CHAPTER-3
NETWORK SECURITY ON INTERNET

Internet Security: -

- Internet security is the practice of protecting and preserving private resources and information on the Internet.
- In the computer industry, **security** refers to the techniques for ensuring that data stored in a computer cannot be accessed by any individual without authorization.
- Most security measures involve data encryption and passwords.
- Data encryption is the translation of data into a form that is unintelligible without a decoding mechanism.
- A **password** is a secret word or phrase that gives a user access to a particular program or system.

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:

(i) Viruses
(ii) Worms
(iii)Trojans

Network Security Threats and Attacks: -

I.Virus: -

- It means Vital Information Resources Under Seize, is a maliciously written code that replicates itself.
- Viruses are computer programs developed to copy themselves and infect other files stored on the computer.
- These are malicious programs that damage hardware, software or information files.
- By definition, human interaction is necessary for a virus to spread to another user's files.
- 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.
- 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 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.

- Viruses are classified on the basis of their mode of existences and there are three categories of virus.

(a) Boot Infectors :- Some viruses reside in the boot sector of the disk and not in the program file. It gets loaded as soon as the system is switched on and takes the control of the system.

(b) System Infector : - The system infectors attach themselves to memory resident files such as COMMAND.COM. These infectors take control after the computer's system is booted and directly affects the hard disk.

(c) Executable Program Infectors: - These are the most dangerous virus around. They attach to the program files and can spread immediately to any of the executable files. The size of .EXE and .COM files becomes too large to be executed.

II. WORM (Write Once Read Many) : -

- It is similar to Virus.
- 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.
- The main difference is that worms reside in memory and usually remain unnoticed until their effects become apparent, obnoxious or overwhelming.
- 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.
- To protect against a Worm, networked users must keep up with operating system patches and update as well as antivirus software and be aware of any suspicious traffic.

(iii)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.
- 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

Difference among VIRUS ,WORM AND TROJAN : -

VIRUS	WORM	TROJAN
(i) It stands for Vital Information Resources Under Seize	(i) It stands for Write Once Read Many.	(i) The term Trojan is derived from the Trojan horse story in Greek mythology
(ii) Virus is a software or computer program that connects itself to another software or computer program to harm computer system.	(ii) Worms replicate itself to cause slow down the computer system.	(ii) Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
(iii) Virus replicates itself.	(iii) Worms are also replicates itself.	(iii) But Trojan horse does not replicate itself.
(iv) Virus can't be controlled by remote.	(iv) Worms can be controlled by remote.	(iv) Like worms, Trojan horse can also be controlled by remote.
(v) Spreading rate of viruses are moderate.	(v) While spreading rate of worms are faster than virus and Trojan horse.	(v) And spreading rate of Trojan horse is slow in comparison of both virus and worms.
(vi) The main objective of virus to modify the information.	(vi) The main objective of worms to eat the system resources.	(vi) The main objective of Trojan horse to steal the information.

How to secure your computer from the Internet Threats: -

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 antivirus 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, MacAfee, AVG , Avast, Kasper Sky, Quick Heal etc.

An Anti-virus software is used to prevent, detect, and remove various computer threat, including computer viruses, worms, and Trojan horses.

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.
- Avoid using open Wi-Fi.
- Never download any email attachment from an unknown sender.
- Avoid even browse email sent by some unknown sender.
- Must take back up 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.

Network Security : -

The network security (or information security) is to provide protection to the computer system from the hackers (intruders).

The following are the key components of network security architecture:

(i) Authentication: It is the action of verifying information such as identity, ownership or authorization. It verifies that a user requesting access is the one who (he or she) claims to be prior to being allowed access to the network and network services.

(ii) Access Control : - Access control is a security measure that defies who can access a computer, when they can access it, and what actions they can take while accessing the computer. These are numerous approaches in providing access control, ranging from password protection to token-based mechanism to biometric encryption technologies.

(iii) Authorization: - Authorization means providing a proper username and password for an individual by the vendor (Ex: ISP). Wherein "Username" is an enable character for identifying a particular user and a "Password" is secrete code or phrase that gives a user to access a particular program or system.

(iv) Privacy: - Privacy is the state of quality of being isolated from the view and or presence of others. The goal of privacy is to ensure that unauthorized users on the network cannot see the contents of the message being sent. It is synonymous with confidentiality and security.

