear as if every program on the [computer system](http://www.webopedia.com/TERM/C/computer_system.html) is infected; however, a cluster virus is only in one place on the system.

***Appending Virus****:* A virus that inserts a copy of its malicious code at the end of the file is called appending virus. The goal of an appending virus is not to harm the host program, but to modify it to hold the virus code and then be able to run itself.

# *Polymorphic Virus:* A [virus](http://www.webopedia.com/TERM/V/virus.html) that changes its [binary](http://www.webopedia.com/TERM/B/binary.html) pattern every time it replicates and it infects a new file in order to keep from being detected by an [antivirus program](http://www.webopedia.com/TERM/A/antivirus_program.html) is called polymorphic virus.

***Tunneling Virus****:* A virus that intercepts the actions before the anti-virus software can detect the malicious code is called Tunneling Virus. Tunneling is a virus technique designed to prevent anti-virus applications from working correctly. Anti-virus programs work by intercepting the operating system before it can execute a virus.

***Armored Virus:*** A virus that has been designed to thwart attempts by analysts from examining its code by using various methods to make tracing and disassembling is called armored virus. It may also protect itself from antivirus programs, making it more difficult to trace. To do this, the Armored Virus attempts to trick the antivirus program into believing its location is somewhere other than where it really is on the system.

# *Virus signature:* A unique string of [bits](http://www.webopedia.com/TERM/B/bit.html), or the [binary](http://www.webopedia.com/TERM/B/binary.html) pattern, of a [virus](http://www.webopedia.com/TERM/V/virus.html). The virus signature is like a fingerprint in that it can be used to detect and identify specific viruses. Anti-virus software uses the virus signature to scan for the presence of malicious [code](http://www.webopedia.com/TERM/C/code.html).

***Macro virus****:* A virus that is encoded as a macro embedded in a document is called a macro virus. Many applications, such as Microsoft Word and Excel, support powerful macro languages. These applications allow embedding a macro in a document, and having the macro execute each time the document is opened.

# *Overwriting virus:* A virus that will copy its own code over the host [computer](http://www.webopedia.com/TERM/C/computer.html) system's file [data](http://www.webopedia.com/TERM/D/data.html) is called overwriting virus. It can destroy the original [program](http://www.webopedia.com/TERM/P/program.html). After computer system has been cleaned using an [antivirus program](http://www.webopedia.com/TERM/A/antivirus_program.htm), users will need to install the original program again.

# *Companion virus:* A virus that compromises a feature of [DOS](http://www.webopedia.com/TERM/D/DOS.html) that enables [software](http://www.webopedia.com/TERM/S/software.html) with the same name, but different extensions, and operate with different priorities is called companion virus. For example a computer may have *program.exe* , and the [virus](http://www.webopedia.com/TERM/V/virus.html) may create a [file](http://www.webopedia.com/TERM/F/file.html) called *program.com*. When the computer [executes](http://www.webopedia.com/TERM/E/execute.html) *program.exe*, the virus runs *program.com* before *program.exe* is executed.

# *Stealth virus:* A virus that actively hides itself from [antivirus software](http://www.webopedia.com/TERM/A/antivirus_program.html) by either masking the size of the file is called stealth virus. It hides in or temporarily removing itself from the infected file and placing a copy of itself in another location on the drive, replacing the infected file with an uninfected one that it has stored on the [hard drive](http://www.webopedia.com/TERM/H/hard_disk_drive.html).

**18.1.3 Worm and Trojan horse:**

Worms and Trojan horses are all malicious programs that can cause damage to a computer, but there are differences between them.

**Worm:** A worm is sub-class of a virus. Unlike a virus, worms spread from computer to computer because of its capability to replicate itself on the system and then travel without any human action. A worm takes advantage of file or information transport features on the system. For example a worm can send a copy of itself to everyone listed in the e-mail address book of a user. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line.

**Trojan horse**: The Trojan Horse is a malicious virus that appears to be useful software but will actually damage once installed or run on a computer. A common method to receive a Trojan is through downloading free software.  On the receiving end, a Trojan horse is usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.  When a Trojan is activated on a computer, the results can vary. Some Trojans are designed to be more annoying than malicious like changing desktop, adding silly active desktop icons or they can cause serious damage by deleting files and destroying information on system. Trojans do not reproduce by infecting other files nor do they self-replicate.

