3 Information Security and Social Networking

Learning Objectives

After learning this chapter the students will be able to:

- co-create knowledge in collaboration
- understand the threats to a computer system
- learn about Virus, Worm, Trojan Horse and their effects on a computer system
- use Anti-virus and other measures to protect computer
- apply desktop security involving cookies and firewalls
- understand about Cyber Crime and Cyber Police
- learn about Social networking

One day, Nalin received a strange email from his very good friend asking him to lend some money. In that mail his friend wrote that he is very far away from his place and has been trapped in some financial crisis. So he requested Nalin to transfer some amount of money to some specified bank. Nalin could not believe it and decided to first call up his friend and verify. And this was a wise thought as when he called up his friend he told him that everything is fine at his end. He also told Nalin that his email account password has been hacked by someone and now that person is sending the same mail to all the people in his contact list. This is just an example of cyber crime.

Crime has always been an unpleasant and unavoidable ingredient of our society. In the past couple of decades, computers and internet have dominated our society. We depend on computer and internet for communication, banking, finance, examination and many other serious matters. Computers have become virtual lockers used to store our secrets. Since computer is an essential and important part of our lives, crime cannot spare it too. Every day criminals evolve new methods to invade our virtual lockers or even our privacy created in or via computers. The crimes which involve computers are termed as cyber crimes. In this chapter, we focus on some of the common threats to a computer system and explain certain means of how one can deal with these threats.

Threats to a Computer System

Information security commonly refers to as CIA (short form of Confidentiality, Integrity and Authentication), protects our computer from any unauthorized access and maintains the system resources. Precisely,

- Confidentiality ensures protection of the computer system from any unauthorized access
- Integrity ensures that information stored in the computer is protected
- Authentication ensures the authenticity of the authorized user

CIA can be weakened or broken in many ways. Some of the possible attacks are the following:

- Viruses
- Worms
- Trojans

We will explain below these threats in details and possible measures to be taken to prevent these situations.

Viruses

Viruses are computer programs developed to copy themselves and infect other files stored on the computer. These are malicious programs that move from computer to computer by attaching themselves to files or boot records of disks and diskettes. Virus can automatically be transferred from one computer to another when its host is taken to the target computer, for example an user can sent it through a network or the internet, or carried it on a removable storage medium such as CD, DVD, USB pen drive or Memory Cards.

Viruses can cause destruction to the entire file system which in result would need to reinstall and reload the whole system again. They can also create effected sectors on the disk destroying one or more files and part of some programs. Viruses also lesser the space on the hard disk by duplicating and attaching itself to various files. Through these viruses, system gets hang-up and the entire system stops working.

These days' viruses are spread through email attachments and other programs that can be downloaded from the internet. A virus acts like an agent that travels from one file to another on the same computer through an infected file.

The first ever virus named "Creeper" was first detected on ARPANET, in the early 1970s. It was an experimental self-replicating program written by Bob Thomas at BBN Technologies. Creeper infected some DEC PDP-10 computers running on the TENEX operating system. Via the ARPANET, Creeper copied itself to the remote systems where the following message was displaced:

"I'm the creeper, catch me if you can!"

To counter its effect, a program called "Reaper" was created.

Worms

It is a program made to replicate automatically. A worm replicates continuously until the entire hard disk space and memory are eaten up and it may do so without any user intervention. This kind of self replicating programs spread over the entire hard disk and memory consequently and slow down the system.

Unlike a virus, a worm does not need to attach itself to an existing executable program or code. Worms harm to a computer or a computer network by consuming bandwidth and slow down the network speed whereas viruses almost always corrupt or modify files on a targeted computer. After the worm has infected a system, it can propagate to other systems via internet or while copying files from one system to another without user interaction. The nasty result is a worm traversing through the Internet in a matter of hours, infecting numerous machines.

The destruction from a worm is less alarming than a virus in the sense that worm does not corrupt other files. It only eats up the memory.