(v) Integrity: - Integrity includes the security of the network environment, the network devices, and the flow of information between them. It addresses the problems of unauthorized manipulation or destruction of data. Data integrity is ensured by encryption. If information is received that cannot be decrypted properly, then the recipient knows that the information has been tampered with during transmission.

Network Management : -

Network management keeps track of detailed records of user identities, the communications on the network, the network services users are accessing, and the network resources being utilized. It provides this information for billing, auditing, reporting, and subsequent reviews of related security events.

Some of the precautionary methods to guard the security of data in store or on the move over a network. The most common methods include

(i) Encryption (ii) Firewall (iii) Digital Signature

(i) Encryption :

- Encryption is a security method in which information is encoded in such a way that only authorized user can read it.
- In this process a plaintext gets transformed into unreadable form(called cipher-text) using a mathematical process.

An encryption process includes four elements :

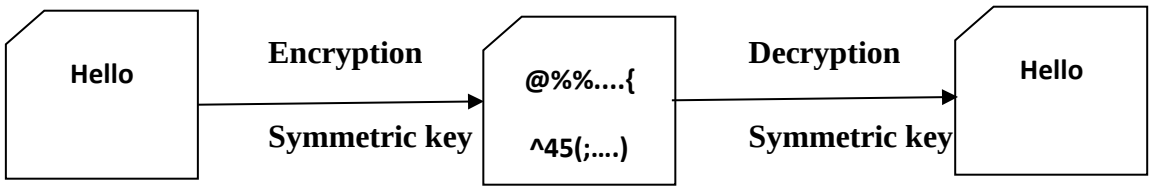
1. The plaintext, the raw data or message to be encrypted
2. The cryptographic algorithm, a mathematical method that determines how plain-text is to be combined with a key.
3. The key, a string of digits
4. The cipher text, the encrypted message.

There are two types of encryptions schemes as listed below

(a)Symmetric (private-key or secret-key) Key encryption

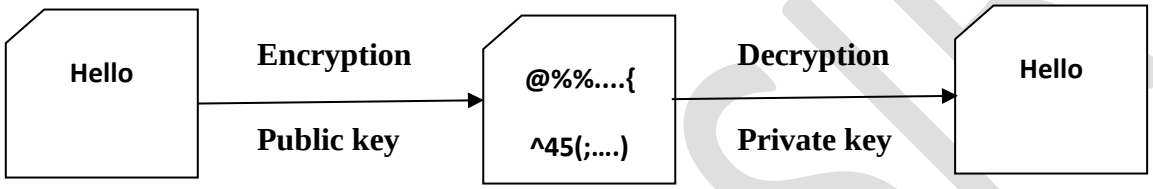
(b)Asymmetric (public-key) Key Encryption

(a) Symmetric Encryption : Symmetric key encryption algorithm uses same cryptographic keys (a mathematical function) for both encryption (of original text) and encryption (of cipher text).



(Original Data) **(Original Data)**

(b) **Asymmetric Encryption :**Public key encryption algorithm uses pair of keys, one of which is a secret key(known only to the receiver) and one of which is public (for sender).These two keys are mathematically linked with each other.



(Original Data) **(Original Data)**

Difference between Encryption and Decryption : -

Encryption	Decryption
(i) Encryption is the process of converting normal message into cipher text.	(i) Decryption is the process of converting cipher text into its original form.
(ii) Encryption is the process which take place at sender's end.	(ii) Decryption is the process which take place at receiver's end.
(iii) Any message can be encrypted with either secret key or public key.	(iii) The encrypted message can be decrypted with either secret key or private key.
(iv) In encryption process, sender sends the data to receiver after encrypted it.	(iv) In decryption process, receiver receives the information(Cipher text) and convert into plain text.

Difference between Private key and Public key : -

Private key	Public key
(i) In this, the same key (secret key) and algorithm is used to encrypt and decrypt the message.	(i) In public key cryptography, two keys are used, one key is used for encryption and while the other is used for decryption.
(ii) Private key is **Symmetrical** because there is only one key that is called secret key.	(ii) Public key is **Asymmetrical** because there are two types of key: private and public key.
(iii) In this, sender and receiver need to share the same key.	(iii) In this, sender and receiver does not need to share the same key.
(iv) Private key is faster than public key.	(iv) It is slower than private key.

