MASTER OF COMPUTER APPLICATION

MCA-34

CYBER SECURITY

Directorate of Distance Education

Guru Jambheshwar University of Science &
Technology, Hisar – 125001

CONTENTS

SUBJECT: Cyber Security	
COURSE CODE: MCA-34	**AUTHOR: DR. ABHISHEK KAJAL**
CHAPTER NO. 1	

Introduction to Network Security

INDEX **Page No.**

Network and Security Concepts:

Network and Security

Lesson-1

(Network and Security Concepts)

Before we study Network and Security concepts, we should also know about network definition, types of network and what are the security threats measurements and how to protect our data and information on a network. Without knowing the basics of networking, it will be difficult to understand the security methods and concepts.

1.1 Introduction to Network

Two or more computers that are connected to each other to share resources, transfer files, or communicate electronically make up a network. Cables, telephone lines, radio waves, satellites, or infrared light beams can connect computers in a network. A network is a collection of servers, networking devices, and computer systems connected to each other to share resources like a printer or file server computer. Wireless or cable media can be used to establish connections.

1.2 Network Types

A group of computers connected to each other to communicate and to share their resources, data, and applications is called Computer Network. Computer networks can be used for the following purposes:

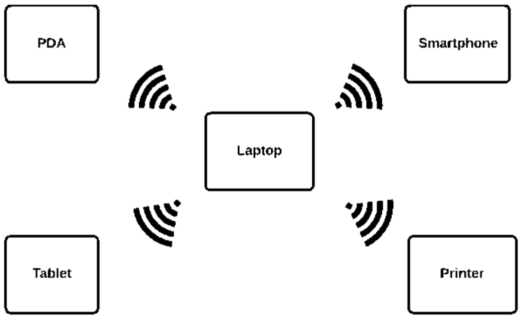
- To communicate using instant messaging, email, audio, video etc.
- To share resource devices such as scanners, printers and even hard disks etc.
- To share data or files
- To share applications or programs and softwareon remotely on computer systems.
- To allow maintaining information easily and accessing by network users.

Networks of Computer:

- PAN - Personal Area Network
- LAN - Local Area Network
- MAN - Metropolitan Area Network
- WAN - Wide Area Network
- VPN - Virtual Private Network

1.2.1 PAN - Personal Area Network:

One of the most common computer network type is PAN (Personal Area Network). This network can be controlled by a single person. An individual can do communication between the computer devices in work space which is centered. PAN provides network area of 10 meters from source to destination device.

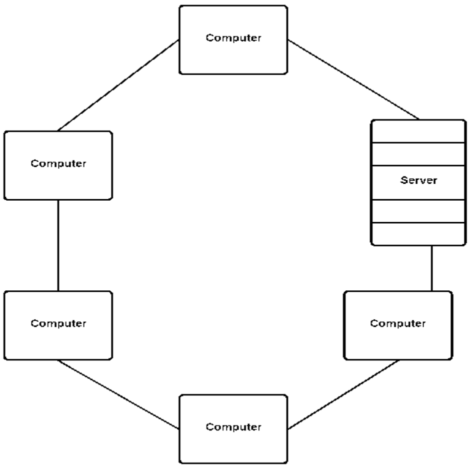


(fig. 1.1)

USB, computer, mobile, Tablet, printer, PDA etc. are few examples of PAN.

1.2.2 LAN - Local Area Network:

A network that links computers all together via a common communication line within a local limited area is called LAN (Local Area Network). A LAN consists of at least two or more than two computers linked to one server. Ethernet and Wi-Fi are two communication methods used in this type network.

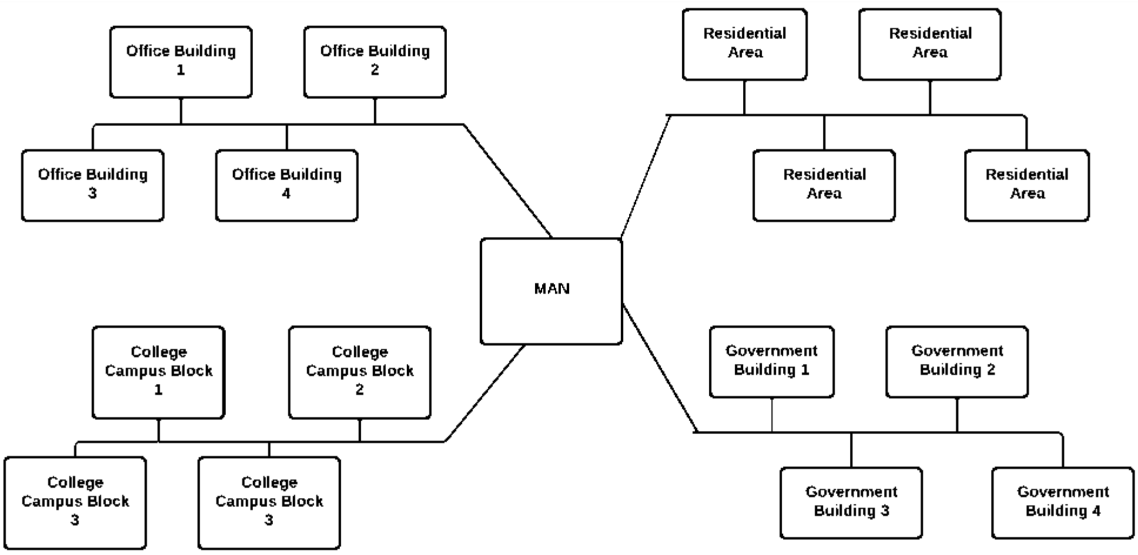


(fig. 1.2)

Most networks used in any home, office, school, college, library, laboratory, etc. are few examples of LAN.

1.2.3 MAN - Metropolitan Area Network:

MAN (Metropolitan Area Network) is a network bigger than LAN (Local Area Network), but smaller than WAN (Wide Network Area). In this network type all the computers are connected in a geographical distance via shared lines for communication within anytown, a city, or any metropolitan area.

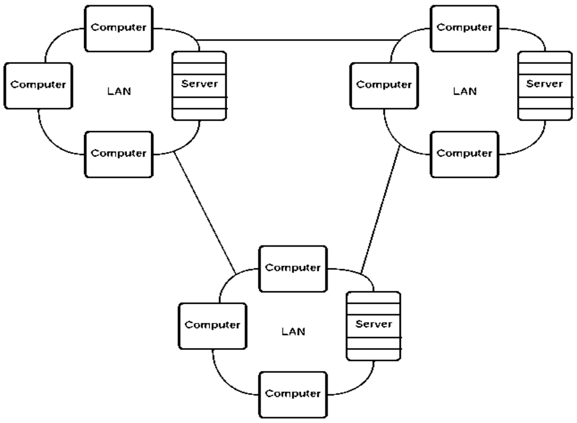


(fig. 1.3)

Examples of MAN Network are all such networks which are spread amonglarge area within multiple buildings, cities, towns ora single large city.

1.2.4 WAN - Wide Area Network:

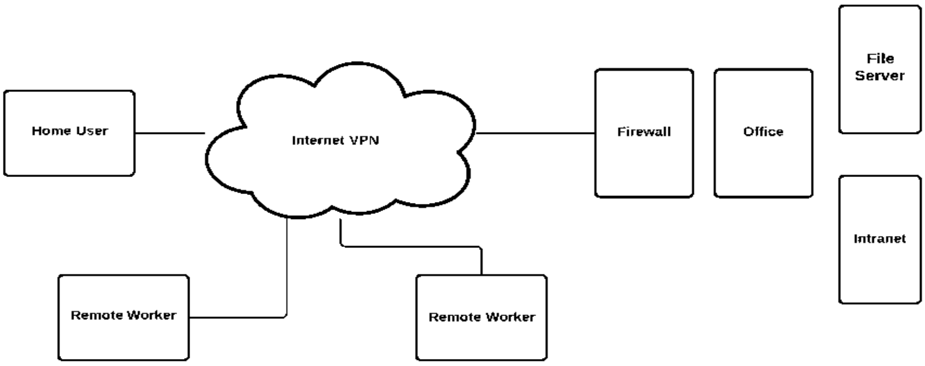
A network of computer that links computers in distance of a large geographical area using sharedcommunicating lineis called WAN (Wide Area Network). WAN is also called a huge network of many networks of local area that is usedfor communication toeach other. The very commonly used WAN network is INTERNET.



(fig. 1.4)

1.2.5 VPN - Virtual Private Network:

A network of computers that widens across the internet and constitutesa private network is called VAN (Virtual Private Network). It provides facility to send or receive data to the user like they are linked in real, while in reality they are not linked, but seems to constitute a private networkvia a connection that is virtual and point topoint.Such type of networks helps in prevention of malicious sources as the connection make use of encrypted one so as to ensure that sensitive data is securely transmitted over VPN.



(fig. 1.5)

1.3 Computer Network Characteristics

- **Fault Tolerance:** It means, a network has the ability to work continuously even if the failures occur, and ensure no loss of services to web server by finding alternate connection with another connection as a substitute.

- **Scalability:** It means, a network has the ability to extend with the needs,and continue performing good performance. The Internet itself is the example of scalability.
- **Quality of Service (QoS):** It means, a network is able to set priorities, reduce data loss, delay and manage data traffic etc.
- **Security:** Security means a network is able to protect our network from unauthorized access, forgery or misuse. Also it can provide integrity, confidentiality and availability.

1.4 About Network Security

Network Security is known as a methods used for precautions and for protecting Computer network structure from leaking private data, misuse, failure, alteration, destruction and unauthorized access. It is a process to secure networks from possible security threats. Network security allows registered users use networks, while on the other hand, it protects from malicious actors from misusing threats and exploits the system. As hackers are exponentially growing in numbers and day by day upgrading themselves with smarter techniques, world definitely need network security tools to prevent network from numbers of hackers who are growing and getting smarter by each passing day.

A technique used by any organization to ensure the security of organization's assets besides all traffic and data transferring in network is known as Network Security. It protects both software and hardware of a system. Network security protects and monitors network usage by detecting and preventing many of threats exploiting or using the network. Network security is necessary and essential these days while doing transactions and communication within the individuals, businesses and for government. Because of the frequency and different types of attacks or possible disruptive attacks in the future, Network security has become a key for security essentials. By using network security measures, users, computer systems and programs operate their tasks in a network by using authorized critical functions safely. Network security is a multilayered approach which can be defined at the data link layer, network layer and application layer.

1.5 Types of Network Security

In an enterprise, network security has several levels. Attackers can attack at any layer of the network model, so it is important to protect your system hardware, software, and policies by configuring network security. Types of network security are described further.

1.5.1 Physical Network Security:

There are so many types of attacks on physical devices as devices have become more compact and easy to breach. Physical network security is essential to safeguard private data and information from stealing, unauthorized access or sometimes computer hardware theft.

1.5.2 Technical Network Security:

We can protect confidential data on the network either in inbound or outbound by using technical network security. It is important to stop unauthorized access of data and systems as well as malicious activities done by employees.

1.5.3 Administrative Network Security:

Network security that controls organizational-level security policies by governing user actions like authentication, level of access, and execution of infrastructure changes by IT staff is called Administrative network security.

1.5.4 Access Control Security:

It is a technique of improving organizational private network security by controlling network resources from source to destination devices which follows security policies. Two components of a standard network access control scheme are given below:

- **Restricted access:** Restricted access is a process of allowing or refusing access permissions to protect resource. It is also known asauthorization.
- **Network Boundary Protection:** It controls logical communication to and from networks. Many firewalls can be used to protect network infrastructure. Besides it, intrusion detection & prevention tools are used for network boundary protection.

1.5.5 Application Security:

The method of detecting, identifying, repairing and improving software is called application security. As many hackers are trying to hack applications with different type of attacks. So,many application security methods are developed to protect application data from locking down coding, assessing coding, evaluating encryption tools, monitoring permissions and access rights. Besides, a lot of advance methods designed for security of web based applications, smart phone based apps, network-based apps and firewalls.

1.5.6 Firewalls Security:

A network security system which checks and controls incoming and outgoing traffic of a network, allowing or stopping data packets within security rules is known as Firewall. It creates a firewall between internal network and traffic coming from other internet sources to protect network from malicious codes, viruses and hackers. The main significance of a firewall is to stop dangerous traffic access and only allowing non-threatening traffic to pass through.

1.5.7 Virtual Private Networks (VPN):

An encrypted connection which connects a computer and a network over the internet is known as VPN (Virtual Private Network). It helps to secure transmission of sensitive data. It protects network from unwanted data on the traffic and allow users to operate remotely. VPN technology is usually used in corporate networks.

1.5.8 Wireless Security:

Wireless security mainly prevents unauthorized and malicious access to or from a wireless network. It is provided by wireless devices such as a wireless routeror switch that encrypts and protects all communication by default in wireless environment. Two common standards for ensuring wireless network security are Wired Equivalent Policy (WEP) and Wireless Protected Access (WPA).

1.6 Services provided by Network Security

Services which are provided by a network security are given below:

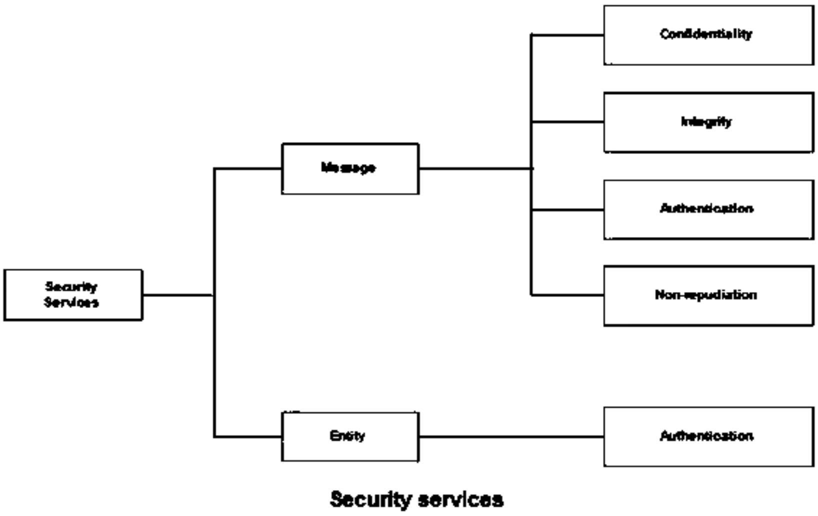
1. Message confidentiality

2. Message Integrity

3. Message Authentication

4. Message non-reproduction

5. Entity Authentication



(fig. 1.6)

1.6.1 Message confidentiality

- This indicates that the message that is sent over the network should be private, i.e. only the recipient in the network can access it.
- Priority is to send the message to the intended recipient only, and also to make ensure that contents should be read by him only;for tisthe message is encrypted to prevent any unauthorized access.

1.6.2 Message Integrity

- This indicates that the data or message should arrive at its destination unaltered and exactly where it was sent.
- During transmission, the data should not be altered maliciously or accidentally.
- A checksum is added to a message to guarantee its integrity.
- The purpose of an algorithm is to guarantee that neither the message nor the checksum can be altered.

1.6.3 Message Authentication

• First of all, the receiver confirmsof sender's identity i.e. Receiver checks whether actual sender is the same, who was supposed to send the message.

There are different methods to identify senders:

1. A common secret code is used so that both parties can confirm their identity while transferring and authenticating any message.

2. A Digital signature is sent to confirm authentication.

3. A digital certificate is issued by a recognized certification authority who verifies the authenticity.

1.6.4 Message non-reproduction

- It means that a sender must not be able to deny sending a message which was already sent.
- The receiver must prove the ownership that the sender sent same contents of the message.
- Authentication and integrity mechanisms are used for non-reproduction.

1.6.5 Entity Authentication

- The entity or user is verified before accessing any system resources that’s called entity authentication or user identification.

IAAA Standard:

- The assertion of a user's name or identity, such as an email address or user ID, is called identification.
- Authentication is a process of confirming user’s originality. This is donewith many layer passwords.
- Giving some permissions to user or not is called authorization. The user may be granted read, write, full control, etc., or they may not be authorized and have no permissions.
- Keeping track of what happened is accountability. User attempted or gained access is recorded in the log. Additionally, the user's actions may be recorded in the log.

1.7 Network Security Devices

1.7.1 Active Devices: The extra traffic is blocked by these security devices. Examples of such devices are firewalls, antivirus scanning devices and content filtering devices.

1.7.2 Passive Devices: The unwanted traffic is identified and reported by these devices. Example of these devices is intrusion detection systems.

1.7.3 Preventative Devices: The suspicious network activities and potential security threats are identified by scanning through these devices. Penetration testing devices and vulnerability assessment appliances are examples of such devices.

1.7.4 Unified Threat Management (UTM): All-in-one security devices are served by these devices. Firewalls, content filtering, web caching are few examples of these devices.

1.8 Check Your Progress

1. A network includes two or more computers that are connected or linked to ________________ resources.
2. WAN means ______________________and VPN means ___________________________
3. The example of WAN most commonly used is the ___________________.
4. A network of computer that widens across the internet a private network is called ________________________________.
5. Access Control is broken into IAAA – What's the full form of IAAA? ____.
6. QoS means ____.
7. Message Authentication is one of the services of _______________________________.
8. ______________________Network can be controlled by a single person, it means, an individual can do communication between the computer devices in work space which is centered.
9. A network larger than LAN (Local Area Network) but smaller than WAN (Wide Network Area) is called ____.
10. ___________________ is a security system network that checks or controls incoming and outgoing traffic of a network, on basis of security rules allow or disallowdata packets.

1.9 Summary

Two or more computers that are connected to each other to share resources (like hard drives, printers, and CDs), transfer files, or communicate electronically make up a network. Cables, telephone lines, radio waves, satellites, or infrared light beams connect computers in a network. An organization is a gathering of PC frameworks, framework servers, gadgets for systems administration connected together to share assets including a hard circle or printer or record server PCs. These cable and wireless media can be used to make connections.

Computer Networks:

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Virtual Private Network (VPN)

Computer Network Characteristics:

- Fault Tolerance
- Scalability
- Quality of Service(QoS)
- Security

About Network Security:

It is known as a methods used for precautions and to protect Computer network structure from leaking private data, misuse, failure, alteration, destruction and unauthorized access. It is a process to secure networks from security threats possibly; Network security allows only registered users to use networks, while on the other hand, it protects networks from malicious actors from misusing threats and exploits. As there is growth in the number of hackersand day to day they are getting upgraded, we definitely requiresecurity tools for network to prevent network from numbers of hackers who are growing and getting smarter daily.

Types of Network Security

- Physical Network Security
- Technical Network Security
- Administrative Network Security
- Access Control Security
- Application Security
- Firewalls Security
- Virtual Private Networks (VPN)
- Wireless Security

Services of Network Security

Services which are provided by a network security are given below:

1. Confidentiality of Message

2. Integrity of Message

3. Authentication of Message

4. Non-reproduction of Message

5. Authentication of Entity

Network Security Devices

- Active Devices
- Passive Devices
- Preventative Devices
- Unified Threat Management (UTM)

1.10 Keywords

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)

- Virtual Private Network (VPN)
- Network Security
- Firewalls Security
- Wireless Security
- Message confidentiality
- Message Integrity
- Message Authentication
- Message non-reproduction
- IAAA - Identification , Authentication, Authorization, Accountability
- Encryption
- Unified Threat Management (UTM)

1.11 Self Assessment Test

1. What is a computer network? Describe types and characteristics of network?
2. Differentiate between LAN, MAN and WAN.
3. What do you mean by network security? Explain types and services of network security.
4. Describe VPN (Virtual Private Network).
5. What are the types of network security devices?

1.12 Answers to Check Your Progress

1. share
2. Wireless Area Network, Virtual Private Network
3. Internet
4. VPN (Virtual Area Network)
5. Identification , Authentication, Authorization, Accountability
6. Quality of Service
7. Network Security
8. PAN (Personal Area Network)
9. MAN (Metropolitan Area Network)
10. Firewall

1.13 References

1. James Graham, Richard Howard, “Cyber Security Essentials”, CRC Press, Taylor & Francis Group, ISBN: 978-1-4398-5126-5, 2011.
2. Thomas A. Johnson, “Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, CRC Press, ISBN:978-1-4822-3923-2, 2015.
3. https://www.geeksforgeeks.org/network-security
4. https://www.tutorialspoint.com/

SUBJECT: Cyber Security	
COURSE CODE: MCA-34	**AUTHOR: DR. ABHISHEK KAJAL**
CHAPTER NO. 2	

Network Security Techniques

(Firewalls, Virtualization, DNS, Radio Frequency Identification)

INDEX **Page No.**

FIREWALL

VIRTUALIZATION

DNS

RADIO FREQUENCY IDENTIFICATION (RFID)

Lesson-2

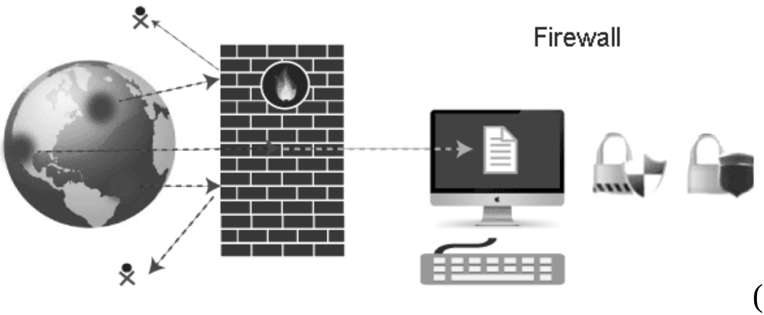
(Firewalls, Virtualization, DNS, Radio Frequency Identification)

FIREWALL

2.1 Introduction to FIREWALL

A firewall is a protocol-based network security system that controls and monitors network traffic. An internal trusted network is separated from Internet by a firewall. Both software and hardware versions of firewalls are available. Software-based firewalls are used by the majority of personal computers to shield data from Internet threats.

Firewalls are typically used in private networks or intranets to block and filter unauthorized Internet access. Using security measures, the firewall examines each message entering or leaving the intranet.



(fig. 2.1)

A firewall refers to any specificdevice type for security of network or anapplication or software whichdetects as well as controls or cleans traffic coming to andtraffic going out in network by using the predefined set of rules of security. This works like a checkpoint in between private internal networks and public externalnetworks.

A firewall allows non-threatening traffic and stops malicious or unwanted data traffic for protecting the computer system from viruses and other serious attacks. It is a cyber security tool which helps users to block malicious access from infected computers in internet.

2.2 Firewall History

For last 40 years, the most consistent and first important defense tool in security ofnetwork is firewalls. In the late 1980s, it was first used. In starting, these were created as filters of data packet. In 1993, there was the first inspection at state levelof firewall introduced by Gil Shwed from Check Point

Technologies. It was known as FireWall-1. In 2000, a company named Netscreen designed its appliances with built-in firewall.

During the mid-2010, simple Firewalls mostly used and implemented. Palo Alto Networks introduced improved firewalls named Next-Generation Firewalls. There were so many built-in functions and facilities in firewalls like Network Threat Prevention, Hybrid Cloud Support, Application and Control on the basis of Identity and Performance scalable etc. These are seemed to be at first place in defense tools of Network security.

2.3 Firewall as Hardware and Software

A firewall can be used at both levels - hardware and software. That system is best which uses both.

2.3.1 Broadband routers have Hardware firewalls inside. A minimum of four network ports are provided by most hardware firewalls to connect other computers. For business purpose, there are solutions of business networking firewall. Devices whichconnect computer network with a gateway are called hardware firewall. Modem and Broadband router are few examples of it.

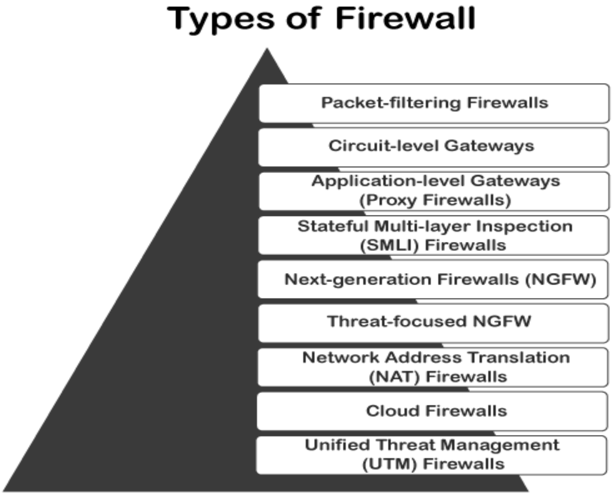
2.3.2 Usually your computers haveSoftware firewalls installed in it. It protects your computer system from internet threats. Simply, it is a program which is deployed on a computer which works with port numbers as well as with other application software.

2.4 Types of Firewall

We already discussed about firewalls which are of three types: firewall insoftware, firewall in hardware, or firewalls in both, which depends on structure of them. Everyfirewall type has the same purpose but different functionalities.

- A physical device that connects a gateway to a network of computer is called hardware firewall. A broadband router is an example of it that’s why sometimes it referred to as an Appliance Firewall.
- Where a computer system has deployed any simple program that operates by numbers of port and deployed other applications is called software firewall. This kind of firewall is also referred as Host Firewall.

Further, firewalls have many different types based on theirstructure, characteristics,functionalities and security level.


Types of Firewall
Packet-filtering Firewalls
Circuit-level Gateways
Application-level Gateways (Proxy Firewalls)
Stateful Multi-layer Inspection (SMLI) Firewalls
Next-generation Firewalls (NGFW)
Threat-focused NGFW
Network Address Translation (NAT) Firewalls
Cloud Firewalls
Unified Threat Management (UTM) Firewalls

(fig. 2.2)

- Packet-filtering Firewalls
- Next-generation Firewalls (NGFW)
- Cloud Firewalls
- Application-level Gateways (Proxy Firewalls)
- Circuit-level Gateways
- Stateful Multi-layer Inspection (SMLI) Firewalls
- Network Address Translation (NAT) Firewalls
- Unified Threat Management (UTM) Firewalls

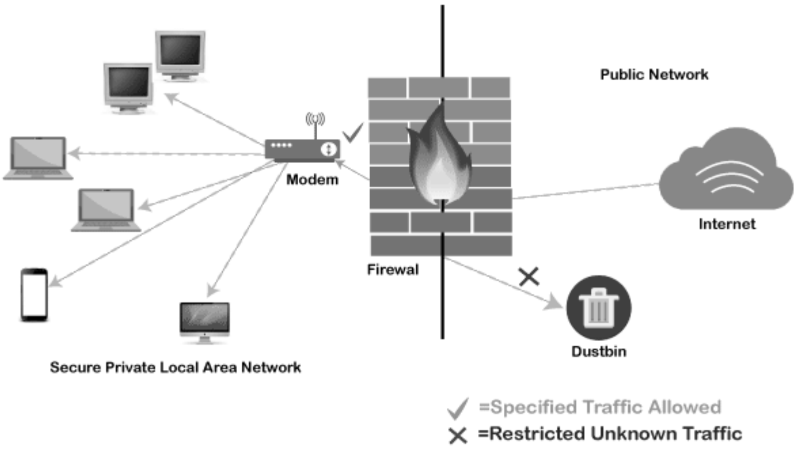
- **Packet-filtering Firewalls:**It is type of a program in management that filters and checks incoming packets in network traffic on basis of security rules already configured.
- **Next-generation Firewalls (NGFW):**This type of firewall is treated as combination of the features and functionalities of other firewalls as a security device. Surface-level packet inspection, include deep-packet inspection (DPI) and TCP handshake testing, etc. are few examples of it.

- **Cloud Firewalls:**FaaS (firewall-as-a-service) or a cloud firewall are another names for this term because it is designed using a cloud solution and can be stored on cloud online. Third-party vendors maintain and run Cloud firewalls on the Internet. It is also referred to proxy firewall.
- **Application-level Gateways (Proxy Firewalls):**These function at the layer of application to filter traffic coming insidein betweensystems of network and systems of traffic.
- **Circuit-level Gateways:** These firewalls functionin the OSI model at the session-level and also verify Transmission Control Protocol - TCP sessions as well as connections.
- **Stateful Multi-layer Inspection (SMLI) Firewalls:** SMLI firewalls storesthe status track of connections created by using both technologies which are inspection of packet and verification of TCP handshake.
- **Network Address Translation (NAT) Firewalls:** For accessing Internet traffic and to stop all unwanted or unauthorized connections NAT firewalls were introduced. These types of firewalls usually save us from attackers by hiding the IP addresses of our devices.
- **Unified Threat Management (UTM) Firewalls:** These firewalls use a stateful inspection firewall with intrusion prevention support anti-virus and. Many other services can be also added by these firewalls like cloud management, etc.

2.5 Functions of Firewall

Like a gatekeeper, Firewall monitors everythreatcoming to get access to operating system of our network and stops the traffic from non-recognized or unwanted sources. As a traffic controller, it works as a filter barrier between the system of private network of computer and other public internet networks. Therefore, a Firewall works as a security tool for our network and computer systems by controlling and monitoring traffic of network, stopping unwanted traffic incoming in network, and authenticating use for malicious things like hackers and malware by assessing network traffic.

A variety of functions is included in firewalls and facilities with predefined features and has become so powerful:


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✕ =Restricted Unknown Traffic

(fig. 2.3)

- Network Threat Prevention
- Access Validation
- Record and Report on Events
- Application and Control based on Identity
- Network Traffic Management and Control
- Performing Scalable
- Hybrid Cloud Support

2.6 Advantages of Firewall

Some essential advantages of firewall are:

1. Prevents Open Access: If a computer have a firewall, then it doesn’t allow open access to other networks.

2. Prevents Data Loss or Comprised Data: Firewall controls traffic and incoming or outgoing data on network. That’s why Cyber criminals can’t control over network easily and they can’t delete our data or access our personal information.

3. Avoids Network Crashes: Without firewall, our network can be accessed and shut down easily. It might take lots of time and money to make our network working again.

So firewall is very necessary tool for our network to keep it safe and secure from unwanted sources.

2.7 Limitations of Firewall

Firewalls are considered at first place when we talk about defense and security tools. It is very important to have firewalls in our systems, but beside that, firewalls have some limitations as well:

- Malicious websites cannot be stopped from users accessing by Firewalls and that makes it vulnerable for internal threats or attacks.
- Transmission of files infected with virus or software or application cannot be detected by a firewall.
- Firewalls cannot stop misuse of secret codes and passwords.
- If there are rules of security which are mis-configured,then firewall cannot safeguard the network.
- Risks of security in Non-technical system like social engineering cannot be protected by firewall.
- Internal network dialing to or from the network used by attackers with modems cannot be stopped or prevent by firewalls.
- Already infected systems cannot be protected by firewalls.

Therefore, we should always update all our Internet-enabled devices as well as windows operating systems, web browsers, applications and other software of security like anti-virus.

VIRTUALIZATION

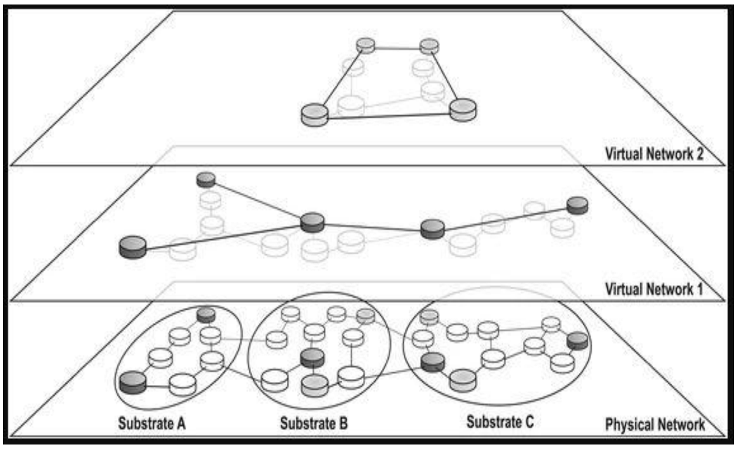
2.8 Introduction to Virtualization

The process of operating a device with multiple virtual instances on a single physical hardware system is called Virtualization. Security Virtualization process assures protection of virtualized hardware infrastructure and a dedicated security assistance within the cloud, along with customizable firewall.

A single physical infrastructure is used to create multiple virtual platforms by using virtualization technique, runs and allows heterogeneous architectures on the same hardware. Future Internet research organizations commonly use network and Industry virtualization.

2.9 Network Virtualization:

Sharing of resources from physical network devices like routers, switcheswithin various virtual networks is known as network virtualization.Network virtualization can be used in real-world at a large-scale.



(fig. 2.4)

VLAN (Virtual Local Area Network) and VPN (Virtual Private Network) have become the most common virtualization networks over the time. The following approaches describe network virtualization:

2.9.1 Protocol-based approaches: It consists of a network protocol that enables tagging or tunneling techniques for the distinction of virtual networks.

2.9.2 Machine virtualization-based approaches: It consists of groups of interconnected virtual machines to create virtual networks. To instantiate virtual routers and virtual links, Virtual Machine Monitors are used regardless of physical network topology.

2.9.3 Programmable networks: Virtual networks can be created using programmable routers. We can do it in network devices by decoupling the data plane and the control plane.

2.10 Virtualization Security

Software is deployed as abstraction of a layer to create over the hardware physical device in virtualization. Making partition into several virtual servers by a single physical server is the principle of virtualization.

By virtualization against various risks or attacks, we can enhance the level of protection.

Virtualization is of two types:

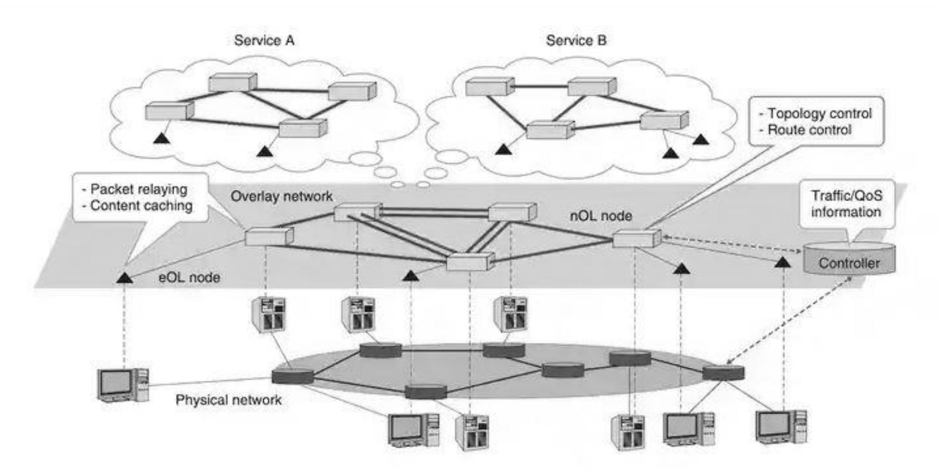
1. Full virtualization: This is most commonly used and known as Type 1.

2. Para virtualization: This is known as Type 2.

Type 1 runs on bare metal and Type 2 runs on top of an operating system.

There are many benefits of this, For example:

- Systems High availability
- The underlying hardware decoupling by operating system
- Between hosts movement of freedom
- Security



(fig. 2.5)

Multiple virtual networks can operate on an underlay network.

Virtualization techniques to improve security for enterprise system infrastructure:

Resourceslike memory, bandwidth, disk space or even machines may be used by virtualization to share - like if a project needs 10 servers to be connected. Various techniques are described below:

2.10.1 Containerization: Another name for this is OS-Level virtualization. In this, for each and every application spaces are separated, completely isolated and are created by the operating system.

2.10.2 Sandboxing: Separately, the programs executionand codes execution from unknown websites, vendors or parties is known as Sandboxing process. The isolation of the application is allowed by sandboxing to protect from the viruses, external malware or any threats.

2.10.3 Server Virtualization: It helps in maximization of resources and this technique is used in resources server for masking. Virtual chunks of several smaller physical servers andvirtual environment of own diverse for each is sub-divided by the admin.

2.10.4 Network Virtualization:A single virtual network is formed by combining Software and hardware network resources. Two basic types of virtualization in network are Isolation and segmentation.

- **Isolation:** Over the cloud end-to-end services allow several isolated virtual networks to have the co-existence.
- **Segmentation:** The traffic minimized, and providesthe performance boost by sub-dividing the network into sub-networks.

2.10.5 Desktop Virtualization: From any physical computer, the access to create, change or erase images is given to users in desktop virtualization. It is also used for the separation of the desktop environment.

2.10.6 Hypervisor Security: It is the process of ensuring the hypervisor, the software to enables virtualization, a secure throughout development and implementation of life cycle. The hypervisor is contained in host machine and used for enabling virtualization.

2.10.7 Virtual and Physical Switches: Virtual machines security by isolation and inspection control is provided by a virtual switch. It stops attacks of inter-switch link and allows for communication to network connectivity within the virtual network with applications and the physical network.

2.10.8 Infrastructure & Guest OS Security: Resources access restriction is facilitated by virtualized information infrastructureand due to visibility handling of information is easy and in proper way.

2.10.9 Server Isolation & Virtual Hard Disk (HD) Encryption: In server Isolation, a single machine can run multiple servers by using virtualization, at the same time isolating them from each other. It is very difficult to read data with technology of present day if the virtual HD is encrypted, even if the attacker stoles a copy of HD.

2.10.10 Availability and Disaster Recovery: The backup of data in the type of a big and special file can be done by use of virtualizations permission. Moderate failures required by reducing cost and time by the fast redeployment of Operating System and data restoration.

DNS

2.11 Introduction to DNS

The term DNS refers to"Domain Name System". A numerical connection between a host name and its network address is provided by this directory service.

DNS is necessary for the Internet to function. It can convert IP addresses into domain names using the DNS service. Users of the network give other hosts names that are easy to remember rather than IP addresses.

For example, consider the EduSoft FTP site, which has an IP address of 130.143.166.50 and can be accessed by typing ftp.EduSoft.com in the address bar. Since IP addresses are difficult to remember for many websites, using a domain name rather than an IP address is more reliable.

In other words we can say DNS is a naming database where Internet Protocol (IP) addresses are located and translated into human readable domain names. For instance, if any person willing to access Amazon website, she needn’t to type machine readable IP address192.0.2.44, but simply needs to type amazon.com in the address bar.

The client requests are taken by web server of domain name for most web addresses / Uniform Resource Locators (URLs).

2.12 DNS History

In the 1970s, a single file was created called "HOSTS.TXT" to store all hostnames and their corresponding numerical addresses and Elizabeth Feinlerin the Stanford Research Institute was preserved it. This got popular as ARPANET or Advanced Research Projects Agency Network.

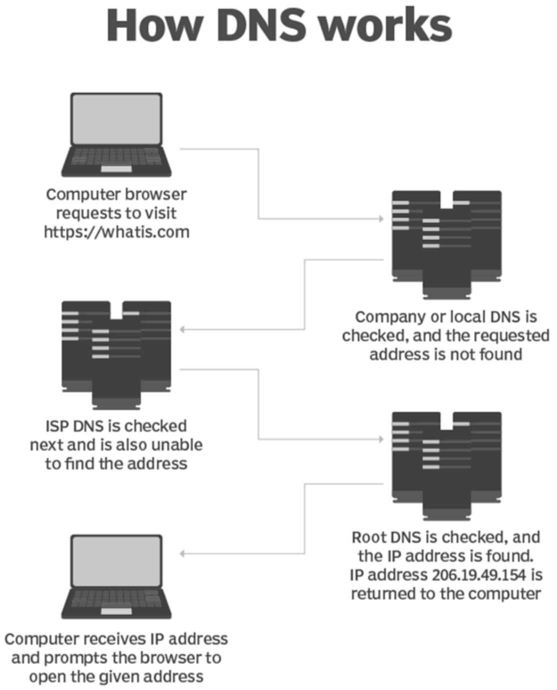
By the 1980s, this system was not so efficient to maintain. In 1983, in multiple servers and locations, one centralized file with every address was created to distribute by the domain name system.

In 1986, one of the original internet standards IETF listed DNS. Since then, DNS has been used commonly and spread all over the internet. Today, large companies of current information technology offer their own DNS hosting services, like Microsoft and Google.

2.13 DNS Working Process

The DNS responds to all of your domain's incoming and outgoing queries. When a server within the domain receives a request from outside the domain for information about a name or address, this produces an authoritative response.

ISP manages servers so when a request is received by a server fora name or address of its domain from outside that domain, another server receives itsrequest that is forwarded.


How DNS works
Computer browser requests to visit https://whatis.com
Company or local DNS is checked, and the requested address is not found
ISP DNS is checked next and is also unable to find the address
Root DNS is checked, and the IP address is found. IP address 206.19.49.154 is returned to the computer
Computer receives IP address and prompts the browser to open the given address

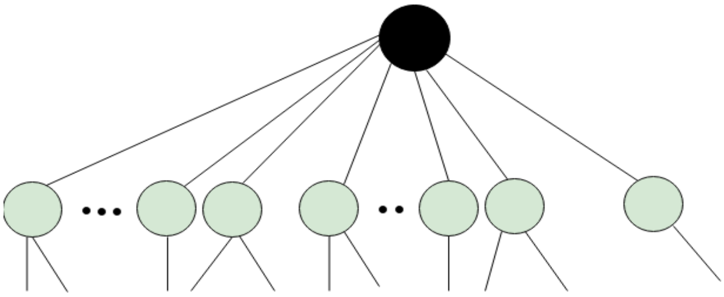
(fig. 2.6)

- A network communication protocol between clients and servers in which DNS clients send requests to servers and servers send responses to clients.
- When a client demand with a name is switched over completely to an IP address, it is alluded to as a forward DNS query, while demands with an IP address are alluded to as a converse DNS query.

- The names of all of the DNS hosts can be stored in a distributed database accessible on the Internet.
- The DNS resolver sends a request to the DNS server to obtain the hostname IP address whenever a client with a hostname sends a request via a web browser. If the IP address is not included by the DNS server associated with the hostname, the request is forwarded to another DNS server. If the resolver has received an IP address, it serves the request over Internet Protocol.

2.14 Types of Domain

DNS is referred as A TCP/IP protocol used on different-2 platforms. There are three different types of domain name space: Generic domains, Country domains, and Inverse domain.

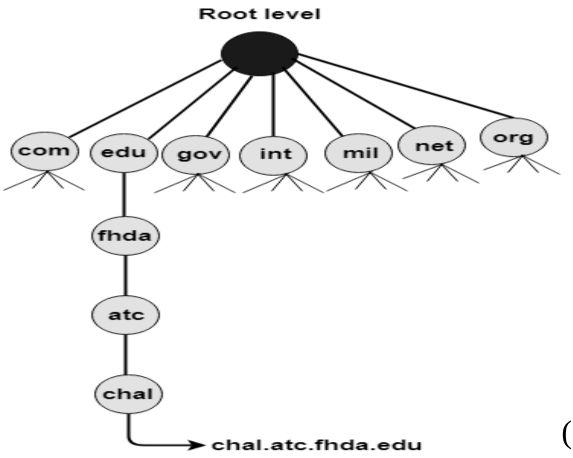


Generic Domains **Country Domains** **Inverse Domains**

(fig. 2.7)

2.14.1 Generic Domains

- According to their generic behavior, registered hosts are defined.
- The domain name is defined by each node in a tree, that’s an index to the DNS database.
- It uses three-character labels which describes the organization type.



(fig. 2.8)

Biz	-	Businesses or firms
Com	-	Commercial Organizations
Edu	-	Educational institutions
Gov	-	Government institutions
Info	-	Information service providers
Mil	-	Military groups
Net	-	Network Support centers
Org	-	Nonprofit Organizations
Pro	-	Professional individual Organizations

2.14.2 Country Domain: It is also same known as generic domain, but it uses two-character country abbreviations (e.g., in for India, us for the United States) in place of three character organizational abbreviations.

2.14.3 Inverse Domain: Mapping an address to a name is done by the inverse domain. The server contains the files of only authorized clients when the server has received a request from the client and whether the client is on the authorized list or not, it asks for mapping an address to the name and sends a query to the DNS server.

2.15 DNS structure

The domain name is contained within the web address of a URL. The components that make up a domain name are called labels. Reading the domain levels from right to left is required, and each part represents a subdivision.

High level spaces are composed after the period in the area name. We also have other top-level domains, such as.org.com, and .edu denotes a specific country or geographical location, such asus for the United States,.in for India, or .ca for Canada.