Trojan

The term Trojan is derived from the Trojan Horse story in Greek mythology. Trojan horse is virtually a harmless program in itself. Like a virus or a worm, it neither corrupts other files on the system nor takes up the memory part. Nevertheless, the effect of a Trojan could be even more dangerous. In fact, at the backend, these programs perform some malicious activities like upload (send) some security files and information from the computer and at the same time download some unwanted files onto the computer. This

way not only it slows own the network speed but also uploads (sends) some non shareable information to other computers like our user name, password, emails, credit card details and other secured information over the network. They are generally transferred by emails, attachments and freeware & shareware software.

Trojan horses are designed to allow a hacker to target a remote computer system. Once a Trojan horse has been installed on a target computer system, it is possible for a hacker to access it remotely and perform various operations and it may do so without any user intervention at the remote end.

There are many ways in which a Trojan Horse can propagate. The most common of them is through email attachments. Unintentionally, a user can download some Trojan from the internet as a freeware with the assumption of utility software. Other sources for Trojan horse are the chat software and email manager.

With the help of Trojan, harms that could be done by a hacker on a target computer system are:

- Data theft (e.g. passwords, credit card information, etc.)
- Installation of unwanted software
- Downloading or uploading of files
- Modification or deletion of files
- Keystroke logging
- Viewing the user's screen
- Wasting computer storage space
- Crashing the computer

Anti-Virus Tools

As explained earlier, virus, worm and Trojan are all different in some sense but a common user calls all of them by the term "virus" only. Thus when we talk about anti-virus tools, these tools take care of worm and Trojan as well along with viruses.

Anti-Virus tools not only remove virus and other infected threats from our computer system but at the same time also protect our systems from data loss, destruction and attack of any external threats like virus, worm and Trojan. There are many anti-virus

software which are available commercially such as Norton, Mcaffee, AVG , Avast, Kasper Sky, Quick Heal etc.

Before Internet era, viruses were typically spread by infected floppy disks or removable storage devices. Antivirus software came into use even at that time, but was updated relatively less frequently, like once a month. During this time, virus checkers essentially had to check executable files and the boot sectors of floppy and hard disks.

As internet usage became common, initially through the use of hubs and modems, viruses spread throughout the network and internet. The problem multiplied when virus writers started using the macros to write viruses embedded within documents. This meant that computers could also be at risk from infection by documents with hidden attached macros as programs.

Later email programs were vulnerable to viruses embedded in the attachments or even the email body itself. Now, a user's computer could be infected by just opening or previewing a message. This meant that virus checkers has to check many more types of files. An Anti-virus software is used to prevent, detect, and remove various computer threat, including computer viruses, worms, and Trojan horses. A variety of strategies like Signature-based detection are being used which involves searching for known code or patterns of some known viruses in executable code or macros.

There are several methods which anti-virus software can use to identify viruses. Signature based detection is the most common method. To identify viruses and other threats, antivirus software compares the contents of a file to a dictionary or database of virus signatures. Because viruses can embed themselves anywhere in the existing files, the entire file is searched.

Although the signature-based approach can effectively contain virus outbreaks, virus authors have tried to stay a step ahead of such software by writing "oligomorphic", "polymorphic" and "metamorphic" viruses, which encrypt parts of themselves or modify themselves as a result, are difficult to identify.

However, it is possible for a computer to be infected with new viruses for which no signature exists or identified yet. To counter such so-called "zero-day threats", comparatively, new techniques like Heuristics & Rootkit detection methods are used.

No matter how useful antivirus software is, it always has some limitations. Thus it is always advised to adopt and practice some security measure to minimize the threats.