Note :

Hashing : Hashing is a technique used to encrypt data and generate unpredictable hash values.
Hashing Algorithm : It provides a way to verify that the message received is the same as the message sent.

(ii)Firewall : -

- A firewall system is a hardware/software configuration, physically located between an internal and external network that protects the internal network from unwanted intrusion from the outside network.
- Firewalls restrict information entering and leaving at carefully controlled points.
- If implemented properly, they are very effective at keeping out unauthorized intruders and stopping unwanted activities on the internal network.

There are many different ways to implement the firewalls :

(i) Packet-level authentication – access by protocol
(ii) Address- based authentication – access by IP address (both source and destination)
(iii) User authentication by login/password over Secure Socket Layer (SSL)
(iv) Performing IP address translation ,and
(v) Point –to – point encryption at IP – level in Virtual Private Networks (VPNs).Firewalls can also be used for intranet access control.

- Firewalls can also be used for Intranet access control.
- It is a barrier between Local Area Network (LAN) and the Internet.
- There are two types of Firewall System: One works by using filters at the network layer and the other works by using proxy servers at the user, application or network layer.

Note :

Proxy Server : A proxy server is a bridge between you and the rest of the Internet. Normally, when you use your browser to surf the Internet, you'll connect directly to the website you're visiting.

(iii)DIGITAL SIGNATURE: -

Signature is unique to a person when we sign a document i.e. we agree whatever is there in the document. If our sign is placed / stored by computer in the form of digital is called as Digital Signature. A digital signature is basically a way to ensure that an electronic document (E-Mail, spreadsheet, text file etc) is authentic.

In case of Cyber Crime, a digital signature plays a significant role to ensure authenticity and thus protect security of a computer system.

Use of Digital Signature: -

- With time, the importance of digital signature is increasing in India and all over the world.
- The most use of digital signature in the field of e-Governance.
- The departments of Government use digital certificates through websites, e-mail, sms etc.
- The other agencies like Companies or Individual rely mostly on this like e-tender, e-tax, e-banking etc.
- This allows online financial transactions like filing of online return.
- In futuristic paperless office, the digital signatures will be an integrated and indispensable (essential) part.

Applications: -

There are several reasons to implement digital signatures during important electronic communications. The reasons are

(a) Authentication: Digital signatures help to authenticate the sources of messages.

(b) Integrity: Once the message is signed, any change in the message would invalidate the signature.

(c) Non-repudiation: By this property, any entity that has signed some information cannot at a later time deny having signed it.

Cookies :

- Cookies are messages that web servers pass to your web browser when you visit Internet sites.
- Your browser stores each message in a small file (only up to 4kb in size), called'cookies.txt'.
- When you request another page from the server, your browser sends the cookie back to the server.
- These files typically contain information about your visit to the web page, as well as any information you've volunteered, such as your name and interests.

Use of Cookies : -

(i) Cookies are most commonly used to track website activity.
(ii) Cookies are also used for online shopping.
(iii) Many portals and search engines use cookies to provide personalized web pages.
(iv) Only the website that creates a cookie can read it, so other servers do not have access to your information.
(v) Webmasters have always been able to track access to their sites, but cookies make it easier to do so.
(vi) Many websites use cookies to log their users in automatically.
(vii) Visitor tracking and statistics systems often use them to track visitors.

Cyber Crime : -

Definition:

Cyber Crime is defined as crimes committed on the Internet using the computer as either a tool or a targeted victim.

(or)

Cyber crime may be "Unlawful acts wherein the computer is either a tool or a target or both".

1. **The Computer as a target:** - Using a computer to attack other computers.
   (i) Hacking
   (ii) Virus / Worm
   (iii) Cookies / Spam
   (iv) Denial of Service
   (v) Snooping
   (vi) Spoofing
   (vii) Cyber stalking
   (viii) Software piracy etc.
2. **The computer as a tool:** - Using a computer to commit real world crimes.
   (i) Cyber Terrorism
   (ii) Intellectual Property Right violations
   (iii) Cyber Squatting
   (iv) On-line frauds
   (v) Pornography etc.

