Unit
11

DIGITAL SECURITY

UNIT STRUCTURE

11.0 Learning Objectives :

After working through this unit, you should be able to :

- Understand the importance of Digital security.
- State the different Digital Security Risks and Cybercrime
- Name various types Internet attacks
- Learn the use and importance of Firewall
- Learn to protect the system and network from unauthorised access.

11.1 Introduction :

Internet plays a vital role to our today's life. Lots of activities we can perform online. We shop any product and make the payment online using net–banking, mobile–banking, credit or debit cards and save time and fuel to find the product. We can pay electricity, gas or water bill online using Internet. We can

book movie tickets, reserve hotel rooms, buy a bus ticket, book a railway or flight reservation online. We can even transfer the fund (money) from one account to another account using Internet. Many people share photos and videos with friends and family members with Internet. Day to day, we are increasing our transaction activities on the Internet.

With the increasing use of Internet, day to day number cases of cybercrimes are also increasing. In this unit we will observe different types of digital security risks and their solutions, so that the we can take maximum benefits of the Internet without any kind of fear or with very limited risk.

11.2 Digital Security Risks :

With the increasing use of Internet, it is crucial that users take measures to safeguard or protect their computers, mobile devices and data from damage, loss or misused by someone else. Individual must ensure that their net–banking credentials or credit card numbers are secure while doing online payment.

Digital security risks are an event or action that could cause a trouble to its users like loss of data, damage of hardware and software of the computers or mobile devices, theft of your financial credentials etc. The more common digital security risks include Internet or network attack, use of your system or financial credentials by unauthorised person, hardware of software theft, or system failure.

Security breaches to the digital security may be accidental or intentional.

Some intruders do not disturb any functionality of your computer system, they simply access data and information stored in the system or mobile device before signing out. While other intruders indicate some evidence of their presence either by leaving a message or by intentionally damaging or altering the data.

11.2.1 Cybercrime :

Any illegal act in which computer or its related devices are used is generally referred to as computer crime. Basically, the term 'cybercrime' refers to online illegal act using Internet such as sharing or distributing malicious software or doing identity theft. Cybercrime can be categories as hacker, cracker, script kiddie, unethical employee or cyberterrorists.

- The term **hacker**, is used for a computer enthusiast who also wants to test the various security areas of the application. Hackers test their hacking skills to find out security breaches in the software. The intention is not to perform any malicious activity, but to find out security breaches in the software so that it can be improved.
- The term **cracker**, is used for an unknown user, who illegally access your computer or device through network or Internet to perform destructive actions such as destroying data, stealing information or other malicious activity. Both hacker and cracker have advanced knowledge and skill of using computer, network and Internet technologies.
- The term **script kiddie**, is used for a user who has same intent as cracker but does not have technical skills and proper knowledge. Script kiddies often use prewritten hacking or cracking programs to break into computer and networks.
- The term **Unethical employee**, is used for a user who may break into their employers' computer for different reasons. Some employees are doing this

to exploit a security weakness, and some other employees are doing this for financial gains by selling confidential information of the organization.

- The term **cyberterrorist** is used for the user who uses the Internet to destroy or damage computers for political reasons. The cyberterrorists may target air traffic control of the nation, electricity control system, telecommunication infrastructures and more.

❑ **Check Your Progress – 1 :**

1. _____ test their hacking skills to find out security breaches in the software, but not for destructive purpose.

   [A] Hacker [B] Cracker

   [C] Cyberterrorist [D] Unethical Employee

2. _____ refers to online illegal act using Internet such as sharing or distributing malicious software or doing identity theft.

   [A] Computer crime [B] Cybercrime

   [C] Civil crime [D] None of the above

3. If someone create a profile with your name, photos and other personal information without your permission is called _____.

   [A] Financial theft [B] Data corruption

   [C] Unethical employee [D] Identity theft

11.3 Internet Attacks :

When the information is transmitted using Internet, has higher risk then the information transmitted withing the network of an organization. Within the organization network administrators usually takes all measures to take care or protect your data from the possible security risks. Internet on the other hand, is a public network. Anyone can pay for the services and access Internet. There is no central administrator is present on the Internet to take care of your data. While accessing, you need to protect your system and data from malware, botnets, denial of service attack, backdoor and spoofing types of attacks.