The label that comes before any dot on the right denotes the domain's subdomains on the left. This URL, for instance, contains www.techinfo.com, "techinfo.com," and a "www" subdomain is a part of techinfo.com subdomain.

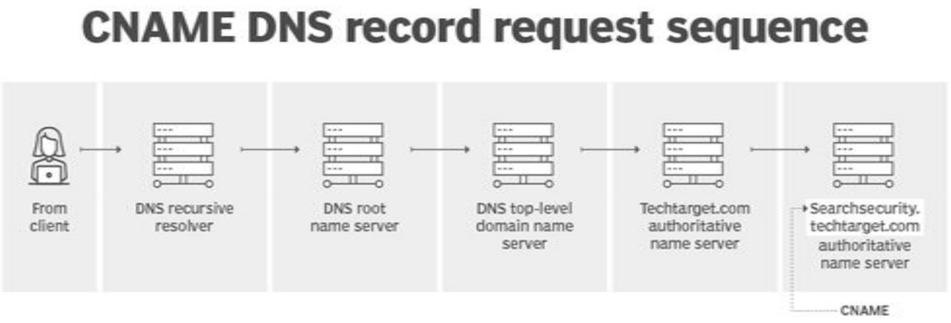
2.16 DNS Queries Types

In the DNS resolution at different points, there are many types of DNS queries discussed below:

- **Recursive DNS queries:**In this, DNS server communicates with many other DNS servers to look for an IP address and revert back it to the client. Recursive queries give the answer or an error in the end.
- **Iterative DNS queries:** These are used between the local DNS server (recursive resolver) and the root (the server non-local name), TLD (top level domain) and authoritative name servers. Iterative queries give an answer or a referral in the end.
- **Non-recursive queries**: In this, the recursive resolver gets the reply which is either the recursive server knows for skipping the root or caching on the recursive server and TLD (top level domain) servers and go directly to a particular authentic server. Non-recursive queries give only the answer.

2.17 Common DNS Records

A query seeks the information, basically called DNS records. Different information is required depending on the query of client or application.


CNAME DNS record request sequence
From client
DNS recursive resolver
DNS root name server
DNS top-level domain name server
Techtarget.com authoritative name server
Searchsecurity. techtarget.com authoritative name server
CNAME

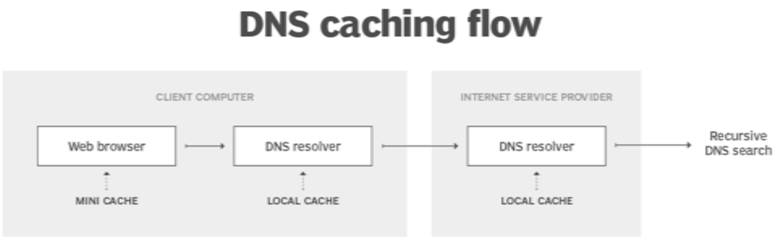
(fig. 2.9)

Each DNS records have their own purpose in representing that how to treat a query. There are many DNS records commonly used as follows:

- **A record:**'A' means address and it contains the IP address of domain. IPv4 addresses have 'A' records but not IPv6. There must be 'A' record in every website but some have more.
- **NS record:**It means Name Server record. Its responsibility is to contain all information related to a domain.
- **TXT record:** It means Text record. It allows administrator to enter text in DNS. These records contain ownership of domain, email security and tackle email spam to confirm.
- **CNAME record:** It means Canonical name records, these are used when there is an alias instead of an A record. In the URL It is an example searchsecurity.techtarget.com where techtarget.com is the CNAME query.

2.18 DNS Caching

When a DNS query is taken to get a reply, then DNS caching is used for reducing the time. Caching is used to enable DNS for storing previous replies to queries linked to clients and receives that similar information to them to make it fasterenough for next time.



(fig. 2.10)

- **Browser:**DNS data caching is by pre-stored default for a predefined amount of time for many browsers, like Google Chrome, Apple Safari and Mozilla Firefox.
- **Operating system (OS):** Cache DNS data and queries are handled by built-in DNS resolvers called stub resolvers before an external server receives them.
- **Recursive Resolver:** DNS recursive resolver can cache the answer to a DNS query. To return a response and to avoid some of the steps in processing of the DNS resolution, resolvers can have some necessary records.

2.19 DNS Common Attacks

For utilizing and targeting DNS servers there are a number of ways attackers can use. The most common are given below:

2.19.1 Denial of service (DoS): It isan attack in which by making a resource unavailable or by flooding the system with traffic, the attacker renders a computer useless to the user.

2.19.2 Distributed denial of service (DDoS): In order to span or spread malware and flood the victim's computer with unnecessary and overloading traffic, the attacker monitors and controls hundreds or thousands of amount of computers.

2.19.3 Fast flux: In order to hide the actual source of the attack, attackers use this technique to constantly change location-based data.

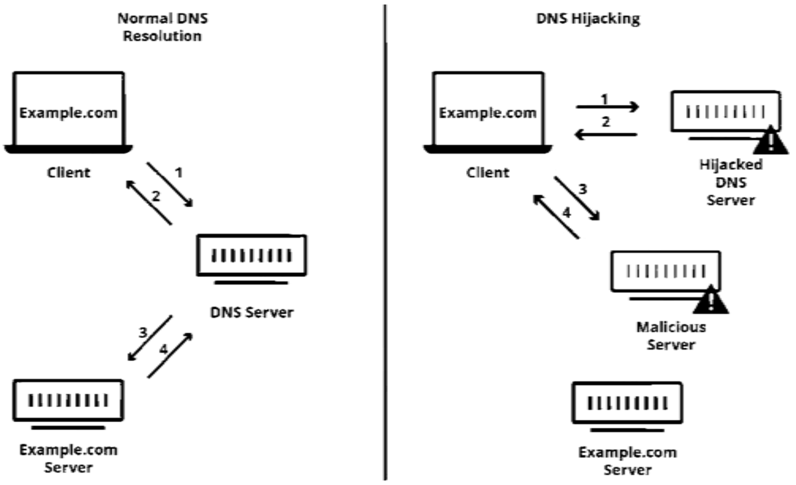
2.19.4 Reflected attacks: Attackers use victim's source address by sending thousands of queries by spoofing their own IP address. It's attempted to get all the answers of queries by the victims.

2.19.5 Reflective amplification DoS:A flux is triggered with an amplification effect when the size of the answer is larger than the query itself considerably. In this, the user's system's infrastructure is further overwhelmed by this attack.

2.19.6 DNS spoofing/poisoning of cache: It is a type of attack in which already used data of DNS is stored into cache of a DNS resolver, and for a domain an incorrect IP address is returned by the resolver.

2.19.7 DNS tunneling: Undetected by most firewalls, SSH, TCP, or HTTP can be utilized by attackers into DNS queries to bypass malware or stolen information, other protocols are used in this attack DNS queries and responses to pass through.

2.19.8 DNS hijacking: In DNS hijacking, a different domain name server is redirected with queries by the attacker. By using malware or with a DNS server's unauthorized modification, in either way attackers can do it.



(fig. 2.11)

2.19.9 NXDOMAIN attack:A DNS flood attack in which, attackers flood with requests to a DNS server and asks for non existing records to attempt denial-of-service for legitimate traffic.

2.19.10 Phantom domain attack: In this, the attacker creates many 'phantom' domain servers to respond request very slowly or not at all. The resolvers are flooded by these requests to the domains and the resolver tends to wait for responses, which leads system to make performance slow and service denial.

2.19.11 Random sub-domain attack: In this type of attack, several random sub-domains(nonexistent) gets DNS queries sent by the attackers in one legitimate site. Due to this side effect, the Internet Service Provider which is used by attacker can also getaffected, andcache of resolver which is recursive will also be filled with bad requests.

2.19.12 Domain lock-up attack: Attackers arrange these types of attacks by configuring up domains,and TCP connections are built by resolvers with other legitimate resolvers.

2.19.13 Botnet-based CPE attack: Customer Premise Equipment is hardware sold by service providers to customers for use, such as modems, routers, cable boxes, etc.). The attackers settle the CPEs and the devices become part of a botnet, which is used to execute random sub-domain attacks against domain or website.

2.20 DNS Firewall

A DNS firewall is a piece of software that can provide a DNS server with a variety of security and performance-related services. The authoritative nameservers of a website user and the recursive resolver or associated service are separated by a DNS firewall. The cache is being used to serve DNS responses; A DNS firewall is in charge of maintaining the operator's website or service.

A DNS firewall may offer some performance-related security features, such as faster DNS lookups and lower bandwidth costs for the DNS operator.

2.21 DNS as Security Tool

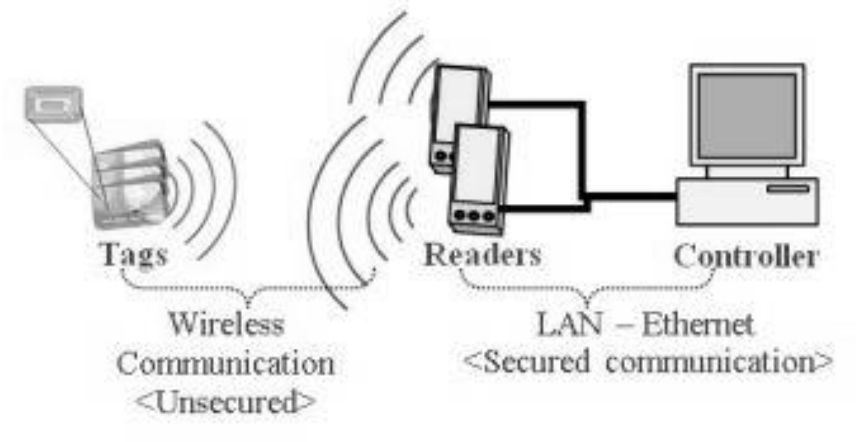
DNS resolvers are configured to provide security solutions and also for end users (people using and surfing the Internet). Content filtering is one of the features of DNS resolvers, which can block spam sites and malware and botnet protection feature, which blocks communication with known botnets. DNS resolvers, most of themare secured and free to use and by changing a single setting in their local router, a user might switch between these DNS services which are recursive. Cloudflare DNS an example in security whether it comes to DNS as security tool.

Radio Frequency Identification (RFID)

2.22 Introduction to Radio Frequency Identification (RFID)

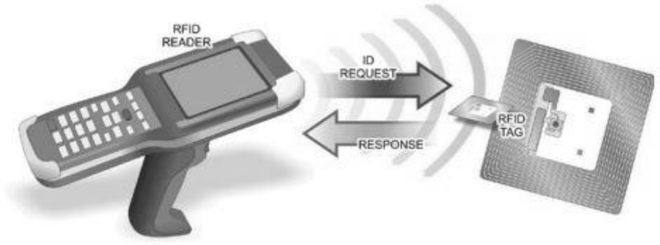
Radio waves to passively identify a tagged object that uses a technology called Radio Frequency Identification (RFID). Several commercial and industrial applications use this to track items out of a library to keep track of checked items with a chain of supply.

- It allows to track or matching of an item or individual by using passive wireless technology.
- The reader and the tag are the system's two most fundamental components. While the RFID tag uses radio waves to transmit identification and other information, the reader sends and receives signals from the tag.
- This technology was approved before the 1970s, but its use in global supply chain management, pet micro chipping, and other applications has made it much more common in recent years.


Tags
Readers
Controller
Wireless Communication <Unsecured>
LAN – Ethernet <Secured communication>

(fig. 2.12)

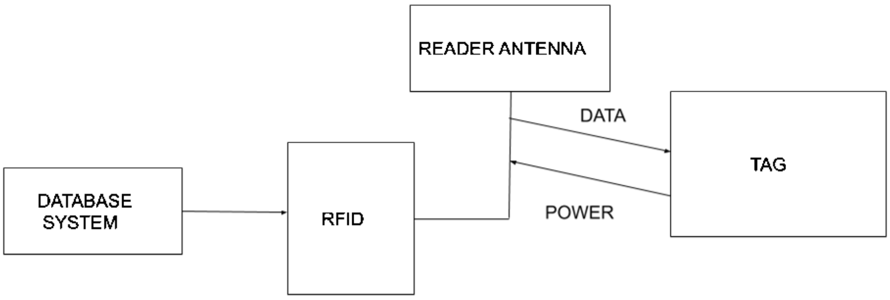
Radio-frequency identification (RFID) signals provide hands-free access-control tools that enhance bar code, magnetic stripe, and proximity reader technologies. An RFID system uses radio signals to identify unique objects by utilizing an RFID reader and tag.



(fig. 2.13)

A reader sends or receives radio frequency data from an RFID tag. Each tag stores the data that is sent to an embedded IC device. The specific information that is stored on the RFID is determined by the RFID system programmer, but it is typically identified by a serial number and a tag with information attached to it. The function of passive RFID tags can be carried out without the need for an external power source.

The web uses radio transmission to identify or track an object, Radio Frequency Identification (RFID) is used. In an RFID tag the data is encoded digitally that is read by reader. To read data from tags that the reader stores in database, a tag or label is used in this device in comparison to traditional QR codes and barcodes. It can read by either passive or active RFID.



(fig. 2.14)

2.23 RFID Types

Each type of RFID has different properties, mentioned as under:

2.23.1 UHF RHID (Ultra-High Frequency RFID): Shipping pallets and some driver's licenses use this type of RFID. Readers send signals in the 902-928 MHz band. Tags communicate to distances of several meters; the reader picks up these reflections. This way of operating is called backscatter.

2.23.2 HF RFID (High-Frequency RFID): It is operated at 13.56 MHz band and is used in your books, passport, credit cards, and noncontact payment systems. Range of HF RFID is short, typically a meter or less because the physical mechanism is based on induction instead of backscatter.

2.23.3 Low-frequency RFID systems: The Range varies from 30 KHz to 500 KHz, but typical frequency is 125 KHz. LF RFID has short transmission ranges, generally anywhere from a few inches to less than six feet.

2.23.4 Microwave RFID systems: The range in it is at 2.45 GHz and can be read from 30-plus feet away.

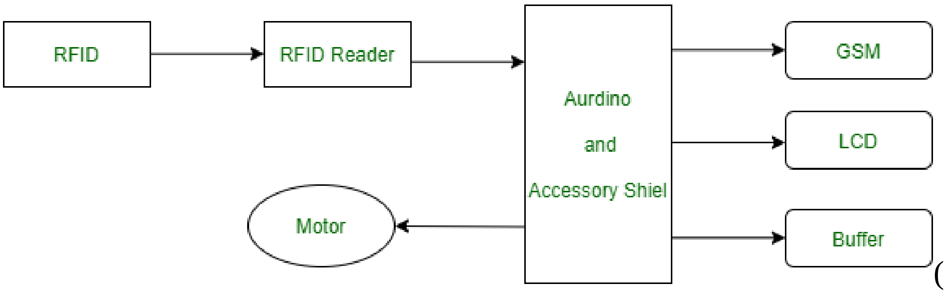
2.23.5 Passive RFID: In this device, a power supply is not attached to RF tags and passive RF tag stored their power. When it is produced from active antennas and the RF tag are used specific frequency like 125-134MHZ as low frequency, 13.56MHZ as a high frequency and 856MHZ to 960MHZ as ultra-high frequency.

2.23.6 Active RFID: In this device, a power supply is attached to RF tags that produce a signal and there is an antenna which receives the data.

2.24 Working of RFID

Automatic Identification and Data Capture technology refers to as AIDC to perform AIDC function generally, RFID uses radio waves. AIDC executes identification of object and data collection and data mapping.

To convert power into radio waves a device is used called antenna. Between reader and tag, it also makes a communication connection. RFID tag provides information to RFID readers for detecting the tag and read or writesthe tag data. This requires one transmitter and receiver unit, processor, storage, package and is needed in this.



(fig. 2.15)

2.25 Features of RFID

- A microcircuit and an antenna are two parts of an RFID tag.
- The outer environment effects as this tag acts as a shield against and is covered by protective material.
- There can be two states of nature active or passive for this tag but mainly passive RFID is popular and widely used.

2.26 Applications of RFID

- Cars, trucks and Tracking containers of ships and rail-road utilize this.
- Tracking of asset and equipment tracking also use it.
- Credit-card for accessing application utilizes it.
- Tap-and-go credit card payments.
- Personnel tracking use it.
- Used in restricted areas access controlling.
- ID badging uses it.
- Management of supply chain for improved visibility and distribution.

- Prevention of counterfeit (in the pharmaceutical industry).
- pet and livestock tracking
- inventory control and management
- cargo and supply chain logistics
- vehicle tracking
- access control in security situations
- customer service and loss control
- retail sales
- healthcare
- manufacturing

2.27 Advantages of RFID

- Without taking too much time, real-time information and data access is provided by it easily.
- The technology of the RFID system is sight nature of non-line type.
- The instructions are followed by RFID tags and a large amount of information stored.
- The Efficiency as well as production traceability is improved by it.
- In very short period of time in RFID Hundreds of numbers of tags are read.

2.28 Disadvantages of RFID

- When RFID devices are programmed, it takes longer.
- Even RFID is encrypted but is intercepted easily.
- To block the radio wave, two at least or more layers of ordinary foil of household are used in an RFID system.
- Anybody can access information about anything and that is a privacy concern about RFID devices.
- Due to battery, Active RFID can costlier.

2.29 RFID vs. Barcodes

For barcodes another option i.e. RFID is expanding fast in use. Barcode and RFID technologies have same ways for trackingstock, besides that there are some reasonable and important kind of differences between them.

RFID tags	Barcodes
Can recognize individual objects with no direct line of sight.	For scanning, direct line of sight needed
Can scan items from inches to feet away, which depends on type of reader and tag.	For scanning, need a closer proximity.
In real time, Updating of Data can be completed.	Read-only data can't be changed.
Need a source i. e. power.	There is no power source needed.
Read time is less than 100 milliseconds per tag.	Read time is half a second or more per tag.
Consists a sensor attached to an antenna, most of the time made into a plastic cover and barcodes is cheaper than this.	Printed on the outside of an object and more subject to wear.

2.30 RFID vs. NFC

NFC - Near-field communication exchanges data after enabling between devices by using range of short distance, wireless communication technology with high-frequency. A smart card interface combines in NFC and a single device with reader.

Radio frequency ID	Near-field communication
Uni-directional	Bi-directional
Range up to 100 m	Range less than 0.2 m
LF/HF/UHF/Microwave	13.56 MHz
Continuous sampling	No continuous sampling
Bit rate varies with frequency	Up to 424 Kbps
Power rate varies with frequency	<15 milliamperes

2.31 RFID Problems

There are two main issues in RFID:

- **Reader Interference:** Reader collision occurs when one RFID reader sends a signal to interfere with another reader. Anti-collision protocols can be used to make RFID tags to protect against reader collision. The transmission is sent to the correct reader.
- **Collision of a Tag:** When an RFID reader becomes confused by too many tags transmitting data simultaneously, tag collision occurs. A reader that prevents this issue by collecting data one tag at a time has been selected.

2.32 RFID standards

RFID technology has various kinds of specifications and important guidelines, but the main standards organizations are:

- International Organization for Standardization (ISO)
- Electronics Product Code Global Incorporated (EPCglobal)
- International Electro-technical Commission (IEC)

Each radio frequency has associated standards, including ISO 14223 and ISO/IEC 18000-2 for LF RFID, ISO 15693 and ISO/IEC 14443 for HF RFID, and ISO 18000-6C for UHF RFID.

2.33 Check Your Progress

1. ___________________ is a cyber security tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.
2. A physical device that connects a gateway and a network of computer is called _________________________________.
3. TCP means ____.
4. __________________________technique enables the creation of multiple virtual platforms over a single physical infrastructure, allowing heterogeneous architectures to run on the same hardware.
5. DNS stands for ___________________________________.
6. Types of domain are generic domain, _______________________ and Inverse domain.

7. DoS means ____and DDoS means ____.
8. ___________________________________ is a technology that uses radio waves to passively identify a tagged object.
9. RFID means ____.
10. ISO and IEC stands for ____ and ____

2.34 Summary

Firewalls:

A firewall is a protocol-based network security system that controls and monitors network traffic. An internal trusted network is separated from Internet by a firewall. Both software and hardware versions of firewalls are available. Software-based firewalls are used by the majority of personal computers to shield data from Internet threats.

- **Hardware Firewall**
- **Software Firewall**

Types of Firewall:

- Packet-filtering Firewalls
- Circuit-level Gateways
- Application-level Gateways (Proxy Firewalls)
- Stateful Multi-layer Inspection (SMLI) Firewalls
- Next-generation Firewalls (NGFW)
- Threat-focused NGFW
- Network Address Translation (NAT) Firewalls
- Cloud Firewalls
- Unified Threat Management (UTM) Firewalls

Functions of Firewall:

Like a gatekeeper, Firewall monitors every threat coming to get access to operating system of our network and stops the traffic from non-recognized or unwanted sources. As a traffic controller, it works as a filter barrier between the system of private network of computer and other public internet networks. Therefore, a Firewall works as a security tool for our network and computer systems by controlling and monitoring traffic of network, stopping unwanted traffic incoming in network, and authenticating use for malicious things like hackers and malware by assessing network traffic.

Advantages of Firewall:

- Prevents Open Access
- Prevents Data Loss or Comprised Data
- Avoids Network Crashes

Limitations of Firewall:

Firewalls are considered at first place when we talk about defense and security tools. It is very important to have firewalls in our systems but besides that, firewalls have some limitations

Virtualization:

The process of operating a device with multiple virtual instances on a single physical hardware system is called **Virtualization**. When virtualization process with procedure and policy secures and protects the virtualized hardware infrastructure, that's called security virtualization.

Network Virtualization:

Sharing of resources from physical network devices like routers, switches, etc. between various virtual networks. is known as virtualizing the network. A solitary actual foundation is utilized to permit the conjunction of different heterogeneous organizations. Virtual switches and connections are devoted actual gadgets of a virtual organization.

Virtualization Security:

- Containerization
- Sandboxing
- Server Virtualization
- Network Virtualization
- Virtualization of desktops
- Safety of the Hypervisor
- Physical and Virtual Switches

- Security for the guest OS and Infrastructure.
- Virtual Hard Disk (HD) Encryption and Server Isolation
- Accessibility and Catastrophe Recuperation

Virtualization of protection: The process of operating a device with multiple virtual instances on a single physical hardware system is called Virtualization. Security Virtualization process assures protection of virtualized hardware infrastructure and a dedicated security assistance within the cloud, along with customizable firewall.

DNS:

The term DNS refers to "Domain Name System". A numerical connection between a host name and its network address is provided by this directory service.

DNS is necessary for the Internet to function. It can convert IP addresses into domain names using the DNS service. Users of the network give other hosts names that are easy to remember rather than IP addresses..

Types of Domain:

DNS is referred as A TCP/IP protocol used on different-2 platforms. There are three different types of domain name space: Generic domains, Country domains, and Inverse domain.

- **Generic Domains**.
- **Country Domain**
- **Inverse Domain**

DNS structure:

The domain name is contained within the web address of a URL. The components that make up a domain name are called labels. Reading the domain levels from right to left is required, and each part represents a subdivision.

Types of DNS Queries:

In the DNS resolution at different points, there are many types of DNS queries discussed below:

- Recursive DNS queries
- Iterative DNS queries

- Nonrecursive queries

Common DNS Records:

A query seeks the information, basically called DNS records. Different information is required depending on the query of client or application.There are many DNS records commonly used as follows:

- **A record**
- **NS record**
- **TXT record**
- **CNAME record**

DNS Caching:

When a DNS query is taken to get a reply, then DNS caching is used for reducing the time. Caching is used to enable DNS for storing previous replies to queries linked to clients and receives that similar information to them to make it faster enough for next time.

Common Attacks Involving DNS:

- Denial of service (DoS)
- Distributed denial of service (DDoS)
- Fast flux
- Reflected attacks
- Reflective amplification DoS
- DNS spoofing/cache poisoning
- DNS tunneling
- DNS hijacking
- NXDOMAIN attack
- Phantom domain attack
- Random subdomain attack
- Domain lock-up attack

- Botnet-based CPE attack

A DNS firewall: A DNS firewall is a piece of software that can provide a DNS server with a variety of security and performance-related services. The authoritative name servers of a website user and the recursive resolver or associated service are separated by a DNS firewall. The cache is being used to serve DNS responses; A DNS firewall is in charge of maintaining the operator's website or service.

Radio Frequency Identification:

Radio waves to passively identify a tagged object that uses a technology called Radio Frequency Identification (RFID). Several commercial and industrial applications use this to track items out of a library to keep track of checked items with a chain of supply.

The passive wireless technology known as **Radio Frequency Identification (RFID)** enables the tracking or identification of an individual or object.

RFID Types:

- UHF RHID (Ultra-High Frequency RFID)
- HF RFID (High-Frequency RFID)
- *Low*-frequency RFID systems
- Microwave RFID systems
- Passive RFID
- Active RFID

Working of RFID:

Automatic Identification and Data Capture technology refers to as AIDC to perform AIDC function generally, RFID uses radio waves. AIDC executes identification of object and data collection and data mapping.

Features of RFID:

- A microcircuit and an antenna are two parts of an RFID tag.
- The outer environment effects as this tag acts as a shield against and is covered by protective material.

- There can be two states of nature active or passive for this tag but mainly passive RFID is popular and widely used.

Applications of RFID:

- Cars, trucks and Tracking containers of ships and rail-road utilize this.
- Tracking of asset and equipment tracking also use it.
- Credit-card for accessing application utilizes it.
- Tap-and-go credit card payments.
- Personnel tracking use it.
- Used in restricted areas access controlling.
- ID badging uses it.
- Management of supply chain for improved visibility and distribution.
- Prevention of counterfeit (in the pharmaceutical industry).
- pet and livestock tracking
- inventory control and management
- cargo and supply chain logistics
- vehicle tracking
- access control in security situations
- customer service and loss control
- retail sales
- healthcare
- manufacturing

Advantages of RFID

- Without taking too much time, real-time information and data access is provided by it easily.
- The technology of the RFID system is sight nature of non-line type.
- The instructions are followed by RFID tags and a large amount of information stored.
- The Efficiency as well as production traceability is improved by it.
- In very short time, reading of hundred of tagsin RFID.

Disadvantages of RFID

- When RFID devices are programmed, it takes longer.
- Even RFID is encrypted but is intercepted easily.
- To block the radio wave, two at least or more like three layers of ordinary foil of household are used in an RFID system.
- Anybody can access information about anything and that is a privacy concern about RFID devices.
- Due to battery, Active RFID can costlier.

2.35 Keywords

- PAN- Personal Area Network
- LAN- Local Area Network
- WAN- Wide Area Network
- CAN- Campus Area Network
- MAN- Metropolitan Area Network
- VPN- Virtual Private Network
- Encryption
- Network Segmentation
- UTM - Unified Threat Management Firewall
- WLAN- Wireless Local Area Network
- Packet-filtering Firewalls
- Circuit-level Gateways
- Proxy Firewalls - Application-level Gateways
- SMLI - Stateful Multi-layer Inspection Firewalls
- NGFW - Next-generation Firewalls
- Threat-focused NGFW
- NAT - Network Address Translation Firewalls
- Cloud Firewalls
- EPN- Enterprise Private Network
- DNS (Domain Name System)
- DNS (Domain Name Server)
- Virtualization
- Network Virtualization
- Sanboxing
- POLAN- Passive Optical Local Area Network
- Hypervisor Security
- Security Vitualization
- Domain
- Generic Domain
- HAN- Home Area Network
- Country Domain
- SAN- Storage Area Network
- Inverse Domain
- DNS Caching

- SAN- System Area Network
- DoS - Denial of Service
- DNS Spoofing / Cache poisoning
- DNS Tunneling
- DNS hijacking
- NX Domain Attack
- DNSSEC
- DNS Firewall
- DNS Query
- RFID - Radio Frequency Identification
- UHF RHID means Ultra-High Frequency RFID
- HF RFID means High-Frequency RFID
- Low-frequency RFID systems
- Microwave RFID systems
- Passive RFID
- Active RFID
- RFID vs. Barcodes
- RFID vs. NFC -Near Field Communication

2.36 Self Assessment Test

1. What is a firewall? Describe its functions and limitations.
2. Explain types of firewall.
3. What is virtualization and how it can improve security?
4. What do you mean by DNS? Describe its types and working of DNS.
5. Describe common attacks involving in DNS.
6. What is a Radio Frequency Identification (RFID). Write its applications, advantages and disadvantages.

2.37 Answers to Check Your Progress

1. Firewall
2. Hardware Firewall
3. Transmission Control Protocol
4. Virtualization Technique
5. Domain Name System
6. Country domain
7. Denial of service, Distributed denial of service
8. Radio Frequency Identification
9. Radio Frequency Identification
10. International Organization for Standardization & International Electro-technical Commission

2.38 References

1. James Graham, Richard Howard, “Cyber Security Essentials”, CRC Press, Taylor & Francis Group, ISBN: 978-1-4398-5126-5, 2011.
2. Thomas A. Johnson, “Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, CRC Press, ISBN:978-1-4822-3923-2, 2015.
3. https://www.geeksforgeeks.org/
4. https://www.tutorialspoint.com/
5. https://www.techtarget.com/

SUBJECT: Cyber Security	
COURSE CODE: MCA-34 CHAPTER NO. 3	AUTHOR: DR. ABHISHEK KAJAL

Cyber Attack Techniques

(Motivation, Tunneling Techniques, Fraud Techniques, Threat Infrastructure) Exploitation, Malicious code, Defense and Analysis Techniques.

INDEX **Page No.**

Introduction to Attacker Techniques and Motivations

TUNNELING TECHNIQUES

FRAUD TECHNIQUES

THREAT INFRASTRUCTURE

EXPLOITATION

MALICIOUS CODE

DEFENSE AND ANALYSIS TECHNIQUES

Lesson-3

(Attacker Techniques)

Introduction to Attacker Techniques and Motivations

3.1 About Network Attack

A network attack is executedif an unauthorized action is taken on a digital asset within an organizational network. Typically, malicious parties use or carry out these network attacks to alter, destroy, or steal private data. An assault on PC frameworks and organizations to harm information or upset tasks is known as digital assault or malevolent assault. In chapter we will learn aboutsome typical types of cyber attacks:

3.2 Types of Network Attacks

We frequently communicate using networknowadays, which results confidential data frequently exchanged between networks; consequently, modern businesses are entirely dependent on the Internet. Users' privacy settings are breached by malicious parties with data interception vulnerabilities, and internet-connected devices can be accessed remotely, causing network issues.

There are various types of organization assaults. Enterprises ensure that the highest cyber security standards, network security policies, and employee training are maintained in order to safeguard the organization's assets against increasingly sophisticated cyber threats.

- **Malware Attacks:** Malware, which is typically malicious software, is used by attackers in cyber attacks to carry out unauthorized activities on a victim's system. Ransomware, spyware, command-and-control, and other specific types of attacks are all spread by malicious software or viruses.
- **Ransomware Attacks:** Malware is used in this kind of attack to prevent a user or organization from accessing their computer's files. Since this is the quickest and cheapest way to gain access to an organization's files, cyber attackers use these attacks to collect large sums of money.
- **Phishing Attacks:** In this kind of attack, people receive emails or messages that pretend to look authentic, but actually fake communications designed to get users' personal

information. Phishing attacks are most effective when sent via email. Phishing primarily aims to install malware on the victim's system to steal sensitive data like login and credit card numbers.

- **Zero-day Attacks:** Day zero is also a name for this attack. It's possible that developers or vendors are unaware of this attack, which takes advantage of any vulnerability in software security that has the potential to be very serious. The software developer needs to take prompt action as soon as the vulnerability is discovered to address it and reduce the risk to the software user.
- **DDoS (Distributed Denial of Service) Attacks:** An attacker installs and spreads a botnet, also known as malware-compromised devices, which are connected to the Internet. Malicious attackers are increasingly targeting time-sensitive data, such as healthcare institution data, preventing access to crucial patient database records.
- **Network attacks known as Man-in-the-middle (MITM):** When malicious parties intercept traffic that is sent between the network and external data sources or within the network, this attack takes place. For most man-in-the-middle attacks, hackers use weak security protocols.
- **Unauthorized Access:** When malicious parties gain access to enterprise assets without first obtaining permission, this kind of attack takes place. This is brought on by inactive roles with administrator rights, unencrypted networks, internal threats that abuse role privileges, and weak password protection for accounts.
- **SQL Injection:** Uncontrolled user data input on the organizational network puts SQL injection attacks in jeopardy. The network is configured and user passwords can be accessed by attackers. Some examples of various SQL injections include probing a database for details on its version and structure, breaking logic at the application layer, and disrupting the logic sequence and function of the database.

3.3 Types of Cyber Attackers:

There are broadly two categories of Cyber Attackers: one that creates risks from the inside and other that creates threats to your business from the outside of your organization.

Insiders: Any person who has physical or remote access to your assets of organization and can be a cyber risk to your business. For example:

- Misplacing information by trusted employees accidentally.
- Remiss of policies and procedures by careless employees.
- Damage to your business by intention of disgruntled employees or ex-employees.
- Legitimate access to critical systems and information by malicious inside person.

There are many insider threats to cyber security that have access to your business-critical assets such as business partners, clients, suppliers and contractors.

Outsiders: There are many varieties of sources that can come as external cyber security threats as following:

- Criminal groups or organized criminals
- Whether malicious or not but professional hackers
- Script kiddies sometimes known as amateur hackers

You should fully be aware of motivations behind possible attacks in order to control cyber risk, regardless of its source, if cyber crime does happen to your business then you should also need to know where and how to report a cyber crime,.

3.4 Motivations behind Cyber Attacks

A potential target of cyber attack can be in every business, regardless of its size. Criminals may seek to exploit key assets that every business has (financial or otherwise). You can understand risks better by recognizing the common motives behind cyber attacks, you are facing, and understand how best to tackle them.

Most of the cyber attacks happen because criminals want your:

- Business' financial details
- Customers' financial details (e.g. credit card data)
- Customer databases
- Customers' or staff email addresses and login credentials
- Sensitive personal data

- It infrastructure
- Clients lists
- Intellectual property (e.g. trade secrets or product designs)
- It services (e.g. the ability to accept online payments)

Despite the fact that cyber attacks employ a variety of strategies and have a variety of goals, the following are the primary motivations that can be used to combat this issue:

- **To Make a Political or Social Point:** Attacks can be launched by hackers to criticize governments, politicians, society, big brand companies, and current events. When they disagree with their targets, they attack them, such as crashing their websites.
- **Radical Hackerism:** Most of the time, teenagers who are bored and want an adrenaline rush or a way to vent their anger or frustration at institutions (like school) or people they think are wrong form this group.
- **For Financial Gain:** An organization is most likely attacked for this reason. The purpose of nearly three-quarters of cyberattacks is primarily financial gain, such as data breaches, ransom demands, and the theft of money directly from financial accounts.
- **For Intellectual Challenge:** This group of hackers, like radical hackers, use network security to their advantage by launching cyberattacks that draw attention and respect from their peers.
- **Business Competition:**DDoS attacks are becoming a more common competitive business strategy. While some of these attacks aim to completely shut down online businesses for months, others aim to prevent competitors from participating in major events.
- **Cyber warfare:** Cyberwarfare is the conflict over the internet and the flow of information. Cyberattacks supported by the state are being used to silence critics of the government and internal opposition, as well as to undermine vital infrastructure, health, and financial services in hostile nations.
- **State Actors:** A nation-state provides support and funding for actors sponsored by the state. They exclusively engage in cybercrime for their nation's interests. They typically

commit additional espionage and exploitation, steal funds to fund, steal personally identifying information, and steal intellectual property.

- **Crackers:** Crackers are people who alter applications' programming so that they can use them for free. Some websites, like getintopc.com, use cracking software to make money from ads.
- **Pornography:** Some hackers use hacking to create pornography and blackmail and upload their videos to porn sites by hacking the phone and computer of users and obtaining their personal information. e.t.c.
- **Drugs:** Some people engage in illegal activities like the sale of drugs by utilizing their technical skills. Hackers use the darknet for this purpose because normal browsers cannot open darknet websites. They are using various browsers, including Tor and others.

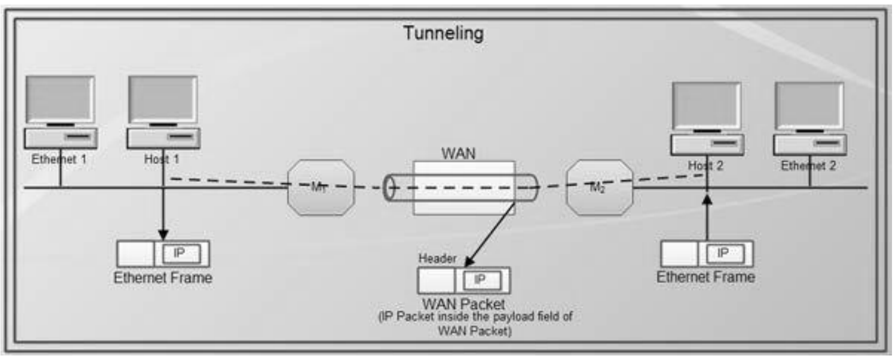
Tunneling Techniques

3.5 Tunneling

Tunneling is the process of connecting the same type of source and destination network through a different type of network, then that internetworking strategy is called Tunneling. Tunneling is often used by VPNs - Virtual private networks. Efficient and secure connections can also be configured by it between all networks, Itenables protocols of unsupported network for use and in some cases bypass firewalls is allowed by it to users.

In this normal but real physical world, there is a way for crossing boundaries or limitations and terrain that normally could not be crossed, that way is called tunneling. In similar way, tunnels are a strategy to transport any type of data beyond a network using some protocols in networking even though in network that is not compatible. By encapsulating packets, Tunneling is used to wrap packets inside of other packets. (Small pieces of data can be assembled again at the location of destination into a bigger file are called Packets)

For an example, let's say one Ethernet is connected to another Ethernet via WAN and IP packets are sent from Host 1 of Ethernet 1 to Host 2 of Ethernet 2.



(fig. 3.1)

- Host 1 creates a packet with the IP address of Host 2 in order to send an IP packet to Host 2. This packet is then inserted into an Ethernet frame. Ethernet is used to send this frame to the multi-protocol router M1.
- The IP packet is removed from this packet and placed in the payload field of the WAN network layer packet when it reaches the multiprotocol router MI.
- The multi-protocol router M2 receives this packet at the WAN network layer.
- When this packet reaches M2, the IP packet is extracted, placed in an Ethernet frame, and sent to Host 2.
- In the above procedure, IP packets simply move from one end of the tunnel to the other rather than traversing the WAN. Two Ethernet hosts, Host 1 and Host 2, do not have to deal with the WAN either.
- The M1 and M2 multi-protocol routers comprehend IP and WAN packets.
- The multi-protocol routers M1 & M2 understand about IP and WAN packets.

VPN Tunnel: A network which is public, shared and secure and has encrypted connection is a VPN. VPN packets reach their intended destination by using Tunneling process, which is typically a private network. So that creates a VPN Tunnel, when we use tunneling process in VPN.

3.6 Tunneling Technique as Protocol

Data can be safely transferred from one network to another using the protocol tunneling. The embodiment strategy permits burrowing for private organization correspondence to be sent over a public organization by means of the Web. When they are private data packets, encapsulation makes them appear normal on a public network, allowing them to go unnoticed. **Port forwarding** is another name for **tunneling**.

As the data travels through the tunnel, it is broken up into smaller pieces known as packets during tunneling. Bundles are encoded through the passage, and for this the exemplification interaction is utilized. The broadcast is accompanied by private network data and protocol details in public network broadcast units. The units make it possible to send public data over the Internet. Packets can more easily reach their intended destination thanks to encapsulation. At the final destination, de-encapsulation and decryption take place.

3.7 Tunneling Techniques

- Split Tunneling
- Generic Routing Encapsulation (GRE) Tunneling
- IP-in-IP Tunneling
- The Secure Shell (SSH) Tunneling
- PPTP- Point-to-Point Tunneling Protocol
- SSTP- Secure Socket Tunneling Protocol
- L2TP- Layer 2 Tunneling Protocol
- VXLAN- Virtual Extensible Local Area Network

3.7.1 Split Tunneling: Usually, all the network traffic goes through the VPN tunnel when a VPN is connected to the devices of a user. By split tunneling we transmitsome of the traffic to outside of the tunnel ofVPN. In fact, there are two networks simultaneously which are connected at the same time: one is public and other is private by using split tunneling in user devices.

3.7.2 Generic Routing Encapsulation (GRE): GRE combines data packets by using protocol of one routing inside another protocol packets. GRE set up a point-to-point direct connection over a network, to simplify connections between different-2 networks.

3.7.3 IP-in-IP: In this tunneling technique, IP packets are encapsulated inside IP packets of other VPN. IP-in-IP are not encoding packets and VPNs are not using. Its main work is to set up some network routes which are normally not available.

3.7.4 SSH (Secure Shell): This protocol creates a secure tunnel and configures encrypted connections between the server and the client. The Application Layer, which is the seventh layer of the OSI model, is where SSH operates.

3.7.5 Protocol for Point-to-Point Tunneling (PPTP): The PPTP network protocol is used to create VPN tunnels between public networks. PPTP servers are another name for Virtual Private Dialup Network (VPDN) servers. PPTP is preferred over other VPN protocols because it is fast and can be used on mobile devices.

3.7.6 Secure Socket Tunneling Protocol (SSTP): PPP traffic can be moved through an SSL/TLS channel using this kind of Virtual Private Network (VPN) tunnel. Transport-level security is given by SSL/TLS with key discussion, encryption, and traffic uprightness checking.

3.7.7 Protocol for Layer 2 Tunneling: Virtual Lines, otherwise called Layer 2 Burrowing Convention (L2TP) associations, lessen costs for far off clients by permitting corporate organization frameworks to deal with the IP addresses allotted to their distant clients. The access is effective.

3.7.8 VXLAN (Virtual Extensible Local Area Network): VXLAN is an encapsulation protocol that connects data centers. It uses tunneling to extend Layer 2 connections over an underlying Layer 3 network. The most widely used protocol in data centers is VXLAN, which makes it possible to use virtual networks and build an overlay network on top of the physical network.

Fraud Techniques

3.8 Internet Fraud / Cyber Fraud:

Internet fraudsters use certain online services and application software with access to the Internet in order to exploit the victim or commit fraud. **Internet fraud** refers to activities of hacking intended to defraud people for money, such as phishing, identity theft, and other forms of cybercrime that typically take place via email, a network, or the internet.

Online services are misused to target victims andevery year there is fraudulent activity worth for millions of dollars by targeting account of people by **Internet scams**. And there is increment growing day by day in figures and continued as there is much internet usage by people and cyber-criminals are using more complicated techniques.

To describe crimes committed by cyber attackers by the internet a term is called **Cyber fraud**. Intention of these crimes are dedicated to illegally obtain and control an individual's or business's sensitive private information for financial gain.

There are several different techniques that hackers use to steal your private information. To protect yourself from becoming a victim, one must know all possible threats and steps to stop these.

The common thing in all different types of cyber frauds is to use the technology to commit a crime. Few of those cyber frauds are discussed below:

3.9 Fraud Techniques (Types of Fraud)

3.9.1 Phishing: To trick individuals for getting sensitive private information (usernames, passwords and banking details) by pretending to be a trusted source of message links or email communication often is called a fraudulent attempt means Phishing.

3.9.2 Spear phishing: Targeting many specific users in an organization by email communication at same time is called Spear phishing.

3.9.3 Whaling / CEO fraud: Another type of fraud using phishing email targeted against senior executives of a company, or those with special access to information (called the big fish). Like spear-phishing, it targets special individuals within the institution.

3.9.4 Business email compromise (BEC): It is a type of phishing in that a criminal pretends to be a trusted company member and attempts to get company's any employee, worker, customer or vendor to disclose private information by phone call or email and asks to send money, by showing that that criminal is a trusted person.

3.9.5 Malware: To damage or disable computers, software is designed for this purpose that's called malware. Attackers can steal personal and private information, delete files, or even build backdoors by which cyber criminals can find a way to enter and control computer of victim.

3.9.6 Ransomware: It is also a type of malware by using that cyber criminals encrypt victim's files and demand ransom in exchange to decrypt them. Malicious links or email attachments can be used for this type of attack.