**18.2.4 Network Security**

Network security is a specialized field of computer network that involves securing a computer network infrastructure. It is typically handled by a system administrator who implements the security policy and hardware needed to protect a network. It also ensures that employees have adequate access to the network and resources to work. A network security system typically relies on layers of protection and consists of multiple components including network monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network.

**18.1.5 Network Attacks**

Without security measures, data might be subjected to an attack. Some attacks are active, meaning the information is altered with intent to corrupt or destroy the data or network itself, whereas some attacks are passive, meaning information is monitored. Without the security plan, a PC may be subjected to following types of attacks

**Eavesdropping**: In eavesdropping, an attacker has gained access to data paths in the network to listen in or interpret the network traffic. When an attacker is eavesdropping, it is referred to as sniffing or snooping. Eavesdropping can be prevented with strong encryption based on cryptography.

**Data Modification:** After eavesdropping, an attacker can modify the data in the packet without the knowledge of the sender or receiver.

**Identity Spoofing**: This is also called IP address spoofing. A PC is identified in a network by IP address. In this case, an attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete data.

**Denial-of-Service Attack:** Unlike a password-based attack, the denial-of-service (DoS) attack is an attempt from the attacker to make a network or a machine resource unavailable to its legitimate users. The adversary can launch a DoS attack by studying the flaws of the network protocols or applications and then sending malformed packets which might cause the corresponding protocols or applications getting into a faulty state.

**Sniffer Attack**: A sniffer is an application or device that can read, monitor, and capture network data exchanges and then read network packets, if the packets are not encrypted. Sniffers can be used both for legitimate [network management](http://www.webopedia.com/TERM/N/network_management.html) functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the [hacker's](http://www.webopedia.com/TERM/H/hacker.html) arsenal. Figure 17.2.1 shows sniffer attack when a mail client is downloading email messages.

***Figure 17.2.1:*** Sniffer Attack

### Application-Layer Attack: An application-layer attack targets application servers by intentionally causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls.

**18.1.6 Key Points**

* Computer security refers to protection of valuable information and services of a computer network.
* Most computer security measures involve data encryption and passwords.
* The security of software is the idea of engineering software so that it continues to function correctly under malicious attack.
* The software’s security can be threatened: During its development or its deployment (distribution and installation) or its operation or its sustainment.
* Data Security is a process of protecting a database from destructive forces or unauthorized access.
* Network security is typically handled by a network administrator or system administrator who implements the security policy, network and hardware needed to protect a network
* A virus is a man-made computer program or piece of code that is loaded onto a computer and run without the knowledge of the user.
* A cluster virus associates itself with the execution of programs by modifying directory table entries to ensure the virus itself will start when any program on the computer system.
* Appending virus that inserts a copy of its malicious code at the end of the file
* Overwriting virus copies its own code over the host computer system's file data.
* A virus that actively hides itself from [antivirus software](http://www.webopedia.com/TERM/A/antivirus_program.html) by either masking the size of the file is called stealth virus.
* A worm is sub-class of a virus. It spreads from computer to computer because of its capability to replicate itself on the system.
* Trojan horse is a malicious virus that appears to be useful software but will actually damage once installed or run on a computer.
* Network security is a specialized field of computer network that involves securing a computer network infrastructure.
* In eavesdropping, an attacker has gained access to data paths in the network to listen in or interpret the network traffic.
* A sniffer is an application or device that can read, monitor, and capture network data exchanges and then read network packets, if the packets are not encrypted.
* An application-layer attack targets application servers by intentionally causing a fault in a server's operating system or applications.

**18.1.7 Practice Sets**

**Multiple Choice Questions**

1. Computer security refers to techniques by which \_\_\_\_\_\_\_\_\_\_\_.
2. valuable information and services of a computer network are protected from publication.
3. valuable information and services are collapsed by unauthorized activities.
4. valuable information and services of a computer network are protected from tempering.
5. valuable information and services are collapsed by trustworthy individuals.
6. Data Security is a process of protecting a database from\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
7. lack of sufficient system security
8. enables more flexible working practices
9. destructive forces or unauthorized access.
10. All
11. A virus is a \_\_\_\_\_\_\_.
12. program run with the permission of the user
13. cryptographic algorithm run without the knowledge of the user
14. program run without the knowledge of the user
15. none
16. A virus that compromises a feature of [DOS](http://www.webopedia.com/TERM/D/DOS.html) that enables [software](http://www.webopedia.com/TERM/S/software.html) with the same name, but different extensions, and operate with different priorities is called \_\_\_\_.
17. Overwriting virus
18. Stealth virus
19. Companion virus
20. Macro virus
21. Computer virus that inserts a copy of its malicious code at the end of the file is called \_\_\_\_\_\_\_\_\_\_\_.
22. Overwriting virus
23. Stealth virus
24. Companion virus
25. Macro virus
26. \_\_\_\_\_\_\_\_\_\_\_\_\_\_attack is an attempt from the attacker to make a network or a machine resource unavailable to its legitimate users.
27. Spoofing
28. DoS
29. Sniffer
30. Application layer