Types of Cyber Crime:

There are a good number of cyber crime variants or types. A few varieties are discussed here for the purpose of the basic idea about the cyber crime.

I. Hacking : -

- The activity of breaking into a computer system to gain an unauthorized access is known as hacking.
- The act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system is called as hacking.
- Computer hacking is the most popular now a days, especially in the field of computer security, but hacking exists in many other forms, such as phone hacking, brain hacking etc.
- Hacking web servers taking control on another person's website called as web hijacking.

II. Online Fraud : -

- It is basically refers to the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them.
- For example by stealing personal information, which can even lead to identity theft.
- A very common form of Internet Fraud is the distribution of rogue (rascal) security software.
- Some of the online frauds are as: Purchase Fraud, Online auction, PayPal Fraud, Work-at-home donation processing, SEO (Search Engine Optimization) fraud etc.

III. Pornography : -

- Pornographic (often abbreviated as "porn") is the explicit portrayal of sexual subject matter for the purpose of sexual gratification.
- Pornography may use a variety of media, including books, magazines, postcards, photos, video etc.
- In internet pornographic websites displaying obscene (unseen) pictures or films, exercise damaging influence on the mental and moral fabric of the children of adolescent age.
- Modern pornography involves like Capturing Picture/Video from Mobile/Camera and sending through websites, MMS (Multi Media Service), Bluetooth etc.

IV. Snooping: -

- The act of secretly checking one's mail, writing or any such information without his/her knowledge is called as 'snooping'.
- In context of network security, snooping refers to gaining unauthorized access to another person's or organization's data.
- This may be done in a number of ways:
  - By getting someone's login information by casually watching what he/she is typing.
  - Reading the files on someone's computer in an unauthorized manner
  - Using some software which keeps track of the activities and data being sent or received on someone's computer.

V. Spooling: -

- Acronym for *S*imultaneous Peripheral Operations O***n-Line***.
- *Spooling* refers to putting jobs in a buffer, a special area in memory or on a disk where a device can access them when it is ready.
- The most common spooling application is *print spooling.*
- In print spooling, documents are loaded into a buffer (usually an area on a disk), and then the printer pulls them off the buffer at its own rate.

VI. Spoofing: -

- Spoofing as the word is used in computer parlance, means falsifying (fake) one's identity.
- In the context of network security, a spoofing refers to introducing traffic pretending to be someone else.

Some examples of spoofing are given below:

(i) **Caller ID Spoofing:** This spoofing is the practice of causing the telephone network to display a number on the recipient's Caller ID display that is not that of the actual originating station.

(ii) **IP Address Spoofing:** This spoofing refers to the creation of IP packets with a forged source IP address, with the purpose of concealing the identity of the sender.

(iii) **Protocol Spoofing:** This spoofing is used in data communications to improve performance in situations where an existing protocol is inadequate.

(iv) E-Mail Spoofing : This spoofing is the practice of sending an email pretending to be someone else.

VII. Cyber Stalking: -

- It is the use of Internet or other electronic means to stalk someone.
- This term is used interchangeably with online harassment and online abuse.
- Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly such as: Threatening e-mails, live chat harassment, leaving threatening message on face book, sending electronic viruses, sending unsolicited e-mail, tracing computer/Internet resources, impersonation of the victim to solicit sex acts, identity theft etc
- Key factor to identify cyber stalking cases include :
    a) False accusations
    b) Gathering information about the victim
    c) Monitoring victim's activities
    d) Encouraging others to harass the victim
    e) False victimization

VIII. Software Piracy: -

- Illegal copying, distribution, or use of software is often termed as software piracy.
- This can be done in a number of ways.
- Usually pirates buy an original version of a software, movie or game and illegally make copies of the software available online for others to download and use without the notification of the original owner of the software. This is known as Internet piracy.
- Different types of software piracy include :
    a) **Soft-lifting:** Borrowing and installing a copy of a software application from a colleague.
    b) **Client-Server overuse:** Installing more copies of the software than you have licenses for.
    c) **Hard-disk loading:** Installing and selling unauthorized copies of software on refurbished or new computers.
    d) **Counterfeiting:** Duplicating and selling copyrighted programs.
    e) **Online piracy:** Typically involves downloading illegal software from peer-to-peer network, Internet auction or blog.