3.9.7 DDoS Attacks:DDoS attacks are used to flood a website, a server or network to disturb performance. These are few kinds of DDoS attacks:

- **Volumetric attacks**
- **Protocol attacks**
- **Application layer attacks**

3.9.8 Greeting Card Scams: This type of fraud happened on special occasions including birthday's celebration, Christmas and Easter, which are celebrated commonly by sending wishes and greetings by sending greeting cards to friends and family members by email. Hackers change these email greetings and attach malicious software within email of greeting card, when victim opens that greeting card actually the malicious software downloads and installs in the victim's computer to destroy computer or to take personal information.

3.9.9 Credit Card Scams: When attackers tries to steal information of your credit card or bank details to buy or purchase anything online using your credit card details then Credit card scam occurs. To get these details, internet fraudsters usually use the trick of being good and true by showing themselves as credit card or loan giving company.

3.9.10 Online Dating Scams: Most of the online dating applications and websites are fake and try to misguide people. To attract victims hackers create these kinds of apps making them sending money and by using new love interests technique they distribute personal data. For this they make fake girls/boys profiles and try to communicate with users, try to develop a relationship, takes their trust slowly, use a phony story, and ask for financial help from the user.

3.9.11 Lottery Fee Fraud: In this fraud, Scammers sends emails to victim by stating that they won a lottery prize. Then scammers tell recipients to pay a little fee to claim their prize. Lottery fee fraudsters make emails look like it sound believable. Fraudsters just try to show victim dreams of having a huge amount of money. But in real that lottery thing is totally fraud and no one gets any prize.

3.9.12 The Nigerian Prince: This fraudtakes the name of a rich Nigerian family or individual person who is willing to distribute their money in exchange for help to access their inheritance. It utilizes phishing tactics with an emotional backstory in emails to attract victims to have financial reward of promise. Scammers are also asks for little fee on the name for legal procedure and to make if official but in real all that is just fake and fraud.

3.9.13 Social engineering scams: In social engineering scams, Scammers use and play with emotions of the victim to make them trust scammers so that criminal can get their confidential information for money purpose, a criminal tries to gather information from their intended target through social media and general search queries.

3.9.14 Institutional payments fraud: Either outsider Attackers use computers remotely or the institution's own employees commit this fraud. External parties install malware on a financial institution's payment infrastructure to carry out these attacks.

3.9.15 Insider fraud: Insider implies a representative or project worker of an association or organization. Access to the company's systems and data can be used to commit fraud and attempt to leak information. These individuals are known as insider fraudsters.

3.9.16 Application fraud: This type of fraud is usually called identity fraud or identity theft, in which criminals take personal information of victim to apply for financial products such as a credit card, loan or bank account in the name of victim somehow;. It can be very difficult to detect such type of fraud when the individual whose identity has been used realizes they have unwarranted debts.

3.10 Solutions to Cyber Fraud

One of the most challenging aspects of the current financial ecosystem is reducing fraud. Cyber criminals constantly attempt to gain access to financial institutions' intricate and highly secure systems by manipulating and employing strategies. Threat actors are targeting payment systems, and it is critical to comprehend the various attack strategies and behaviors in order to safeguard your institutions from fraud.

Suggestions to be protected from cyber frauds:

- Always update software and devices to make ensure your systems have the most up-to-date security features and tools.
- Make sure antivirus and malware protection software is installed on your devices and updated.
- Always use unique passwords and update it time to time for all your accounts. Never use the same and predictable passwords such as birthdates or names.
- Enable two-factor authentication option to your passwords so that your account can’t get opened without your mobile security code.
- Always try to back up your data time to time on the cloud or external drive.

Threat Infrastructure

3.11 Threat Infrastructure

Threat Infrastructure refers to an event, when a cyberattack disrupts or manipulates the operation of financial, healthcare, military, water or electricity systems even for a few hours, it has a significant impact on the organization and has widespread and significant consequences.

Security has grown in importance as a result of the numerous threats to cyber networks that are faced by leaders of industrialized nations' governments, international economic organizations, and communities.

The energy sector, government operations, financial systems, transportation networks, national security, blood supplies, and health systems are all examples of critical infrastructures that are essential to our day-to-day lives and heavily rely on cyber networks. Cyber network threats are increasing in number, frequency, and impact on a daily basis. Digital assaults can be started by different individuals, for example, monetary entrepreneurs, activists or states and the goals of such goes after are similarly changed. Cyberattacks are motivated by monetary gain, malicious intent, gaining power, or making a political statement.

Cybersecurity is currently the most significant risk. Cyber security measures must be an essential and overarching part of every critical infrastructure operation. The primary objective is to stay informed about all business operations and ongoing fabric and prevent cyber security threats.

Various threat actors can create cyber threats, including:

- Hostile Nation-States
- Terrorist Groups
- Disgruntled Insiders
- Hacktivists
- Hackers
- Natural Disasters
- Corporate Spies and Organized Crime Organizations
- Accidental Actions of Authorized Users

Hackers and malicious applications that attempt to gain control of network infrastructure pose the greatest threat to its security. A network infrastructure consists of firewalls, routers, switches, servers, intrusion detection systems (IDS), load balancers, domain name systems (DNS), and storage systems—all of which are necessary for network communication. The majority of cybercriminals intend to use these devices as a point of entry for malicious software on a target network.

- **Gateway Risk:** To monitor, modify and deny traffic in and out of the network hackers attempt to get control and access to a gateway route. That's called gateway risk.
- **Infiltration Risk:** To monitor, modify and deny traffic between key hosts inside the network and utilize the trusted relationships between internal hosts to other hosts hacker can access more control from the internal routing and switching devices. That's called infiltration risk.

3.12 Network Infrastructure Security

Network infrastructure security is typically used in enterprise IT environments to safeguard the underlying networking infrastructure by implementing preventative and security measures to thwart unauthorized access to resources and data.

Some of these safeguards might be:

- **Access Control:** To prevent network access to the system by unauthorized users and devices.
- **Application Security:** To take precautions against potential flaws in both software and hardware.

- **Firewalls:** To use a firewall, which is a gate-keeping device, to allow or deny specific traffic access to the network.
- **Virtual Private Network (VPN):** To encrypt the connection between endpoints by establishing a safe communication channel via VPN over the Internet.
- **Behavioral Analytics:** These are apparatuses to recognize network action that goes amiss from typical naturally.
- **Wireless Security:** In many ways, hardwired networks are better than wireless networks, and new mobile apps and devices are making it easier for hackers to get into networks.
- **Web Defacement Detection:** Web defacement is a solution that enables to monitor website hack before it affects the organization.
- **Website Scanning:** To prevent websites from the bad actors, vulnerability scanning on your web applications is needed.
- **Port Scanning:** To prevent network infrastructure from the bad actors, scan all the ports presented in your network infrastructure and identify the vulnerabilities in them.
- **SSL Scanning:** Sometimes sensitive data is exposed to the bad actors that cause harm to the organization. To prevent from this, a scan of the organization’s SSL/TLS implementations is performed and is detected any type of vulnerability.

3.13 Working of Network Infrastructure Security

In network Infrastructure Security, it is necessary to upgrade yourself with ongoing processes and practices to ensure that the current infrastructure remains protected. Follow these steps to make sure that network infrastructure security is working properly:-

- Segment and segregate networks and functions
- Harden network devices
- Limit unnecessary lateral communications
- Perform out-of-band (OoB) network management
- Validate integrity of hardware and software
- Secure access to infrastructure devices

3.14 Advantages of Network Infrastructure Security

To provide several key benefits to an organization’s network, Network infrastructure security is to be implemented very well. Advantages of network infrastructure security are given below:-

- **Saves on costs by improving resource sharing:** Because of protection, resources on the network can be operated by multiple users without threat, and that reduces the cost of operations.
- **Site licenses sharing:** Site licenses would be cheaper than licensing every machine that is protected by security.
- **Improves productivity by file sharing:** Users can share files across the internal network securely.
- **Secures Internal communications:** By using security measures, internal email and chat systems will be secured from prying eyes.
- **Secures files and Compartmentalization:** As compared with using machines that multiple users share, user files and data are now protected from each other.
- **Protects Data:** To protect vital intellectual property, data back-up to local servers is simple and secure.

Exploitation

3.15 Introduction to Exploit

A program or piece of code known as an exploit is one that is made to find and take advantage of a security hole or vulnerability in a program or computer system, typically for malicious purposes like installing malware. Cybercriminals use exploits to send malware, but exploits are not malware themselves.

System intruders exploit a specific vulnerability, or computer exploit, through an attack on a computer system. If exploit is used as a verb, then it means to successfully carry out an attack of this kind.

An exploit, which can be an application or any other software code, such as application plug-ins or software libraries, can be used by an attacker to exploit a flaw in an operating system. The software developer can either download the patch or fix from the internet, or it can be automatically downloaded by the operating system or application that needs it and for; the system or application's users are accountable. A computer exploit for the user and a system security breach occur if the installation of a problem patch fails.

3.16 Types of Exploits

Exploits is usually classified into five categories:

1. **Hardware Exploit:** Lack of configuration management or firmware vulnerability, Poor encryption.
2. **Software Exploit:** Input validation errors (cross-site scripting (XSS), code injection), Memory safety violations (over-reads, buffer overflows, dangling pointers), format string attacks, directory traversal, HTTP header injection, email injection, HTTP response splitting, SQL injection, privilege-confusion bugs (cross-site request forgery, FTP bounce attack, click jacking), race conditions (time-of-check-to-time-of-use bugs, symlink races), user interface failures (blaming the victim, race conditions, warning fatigue), side channel attacks and timing attacks.
3. **Network Exploit:** Poor network security, unencrypted communication lines, lack of authentication or default passwords, man-in-the-middle attacks, typo squatting, domain hijacking.
4. **Personnel Exploit:** Lack of security awareness training, poor recruiting policy and process, poor adherence to information security policy, poor password management or common social engineering attacks fallen like phishing, whaling, pretexting, spear phishing, smishing, honey trapping, water holing.
5. **Physical site Exploit:** Lack of keycard access control, poor physical security, tailgating.

Each of these categories has vulnerabilities that can be categorized into two groups: known vulnerabilities and zero-day exploits:

- **Known vulnerabilities:** The vulnerabilities that are known by exploits security researchers and have documented are termed as known vulnerabilities. Often it is already patched but still remain a viable threat because of slow patching and that target known vulnerabilities.
- **Unknown vulnerabilities / Zero-day exploits:** Those vulnerabilities which are not been reported to the public or listed are termed as unknown vulnerabilities. In some cases the developer might not even know of the vulnerability and this means cybercriminals have found the exploit before developers have been able to issue a fix or a patch.

3.17 Causes of Exploits

These are some common causes of exploits to be occurred:

- **Remote exploits:** Without prior access to the vulnerable system, It works over a network and exploits the vulnerability remotely.
- **Local exploits:** It increases the privilege of the attacker granted by the security administrator and requires prior access to the vulnerable system.
- **Client exploits:** While accessing a client application, an exploit is sent against client applications that exist and consist of modified servers. Social engineering techniques like phishing or spear phishing to spread or adware are also required interaction from the user.

3.18 Detecting an Exploit Attack

There are not available any typical signs to get you detect of exploits that take advantage of security holes in software. Sometimes it gets too late until a user has known of system infection. That’s why users must always update their software and install security fixes or patches released by software’s developer.

A malware infection has common signs such as:

- Slow performance
- Loss of storage space
- Unexplained changed settings
- Frequent crashes or freezes
- Tons of pop-ups or ads where they shouldn’t be

3.19 Exploit Solutions

1. It is responsibility of developers to remove exploits by plugging vulnerabilities which caused exploits and resulting in failures. Developers write code and distribute patches fixes for all known exploits. To identify zero-day exploits, many cyber security watchdog organizations lookout and develops fixes can be solution to unknown exploits.
2. Numerous software companies offer patches for known flaws to address the vulnerability. Additionally, suspicious operations are detected, reported, and blocked by security software. The exploit is prevented from occurring and causing harm to the computer system as a result of this.
3. Endpoint, Detection, and Response (EDR) software and Threat Defense software are two types of software that businesses use to guard against exploits. In order to confirm the defense's effectiveness, a program of penetration testing is initiated.
4. If an exploit attack infects your machine with malicious cod then try immediately to remove the malware and then update your software including installing driver updates.

Malicious Code

3.20 Introduction to Malicious Code

- Malicious code is the language used to manipulate computer systems in order to produce dangerous behavior.
- Malicious code is any code in a software system or script that is designed to harm the system, breach security, or cause unwanted effects.
- An application's security is compromised by malicious code, which cannot be effectively controlled by conventional antivirus software on its own.
- Malicious code is referred to in system security terms such as attack scripts, Trojan horses, worms, viruses, backdoors, and malicious active content.
- Time bombs, deliberate data and information leakage, hardcoded cryptographic constants and credentials, rootkits, and anti-debugging techniques are all examples of malicious code.
- The most prevalent type of malicious code is computer viruses, which attach to another program and then spread when that program is run.

- Malicious code can take the form of Java Applets, pushed content, ActiveX controls, scripting languages, plug-ins, or other programming languages and is self-executing. Malicious code can expose modifying, destroying, or stealing data, performing tasks, obtaining or allowing unauthorized access to an organization's systems, private and sensitive data, and valuable information assets that the user did not intend.

3.21 Problems caused by Malicious Code

The following problems may occur due to malicious code:

- Data Corruption
- Credential theft and private info theft
- Distributed denial-of-Service (DDoS)
- Nuisance and inconvenience
- Ransom and extortion

3.22 Malicious Code Working Process

Malicious code can manipulate and control any programmed component of a computer system. Common targets of malicious codes are usually infrastructure of computer networking and mobile or desktop apps like smaller components, websites and online servers etc. By using a computer operation any device can be infected by malicious code, for example:

- o **IoT devices** — smart home devices, in-vehicle infotainment systems (IVI).
- o **Traditional computer devices** — desktops, laptops, mobile phones, tablets.
- o **Computer network devices** — modems, routers, servers.

A few distinct phases are created and used by malicious code. At each stage, it is needed to trigger interaction of human or actions of other computer to the next event and is required by malicious scripted code to be executed. But sometimes some of the codes can operate whole by themselves automatically. There are many steps most of the malicious code can follow to get spread:

1. Search and inspect for vulnerabilities.
2. To exploit vulnerabilities write program code.
3. Malicious code can enter and expose computer systems.

4. A related program or by itself own to execute the code.

When the malicious code is compatible in an exposed system then it executes. Once device or system is searched and found that is actually a target thenmalicious code connects to it, the attack may cause following problems:

- **Modify data**: weaken security, unpermitted encryption etc.
- **Corrupt or Delete data**: servers of website etc.
- **Obtaining data**: personal information, credentials details of account etc.
- **Restricted systems access:** email accounts, networks which are private etc.
- **Actions execution:** remote device control, duplicating itself, distribution of malicious code etc.

3.23 Ways Malicious Code Spreads

Malicious code can be infectedintothe systems byautomatically on its own, activity of secondary malicious code can be enabled, or can replicate and spread it. To do so locations are changing from one device to another as there must be the movement of original malicious code. To transmit data of malicious code any communications channel can be used to spread it. Some are given below:

- **Online networks** — file-sharing in P2P, intranets, internet websites which have public access etc.
- **Communications Social**— mobile messaging apps, SMS, push content, email etc.
- **Connecting Wireless** — Bluetooth etc.
- **Interfaces of Direct device** — USB etc.

3.24 Types of Malicious Code

It can lead to your private or special confidential data if entry points are found, malicious code can harm your computer in many ways. Here are some common types of malicious codes:

1. **Viruses:**malicious code that duplicates itself to execute that connects to programs that are macro-enabled is called a virus. These files can be spread bydownloading other file and documents, allow that virus to get into your system device.

2. **Worms:** These are self-spreading and self duplicating code such as viruses but do not need any other action. Once your device got infected with a computer worm, these worms can operate automatically by own itself without any help from a program run by user.
3. **Trojans:**Malicious code enters into files that carry it payloads and needed a user to execute and to use program or any file are called Trojans. These threats can have malicious code containing worms, viruses or any other code.
4. **Cross-site scripting (XSS):** The user's web browsing is interfered by Cross-site scripting by using the web applications containing malicious commandsusers use. This hacks confidential information, web content changes, or the user's device gets an infection.
5. **Backdoor attacks:** A cybercriminal can get and compromise system by coding application backdoor access. An attacker with a backdoor is allowed to become an advanced persistent threat (APT) to the computer system.

3.25 Prevent Malicious Code Attacks

Most malicious threats can be best defended by any antivirus software that has automatic updates, capabilities of removing malware and security of webbrowsing. However we cannot prevent malicious code just only with antivirus software on its own in most cases.

To removemalicious code infection and tocreate defense mechanism,antivirus is very essential. Here are some ways to protect you from malicious codes:

1. Avoid running unauthorized programs of JavaScript and related code,Install anti-scripting software.
2. Malicious code can be contained in email or attachment of files or in text message. So avoid any URL links or attachments contained in any message containing. Exercise caution against links and attachments.
3. In unwanted browser windows, avoid serving malicious content to safeguard scripts, activate your browser's popup blocker.
4. To run scripts and programs it is needed usually to allow with high-level permissions automatically**.** Avoid using admin-level accounts for daily use.

5. To protect irreplaceable files and documents utilize data backups to.
6. USB connections and a common threat is public Wi-Fi also that can be used to sendmalicious code by attackers.Beware of using any public data connection.
7. Ensure that by default your firewall is set and configured to block and white list any trusted or expected connections. To block unauthorized connections use a properly configured firewall.

Defense and Analysis Techniques

3.26 Cyber Defense

Due to the increasing size, frequency, and complexity of cyberattacks, cyber security is the most important and challenging component of any organization's cyber security strategy. Digital safeguard is the arrangement of security for data, frameworks and organizations from assaults by utilizing defensive cycles like organization recognition and reaction (NDR), firewalls, endpoint identification and reaction (EDR) to identify, dissect and report occurrences inside an organization. A task exists, being well-versed in the tactics, capabilities, and goals of attackers are essential for cyber security.

As the Internet has become a part of our daily lives, cyber defense requires rapid improvement and security, but the adversary has found a way through each new defense system. Commercial antivirus software, firewall technology, end-point detection, and network detection, for instance, aren't enough to stop the most recent viruses and attacks because malware like phishing schemes, polymorphic viruses, ransomware, and zero-day attacks are spreading quickly. However, we must consider our cyber defense strategies.

3.27 Cyber Defense Vs. Cyber Security

Cyber security and cyber defense are used interchangeably frequently. These are related, but distinct in many important ways.

- Cyber security is a set of solutions or strategies that an organization uses to avoid threats in cyberspace.

- A vital part of any network safety technique to incorporate digital wrongdoing, consistence and others is called digital danger counteraction. Solutions for cyber defense concentrate on actively repelling an attack.

Common cyber defense activities include the following:

- For your security infrastructure to install and maintain software and hardware.
- For analyzing, identifying, and repairing or patching system flaws within your network.
- For putting real-time solutions into place to stop zero-day attacks.
- For recovering from invasion missions that were partially or completely successful.

Cyber Defense Forensics Analyst role is to derive useful information in support of system/network vulnerability mitigation, to analyze digital evidence and investigate computer security incidents.

Person performing this role may unofficially or alternatively is called:

- Computer Forensic Analyst
- Digital Forensic Examiner
- Computer Network Defense (CND) Forensic Analyst
- Forensic Analyst (Cryptologic)
- Cyber Forensic Analyst
- Network Forensic Examiner
- Forensic Technician
- Host Forensic Examiner

From the perspective of cyber security defense, researchers have reached comprehensive conclusions. Traditional cyber defense technologies like authentication, access control, intrusion detection systems, information encryption, vulnerability scanning, and virus protection all offer some level of protection.

3.28 Defense Analysis Techniques

3.28.1 Moving Target Defense (MTD): This technique is anticipated by United States of America for cyber security. Main purpose of this technique is to puzzle the attackers withconstant and vibrant changes that are why it increases the cost, complication and rate of failure of the attack. MTD is a designed guideline but it’s not the particular defense method. MTD is to hire the resources, time or and space environment to present the attacker of the targeted system with a continuously altering attack locations, that creates more complexity for the attacker to attack system and decreases the time period of system weakness exposure. So, for improving the flexibility and lively defense facility of the targeted system, attackers hardlygrow effective attack methods in opposition to the target system in a limited period of time.

3.28.2 Mimic Defense (MD): The main purpose of Mimic Defense is arranging multiple unnecessary various functionalities for handling the same external request. On basis of negative feedback, to balance the security flaw in the existingpresent cyberspace, MD implements vibrant scheduling among multiple redundancies.

3.28.3 Defense in Cyber Security: Many researches and practices on the dynamic defense in security of cyber have created. Many dynamic defense strategies are available to bridge this gap. Defense in cyber security has an essential role in securing and protecting the organization from unwanted attacks and problems.

3.28.4 User and Entity Behavior Analytics (UEBA): It is the process of gathering insight into the network events that users generate every day. User and entity behavior analytics (UEBA), also refers to as user behavior analytics (UBA). It can be used to detect the use of compromised credentials, lateral movement, and other malicious behavior once collected and analyzed.

The academic and dynamic defenses of cyber security based on MTD and MD have grown steadily in recent years. Certain defense capabilities have been achieved and dynamic defense technologies for information systems have been proposed. The theoretical model of dynamic defense medium, the medium strategy of dynamic defense, dynamic defense similar to the theoretical system Indicator systems for measuring the effectiveness of, and the impact of, dynamic defense on system performance, etc. are just a few of the many problems and challenges that theoretical studies and engineering operations face today in their exploration of dynamic defense technologies. As a result, the development of the system of dynamic defense through extensive theoretical research has significant theoretical guidance and practical significance for the enhancement of active defense capability.

3.29 Methods to Detect and Analysis Cyber Threats:

There are several methods available that can help to detect any threat and defend in the defender's attack:-

- Leveraging threat intelligence
- Conducting threat hunts
- Setting intruder traps
- Analyzing user and attacker behavior analytics
- Threat detection requires a two-pronged approach

3.30 Techniques to Defend Against Cyber Attacks

In any organization, you can shield your enterprise from malware, viruses, ransom ware, hacking, social engineering, and the numerous other threat types on the web. There are also possible ways and different methods to avoid intrusion attempts and to secure away would-be dangers.

3.30.1 Proven Cyber Security Tactics: Indeed though cybercrime and malware are evolving in complexity, there are lots of ways to alleviate the damage they beget, or outright help attacks. The best part is a lot of methods used to stay safe from third- party attacks are easy to do and bring-effective.

3.30.2 Two Factor Authentication: Two-factor authentication (or 2FA) means user must provide a username and login with an additional code via a mobile or device only they have. This is the easiest and most robust ways to immediately improve cyber-defense. It means both their login and the personal device would need to be configured. It’s an important defense method.

3.30.3 Encryption: Encryption is difficult if an organization uses a public network. So organizations should not use a public network. Encryption secures information sent by your intranet and keeps it away from digital theft.

3.30.4 Keep Software Updated: Organizations should utilize the latest version of software and keep it updated. Zero-day exploits and attacks can corrupt old apps easily, which can steal information, because many damages penetrate networks. Antivirus software can update automatically, but other programs may not be updated automatically.

3.30.5 Identify Phishing Attempts: It is very important to train organization’s staff on suspicious messages to identify phishing attempts and social engineering;they often use legitimate-looking messages from friends or accounts trying to trick the user into giving away login info.

3.30.6 Set Staff Guidelines: Everyone in organization staff should be well known to cyber security practices. In fact, not everyone needs to be an IT expert, just having some basic knowledge with common cyber security trends, threats and good practices will be better for an organization for safety.

3.30.8 Diversify Network Infrastructure: Hackers get successful in stealing information because they access valuable info from simple intrusions. In other words, once they get into your system and access your information then general staff can’t access things as a manager can. In the same sense, business sections can be separated by VPN is essential.

3.30.9 Create a Risk Profile: This technique is mainly to guess any suspicious data that can be attacked. In other words, you have to look at your infrastructure and guess what hackers are looking for to take access/damage. By this, you can better invest resources in the proper areas by assuring efficient distribution of security policies.

3.30.10 Identify Staff Risk: Sometimes Internal threats means insiders, who are also as much concern as outsider ones. Make sure you take sharp looks on extensive background checks on staff to establish risk. It is also hard to judge to assume that a worker can harm your company; human error plays a role in upsetting a good security policy.

3.30.11 Beware of Hardware Theft: If any company makes use of mobile devices – such as a laptop or through a policy that have a way to remotely protect data. Then you should track devices. In the worst case, if a device is stolen then limit login capabilities. A third-party can take control or access to a lots of information based in one stolen device, so prepare for these types of attacks in advance.

3.31 Check Your Progress

1. ______________________________ is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key.
2. ___________________________ is an internetworking strategy that is used when source and destination networks of same type are connected through a network of different type.
3. _______________________________ is another name for Tunneling.
4. ___________________ is a tunneling protocol in which IP packets are encapsulated inside IP packets of other VPN
5. Full form of SSH Protocol _____________________________.
6. _______________ is gatekeeping technique that can allow or prevent specific traffic from entering or leaving the network.
7. A computer ___________________ is an attack on a computer system, particularly one that gets advantage of a specific weakness the system offers to intruders.
8. The most common form of malicious code is the ________________________.
9. __________________ are also self duplicating and self distributing code such as viruses but do not need any other action to do so.
10. XSS refers to _______________________________________.

3.32 Summary

About Network Attack

A network attack is executed if an unauthorized action is taken on a digital asset within an organizational network. Typically, malicious parties use or carry out these network attacks to alter, destroy, or steal private data. An assault on PC frameworks and organizations to harm information or upset tasks is known as digital assault or malevolent assault.

Types of Network Attacks

- Malware attacks
- Ransomware attacks

- Phishing attacks
- Zero-day attacks
- DDoS (distributed denial of service) attacks
- Man-in-the-middle (MITM) network attacks
- Unauthorized Access
- SQL Injection

Types of Cyber Attackers:

There are broadly two categories of Cyber Attackers: one that creates risks from the inside and other that creates threats to your business from the outside of your organization.

Insider attacker and Outsider attackers

Motivations behind Cyber Attacks

A potential target of cyber attack can be in every business, regardless of its size. Criminals may seek to exploit key assets that every business has (financial or otherwise). You can understand risks better by recognizing the common motives behind cyber attacks, you are facing, and understand how best to tackle them.

- To Make A Political Or Social Point
- Radical Hackerism
- For Financial Gain
- For Intellectual Challenge
- Business Competition
- Cyberwarfare
- State Actors
- Crackers
- Pornography
- Drugs

Tunneling

Tunneling is the process of connecting the same type of source and destination network through a different type of network, then that internetworking strategy is called Tunneling. Tunneling is often used by VPNs - Virtual private networks. Efficient and secure connections can also be configured by it between all networks, It enables protocols of unsupported network for use and in some cases bypass firewalls is allowed by it to users. **Port forwarding** is another name for **Tunneling**.

Tunneling Techniques

- Split Tunneling
- Generic Routing Encapsulation (GRE) Tunneling
- IP-in-IP Tunneling
- The Secure Shell (SSH) Tunneling
- PPTP - Point-to-Point Tunneling Protocol
- SSTP- Secure Socket Tunneling Protocol
- L2TP- Layer 2 Tunneling Protocol
- VXLAN- Virtual Extensible Local Area Network

Internet Fraud / Cyber Fraud

Internet fraudsters use certain online services and application software with access to the Internet in order to exploit the victim or commit fraud. Internet fraud refers to activities of hacking intended to defraud people for money, such as phishing, identity theft, and other forms of cybercrime that typically take place via email, a network, or the internet.

Fraud Techniques (Types of Fraud)

- Phishing
- Spear
- phishing
- Whaling / CEO fraud
- Business email compromise (BEC):
- Malware
- Ransomware
- Attacks
- DDoS

        - Volumetric attacks
        - Protocol attacks
        - Application layer attacks
    - Greeting Card Scams
    - Credit Card Scams
    - Online Dating Scams
    - Lottery Fee Fraud
    - The Nigerian Prince
    - Social engineering
    - Institutional payments fraud
    - Insider fraud
    - Application fraud

Solutions to Cyber Fraud

- Always update software and devices to make ensure your systems have the most up-to-date security features and tools.
- Make sure antivirus and malware protection software is installed on your devices and updated.
- Always use unique passwords and update it time to time for all your accounts. Never use the same and predictable passwords such as birthdates or names.
- Enable two-factor authentication option to your passwords so that your account can’t get opened without your mobile security code.
- Always try to back up your data time to time on the cloud or external drive.

Threat Infrastructure

Threat Infrastructure refers to an event, when a cyber attack disrupts or manipulates the operation of financial, healthcare, military, water or electricity systems even for a few hours, it has a significant impact on the organization and has widespread and significant consequences.

Security has grown in importance as a result of the numerous threats to cyber networks that are faced by leaders of industrialized nations' governments, international economic organizations, and communities.

The energy sector, government operations, financial systems, transportation networks, national security, blood supplies, and health systems are all examples of critical infrastructures that are essential to our day-to-day lives and heavily rely on cyber networks.

Cyber threats come from numerous threat actors, including

- Hostile Nation-States
- Terrorist Groups
- Disgruntled Insiders
- Hacktivists
- Hackers
- Natural Disasters
- Corporate Spies and Organized Crime Organizations
- Accidental Actions of Authorized Users

Network Infrastructure Security

These security measures can include:

- Access Control
- Application Security
- Firewalls
- Virtual Private Networks (VPN)
- Behavioral Analytics
- Wireless Security
- Web Defacement Detection
- Website Scanning
- Port Scanning
- SSL Scanning

Advantages of Network Infrastructure Security

- Saves on costs by improving resource sharing
- Site licenses sharing
- Improves productivity by file sharing

- Secures Internal communications
- Secures files and Compartmentalization
- Protects Data

Introduction to Exploit

A program or piece of code known as an exploit is one that is made to find and take advantage of a security hole or vulnerability in a program or computer system, typically for malicious purposes like installing malware. Cybercriminals use exploits to send malware, but exploits are not malware themselves.

Types of Exploits

- Hardware Exploit
- Software Exploit
- Network Exploit
- Personnel Exploit
- Physical site Exploit

Causes of Exploits

- Remote exploits
- Local exploits
- Client exploits

Detecting an exploit attack

Common signs of a malware infection, such as:

- Slow performance
- Loss of storage space
- Unexplained changed settings
- Frequent crashes or freezes
- Tons of pop-ups or ads where they shouldn’t be

Introduction to Malicious Code

- Malicious code is the language used to manipulate computer systems in order to produce dangerous behavior.

- Malicious code is any code in a software system or script that is designed to harm the system, breach security, or cause unwanted effects.
- An application's security is compromised by malicious code, which cannot be effectively controlled by conventional antivirus software on its own.

Problems caused by Malicious Code

- Data Corruption
- Credential theft and private info theft
- Distributed denial-of-Service (DDoS)
- Nuisance and inconvenience
- Ransom and extortion

Ways malicious code spread?

- **Online networks** — file-sharing in P2P, intranets, internet websites which have public access etc.
- **Communications Social** — mobile messaging apps, SMS, push content, email etc.
- **Connecting Wireless** — Bluetooth etc.
- **Interfaces of Direct device** — USB etc.

Types of Malicious Code

- Viruses
- Worms
- Trojans
- Cross-site scripting (XSS):
- Backdoor attacks

Prevent malicious code attacks

- Install anti-scripting software
- Exercise caution against links and attachments
- Activate your browser’s popup blocker
- Avoid using admin-level accounts for daily use
- Utilize data backups to protect irreplaceable files and documents

- Be wary of using any public data connection
- Use a properly configured firewall to block unauthorized connections

Cyber Defense

Due to the increasing size, frequency, and complexity of cyber attacks, cyber security is the most important and challenging component of any organization's cyber security strategy. Digital safeguard is the arrangement of security for data, frameworks and organizations from assaults by utilizing defensive cycles like organization recognition and reaction (NDR), firewalls, endpoint identification and reaction (EDR) to identify, dissect and report occurrences inside an organization. A task exists, being well-versed in the tactics, capabilities, and goals of attackers are essential for cyber security.

Cyber Defense Vs. Cyber Security

Cyber security and cyber defense are used interchangeably frequently. These are related, but distinct in many important ways.

- Cyber security is a set of solutions or strategies that an organization uses to avoid threats in cyberspace.
- A vital part of any network safety technique to incorporate digital wrongdoing, consistence and others is called digital danger counteraction. Solutions for cyber defense concentrate on actively repelling an attack.

Typical methods of cyber defense include:

- For your security infrastructure to install and maintain software and hardware.
- For analyzing, identifying, and repairing or patching system flaws within your network.
- For putting real-time solutions into place to stop zero-day attacks.
- For recovering from invasion missions that were partially or completely successful

Cyber Defense Forensics Analyst role is to derive useful information in support of system/network vulnerability mitigation, to analyze digital evidence and investigate computer security incidents.

Person performing this role may unofficially or alternatively is called:

- Computer Forensic Analyst

- Digital Forensic Examiner
- Computer Network Defense (CND) Forensic Analyst
- Forensic Analyst (Cryptologic)
- Cyber Forensic Analyst
- Network Forensic Examiner
- Forensic Technician
- Host Forensic Examiner

Defense Analysis Techniques

- Moving Target Defense (MTD)
- Mimic Defense (MD).
- Defense in Cyber Security
- Entity Behavior Analytics (UEBA)

Methods to Detect and Analysis Cyber Threats:

- Leveraging threat intelligence
- Conducting threat hunts
- Setting intruder traps
- Analyzing user and attacker behavior analytics
- Threat detection requires a two-pronged approach

Techniques to Defend Against Cyber Attacks

- Proven Cyber Security Tactics
- Two Factor Authentication
- Encryption
- Keep Software Updated
- Identify Phishing Attempts
- Set Staff Guidelines
- Diversify Network Infrastructure
- Identify Staff Risk
- Beware of Hardware Theft

3.33 Keywords

- Network Attacks
- Cyber Attackers
- Tunneling Technique / Protocol
- Generic Routing Encapsulation (GRE)
- Virtual Extensible Local Area Network (VXLAN)
- Secure Socket Tunneling Protocol (SSTP)
- Point-to-Point Tunneling Protocol (PPTP)
- The Secure Shell (SSH)
- IP-in-IP
- Split Tunneling
- Moving Target Defense (MTD)
- Mimic Defense (MD)
- User and Entity Behavior Analytics (UEBA)
- Two Factor Authentication
- Layer 2 Tunneling Protocol
- Phishing
- Whaling / CEO fraud
- Malware
- Ransomware
- DDoS Attacks
- Social engineering
- Online Dating Scams
- The Nigerian Prince
- Lottery Fee Fraud
- Authorised push payments fraud
- Threat Infrastructure
- Malicious Code

3.34Self Assessment Test

1. What is a Network attack? Describe different types of network attacks?
2. Who are cyber attackers and what are their motivations to do cyber attacks?
3. What is a tunneling technique and its protocols?
4. Explain Fraud techniques and Solutions to Cyber Fraud.
5. Describe Threat Infrastructure and Exploitation
6. What are types of malicious code and how to protect against malicious code attacks?
7. Describe defense and analysis techniques.

3.35 Answers to Check Your Progress

1. Ransom
2. Tunneling
3. Port Forwarding
4. IP-in-IP
5. Secure Shell Protocol
6. Firewall
7. Exploit
8. Computer Virus
9. Worms
10. Cross-Site Scripting

3.36 References

1. James Graham, Richard Howard, “Cyber Security Essentials”, CRC Press, Taylor & Francis Group, ISBN: 978-1-4398-5126-5, 2011.
2. Thomas A. Johnson, “Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, CRC Press, ISBN:978-1-4822-3923-2, 2015.
3. https://cyberdefenses.com/
4. https://www.sciencedirect.com/science/article/pii/S235286482100047X
5. https://www.ironnet.com/topics/what-is-cyber-defense

SUBJECT: Cyber Security	
COURSE CODE: MCA-34 CHAPTER NO. 4	AUTHOR: DR. ABHISHEK KAJAL

Ethics in Cyber Security

Privacy, Intellectual property in the cyberspace, Professional ethics, Freedom of speech, Fair user and Ethical Hacking

INDEX **Page No.**

ETHICS IN CYBER SECURITY

PRIVACY

INTELLECTUAL PROPERTY IN CYBERSPACE

PROFESSIONAL ETHICS

FREEDOM OF SPEECH

FAIR USE AND ETHICAL HACKING

Ethics in Cyber Security

Lesson-4

(Privacy, Intellectual property in the cyberspace, Professional ethics, Freedom of speech, Fair user and ethical hacking)

4.1 Introduction to Ethics in Cyber Security:

Walter Manner coined the term "computer ethics" in the middle of the 1970s. He also advocated teaching computer ethics in computer science. Ethics can be defined as a person's moral code of conduct. In computer security, cyber-ethics is what differentiates security personnel from attackers; It defines the capacity to adhere to ethical principles at work and shares knowledge of right and wrong.

Cyber ethics, which examines ethical, legal, and social issues at a common point between computer/information and communication technologies, is a branch of applied ethics. Cyber ethics is sometimes referred to as information ethics, computer ethics, and Internet ethics. Because of its narrow scope, internet ethics is unable to address the majority of cyber-related ethical issues that are unrelated to the internet or computer networks. Cyber ethics can easily overlook a plethora of pertinent issues that fall under it, regardless of whether it affects ethical issues like computer professionals or computers. However, information ethics extends far beyond the scope of cyber technology.

4.2 Four Ethical Issues of the Information Age

Not any much people are engaged with any task as much employed in the modern world to collect, manage, and distribute information. The computers in the world are connected in a variety of ways, including devices that connect millions of computers and handle massive amounts of information, millions of miles of optical fiber, wire, wireless, or air wave links.

In this era of information, we face many unique problems and challenges. Sometimes it stops by the nature of information itself. However, in many ways, intellectual capital is vulnerable.

In the information age, there is an important social bond between the people that have responsibilities to deal with threats to human dignity. There are many different types of the ethical issues, however, it is enough to focus on just these four. **These four ethical issues can be defined by an acronym -- PAPA**.

- **Privacy:** It means, under what conditions and with what safeguards, what information about anyone or any association must a person reveal to others? People can keep things to only them and not be forced to reveal to others?
- **Accuracy:** Who is responsible for accuracy of information, the authenticity and fidelity? Similarly, who have to give accountability reasons for errors in information and how can the injured party means the intellectual property will be build whole again?
- **Property:** Who is the real owner of information? What is to be done or fair prices to exchange it? Who is the owner of the channels, like the airways especially, by which information is to be transmitted? How this rare resource should is to be accessed to allocate?
- **Accessibility:** Under what conditions and with what safeguards, a person or an organization has what right or privilege to obtain what information?

4.3 Do and Don’t of Cyber Ethics

Ethics are principles or standards of human conduct. A code of behavior on the Internet is Cyber Ethics. Some of do and don’t of Ethics:-

• DOs of Ethics:

- Connect with others via the Internet to communicate.
- Report Digital Tormenting.
- Play games, music, and videos online.
- Utilize the Internet for information and research.
- Make use of the Internet to broaden your professional and social circle.
- Shop, deposit money, and pay bills online.

• DON’Ts of Ethics:

- Don't support cyberbully.
- Avoid cyberbullying.
- Copyright-protected content should not be downloaded or shared.

- Don't lie when you talk to people online. Always be real and don't pretend to be someone else.
- Do not use information that is protected by copyright as your own.
- Don't give out too much personal information. Be cautious about the kind and measure of data you share with individuals on the web.

4.4 Problems without Computer Ethics

4.4.1 Increased cyber crimes

A result of the growing number of computer crimes, companies are facing problems as attributed to technological advancements. For Example: these problems are money exchange and mobile frauds, ATM frauds and telemarketing frauds.

4.4.2 Computer Privacy

In the current society, another issue is computer privacy that is becoming very difficult to handle where computer systems are storing, processing, manipulating and transmitting a lot of information about individuals and organizations.

4.4.3 Arrival of artificial intelligence and expert systems

The arrival of artificial intelligence (AI) and expert systems of technology advancements have ethical, technical and legal issues. Many people are still doubtful about these problems have advancements towards the holy grail of AI.

4.4.4 Workplace computerization

The protection of individuals from online attacks is a responsibility involved in computer ethics, This can be done by preventing the use of original software without permission, work interference, privacy breaching and among many other occurrences.

4.5 Advantages of Computer Ethics

4.5.1 Individuals and further developments

- Fosters computer knowledge and understanding
- Enhances safety of data
- Promotes honesty and trustworthiness

4.5.2 Social advance and legal enhancement

- Increases societal well-being
- Creates job opportunities
- Property rights are followed

4.5.3 Public information security

- Avoids misuse of personal information
- Privacy is respected
- Reduces spread of false information

4.5.4 Timely and effective supervision

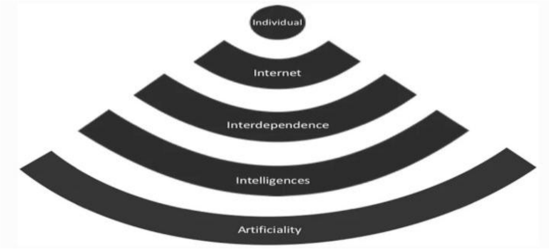
- Controls the use of artificial intelligence
- Computer and internet advancement

PRIVACY

4.6 Privacy

What information is required to describe you to others? Which conditions or circumstances apply? What information ought to be kept strictly confidential by an individual? These are the questions that arise regarding privacy.

As privacy, trust, and security are all intertwined with law and ethics, trust is a crucial component of privacy protection and security provisions. When privacy is violated, it poses a threat to security and poses a risk. When morality cannot, the law can (morality recognizes that theft is wrong; Theft is punished by law). Ethics provides a framework for law (law permits business with a profit motive, whereas ethics ensures fair business practices). When confidentiality is violated, risk is reduced, or security is lost, trust is shaken. It is a violation of the law and an insult to moral principles.



(fig. 4.1)Expansions of privacy contexts

There are many different points of views about **the right to privacy**. By this, the privacy concepts stay in doubtful state. Due to the legal governing of privacy societies has to adopt these different points of views because of the cultural difference as well. Some scholars thinks of no need to adopt new rules for this privacy right whether others people argues to adopt new rules especially in the era of new technology and that the privacy concept is an independent concept from other concepts. So the right to privacy is important and consideration.

4.6.1 Data Privacy

Data privacyis also known as information privacy or data protection that is about access, collection and use of data and about the legal right of the data. This is known to:

- Freedom from unauthorized usage to private data
- Accuracy and completeness while collecting data about a person or organization or company by technology
- Inappropriate use of data
- Availability of data content and ownership means legal right to access
- The rights to inspect, update or correct these data

If data privacy is breached then data privacy is also concerned with the costs, such costs include also called hard costs, For example: compensation payments in lawsuits, financial penalties imposed by regulators and the soft costs For Example: loss of client trust, reputational damage.

4.6.2 Data Protection Principles:

1. **Data Collection and Purpose Principle:**
   - For a purpose which is directly related to a function or activity of the data user, personal data must be collected in a fair way and lawful.
   - Data subjects means individuals from whom personal data are collected; must be notified about the purpose and transferring of data to which persons.
   - Data collected should be necessary, but not too much.
2. **Accuracy and Retention Principle:** Need to keep personal data for a period of time not longer than it is necessary and data must be accurate to fulfill the purpose for which they are used.

3. **Data Security Principle:** To safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use, a data user must practical steps.
4. **Data Use Principle:** Personal data must be used for a directly related purpose or for the purpose for which the data are collected; a new purpose is obtained from the data subject.
5. **Data Access and Correction Principle:** If the data are inaccurate, then data subject means individuals must be allowed to make corrections by giving access to their personal data.
6. **Openness Principle:** Regarding the types of personal data it holds and how the data are used, a data user must make personal data policies and practices known to the public.

4.6.3 Methods to avoid Privacy Violation:

When an unauthorized person learns about someone else's private information then a privacy violation occurs. These are some methods to avoid Privacy Violation:-

1. **Adding security extensions to browsers:** The security and privacy of a web browser can be increased by security or privacy extensions. For example: uBlock.
2. **Clearing cookies regularly:** Data is stored in cookies most of the time. So clear cookies regularly prevents risks such as data stolen.
3. **Using a webcam cover:** Webcams can be accessed by devices that have been compromised already. To limit breaches to privacy and data, use webcam cover.
4. **Reviewing social media privacy settings:** To make sure personal data is not exposed, check your privacy settings on social media accounts regularly.
5. **Reviewing permissions for apps and online services:** Check and review privacy settings of some apps and online services which request information from devices for use.
6. **Using private browsing windows:** Private browsing should be used and enabled by default if workplace devices are shared between colleagues.