**Review Question**

1. What do you understand by Computer Security?
2. List basic security issues of different information systems
3. What do you understand by Network Security?
4. Define a computer virus. Write the name of different computer viruses.
5. Distinguish between worn and Trojan horse.
6. List the name of different typs network attacks.

**Analytical Questions**

1. Explain basic security issues of different information systems
2. Distinguish between software security and data security.
3. Explain the data security techniques.
4. Write a short note on computer virus.
5. Explain different type network attacks.

**

***Lesson 18.2***

***Protective Measures***

**18.2.0 Objectives**

*On completion of this lesson you will know:*

* *Hackers and Scanners*
* *Virus and spyware protection softwares*
* *Different types of network protection*
* *Backup*

**18.2.1 Hackers and Scanners:**

Hackers are individuals or programs that attempt to gain access to a system without permission or knowledge. Some hackers are automated, searching for details inside the computer in order to improve targeted advertising. Other hackers are individuals searching for private information such as financial account access data.

Scanners are tools used by hackers to detect computer's vulnerability; they are usually attached with worms. The scanner will check ports looking for an open one to gain access to a system. Firewalls use scanners to detect open ports in order to secure them before they are breached.

**18.2.2 Virus and Spyware Protection Software:**

Virus protection software prevents a computer from viruses, worms and Trojan horses and also removes any malicious software code that has already infected the computer. Most virus protection utilities now pack anti-spyware and anti-malware capabilities to go along with anti-virus protection. Internet security suites go a step further by including additional capabilities like anti-spam, anti-phishing, firewall, file protection and PC optimization.

Virus scanner is a type of antivirus program that searches a system for virus signatures that have attached to executable programs and applications such as e-mail clients. A virus scanner can either search all executables when a system is booted or scan a file only when a change is made to the file as viruses will change the data in a file.

Spyware can result in data corruption, pop-up ads, hacker attacks and identity thefts so it is important to have software on a computer that can detect and delete spyware. This software can be part of antivirus software or purchased separately.

**18.2.3 Defense-against Network Attack**

There are three methods that can defense in network attach, these are configuration management, firewall and encryption. These are discussed below:

**Configuration management:**

The configuration management is the main defense in network attack. The following measures should be strictly implemented as part of configuration management.

* Running up-to-date copies of the operating system and immediately update whenever a new service pack or patch is released.
* All your configuration files in Operating Systems (OS) should have enough security.
* All the default passwords in OS and applications should be changed after the installation.

**Firewall**

Firewall is another weapon for defense against network attack. It is a device and/or a software that stands between a local network and the Internet, and filters traffic that might be harmful. Figure 18.2.1 shows a Firewall that is placed between Internet and LAN to protect LAN. Firewalls can be classified in to four based on whether they filter at the IP packet level, at the TCP session level, at the application level or hybrid.

* ***Packet Filtering***: Packet filtering firewalls are functioning at the IP packet level. Packet filtering firewalls filters packets based on addresses and port number. It can prevent DoS attacks and IP Spoofing attacks.
* ***Circuit Gateways***: Circuit gateways firewalls operate at the transport layer, which means that they can reassemble, examine or block all the packets in a TCP or UDP connection. Circuit gateway firewalls can also VPN over the Internet by doing encryption from firewall to firewall.
* ***Application Proxies***: Application proxy-based firewalls function at the application level. At this case, traffic generated by applications can be controlled or blocked. It can provide very comprehensive protection against a wide range of threats.
* ***Hybrid***: A hybrid firewall may consist of a pocket filtering combined with an application proxy firewall, or a circuit gateway combined with an application proxy firewall.



Figure 18.2.1: Firewall

**Encryption and Decryption**

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. Encryption is used to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption. Figure 18.2.2 shows the encryption and decryption process

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.