11.3.1 Malware :

Malwares are malicious software or programs that runs in your computer without your knowledge. Malwares sometimes deliver destructive action or simply pranks to your computer system or mobile device. A common way that gets infect your system or mobile device from viruses or other malware is opening any infected attachment receive in the Email. The following table gives you an idea about different types of Malware and its actions.

Type	Description
Virus	Viruses can damage the programs that affects, or infects. It can alter the settings of system or device, corrupt any software without user's permission or knowledge.
Worm	Worm is program that replicate itself without user's knowledge or permission. It can possibly shut down the system, device or network which you are using from the network.
Trojan horse	Trojan horse does not replicate itself like viruses and worm. It is a program that look like a genuine program or software.

Rootkit	Rootkits are the program which hides itself into the user's machine without user's knowledge and permission. It provides remote access of the system or device without use's knowledge.
Spyware	Spyware hide itself into the user's machine, without user's permission and collect secret information of the system and device and provide it to some outsider or creator of that spyware.
Adware	Adware is a program which displays various online advertisements in the form of banner or pop–up windows.

❑ **Check Your Progress – 2 :**

1. Identify the malwares from the given below :

   [A] Virus [B] Worm [C] Spyware [D] All of the above

2. _____ malware does not replicate itself, but it looks like a genuine software.

   [A] Virus [B] Trojan horse [C] Rootkit [D] Spyware

3. _____ malware collect the secret information of your device and give it to the creator of that malware.

   [A] Adware [B] Trojan horse [C] Spyware [D] Rootkit

11.3.2 Botnets :

A botnet is also known as zombie army or simply zombies. It infects any device which is connected with the network or Internet. The infected device is known as zombie, whose owner is not aware that the device is infected and it is being remotely controlled by some outsider. A bot is a program that performs repetitive tasks on a network. Cybercriminals install malicious bots on the device which is not protected and create botnet. The criminal the uses the botnet to send spam mails, spread viruses and other malware.

11.3.3 Denial of Service Attack :

Denial of service attack is an attack whose main purpose is to disturb device access to an Internet services. The infected device can not access the web or Email services.

11.3.4 Back Doors :

Back door is a program that allows use to bypass security checks while accessing network or Internet. Once attacker gain access to such unsecure device, they install a back–door program into the machine can access that device remotely without user's knowledge or permission. A root kit can be a back–door. Some worm installs back–door, which can be used to spread other worms to disturb device activity and performance.

11.3.5 Spoofing :

Spoofing is a technique; which attacker use to make their Internet transmission appear genuine to a victim device. Two common spoofing techniques are : [1] IP–spoofing and [2] Email spoofing.

[1] IP–spoofing : In an IP–spoofing, attacker making fool to the user, and shows that the IP address used by the attacker is of some genuine source.

[2] Email spoofing : Email spoofing occurs when the address of an Email sender or other information of Email is altered in such a way that recipient

will understand, that the Email is originated by different sender. Email spoofing is mainly used in phishing scams and spams.

❑ **Check Your Progress – 3 :**

1. In _____ attack security checks of the system are bypassed so that attacker can access that system in future.

   [A] Spoofing [B] Denial of Service

   [C] Back door [D] Botnet

2. In _____ attack, device becomes zombie and provide remote access to outsider.

   [A] Spoofing [B] Denial of Service

   [C] Back door [D] Botnet

3. Phishing can be done by _____.

   [A] Email spoofing [B] Trojan horse

   [C] Spyware [D] Rootkit

11.4 Securing System From Attacks :

To protect the system or device from the attacks which are explained earlier we need to follow the steps given below :

- Use virus protection software and update it regularly.
- Use Firewall software.
- Be suspicious of all unsolicited Email and text messages.
- Disconnect your computer from the Internet if you are not using any services of Internet.
- Download software with caution. Before downloading the software check the authenticity of the website.
- Close spyware windows, if it opens in your computer. Active window runs spyware program into the memory and continues its destructive actions.
- Before using any removable media, scan it for malware and viruses by antivirus software.
- Keep current. Use the updated versions of software. Older version may have security breaches.
- Back up regularly. Take a back up of data into another system or on the cloud storage.