4.6.4 Data Privacy Issues and solutions:

A sailor ignoring a rising sea and a falling barometer is as risky in today's world as ignoring or avoiding data privacy issues. Due to the significant increase in the use and misuse of personal data, data privacy is a crucial component of business risk management. It is risky and a challenge that can be avoided to ignore it.

1. Embedding data privacy:

IT security and disaster recovery plans are used by many businesses to safeguard the privacy of their data. However, given that data privacy is everywhere in business, this is insufficient.

After access or theft, it is pointless to consider privacy protection. A solid data strategy and employee training are essential. Make sure the tools you use for your data are appropriate and in line with current privacy regulations, such as making data anonymity easier.

2. Proliferating devices:

When you treat data across multiple services and devices, such as the Internet of Things (IoT), with your own devices, IT policies, and a proliferation of Internet-connected tablets, watches, and phones, data privacy is difficult to manage.

Your organization must be able to manage complexities and data privacy from any different operating system, any source, and multiple applications if you use more devices in the workplace. At work, you must have the appropriate data management procedures in place to solve this problem.

3. Access control is difficult in many industries:

From poorly managed data access, data privacy attacks frequently occur within an organization. People and procedures aren't as important as technology. The weakest link in the privacy and security chain is human beings. However, managing user access and protecting sensitive data on a distributed network is challenging.

Effective data architecture and solid data governance processes are necessary for your data security in order to address this issue.

4. Increasing maintenance costs:

It can be costly to secure your enterprise-level systems and avoid data privacy issues. However, properly investing in a data breach necessitates an accurate cost estimate.

Utilizing automated procedures is crucial as a result. It aids in numerous ways:

- Reducing the number of data storage
- Improved governance and control
- Eliminating points of manual processing and friction
- Lower costs
- More opportunities for de-duplication
- Reducing the risk of human error

5. Getting visibility into all your data:

If anyorganization is unaware of the nature, location, and sensitivity of the data, it will almost always be impossible to keep the appropriate information private.

It is very important to use tools to search and classify your data. By doing this, you can guarantee the data's unique treatment and shield your private, sensitive data from any privacy concerns.

6. The Increasing scale of data:

Businesses are storing more data nowadays because of low cost of cloud storage and computation costs. Indeed, also global data grows in the tens of zettabytes for businesses. So it is a difficult challenge to maintain huge data. So solve this issue, you need to have a technique to handle this large scale data stored in hundreds of systems and millions of data records.

7. A bad data culture:

The development in putting away heaps of information can be a gamble as opposed to a resource. When it comes to big data promotion, many organizations and IT leaders believed that more data was always better. However, this is no longer the case.

In today's world, storing data for an extended period of time raises both the likelihood of data theft and the attack surface for data theft. In order to safeguard data privacy, security, and complexity, IT professionals must strike a balance between the benefits of processing and storing a lot of data.

To address this issue, a great data culture that recognizes the value of data and data privacy must be established.

8. A regulations and documentation to follow:

With such countless guidelines to adhere to while accomplishing the essential information protection for your different datasets monitoring the data can be troublesome. By building processes, automating data, and building data models, you can make it easier to deal with the complexity of various regulations.

4.7 Intellectual Property in Cyberspace

Intellectual Property:

Simply, the creation of the mind refers to as Intellectual Property (IP)when someone comes up with the possession of thought or design. Intellectual property means without the owner’s permission some exclusive rights provided by any creative design owner or any distinct work type, others cannot copy or reuse that work. Property law is applicable in this case. It can be use apply in business practices including people connected or related with music, art, literature, invention etc.

Intellectual Property is using numerous types of tools for protection. Such properties are given below:

- Patent
- Copyrights
- Trademark
- Geographical locations
- Designs of Industries
- Secrets of Trade
- Layout Designs of Integrated Circuits

Cyberspace: It refers to a space with many computers attached and connected via networks of computer to communicate between these. Cyberspace is a non-physical domain. Cyberspace is now accessible to reach of every individual with the expansion of technology. Due to this fact, organizations use cyberspace as a platform of business and Intellectual Property can have a lot of pressure. These days, cyber-criminals do not involved only to identity thefts, fraudster or cyber bullying but also copyrights violation and many organizations having trademarksand new inventions. So it’s essential to protect online content along with Intellectual Property Rights with their Cyber laws.

In cyberspace, sometimes Owner’s content can be used by someone else for making profit without owner’s permission. That is what we call violation of privacy and can be protected by Intellectual Property Rights. There arepredefined laws to stopIntellectual Property Rights violation in the cyberspace.

Intellectual Property Rights Violation Laws:

1. Copyright and its Violation:

A legal right known as copyright allows certain works—musical, literary, dramatic, artistic works, producers of cinematograph films, and sound audio recordings—to perform or make related to their creations for a limited time, but it prevents any work from being used improperly or unauthorized.

The Indian Copyright Act grants the following major rights:

a) Right of Reproduction
b) Rights of Public Performance
c) Right to Issue Copies of a Work
d) Translation Right
e) Adaptation Right
f) Right of Communication to the Public

Authorship, reproduction, distribution, public communication, broadcasting, adaptation, and translation rights are typical examples of rights.

The Copyright Act of 1957, the Copyright Rules of 1958, and the International Copyright Order of 1999 govern copyright in India. In terms of copyright, the Copyright Act provides the fundamental law, the Copyright Rules contain guidelines, and the International Copyright Order protects works created by citizens of particular foreign nations.

According to India's Copyright Act, works are divided into the following three categories::

(a) Literary, Dramatic, Musical and Artistic Works

(b) Cinematograph Films, And

(c) Sound Recordings.

The owner of actual work such as any published literary, artistic, or scientific work protection against copyright is provided to restrict everyone else from misusing or duplicating that content work on his own name and to earn profit from it. If duplicate copies of the content is used and without the permission of the owner, It is sold out on the internet or even duplicating any content from any source online, then these can be referred asviolations of copyright.

Copyright Issues in Cyberspace:

- **Linking:** In this,a website user is allowed to go to any different location on the Internet. Linking destroys the interests or the owner's rights of the Linked webpage.
- **Software Piracy:** Lawfully stealing act of any software which is legally shielded is referred to as Software piracy. This software piracy includes different types of actions like spreading, copying, altering, or the software trading. It is also referred to the Indian copyright act.

  If anyone downloads a duplicate copy of MS Word from any website other than Microsoft, then it is an example of software piracy.It is done to save money, rather payingfor any paid software.

  There are 3 types piracy can be included:

  - Soft lifting
  - Uploading-Downloading
  - Software Counterfeiting
- **Cyber squatting:**Using unauthorized registration or any Internet website domain names that have same name as any company names of business, marks of service, trademarks. For example, let us think Adidas is a very popular company and the company did not have a website yet. A cyber squatter tends to buy adidas.com to sell the website domain of the company Adidas at a huge amount of money later.

2. Trademark Issues in Cyberspace:

A mark representing company graphically and that differentiate the services or products of one person or company from others which includes colors combination, the type of productsand their packaging that's called a **Trademark**. Trademark violation occurs because a trademark is used unlawful or any service mark is used by someone that creates doubts or confusion about the real company. Trademark owners can use right of the law if there trademarks is being violated by someone.

Cyberspace is like a centre for intellectual property rights violation. If any cyber site operators search for any web content without legitimate permission, then it could be resulted in the intellectual property rights violation and different other rights of owners of the website.

Also, Copyright Act 1957 and the Indian Trademark Act 1999 are not used properly on problems of Copyright violation and online Trademark. Though the Copyright Act, 1957 is protecting computer programs under, proper solutions are not provided for cyber piracy.

4.8 Professional Ethics

Simple description about Ethics isa sense by which you decide wrong and right or bad and good in many aspects. A real guidance to one's life can be provided by Ethics. Responsibility of an engineer is to solve the problems as well as make things better around the world.

In engineering, some importance of ethics is as follows:

- Engineering Projects Can be solution to People's Safety
- People can have ability to avoid or block bad decisions
- Artificial Intelligence Systems are being explained by Ethics

Ethics can be different-different from one location to another location and one person to another person. Ethics have severaltypes or forms but Personal ethics and Professional ethics are considered to be majors.

1. Personal Ethics:

Personal duties of an individual or principles and code of behavior can be referred to Personal Ethics. These ethics are already given to the person's understandings from the very beginning by friends, family, and parents. The human life is not complete and low without any personal ethics. Openness, honesty, sense of responsibility of an individual etc. are examples of personal ethics. While talking to anyone including person's friends, relatives and elderly people, If that person has excellent personal ethics then he will behave with his virtues and moral automatically. A person's behavior can reveal a person's personal ethics professional situation.

2. Professional Ethics:

A person's values and principles that are shown to an individual in a professional organization are referred to as Professional Ethics. In every organization, there are some rules employees need to follow because they don't have any other choice. Professional ethics are very essential in the professional world because it helps an individual to bring the sense of disciple into his life and maintains the modesty of the organization. Some examples of professional ethics are confidentiality, transparency, fairness etc.

Some personal and professional ethics:

- Kindness
- Transparency
- Accountability
- Commitment
- Punctuality
- Sustainability
- Fairness
- Least Harm

4.9 Freedom of Speech

One of the important fields of cyber law is Freedom of speech. Cyber laws to freedom of speech also provide freedom and their minds speak to people. In Free speech cyber lawyers must advise their clients about laws that prohibit obscenity. Sometimes clients are also being protected by lawyer when there is a discussion about their actions permissibility in free speech.

4.9.1 Freedom of speech and expression:

Every person has the right to express themselves freely naturally through any media.

Freedom of expression is a composite right. Because freedom of expression is not totally complete and contains special duties and responsibilities that's why it may have certain restrictions provided by law.

Since ancient times, the term freedom of expression had existed during the Greek Athenian era more than 2400 years ago. The right to freedom of opinion and expression is given to everyone means freedom to hold belief without interference. It means freedom to find, receive and share information or ideas of all kinds, regardless of barriers, either orally, in writing or in print or by any other media of his choice.

4.9.2 Restrictions on Freedom of Speech:

Citizens do not have the right to publish or speak without responsibility as a result of their freedom of speech and expression. Protecting language use and avoiding punishment for those who abuse it is not a license.

The following are prohibited by Article 19(3) of the ICCPR:

(a) The rights of reputations of others for respect

(b) For protection of national security, public health or morals or public order.

As per Article 19(2) of the constitution of India, the governing body may pass laws to force restrictions on the right to speech and expression on the following:

(a) Indian sovereignty and integrity

(b) State Security

(c) Foreign States Friendly relationship

(d) Contempt of court

(e) Decency or morality

(f) Public order

(g) Defamation

(h) An offence Incitement

As defined on the official website Internet Rights & Principles Coalition, For the issues of freedom of speech in the cyber world and human rights issues, there are some rules of the rights and principles of internet freedom.

4.9.3 Principles and Human Rights on the Internet:

1) Universality and Equality: We all are born free, equal in distinction and rights, it must be protected, respected and fulfilled for the online atmosphere.

2) Rights and Social Justice: For the protection, promotion and fulfillment of human rights and for social justice advancement Internet is a free platform. It is duty of everyone to respect all others and the human rights in the online atmosphere.

3) Accessibility: An equal right is given to everyone for accessing and using a secure and open Internet.

4) Speech and Association: The right is given to everyone to find, get and share information freely on the Internet without restriction or other problem. Everyone also have right to communicate for social, political, cultural or other purposes online.

5) Privacy and Data Protection: The right to privacy is given to everyone online and the right to data protection, including control over personal data processing, deletion and sharing.

6) Life, Liberty and Security: These rights include the rights to liberty, life, and security respect must not be violated for online purpose.

7) Diversity: To facilitate plurality of speech Cultural and linguistic diversity on the Internet must be promoted, also technical and advance policy should be encouraged.

8) Network Equality: Everyone shall have universal and open access to the content of the Internet, free from discriminatory preference, filtering or traffic control on commercial, political or other grounds.

9) Standards and Regulation: The Internet's infrastructure, communication systems and document and data formats will be based on open standards that ensure full interactivity, inclusion and equal opportunities for all.

4.10 Fair Use and Ethical Hacking

4.10.1 Fair Use:

Fair use of a copyrighted work is not a violation of copyright.

Fair use gives users the right to use copyrighted material without permission in certain circumstances. If a use is justified, the user is not required to inform the copyright holder or obtain permission.

An affirmative protectionknown as fair use that is raised in result to a copyright claim ofowner that any person is violating copyright.A party is allowed fair use to use a copyrighted work for doing some actions likedisapproval, comment, teaching, news reporting, scholarship, or studywith no permission of the owner of copyright.

Segment 107 of the Copyright Act gives instances of inspirations that favor fair use: “criticism, remarks, reporting on the news, instruction (including multiple copies for use in the classroom), scholarship, and research" It is not always fair to use for one of these "example purposes," but it may be fair to use for other purposes. The law specifies four criteria for determining whether a particular use is appropriate.

The four factors of fair use:

1. **Purpose and character of use, including whether such use is of a commercial nature or for non-profit educational purposes**

   Courts typically focus on whether the use is "transformative". That is, does it add new expression or meaning to the original, or does it simply copy from the original.

2. **The nature of the copyrighted work**

   It is advisable to use material mainly from factual works than to use purely fictional works.

3. **Quantity and adequacy of the portion used in relation to the copyrighted work as a whole**

   Borrowing small pieces of material from the original work is more likely to be considered fair use than borrowing larger chunks. However, even a small take can weigh against proper use in some situations if it constitutes the "heart" of the work.

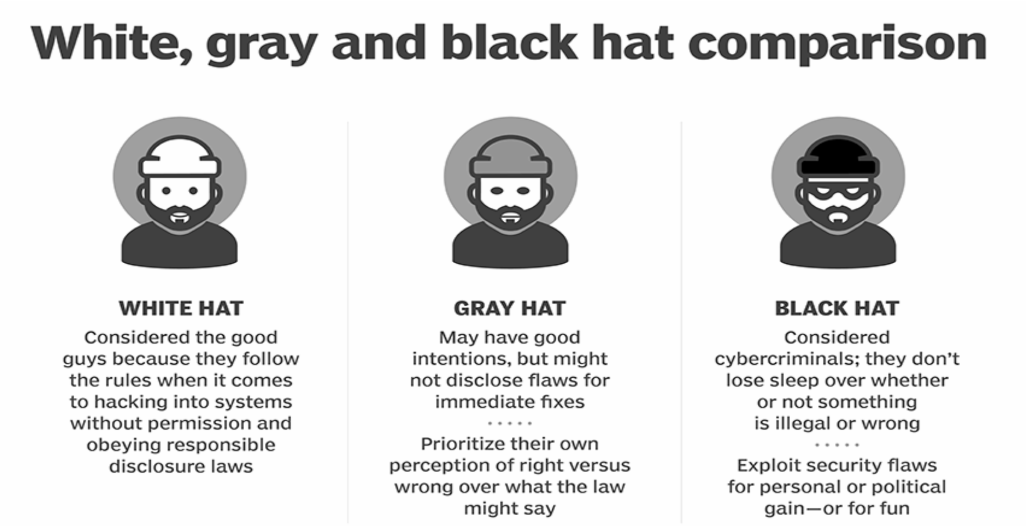
4. **The effect of the use, or the value thereof, on the potential market for the copyrighted work**

   Uses that harm the copyright owner's ability to profit from their original work by serving as a replacement for that work's demand are less likely to be fair uses.

4.10.2 Ethical Hacking:

Is Ethical Hacking Stealing Data or Cracking Passwords? No, it goes far beyond that. A computer or network's vulnerabilities and potential threats are the focus of ethical hacking. An ethical hacker notifies the organization of vulnerabilities or flaws in computers, web applications, or networks. Therefore, let's examine ethical hacking one step at a time.

4.10.3 Types of Hackers:


White, gray and black hat comparison
WHITE HAT
Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws
GRAY HAT
May have good intentions, but might not disclose flaws for immediate fixes
Prioritize their own perception of right versus wrong over what the law might say
BLACK HAT
Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong
Exploit security flaws for personal or political gain—or for fun

(Fig. 4.2)

Hacker is a human individual who attempts to access into any secured network or try to take control of operating system with different strange ways. Often many programmers act as hackers nowadays. They collect advanced information and knowledge of operating systems and learn programming of many languages and find loopholes in systems and the reasons for such loopholes. There are many Hackers’types written below:

1) White Hat Hackers
2) Black Hat Hackers
3) Gray Hat Hackers
4) Script Kiddies
5) State/Nation Sponsored Hackers
6) Hacktivist
7) Green Hat Hackers
8) Red Hat Hackers
9) Blue Hat Hackers

10) Malicious Insider or Whistleblower

4.10.4 Difference between Hacking and Ethical Hacking:

- The practice of getting private stored data by cyber experts is called **Hacking**. When any programmer makeserrors or mistakes, those mistakes make the system weak and vulnerable; these weaknesses are being taken up by the hackers for hacking the system. Some hackers do not follow or work on the ethical hacking principles iscalled unethical hackers. Hackers are well known that they are performing illegal activities and further result of such activities used in crime. In other words, trying to attack a private network computer system by entering inside the computer is called **hacking.**
- Any legal access to private information that is unauthorized to the rest of the world is called **Ethical hacking**. For protecting the computer system or websites from malicious codes,viruses and hackers Ethical hacking is widely used. If the principles of ethical hacking are followed then these hackers are calledEthical hackers. These hacker are highly skilled to break and breach into system applications or programs, professional ethical hackers can restore a compromised system security and catch the criminal with their skills and abilities.

4.10.5 Similarities between Hacking and Ethical Hacking:

The same tools for hacking are used by almost all hackers like white-hat hackers or a black or grey. All hackers are skilled and studied deeply the topics ofoperating system, network and computer fundamentals. In starting, they can easily find weakness of the system from the zero-day attack.

4.10.6 Solutions to avoid being hacked:

- Turn off your internet connection.
- Open Firewall and enable it.
- Change your passwords time to time.

Ethical hacking is compromising to assess the security of computer systems and act in good trust by notifying the weakness of system. For many job roles, ethical hacking is an essential and special skill to securean organization’s assets online. Professional people who workon these kind of job roles uphold the computers system, servers and other many components of organization, infrastructure of this in operating condition to prevent accessing unauthorized by non-physical channels.

4.10.7 Reasons to Learn Ethical Hacking:

As any student or professional IT related person you will be thinking to learnhacking ethical just like an option of career. In this you will know, How you are thinking right. Reasons of this are assessed on the parameters of earnings, scope of future, status in social, satisfaction of one self and logical development.

1) **Pays Well (More Than well)**
2) **Highly In-Demand Skill**
3) **Help to Create a Secure Internet for All**
4) **One Can Become a National Asset**
5) **Good to Learn Something New**

4.11 Check Your Progress

1. __________________ is a branch of applied ethics that examines moral, legal, and social issues at the intersection of computer/information and communication technologies.
2. IOT means ____.
3. Where many computers are attached and connected via networks of computer to communicate between those, __________________ is a non-physical domain.
4. Toauthorize some acts such as to people creating musical, literary, dramatic, cinematograph films producers' artistic works and audio recordings to execute or related to their creations, a right is given by law called __________________.
5. Lawfully stealing act of any software which is legally shielded is referred to as ______________________piracy. This software piracy includes different types of actions like spreading, copying, altering, or the software trading.
6. Any legal access to private information that is unauthorized to the rest of the world is called _______________________________ hacking.

4.12 Summary

Walter Manner coined the term "computer ethics" in the middle of the 1970s. He also advocated teaching computer ethics in computer science. Ethics can be defined as a person's moral code of conduct. In computer security, cyber-ethics is what differentiates security personnel from attackers; It defines the capacity to adhere to ethical principles at work and shares knowledge of right and wrong.

Cyber ethics, which examines ethical, legal, and social issues at a common point between computer/information and communication technologies, is a branch of applied ethics. Cyber ethics is sometimes referred to as information ethics.

PAPA refers to Privacy, Accuracy, Property and Accessibility.

Problems without Computer Ethics:

- Increased cyber crimes
- Computer Privacy
- Arrival of artificial intelligence and expert systems
- Workplace computerization

Advantages of Computer Ethics:

- Individuals and further developments
- Social advance and legal enhancement
- Public information security
- Timely and effective supervision

As privacy, trust, and security are all intertwined with law and ethics, trust is a crucial component of privacy protection and security provisions. When privacy is violated, it poses a threat to security and poses a risk. When morality cannot, the law can (morality recognizes that theft is wrong; Theft is punished by law). Ethics provides a framework for law (law permits business with a profit motive, whereas ethics ensures fair business practices). When confidentiality is violated, risk is reduced, or security is lost, trust is shaken. It is a violation of the law and an insult to moral principles.

Data privacy is also known as information privacy or data protection that is about access, collection and use of data and about the legal right of the data. This is known to:

- Data Collection and Purpose Principle
- Accuracy and Retention Principle
- Data Use Principle
- Data Security Principle
- Openness Principle
- Data Access and Correction Principle

Invasion of Privacy:

- Intrusion on a person’s seclusion or solitude
- Public disclosures of embarrassing private facts about a person
- Publicity that places a person in a false light in the public eye
- Appropriation, for the Defendant’s gain, of a person’s name or likeness

Privacy Violation:

Methods to avoid Privacy Violation:

- Using a webcam cover
- Clearing cookies regularly
- Reviewing privacy settings and permissions for apps and online services
- Reviewing social media privacy settings
- Removing personal details from the open voters register
- Using private browsing windows

Data Privacy Issues and solutions:

A sailor ignoring a rising sea and a falling barometer is as risky in today's world as ignoring or avoiding data privacy issues. Due to the significant increase in the use and misuse of personal data, data privacy is a crucial component of business risk management. It is risky and a challenge that can be avoided to ignore it

1. Embedding data privacy
2. Proliferating devices
3. Increasing maintenance costs
4. Access control is difficult in many industries

5. Getting visibility into all your data
6. A bad data culture
7. The ever-increasing scale of data
8. A long list of regulations and documentation to follow

Intellectual Property in Cyberspace

Simply, the creation of the mind refers to as Intellectual Property (IP) when someone comes up with the possession of thought or design. Intellectual property means without the owner's permission some exclusive rights provided by any creative design owner or any distinct work type, others cannot copy or reuse that work. Property law is applicable in this case. It can be use apply in business practices including people connected or related with music, art, literature, invention etc.

Notable among these are the following:

- Patent
- Trademark
- Geographical indications
- Layout Designs of Integrated Circuits
- Trade secrets
- Copyrights
- Industrial Designs

Professional Ethics:

Simple description about Ethics is a sense by which you decide wrong and right or bad and good in many aspects. A real guidance to one's life can be provided by Ethics. Responsibility of an engineer is to solve the problems as well as make things better around the world.

In engineering, some importance of ethics is as follows:

- Engineering Projects Can Have an Immediate Impact On People's Safety
- It Gives Them Ability To block Against Bad Decisions
- Ethics Have To Be Explained to AI Systems

Freedom of Speech: One of the important fields of cyber law is Freedom of speech. Cyber laws to freedom of speech also provide freedom and their minds speak to people. In Free speech many clients cyber lawyers must advise their about laws that prohibit obscenity. Sometimes clients are also being protected by cyber lawyers when there is a discussion about their actions permissibility in free speech.

Principles and Human Rights on the Internet:

- Universality and Equality
- Rights and Social Justice
- Accessibility
- Privacy and Data Protection
- Life, Liberty and Security
- Diversity
- Network Equality
- Standards and Regulation
- Governance

Fair Use:

Fair use of a copyrighted work is not a violation of copyright.

Fair use gives users the right to use copyrighted material without permission in certain circumstances. If a use is justified, the user is not required to inform the copyright holder or obtain permission.

The four factors of fair use:

- The purpose and character of the use, including whether such use is of a commercial nature or for non-profit educational purposes
- The nature of the copyrighted work
- Quantity and adequacy of the portion used in relation to the copyrighted work as a whole
- The effect of the use, or the value thereof, on the potential market for the copyrighted work

Ethical Hacking:

Is Ethical Hacking Stealing Data or Cracking Passwords? No, it goes far beyond that. A computer or network's vulnerabilities and potential threats are the focus of ethical hacking. An ethical hacker notifies the organization of vulnerabilities or flaws in computers, web applications, or networks. Therefore, let's examine ethical hacking one step at a time.

Difference between Hacking and Ethical Hacking:

The practice of getting private stored data by cyber experts is called **Hacking**. When any programmer makes errors or mistakes, those mistakes make the system weak and vulnerable

Any legal access to private information that is unauthorized to the rest of the world is called **Ethical hacking**. For protecting the computer system or websites from malicious codes, viruses

Solutions to avoid being hacked:

- Turn off your internet connection.
- Open Firewall and enable it.
- Change your passwords time to time.

4.13 Keywords

- Ethics in Cyber Security
- Computer Privacy
- Privacy Violation
- Cyberspace
- Privacy Violation
- Intellectual Property
- Professional Ethics
- Freedom of Speech
- Ethical Hacking
-

4.14Self Assessment Test

1. What is Ethics in Cyber Security, Its consequences and positive impacts?
2. What is Privacy? Explain Data Privacy and Privacy Violation
3. Describe Intellectual property in cyberspace.
4. Explain personal and professional ethics.
5. What is freedom of speech and human rights on internet.
6. What is Ethical hacking? Difference between hacking and ethical hacking.

4.15 Answers to Check Your Progress

1. Cyber Ethics
2. Internet of Things
3. Cyberspace
4. Copyright
5. Software
6. Ethical

4.21 References

1. Nathan House, “The Complete Cyber Security Book” Volume-I, First edition: January 2017, published by StationX Ltd.
2. Thomas A. Johnson, “Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, CRC Press, ISBN:978-1-4822-3923-2, 2015.
3. https://www.geeksforgeeks.org/digital-evidence-collection-in-cybersecurity/
4. https://www.devry.edu/online-programs/area-of-study/technology/what-is-computer-forensics.html
5. https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools

SUBJECT: Cyber Security	
COURSE CODE: MCA-34	AUTHOR: DR. ABHISHEK KAJAL
CHAPTER NO. 5	

Trademark and Cyber Forensics

(Internet fraud, Electronic evidence, Forensic technologies, Digital evidence collections)

INDEX **Page No.**

TRADEMARKS

INTERNET FRAUD

ELECTRONIC EVIDENCE

FORENSIC TECHNOLOGIES

DIGITAL EVIDENCE COLLECTIONS

Lesson-5

(Trademarks, Internet fraud, Electronic evidence,

Forensic technologies, Digital evidence collections)

5.1 Trademarks

5.1.1 Introduction to trademark

A trademark is a distinctive mark that a company uses to represent its unique identity, identify its goods and services to customers, and distinguish the company and its goods and services from those of other similar type of businesses. A trademark typically consists of a design, logo, image, name, word, phrase, symbol, or a combination of two or more of these elements.

A trademark's primary function is to specifically identify a product or service's source market or origin. As a result, it signifies the identification of products and services that meet consumer needs and prospects in terms of quality and other attributes. In a similar vein, a law known as the trademark law was enacted to safeguard consumer interests and ensure that consumers are not misled by businesses regarding the quality or manufacturing of any product or service. In order to protect a company's reputation, trademarks also encourage providers, manufacturers, or suppliers to provide high-quality goods or services.

5.1.2 Establishing Trademark Rights

The law treats trademarks as a form of property. By actual use in the marketplace, a trademark may establish proprietary rights in relation or by the mark registration or business mark with Office of the Trade Marks in that city jurisdiction. A trademark can be registered only if is eligible to serve the important trademark with a unique reputation of company.

A registered trademark grants the owner of the trademark a number of exclusive rights, including the right to use the trademark solely for the registered goods or services. Unauthorized use of a mark relating to similar products or services to registered products or services constitutes trademark infringement, and in some instances, any use relating to distinct products or services is covered by the law.

A trademark's actual use must be protected by trademark rights. If no one used the mark, the rights would expire periodically. When a trademark is registered, misuse of the mark or failure to enforce the registration for infringement may occasionally result in the mark's removal from the register.

Even though the official trademark registry of a particular jurisdiction has not actually registered the mark, there are claims that the symbolTM may be used for trademark rights. The TM symbol, on the other hand, signifies that the mark has been registered. Because of the widespread use of symbols worldwide, it is not necessary to use any symbol forcefully.

5.1.3 Passing off Trademarks

If the trademark has not been registered by that time, common law countries, particularly in some jurisdictions, provide protection by passing unregistered trademarks to maintain business reputation. When a company is conducting business under a trade mark that has not been registered for many years and there may be a conflict between businesses that use the same or a similar mark, trademark passing is helpful.

A person cannot misrepresent his goods or services because the plaintiff owns them and a person cannot misrepresent his goods or services because he has some relationship or connection with the plaintiff. This passage law prevents misinformation.

Covering circumstances can be managed by suit at regulation by passing off and enrolling brand names in various ways. Any name, mark, setup, or other mark is not monopolized by the passing off. They are not considered assets in and of themselves by it. However, where there is some kind of relationship between the plaintiff and the defendant, the law of tracts is intended to protect the public from being misled.

The defendant may bring an action against himself brought about by the plaintiff if the defendant does something likely to mislead the public into thinking that the activity relates to the plaintiff and causes some harm to the plaintiff. Therefore, the three primary components are misrepresentation, harm to reputation, and goodwill caused by the pass off. By passing unregistered trademarks, some common law jurisdictions safeguard business reputations.

5.1.4 Solutions for Trademark Breach

It resembles and equivalent to forestalling unapproved utilization of a brand name which helps the brand name proprietor. Likewise, whether a brand name is enlisted relies upon various variables, including brand name similitude, closeness of items or potentially administrations, and whether the proprietor's brand name is famous. If a trademark is registered, its owner will have an easier time proving his or her rights under the Infringement Act and trademark rights.

Passage litigation can be used to enforce rights in an unregistered trademark, whereas an action for trademark infringement can be used to enforce exclusive rights in a registered mark.

5.2 Internet Fraud

5.2.1 Introduction to Internet Fraud

Online services and software used to do fraud and take advantages of victims by accessinginternet. The cybercrime activity which can be executed using internet or by email message can generally be covered in term "internet fraud" if it includes criminal activities like stealing identity, phishing links, and other hacking activities created to scam people for making money.

Online services are misused to target victims and every year there is fraudulent activities worth for millions of dollars by targeting account of people by **Internet scams**. And there is exponential growth day by day.

5.2.2 Internet Fraud Types

Many different types of attacks and strategies are used by cyber criminals to commit internet fraud. To steal private user data and its details, for spreading phishing scams, cyber criminals use malicious software, email and instant messaging services to distribute malware, complex websites.

Internet fraud can be categorized in many kinds of attacks as follows:

- **Phishing and spoofing:** Using online messaging and email services to trap victims to access his personal data, login credentials and financial details.
- **Data breach:** Stealing secret, protected, or private sensitive data from a protected location and transferring it into an untrusted environment. That data is being stolen from users and organizations.

- **Denial of service (DoS):** Interrupting access of online services, system, server or network access to legitimate usersby flooding the network traffic with numerous requests by cyber attacker with malicious intent.
- **Malware:** Use of malicious software to damage or disable users' devices or steal personal and sensitive data.
- **Ransomware:** A type of malware that blocks users from accessing important data and then demands payment in a promise to restore access. Ransomware is usually distributed through phishing attacks.
- **Business email compromise (BEC):** Often a sophisticated form of attack targeting wire paying businesses. It compromises legitimate email accounts through social engineering techniques to collect unauthorized payments.
- **Email Phishing Scams**

  One of the most common forms of Internet fraud, email-based phishing scams that pose a serious threat to Internet users and businesses. These types of threats, which are designed to target specific individuals, can be as straightforward as they are complex.

  When attackers send a link to the user mail of a malicious website or any online portion of a webpage that pretends to be a legitimate website, users click on it and open an attachment with malicious content.

  The hacker starts by working on a real website or creating a fake version of one. After that, they get a list of the email addresses they want to target and send messages or attachments to those addresses in the hopes of getting people to click on links to a fictitious website. When a victim clicks on that link of the fictitious website, they are actually visiting the fictitious website, which may automatically execute malware to steal personal login information and data or request a username and password. It can be stored in the device used by user’s system. A hacker can gain access to a user's online accounts and steal additional data, such as credit card information, gain access to system-connected corporate networks, or store widespread identity fraud.

- **Greeting Card Scams**

  This type of fraud happened on special occasions including birthday’s celebration, or any festival that are celebrated commonly by sending wishes and greetings to friends and family members by email. Hackers change these email greetings and attach malicious software within email of greeting card, when victim opens that greeting card actually the malicious software downloads and installs in the victim’s computer to destroy computer or to take personal information.

- **Credit Card Scams**

  When attackers tries to steal information of your credit card or bank details to buy or purchase anything online using your credit card details then Credit card scam occurs. To get these details, internet fraudsters usually use the trick of being good and true by showing themselves as credit card or loan giving company.

- **Online Dating Scams**

  Most of the online dating applications and websites are fake and try to misguide people. To attract victims hackers create these kinds of apps making them sending money and by using new love interests technique they distribute personal data. For this they make fake girls/boys profiles and try to communicate with users, try to develop a relationship, takes their trust slowly, use a phony story, and ask for financial help from the user.

- **Lottery Fee Fraud**

  In this fraud, Scammers sends emails to victim and say that they won a lottery prize. Then scammers tell recipients to pay a little fee to claim their prize. Lottery fee fraudsters make emails look like it sound believable. Fraudsters just try to show victim dreams of having a huge amount of money. But in real that lottery thing is totally fraud and no one gets any prize.

5.2.3 Protection from Internet Scams

Above we discussed some commonly used types of internet fraud list, With awareness internet users can avoid and protect themselves from these frauds.

- Never send money to someone if you meet on the Internet,

- Never tell or share your private or financial details with strangers that are not real or trustable.
- Never try to click on any link or hyperlinks of websites, instant messages or attachments in emails.
- Internet users must report to authorities online about these scammer activity and phishing emails if once targeted.
- Checking of your bank accounts time to time can avoid credit card frauds as well.
- Configure and set notification for any activity related to your credit card.
- Credit monitoring by signing up.
- Use services for consumer protection.

5.3 Electronic Evidence

5.3.1 What is Electronic Evidence?

Any part of evidence which is generated by some mechanical or electronic type process can be referred to the term 'electronic evidence' used for proving or disproving any kind of fact or the evidence as information to be represent in court. Digital evidence can be used a secondary name for electronic evidence commonly. A forensic expert or person checking for electronic evidence has skills to recover any data saved in electronic devices or systems and to examine it before presenting evidence in court.

Since these records which are electronic can easily be changed or altered, tempered, transferred etc. In absence of such safeguards, there can be problem of deformation of justice if there is only electronic evidence and case is based on it. The e-documents legality is debatable because they are prone to tampering, with agencies investigating such e-documents grappling with the admissibility of similar electronic evidence.

5.3.2 Digital Evidence

Electronic evidence, also commonly known as digital evidence, is data stored within electronic devices or systems that can be retrieved by forensic experts and used as admissible evidence in court. Any information or value of data which is used for investigation by storing, collecting or transferring via electronic device is called Digital evidence. Emails, messages of text, images and videos format and searches on Internet are few usual types of digital evidence.

Digital Trail: Many criminals are currently leaving a footprint in digital form; Posting anIP address of suspecton platforms of social media or by your device like mobile in daily use in traditional computers place and cameras. The information that can be revealed:

- Intent,
- Location and time of crime,
- Relationship with victim(s), and
- Relationship with other suspect(s)

5.3.3 Examiner of Electronic Evidence

The Information Technology Act, 2000 Section 79A has been inserted to serve with the electronic evidence examiner. In the IT Act Chapter XIIA, it protects the rule to highlight the role of the electronic evidence examiner, as feeling of legislators is that a particular department, for the central government agency needed to share opinion of expert on the electronic type of evidence in any other authority or court.

According to the above definition "Electronic Form Evidence", Courts may permit the use of digital evidence just like chats of WhatsApp, chats of social media, data and history of browser, e-mails, digital images, documents of word processing, material Huh. HDD Hard disk, database, tracking of Global Positioning System etc. during criminal trial or proceedings of civil.

- **Scope of the scheme:**

The approval scope in applicant forensic science laboratories has one or more areas or disciplines of activities:

- Computer (media) forensics
- Network (Cyber) Forensics
- Mobile Equipment Forensics
- CCTV forensics and Digital video/image
- Forensics digital audio
- Equipment particular forensics
- Machines of Digital equipment

5.3.4 Electronic Evidence and the Indian Evidence Act, 1872

Obviously, when electronic or digital evidence is compared to predictable or conventional evidence, it has been observed that electronic evidence evaluation needs specific expert training in the area of cyber security to check its authenticity and requires the method used in investigation and facts analysis, data figures or details held or recovered from any electronic device to be acceptable in front of court.

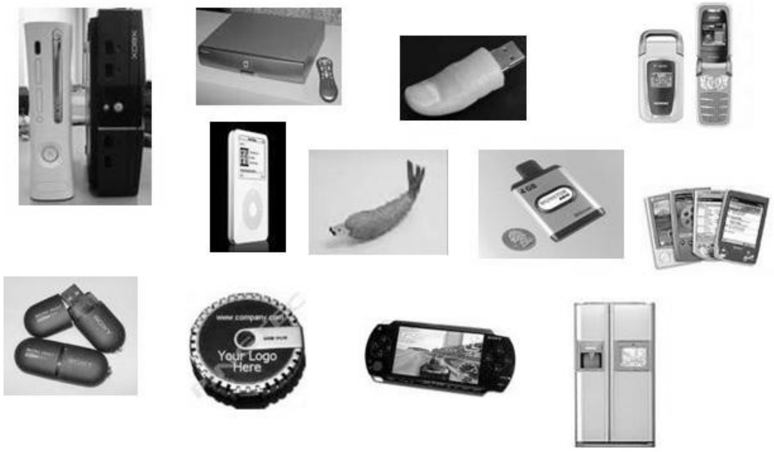
Indian evidence alteration comes as a result of the Information Technology Act section 92. Amendments to the Evidence Act include adding term "electronic record" to the evidence definition, allowing electronic evidence admissibility. Further, sections 65A and 65B were added through changes to give electronic evidence admissibility. In addition, the IT Act Section 79A has extended the Section 45 scope of the Indian Evidence Act. The Indian Evidence Act Section 45 provides for experts opinion.

Section 45 of the IEA states that, when an opinion is required to be formed by the Court on matters such as law of foreign or art or science or handwriting or fingerprints identification, the opinion of such persons shall be relevant to the point which is specifically Proficient in the field of law, art, science or in a form of handwriting or fingerprint recognition. These persons are called experts and opinion of them is relevant with this section.

5.3.5 Forms of Media for Electronic Evidence

The data obtained from the following devices and applications are treated as evidence. However, this is only acceptable if retrieved using a forensic method by a certified expert.

- Computers, laptops and tablets
- HDD, RAID and SSD hard drives
- Mobile phone data
- USB memory sticks and SD cards
- Whatsapp messages
- Social media information
- CCTV
- Digital photographs
- Cloud storage data



(fig. 5.1)

5.3.6 Guidelines for Electronic Evidence

A set of guidelines for handling electronic / digital evidencesare defined under Section 65B (1) of Information Technology Act 2000. It is important that these are strictly followed while examining computer or digital media as it ensures continuity of evidence and admissibility of digital evidence in court. Besides various defined principles for evidence handling, four governing principles by ACPO are most recognized suggestions for electronic evidence in cyber forensic. These principles of handling Computer Based Electronic Evidence are:

Principle 1:

Any action taken by law enforcement agencies or their agents must not alter data held on computers or storage media that can later be relied upon in court.

Principle 2:

In exceptional circumstances, where a person finds it necessary to use original data held on a computer or storage media, that person should be able to do so and be able to give evidence explaining the relevance and implications of their actions needed.

Principle 3:

An audit trail or other record of all procedures applied to computer-based electronic evidence must be created and preserved. An independent third party should be able to investigate those processes and obtain similar results.

Principle 4:

The person in charge of the investigation has the overall responsibility of ensuring that the law and these principles are complied with.

Applying the ACPO guidelines in practice means that a chain of custody must be established. This ensures that there is no unauthorized access to digital media. A write-blocker is required when digital evidence is forensically interrogated, so that the data cannot be overwritten or altered from its original format, while preserving the evidence. Specialist forensic equipment must be used, and all inquiries must be completed on a forensic image (or clone), not the original media device.

5.4 Forensic Technologies

5.4.1 Computer Forensics:

A field of technology that uses techniques to identify for investigative purpose and store evidence from computer devices is called Computer forensics. Often, it is used to present evidence in court.

Areas outside of investigation can also be covered by Computer forensics. Sometimes we need professionals to recover deleted or lost data from failed hard drives, server computers that have stopped working or reformatted the operating systems.

5.4.2 Computer Forensics vs. Cyber Security:

Computer forensics and cyber security may look like similar to people who don’t have this profession. Both are related to criminals and computers, besides these initial similarities, each exercise of the function is very different.

Computer forensics largely focuses on recovery of data. In criminal trials evidence is often used after recovering data, but is also recovered data loss of companies. Besides that, criminals are not always cybercriminals who are investigated by computer forensics professionals. Since nearly a computer is used by almost everyone, their personal computer has valuable important information which can help in investigations.

Secondly, **cyber security** is more dedicated for defense. Cyber security professionals work with different types of job titles, but almost all work for same job goal to make networks secure and systems protected from possible attackers. Sometimes to test their abilities they also do hacking to check network or client's network to find weak areas and strengthen them.

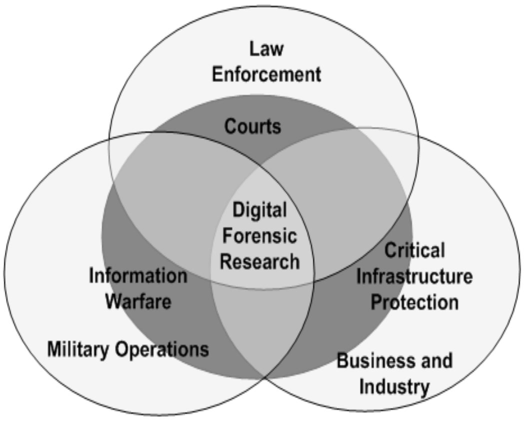
5.4.3 Skills needed for Computer Forensics:

Cyber Forensics is quite complex domain than being a computer science. Highly expertise in following skills is a must prerequisite for turning into a Cyber Forensic:

- **Programming:** While using any tools to recover hard-to-search, lost data or encrypted data requires an understanding of programming languages.
- **ISO Standards:** An ISO standard is protocol and rules set that determine the most efficient way to execute a task. Computer forensics makes use of these parameters, making it important to understand them.
- **Operating System:** Operating systems are those which enable the devices to perform their main functions. Since professionals related to computer forensics mostly work on broken or damaged equipment, they can have an understanding the operating system for recovering data loss.
- **Computer hardware and software:** It is responsibility of computer experts to find out the best way for searching data in software and hardware elements of a computer. It is also helpful when a repair is needed to recover the data.
- **Organization:** It is important for people in the computer forensics profession to have a strong sense of organization. In this area people, deal with data and need organizational skills that can support those different unrelated data from information which is essential.
- **Cyber Security Standards:** A computer forensics specialist should have a strong knowledge and understanding in the cyber security industry.
- **Analytical Capabilities:** Lastly, a computer forensics specialist must be able to monitor the data revealed by them. This can support them to identify data that is important to investigate.

5.4.4. Digital Forensics:

Computerized crime scene investigation is the most common way of confirming and agreeing with electronic information. While conducting a structured investigation to collect, identify and validate digital information to reconstruct past events, the process aims to preserve any evidence in its most original form. The use of data in court is frequently mentioned, but digital forensics may also be used in other situations.



(fig. 5.2)

- **Stages of Digital Forensics**

  For digital evidence to be accepted in court, it must be handled in a very specific manner so that cybercriminals do not have any chance to tamper with the evidence.

  1. Identity: First, find the evidence, pay attention to where it is stored.

  2. Security: Next, keep data separate, safe and secure. This includes preventing people from potentially tampering with evidence.