Note :

Other Cyber crimes are :

(i) Denial of Service : -

- DoS is the acronym for **D**enial **o**f **S**ervice.
- DOS is an attack used to deny legitimate users access to a resource such as accessing a website, network, emails, etc. or making it extremely slow.
- This type of attack is usually implemented by hitting the target resource such as a web server with too many requests at the same time.
- This results in the server failing to respond to all the requests.
- The effect of this can either be crashing the servers or slowing them down.
- Examples of such attacks include :
    a) Flooding the network to prevent legitimate network traffic.
    b) Disrupting the connections between two machines, thus preventing access to a service.
    c) Preventing a particular individual from accessing a service.
    d) Disrupt a specific website.

(ii) Spam: - Spamming is the act of sending unsolicited messages to many users at a time, possibly up to thousands, with the usual intention of advertising products to potential customers.

(iii) Eavesdropping : -

- Eavesdrop means secretly listening others private conversation without their knowledge.
- Eavesdropping refers to unauthorized access to another person's or organization data while the data is on its way on the network.
- The various form of communication includes phone calls, emails, instant message or any other Internet service.

(iv) Cyber Terrorism : -

- Cyber Terrorism essentially consists of using computer technology to engage in terrorism.
- Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets.
- Others like police, medical, fire and rescue systems etc.

(v) Intellectual Property Rights (IPR) violations : -

- Intellectual Property Rights are rights to intangible things, that is, ideas as expressed (copyrights), or as embodied in practical implementation (patents).
- These include software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

(vi) Cyber Squatting: - It is practice of registers domain name identical to popular service provider's domain so as to attract their users and get benefit from it.

(vii) Phishing :-

- Phishing is a just one of the many frauds on the Internet, trying to fool people into parting with their money.
- Example :
  - Stealing bank transaction password from users.
  - Stealing login credentials from users.

(viii) Vishing : -

- Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private, personal and financial information from the public for the purpose of financial reward.
- The term is a combination of "voice" and "phishing".
- Example :
  - Asking for bank transaction OTP from users.
  - Asking for UPI PIN from users.

Difference between Phishing and Vishing : -

Phishing	Vishing
(i) Phishing attack is targeted for a wide range of people through emails.	(i) Vishing attack is also targeted for a wide range of people through voice communication.
(ii) Victim needs to click on malicious links.	(ii) Victim needs to tell the information on own.
(iii) It is an automated attack.	(iii) While it is a manual attack.
(iv) A single attacker can send various emails at a time.	(iv) Voice calling to target can be done by a attacker one a time.
(v) The banking industry as a soft target for phishing scams in India.	(v) It is used to steal credit card numbers or other information used in identity theft schemes from individuals.

Cyber Laws: -

- Cyber Law is the law governing cyber space.
- Cyber space is a term, which is used to describe the application domain of computer, networks, software, data storage devices, the Internet, websites, emails and even electronic devices such as cell phones, Point of Sales terminals and ATM machines.

Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property Rights
4. Data Protection and Privacy

Need for Cyber Law : -

1. Disrespect for jurisdictional boundaries
2. Gigantic traffic volumes every second
3. Open to participation by all
4. Enormous potential for anonymity
5. Economic efficiency
6. Extreme mobility
7. Pirated across the globe
8. Theft of corporeal information (ex books , papers , auxiliary memory devices)

Cyber Law in India (IT Act 2000): -

- The primary source of cyber law in India is the Information Technology Act, 2000(IT Act) which came into force on the 17th,October 2000.
- There are various penal provisions have also been included in the IT Act 2000 under the **IT (Amendment) Act, 2008.**
- The Act totally has 13 chapters and 90 sections (the last four sections namely sections 91 to 94 in the ITA 2000).

Some important Sections under the IT Amendment Act-2008 are given below :

(i) Chapter – III / Section -4
(ii) Chapter – IX / Section 43
(iii) Section 65
(iv) Section 66
(v) Section 66A
(vi) Section 66B
(vii) Section 66C
(viii) Section 66D
(ix) Section 66E
(x) Section 66F
(xi) Section 67
(xii) Section 69
(xiii) Section 69A
(xiv) Section 69B