❑ **Check Your Progress – 4 :**

1. To use the removable media into the computer, what will you do after plugging removing media ?

   [A] Update antivirus [B] Scan the media

   [C] Backup the data [D] Open the firewall

2. How to protect the system from outsiders ?

   [A] Installing Antivirus [B] Taking backup

   [C] Implementing Firewall [D] None of the above

3. How to protect yourself from phishing ?

[A] Be suspicious of all unsolicited Email and text messages.

[B] Using the latest version of the software.

[C] Taking backup of the system regularly.

[D] Updating antivirus software regularly.

11.5 Firewalls :

A Firewall is available in the form of Hardware or Software, that protect the user's network resources from another (outsider) networks of the Internet. To protect the systems of the LAN from the different types of attacker on the Internet Firewall is a key solution.

Organizations are implementing Firewall to protect the network resource of an organization from the outsider as well as to restrict the Employees of the organization to access some sensitive data like personal data records of the Employees or Payroll records.

Firewall is usually implemented into the system which actually act as gateway system. It is implemented at the point where LAN connects to the WAN. Firewall will block all the ports of gateway machine accept those which are in used by the personal or organization. If all unnecessary ports are blocked, it is difficult for the attacker to cross the firewall and access any sensitive data of the organization. Firewall, thus act as a protective layer between LAN of the organization and the Internet.

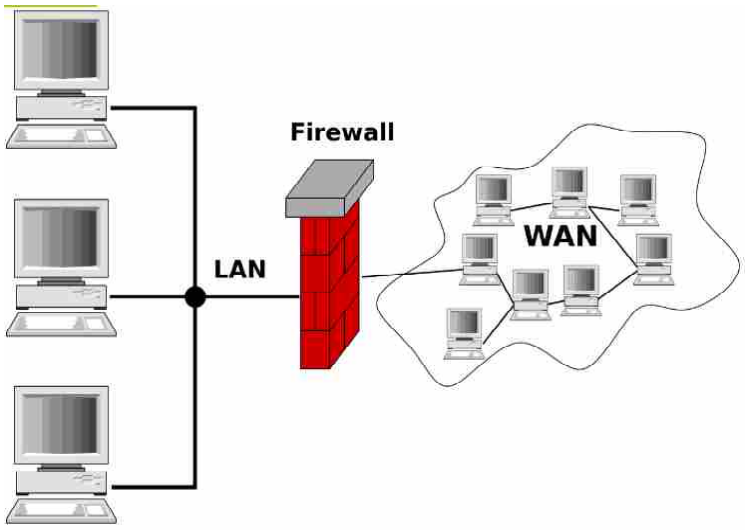

Fig. 11.1 : Firewall

Home and small office user in which system is directly connected to the Internet, can use personal Firewall. It will be installed in the systems which directly interact to the Internet. Windows and Mac operating system, provides Firewall software bult–in to the operating system itself. Now, a day some antivirus software products are providing the Firewall software as a bundled with their antivirus product.

11.6 Prevention From Unauthorized Access :

Unauthorized access means any user access the computer or network resource without permission or without the knowledge of actual user of the system or network. Unauthorized use is the use of a computer or its data for unapproved or possibly illegal activities.

To prevent the system from unauthorized access Firewall is obviously one solution, apart from Firewall and use of Antivirus software, you can also implement [1] Authentication and [2] Authorization.

11.6.1 Authentication :

Authentication is the process of identifying user. Various mechanisms can be used to do authentication. Username and Password is the simplest method to identify the user (Authentication). Operating system or any software, when start they ask to enter username and password. If user enters correct username and password then system grant the resources to that user. The person who has given valid login credential is called authenticated user. Some website allows user to access some areas of the website without login, for example you can view the products on Amazon or Flipkart without login. A user who access some part of the software without providing their login credential is called Anonymous user or visitor.