  3. Analysis: Next, reconstruct the pieces of data and draw conclusions based on the evidence found.

  4. Documentation: After that, make a record of all the data for the reconstruction of the crime scene.

  5. Presentation: At the end, summarize and draw conclusions.

Digital evidence is same as other evidence used in investigations and legal procedures:

- **Data theft and network breaches:**to understand about the breach and the attacker, Digital forensics is used to know that.

- **Digital forensics is used to understand online fraud and identity theft:** The use of digital forensics for measuring the effect of a breach or breach to a people or organization.
- **Violent crimes such as theft, assault, and murder:** Digital forensics is used to get digital evidence from mobile phones, cars or these kinds of other devices in the vicinity of a crime.
- **White Collar Crime:** Digital forensics is used to gather evidence that can support to identify and prosecute crimes such as corporate fraud, embezzlement and extortion.

5.4.5 Digital Forensics Tools:

Due to the wide variety of potential data sources, digital forensic tools often have different specifications. This list outlines some of the most common and widely used tools for carrying out various parts of computer forensic investigations.

- Disk Analysis: Autopsy/The Sleuth Kit
- Image Creation: FTK Imager
- Memory Forensics: Volatility
- Windows Registry Analysis: Reorganizing the Registry
- Mobile Forensics: Celebrite UFED
- Network Analysis: Wireshark
- Linux Distribution: Cain

5.4.6 Digital Forensic Techniques:

Making copies of a compromised device and then analyzing the data with a variety of methods and tools is digital forensics. Digital forensics methods aid in the search for copies of encrypted, damaged, or deleted files in unallocated disk space and hidden folders. The most prevalent methods are:

1. Reverse Steganography:

Cybercriminals employ steganography to conceal digital files, messages, and data links. Hashing data from a specific file is reverse steganography. The hidden information in a digital file or image may not appear suspicious when examined. The hidden information, on the other hand, can be found beneath the image or replace string data.

2. Stochastic Forensics:

Digital activity that does not produce digital artifacts can be analyzed and reconstructed with the assistance of stochastic forensics. A data change that occurs unintentionally as a result of digital processes is known as a digital artifact. Text records, for instance, are computerized relics that might contain hints connected with a computerized wrongdoing, for example, information robbery that modifies document credits. Stochastic forensics aids in the investigation of data breaches caused by insider threats that cannot leave digital evidence behind.

3. Cross-drive analysis:

Anomaly detection, also known as cross-drive analysis, helps uncover commonalities to provide a context for the investigation. Thissimilitude acts as a pattern for identifying dubious occasion. In order to locate, evaluate, and store any information that is pertinent to the investigation, this typically entails relating and cross-referencing data across multiple computer drives.

4. Live Analysis:

The operating system performs live analysis while the device or computer is running. Usually, this involves finding, analyzing, and removing volatile data stored in RAM or cache with the help of system tools. To properly maintain the chain of evidence, live analysis typically necessitates placing the inspected computer in a forensic laboratory.

5. Deleted File Recovery:

A method for recovering deleted files, also known as data carving or file carving, is deleted file recovery. This entails searching a computer's memory and system for files that have been partially deleted in one location but left traces elsewhere on the machine being inspected.

5.5 Digital Evidence Collections

As people are using Personal digital devices in huge number, and internet is accessible to almost everyone, so there is no exception in reporting growth ofcyber criminal activities at peak with each next day. At forefront there are more and more computer related crimes are happening like cyber fraud, cracking software etc. The computer forensic rules appeared with it. Today in the investigation, digital evidence collection is used in different types of crimes like fraud, spying, cyber stalking etc. The forensic experts and techniques used knowledge to explain the contemporary condition of digital artifacts from confiscated evidence such as computer systems, storage devices (such as hard disks, SSDs, CD-ROMs, USB flash drives etc.), or electronic Documents such as emails, pictures, chat logs, documents phone logs etc.

5.5.1 Digital Evidence Collection Procedure:

Digital evidence collection involves the following processes written below:

1. **Data Collection:** To investigate, data is firstly checked and collected in this process.
2. **Examination:** The data collected in the second stage is cautiously scrutinized.
3. **Analysis:** Different tools and techniques with collected evidence are used and analyzed to make a conclusion, in this process.
4. **Reporting:** All the documents, files, reports in this final stage are checked before presenting in the court.

5.5.2 Types of Collectible Data:

Computer experts and investigators should well aware of equipments for examiningof possible search methods for evidence, so asenable them to alter their technique of searching, if need arise. Computer crimes and criminal activities can vary and broad in wide range; they can go as far as rare illegal things, intellectual property damage, personal data stealing etc.Cyber Forensic Analysts also need to be well aware of Anti-forensics tools and techniques, what may assist forensic investigation analysis inconclusive particularly in a cloud environment. Investigators need to be aware of specific types of malware and obfuscation methods, which can compromise the authenticity of electronicevidences, which make conclusions tough to present in the court.

The examiner should choose appropriate equipment to use during the analysis. Investigators may face many problems while probing the case such as files may have been deleted from the computer, they may have been destroyed or even using encryption, so the investigator has to prevent various tools, methods and software should also be familiar with data from getting damaged during process of data recovery.

For computer forensic investigation, two types of data can be acquired:

Persistent Data: Storage device having non-volatile memory can store this type of data like in external storage device like SSD, HDD, pen drive, CD or in local hard drive etc. These devices store data permanently.

Volatile Data: Volatile memory storage devices can temporary store this type of data like in memory, register, cache, RAM, or it is present in transfer, which will be lost after the computer is powered off or lost power. Since explosive data is unrecoverable, it is important that an examiner knows how to retain it reliably.

5.5.3 Types of Evidence:

It is really important to collect pieces of evidence in any analysis to sustain the claims in court. Some major types of evidence are written below:

- **Real evidence:** Physical or countable evidence such as hard drives, flash drives, documents etc. A witness may also be considered a piece of tangible evidence.
- **Heard Evidence:** These evidences are known to statements as out-of-court. These are created in the courts to verify the reality of the matter.
- **Original Evidence:** A declaration report has these parts of evidence made by a person that is not a testifying witness.
- **Testimony:** When a witness takes a pledge in a law court and gives his testimonial in court. The pieces of evidence offered can be challenged in court and must be genuine, true, believable and admissible.

5.5.4 Digital Evidence Collection Challenges:

- Evidence must be managed with maximum care as data is stored in electronic medium and can be easily smashed.
- Volatile storage to collecting data.
- Lost data recovering.
- Ensuring the collected data reliability.

5.6 Check Your Progress

1. A distinctive sign used by business to represent its identity itself uniquely is called a ________________________ and it also identify its products and services for consumers and also used to differentiate the business and its products or other services from other businesses.
2. The term _______________________________ generally includes cybercrime activity that occurs over the Internet or email, including crimes such as identity theft, phishing and other hacking activities designed to extort people out of money.
3. BEC stands for ____.
4. Electronic Evidence is also known as ___________________ evidence.

5.7 Summary

Trademarks:

A trademark is a distinctive mark that a company uses to represent its unique identity, identify its goods and services to customers, and distinguish the company and its goods and services from those of other similar type of businesses. A trademark typically consists of a design, logo, image, name, word, phrase, symbol, or a combination of two or more of these elements.

Establishing Trademark Rights

The law treats trademarks as a form of property. By actual use in the marketplace, a trademark may establish proprietary rights in relation or by the mark registration or business mark with Office of the Trade Marks in that city jurisdiction. A trademark can be registered only if is eligible to serve the important trademark with a unique reputation of company.

Passing off Trademarks

If the trademark has not been registered by that time, common law countries, particularly in some jurisdictions, provide protection by passing unregistered trademarks to maintain business reputation. When a company is conducting business under a trade mark that has not been registered for many years and there may be a conflict between businesses that use the same or a similar mark, trademark passing is helpful.

Solutions for Trademark Breach

It resembles and equivalent to forestalling unapproved utilization of a brand name which helps the brand name proprietor. Likewise, whether a brand name is enlisted relies upon various variables, including brand name similitude, closeness of items or potentially administrations, and whether the proprietor's brand name is famous. If a trademark is registered, its owner will have an easier time proving his or her rights under the Infringement Act and trademark rights.

Types of Internet Fraud:

- Phishing and spoofing
- Data breach
- Denial of service (DoS)
- Malware
- Ransomware
- Business email compromise (BEC)

What is Electronic Evidence?

Any part of evidence which is generated by some mechanical or electronic type process can be referred to the term 'electronic evidence' used for proving or disproving any kind of fact or the evidence as information to be represent in court. Digital evidence can be used a secondary name for electronic evidence commonly. A forensic expert or person checking for electronic evidence has skills to recover any data saved in electronic devices or systems and to examine it before presenting evidence in court.

Forms of Media for Electronic Evidence

The data obtained from the following devices and applications are treated as evidence. However, this is only acceptable if retrieved using a forensic method by a certified expert.

- Computers, laptops and tablets
- Mobile phone data
- HDD, RAID and SSD hard drives
- USB memory sticks and SD cards
- Social media information
- Whatsapp messages

- Cloud storage data
- Digital photographs
- CCTV

Computer Forensics

A field of technology that uses techniques to identify for investigative purpose and store evidence from computer devices is called Computer forensics. Often, it is used to present evidence in court.

Areas outside of investigation can also be covered by Computer forensics. Sometimes we need professionals to recover deleted or lost data from failed hard drives, server computers that have stopped working or reformatted the operating systems.

Digital Forensics Tools:

Due to the wide variety of potential data sources, digital forensic tools often have different specifications. This list outlines some of the most common and widely used tools for carrying out various parts of computer forensic investigations.

- Disk analysis: Autopsy/the Sleuth Kit
- Image creation: FTK imager
- Memory forensics: volatility
- Windows registry analysis: Registry recon
- Mobile forensics: Cellebrite UFED
- Network analysis: Wireshark
- Linux distributions: CAINE

Digital Forensic Techniques:

- Reverse Steganography
- Stochastic Forensics
- Cross-drive Analysis
- Live Analysis
- Deleted File Recovery

5.8 Keywords

- Trademarks
- Internet Fraud
- Trademarks Rights
- Trademark Breach
- Electronic Evidence
- Digital Evidence
- Computer Forensics
- Digital Evidence collections

5.9 Self Assessment Test

1. Explain Trademark, Trademark rights and solutions for trademark breach.
2. What is Internet fraud and its types ?
3. What is an Electronic Evidence? Explain Forensic Technologies.
4. Process for digital evidence collection, types of collective data and types of evidence.

5.10 Answers to Check Your Progress

1. Trademark
2. Internet Fraud
3. Business Email Compromise
4. Digital

5.11 References

1. Nathan House, “The Complete Cyber Security Book” Volume-I, First edition: January 2017, published by StationX Ltd.
2. Thomas A. Johnson, “Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, CRC Press, ISBN:978-1-4822-3923-2, 2015.
3. https://www.geeksforgeeks.org/digital-evidence-collection-in-cybersecurity/
4. https://www.devry.edu/online-programs/area-of-study/technology/what-is-computer-forensics.html
5. https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools

SUBJECT: Cyber Security	
COURSE CODE: MCA-34 CHAPTER NO. 6	AUTHOR: DR. ABHISHEK KAJAL

Tools and Methods Used for Cybercrime

Password cracking, Keyloggers and spywares, Virus and worms, Phishing and identity theft, Trojan horses and backdoors, Steganography

INDEX **Page No.**

Tools and Methods Used in Cybercrime

Introduction

Password Cracking

Key loggers and Spywares

Virus and Worms

Phishing and Identity Theft

Trojan Horses and Backdoors

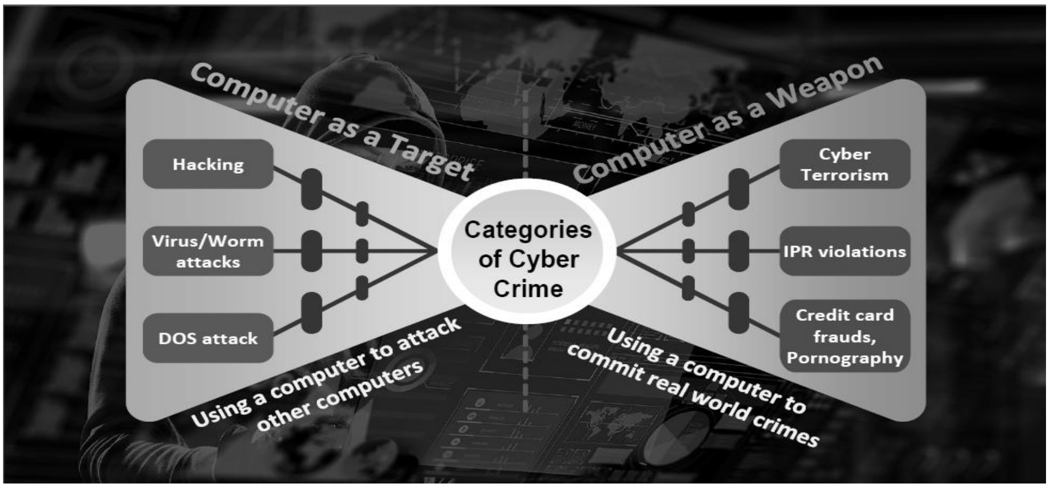
Steganography

Lesson-6

Tools and Methods Used in Cybercrime

6.1 Introduction to cybercrime

Cyber Criminal just needs a computer connected with a network to commit a crime that's called Cybercrime or a computer-oriented crime. The computer may have been used to commit a criminal activity on a target. Cybercrime uses computersystems as any weapon to commit criminal activitieslikeidentity theft, online fraud or breach of personal privacy. Through the Internet, Cybercrimehas expanded in significance as computers have turned into central point to every sector such as entertainment, business commerce and government. Cybercrime can put the security and financial health of an individual or country at risk.


Computer as a Target
Computer as a Weapon
Hacking
Virus/Worm attacks
DOS attack
Categories of Cyber Crime
Cyber Terrorism
IPR violations
Credit card frauds, Pornography
Using a computer to attack other computers
Using a computer to commit real world crimes

(Fig. 6.1)

Cybercrime covers various types of actions, except can normally be categorized into two types:

1. Criminal activities that attack on network systems of computer or system devices. Crimes of these types include various attacks (like bugs, viruses etc.) and DoS attacks - denial of service.

2. Criminal activities that make use of networks of computer to carry out further criminal actions. Those crimes types comprises of stalking in cyber, fraud of financial or stealing of identity.

6.1.1 Classification of Cyber Crime

- **Cyber Terrorism:**

  Cyber terrorism used to commit aggressive acts that might result in loss of life by using computers and the Internet. It may involve a variety of actions by software or hardware to endanger the citizens' lives.

  Overall, cyber terrorism might be treated as terrorism activitydedicatedbyuse of cyberspaceor computer resources.

- **Cyber Extortion:**

  Cyber extortion comes once any website, any server of e-mail or any system of computer is targeted or in danger by repetitiveservice rejectionor many attacks by malicious attackers. They insistto give large amount of money in given for the guarantee of preventing attacks and providing security.

- **Cyber Warfare:**

  Cyber warfare is targeting by use of computers, online control systems and networks in a war zone or in a combat context. This includes eachdefensive operation and offensive involving the cyber attacks threat, spying and disrupt.

- **Internet Fraud:**

  A kind of deceit / fraud is Internet fraud that uses the Internet and may involve concealment of data or giving false information with an aim of defrauding victims for getting money or taking property. Internet fraud doesn't consider as a single, specific criminal activity but rather encompasses a number of unlawful and illegal actions performed through cyberspace.

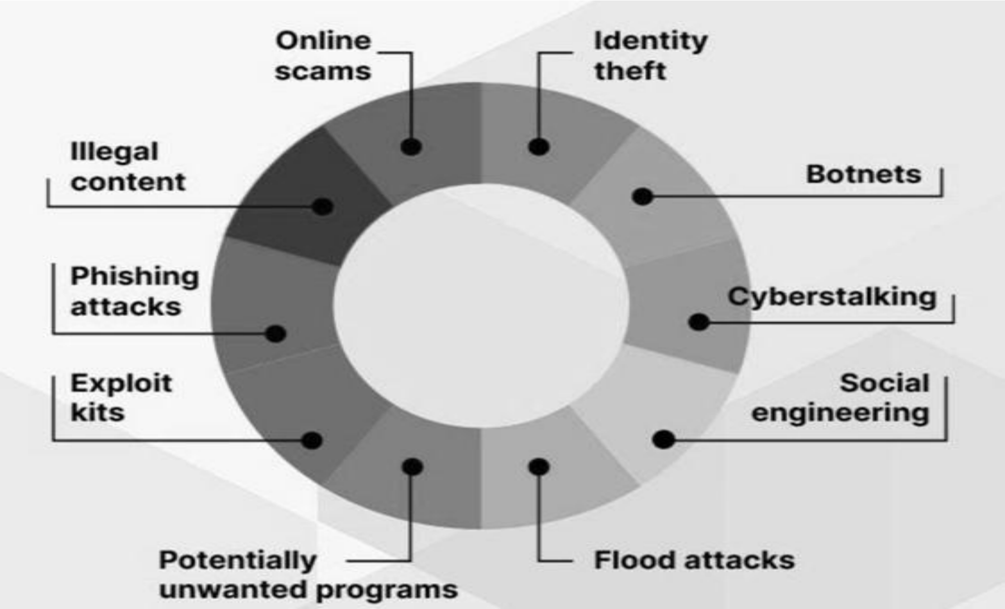
- **Cyber Stalking:**

  Cyber Stalking is a type of cyber crime in which the victim has to face a stream of text messages,emails or offended comments on social media. So these stalkers are familiar with their prey and in its place of stalking offline, they utilize Internet to chase. Yet, if they see that cyber stalking doesn't have the desired effect, they start stalking without internet as well as cyber stalking to create more problems for the lives of the victims.

6.1.2 Example of Cybercrime

Most common cybercrimes that occur:

- The fraud did by manipulating computer network
- Unauthorized access to or modification of data or application
- Intellectual property theft that includes software piracy
- Industrial spying and access to or theft of computer materials
- Writing or spreading computer viruses or malware
- Digitally distributing child pornography



(Fig. 6.2)

6.1.3 Cybercrime Attack Types

Cybercrimes can be executed by various types of attack. Here, some of the most common cybercrime attack modes are:

1. **Hacking:** It is an act of gaining unauthorized access to a computer system or network.
2. **Denial of Service Attack:** In this cyber attack the cyber criminal uses the bandwidth of the victim's network or fills his e-mail box with spam mail. Here the intent is to disrupt their regular services.

3. **Software Piracy:** The piracy of software by illegally copying genuine programs or by counterfeiting. It also includes the distribution of products for the purpose of passing for origin.
4. **Phishing:** Phishing is a technique to extract confidential information from bank/financial institutional account holders through illegal means.
5. **Spoofing:** It is the act of making a computer system or network pretending to be the identity of another computer. It is mostly used to gain access to special privileges enjoyed by that network or computer.

6.1.4 Cyber Crime Tools

There are several types of digital forensic tools.

- **Ophcrack:** This tool is mainly used to crack hashes, which are generated by the same file of Windows. It provides a secure GUI system and allows you to run on multiple platforms.
- **Kali Linux:** Kali Linux is open source software maintained and funded by Offensive Security. Digital forensics and penetration testing use this specially designed program.
- **Md5sum:** A tool to check that helps you to check whether the data has been successfully copied to another storage or not.
- **SafeBack:** To make images of the hard disks of Intel-based computer systems and restoring images to some other hard disks, SafeBack is primarily used.
- **EnCase:** To image and examine data from hard disks and removable disks an investigator is allowed by this software.
- **Data Dumper:** This is a command-line computer forensics tool. For digital forensic analysis, it can make exact copies of discs suitable and it is free to use for the UNIX operating system.

6.1.5 Prevention from Cyber Crime:

We can prevent cybercrime by following these precautions:

• Use Strong Passwords:

Always use mixed different password and username combinations with letters symbols and numbers for each account and try not to write them down. Weak passwords can be easily cracked by using some attacking methods like Brute Force Attack, Rainbow Table Attack etc, so make them complex. i.e. a combination of letters, numbers and special characters.

• Use reliable antivirus across devices:

Always use reliable and highly advanced antivirus software in mobile and personal computers. This prevents the attack of various viruses on the devices.

• Keep social media private:

Always keep the data privacy of your social media accounts with your friends. Also make sure to only make friends who know you.

• Keep your device software up to date:

Whenever you get updates for system software, update it at the same time as sometimes the previous version can be easily attacked.

• Use secure networks:

Public Wi-Fi is unsafe. Never use these networks for any financial task or corporate transactions.

• Never open attachments in spam emails:

A computer becomes infected with malware attacks and other types of cybercrime through email attachments in spam emails. Never click or open any attachment file send from unknown person.

• The software should be updated:

When it comes to internet security the operating system should be updated regularly. This can become a potential threat when cybercriminals take advantage of system flaws.

6.2 Password Cracking

Most common mechanism used for hacking is password cracking. For new entrants in the field of Cyber Security, Password cracking is the most enjoyable hacks that hikes a sense of exploration and useful in figuring out the password. Exploit use it to utilizeprograms by cracking admin or other crucial accounts password of any organization for accessing crucial information or unauthorized access of organization’s critical resources.

So, one must learn password cracking techniques to become a good ethical hacker. Some of these techniques are given below:

1. Crunch:

To hack passwords, we need to attempt many combinations of probable passwords to get the correct one. When thousands or even millions of word or combinations of character to break a passwordare used by attacker, there is no conviction, whether millions of combinations can work. This distinct combinations collection of letters is called a vocabulary and for cracking the password or hash, we must have a good quality wordlist which can crack password. So in Kali Linux there is a tool called Crunch.

2. Rainbow Crack:

Rainbow Crack is a tool using a time-memory method to break a hash of a password. Rainbow Table is used by it to crack the hash of the password. It does not use the traditional method of brute force to crack passwords. It creates possibly all plaintexts and calculates the hash accordingly. Then, it compares the hash with hash of all words in a dictionary. When it discoveranidentical hash, it resultsa hacked password.

3. Burp Suit:

The very famous web application for testing security software is Burp Suit. A proxy is used by it, so all requirementsby the web browser through the proxy bypassduring it. And as the requests pass throughout the burp suite, it gives permission to users for modifying requests according to our requirement for testing weaknesses such as XSS or SQL or any weaknessassociated with web. Burp Suite Community Edition has Kali Linux that is free software but there is also anedition of this tool which is paid calledProfessional Burp Suite with many of tools and features in comparison to Burp Suite Community Edition. It has an intrusion tool that runs automatically the procedure of passwords cracking by usinglists of words.

4. Maltego:

Maltego is a platform that has been developed to convey and put forward a clear picture of the environment of ownership and operation of an organization. Maltego provides a unique perspective for both network and resource-based entities that is the aggregation of information distributed across the Internet – whether it is the current configuration of routers on the edge of our network or any other information Maltego can detect. , could collect and visualize this information. It provides the user with unprecedented information that is leverage and power.

5. John the Ripper:

For dictionary attack or manipulated wordlist attack,exploit uses some famous brute force. For cracking passwords, a great tool can be used called John the Ripper. Even to crack hashes or passwords for zipped or compressed files and even locked files, it can also be used.There are many options available in it to crack the hash or password.

Key loggers and Spywares

6.3 Key loggers

6.3.1 Introduction to Keylogger:

Keystroke logger is also second name for**KeyLogger**, basically it is recording of key pressed on keyboard of the system and stored in a fileand this kind of file can be stored by the individual person using this types of malware. The key logger might be in the form of software or hardware.

Function: To steal password or confidential private details like details of bank account Keylogger is mainly used for this purpose.Invention of the first key logger was in the 1970s and was a key logger in hardware and development of the first software key logger was in 1983.

1. Software key loggers: Software key loggers are developed for stealing passwords from the computer of victim and these are basically computer programs. However, IT companies use key loggers to troubleshoot or solve technical issues with computers and networks in business. In addition, a key logger is also installed in Microsoft Windows 10.

- **Javascript based key loggers:**Any script of malicious code that is deployed on internet page, and saves keys such as oneKeyUp. A variety of ways can be used to sendthese scripts, such as likesocial media sharing, a file of email sending or by a RAT file.

- **Form based key loggers:**The key loggers that are activated whilethe online form is filled by a person and when to submit all the data he clicks on the button or a file is sent on computer with the written word. In the running application most of the key-loggers work as APIs, Yet a simple application and it records every key pressed on keyboard.

2. Hardware Key loggers: The hardware key loggers don't depend on any type of software as its name suggests. Keyboard hardware works as a circuit that is embedded in the keyboard and it records any key pressed in keyboard.

- **USB Key loggers:**These key loggers are USB connectors and linked to any computer to steal information or data. As well as some keyboards have predefinedcircuits without any external wires and looks like a simple keyboard.
- **Smartphone sensor:** These key loggers have some cool Android tricks for example the Android accelerometer sensor located near the keyboard just to vibrate and create sentences from any graphs.In this technology,there is about 80% accuracy.These days keystroke logging Trojan, a malware are used by crackers to send to the computer of victim for stealingdetails of data and login.

So malware or hardware is treated as a keylogger software used for stealing or to get our login details, private credentials, information related to bank and much more.

In 2020, most of keylogger applications used are:

1. Kidlogger
2. All in One Keylogger
3. Windows Keylogger
4. Best Free Keylogger
5. Refog Personal Monitor

6.3.2 Key loggers Solutions:

- **Anti-Key Logger:**Anti-key loggers are software used foridentifying the key logger from the computer system.

- **Anti-virus:**Key loggers can also be detected by many anti-virus software these anti-virus software can remove those key loggers from any computer system. Anti-virus are software therefore they might not detect or work on key loggers of hardware.
- **Form Filler Automatic:**By using the feature users can't use it to fill forms online on daily basis, in fact automatic form filler are used to protect our data from key-loggers because no key will be pressed during auto fill.
- **One-time-password:**Password can be used as OTP are secured as we a new password every time we login.
- **Pattern or mouse-detection:** Patterns are used as passwords for applications on Android devices and mouse recognition on PCs, with the program of mouse using gestures of mouse rather than a stylus.
- **Voice to Text Converter:**As in the technique we don't use keyboard we use our voice for typing text so key loggers can't detect specific part of our keyboard.

6.4 Spywares

6.4.1 Introduction to Spyware:

Cyber security has a famous breach called Spyware.Itusually makes intrusion or secretly gets downloadedinto systems of any computer, laptop or any digital device,when any user inadvertently clicks at an unidentified link or clicks a maliciousfile sent asattachment. It requires a lot of practice to choose the sites carefully to download the data on the system. Any kind of software is spyware ifthat software steals personal or business information of a user illegally without permission or approval and then sends that data to a third-party. Spyware gets inside your computer or any laptop like any hidden spy element by free version or shared version software. Pegasus spyware is the most recent example of spyware alleged to be injected in many devices belonging to VVIP personalities.

Spyware functions to maliciously track user activity, gain access to private and sensitive data, or even cause computer/laptop systems to crash. Mostly spyware operates in background process and reduces speed of the functioning of the computer system.

There are several ways a spyware can enterinto systems of the laptop/computer:

- **Phishing:** This is a form of security breach where spyware enters the system when a suspicious link is clicked or an unknown dangerous attachment is downloaded.
- **Spoofing:** This goes along with phishing and shows that the unauthorized emails have come from legitimate users or business entities.
- **Free software or shared software:** This occurs when a user installs software that is free but has additional spyware added to the system.
- **Deceptive software:** It is advertised as very beneficial to the system and will increase the speed of the system but lead to stealing of confidential information from the system.

6.4.2 Working of Spyware:

If your system has spyware then it's very dangerous for personal information, hence awareness about spyware can preservemuch reliable info from available to third parties. There are various categories of spywares according to their functionality. Many types of spywares can attack our systems.

- **Adware:** This is a type of spyware that monitors user activity and delivers advertisements based on the user's tracked activity.
- **Tracking Cookies:** This is a type of spyware that tracks user activity and supplies it to third parties.
- **Trojan:** This is a type of spyware which is the most dangerous for functioning of a device. Its purpose is to steal confidential user information such as bank details, passwords and transfer it to a third party to conduct illegal transactions or fraud.
- **Key loggers:** This is a type of spyware that keeps track of all the keystrokes that the user enters through the keyboard. This is dangerous as it contributes to brow cyber fraud where sensitive passwords can be stolen by keeping tabs on the user entering the information.
- **Stalkerware:** This is a type of spyware that is installed on a mobile phone to stalk the user. It tracks the movement of the user and sends it to third parties.
- **System Monitor:** This is a type of spyware that monitors and monitors the entire system including user activity, sensitive information, keystrokes, calls and chats. This is very dangerous for the privacy of the user.

6.4.3Prevention from Spyware

1. **Installing Antivirus/ Antispyware:**You need to install a good anti-virus if you want to protect your system against spywares, antivirus like Adware, Malwarebytes, AVG SpywareBlasterAntivirus, etc. Spyware always tends to connect to your system to steal private information. Antivirus or antispyware protects our system by filtering incoming requests and also blocks harmful threats by site blocking that steals our data/info or reveal our data to users of third-party.
2. **Beware of Cookie Settings:**Many websites can transfer our private secretdata or info along with cookies. It’s all the timerecommended to maintain checking and monitoring settings of cookies and set high security for those settings.
3. **Beware of pop-ups on websites:**Without reading, Pop-ups windows should notbe clickedby you that display on your website. It is very dangerous to accept their terms and conditions so never do that. Always without clicking 'OK' you should close the pop-up window.
4. **Never Install Free Software:**For all time be extremelycareful to install any free software on your computer system. Spyware can be included with that free software mostly and can cause problems by leaking private or confidential user data directly.
5. **Always read the terms and conditions:**Never click agree button or “Ok” without reading the terms and conditions earlier than installing software on your system. By no means, ever accept policies that violate your privacy. To protect mobile phones from spyware, Always download trustable and verified apps only from Play Store of Google or Apple.

6.5 Virus and Worms

Viruses and worms are malicious programs that self-replicate on a computer or through a computer network without the user being aware. Each subsequent copy of such malicious programs is also capable of self-replicating.

There are many Malicious files and programs that goes viral by networks or remote machines is infected when owner ordered it like backdoors or programs that make multiple duplicate copies and are incapable of self-replication are viruses. And Worms are not part of the subclass.

The main characteristic used to determine whether a program is classified as a distinct behavior within the Viruses and Worms subclasses is how the program spreads (i.e. the malicious program is transmitted through local or network resources). How does it spread copies of itself?

Most known worms are spread as files sent as email attachments, through links to web or FTP resources, through links sent in ICQ or IRC messages, through P2P file sharing networks, etc.Some worms spread as network packets. These enter the computer memory directly, and then the worm code is activated.

Worms use the following techniques to log into remote computers and launch copies of themselves: social engineering (for example, an email message suggesting a user to open an attached file), controlling network setting errors (like doing copy to a fully accessible disk), and creating loopholes in operating system and security of application.

Viruses can be divided according to the method used to infect computers:

- File virus
- Boot Sector Virus
- Macro Virus
- Script Virus

Any program within this subclass may have additional Trojan functions.

It should also be noted that many worms use more than one method to spread copies through the network. To classify these types of worms, the rules for classifying discovered objects with multiple functions should be used.

Malicious programs can have many subclasses as follows:

- Email-Worm
- IM-Worm
- IRC-Worm
- Net-Worm
- P2P-Worm

Difference Between Virus and Worm	
Computer Virus	**Computer Worm**
A program with a code that copies itself and replicates itself to other programs or files on a device can be a computer virus, which can damage or corrupt the device.	A computer worm is a separate malicious program that, upon entering the system, can begin causing harm to the device.
Needs to be started by the host, so a virus only spreads when an infected program is run on a device.	Once it getinside the device, a worm can automatically affect other programs and files. no need to execute
Few different types of computer viruses include: • Boot sector virus • Direct Action virus • Polymorphic virus • Macro virus • Spacefiller virus • Overwrite virus • File Infector virus	Few of the different types of computer worms are as follows: • Internet worms • Instant messaging worms • Email worms • File sharing worms • Internet relay chat (IRC) worms
A virus can spread when a file is opened, then when other files are opened on the host computer; the same malicious code is copied and spreads.	To enter the device, the worm only requires a medium. This can be done via email, online messaging applications, the Internet, etc.
Virus takes less time to spread in the system than worm	A worm can quickly spread through a device
A virus corrupts the files or deletes them automatically	On the other hand, a worm also affects the bandwidth and network connections of the device
Examples of computer virus include Creeper, Blaster, Slammer, etc.	Examples of computer worm include Morris worm, storm worm, etc.

Phishing and Identity Theft

6.6 Phishing

A cyber security attack that tries to gain sensitive private data such as usernames, passwords, and much more is called Phishing. It attacks the user bydirect message, email or text. Now the user opened the attachment file or link sent by the attacker then the user thinks that the message, email, text have sent from a trustful source. This is a kind of attack of social engineering. For example, the user can also get some messages saying you are a winner of lottery. When the user clicks on any link or the attachment, it activates malicious code to get your access of private sensitive information. Or that link can also be redirected to a strange different website asking for the user login details or credit card details or credentials of the bank.

6.6.1 Types of Phishing Attack:

1. Spear Phishing:

An individual person or a specific organization can be targeted by this attack for unauthorized access.Any random hacker doesn't create these types of attacks, but these attacks are developed and executed by someone who wants to steal financial details for monetary gain. As phishing attacks, spear-phishing also tends to come from a trustful source. It is well thought-out to be one of the most successful methods because both the attack (phishing attack and spear-phishing attack) is an attack using online services against the users.

2. Clone Phishing:

In this type of phishing, mostly trusted source sends email messages and its copies are used for this attack. Now hackers alter the message by adding a fake link which looks real authentic message that redirects to a malicious code or fake website to steal user data. Now, this kind of attack is sent to a large number of millions of users and the person checks to see who clicks on the link in attachment sent byemail. When user clicks on that attachment then it spreads by that link.

3. Cat Phishing:

It refers to as a social engineering attack.By using this,attacker plays with the emotions of person and develops them to get monetary gain and personal information. Sometimes attackers target peopleby showing them dating sites. This is also known as engineering hazard.

4. Voice Phishing:

Almost all attacks need a fake website for user to redirect to it, but some attacks don’t need fake websites which is known asvishing means voice phishing. Some using phishing method of caller ID hidden details to convince victim that the call comes from any trustful source. They also misuse IVRs to make situation tricky for legal system to monitor, trace, block. User's credit card numbers or some secret private data can be stolen by using it.

5. SMS Phishing:

By using this all account information of user can be revealed by the attacks. Cybercriminals use these attacks that are same like a phishing attack for stealing details of credit card or sensitive private information, pretending like appear to have come from a trusted party. Cybercriminals try to send text messages to redirect you to a fake malicious website to get personal information. Such fakewebsitesare actually looks like that ofan original websites.

6.6.2 Phishing Symptoms:

- It asks user to share the personal details like user and login details, details related to the credit card or bank.
- If the user clicks on the link sent in the email, it redirects to the website.
- If you are redirected to a website by attackers and asking certain details like the credit card details of user or banking details.

6.6.3 Preventive measures of phishing:

- Never open any doubtful email attachments.
- Never open any link that looks doubtful.
- Nevergive any sensitive info such as personal information or banking information by any of their email, text or messages.
- Always use antivirus to ensure system protection from the system.

6.7 Identity Theft

Another name for Identity Theft is Identity Fraud; it is kind of a crime that commits a lot inlarge numbers nowadays. When someone commits fraud to steal your confidential information then Identity theft occurs. This theft can be done in different ways to gather private information like info related to transactions or any other secret information carrying credentialsforperforming transactions of another person.

Example: In this corporate databases are used for getting credit card details, for this purpose thieves use different methods to get personal information about customer.Once they got the required information they can simply decrease the credit card rating of the victim. If thieves have these information and you are not informed quickly, If could be a huge loss for you. Attacker can get the credit card on the victim name as they have false credential so can apply for false loans.

6.7.1 Types of Identity Thefts:

Among many different types, here are described some common types of identity thefts:-

- **Criminal identity theft:**The victim is convinced in this theft and will suffer loss while the perpetrator or identity thief supports his job with false/fake documents like Identity proof or other documents for verification of the victim and hoax of him is successful.
- **Senior Identity Theft:**Most of the thieves make targets in the age group of 60. Thieves send information which looks real and then by using that trick they get personal information by using this trick. The superiors don’t get aware of this that he is a victimized person.
- **Driver's License ID Identity Theft:**In area of stealing Identity License of Driver identity is usually common. Because Driving License contains details like the identification number of state driver along with its name, its postal address and birth date as well. Thieves misuse this information for applying loans or for credit cards as attempt to open accounts in bank to get money or pay money forelectronic devices, vehicles, cars, homes, anything valuable, jewelry and all The fee is deducted in the name of the owner.
- **Medical identity theft:** In thistheft, a cyber criminal gathers information related to health of a victim and after that a fraudulent requirement of service of medical is madeby way of fraudulent bills, and that uses bank account details of victim for these facilities.

- **Tax identity theft:** In this, cyber criminal steals employer identification number for applying a tax refund to get money. This can be noticed and checked easily when you will try to file your return of tax or a notice for the same is sent to you by the Income Tax Return Department.
- **Social Security Identity Theft:** In this theft, cyber criminal required to recognize your SSN Social Security Network.That can be harmful to you as they will have your personal details with that number so that is considered to be a major threat for any individual.
- **Synthetic identity theft:**It is used for another theft, any cyber criminalmerges all the gathered people's details to make another new identity and usage of this identity can affect all victims of that identity.
- **Financial identity theft:**Most common type of attack is financial identity theft for money purpose.The credits stolen are used for money gains. The theft is recognized by the victim when he checks his bank balance time to time because it is done very slow theft.

6.7.2 Identity Theft Techniques:

This hack technique is used to steal identity of corporate databases for personal detailed credentials, it is little difficult and needs efforts, but because of many social-engineering methods, it's easy. Mostly used techniques related to identity theftsare:

- **Calling under the pretext:** Cyber criminals attempting on the phone to pretend to be an employee of a company to solicit financial information. Pretending to be a legitimate employee, cyber criminal asks for personal data along with some lucrative returns.
- **Mail theft:** This is a technique in which credit card information along with transactional data is extracted from public mailboxes.
- **Phishing:** This is a technique in which emails related to banks are sent to a victim with malware. When the victim replies to the mail, their information is mapped by the cyber criminals.
- **Internet:** Internet is widely used in the world because attackers are aware of many techniques to connect to public networks on the Internet that are controlled by them and they add spyware with downloads.

• **Dumpster diving:** This is a technique that has gained a lot of information from known institutions. Since garbage collectors are aware of this, they search for documents related to the account that contain Social Security numbers along with all personal documents before disposal.

• **Card Verification Value (CVV) Code Request:** The Card Verification Value number is located on the back of your debit card. This number is used to enhance the security of the transaction but many attackers ask for this number pretending to be a bank official.

6.7.3 Steps of Prevention from Identity Theft:

Many ways enhance your protection against identity theft, some most common are described as under:

1. Never tell your PIN or password with any person on the phone or offline.Make and use a strong password always.
2. Enable two-factor notifications for email.
3. Password protects all your devices.
4. Never installor download random software from internet.
5. Never postpersonal or sensitive private information on social media.
6. Never disclose your personal information over the phone.
7. While entering the password ensure its authenticity on the payment gateway.
8. Limit access to all personal information that is taken out.
9. While travelling, never disclose your personal information to strangers.
10. Make it a practice to change your PIN and password regularly.
11. Never tell your SSN no.to any person if you don't recognize/trust.
12. Please never share the Aadhaar OTP received on the phone with anyone on any call.
13. Never fill in your private information on any website whichoffersprofitof anything in return.
14. Neverwrite your all personal details on your social media website accounts publicly.
15. Finally, be the keeper of personal knowledge.

Trojan Horses and Backdoors

6.8 Trojan Horses

A type of malware that pretends itself as legitimate code or software is called a Trojan horse. After getting inside of any network, attackers will perform any act that a legal user might carry out, such as files export, modification of data, deletion of files or anything elsechanging the contents of the device. Trojans can be bundled in files for downloads of gaming, apps, tools, or software patches. Most of the attacks by Trojan take advantage of social engineering tactics in addition to spoof and phishing to signal the action to the user.

6.8.1 Trojan: Virus or Malware?

- Trojans are many times called as Trojan viruses / Trojan horse viruses, but those words are incorrect in technical prospective.Like a virus/worm, Trojan malware don't getreplicate itself or run itself. User needs to do specific actions in this.
- Trojans are malware and most likelytypes of malware, Trojans are considered for damaging files, redirectingtraffic of Internet, monitoringactivity of user, stealing sensitive private data, or setting up access points of backdoor into systems has gone. Trojans can modify, leak, delete, block or copy data, after that can be sold on the dark web to the user for ransom or back.

6.8.2 Types of Trojan Virus

Some of the most common types of Trojan viruses include:

- **Backdoor Trojan:** This type of Trojan allows hackers to remotely access and control computers, often for the purpose of uploading, downloading files or executing these automatically.
- **Exploit Trojans:** These Trojans inject a machine with code that is intentionally designed to take advantage of a weakness inherent in a specific piece of software.
- **Rootkit Trojans:** The purpose of these Trojans is to prevent the discovery of malware already infecting the system so that it can cause maximum damage.
- **Banker Trojan:** This type of Trojan specifically targets personal information used for banking and other online financial transactions.

- **Distributed Denial of Service (DDoS) Trojans:** These are programmed to carry out DDoS attacks, where a network or machine is disabled by a flood of requests originating from many different sources at a particular instance.
- **Downloader Trojans:** These are files written to download additional malware to a device, which often contain more Trojans.

6.8.3 How to Prevent Trojan Horse Attacks?

1. Never click on unwanted links or unexpected attachments downloading.
2. Apply strong, unique different passwords for devices and online accounts for all.
3. Access only HTTPS URLs websites.
4. Sign in to your email account in a new private browser tab or via the official app –which is not linked by any email or any text.
5. Any password manager should be used thatcan automatically enter already saved password into aidentified real site but not a fake site.
6. Try to use spam filters to block most fake emails messages toenter into your inbox.
7. Always turn on two-way authentication thatstops attackers to exploit and makes it difficult for them.
8. Make sure that updating software programs and Operating Systems are completed on time.
9. Regularly back up your files to restore later in the computer if any attack happens.

6.9 Backdoor

6.9.1 Introduction of Backdoor:

A backdoor is a type of hacking that takes advantage of a security flaw in a computer. Malware, bad design, or coding errors all can lead to some vulnerability, either intentionally or unintentionally. Backdoor threats are frequently used to install malware on a system or gain unauthorized access to data or systems.

6.9.2 Working of a backdoor attack:

Backdoor threats can be executed in many different ways as given below:

- By exploiting vulnerabilities known as weakness in systems security that enables unauthorized right to systems or data.

- By deploying malware on the computer system that allows attacker to take control over system.
- By misusing passwords that are stolen or cracked to get access to the system.
- By interrupting communication between users or systemsand by secretly put in these communication messages to provide the attacker right to control over the users or system.

6.9.3 Backdoor Types:

Backdoor attacks have two main types:

1. **Backdoor exploits:** Attacks of these typesidentifiesweakness in the system or application software to get illegal access. For example, a backdoor can be used to exploit afault in a program of security deployed on a computer in a corporate office of bank. This exploit willpermit attackers to break into the computer system and will drop a virus that providesoptions to control over most of online transactions of the bank.
2. **Remote Access Backdoor:**Attacks of these types provide hackers remote access to the systems which is not so easy. For example, if any hacker is not able to secretly insert messages into this data stream being sent between two users, they can send fake messages through email relays that can be downloaded to the recipients of the messages carrying suggestions like critical security updates need to be installed. Unintended users will store and deploy this update that installs malware providing attackers access to the systems remotely.

6.9.4 Purpose to do backdoor attacks:

There are many reasons for which cybercriminals can use backdoor threats:

- **Data theft or fraudulent transactions:** Backdoor attacks can be executed for stealing sensitive private information or any systems, such as records of customer or databases of transaction. To target individuals or organizations, these sensitive data can be used in fraudulent activities sold on the black market.
- **Installing spyware or key loggers**: Hackers can take efforts for stealingprivate sensitive papers or other document files from computers they have negotiated, by deployingsecretedinvestigation tools such as key loggers and spyware. To perform identity

theft or other crimes related to financial, they may also capture and gather passwords and other sensitive private information or data.