Some common security measures are given below:

- A computer should be used only by authorized users [user login];
- Password should be changed regularly;
- Password should not be shared;
- Always be careful about some suspicious person who might see your password while typing;
- Scan your computer regularly with anti-virus software;
- Regularly update your antivirus software;
- Restricted use of removable storage devices, especially USB Pen Drive;
- Properly configure the email-filter option;
- Never download any email attachment from an unknown sender;
- Avoid even browse email sent by some unknown sender;
- Must take backup of the computer system regularly;
- Preferably use sky drive (online storage) to have additional copies of important documents so that in case of natural calamities, at least your important documents are safe;

Desktop Security

Using anti-virus software is one way to counter computer threats. Moreover, these software are used after a virus has attacked the computer. There are ways and measures by which we can restrict viruses to enter into the computer. These measures collectively come under "Desktop security" which includes software authorization, authentication, firewalls, encrypted channels, anti-virus tools and user education. It is a mechanism through which we can stop entry of viruses and other threats into our computer system and also restrict the access of unauthorized users to protect our system file and folders. We explain below some of these measures.

Username

It is a code which can be set to log on to a computer access to its resources. Although setting a username is not mandatory, but it must be set for each user so that only the authorized ones have the access.

Password

A password is a secret code or string of characters that is used to authenticate or confirm, to prove identity or permission to access to a resource. It is used in combination with the username. It should be kept secret. There are software which can encrypt your passwords. Thus a password should be strong enough. Following points must be taken care of while deciding a password:

- Must contain alphabets (preferably a mix of lowercase and uppercase), digits and some special characters;
- Always prefer a non dictionary word attached with some digits and special characters;
- Passwords must be changed at least after every 30 days;
- Should not contain the user's username;
- Should not contain any word, name or number related to the user's identity like birth details or names of family members;
- No password should be re-used for a period of 1 year.

CAPTCHA (Telling Humans and Computers Apart Automatically)

A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. For example, humans can read distorted text as the one shown below, but current computer programs can't:

Figure 3.1 A CAPTCHA Screen

The term CAPTCHA (for Completely Automated Public Turing Test To Tell Computers and Humans Apart) was coined in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University.

Network Security

The network security (or information security) is to provide protection to the computer system from the hackers (intruders). Network security focuses on protecting data resources from external attack and also from simple mistakes made by the users within an organization. Network security also designs computer network infrastructure, policies and rules adopted by the network administrator to protect the network and the network-shareable resources from. The security system also monitor consistently and continuously the effectiveness of all the security measure.

File Access Permission

In a computer network or even in the internet, some files or documents are made shareable and some are made public. The protected sharable files and documents are shared among few users or even by a group having the access rights. Access rights are generally decided and given by the owner of the file or the network administrator. Thus the three types of users can access a file or a folder i.e. Owner, user having access rights, or all other users.

Firewall

A firewall is a technique used in a secured computer system or network to block unauthorized access and allow only the authorized user. Firewalls can be implemented in either hardware or software, or a combination of both. It is a device or set of devices or software running on a computer, which is configured to permit or deny computer

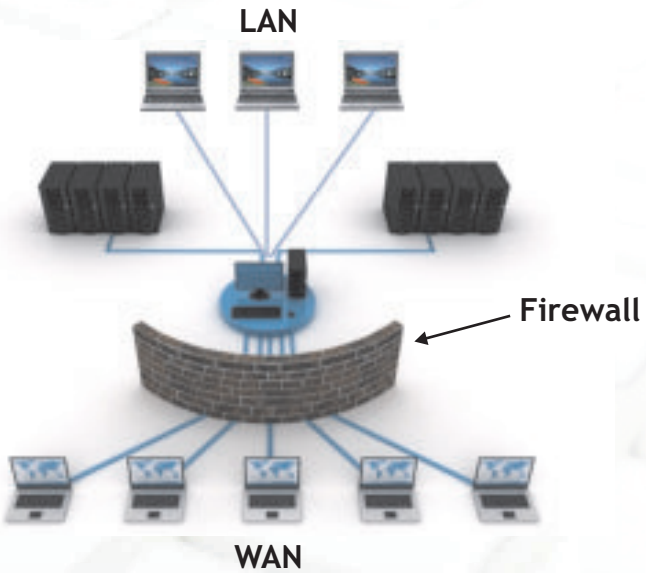


Figure 3.2 Firewall

applications and set of other software based upon a set of rules and other criteria designed by the network administrator. It also inspects network traffic passing through it, and denies or permits passage.