Keeping strong password is a skill. Some users don't understand the seriousness of authentication, and choose weak password. Those users become an easy target to the attackers. Here, we have given some tips to keep strong password.

1. Try to avoid personal information in the password. Some user set their mobile number, name or vehicle number as a password. Such type of password is easily guessable and system can be accessed by unauthorized user.
2. Maintain minimum length of the password. Password should be more than 8 characters. Small passwords can be easily tracked by the person standing nearer to you while entering the password or by some software.
3. Password must be difficult. It should have combination of uppercase letters, lowercase letters, digits and special symbols.
4. Change your password on regular time interval basis.
5. Use variations in the password. Do not keep same password for all the websites.
6. Use passphrase in the password. Do not keep a password which spell correctly as per dictionary. If you keep a password which available in the English dictionary, it can be easy recovered by unauthorised person by applying dictionary attack.
7. Avoid common sequence in the password. Your password should not be like '1234' or 'abcd' etc.
8. Manage the password properly. Make sure you need to remember your password. You do not have to write the password which can be easily accessible to someone. Many users are wrongly writing their ATM access password on the ATM card itself.

Apart from the text–based username and password, the other methods are also there to authenticate the user. Some application allow user to enter PIN number to authenticate the user. PIN (Personal Identification Number) is either 4–digit or 6–digit number to authenticate the user. Where some applications do the authentication by taking finger prints of the user by using finger print scanner or by face recognition using front camera module.

11.6.2 Authorization :

Authorization is process that has to be performed after authentication. It is a security mechanism that determines user privileges or access levels related to the resource of a system including data, files, services or applications installed in the system. Once the username and password are verified and user is identified by the system then system will grant only those resources to the user, which are granted to that user by network administrator. To implement authorization, network administrator can implement ACL (Access Control List).

❑ **Check Your Progress – 5 :**

1. _____ is the process of identifying user.

   [A] Authorization [B] Access Control List

   [C] Authentication [D] Firewall

2. _____ can be installed between LAN and WAN to protect the resource of LAN from outsiders.

   [A] Antivirus [B] Firewall

   [C] ACL [D] None of the above

3. Identify the method of Authentication from the given options :

   [A] By accepting text–based Username and Password.

   [B] By taking PIN from the user.

   [C] Using biometric devices.

   [D] All of the above.

11.7 Let Us Sum Up :

In this unit :

- We have discussed about digital security risks and cybercrimes.
- We gain awareness about different types digital threats.
- We have seen, how secure the computer system and network.
- We have understood the importance of Firewall
- Finally, we have ended our discussion with how to protect the system from unauthorised access, Authentication and Authorization.

11.8 Suggested Answers For Check Your Progress :

❑ **Check Your Progress 1 :**

1. [A] 2. [B] 3. [D]

❑ **Check Your Progress 2 :**

1. [D] 2. [B] 3. [C]

❑ **Check Your Progress 3 :**

1. [C] 2. [D] 3. [A]

❑ **Check Your Progress 4 :**

1. [B] 2. [C] 3. [A]

❑ **Check Your Progress 5 :**

1. [C] 2. [B] 3. [D]

11.9 Glossary :

ATM : Automated Teller Machine. It is a machine managed by banks so that its customer can withdraw the money.

ACL : Access Control List. It can be made by the network administrator to grant the various resources to different network users.

PIN : Personal Identification Number. It is an authentication method to identify user.

11.10 Assignment :

1. List and explain different types of Digital Treats in detail.
2. Write a short–note on Authentication process.
3. Explain the term : 'Firewall'.

11.11 Activity :

Make a list of different types of authentication methods which you have observed.

11.12 Case Study :

- Find "What is Encryption ?" and different types of Encryption techniques on the Internet.