- **Denial of Service:** To launch denial of service (DoS) attacks,Backdoor threats can be against systems or organizations. In attempt to make a system unavailable a DoS attack is used at users by over-flooding them with massive amount of requests so that it cannot reply to genuine requests. For example, to disrupt any online services.

6.9.5 How to prevent backdoor attacks:

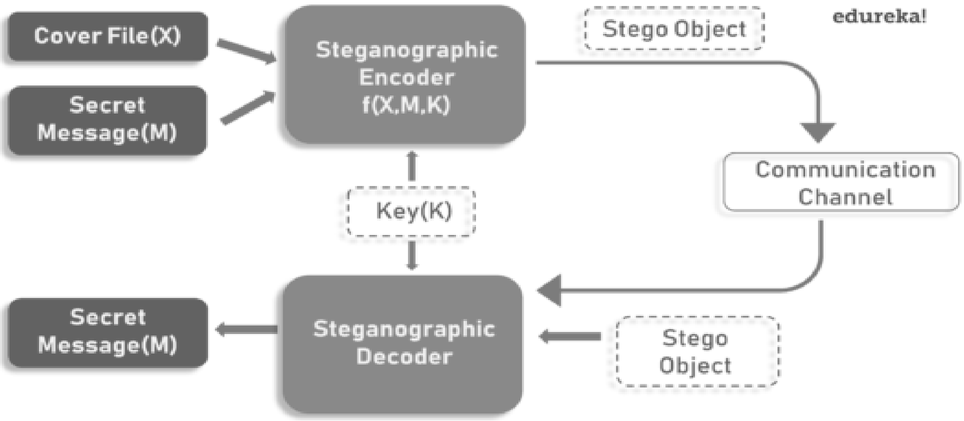
Backdoor threats can be prevented by different ways:

- Update system and with the most recentpatches of security.
- Cautiously manage accounts or permissions of user.
- Use a policy that makes password strong.
- On all systems, set up antivirus and software for malware protection.
- Monitor traffic of network for activity which is doubtful and other signs that indicated a possible attack.

Steganography

6.10 Steganography

Steganography is the art and science of embedding secret messages into a cover message in such a way that no one other than the sender and intended recipient suspects the existence of the message.



(fig. 6.1)

As the image shows, both the cover file (X) and the secret message (M) are fed into the steganographic encoder as input. The steganographic encoder function, f(X,M,K) embeds the secretmessage into a cover file. The resulting Stego object looks identical to your cover file, with no visible changes. This completes the encoding. To retrieve the secret message, a stego object is fed into the steganographic decoder.

Steganography is the technique of hiding secret data in a simple, non-secret, file or message in order to avoid detection; Secret data is extracted at its destination. The word steganography is derived from the Greek word steganos (meaning to hide or cover) and the Greek root graph (meaning to write). Steganography can be used to disguise almost any type of digital content, including text, image, video or audio content; Concealed data can be hidden inside almost any other type of digital content.

6.10.1 History of Steganography

Steganography is the practice of hiding a secret message behind a general message. It is composed of two Greek words, which are steganos, which means to cover and graphia, which means to write. Steganography is an ancient practice, practiced in various forms for thousands of years to keep communication private. For example:

- The first use of steganography dates back to 440 BC during times of ancient Greece, when people wrote messages on wood and covered it with wax, which acted as a covering medium.
- The Romans used various forms of invisible ink; light or heat were used to decipher the hidden messages
- During World War II the Germans introduced microdots, which were complete documents, drawings and plans that were reduced in size to the size of a point and were attached to general paperwork
- Null ciphers were also used to hide unencrypted secret messages in an innocent-looking generic message

6.10.2 Steganography Today:

Modern digital steganography involves first encrypting or hiding the data in some other way, and then embedding a special algorithm into the data, which is part of a specific file format like a JPEG image, audio, or video file. Simple data files can contain secret messages in a variety of ways. In an image file, one method is to conceal the data using bits that represent rows of identical color pixels. By applying the scrambled information to this excess information in some fluffy manner, the outcome will be a picture record that seems to be indistinguishable from the first picture however contains "commotion" examples of normal, decoded information.

Steganography is often used to add a watermark, which is a trademark or other identifying data that is hidden in multimedia or other content files. Online publishers frequently use watermarking to trace the origin of media files that have been shared without permission.

6.10.3 Difference between Steganography and Cryptography

	STEGANOGRAPHY	CRYPTOGRAPHY
Definition	It is a technique to hide the existence of communication	It’s a technique to convert data into an incomprehensible form
Purpose	Keep communication secure	Provide data protection
Data Visibility	Never	Always
Data Structure	Doesn’t alter the overall structure of data	Alters the overall structure of data
Key	Optional, but offers more security if used	Necessary requirement
Failure	Once the presence of a secret message is discovered, anyone can use the secret data	If you possess the decryption key, then you can figure out original message from the ciphertext

In simple words, when anyone wants to send crucial secret personal information, steganography is more reliable than cryptography. The downside is that if the secret's presence is discovered it is easier to extract the hidden message.

6.10.4 Steganography Techniques

Depending on the nature of the cover objects (actual object in which secret data is embedded), steganography can be divided into five types:

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

1. Text Steganography

Text steganography is hiding information inside text files. This includes things like changing the format of existing text, replacing words within text, generating random character sequences, or using context-free grammar to generate readable text. The different techniques used to hide data in text are:

- Format Based Method
- Random and statistical generation
- Linguistic Method
- Image Steganography

2. Image Steganography

Hiding the data by taking the cover object as an image is known as image steganography. In digital steganography, images are widely used as cover source because a large number of bits are present in the digital representation of an image. There are several ways to hide information inside an image:

- Least significant bit insertion
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and scatter
- Coding and Cosine Transformation

3. Audio Steganography

In audio steganography, the secret message is embedded in an audio signal that transforms the binary sequence of the associated audio file such as WAV, AU and even MP3 sound files.

Different methods of audio steganography include:

- Least significant bit encoding
- Parity Encoding
- Phase Coding
- Spread spectrum

4. Video Steganography

In video steganography you can hide a type of data in a digital video format. A large amount of data can be hidden inside and the fact that it's a moving stream of lots of images and sounds. The two main classes of video steganography include:

- Embedding data in raw video which is uncompressed and compressing it later
- Embedding the data directly into the compressed data stream

5. Network Steganography (Protocol Steganography)

It is a technique of embedding information within a network control protocol used in data transmission such as TCP, UDP, ICMP, etc. You can use steganography in some of the covert channels you can find in the OSI model.

6.10.5 Steganography Tools:

There are a lot ofsoftwares available that provide steganography. Some provide generic steganography, but some provide encryption before data hiding. These are the steganography tools that are available for free:

• Java is used to write a free steganography tool called**StegoSuite**. By using Stegosuite you can easily hide secret private information in image files.

• **StegHide** is open source steganography software that lets you hide a secret file in an image or audio file.

- **Geo Steganography** is free software that can be used to hide data in BMP images or WAV files.
- **SSuitePicsel** is another free portable application for hiding text inside an image file but it takes a different approach than other tools.
- **OpenPuff** is a professional steganographic tool where you can store files as image, audio, video or flash files

Well, these are some of the tools for doing steganography.

6.11 Check Your Progress

1. ____________________is a type of fraud or deceit that uses the Internet and may involve concealment of data or giving false details with an aim of defrauding victimized persons for getting money or taking property.
2. __________________ is an act of gaining unauthorized access of a computer system or network.
3. _________________is a technique to extract confidential information from bank/financial institutional account holders through illegal means.
4. Basically, ______________________ is recording of key pressed on keyboard of the system and stored in a file, and this kind of file can be stored by the individual person using these types of malware.
5. There are many Malicious files and programs that goes viral by networks or remote machines is infected when owner ordered it like backdoors or programs that make multiple duplicate copies and are incapable of self-replication are _________________________.
6. A computer _____________________ is an independent malicious program, which when enters a system can start causing harm/damage to the device.
7. ________________________________is a crime that is being committed in large number nowadays, when someone commit fraud to steal your confidential information then Identity theft too occurs.

8. A type of malware that pretends itself as legitimate code or software is called a__________________________________
9. A kind of hacking is known as a ________________________ that takes benefit of weakness of security system in computer. Some weaknesses can be caused by poor design, coding errors, or malware intentional or unintentional.
10. ______________________________is the technique of hiding secret data in a simple, non-secret, file or message in order to avoid detection; Secret data is extracted at its destination.

6.12 Summary

About Cyber Crime:

Cyber Criminal just needs a computer connected with a network to commit a crime that’s called Cybercrime or a computer-oriented crime. The computer may have been used to commit a criminal activity on a target. Cybercrime uses computer systems as any weapon to commit criminal activities like identity theft, online fraud or breach of personal privacy. Through the Internet, Cybercrime has expanded in significance as computers have turned into central point to every sector such as entertainment, business commerce and government. Cybercrime can put the security and financial health of an individual or country at risk.

Classification of Cyber Crime:

- Cyber Terrorism
- Cyber Extortion
- Cyber Warfare
- Internet Fraud
- Cyber Stalking

Example of Cybercrime:

Here, are some most commonly occurring Cybercrimes:

- The fraud did by manipulating computer network
- Unauthorized access to or modification of data or application
- Intellectual property theft that includes software piracy

- Industrial spying and access to or theft of computer materials
- Writing or spreading computer viruses or malware
- Digitally distributing child pornography

Cybercrime Attack Types

- Hacking
- Denial of Service Attack
- Software Piracy
- Phishing
- Spoofing

Cyber Crime Tools:

- Ophcrack
- Kali Linux
- Md5sum
- SafeBack
- EnCase
- Data
- Dumper

Prevention from Cyber Crime:

- Use Strong Passwords
- Use reliable antivirus across devices
- Keep social media private
- Keep your device software up to date
- Use secure networks
- Never open attachments in spam emails
- The software should be updated

Password Cracking:

Most common mechanism used for hacking is password cracking. For new entrants in the field of Cyber Security, Password cracking is the most enjoyable hacks that hikes a sense of exploration and useful in figuring out the password. Exploit use it to utilize programs by cracking admin or other crucial accounts password of any organization for accessing crucial information or unauthorized access of organization's critical resources.

Although passwords are easy to crack using only guessing techniques.

- Crunch
- Rainbow Crack
- Burp Suit
- Maltego
- John the Ripper

Key Loggers:

Keystroke logger is also second name for **Key Logger**, basically it is recording of key pressed on keyboard of the system and stored in a file and this kind of file can be stored by the individual person using this types of malware. The key logger might be in the form of software or hardware.

Function: To steal password or confidential private details like details of bank account Key logger is mainly used for this purpose. Invention of the first key logger was in the 1970s and was a key logger in hardware and development of the first software key logger was in 1983.

- **Software key loggers**
- **Hardware Key loggers**.

Prevention from Key loggers:

- Anti-Key Logger
- Anti-virus
- Automatic Form Filler
- One-time-password
- Pattern or mouse-detection
- Voice to Text Converter

Introduction to Spyware

Cyber security has a famous breach called Spyware. It usually makes intrusion or secretly gets downloaded into systems of any computer, laptop or any digital device, when any user inadvertently clicks at an unidentified link or clicks a malicious file sent as attachment. It requires a lot of practice to choose the sites carefully to download the data on the system. Any kind of software is spyware if that software steals personal or business information of a user illegally without permission or approval and then sends that data to a third-party. Spyware gets inside your computer or any laptop like any hidden spy element by free version or shared version software. Pegasus spyware is the most recent example of spyware alleged to be injected in many devices belonging to VVIP personalities.

How does spyware enter a computer system?

- Adware
- Tracking
- Cookies
- Trojan
- Key loggers
- Stalkerware
- System Monitor

How to Prevent Spyware?

1. Installing Antivirus/ Antispyware
2. Beware of Cookie Settings
3. Beware of pop-ups on websites
4. Never Install Free Software
5. Always read the terms and conditions

Viruses and Worms:

Viruses and worms are malicious programs that self-replicate on a computer or through a computer network without the user being aware. Each subsequent copy of such malicious programs is also capable of self-replicating.

The main characteristic used to determine whether a program is classified as a distinct behavior within the Viruses and Worms subclasses is how the program spreads (i.e. the malicious program is transmitted through local or network resources). How does it spread copies of itself?

Worms use the following techniques to log into remote computers and launch copies of themselves: social engineering (for example, an email message suggesting a user to open an attached file), controlling network setting errors (like doing copy to a fully accessible disk), and creating loopholes in operating system and security of application.

Phishing:

A cyber security attack that tries to gain sensitive private data such as usernames, passwords, and much more is called Phishing. It attacks the user by direct message, email or text. Now the user opened the attachment file or link sent by the attacker then the user thinks that the message, email, text have sent from a trustful source. This is a kind of attack of social engineering.

Types of Phishing Attack

- Spear Phishing
- Clone
- Phishing
- Cat Phishing
- Voice Phishing
- SMS Phishing

Preventive measures of phishing:

- Never open any doubtful email attachments.
- Never open any link that looks doubtful.
- Never give any sensitive info such as personal information or banking information by any of their email, text or messages.
- Always use antivirus to ensure system protection from the system.

The user should always have an antivirus to ensure that the system is not affected by the system.

Identity Theft:

Another name for Identity Theft is Identity Fraud; it is kind of a crime that commits a lot in large numbers nowadays. When someone commits fraud to steal your confidential information then Identity theft occurs. This theft can be done in different ways to gather private information like info related to transactions or any other secret information carrying credentials for performing transactions of another person.

Types of Identity Thefts:

- Criminal identity theft
- Senior Identity Theft
- Driver's License ID Identity Theft
- Medical identity theft
- Tax identity theft
- Social Security Identity Theft
- Synthetic identity theft
- Financial identity theft

Identity Theft Techniques:

This hack technique is used to steal identity of corporate databases for personal detailed credentials, it is little difficult and needs efforts, but because of many social-engineering methods, it’s easy. Mostly used techniques related to identity thefts are

- Calling under the pretext
- Mail theft
- Phishing
- Internet
- Dumpster diving
- Card Verification Value (CVV) Code Request

Trojan Horses:

A type of malware that pretends itself as legitimate code or software is called a Trojan horse. After getting inside of any network, attackers will perform any act that a legal user might carry out, such as files export, modification of data, deletion of files or anything else changing the contents of the device. Trojans can be bundled in files for downloads of gaming, apps, tools, or software patches. Most of the attacks by Trojan take advantage of social engineering tactics in addition to spoof and phishing to signal the action to the user.

Types of Trojan Virus:

Backdoor Trojan

Exploit Trojans

Rootkit

Trojans

Banker Trojan

Distributed Denial of Service (DDoS) Trojans

Downloader Trojans

How to Prevent Trojan Horse Attack?

1. Never click on unwanted links or unexpected attachments downloading.
2. Apply strong, unique different passwords for devices and online accounts for all.
3. Access only HTTPS URLs websites.
4. Sign in to your email account in a new private browser tab or via the official app – which is not linked by any email or any text.
5. Any password manager should be used that can automatically enter already saved password into a identified real site but not a fake site.
6. Try to use spam filters to block most fake emails messages to enter into your inbox.
7. Always turn on two-way authentication that stops attackers to exploit and makes it difficult for them.
8. Make sure that updating software programs and Operating Systems are completed on time.
9. Regularly back up your files to restore later in the computer if any attack happens.

Introduction of Backdoor:

A backdoor is a type of hacking that takes advantage of a security flaw in a computer. Malware, bad design, or coding errors all can lead to some vulnerability, either intentionally or unintentionally. Backdoor threats are frequently used to install malware on a system or gain unauthorized access to data or systems.

BackDoor Types:

Backdoor exploits: Attacks of these types identifies weakness in the system or application software to get illegal access.

Remote Access Backdoor Attacks of these types provide hackers remote access to the systems which is not so easy.

Purpose to do backdoor attacks:

- Data theft or fraudulent transactions
- Installing spyware or key loggers
- Denial of Service

How to prevent backdoor attacks:

Backdoor threats can be prevented by you or company by these several different ways:

- Update system and update with the most recent patches of security.
- Cautiously manage accounts or permissions of user.
- Use a policy that makes password strong.
- On all systems, set up antivirus and software for malware protection.
- Monitor traffic of network for activity which is doubtful and other signs that indicated a possible attack.

Steganography:

Steganography is the art and science of embedding secret messages into a cover message in such a way that no one other than the sender and intended recipient suspects the existence of the message.

Steganography Techniques

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

6.13 Keywords

- Cyber Crime
- Password Cracking
- KeyLogger
- Spyware
- Virus
- Worm
- Trojan Horse
- Phishing
- Phishing Identify Theft
- Trojan Viruses
- Malware
- Backdoor attacks
- Steganography

6.14 Self Assessment Test

1. What is a cyber crime? Explain it's types, tools and preventions.
2. Explain Key Logger and how we can be protected our system from KeyLogger?
3. What is spyware? Write about spyware prevention.
4. What are the differences between Viruses and Worms?
5. Describe Phishing, It's types, symptoms and How to avoid phishing?
6. What is identity theft? Write it's type, techniques and prevention?
7. Write about Trojan horse, it's types and prevention.
8. What do you mean by backdoor? Explain types of backdoor and how to stop backdoor attack?
9. Meaning of Steganography, It's techniques and tools?

6.15 Answers to Check Your Progress

1. Internet fraud
2. Hacking
3. Phishing
4. KeyLogger
5. Viruses
6. Worm
7. Identity Theft
8. Trojan horse
9. Backdoor
10. Steganography

6.16 References

1. Nathan House, “The Complete Cyber Security Book” Volume-I, First edition: January 2017, published by StationX Ltd.
2. Thomas A. Johnson, “Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, CRC Press, ISBN:978-1-4822-3923-2, 2015.
3. https://www.edureka.co/blog/steganography-tutorial
4. https://www.techtarget.com/searchsecurity/definition/identity-theft
5. https://www.crowdstrike.com/cybersecurity-101/malware/trojans/

SUBJECT: Cyber Security	
COURSE CODE: MCA-34 CHAPTER NO. 7	AUTHOR: DR. ABHISHEK KAJAL

Cyber Laws

(Cyber crime and legal landscape around the world, Cyber laws, The Indian IT Act 2000, Challenges, Digital signatures and Indian IT Act, Amendments to the Indian IT Act)

INDEX **Page No.**

Cyber Crime

Cyber Crime and Legal Landscape around the World

Cyber Laws

The Indian IT Act

Challenges

Digital Signatures and Indian IT Act

Amendments to the Indian IT Act

Lesson-7

(Cyber crime and legal landscape around the world, Cyber laws, Indian IT Act 2000, Challenges, Digital signatures and Indian IT Act, Amendments to the Indian IT Act)

Cyber Crimes and Cyber Security

7.1 Introduction to Cyber Crime and Cyber Security

The term "cybercrime" refers to any illegal behavior that is carried out over internet. It is known as the crime that is executing with the assistance of computer system,digital devicesand internet. Cyber crime may be targeted against an individual or group; it can also be committed against private organizations and the government as well. It can cause various kinds of damage like monetary loss, mental harm, physical harm or even one's reputation. It has posed a big threat to internet users by stealing information from millions of users in past years. It has also caused a huge dent in the global economy.

Cyber security is a technology or activity that helps to prevent and defend against cyber crimes.Cyber Security techniques assist any person or group to be protected from any kind of harm caused by anycyber crime. Overall it is a technique of securing your data, system or any kind of intellectual property. According to Gartner, the global demand for Cyber Security is expected to hit $170.4 billion by 2022. 95% of Cyber Security violations occur because of human error, according to Cybint.

7.1.1 Cyber Crime:

Whoever the victim is, cyber crime can cause direct or indirect harm. However, the biggest threat of cyber crime can be an individual with the government and the financial security. Cyber crime can be the biggest threat to financial and business companies and cause billions of USD in damages every year.

7.1.2 Cyber Crime Types:

Some types of cyber crime are given below:

- **Hacking**

An illegal activity used by a hacker tobreach any system security of computer users to steal crucial and personal information.

- **Improper crowd surveillance**

  A large part of a group of people with Surveillance by authority mainly for purpose of security is called mass surveillance.But it is considered as cyber crime, if one does so for personal interests.

- **Child pornography**

  One of the most horrific crimes is child pornography and it is openly practiced around the globe. Children are abused sexually and videos recorded to upload on the websites.

- **Hair Grooming**

  Child grooming is the illegal activity of creating an emotional connection with a child, mainly for child prostitution and child-trafficking purpose.

- **Copyright violation**

  If anyone's private data or secured copyrighted material is used or misused by someone without permission; and published that material in own name of him, is called as copyright infringement.

- **Money laundering**

  An individual or organization has Illegal possession of funds is called laundering of money. Such cyber crime takes transfer of funds via banks of foreign countries and/or business that are legitimate. In other words, this is the activity of illegally converting money earned into a financial system legitimately.

- **Cyber Extortion**

  Cyber extortion is crime when hacks by a hacker into anyone's computer system or server and money demanding as ransom to restore the system, that’s called as cyber extortion.

- **Cyber Terrorism**

  When any person hacks the system security of the government or frightens the government or a large organization, it is known as cyber terrorism.It’s executed for social or political purposes by hacking the system security usually via network of computer of utmost importance for any group or state.

7.1.3 Cyber Security:

The potential activity that protects information and other communication systems and/or protects data from unauthorized access or exploitation or modification or even theft is called Cyber Security. In general,a well-designed method to secure networks, personal data, computers, various programs etc. from unauthorized use is called Cyber Security.

Data of any type whether government, corporate, or personal, or data related to the defense system, research, banks ororganization development are very crucial.A slight alteration or unauthorized access of such data can cause big harm to the entire country. So a high level of security is required for all such type of sensitive data.

7.1.4 Techniques to secure data:

You need to pay attention for these important things to make your system security much stronger:

- Architecture Security
- Process of Safety assessment
- Backup and restore procedures
- Security policies
- Risk assessment process
- Network diagram
- Risk management policy
- Disaster recovery plan

Cyber Crime and Legal Landscape around the World

7.2 Cyber Crime and Legal Landscape

Cyber law is a term used to describe the legal aspects in concern to use of technology, specially "cyberspace", i.e. the Internet. Laws related to information crime, internet crime, computer crime, technology crime and communication crime are included in Cyber crime legal law. For criminal activity, Internet and digital economy shows an important opportunity. Offenses and punishments for cyber crimes are created by the cyber crime laws. In essence, cyber law is an attempt to handle the challenges presented by human activities on the Internet with legacy system of laws applicable to the physical world.

Cyber crime states:

- Computers, data or information communication technologies related offenses.
- People using computers or ICTs committed to crimes.

A global problem called Cyber crime in which a coordinated international response is required. Regulatory requirements rising from cyber laws are complied with some organizations.

7.2.1 Legal Actions against Cyber Crime:

- To align your compliance with the Act, try to take practical steps by joining Cyber crime Law Program.
- By attending online workshop on the Cyber Crime Act try to understand how the Act affects your organization.
- On your organization, try to find to help in determining the impact of cyber crimes and follow the steps by taking an assessment of online cyber crime impact.
- By reading simple language summary on the Cyber Crime Act try to get an overview and you can also download it.
- By reading about it online or by downloading about it, try to know what is in the Cyber Crime Act.
- By asking opinions of legal interpretation of the law, try to learn how the law applies to you.
- By reading about the practical impact on different organizations and people, try to determine the impact of cyber crimes on your organization.
- By telling board of directors about cyber crimes risks and the legal implications for your organization, try to enable website notifications to fulfill their duties.
- By getting help try to comply with regulatory requirements, If you are an ECSP or Financial Institution.

- Try to defend yourself by asking opinions of legal advisers whether you have committed a cyber crime and what are your chances of being convicted, If you have been accused of committing a cyber crime (or are allegedly being prosecuted),.
- Try to compliant with cyber crime law by getting advice and assistance to make sure your incident responded.
- By training your employees about cyber crimes, try to keep your employees and the CEO out of jail.
- By finding advices on the law relating to electronic evidence, try to make sure you can accept cyber crime records and evidence.
- By subscribing to the newsletters, try to receive future updates or alerts about the Cyber crime Act.

7.2.2 Models of cyber crime law:

- **CW Model Law**: Computers and Computer Related Crime Model Law.
- **SADC Model Law**: Computer Crime and Cyber crime SADC Model Law
- **HIPCAR**: Harmonization of ICT Policies, Legislation and Regulatory Processes in the Caribbean (Cyber crime / E-Crime)
- **ITU:** International Telecommunication Union Cyber crime Law Resource - ITU Toolkit for Cyber crime Law

7.2.3 Some specific cyber crime laws: There are many countries who follows cyber crime laws for cyber security and integrity.

Africa:

- **Botswana** - Cyber crimes and computer related crimes
- **South Africa**
    - Cyber Crime Act 2021 - South Africa
    - NCPF - National Cyber Security Policy Framework
- **Tanzania** - Cyber Crime Act 2015

America:

- **United States of America**

  - CISA - Cyber Security Information Sharing Act
  - United States code
- **Brazil** stipulates internet act to store personal data and private communications complied by connection and application providers with certain security standards.

Canada:

- PIPEDA - A privacy statute called The Personal Information Protection and Electronic Documents Act, SC 2000 that establishes two central cyber security obligations in Canada for private sector organizations.

Asia Pacific:

- **Australia**
  - APP – Australian Privacy Principles include information security obligations under the Privacy Act 1988.
  - Australian Cyber crime act 2001
- The Computer Abuse Act, 2007 in **Brunei Darussalam**
- Laws governing cyber crimesin **China**:
  - Cyber Security Act 2016
  - The data protection law September 2021 of the People's Republic of China.
- Laws for cyber security in **India**:
  - Information Technology Act 2000
  - The Information Technology Rules, 2011 (Sensitive Personal Data or Information Reasonable Security Practices and Procedures).
  - Companies Act of 2013
  - National Institute of Standards and Technology (NIST) Compliance.
- The central law governing cyber security **is b**asic Act on Cyber Security in **Japan**.
- Computer Crimes Act in **Malaysia**.
- The Cyber Crime Prevention Act 2012 in **Philippines**.
- Act on computer crimes in **Thailand**.
- Information Privacy Principle 5 under the Privacy Act 2020 in **New Zealand**. The Crime Act, 1961 also contains provisions related to cyber crimes.

Europe:

- Law of Network and Information Security.
- Criminal Code in **France.**
- Computer Abuse Act 2013 in **UK**

Middle East:

- Laws and regulations covering various types of cyber security in Israel such as:
    - Privacy law Protection
    - Privacy Rules Protection (Data Protection)
- **Jordanian** laws are only in Arabic:
    - Cyber Security Law 2019
    - Cyber Crime Law 2015
- Law on the use of information communication technology in **Saudi Arabia** in government agencies (only in Arabic)

Cyber Laws

7.3 Cyber Laws of India

Illegal act in which computer has a device or target or both that refers to Cyber Crime. In natural way Criminal activities are included in cyber crimes like fraud, theft, forgery, mischief and defamation, Indian Penal Code has control over the entire subject related to it. New age crimes are increased because of the misuse of computers that makes need of introduction of new law to punish the cyber criminals, i.e. Information Technology Act 2000.

We can classify cyber crimes in two ways:

- **Target Computer:** To attack other computers need to use a computer.

  For hacking, attack of virus/worm, dos attack etc.
- **A Weapon using Computer:** To Commit Crimes Using Computers in the true World.

  Such as IPR violation, cyber terrorism, EFT fraud, pornography, credit card fraud etc.

IT law also refers to Cyber law, the law which is related to information-technology, involving internet networks and computers. It handles with legal informatics laws and takes care of the software, information security, digital movement of information and e-commerce.

Although intellectual property is a key component of IT law, it is not considered a separate area of law. Instead, IT law covers intellectual property-related agreements, privacy, and data protection laws. Regarding software licensing, the field is contentious and still growing in Europe and elsewhere.

7.3.1 Cyber Law Importance:

- All transactions on the Internet are covered in it.
- All the activities on the Internet are monitored in it.
- Every action and every reaction is reached by it in cyberspace.

7.3.2 Need of Cyber Law in India:

From the time any user register his Domain Name, to the time setting up website, to the time promote website, to the time when send and receive emails , to the time conduct electronic commerce transactions on the said site, at every point of time, there are various Cyber law issues involved. Cyberlaw is a word by which legal issues are defined, the issues related to communications technology use, specifically "cyberspace", it means the Internet. Indeed, cyber law treats like a link to protect the challenges created by human activity on the Internet by laws applicable to the physical world with the traditional system.

The people who started the Internet were speculating at the time about whether or not the Internet could become a major revolution that could be turned against law enforcement and criminal activity. Today, numerous troubling events are taking place online. Different kinds of criminal activity are common on the Internet because of its strange nature, and intelligent people are increasingly using the Internet for criminal purposes in cyberspace. As a result, cyber law is in high demand in India.

7.3.3 Areas of Cyber Law:

Laws in Cyber world have a variety of different-different goals. How individuals and organizations or companies can utilize computers and the Internet are some laws govern, while others save people not to be victims of crime using unethical activities on the Internet. Cyber law key areas include:

- **Fraud:** Cyber laws are needed to defend consumers from online fraud. These Laws are created to stop credit card theft identity theft and crimes related to financial online. A person could face federal or state criminal charges, who are committing identity theft. Civil action brought by the victim can also be faced by them. Cyber lawyers work using the Internet to defend as well as prosecute allegations of fraud.
- **Copyright:** Copyright infringement is easy due to use of the Internet. Copyright infringement was very easy in the early days of online communication. To take action for copyright protection, attorneys are required by both companies and individuals. To protect individual person's rights and rights of companies, copyright violation is a cyber law area to make profit from their creative works.
- **Defamation:** The Internet is used by many employees to express their mind. Many things are not true when people try to say through internet, that can be beyond the border line into defamation. To protect individuals to make fake or false public statements civil laws came into existence that are called Defamation laws as well. Those fake statements can cause big problems and can damage a business or reputation of someone. When to make statements people use the Internet which violates civil laws, it is known as defamation law.
- **Harassment and stalking:** Those criminal laws are forbid harassment for online statements that can violate. When threatening statements are created by a person repeatedly about any person else online, this violates both civil and criminal laws. Doing this using the Internet and any other type of electronic communication, cyber lawyers prosecute and defend people.
- **Freedom of Speech:** Cyber law has an essential area called Freedom of expression. Whether cyber laws protect and stop some certain behaviors online, but people can speak free mind online due to freedom of speech laws. People should know the limits of freedom of expression including prohibiting laws about pornography and Cyber lawyers should advise clients. Even if there is a debate and their actions are acceptable free speech but cyber lawyers can defend their clients.
- **Trade Secrets:** To protect trade secrets and privacy, companies often depend on cyber laws while doing online business. For example, many companies like Google and search engines of other websites invest lot of time for developing algorithms for generation of search results.

- **Contract and Employment Law:**Most of the time using a website there is always a button to click to agree to the terms and conditions of that website, It means cyber Law is applied. To deal with privacy concerns every website have terms and conditions in one way or different types of ways.

7.3.4 Benefits of Cyber Laws:

To deal with cyber crimes, many outdated laws are replaced with the IT Act 2000 which provides solutions. Such laws are essential for people so that they can do online purchase or transactions without any fear of misuse while using their credit card. The Act offers a legal framework for legal effect, validity or enforceability don't get deprived for information merely on the ground whether that information is in the form of an electronic record.

These days, transactions and communication by electronic records are more often and online, the Act finds empower government departments for acceptance of the filing, creation and maintenance for official documents in digital type format. By using digital signatures, the Act applied a legal framework for authentication and origination of electronic records/communications.

- The IT Act 2000 and its rules and laws have positive aspects if we see by the point of view of e-commerce in India. First, in our country, applicability of these laws for e-businesses email is allowed as a valid and legal form of communication that can be duly presented in a court of law and approved.
- The Act provided a legal infrastructure by using that companies are able to do electronic commerce.
- The Act has provided sanction and legal validity to digital signatures.
- This act issues Digital Signature certificates for the corporate companies in the business of being the Certifying Authority.
- The Act now issues notifications on an e-governance web portal and that allows the government to access it.
- By using the Act companies are able to file any form, application or any other document related to any office, body, authority or agency created or controlled by appropriate government enabled any office, body, authority or agency in electronic form by such electronic form.

- For the success of electronic transactions critical security issues are very important which are also addressed by IT Act. Thus a legal definition has given to the concept of digital signature security that goes through a process of system security guided by the government at a later date.
- If anyone breaks into computer system of any company or networks to damage copies of data then under the IT Act, 2000, Company or corporate can take legal action against that person using this law. If there is any kind of monetary damages then penalty given by the Act can be up to Rs. 1 crore.
- Hardware security as well as software security, both are provided by Cyber law.

The Indian IT Act

7.4 The Indian IT Act

The IT Act is referred to as the Information Technology Act, 2000. The Indian Parliament created and reported on this Act on 17 October 2000. By a resolution on January 30, 1997, General Assembly of the United Nations suggested UNCITRAL Model (the United Nations Model Law on Electronic Commerce 1996) on which this Information Technology Act is based. To deal with cyber crime and e-commerce in India, IT Act is most important.

The main goal of this IT act is to perform legitimate, reliable electronic, online digital transactions to prevent and decrease rate ofcyber crimes. This IT Act consists of 13 chapters with 90 sections. These sections begin with 'Section 91 - 94' i.e. last four sections deal with amendments in the Indian Penal Code (1860).

This IT Act 2000 contains two types of schedules:

- The Act will not apply to these related documents - **First Schedule**.
- An electronic signature or electronic authentication method related to it- **Second Schedule**.

7.4.1. Offenses and Penalties in IT Act 2000:

The IT Act, 2000 covers the following offenses and punishments under:-

a. Computer source documents tampering.
b. When an electronic form of information is published.
c. To decrypt the information, the controller's instructions to a client to extend the facilities.

d. Hacking for malicious purposes.
e. Penalties for breach of private confidential data or files online.
f. Penalty for misrepresentation.
g. False digital signature certificate for publishing is covered by a penalty.
h. Right and power to investigate offences.
i. System protection.
j. Publication for fraudulent purposes.
k. Outside India, Act if offense or contravention is committed.
l. To give directions right and power of controller.
m. Punishment for forfeiture for not interfering with other punishments.

7.4.2 Sections and Punishments

These are the sections and punishments according to the Information Technology IT Act 2000:

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 defines of deleting data with malicious intentions without permission or destroying, altering or stealing computer system/network without permission as compensation for damages from computer systemowner who is responsibleto pay money to owner.
Section 43A	This section of IT Act, 2000 defines that any company body working with perceptiveprivate data that gets failure to executelogicalsafetydo practice can cause loss of that other person will also responsible as criminal for reimbursement to the affected person or party.
Section 66	Computer System hack with malicious goals like online fraud is punishablefor 3 years locking upin jail or the charge of Rs.5,00,000 or both.
Section 66 B, C, D	Online fraud or cheatingby misusing or transmitting data or stealing of identity is carrying a punishment of custody of 3 years or Rs. 1,00,000charge or both.

Section 66 E	This Section is for infringement of personal privacy by transferringany image or confidentialpart is carrying a punishment ofimprisonment for 3 years or 2,00,000 charge or both.
Section 66 F	This Section tells about Cyber Terrorism disturbingunion, security,reliability, independence of India by using any media of digital world is accountable for lifelong locking up.
Section 67	This definesdisplaying or printing in public any of obscene details or pornography or transferring of private content in public is responsible for locking up to 5 years or charge of Rs. 10,00,000 or both.

Challenges

7.5 Introduction to Cyber Laws:

Millions of users use internet currently in the country, and those users are increasing in numbers rapidly to increase internet accessibility with the government's initiatives. It shows the importance and need of internet in our lives as well as our existence in cyberspace. However, in field of cybercrime, these users are increasing in a wide. As Information technology get to specific level, new types of abuses also occurs. As there are different types of crimes so It is impossible for the law to identify and recommend remedies accurately. In the end, It is difficult for legal embodiment to implement and it lags far back from advance technological.

To translate the laws in the physical world into the virtual space, Cyber law is an attempt to apply. People connect and communicate using modern technology encompassed in all the ways. Advance technology complies with the regulation of cyberspace.

7.6 Challenges of Cyber Laws:

- **Challenges in mobile laws**

  These days, most popular thing is using Smart phones and tablets. The ecosystem is expanded with mobile devices with near-universal reach and Projection of content production lead to provide new difficulties to cyber legal jurisprudence around the world.

Around the world, many countries have no dedicated regulations relating to the use of these new mobile devices communication platforms and besides that for input and output activities the use of mobile devices is increasing day by day. It is very important to handle legal issues regarding the use of mobile devices because of the rise in criminal activity, It is also becoming important to protect and safeguard mobile security and privacy.

- **Legal issues of cyber security**

  For cyber security, there is a need of appropriate cyber law in a legal framework to protect, promote and improve. It is said "Data is New Gold" Which is increasing cyber security incidents and network attacks to perform cyber security breaches and user data leaking like treating data as gold. To protect and protect cyber security, It is not even important but necessary to take appropriate legal actions by the function of a legislator and as well as to create awareness among internet users about cyber security. While using any computer, related resources or devices and even if communication equipments suitable mandatory provisions and rules are establishing to assist for protection, prevention and promotion of cyber security.

- **Cloud computing and law**

  Even though physical computer system resources, specially data storage and computer power resources are needed and available to store data, user don't need to directly interact with computer systems. We can interact with computer devices with an on-demand availability of the systems is called Cloud computing. It is becoming increasingly popular to use Cloud computing these days. At the same time, to protect data, its privacy, jurisdiction and legal activities can have unique challenges to face problems and issues related to cloud computing for lawmakers. To protect the industry and allow meaningful remediation to the companies, there is a lot of pressure on cyber legislators and stakeholders with effective legal framework in the event of cloud computing incidents.

- **Social media and legal rules**

In all sections of the society, during recent years social media has become pervasive. Irresponsible use of social media can cause cyber stalking, cyber harassment, identity theft and other crimes which are common consequences now days. The privacy of social media users is at risk for their sensitive personal data even if various stakeholders do so much effort to avoid it. The main problem for cyber legislators is to provide solutions for victims of the social media crimes as well as to properly control the social media misuse.

- **Spam Law**

Both email and mobile phones are getting spam everyday on massive base. Spam hotspots are established in many countries already. Spammers are now using attractive methods to cheat and target digital users because of increasing of usage of Internet and mobiles consumers. So that's why it is a strong security measure to deal in this situation to handle all spammers.

- **Legal validity of electronic documents and digital signatures**

To be admissible in court, specific provisions are made by The Indian Evidence Act for digital signatures and electronic evidence. Even if there are these provisions but still misappropriation of evidence is a common problem. As police don't have so much information about cyber crimes and theirs modus operandi, that is necessary to identify and handle digital platform as electronic evidence in most cases. In addition due of evidence vulnerability to tamper, court don't accept electronic evidences.

- **Jurisdiction Challenge**

Jurisdictional issues are often created by cyber law often. Jurisdiction has the right to allow which court can hear the case. If one person makes a comment in any jurisdiction and it can be read or heard in another jurisdiction, the issue arises like where to file a lawsuit. Secondly, finding the reason of cause of action can create another problem and can be problematic. Also, it's very difficult to do effective cross-border investigations and cybercrime punishment because legal frameworks are different from country to country. The types of activities have main differences like where it has been criminalized and how investigations are conducted. There is a significant impact on gathering of electronic evidence and criminal online activity surveillance, any cybercrime investigation has these both key elements.

- **Obstacles to international cooperation**

  As in domestic structures there are many problems for countries, so there is lack of a globally consistent legal framework which shows substantial challenges to international cooperation in general. This is especially dangerous across different continents when there are cyber attacks on large-scale.

Digital Signatures and Indian IT Act

7.7 What is a Signature?

When signing a document to prove that it is created by us. It is a proof of that document that the signature is coming from the right source to the recipient. Simply signature on any document means authentication of that document.

For instance, B has to check the authenticity of the message sent by A to B, and confirm that it is not from C but came from A, So A electronically signs the message which can be asked by B. A signature signed electronically that shows the identity of A is also known as a digital signature.

Signature is importantly the legal identity of the person and documents need to be authenticated. The person signing the document assumes the legal responsibility that comes out of it. Thus, a signature is representation or form but not just important part of the document or transaction.

General purposes of **signature writing are as follows:**

- **Evidence:** The signer is identified by a signature that certifies the writing with the signed document. The writing is an attribute to the singer when the signer draws his mark in a particular way.
- **Function:** The legal significance of the signer's act is the act of document signing to drag the singer's attention and that helps to avoid inconsistent engagement.

- **Acceptance:** Law or custom in a certain ways is defined by a signature that expresses the acceptance of signer or the writing authorization or the intention of signatory that has a legal effect.
- **Efficiency and Logistics:** It is a sense of clarity and finality to a transaction when a written document has a signature and no inquiries are needed to beyond the face of the document. For example, formal requirements, including a signature, rely on by negotiable instruments for easily changing ability rapidly and with very less interruption.

7.8 Digital Signature

Messages and Message Digest

- A message is defined by the document.
- Message digests are defined by fingerprints.
- To produce a message digest or fingerprint and to protect integrity, the message has hash functions.

Message Authentication Code (MAC)

- A Modification Detection Code (MDC) is a message digest created by using a hash function.
- A keyless hash function is used in MDC.
- Use Message Authentication Code to provide authentication.
- A keyed hash function is used in MAC i.e. the sender and receiver site have a symmetric key between them.

To provide integrity of message and authentication message, MAC (Message Authentication Code) was used, but a symmetric key is required to establish between the sender and receiver. On the other hand asymmetric pair of keys is used by a digital signature.

The receiver comes to know by the help of a valid digital signature that the message is coming from the authentic sender and is not updated in between the transmission.

The role of 'ticket', 'signature' or 'seal' in the traditional system to create a paper document authentic, digital signatures play the important role of authenticating electronic records. Any electronic record is being authentic by this establishment to which the digital signature subscriber wants to affix his/her digital signature to authenticate the electronic record. One is asymmetric pair of private and other is public keys which are both digital signature unique to each client. Both the private key and the public key is matched to each other so that encryption of the electronic record is done with the help of any private key decryption only with the help of the corresponding public key. A digital ID for the subscriber is generated by this digital signature containing the Digital Signature Certificate. After due verification and process adoption, controller of Certifying Authority issues this certificate. Basic information of that person is written on this certificate holding by the person. Many Information like name, name of Certifying Authority, location of Deed, public key, date of issue and date of expiry of certificate. On web pages through directories or public folders, Certificates are also available publicly.

This law has particularly clarified that a repository for the issuance of all digital signature certificates shall be acted as the controller under the Act and all public keys computerized data base shall be maintained in such a manner that such any member publically can access data base and public key. This is required because the client must have a public key.

7.8.1 Digital Signature Standard (DSS)

Federal Information Processing Standard (FIPS) is referred as Digital Signature Standard (DSS) that creates algorithms which is used to generate digital signatures for electronic documents authenticity with the help of Secure Hash Algorithm (SHA). Only digital signature function is provided by DSS but key exchanging strategy or any encryption.

Sender side:

In DSS approach, the message generates a hash code and signing function takes the following inputs -

1. Hash code.
2. For that particular signature the random number 'k' is generated.
3. The sender's private key i.e. PR(a).
4. A global public key (for communication principles - a set of parameters) i.e., PU(g).

The output signature having two components will be generated by these inputs to the function i.e. -’s’ and 'r'. Thus, the message originally is sent to recipient associated with the signature.

Receiver side:

The sender gets verified at the recipient's end. The sent message hash code is generated. Then a validation function takes inputs as follows-

1. The receiver generates Hash code.
2. Components 'S' and 'R' Signature.
3. Public key of the sender.
4. Global public key.

Signature component 'r' is compared with the verification function’s output. If sent signature is valid, then the values of both will match as only sender can generate a valid signature with the help of its private key.

7.8.2 Digital signature process

1. The document Signing
2. A digest Signing

- **The document Signing**
  - The document encrypts using private key of the sender.
  - The document decrypts using public key of the sender.
- **A Digest Signing**
  - If we are dealing with long messages then using public keys is very inefficient. Signing the digest of the message is the solution.
  - There is one-to-one relationship with the message in the message digest.
  - A digest is created from messages on the site of sender.
  - By using private key of the sender, the digest then goes by signing process.
  - Then a message and signature is received by the recipient sent by the sender.
  - By using the public hash function, from the message it received a digest is created at the receiver site.
  - By using the verification process, signature authentication is determined.