It is normally placed between a protected network (usually a LAN) and an unprotected network (usually WAN or Internet) and acts like a gate to protect all resources to ensure that nothing goes out without permission and nothing unwanted comes in into the system.

Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Digital Signature

In case of Cyber Crime, a digital signature plays a significant role to ensure authenticity and thus protect security of a computer system. A digital signature is a method for proving the authenticity of a message or document or attachment or software sent through email. Digital signatures are commonly used for software distribution, financial

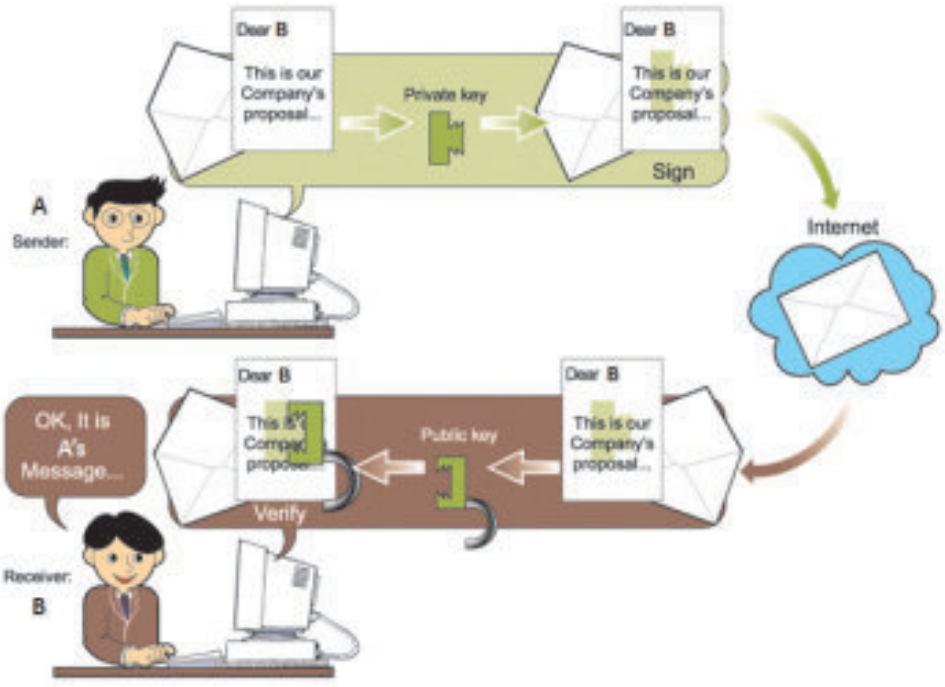


Figure 3.3

transactions, and in other cases where forgery and tampering is possible. A valid digital signature gives a recipient enough reason to believe that the message was created by the known sender, is completely safe and authentic and that it was not modified (got infected).

Digital Certificate

A digital certificate (also known as a public key certificate or identity certificate) is an electronic document which uses a digital signature to bind together a public key or password required for decode and encoded document with an authentic identity such as the name of a person or an organization, their phone numbers or address, and so forth. The certificate can be used to verify that a public key belongs to an authorized individual or organization.

Cookies

A cookie (also known as a web cookie, browser cookie, and HTTP cookie) is a small bit of text or a file that accompanies requests and pages as they go between the web server and browser. The cookie is sent as an header by a web server to a web browser and then sent back by the browser each time it accesses that server. Cookies help web sites to store information about visitors. Some cookies thus may violate privacy concerns. For example, when a user visits your site, you can use cookies to store user preferences or other information like password, address, date of birth etc.(Many sites ask first-time visitors to fill in a form about themselves before they get access to the site). When the user visits your web site another time, the application can retrieve the information it stored earlier. A cookie can also be used for authentication, session tracking (state maintenance), storing site preferences, shopping cart contents, the identifier for a server-based session, or anything else that can be accomplished through storing textual data. As text, cookies are not executable. Since they are not executed, they cannot replicate themselves and not harm the computer directly. However, due to the fact that the browser reads and sends cookies to the web server, they can be used as spyware. Today, most of the browsers ask users whether to accept cookies or not, but rejecting cookies makes some websites unusable.