**Figure: 18.2.2** Encryption and decryption process

**18.2.4 Backup:**

Back up is a process of [copy](http://www.webopedia.com/TERM/C/copy.html)ing [files](http://www.webopedia.com/TERM/F/file.html) or folder to a second [medium](http://www.webopedia.com/TERM/M/media.html) (a [disk](http://www.webopedia.com/TERM/D/disk.html) or [tape](http://www.webopedia.com/TERM/T/tape.html)) as a precaution in case the first medium fails. Even the most reliable computer is apt to break down eventually. A user shall make two, or even three, backups of all files. Files can be backed up by [operating system](http://www.webopedia.com/TERM/O/operating_system.html) [commands](http://www.webopedia.com/TERM/C/command.html) or a special-purpose backup [utility](http://www.webopedia.com/TERM/U/utility.html). Backup programs often [compress](http://www.webopedia.com/TERM/D/data_compression.html) the [data](http://www.webopedia.com/TERM/D/data.html) so that backups require fewer disks.

A backup server backs up and restores files, folders, databases and hard drives on a network in order to prevent the loss of data in the event of a hard drive failure, user error, and accident. Microsoft Windows Server operating systems also include a built-in Windows Server Backup feature that can be used to perform basic backup and recovery operations on backup servers. An alternative to standard backup server software tools are online backup and recovery services that save network's data to a remote location in the cloud. Popular backup software tools include Norton Ghost, Symantec Backup Exec, Acronis True Image and Total Recovery Pro.

Cloud computer [backup](http://www.webopedia.com/TERM/B/backup.html), may also be called "[online storage](http://www.webopedia.com/TERM/O/online_data_storage.html)", means backing up computer files to a remote, cloud-based computer as shown in Figure 18.2.3. Cloud backup solutions enables individuals or organizations to store their [data](http://www.webopedia.com/TERM/D/data.html) on the [Internet](http://www.webopedia.com/TERM/I/Internet.html) using a [storage service provider](http://www.webopedia.com/TERM/S/Storage_Service_Provider.html), rather than storing the data locally on a physical disk, such as a [hard drive](http://www.webopedia.com/TERM/H/hard_disk_drive.html) or [tape](http://www.webopedia.com/TERM/T/tape.html) backup. An alternative to standard backup software tools are online backup and recovery services that save important data to a remote location in the [cloud](http://www.webopedia.com/TERM/C/cloud.html). Examples of cloud backup services include Carbonite, Mozy and IDrive

**Figure 18.2.3:** Online storage.

**18.2.5 Key points:**

* Hackers and predators are programmers who victimize others for their own gain by breaking into computer systems to steal, change or destroy information as a form of cyber-terrorism.
* Virus protection software prevents a computer from viruses, worms and Trojan horses and also removes any malicious software code that has already infected the computer.
* Data that can be read and understood without any special measures is called plaintext or cleartext.
* The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext.
* The configuration management is the main defense in network attack.
* Firewall is a device and/or a software that stands between a local network and the Internet, and filters traffic that might be harmful.
* Firewalls can be classified in to four based on whether they filter at the IP packet level, at the TCP session level, at the application level or hybrid.
* Cryptography is the science of using mathematics to encrypt and decrypt data.
* Back up is a process of [copy](http://www.webopedia.com/TERM/C/copy.html)ing [files](http://www.webopedia.com/TERM/F/file.html) or folder to a second [medium](http://www.webopedia.com/TERM/M/media.html) (a [disk](http://www.webopedia.com/TERM/D/disk.html) or [tape](http://www.webopedia.com/TERM/T/tape.html)) as a precaution in case the first medium fails.
* Cloud computer [backup](http://www.webopedia.com/TERM/B/backup.html), may also be called "[online storage](http://www.webopedia.com/TERM/O/online_data_storage.html)", means backing up computer files to a remote, cloud-based computer.

**18.2.6 Practice Set**

1. \_\_\_\_\_\_\_ individuals or programs that attempt to gain access to a system without permission or knowledge..
2. virus
3. crypto-analysis
4. hacker
5. cracker
6. Virus protection software prevents a computer from \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
7. worm
8. spyware
9. both
10. hacker
11. Circuit gateways firewalls operate at \_\_\_\_\_\_\_ layer.
12. physical
13. network
14. transport
15. application

**Review Question**

1. List three methods that can defense in network attach.
2. Distinguish between virus and spyware
3. Why encryption is needed?
4. Distinguish among virus, worm, Trojan horse.

**Analytical Question**

1. What are the different types of network protection techniques? Explain different types of firewall.
2. What do you understand by encryption? Explain encryption and decryption techniques with an illustration.
3. Write a short note on back up.