7.8.3 Digital Signature Features

- **Integrity of Message:**

  In signing and verifying algorithms, It is stored by using hash functions.

- **Authentication of Message:**

  By using public key the sender, the message is verified. When B receives a message from A. Public key of A is used by B for verification and the public key is different and has not the same signature as private key of C.

- **Disclaimer of Message:**

  A trusted third party but non-repudiation is required to provide a message.

B receives any signature created or sent by A from the message and a signature is also received by the trusted center.

The messages are verified by public key validated by the hub coming from A.

Along with the identity of sender, a copy of the message is saved by the center with identity and timestamp of recipient. To generate a new signature a private key is used by the hub.

A message, a new signature, identification of A, identity of B is sent by the center to B.

Then the message is verified by B using the public key of trusted center.

Authentication, rejection and electronic records verification is the meat and electronic transaction’s bone. Therefore, secure electronic transactions and authentication will be virtual only until all objectives have been achieved. This Information Technology Act 2000 introduced a system of 'Digital Signature' to achieve verification and security of these electronic records.

Thus the regulatory mechanism of information technology is being attempted research on meanwhile, Focusing on the 'digital signature' is very important as well as functional mechanisms, the authorities involved and the objectives it achieves in the environment of electronic. The present study titled, focus of 'Digital Signature' is on its attention with this different technical aspect to achieve authentication goal, rejection and electronic verification records by applying digital signatures.

7.8.4 Types of Digital Signature Attacks:

Three types of attacks can happen on digital signatures:

1. Attack of Chosen-Message
2. Attack of Known Message
3. Attack of Key-only

1. Chosen-Message Attack:

There are two types of attack method chosen:

- **Common chosen method -** In this method A is tricked by C into digitally messages signing that doesn't intend to do by A without knowing public key of A.
- **Direct pick method -** In this method, public key of A is already known to C and A's signature on messages is got by C and a message replaces the original message that C wants signature of A to be unchanged.

2. Known-Message Attack:

In an attack of known message, some previous message and signature of A is already stored by C. Now Signature of A on documents is tried to forge by C that does not intend to sign by A using a brute force method to recreate the previous data signature of A. known-plain text attack is named of this attack like same as in encryption.

3. Key-only Attack:

In a key-only attack, everyone can access available public key of A, and C uses this point and tries to recreate signature of A and signs documents or message digitally that does not intended by A. The authentication of the message would have a major threat and it is rejected because A cannot refuse to sign it.

7.9 Digital Signatures and Indian IT Act

7.9.1 Physical Signature and Signature under IT Act, 2000

The IT Act, 2000 authorized Signatures are treated as manual or physical signature. In another words, the IT Act authorized the signature that is equivalent to one signature handwritten.

The rules are provided by IT Act for the authentication process via signature and even credentialed third party method in the kind of Certification Authority (CA) to issue such signatures to end users through the controller of Certification Authority (CCA).

7.9.2 Signatures Journey so far under the IT Act

There are three phases, Signature journey can be divided into so far under the IT Act:

Phase I- Digital Signature (Year 2000 onwards)

Phase II- Electronic Signature (from 2008 onwards)

Phase III- E-Signature Service of Online Signature or E-Sign (After Sept 2016)

The division into different stages is completed for clarity only otherwise e-Sign online signature service Phase III is present with digital signature certificate system under Phase I.

PHASE I: DIGITAL SIGNATURE (FROM THE YEAR 2000 ONWARDS)

The digital signature concept under Section 2(1) (p) is introduced by the IT Act, 2000 as electronic record authentication by a customer, i.e., 'Signature Certificate' (DSC) of a person name is issued with the provisions of section 3 by using an electronic method or process.

- **Authentication of electronic records (Section 3)**

(i) The rules of this section subjects, electronic records can be authenticated by any subscriber by putting your digital signature.

(ii) Electronic records Authentication will be affected by asymmetric crypto systems usage and wrap and convert the initial electronic record into a different electronic record by using hash functions.

Digital Signatures Creation and Verification Process

Digital Signature Creation (Rule 4)

(a) The message with sender name on the computer is prepared to sent by the sender.

(b) A 'hash function' is applied to the message by the sender so that it can be encrypted using the public key of recipient which returns a hash as result. 'message digest' is refers to 'Hash result'.

(c) By using his 'private key' result of this encryption, this 'message digest' is further encrypted by the sender and is accepted as the digital signature of sender. In another words, this 'message digest encryption' is contained by digital signatures. The message has this unique signature and will be unique for each and every new message.

(d) With the message digital signature of the sender is enclosed.

(e) Recipient gets digitally signed and encrypted message electronically sent by Sender.

Digital Signatures Verification (Rule 5)

(a) The recipient uses the sender's 'public key' to verify the sender's digital signature. Verification proves that the message is authentic, unchanged and sent by the sender only.

(b) The recipient also creates a 'message dice' of the message using the same secure hash algorithm. If this 'Message Digest' is the same as 'Message Digest' received from the sender, the recipient can be sure that no changes have been made to the original message. The recipient

The message can be read by decrypting it with your 'private key'.

The digital signature cannot be copied, tempered or changed. The original the content remains intact with surety of the digital signature and unchangeable. Proof of identity of signer, data the integrity and non-repudiation of the signed document is provided by Digital signature sent only by the sender.

PHASE II: ELECTRONIC SIGNATURE (FROM THE YEAR 2008)

The concept of electronic signature was introduced by the IT Act, 2000 (through the Amendment Act, 2008) by inserting section 2(1)(ta) and s. 3a. According to Sec. 2(1)(ta):

Verification of any electronic record by the subscriber means "electronic signature" by means of electronic technology specified in the Second Schedule to the Act and includes digital signature. According to Sec. 3A, any electronic record may be authenticated by such electronic authentication technology or electronic signature by the subscriber:

(a) Reliable Consideration

(b) As the Second Schedule specifications.

The Central Government may lay down the method to ensure that the electronic signature belongs to the person who said to have been certified or affixed.

Any electronic authentication or electronic signature technology as well as the procedure for creating such a signature may be added or removed from the Second Schedule by the Central Government by notification in the Official Gazette. With effect from January 28, 2015, e-KYC technologies and Aadhaar (Know Your Customer) e-KYC services will be permitted to be included in the Second Schedule.The terms "digital signature" and "electronic signature" cannot be used interchangeably. The two are vastly different from one another.

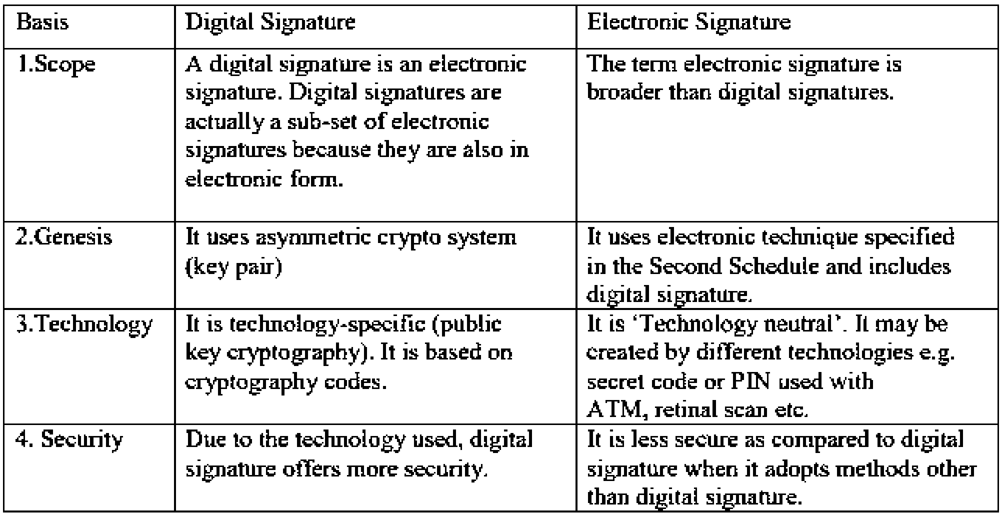
"Section 2(1)(p)” of the Information Technology Act of 2000 defines the legal meaning of the term "electronic signature," while 2 of the Information Technology Act of 2000, subsection (ta).

The Information Technology (Amendment) Act of 2008 added the term "electronic signature" to the Information Technology Act of 2000, whereas the term "digital signature" has existed since its inception.

The Information Technology Act of 2000, Section 2(1)(p), defines the term "digital signature" as follows: any electronic record signed by a subscriber in accordance with the terms of the section. 3 in accordance with a procedure or electronic method, whereas Sec. 2(1)(ta) of the Information Technology Act, 2000 (the IT Amendment Act of 2008 replaced the term "electronic" with "signature") defines the meaning of subscriber authentication of an electronic record. The Second Schedule provides a description of electronic technology, which includes digital signatures.

A digital signature is a "secure" electronic signature, but an electronic signature is not entirely digital.

Table: Differences between a digital and an electronic signature



Basis	Digital Signature	Electronic Signature
1.Scope	A digital signature is an electronic signature. Digital signatures are actually a sub-set of electronic signatures because they are also in electronic form.	The term electronic signature is broader than digital signatures.
2.Genesis	It uses asymmetric crypto system (key pair)	It uses electronic technique specified in the Second Schedule and includes digital signature.
3.Technology	It is technology-specific (public key cryptography). It is based on cryptography codes.	It is 'Technology neutral'. It may be created by different technologies e.g. secret code or PIN used with ATM, retinal scan etc.
4. Security	Due to the technology used, digital signature offers more security.	It is less secure as compared to digital signature when it adopts methods other than digital signature.

PHASE III: E-HASTAKSHAR OR E-SIGN ONLINE SERVICE (SEPTEMBER 2016 ONWARDS)

E-authentication technology was included in Schedule II of the IT Act of 2000 in 2015, marking its introduction. On September 3, 2016, the e-sign or e-signature service was made available by the Indian government. Only the fact that asymmetric cryptosystems are utilized should be noted. India's citizens can legally sign documents online with the Instant e-Sign service. Using this service, anyone can sign any form or document electronically at any time and from any location.

When was the term 'Electronic Mark' embedded in the IT Act by a change in 2008?

When asymmetric crypto was used, a digital signature was sought by adding section 2(1)(ta); when symmetric crypto was used, it was simply an electronic signature. Despite the fact that e-authentication entry technology by Schedule II e-sign (electronic signature using e-KYC services) or e-authentication technology by Aadhaar) or e-sign e-KYC services are utilized; only an asymmetric cryptosystem is utilized.

The e-Hastakshar System Elements:

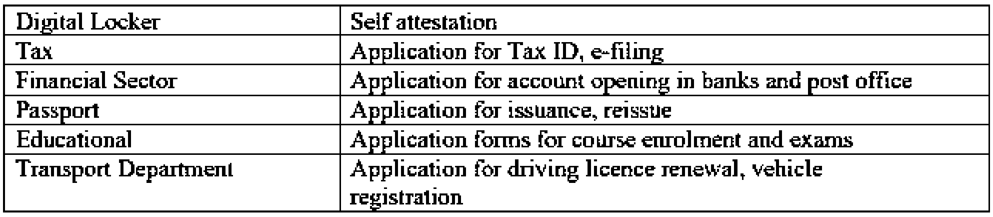
1. ASP, i.e. Application Service Provider. ASPS include government agencies, banks, financial institutions, educational institutions, etc.

2. ESP, i.e. e-Sign Service Provider. As currently authorized under the Certification Authority (CA) IT Act by Controller of Certification Authority (CCA). For this purpose, five agencies were identified away. Creation of user's signature the document is facilitated by E-Sign service provider which applied by the user to the document after acceptance. An agreement is needed for executing between ASP and ESP.

3. E-KYC Service Provider or Aadhaar E-KYC Services

4. E-Sign (or applicant) Usage

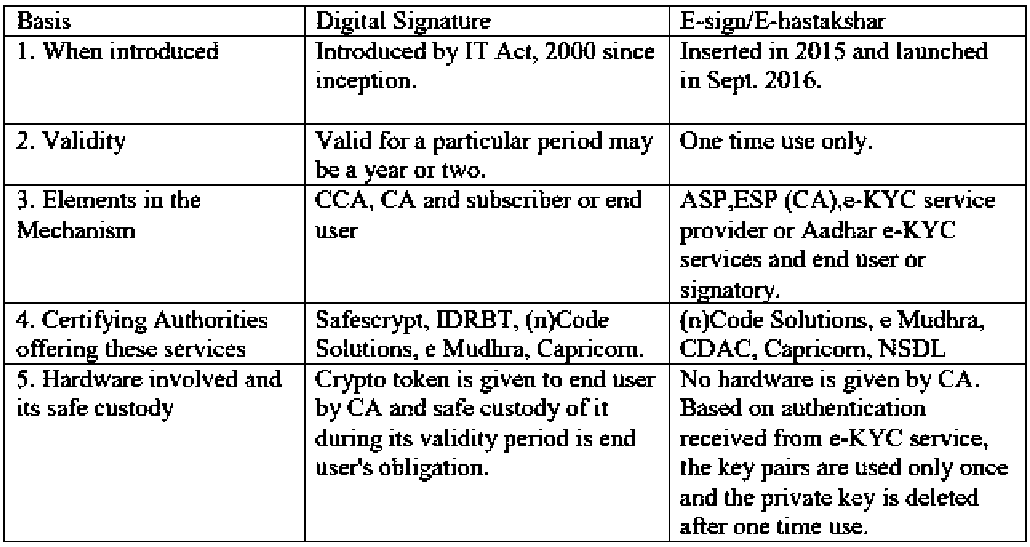
Table: Examples E-Sign Online service usage



Digital Locker	Self attestation
Tax	Application for Tax ID, e-filing
Financial Sector	Application for account opening in banks and post office
Passport	Application for issuance, reissue
Educational	Application forms for course enrolment and exams
Transport Department	Application for driving licence renewal, vehicle registration

The difference between digital signature is important to understand as described in Step I and E-Sign or E-Hastakshar Phase III. Both these systems needs to be repeated (ie, Phase I and Phase III) use asymmetric crypto technology so far have main differences between these two as mentioned in the table as follows.

Table: Digital Signature and E-Sign or E-Hastakshar Differences



Basis	Digital Signature	E-sign/E-hastakshar
1. When introduced	Introduced by IT Act, 2000 since inception.	Inserted in 2015 and launched in Sept. 2016.
2. Validity	Valid for a particular period may be a year or two.	One time use only.
3. Elements in the Mechanism	CCA, CA and subscriber or end user	ASP,ESP (CA),e-KYC service provider or Aadhar e-KYC services and end user or signatory.
4. Certifying Authorities offering these services	Safescrypt, IDRBT, (n)Code Solutions, e Mudhra, Capricorn.	(n)Code Solutions, e Mudhra, CDAC, Capricorn, NSDL
5. Hardware involved and its safe custody	Crypto token is given to end user by CA and safe custody of it during its validity period is end user's obligation.	No hardware is given by CA. Based on authentication received from e-KYC service, the key pairs are used only once and the private key is deleted after one time use.

Digital Signature (End Unit Rules) 2015

Digital Signature (End Entity Rules) 2015 provides for 'XML Digital Signature'. xml means Digital Signature on XML electronic record is refers to as Extensible Markup Language 'XML Digital Signature'. These rules also give for time stamp notation which defines the correct date and the time of action and identification of the person or device sending or receiving the electronic record.

The Indian IT Act Amendments

7.10 Amendments to the Indian IT Act

The Information Technology Act 2000 of India has a significant addition from the Information Technology Amendment Act 2008 (IT Act 2008).

The Indian Parliament passed the Information Technology Amendment Act in October 2008 and was applicable after a year. CERT-In (The Indian Computer Emergency Response Team) administrated the act and the Indian Penal Code has compliant with. It is a progressive step and the Information Technology Amendment Act has appreciated towards protection of India's citizens and cyber infrastructure.

It is on

e of the most inclusive laws addressing IT-related issues and sets a strong standard for another countries functioning to update their own laws.

7.10.1 Why was the Information Technology Amendment Act enacted?

To promote the IT industry, regulate e-commerce, prevent cybercrime, facilitate e-governance, the original version of the Act was developed. However, practices of security within India would promote and provide the country in a global context. In addition, the Office of the Cyber Appellate Tribunal is established by the Information Technology Amendment Act for hearing appeals requests of any person distressed by an order prepared under the Act.

7.10.2 What is included in the Information Technology Amendment Act?

There are nine chapters and 117 sections in the Information Technology Amendment Act 2008 and covers topics related to IT in a wide range, data security and cyber crime.

The provisions in Act contains are as follows:

- Cyber security measures tightening
- A legal framework for digital signatures establishing
- Identifying and applying intermediaries
- Decryption of electronic records, monitoring and regulating the interception
- Cyber forensics
- Cyber terrorism

For addressing problems that the original bill failed to cover and For accommodating further growth of IT and linked security concerns, Amendments to the Act have been made since the original law was passed.

7.10.3 Information Technology Amendment Act updating during times?

The revisions over the years with changes are as follows:

- To reflect current usage as communication devices by redefining terms.
- Electronic signing and validating contracts.
- For responsibility of content accessed or distribution by an IP address, permission is given to the owner.
- Holding corporations accountable and liable for data breaches to implement effective data protection practices.

In recent years, to include provisions for regulation, the IT Act has also been efficient for mediators, a ban on certain types of speech and penalties for cybercrime.

There are many changes which can include like the meaning of cybercrime expanding and updating new punishments for crimes such as publishing personal images, identity theft without consent, deceiving by impersonation and transfer offensive messages or explicit sexual acts by electronic means include.

7.10.4 To whom does the Information Technology Amendment Act apply?

When computer systems, networks or other technology related to information is used by any person, company or organization that is applicable for the Information Technology Amendment Act in India.

This includes the following:

- Web hosting service provider
- Internet service provider
- Network service provider
- Telecom service provider

Many Indian companies and organizations besides foreign companies as well are operating outside India are included with a presence in India.

7.10.5 Penalties for offences under Information Technology Amendment Act

- 1 lakh rupees (about $1,250) to up to 3 years in prison can be fined for the Information Technology Amendment Act violation.
- Up to 5 lakh rupees (about $6,300) for a person or imprisonment of up to seven years is included and can be fined if there are more serious offenses in damages.
- Imprisonment of up to 10 years can be punishment for the offense of cyber terrorism.
- In addition to these punishments, the victim of the crime will get payment from the offender if court will order so.

7.10.6 Challenges with the Information Technology Amendment Act

To reduce punishments for certain cybercrimes, the revision has been criticized and for deficient adequate safeguards for protecting the civil rights of individuals.

For example, to monitor, intercept, decrypt and block data at its discretion, subsection 69, authorizes the Government of India.

Nevertheless, a comprehensive legal framework for IT is instrumented by the IT Act in developing in India. To establish procedures for electronic governance and cyber crime prevention it has been very successful. To reproduce the updated landscape of IT, the Act will continue amend as necessary.

7.11 Check Your Progress

1. ___________________ is known as the crime which takes and takes the help of computer devices and internet.
2. ___________________ is a broad term for various technologies used to prevent and defend against different types ofcyber attacks or cyber crimes.
3. To describe legal issues _________________ is a term used and related to communications technology usage, specifically "cyberspace".
4. The IT Act is also known as the ________________________________ Act, 2000.
5. MAC refers to as ____.
6. DSS Means ____.
7. In encryption Known-Message attack is known as ____________________ attack.
8. The __________________________________Act 2008 is a significant updating to the Information Technology Act 2000 of India.
9. Full Form of CERT-In is ____.
10. E-Authentication with effect from January 28, 2015, the technology using services of Aadhaar e-KYC (means _________________________) was permitted in the second schedule used by to be included.

7.12 Summary

Introduction to Cyber Crime and Cyber Security

The term "cybercrime" refers to any illegal behavior that is carried out over internet. It is known as the crime that is executing with the assistance of computer system, digital devices and internet. Cyber crime may be targeted against an individual or group; it can also be committed against private organizations and the government as well. It can cause various kinds of damage like monetary loss, mental harm, physical harm or even one's reputation. It has posed a big threat to internet users by stealing information from millions of users in past years. It has also caused a huge dent in the global economy..

Cyber security is a technology or activity that helps to prevent and defend against cyber crimes. Cyber Security techniques assist any person or group to be protected from any kind of harm caused by any cyber crime. Overall it is a technique of securing your data, system or any kind of intellectual property.

Types of Cyber Crime:

- Hacking
- Improper crowd surveillance
- Child pornography
- Hair Grooming
- Copyright violation
- Money laundering
- Cyber Extortion
- Cyber Terrorism

Cyber Crime and Legal Landscape:

Cyber law is a term used to describe the legal aspects in concern to use of technology, specially "cyberspace", i.e. the Internet. Laws related to information crime, internet crime, computer crime, technology crime and communication crime are included in Cyber crime legal law.

Models of cyber crime laws:

- **CW Model Law** - Model Law on Computers and Crime related to Computer
- **SADC Model Law** - SADC Model Law on Computer Crime and Cyber crime
- **HIPCAR** - Harmonization of ICT Policies, Regulatory Processes and Legislation in the Caribbean (Cyber crime / E-Crime)
- **ITU** - International Telecommunication Union Cyber crime Law Resource - ITU Toolkit for Cyber crime Law

Some specific cyber crime laws: Most of the leading countries around the globe have defined cyber laws for maintaining cyber security, and topunish the offenders of cyber crimes.

Cyber Laws around the World:

- Electronic Commerce Act (Ireland)
- Electronic Transactions Act (UK, USA, Australia, New Zealand, Singapore)
- Electronic Transactions Ordinance (Hong Kong)
- Information communication Technology Act (Bangladesh)
- Prevention of Electronic Crimes Ordinance (Pakistan)

Besides,Cyber Laws are well defined by Indian Government as well.

Different Laws of**India** to serve the backbone of cyber security:

- Information Technology Act 2000
- Specific regulations, such as the Information Technology (Reasonable Security Practices, Sensitive Personal Data and Procedures or Information) Rules, 2011.
- Companies Act of 2013
- National Institute of Standards and Technology (NIST) Compliance.

Cyber Laws of India:

Illegal act in which computer has a device or target or both that refers to Cyber Crime. In natural way Criminal activities are included in cyber crimes like fraud, theft, forgery, mischief and defamation, Indian Penal Code has control over the entire subject related to it. New age crimes are increased because of the misuse of computers that makes need of introduction of new law to punish the cyber criminals, i.e. Information Technology Act 2000.

Area of Cyber Law:

Laws in Cyber world have a variety of different-different goals. How individuals and organizations or companies can utilize computers and the Internet are some laws govern, while others save people not to be victims of crime using unethical activities on the Internet. Cyber law key areas include:

- Fraud
- Copyright
- Defamation
- Harassment and stalking
- Freedom of Speech
- Trade Secrets
- Contract and Employment Law

Benefits of Cyber Laws:

To deal with cyber crimes, many outdated laws are replaced with the IT Act 2000 which provides solutions. Such laws are essential for people so that they can do online purchase or transactions without any fear of misuse while using their credit card. The Act offers a legal framework for legal effect, validity or enforceability don’t get deprived for information merely on the ground whether that information is in the form of an electronic record.

The Indian IT Act:

The IT Act is referred to as the Information Technology Act, 2000. The Indian Parliament created and reported on this Act on 17 October 2000. By a resolution on January 30, 1997, General Assembly of the United Nations suggested UNCITRAL Model (the United Nations Model Law on Electronic Commerce 1996) on which this Information Technology Act is based. To deal with cyber crime and e-commerce in India, IT Act is most important.

The main goal of this IT act is to perform legitimate, reliable electronic, online digital transactions to prevent and decrease rate of cyber crimes. This IT Act consists of 13 chapters with 90 sections. These sections begin with 'Section 91 - 94' i.e. last four sections deal with amendments in the Indian Penal Code (1860).

This IT Act 2000 contains two types of schedules:

- The Act will not apply to these related documents - **First Schedule**.
- An electronic signature or electronic authentication method related to it- **Second Schedule**.

Offenses and Penalties in IT Act 2000:

The IT Act, 2000 covers the following offenses and punishments under:-

a. Computer source documents tampering.
b. When an electronic form of information is published.
c. To decrypt the information, the controller's instructions to a client to extend the facilities.
d. Hacking for malicious purposes.
e. Penalties for breach of private confidential data or files online.
f. Penalty for misrepresentation.
g. False digital signature certificate for publishing is covered by a penalty.
h. Right and power to investigate offences.
i. System protection.
j. Publication for fraudulent purposes.

k. Outside India, Act if offense or contravention is committed.
l. To give directions right and power of controller.
m. Punishment for forfeiture for not interfering with other punishments.

Challenges of Cyber Laws:

- Challenges in mobile laws
- Legal issues of cyber security
- Cloud computing and law
- Social media and Legal rules
- Spam Law
- Legal validity of electronic documents and digital signatures
- Jurisdiction Challenge
- Obstacles to international cooperation

Digital Signature:

When signing a document to prove that it is created by us. It is a proof of that document that the signature is coming from the right source to the recipient. Simply signature on any document means authentication of that document.

For instance, B has to check the authenticity of the message sent by A to B, and confirm that it is not from C but came from A, So A electronically signs the message which can be asked by B. A signature signed electronically that shows the identity of A is also known as a digital signature.

Signature is importantly the legal identity of the person and documents need to be authenticated. The person signing the document assumes the legal responsibility that comes out of it. Thus, a signature is representation or form but not just important part of the document or transaction.

Digital Signature Standard (DSS)

Federal Information Processing Standard (FIPS) is referred as Digital Signature Standard (DSS) that creates algorithms which is used to generate digital signatures for electronic documents authenticity with the help of Secure Hash Algorithm (SHA). Only digital signature function is provided by DSS but key exchanging strategy or any encryption.

Digital signature process:

1. The document Signing
2. A digest Signing

Digital Signature Features

- Integrity of Message
- Authentication of Message
- Disclaimer of Message

Types of Digital Signature Attacks:

1. Attack of Chosen-Message
2. Attack of Known Message
3. Attack of Key-only

Digital Signatures and Indian IT Act:

Physical Signature and Signature under IT Act, 2000

The IT Act, 2000 authorized Signatures are treated as manual or physical signature. In another words, the IT Act authorized the signature that is equivalent to one signature handwritten.

Signatures Journey so far under the IT Act

There are three phases, Signature journey can be divided into so far under the IT Act:

Phase I- Digital Signature (onwards Year 2000)

Phase II- Electronic Signature (onwards from 2008)

Phase III- E-Signature Service of Online Signature or E-Sign (After Sept 2016)

Digital Signature (End Unit Rules) 2015

Digital Signature (End Entity Rules) 2015 provides for 'XML Digital Signature'. xml means Digital Signature on XML electronic record is refers to as Extensible Markup Language 'XML Digital Signature'. These rules also give for time stamp notation which defines the correct date and the time of action and identification of the person or device sending or receiving the electronic record.

Amendments to the Indian IT Act

The Information Technology Act 2000 of India has a significant addition from the Information Technology Amendment Act 2008 (IT Act 2008).

The Indian Parliament passed the Information Technology Amendment Act in October 2008 and was applicable after a year. CERT-In (The Indian Computer Emergency Response Team) administrated the act and the Indian Penal Code has compliant with. It is a progressive step and the Information Technology Amendment Act has appreciated towards protection of India's citizens and cyber infrastructure.

It is one of the most inclusive laws addressing IT-related issues and sets a strong standard for another countries functioning to update their own laws.

7.13 Keywords

- Cyber Crime
- Cyber Security
- Cyber Laws
- Cyber Crime Laws
- Indian IT Act
- Digital Signature
- Digital Signature Standard (DSS)
- Amendments to the Indian IT Act

7.14 Self Assessment Test

Q.1 Describe Cyber Crime and Cyber Security. What is legal landscape around the world?

Q.2 Describe Cyber Laws of India, Its importance, need, area and benefits.

Q.3 What do you know about Indian IT Act?

Q4. What kind of challenges are there for cyber laws?

Q.5 What is a Digital Signature and how is it related Indian IT Act?

Q.6 Write down Amendments to the Indian IT Act.

7.15 Answers to Check Your Progress

1. Cyber Crime
2. Cyber Security
3. Cyber Law
4. Information Technology
5. Message Authentication Code
6. Digital Signature Standard
7. Known-plain text
8. Information Technology Amendment
9. Indian Computer Emergency Response Team
10. Know Your Customer

7.16 References

1. Surendra Malik and Sudeep Malik, "Supreme Court on Information Technology Act, Internet & Cyber Laws and Aadhaar (1950 to 2019*)", Eastern Book Company Publisher, ISBN: 9789388822916.
2. Nathan House, "The Complete Cyber Security Book" Volume-I, First edition: January 2017, published by StationX Ltd.
3. https://www.tutorialspoint.com/fundamentals_of_science_and_technology/cyber_crime_and_cyber_security.htm
4. https://vikaspedia.in/education/digital-litercy/information-security/cyber-laws
5. https://www.geeksforgeeks.org/cyber-law-it-law-in-india/
6. https://www.geeksforgeeks.org/what-is-digital-signature
7. https://www.yourlegalcareercoach.com/challenges-in-the-field-of-cyber-law/
8. https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world

SUBJECT: Cyber Security	
COURSE CODE: MCA-34 CHAPTER NO. 8	AUTHOR: DR. ABHISHEK KAJAL

Information Technology Act 2000 and Web Treats

(Cyber crime and punishments, Intellectual Property Right (IPR), Web threats for organizations, Social computing and associated challenges for organizations)

INDEX **Page No.**

Information Technology Act 2000 and Web Threats

Cost of Cyber Crimes and IPR Issues

Web Threats for Organizations

Social computing and associated challenges for organizations

Lesson-8

(Cyber crime and punishment, Cost of Cyber crimes and IPR Issues, Web threats for organizations, social computing and associated challenges for organizations)

Cyber Crime and Punishment

8.1 Introduction to Cyber Crimes

If a computer system, network system device or another related device is involved or used in any criminal activity then it is considered as a cyber crime. There are some cases when cybercriminals intend to generate profit by committing cyber crimes while some times cybercriminals intend to commit cybercrimes straight to harm or halt a computer or system device. Possibly others can also use computer systems or networks devices to extend illegal details or data, malware, pictures or another type of content.

Many criminal activities can be committed for profit generating as a result of cybercrime, like attacks of ransomware, Internet and email fraud, identity theft and bank accounts related frauds, credit cards or any other type of payment cards. The cybercriminals can misuse personal and corporate data for theft and resale to a target person.

In India, the Information Technology Act, 2000 and the Indian Penal Code, 1860 covers all types of cyber crimes. The Information Technology Act, 2000 manages with cyber crimes and problems related to crimes of digital commerce. However, in the year 2008, the definition and punishment of cyber crime were outlined because of amendment in the Act. The Reserve Bank of India Act and the Indian Penal Code 1860 were amended time to time.

8.1.1 Types of cyber crimes:

- CSAM - child sexual abuse material or child pornography
- Cyber stalking
- Cyber bullying
- Online Job Fraud
- Cyber Grooming
- Phishing

- Sextortion Online
- Voice phishing
- Fraud of Credit or Debit Card
- Smishing
- Identity Theft and Impersonation

8.1.2 Prevention of cyber crimes:

The risk of a cyber attack according to the International Maritime Organization (IMO) recommendations should be the following approached framework:

- For cyber risk management, it is the first step that defines the roles and responsibilities of personnel responsible.
- To put operations at stake if disrupted, it is the second step that identifies the systems, assets, data or capabilities.
- It is very significant to execute risk-control procedures and emergency plans to safeguard against a possible cyber incident and to preservestability of operations.
- To detect cyber attacks as early as possible, it is also significant to build up and apply measures.
- To restore critical systems and to continued operation of plans, it is needed to prepare and implement by providing flexibility.
- In the end finally, to backup and restore any affected systems, identify and apply measures.

8.2 Cyber crime punishment or law in India:

Cyber law is crucial because it touches almost every aspect of transactions or activities on and in concern to the Internet, the WWW and Cyberspace. At first, it may appear that Cyber law is purely a technical field and doesn't have any impact to most of the activities in Cyberspace. But the actual fact is that nothing could be further than the truth. Whether you realize or not, every activity and every reaction in Cyberspace has some legal and Cyber legal perspectives.

In the context of cyber security, there are five distinct categories of laws that must be adhered to. Cyber laws are becoming more important in nations like India where the Internet is widely used. Information access, electronic commerce, software, and financial transactions in the digital sphere all fall under the purview of a number of stringent laws that govern the use of cyberspace. By increasing the number of connections and decreasing the number of security businesses, India's cyber laws have contributed to the growth of digital commerce and digital governance. Because of this, computerized media is accessible in different exercises or tasks and its compass and effectiveness has expanded.

8.2.1 Information Technology Act, 2000 (IT Act)

Overview of the Act:

The Indian Parliament approved this as the first cyber law. The Act defines its objective as follows:

"Through electronic data cloverleaf in order to provide legal recognition to carry out deals and other forms of electronic communication, generally appertained to as electronic styles of communication and storehouse of information, documents shall be entered into with government agencies." The Indian Penal Code, the Indian substantiation Act, 1872, the Bankers Book substantiation Act, 1891 and the Reserve Bank of India Act, 1934 and for matters associated therewith or accompanying thereto, to make farther emendations to grease electronic form.

However, several amendments are being made to the law due to the tendency of humans by misunderstanding technology as cyber attacks are dangerous and increasing. The severe penalties and restrictions are highlighted and performed by the Parliament of India to safeguard and defend the e-banking, e-governance and e-commerce sectors. The major point to be noted is that to include all the latest communication equipment, the scope of the IT Act has now been widened.

To express electronically, the Act defines that acceptance of a contract is agreed and has legal validity and is enforceable. Further, to implement electronic commerce the Act aims to attain its objectives of promoting and developing a conductive environment.

8.2.2 Important rules of the Act:

In the entire Indian legal framework, the IT Act is very popular, as to control cyber crimes; it orders and guides the entire investigation process. The following are the appropriate sections:

- **Section 43:** To those persons who indulge in cyber crimes, Section 43 of the IT Act applicable to those people, crimes such as causing damage to the computer victim, without the authorization of victim. In this kind of a case, if any computer system is smashed without the consent of the owner, the owner will be given a refund for the full damage.

- **Section 66:** Any conduct dishonest or fraudulent described in section 43 is applicable for this section also. Up to three years imprisonment or fine up to one lakh rupees in such cases 5 lakhs.
- **Section 66B:** This section explains the punishment for dishonestly obtaining stolen computers or communication equipment and carries three years probable sentence in prison. Fine up to one lakh rupees depending on the severity 1 lakh can also be obligatory.
- **Section 66C:** This section has the focal point on digital signature, password hacking and identity theft of other forms. This section provides up to 3 years for imprisonment owith a fine of one lakh rupees.
- **Section 66D:** By using computer resources, this section covers fraud. If found at fault, he can be imprisoned for up to three years and/or fine up to Rs 1 lakh.
- **Section 66E:** According to this section, taking photographs of confidential areas, then publishing or transmitting them lacking the approval of any person is carrying a penalty. If found at fault, he can get up to three years imprisonment for and/or fined up to Rs 2 lakh.
- **Section 66F:** Cyber terrorism acts. A person convicted of any offense can be punished with life imprisonment. An example: when a threatening email sent to the BSE- Bombay Stock Exchange and the NSE - National Stock Exchange challenging the defense forces to stop a planned terror assault on these kind of institutions. The offender was arrested under Section 66F of the IT Act.
- **Section 67:** It includes distributing obscenity electronically. If find guilty, the jail term is up to five years and the fine is up to Rs 10 lakh.
- **Section 69** – Government’s Power to Block Websites. If the government feels it necessary in the interest of sovereignty and integrity of India, it can intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. The power is subject to compliance of procedure. Under section 69A, the central government can also block any information from public access.

8.2.3 IT Act Positive and negative aspects

Benefits of these laws are following:

- Due to the presence of this act major companies are now conducting e-commerce without any fear in mind. Until recently, the development of electronic commerce to control online commercial transactions in our nation was delayed mainly due to the short of legal infrastructure.

- Corporations that conduct online transactions are able to use Digital signatures now. The Act is recognized and sanctioned Digital signatures officially.
- Additionally, the mode of issuance of a digital signature certificate has been included in the Act for commercial items in order to serve as the Certifying Authority. The Demonstration sees no difference regarding which legitimate substance might be picked as the Confirming Power, gave government principles are followed.
- In addition, the Act grants businesses the ability to file electronically using a government-defined electronic form at any workplace or authority, agency, or body that is owned or restricted by that government.
- When electronic transactions are used, crucial information about security concerns is provided to ensure the transaction's success. Word secure digital signatures, which must be included in a system of security procedures, were created and accepted as part of the act. As a result, digital signatures are now considered to be more secure and to play a larger role in the financial system. Digital signatures can help ensure the safety of online transactions.
- It is very typical for businesses to hack their information and systems. Nonetheless, the situation has been totally changed by the IT Act. If someone breaks into their computer systems or deletes or duplicates data on the network, corporate entities now have legal recourse. Damage can result from anyone using a computer, computer system, or computer network without the owner's or someone else's permission.

However, the said Act has some problems:

- Because it does not use the terms "objectionable" and "dangerous," Section 66A is evaluated in accordance with Article 19(2) of the Indian Constitution. The terms "crime," "public order," "provocation," and "principle" were not specified. As a result, conditions can be interpreted however one sees fit.
- The Act has not mentioned the issues that are necessary for the Privacy and Content Directive because the Internet is extremely vulnerable.
- Domain names are not covered by the Act. The Act does not include a definition of a domain name, nor does it specify the rights and responsibilities of domain name owners.

- The Act imposes no conditions on domain name IPR (Intellectual Property Rights) owners. Due to the fact that the aforementioned law does not address the fundamental issues pertaining to patents, copyrights, and trademarks, numerous loopholes exist.

8.2.4 Indian Penal Code, 1860 (IPC):

If to cover specific cyber crimes, the IT Act is not sufficient, IPC sections can be invoked by law enforcement agencies as follows:

Section 292: This section was created specifically to prevent the sale of obscene content. However, various cybercrimes must be dealt with in the digital age. When it is published or transmitted electronically, this provision also governs the exploitation of children in sexually explicit acts or material. Such actions carry the possibility of up to two years in prison and a fine of Rs. 2000, as a result. Any of these offenses will result in a fine of up to Rs. 50,000 and a maximum prison term of five years. 5,000 for people who do it again (second time).

Section 354C: Receiving or publishing photographs of a girl, woman, or woman's private parts or functions without her permission is considered cybercrime under this rule. In this part, voyeurism is explicitly examined as it includes condemning sexual demonstrations of a lady. Sections 292 of the Indian Penal Code and Section 66E of the Information Technology Act are sufficiently broad to cover similar offenses in the absence of essential elements of this section. First-time offenders face a maximum sentence of three years in prison, while second-time offenders face a maximum sentence of seven years.

Section 354D: Cyber and physical stalking are all described and punished in this section. Cyberstalking is the same thing as trying to find or get in touch with a woman electronically when she is not interested. This means using email or the Internet. For the first offense, the penalty is up to three years in prison, while for the second, a fine of up to five years is possible.

Section 379: Under this section, theft is punishable by up to three years in prison and a fine. Because a lot of cybercrimes involve stolen computers, electronic devices, or data, the IPC section is useful to some extent.

Section 420: This section deals with fraud and dishonest abetment to property delivery. Cyber criminals who have committed crimes like creating fake websites and cyber fraud are punishable under this section with a provision of seven years of imprisonment in addition to fine. This section of the IPC covers offenses relating to stealing passwords or creating fake websites for fraud.

Section 463: This section includes if someone use false or fake documents or records electronically. Email spoofing under this section can be punished with imprisonment of up to 7 years and/or fine.

Section 465: This provision for forgery generally manages with penalty for it. Under this section, offenses like spoofing emails in cyberspace and false documents research are dealt with and imprisonment punishment of either explanation for a term that can expand with both or to two years.

Section 468: Fraud committed with intent to defraud can result of punishment of imprisonment longer than extended to seven years and with fine. This section also penalizes email spoofing.

Also, apart from the laws listed above, The IT Act has many more sections and the Indian Penal Code deals with cyber crimes.

8.2.5 Information Technology Rules (IT Rules):

For the gathering, data transmission and data processing, there are many points of views that IT regulations cover and includes as follows:

- **The Information Technology (Fair Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:** The entities like sensitive personal information of individuals are held by these rules and must preserve assured safety standards to be specified.
- **Information Technology (Guidelines for Intermediaries and Digital Media Code of Conduct) Rules, 2021:** These rules govern the role of intermediaries, in order to maintain online security of users' data, including intermediaries of social media and to safeguard transmission of content that’s harmful over the Internet.
- **Information Technology (Guidelines for Cyber Cafes) Rules, 2011:** As per these guidelines, cyber cafes should be registered with an appropriate agency and maintain a record of the identity of the users and usages of their internet.
- **Information Technology (Electronic Service Delivery) Rules, 2011:**Fundamentally, that rules empower the government to identify services by assured the delivery like applications, licenses and certificates through electronic means.
- **The Information Technology (Indian Computer Emergency Response Team and the Mode of Performance of Functions and Duties) Rules, 2013 (CERT-In Rules):**The CERT-In can be

operated in a variety of ways thanks to the CERT-In Rules. A 24-hour Incident Response Helpdesk should always be ready, according to Rule 12 of the CERT-In Rules. If everyone is experiencing a cyber security incident, individuals, organizations, and businesses can report it to Cert-Ins. In accordance with regulations, Cert-In must be informed immediately of any occurrence that is clearly listed on a contract.

- Service providers, data centers, intermediaries, and corporate bodies are also required by Rule 12 to notify CERT-In of cyber security incidents within a reasonable time frame. Cyber security incidents can be reported in a variety of formats and ways on the CERT-In website. Additionally, there is information on how to report vulnerabilities and how to respond to an incident. In point of fact, in addition to reporting incidents involving cyber security to the CERT in accordance with its regulations, information is also required by Rule 3(1)(I) of the Information Technology (Guidelines for Intermediaries and Digital Media Code of Conduct) Rules, 2021.

Cost of Cyber Crimes and IPR Issues

8.3 Cost of Cyber Crime:

Most people have expectations and they are paying attention if the cost of cybercrime has increased in recent years. But a new report is updated to declare it: The estimated cost of cybercrime worldwide is $650 billion USD per year.

This is up from $550 billion USD in 2014, a similar study was released by security vendor McAfee and the think tank Center for Strategic and International Studies. 0.8 percent of global GDP is the new estimate, up from 0.7 percent in 2014.

It is written in a report by author James Lewis CSIS senior vice president "Cyber crime is persistent, low and unlikely to stop". They are also power botnets that can carry out massive denial-of-service attacks.

Other reasons for increasing the cost of cybercrime include:

- Cybercriminals are adopting new attack techniques.

- There are many weak cyber security countries from which many new internet users.
- By other business schemes and Cybercrime-as-a-Service in Online crime is becoming easier.
- Cybercriminals have a lots of money and its very easy for them to monetize their exploits and are becoming more financially able.

Tor (a Web Browser) developers have defended their project by saying that using tor can shield and safeguard user’s privacy from surveillance of government and tracking by corporate. And bitcoin defenders say anonymous transactions of the crypto currency help improve security.

Computer and Internet users face 80 billion malicious scanning every day, a report estimated that. Every day there are 34,000 phishing attacks and 4,500 ransomware, with about 790,000 records lost due to hacking. The report recommends a number of steps to prevent cybercrime, although security researchers have several recommendations over the years.

8.4 IPR (Intellectual Property Rights) Issues:

In India, Awareness of IPR and protection is still limited. It needs to change for fostering an innovation culture. IPR (Intellectual Property Rights) Protection is important for a country development. To develop a creative or innovative product or service, companies and individuals can spend many years and fortunes. All these efforts may fail if the intellectual property owners are not sure of its protection.

The punishment for cyber squatting in India is not yet provided for by law. Every other domain name ending in: is recorded with National-Internet-Exchange-of-India (NIXI with .in suffix in India), which is aself-directed organization. As the IT Act of 2000 comes short on the problem of digital piracy and the Copyright Act and other IP-related laws fail to preciselyexplain the court's international injunction-granting authority, a new regulation related to domain name registration and jurisdiction must pass. Exploitative and bad faith operations on onlineplatforms to offer legal recourse for the handling of domain names, copyright infringement and other IP-related problems.