Cyber crime and Cyber police

As remarked in the beginning of this chapter, Cyber crime (or Computer crime) refers to any crime wherein the computer is either a tool or a target or both.

Some forms of the Cyber Crime are:

- Creating and distributing Spam Mails
- Hacking
- Fraud through Internet or intranet
- Sending Obscene or Offensive messages
- Creating Websites with Obscene or Offensive content
- Harassment through emails and web messages
- Drug trafficking through internet and intranet
- Cyber terrorism

Cyber Law of India

The propagation of a virus, worm or Trojan is one of the common means of making cyber crime. What is the legal aspect in such situations of cyber crimes and how to counter them? First of all, like traditional crimes such as theft, fraud, forgery, defamation and mischief, cyber crimes are also treated criminal in nature and are subject of the Indian Penal Code. Information Technology Act (or The IT Act) is a set of recent legal enactments, currently existing in India, which provide legal support to the computer users against the cyber crime. These laws have been described as "paper laws" for "paperless environment".

The cyber police work as a detector to detect the cyber crime. They have the right in respect of all the offences committed under TITA (The Information Technology Act 2000) Central Act.No.21 of 2000 or crime related to Intellectual property rights.

Know More

The Information technology Act 2000 has been substantially amended through the Information Technology Amendment Act 2008 which was passed by the two houses of the Indian Parliament on December 23,and 24, 2008. It got the Presidential assent on February 5, 2009 and was notified for effectiveness on October 27, 2009.

Social Networking

Rahul moved to a new locality two months back. After spending whole day in the office when he used to come back home he felt lonely and started missing his old pals and family. Like all other human beings he also needed a social life so that after office he could relax and interact with buddies. Then one day one of his colleagues suggested him to go to a club in his area where he can find people with varied interests. On his colleague's advice Rahul went to the club. There he found a group of people playing snooker, another group just gossiping and chatting and yet another group involved in various other activities. Rahul has always been a good player of chess so he headed towards that group and became a part of it. And now he is very happy and doesn't feel lonely. Also he has found the contact number of one of his school time friend whom one of the club members knows, so now he in touch with him also. A common activity just brings two people together but afterwards they share all their thoughts, happiness and sorrows. In today's life people are so occupied that they hardly get time to go to a club but they also need a social circle and since most of the time they are online so nothing like having a friends group available on computer only. And social networking sites on internet provide a platform for this.

Figure 3.4

Initially social networking was an initiative to communicate amongst known and unknown users working over network worldwide. It has now turned into a much matured area to explore and exploit experiences and expertise of individuals sitting miles and miles away from each other. It gives a common platform to find people of varied interests and social backgrounds. Number of people utilize the services of social networking sites as a common place to develop group projects on various subjects. It also helps to find out alumni and old friends. And also allows you to contact and start fresh conversations. It creates an extended network by connecting friends of friends and further enabling the empowerment of knowledge and resources. Some of the common social networking sites are Facebook, Twitter, Netlog, Hi5, Orkut etc.

Although the idea of online social networking sounds very useful but there is certain element of risk and danger involved in it. Through networking you not only communicate with your known ones but also to strangers and revealing your personal

details to strangers can sometimes be very dangerous. Sometimes a stranger may pretend to be someone which he is not in reality. But then this type is risk is involved in real world too. Every day, for the business purpose or otherwise, one has to meet and interact with many unknown people. In such situations we use our wisdom to calculate how much of ourselves to reveal before him. Similarly, while interacting online, one should use his inner voice to react accordingly. The other type of risk involved in social networking is hacking. Even if you are interacting with known people, your information and personal details can be hacked by hackers. So one has to be cautious and supply only minimum required details.