11.13 Further Reading :

1. Computer Fundamentals by P.K.Sinha and Priti Sinha.
2. Discovering Computers 2016 by Shelly Cashman Series. CENGAGE publications.
3. Computer Fundamentals by Pearl Software, Khanna Book Publishing.

BLOCK SUMMARY :

- Two or more devices are connected with each other to share data or resource is called network.
- If the devices are computing devices, then two or more computing devices are connected to each other is called computer networks.
- With the help of network, we communicate with each other, we can transfer the data from one machine to another as well data and resource sharing are main advantages of computer network.
- Computer network can be classified as LAN, MAN, and WAN.
- LAN is a smaller network, geographically located into one campus, one building or two nearby building, MAN is wider than LAN can be spreader withing city or connects two nearby cities.
- WAN is a wide arear network, can be spreader into the country, region or in the world.
- PAN is a Personal Area Network, can be made by any individual by connecting two or more computing devices with help of Bluetooth technology.
- Network can be of two types : Point–to–Point or Broadcast.
- Physical layout or arrangement of the computing devices is called Topology. Star, Bus, Ring, Mesh and Hybrid are the names of different topologies.
- Internet is the network of networks; it is also known as information superhighway.
- Internet has been evolved by Department of Defence of the USA, during their research on nuclear weapons.
- The name given to the first network by Department of Defence, USA was ARPANET : Advanced Research Project Agency Network.
- To access the benefits served by Internet we need to connect our device with Internet. To get the Internet we need to take connection from ISP : Internet Service Provider.
- Machine on the Internet are communicating with each other by a unique address called IP–address. There are two versions are there of the IP addresses : IPv4 and IPv6.
- Browser is the software by using it we can surf any website. The field name in which we are writing name of the site is called URL : Uniform Resource Locator.
- Website is a collection of webpages. Webpages are electronic document, can be linked with each other. The link, which connects two web pages are called Hyperlink.
- To design a webpage a special language is used called HTML : Hypertext Mark–up Language.
- When the device is connected to the Internet, chances are there that someone outsider can damage the machine, data, information or software.
- Crime committed using Internet is called Cybercrime.

- Malware, Botnet, Denial of service attack, Back door, Spoofing are different types of attack, which attacker might use to for their profit or to harass you.
- Cybercrime can be categories as hacker, cracker, script kiddie, unethical employee or cyberterrorists.
- Firewall is the software or hardware system, can be implement between LAN and WAN, to protect the LAN resources from the outsiders.
- Authentication is the process of identifying user.
- Authentication can be done by text–based username and password, PIN–based, or using any Biometric device, like figure print scanner of face recognition.
- Authorization is the process of distributing resource to the user after authentication, so that user can access only those resources which are granted by network administrators.
- ACL : Access Control List can be used to implement Authorization.

BLOCK ASSIGNMENT :

❖ **Short Answer Questions :**

(1) List the limitations of networks

(2) List different topologies

(3) What is PAN ? Explain it with an example

(4) What is ISP ?

(5) List different steps to secure your system from the different types of Internet attacks

(6) What is authentication ?

(7) What is authorization ?

❖ **Long Questions :**

(1) List and explain advantages of computer networks

(2) Explain classification of networks in brief

(3) Explain Point–to–Point and Broadcast network in detail

(4) What is IP ? Explain it in brief

(5) Explain different types of Internet attacks in detail

(6) Explain the function of Firewall in detail

❖ **Enrolment No. :** ☐

1. How many hours did you need for studying the units ?

Unit No.	9	10	11
No. of Hrs.			

2. Please give your reactions to the following items based on your reading of the block :

Items	Excellent	Very Good	Good	Poor	Give specific example if any
Presentation Quality	☐	☐	☐	☐	_____
Language and Style	☐	☐	☐	☐	_____
Illustration used (Diagram, tables etc)	☐	☐	☐	☐	_____
Conceptual Clarity	☐	☐	☐	☐	_____
Check your progress Quest	☐	☐	☐	☐	_____
Feed back to CYP Question	☐	☐	☐	☐	_____

3. Any other Comments

.....

.....

.....

.....

.....

.....

.....

.....