There are some common threats pertaining to these sites which are shared along with the precautions below:

Threat: *Unknown users on internet can misuse your personal information disclosed by you on your account.*

Precaution: *Do not reveal personal information to strangers. Have restricted and brief conversations only.*

Threat: *Lot of abusive and unwanted content may be present on such social networking sites.*

Precaution: *All the service providers of such sites are very proactive and careful about such things. So as an ethical user you should report it to the service provider immediately.**

Threat: *Fake identity of someone known to you or someone famous.*

Precaution: *As soon as you come across a user with a fake identity on such sites, you should immediately report about the same to service provider.**

* Note : These matters are taken very seriously and acted upon by service providers.

Summary

- Information security popularly refers to CIA, which means Confidentiality, Integrity and Authentication.
- A computer virus is a computer program that can copy itself and infect a computer.
- A computer worm is a self-replicating computer program. It uses a computer network to send copies of itself to other computers on the network.

- A Trojan, also referred to as a Trojan horse, is non-self-replicating program that appears to perform a desirable function for the user but instead facilitates unauthorized access to the user's computer system.
- Anti-Viruses Software are the virus detection and threat protection tools.
- Username and password are used to authenticate an authorized user.
- A firewall is used for network security to block unauthorized access and to inspect network traffic.
- A digital signature is an additional barrier for important communications like financial transactions etc.
- A digital certificate is an electronic document which uses a digital signature to bind together a public key or password required to decode and encoded document with an authentic identity.
- A cookie is a small bit of text or a file that accompanies requests and pages as they go between the web server and browser.
- Cyber crime refers to any crime that involves a computer and a network.
- The IT Act or Information Technology Act is a set of recent legal enactments, currently existence in India, which provide legal support to the computer users against the cyber crime.

Multiple Choice Questions

1. Which of the following is not a threat?

a) Trojan

b) Virus

c) Bug

d) Warm

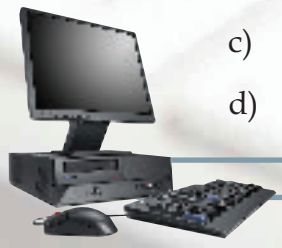
2. Viruses transferred least through:

a) Internet

b) USB Drive

c) Cookies

d) DVD



3. Under which Act cyber police works.

a) Central Act 1998

b) Act No.21

c) Act No.21 of 2000

d) none of the above.

4. Network security is used to protect system from:

a) Hackers

b) Hardware failure

c) Software Piracy

d) All of the above

5. _____is a hidden code in a program for example in a game or spreadsheet that looks safe to execute but has some hidden side effects also.

a) Worms

b) Trojan

c) Encapsulation

d) None of the above.

6. Which of the following is not an anti-virus:

a) Avast

b) Norton

c) AVG

d) Spamming

Exercise

1. What do you mean by security of a computer system?
2. What is a computer virus?
3. How does a virus affect a computer system?

4. How viruses are detected?
5. How does a virus propagate from one computer to another?
6. Name the first computer virus.
7. What is a worm?
8. Differentiate between a virus and a worm.
9. How does a worm propagate?
10. What is the danger of a Trojan Horse?
11. What is meant by a spyware?
12. How does Trojan support spyware?
13. Define anti virus software?
14. What do you mean by a signature in respect of computer virus?
15. Write any four safety measure you follow to protect your computer.
16. How do authorization and authentication implement in computers?
17. Mention any four rules you follow when you decide your next password for your email-id account.
18. Define the term Firewall in computers.
19. How does firewall work?
20. Compare Digital Signature and digital certificate.
21. Explain the usage of Digital Signature.
22. What is a cookie?
23. What is cyber crime? Give four examples.
24. How Cyber Police Works?
25. Name the cyber act in India.