8.4.1 IPR Issues in Cyberspace

- **Copyright infringement in the cyber world:** It is intension of copyright to protect the creativity of actors, authors, creators and others who create theatrical, literature, film, images, sound, visuals, as well as other types of literary and creative audio and video productions. To persuade, inspire and encourage writers, theater actors, musicians, and filmmakers to develop the works of authors the primary legislative goal behind the passage of the copyright law was. Thus the restricted right to duplicate copies (for digital as well as other type of forms), the creation of infringing copies from authentic works, the performance of works for the general population, interpretation and modification. Because of the web, it seems relatively easy to duplicate, by implementing software using freely available digital, using translation, changing (using software like Adobe) and infringing other rights.

- **Trademark vs domain name puzzle:** To register, protect and prevent fraud while using products and services, the Trademark Bill was originally created. Traditionally most trademark holders have recommended purchasing a domain name that is related to their trademark; For example, for "Nippon Cool" a registered trademark of a law office with would decide to buy a domain such as "www.nipponcool.com" over "www.lawcool.com". The core issue is that domain names are issued or sold on a "first come, first served" basis by ICANN (Internet Corporation for Assigned Names and Numbers), giving results in "offensive domain names" being offended for trademarks registering. As a result, domains take places that involve trademark rights. However, still there is no legal right for the holder of the domain name, claim, or actual power over the official title of that trademark.
- **Copyright violation:** Copyright infringement occurs while unauthorized person does something that infringes on the rights of the copyright owner. Copyright is considered infringing when a sale, display, hiring, import of copies, and perhaps other unauthorized material that are brought into the country are unfriendly to the copyright owner. Copy-pasting, downloading and uploading online secure content on platforms is easy like pressing a button on the Internet worldwide, a worldwide interstate of knowledge. Presented copyright law gives the unique right to the copyright owner to authorize the allocation of its individual protected material; However, if material like this is safeguarded on the internet, virtually any person can bean author or writersince it’s so easy to take out and store the work through a web page even if the copyright owner don’t provide any type of license or approval and besides It's very easy to replicate. Other web pages and take credit for talent, effort, ingenuity and skill.

As per Section 51 of the Copyright Act of 1957, the burden of proof is on the copyright owners to show deceptive resemblance and produce a clear case for the offender. It is important to understand that the same level of security can be provided to a website. As a magazine, book or electronic device subjects to copyright violation. Because most of the tools these days can copy pictures, illustrations and scenes, many works that are copyrighted can be simply infringed via the Internet.

- **Jurisdiction:** When certain information on the Internet violates the copyright of user of India, the Court shall have the right by virtue of the universal reading of sub-sections (k), (l), (j), and (o) of section 2(1)— is area. IT Act 2000, whether phrase "computer resource" is "a computer network consisting of one or more computers" thus making the claim that a computer may include a worldwide network besides that the Indian Court of Justice worldwide destruction or may order annulment. while the phrases used by Sections 2(2) and 75 of the IT Act 2000 "infringement committed outside India", the Copyright Act 1957 and the Trademark Act 1999 do not in any way control worldwide authorization Is.

  Further, in YouTube v GeetaShroff, an honorable judge of the Delhi High Court ruled that any kind of information which is offensive in print from the jurisdiction of India may be restricted and deleted by the obtained technique it was outside India. It said that since the idea of "recognition and enforcement of foreign judgment" must be experimented in the country wherever the user resides, the person who took the material abroad may be prepared to delete the illegal data. The Hon'ble Court in Modi Entertainment Network &Orsvs WSG Cricket Pte Ltd concluded that the injunction may have effect overseas, provided the rights to material subjected are in the elite prerogative. Thus the judiciary of India can have exclusive capability.

- **Trademark and domain infringement in cyberspace:** Any graphical mark that can be shown in a graphical format to describe any business or work is called a trademark, so that the servicesor goods included in that it is easy as marks are identifiable and distinguishable from the view point of the person viewing which mark, section 2 (ZB) of the Trademark Act, 1999. For any registration, the technique and reasons have already been elaborated in deep way in Section 11 of the Trademark Act 1999. The key functions and importance associated with together the trademark with its licensing are to extend property, safeguard brand identity and provide a taste of creativity to brand exclusivity. In addition, the trademark mechanismis solely for consumers, customers, affiliates and operators to effectively connect, locate and obtain products and services associated with the Trademark.

An ISP (Internet Service Protocol) is just called a domain. For a certain website, it works like an address. In simple words, a domain name contains digits like 425.236.856 which, like a mobile phone number, can be dialed to get access to where the user wants to browse on the website. The Internet and the introduction of letter-number checking systems is so simple that it has led to requirement of record and memorize numbers, along with phrases such as "www.google.co.in", "www.yahoo.com", "www.gmail" being entered. .com", and so on. On resulting as such IP addresses in real are called the domains whichcreates content easily accessible on the Web.

- **Major Decisions Related to Trademark Vs. Domain Name:** Yahoo! Inc. VsAkashArora and others: Yahoo! AakashArora filed a trademark voilation suit in the Delhi High Court due to a website named "www.YahooIndia.com" was registered and the court ruled Yahoo! Quoting that AkashArora had registered the name of domain in his favor to redirect revenue from unfair use of Yahoo's trademarks. The court said, "Simple registration of a domain name that violates on the rights of a legitimate trademark owner doesn’t confer a complete right." Because a domain name registration does not actually grantrights of that domain, the defendant can be held liable for trademark infringement.
- **To assess the capacity to issue international rules and directions of Indian courts:** Injunctions, indemnities, criminal penalties or limitation fulfillment are seemed to be mainly classic solutions for trademark, copyright or other intellectual property rights violations. But the order measure is mainly common of all the measures. As the Internet is a limitless world in that any competent authority in India can grant relief in the kind of same injunctions, hence avoiding infringing material, these restriction actions can only be enforced within the borders of India, not that globally. Since injunctions, restrictions and India has other reliefs which are limited, ordinary people can use VPNs - virtual private networks to access data illegally, rendering court decisions useless.

Secondly, IPR in India has limited impact and presently facing challenges. Violations are rampant due to rights with poor enforcement and cases of court can go on for many years. This is a raw point especially for corporations that are large and multinational in sectors such as pharmaceuticals and agricultural. For example, India, along with countries such as Indonesia, China, Saudi Arabia, Russia, and Venezuela, is on the United States Trade Representative's (USTR) 'priority watch list' for poor security of the rights of US companies.

In this part, the Indian government has been disinclined in some cases to introduce IPRs to secure the interests of citizens of India. For example, under the compulsory licensing provision, the government can compel the copyright owner or someone else to produce as mass on an special drug in an emergency. Second controversial issue is Section 3(d) of the Indian Patent Act, which prohibits large pharmacy companies from 'perpetuating' patents by making minor changes to an earlier patent.

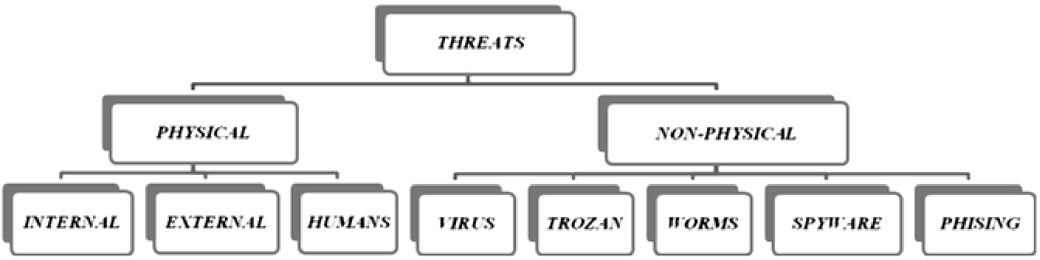
Web Threats for Organizations

8.5 Introduction to Web Threats:

The security of computer system has become an increasingly more important part of the main point for associations of all types. In the starting of the Internet and the Web has a whole modern aspect to protection that we call Internet Security. Unauthorized access draws on system data prior to Internet access and misuses confidential details. The Internet changes the whole picture of computers. Data can be accessed by anyone and anywhere in the world using the Internet. Dial-up access exposes computers to various threats, including those without access the computer system physically. The Internet security crisis and the security risks associated with Internet use including various hazards, security related risks and its prevention. As a whole, users of the Internet have practiced and will remain familiar with the victims of the scheme, which primarily have a direct impact on the critical feature that is their critical information and that their security is of paramount importance to the users. . Day by day, uncovered attacks on the Internet are increased and we will consider the suggested steps to catch Internet security issues before using it.

8.6 Web Threats or Internet Threats:

Web threats are programs with malicious software like adware, spyware, Trojan horses, viruses, bots and worms etc., that are installed on the system without our knowledge or without approval. These types of programs can utilize the web to transmit, hide, change ortransfer stolen data back to thehackers or cybercriminals. This can be better understood with examples – Trojans used to download spyware and Worms used to corrupt systems with bots. Technology has become a predictable component of our lives. But while the Internet provides a cumulative amount of useful information and makes messaging simpler and quicker than it has been for an eternity, it's approach possesses several dangers as well. A computer system is a huge tool for storing essential information. In assured cases, the information is extremely important so that from behind it does not damage the system. The hazards of computer systems can come close to many customs other than human or natural disaster. Example, because someone is stealing your information report by a secret store, threat of this type is much considered away - treated as a threat to human. However, since the computer gets wet in heavy rain, this type is said to be prone to natural disaster.



(fig. 8.1)

8.6.1 Physical threats:

The hidden basis of an incidence that cause canaffectprobably in the failure as well as the systems damage physically is called physical threat. There are three kinds of Physical threats:

- **Internal threats-** these types of threats comprise fire, contribution of unstable power, accommodation hardware, wetness in the rooms etc.
- **External threats-** the floods, earthquakes are few examples of these threats etc.
- **Human threats-** these include theft, communications destruction and trouble, hardware, accidental or planned errors.

8.6.2 Non-physical threats:

These threats can cause following problems:

- System data loss or that kind of fraud
- Interrupt trade process that depends on the systems
- Receptive information lost
- Actions of unlawfulstudy the systems

These are also types of logical threats. Common types of non physical threats are as follows:

- **Malware:** A software program that is secretly placed on a computer system that makes unexpected and attempts unauthorized which are malicious actions.
- **Virus:** It is a program that, like a real-life virus, can copy it and spread rapidly. They are pre-planned to damage computer systems and show unexpected mails and images. It also destroys essential files and slows down the system.
- **Worm:** It is a self-sustaining program that extends its duplicates to other systems while serving as links of network, email connections, messages, and other malware. They can ban you from reaching to and using a variety of web sites and even take away licenses for different applicationprograms that we deployed on our computer systems.
- **Trojan Horse:** A Trojan horse is aapplication program that performs malicious functions except that it cannot copy itself. This kind of program can masquerade as a harmful file and a tool with hidden malicious signals. During execution of this, we may practice unwanted system trouble and get wrong information each time from the system.
- **Spam:** It is a message that is transmitted by email and directs messaging that we do not request and it intends to generate money for the sender.
- **Phishing:** It occurs when we use our emails, phones, messages and faxes to steal our identity and obtain our personal information. Primarily the phishing stabs seem like they are like a legitimate intent, other than essence these are actually designed to be worn out for illegal act.
- **Farming:** It is the act of capturing the web addresses URLs of legitimate websites in order to forward us to a false or fake website that appears as original. Fake website secretly stores our personal data or information whenever it is winter, and illegal activities can be used for any number of times.

- **Spyware:** The software that is deployed on our systems without our knowledge and allows spyware instigators to track and rummage our electronic actions. They are often installed throughout the Trojan system and with the appropriate software which is preferred for downloading and deployment.
- **Adware:** The software that distributes advertisements such as pop-ups and web links to us without our authorization. They are usually deployed secretly during Trojans and throughout genuine application program that all recommend for download and deployment. It may display extremely under attack advertising on basis of data generated by spyware that is formerly on our structure and tracks Internet browsing.
- **Bots:** Botnets are much tiny application programs that are secretly stored throughout the Trojan system. A botmaster can direct multiple bots from one deepest position and carry out phishing and service denial that slows a website so that it can’t be accessed and used. These are generally utilizing to combat spamming and attacks of phishing.
- **Ransomware:** The application software that encrypts files with the extortion purpose. Files are stopped fee by delivery payment to third party waiting for injurious payment amount for decryption key.

8.7 Preventive Measures:

Some securities tips are related to internet are given below so that you can protect yourself and your family safe from these internet threats:

- **Avoid Malware:**

  Assure that your software of Internet Security Is reconstituted frequently as well as regularly, though is not taking it approved it will prevent you from attacks, and don't totally reliant on software of antivirus. Different threats need a multidimensional guard such as a fully derived security group. Attacks of "Zero-day" may be at risk as programs can be terminated by keeping them simplified. Be careful that PDFs, Office documents and Image files sometimes unexplained surprise and apprehension of the program any unexpected record and web link from unlawful source. Also inspect any counterfeit anti-malware packages that recognize invented spyware and virus.

- **Anti Social Network:**

  Condensed URLs such as bit.ly, tr.im and avoid tinyURL.com which is commonly used to hide Bad websites with various links to false login windows or malware. Very low size URLs with pleasure are doubtful. You can place an option forpage of TinyURL your own web browser that does the similartask. "Web" 2.0” sites are looking like fun sites yet actually not safe because these concentrate on attacks of worm similarly like attack of spam and attack of denial service. Be careful during Responsible posting of sensitive info on social networks Sites such as Facebook and LinkedIn as a social website receiving poorer because you can't visualize what awful guys can do harm with your personal data like such as date of birthday, your address of home and your Identification from these social networking sites.

- **Preserving a Healthy System:**

  Update operating system like windows and then use it as well as related Mechanism to update regularly, whenever need. In short, keep your programs and systems modernized and update too many existing malware access the sites are like through office documents, pdf etc. large number of malicious sites. Therefore, Adobe Reader, updated Office and updated system are required to protect various applications and systems. For People doing daily work and playing refrain from means of administrative account with the intention that if there is amalware attacker will reach and use your system it will limit the amount there is no administrative in profile as damage privilege.

- **Protect Your Password:**

  Update all passwords frequently and also intend to make special passwords for alldistinct email accounts thus an unofficial user can’t know it by no means and hack anyway. If any password have been revealed, Passwords from distinct accounts can guide the attacker you can't reach what you have. So all the time make and applymuch stronger passwords that make a combination of lowercase characters and uppercase characters, number and special characters. Don’t use passwords which are easy to guess and don't make stupid errors like Passwords writing to the place can be easily found.

- **(Don't Be) Burned On a Wire:**

Avoid connecting to web sites linked to transfer sensitive private information, like online banking and make a particular user profile with noprivileges of admin for exploring from hotspots in public. Applyand use HTTPs while browsing websites. Wireless type networks are naturally short secured. Don’t share files and weak passwords for Internet access. No backup crackup maintain personal and essential information "off-site" likeadministrators do for professional system. Always carry your laptop with you so stay supporting as above if someone stole your data you will not lose all important information. Try using system Password to prevent unauthorized users from accessing you system.

Social computing and associated challenges for organizations

8.8 Social Computing:

Utilization of social software by organizations and any interested parties, such as partners, customers, and employees refers as Social Computing. The intersection of social behavior and computational systems is the subject of social computing, a subfield of computer science.

Systems that maintain the gathering, processing, display, use, and distribution of information distributed across social groups like communities, teams, markets, and organizations are referred to as "social computing." Also, the data isn't "anonymous," but it's pretty accurate because people are connected to other people. The idea behind "social computing" is that by making information socially available to its users, digital systems can be designed with useful functionality preserved.

It wasn't until 1966 that users were able to send and receive email messages between computers that social computing really took off. By 1979, users were able to read and post "articles" to newsgroups using Usenet, a shared Internet discussion system. Announcement board frameworks (BBS) in the mid 1980s offered the additional comfort of buying into Web gatherings in which neighborhood bunches met up close and personal or get together (GTG?) By the mid-1990s (Advised when new messages show up). The public is able to create and edit content through Wikis, which first appeared online in 1995. In 2001, the free online encyclopedia Wikipedia went live. From 1994 to 1999, the first online diaries were published under the name "blog websites" (web logs). Due to their simplicity and ease of use, wiki and blog websites have gained popularity.

Tools for social networking such as Usenet and BSB,when users specifically request information from a specific source, such as browsing the internet, "pull technologies" are utilized. Ongoing social registering instruments, for example, Web gatherings use push innovation, where information is naturally conveyed to your PC assuming you buy in.

8.9 Social Computing ways:

8.9.1 Social Software:

Any system computation, that allows social interaction between people's groups. It is also called **Application Oriented Social Computing**. Such systems examples are as follows.

- **Social Media:** Interacting via computers has become one of the most often used methods of Social media Software.
- **Social Networking:** To build or improve the social network/relationship between people by using the platform of social networking. These people usually share alike interests, backgrounds or take part in similar activities.
- **Wiki page:** A wiki provides an opportunity for computing users to approach together with a specific goal and collaborate to give content to both novice and expert users, means the public.
- **Blog:** A blog is a way for people to chase a particular user, group, or company and comment in social computing aspects, on the progress of a particular model to be included in the blog.
- **Online gaming:** Using online games while interacting with other users, that is the source of social practice with online gaming.

8.9.2 Social Intelligent Computing:

Groups of people who are involved in Socially Intelligent Computing, they work together with social computing systems in various ways, It is also called **Social Science-Oriented Social Computing** all of these can be explained as socially intelligent computing.

- **Crowd sourcing:** At present, crowd sourcing is a social computing branch that has taken tasks of computing to a new level according to completion speed. It has also provided users to earn income in such a way through things like Amazon Mechanical Turk.
- **Dark Social Media:** A social media tool which is used for collaboration between individual people where content should be available only to participants.

8.10 Challenges of Social Computing:

With the raise in the number of users using social networking sites, new avenues have unlocked up for attackers to get access to individuals' accounts.

Social sites are developing very fast and creating new threats for individual people and organizations in this modern technology world.

1. Phishing Attack:

- Technique or method to access and use sensitive private information.
- Attackers create false and fake web pages that look like genuine ones and ask users to snap their details or credentials and get into trouble when the user enters credentials.

2. Challenges of Identity Association:

- This is a technique or method to share user details or credentials across many different-different domains.

  For example, on many sites offers are provided to users to login with their Facebook account or Google account so that it is more reliable for the user and the user need not to make multiple accounts on various different sites.

- This may seems trustable website but in real the user is not known to how and to what level their personal information may be distributed or shared between various third party applications.

3. Malware:

- Malwares are programs that are deployed on a user's computers or devices without the consent or knowledge of user.
- It spreads rapidly and infects devices.
- This software contains security flaws, Trojan horses and worm are examples of malicious software.
- Attackers can gain access to the user's personal information by monitoring the computer's activities and the computer can also be controlled or can carry out large-scale attacks without the user's knowledge as malware can steal identity of user and malware can even destroy computers.

4. Adware:

Hackers can deploy and setup forms containing adware that can result in endless pop-up windows of ads on a computer or mobile device of user as follows:-

- **'LOL' virus:** This type of virus is spread via Facebook's chatting service or function. The user receives this virus with an attachment stating "lol". And when it is clicked by user on the link a malware is downloaded in the computer or device system of user. The virus transmits and infects the system and spreads through the network getting access to the information of user.
- **Zeus virus:** This type of virus is a Trojan that expends by clicking on a link and when the link is clicked by user, it checks and scans all the files on the system of user and steals important information. This Trojan has specialty to steal the bank details and credentials of user.

5. Click Jacking Attack:

- Also known as UI Redress Attack.
- Where in web pages the Trojan makes the user to click on a malicious link and a malware is placed on the system.
- It is commonly used in Facebook which uses a name like jacking that when a page is liked by a user, picture or video attackers try to trap the user.
- To make a page popular and to make malicious attacks, hackers use these techniques.

8.11 Social Computing Tools:

Social computing has many tools that support people to open the door to latest knowledge and also gather some valuable info with experience. Each device plays an important role to maintain interaction between them. It also shares to a better and stronger accepting of social behavior among user’s different levels.

Social computing has many useful and important tools as follows:

- **Blogging:** Social computing has a very useful tool called blog that is the best way to interact with a specific user, users group, a company or any other communities group and comment on their progress towards a certain idea, which requires to be implemented. Blogging supports different section of users for interacting with each other by using the content given by main admin of the page. An alternative to email can be used by using Blogging. The blogging benefits are that to email it can be an alternative to use as for all. It can be used by users to communicate with each other. It also reduces the problems like using email to connect with people and to send mail to all of them. Some very famous examples of blogs are Sharepoint, Typepad, Weblogs.com or Gawker etc.

- **Wiki:** This is a type of companion software. There are others like Wikipedia like Social Text, Basecamp etc. This combined software generally gives computing users with a better opportunity to collaborate. It also supports by this method to come up with a common goal and also give different content for different levels of the community publically. Both novice and expert users can take help of this method of computing.
- **RSS:** RSS refers to as Rich Site Summary. Really Simple Syndication or RDF Site Summary is secondary names for this different term. It is a program that typically works with a set of standard web feeding formats and so publishes info such as news headlines, blog entries, videos or audios that needs to be updated regularly.
- **Online gaming:** Online gaming refers to those types of games that are played in virtual world over some type of computer network. We can say that a type of social behavior is known as online gaming. Users can communicate with many people around this world while playing game online and can be friends with people from different cultures, nations, traditions or classes. Different platforms can be used for online gaming to play such as Xbox or PlayStation, personal computer etc.
- **Social Networks:** Social networking is used frequently by people all around the world. They are using Facebook, Twitter, Messenger, YouTube, Skype, LinkedIn, MySpace, Viber etc. It’s impossible to imagine of modern world people without using any media of social networking. It supports in building social networks or relationships between people from different sections of the society.
- **Crowd sourcing:** Crowd sourcing is a practice that connects a crowd or an especial group of people for a similar goal that may be some type of innovation, achieving some other goal or solving a problem. Different levels of industries can have this between them. It supports in increasing the connection. With the passage of time, crowd sourcing has become a very important part of the social computing process.

- **VOIP:** VOIP refers to as Voice over Internet Protocol. A method which is very useful which supports in voice communication and sending some multimedia sessions using IP networks such as the Internet. With the use of VOIP, people can easily connect with people from the utmost corners of the world. So it has become important and useful type of social computing.
- **Collective intelligence:** As the name suggests, Collective intelligence is a type of experience of intelligence that occurs in a group of individuals people or also in some another type of collective. These individuals consists certain individual person or another markets, organizations or companies. One of the important social computing branches is this branch because of the group collaboration phases and implications.
- **Online Dating:** Currently, there are many online adult dating websites like OkCupid, eHarmony, Match.com, which support in building a community of adult people. These websites offer users a great chance to communicate with other people and also build some connection by voice calling, online chatting or video chatting etc. The interactions of users using these adult websites may differ from each other based on the partners they are communicating. But the main goal of all the partners will be the same which is the creation of relationships through virtual connections.

8.12 Check Your Progress

1. If a computer system, network system device or another related device is involved or used in any criminal activity then it is considered as a ________________________.
2. In India, cyber crimes are covered by the Information Technology Act, _________ and the Indian Penal Code, ___________.
3. CSAM refers to ____.
4. Section __________________has the focus on digital signature, password hacking and identity theft of other forms.
5. IPR stands for ____.
6. ICANN means ____.

7. ____________________ is considered infringing when a sale, display, hiring, import of copies, and perhaps other unauthorized material that are brought into the country are unfriendly to the copyright owner.
8. An _________________________is just called a domain.
9. _________________ are programs with malicious software like adware, spyware, Trojan horses, viruses, bots and worms etc., that are installed on the system without our knowledge or without approval.
10. ________________________ actually started in 1966 with the facility to transfer email messages between different computers by users.

8.13 Summary

What is Cyber Crime?

If a computer system, network system device or another related device is involved or used in any criminal activity then it is considered as a cyber crime. There are some cases when cybercriminals intend to generate profit by committing cyber crimes while some times cybercriminals intend to commit cybercrimes straight to harm or halt a computer or system device. Possibly others can also use computer systems or networks devices to extend illegal details or data, malware, pictures or another type of content.

In India, the Information Technology Act, 2000 and the Indian Penal Code, 1860 covers all types of cyber crimes. The Information Technology Act, 2000 manages with cyber crimes and problems related to crimes of digital commerce. However, in the year 2008, the definition and punishment of cyber crime were outlined because of amendment in the Act. The Reserve Bank of India Act and the Indian Penal Code 1860 were amended time to time.

Types of cyber crimes:

- CSAM - child sexual abuse material or child pornography
- Cyber stalking
- Cyber bullying

- Online Job Fraud
- Cyber Grooming
- Phishing
- Sextortion Online
- Voice phishing
- Fraud of Credit or Debit Card
- Smishing
- Identity Theft and Impersonation

Cyber crime punishment or law in India:

Cyber law is crucial because it touches almost every aspect of transactions or activities on and in concern to the Internet, the WWW and Cyberspace. At first, it may appear that Cyber law is purely a technical field and doesn't have any impact to most of the activities in Cyberspace. But the actual fact is that nothing could be further than the truth. Whether you realize or not, every activity and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Information Technology Act, 2000 (IT Act)

Overview of the Act:

The Indian Parliament approved this as the first cyber law. The Act defines its objective as follows:

"Through electronic data cloverleaf in order to provide legal recognition to carry out deals and other forms of electronic communication, generally appertained to as electronic styles of communication and storehouse of information, documents shall be entered into with government agencies." The Indian Penal Code, the Indian substantiation Act, 1872, the Bankers Book substantiation Act, 1891 and the Reserve Bank of India Act, 1934 and for matters associated therewith or accompanying thereto, to make farther emendations to grease electronic form.

Important provisions of the Act:

- Section 43
- Section 66
- Section 66B

- Section 66C
- Section 66D
- Section 66E
- Section 66F
- Section 67

Indian Penal Code, 1860 (IPC):

- Section 292
- Section 354C
- Section 354D
- Section 379
- Section 420
- Section 463
- Section 465
- Section 468

Information Technology Rules (IT Rules):

For the gathering, data transmission and data processing, there are many points of views that IT regulations cover and includes as follows:

1. The Information Technology (Fair Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
2. Information Technology (Guidelines for Intermediaries and Digital Media Code of Conduct) Rules, 2021
3. Information Technology (Guidelines for Cyber Cafes) Rules, 2011
4. Information Technology (Electronic Service Delivery) Rules, 2011
5. The Information Technology (Indian Computer Emergency Response Team and the Mode of Performance of Functions and Duties) Rules, 2013 (CERT-In Rules)

Cost of Cyber Crime:

Most people have expectations and they are paying attention if the cost of cybercrime has increased in recent years. But a new report is updated to declare it: The estimated cost of cybercrime worldwide is $650 billion USD per year.

This is up from $550 billion USD in 2014, a similar study was released by security vendor McAfee and the think tank Center for Strategic and International Studies. 0.8 percent of global GDP is the new estimate, up from 0.7 percent in 2014.

Other reasons for increasing the cost of cybercrime include:

- Cybercriminals are adopting new attack techniques.
- There are many weak cyber security countries from which many new internet users.
- By other business schemes and Cybercrime-as-a-Service in Online crime is becoming easier.
- Cybercriminals have a lots of money and its very easy for them to monetize their exploits and are becoming more financially able.

IPR (Intellectual Property Rights) Issues:

In India, Awareness of IPR and protection is still limited. It needs to change for fostering an innovation culture. IPR (Intellectual Property Rights) Protection is important for a country development. To develop a creative or innovative product or service, companies and individuals can spend many years and fortunes. All these efforts may fail if the intellectual property owners are not sure of its protection.

- Copyright infringement in the cyber world
- Trademark vs. domain name puzzle
- Copyright violation
- Jurisdiction
- Trademark and domain infringement in cyberspace
- Major Decisions Related to Trademark Vs. Domain Name
- To assess the capacity to issue international rules and directions of Indian courts

Web Threats or Internet Threats:

Web threats are programs with malicious software like adware, spyware, Trojan horses, viruses, bots and worms etc., that are installed on the system without our knowledge or without approval. These types of programs can utilize the web to transmit, hide, change or transfer stolen data back to the hackers or cyber criminals.

Physical threats:

The hidden basis of an incidence that cause can affect probably in the failure as well as the systems damage physically is called physical threat. There are three kinds of Physical threats:

- **Internal threats**
- **External threats**
- **Human threats**

Non-physical threats:

- Malware
- Virus
- Worm
- Trojan Horse
- Spam
- Phishing
- Farming
- Spyware
- Adware
- Bots
- Ransomware

Preventive Measures:

- Avoid Malware
- Anti Social Network
- Maintaining a Healthy System
- Protect Your Password
- Don't Be) Burned On a Wire

Social Computing:

Utilization of social software by organizations and any interested parties, such as partners, customers, and employees refers as Social Computing. The intersection of social behavior and computational systems is the subject of social computing, a subfield of computer science.

Systems that maintain the gathering, processing, display, use, and distribution of information distributed across social groups like communities, teams, markets, and organizations are referred to as "social computing." Also, the data isn't "anonymous," but it's pretty accurate because people are connected to other people. The idea behind "social computing" is that by making information socially available to its users, digital systems can be designed with useful functionality preserved.

Social Computing Ways:

- Social Software
    - Social Media
    - Social Networking
    - Wiki page
    - Blog
    - Online gaming
- Social Intelligent Computing
    - Crowd sourcing
    - Dark Social Media

Challenges of Social Computing:

With the raise in the number of users using social networking sites, new avenues have unlocked up for attackers to get access to individuals' accounts. Social sites are developing very fast and creating new threats for individual people and organizations in this modern technology world.

- Phishing Attack
- Challenges of Identity Association
- Malware
- Adware
- Click Jacking Attack

Social Computing Tools:

Social computing has many tools that support people to open the door to latest knowledge and also gather some valuable info with experience. Each device plays an important role to maintain interaction between them. It also shares to a better and stronger accepting of social behavior among user’s different levels.

- Blogging
- Wiki
- RSS
- Online gaming
- Social Networks
- Crowd sourcing
- VOIP
- Collective intelligence
- Online Dating

8.14 Keywords

- Cyber Crime
- Cyber Crime and Punishments
- CSAM (Child Sexual Abuse Material)
- IPR (Intellectual Property Rights)
- ICANN (Internet Corporation for Assigned Names and Numbers)
- Copyright Violation
- ISP (Internet Service Protocol)
- Web Threats
- Social Computing
- Indian Panel Code (IPC)
- IT Act 2000

- Physical Threats
- Social Software
- Social Intelligent Computing
- IPR Issues

8.15 Self Assessment Test

Q.1 What is cyber crime and its prevention methods? Describe few of punishments of cyber crime.

Q.2 What are costs of Cyber crime and IPR Issues?

Q.3 Explain Web Threats, Its types and Prevention methods.

Q.4 What do you mean by Social Computing? What are challenges and tools of social computing?

8.16 Answers to Check Your Progress

1. Cyber Crime
2. 2000 and 1860
3. Child Sexual Abuse Material
4. 66C
5. Intellectual Property Rights
6. Internet Corporation for Assigned Names and Numbers
7. Copyright
8. ISP (Internet Service Protocol)
9. Web Threats
10. Social Computing

8.17 References

1. Surendra Malik and Sudeep Malik, “Supreme Court on Information Technology Act,
2. Internet & Cyber Laws and Aadhaar (1950 to 2019*)”, Eastern Book Company Publisher, ISBN: 9789388822916.
3. Nathan House, “The Complete Cyber Security Book” Volume-I, First edition: January 2017, published by StationX Ltd.
4. https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime/
5. https://blog.ipleaders.in/cyber-crime-laws-in-india
6. (PDF) Social computing and its challanges in cyber security (researchgate.net)
7. https://ipbulletin.in/ipr-issues-cyberspace/
8. (PDF) Internet Threats and Prevention -- A Brief Review (researchgate.net)

SUBJECT: Cyber Security	
COURSE CODE: MCA-34 CHAPTER NO. 9	AUTHOR: DR. ABHISHEK KAJAL

Overview of Critical Infrastructure

(CII, Key Assets and worldwide Cyber Attacks on Critical Information Infrastructures, Protection of Critical Infrastructure)

INDEX **Page No.**

Protecting Critical Infrastructure

Critical Infrastructure Interdependencies

Internet, Social Media and Cyber Attacks on Critical Infrastructures

Lesson-9

Critical Infrastructure

Critical Information Infrastructure, Key Assets, Critical Infrastructure Interdependencies, Internet, Social Media and Cyber Attacks on Critical Infrastructures)

9.1 Defining Critical Infrastructure:

Critical infrastructure (CI) includes a group of systems and assets, whether it is physical or virtual, necessary to a nation. Any interruption of its services may have a serious impact on the economic, national security, public health or interests of any large group etc.

Over the time, Critical infrastructure has been defined in different ways, but usually consist "the physical or cyber-based systems essential for the minimal operation of the economy and government." Since the major cyber attack events around the globe start occurring to result a large extent of damage, the definition of critical infrastructure has been further expanded, "all critical national entities that may result a wide weakening effect on the national security, economic security and national public health or safety security from the destruction or getting inaccessible after any cyber attack."

9.1.1 Critical Information Infrastructure (CII):

The term ‘Information Infrastructure’ usually refers to define inter-connected computers and networks, and any information passing through them. A big chunk of such Information Infrastructure could be used for managing and controlling of critical infrastructure providers’ such as Power Grids, Oil and Gas pipelines, or assist any national economy or national fabric such as Telecom and Banking, Emergency Communication systems, Financial Systems, Defense Systems and Air Traffic Control Networks. These infrastructures assist major services and more importantly, the effect of any immediate failure or outage on our National well being or Security defines them as being Critical. It also ensures large scale processes throughout the economy by facilitating individuals, organizations and systems across worldwide networks for business and economic needs.

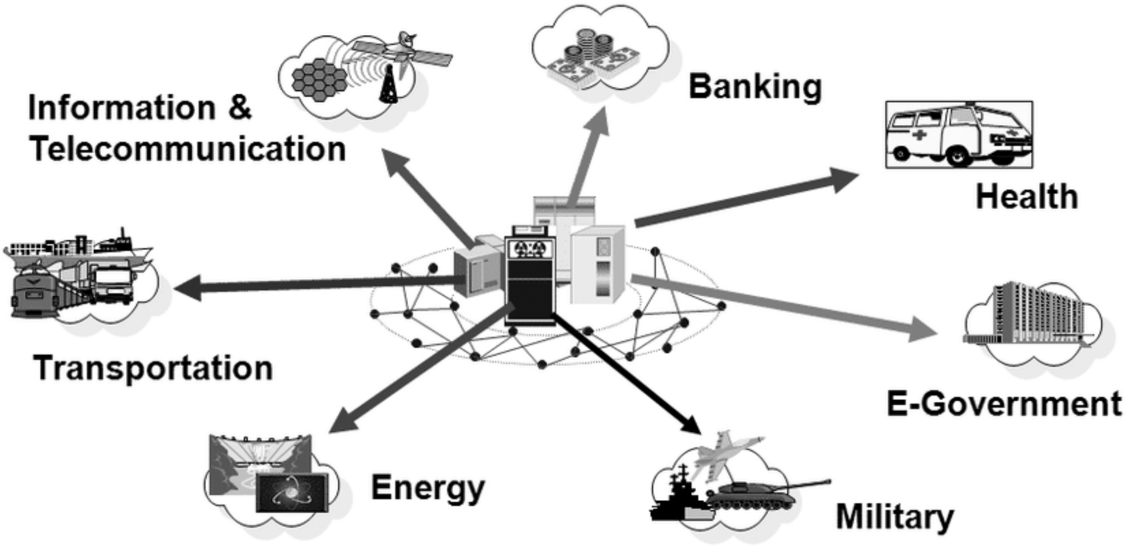
As per section 70 of Indian IT Act 2000 Critical Information Infrastructure (CII) is described as:

"The computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health or safety."

9.2 Key Assets of Critical Infrastructure:

- **Energy:** Energy generation sources, storage and distribution (electricity, oil, gas).
- **Information communication technology (ICT):** information systems and security of network (e.g. the Internet), provision of mobile telecommunications, provision of fixed telecommunications, radio communication and navigation, satellite communication, broadcast.
- **Water:** Quality control, provision of water (e.g., dams), control and control of the amount of water.
- **Food and Agriculture:** Food safety, security and provision.
- **Health Care:** Medical and hospital care, serums, drugs, pharmaceuticals and vaccines, Bio Laboratories and Bio Agents.
- **Financial Systems:** Banking, Payment Services and Government Financial Functions.
- **Civil Administration:** Government Facilities and Functions, Armed forces, Emergency services, civil administration services, Postal and courier services.
- **Public, Legal Order and Security:** Safety and Security, Maintaining Public and Legal order, Administration of justice and detention.
- **Transportation system:** Air transport, Rail transport, Road transport, Inland waterway transport, Border surveillance, Ocean and short-sea shipping.
- **Chemical industry:** Dangerous goods pipeline, production and storage of hazardous substances.
- **Nuclear industry:** Nuclear Materials Storage and Production.
- **Space:** Communications and Research.

9.3 Critical Infrastructure Sectors:



(fig. 9.1)

Important infrastructure sectors include:

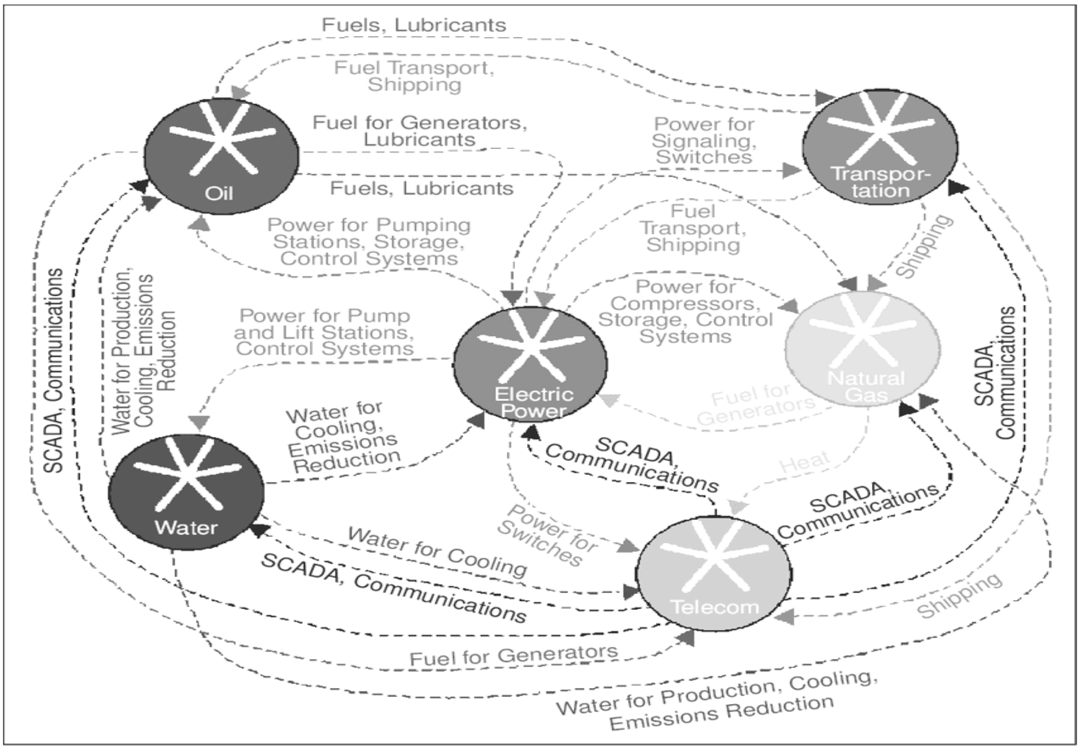
- Chemical Sector
- Commercial Comfort Zone
- Communications Sector
- Transportation System Sector
- Food and Agriculture Sectors Dam area
- Defense Industrial Base Sector
- Important Manufacturing Sectors
- Emergency Service Area
- Information Technology Sector
- Financial Services Sector
- Energy sector
- Government comfort zone
- Health care and public health sector
- Water and Wastewater Systems Sector
- Nuclear reactors, materials and waste areas

Critical Infrastructure Interdependencies

9.4 Critical Infrastructure Interdependencies:

A bidirectional relationship between two infrastructures by which each infrastructure state affects or depends on the state of the other is called interdependency.

When two assets have a bidirectional relationship that's called an interdependency where Asset A's operations affect Asset B's operations and Asset B's operations then affect Asset A's operations. For example, a water treatment plant requires connection for communication in its system and in turn, it gives water that is used by the circulatory system to cool its equipment. So thought of combining of two dependencies is refers to as Interdependency where an understanding of the interdependency needs the understanding, evaluation and characterization of two, one-sided dependencies.


Fuels, Lubricants
Fuel Transport, Shipping
Fuel for Generators, Lubricants
Power for Signaling, Switches
Oil
Transpor-tation
Fuels, Lubricants
Fuel Transport, Shipping
Power for Pumping Stations, Storage, Control Systems
Shipping
Power for Compressors, Storage, Control Systems
Power for Pump and Lift Stations, Control Systems
SCADA, Communications
Water for Production, Cooling, Emissions Reduction
Electric Power
Natural Gas
SCADA, Communications
Fuel for Generators
Water for Cooling, Emissions Reduction
SCADA, Communications
Heat
Water
SCADA, Communications
Power for Switches
Water for Cooling
SCADA, Communications
Telecom
Shipping
Fuel for Generators
Water for Production, Cooling, Emissions Reduction

(fig. 9.2)

This figure clearly represents the important characteristics of critical information infrastructure such as highly complex, interconnected, interdependent and distributed nature among various entities of critical infrastructure.

9.5 Interdependency Classes:

The nature of the system and the resources transmitted between the systems level of interaction has possibility to differentiate four classes' dependency and interdependency.

• **Physical interdependency** between infrastructure assets characterized by associations at operational levels that are related to the movement of goods or resources (water, electricity, chemical products).

• **Cyber interdependency** between infrastructure properties is characterized by relations at individual control levels for the relocating of information or data.

• **Geographic Interdependency** is not considered by general functionality relationship, unlike other dependency classes. Rather, they return infrastructure differences and potential disruption. One infrastructure advantage can take a collision on other infrastructure property placed nearby.

• **Logical Interdependency** connections were initially described as connections that do not fit less than one of the other three categories (geographic, physical or cyber). These mark the judgmental connections planned level typically concerned with the management of human and financial resources.

These four classes characterize the functional organization of critical infrastructure systems:

Through civil infrastructure (pipes, lines) are connected by their Interdependency, cyber interdependency relating to (ICS) Industrial Control Systems and (SCADA) Supervisory Control and Data Acquisition, Geographic the interdependency is directly linked to the place of the infrastructure assets and logical interdependency Interdependent infrastructures are concerned with proactive and reactive decision-making of managers.

A critical infrastructure is in stable connection with its atmosphere, uses and transforms inputs to give result from the environment to the similar environment. Many dimensions of its atmosphere can closely have an effect on the actions and functions of a critical infrastructure:

- Broad operating atmosphere including business, security, legal, policy and political thoughts.
- Coupling and response activities to critical infrastructure after interruption.
- Critical infrastructure is affected by types of failure.

- Infrastructure characteristics that affect the impact of disruption.
- Operating conditions for critical infrastructure (degraded operations, normal day-to-day activities).

Infrastructure interdependencies are compound, dynamic and it is important to consider and visualize avoiding result distribution and potentially increasing failures to manage cascading failures up a disaster. Infrastructure interdependence analysis takes a lot of time, and a complex task as well. In real, making risk-informed decisions with rising resilience can reduce the capability of stakeholders to recognize and use this information. To deal with these problems, the infrastructure groups of people are continuously using systems science approaches based on the supposition that an essential property or feature can be measured as part of a large scheme of infrastructure.

9.6 Critical Infrastructure Interdependency Analysis

The basic idea of The Critical Infrastructure Interdependence Analysis structure aims to set up a flexible move that includes a wide field of options, initial with moderately easy and tight-fisted hard work, culminating in more multifaceted, integrated assessment.

The critical infrastructure interdependence analysis structure includes four steps:

Step 1: Identification of stakeholder needs

Step 2: Identification of key assets

Step 3: Data Collection

Step 4: Infrastructure Analysis

Internet, Social Media and Cyber Attacks on Critical Infrastructures

9.7 Internet Attacks on Critical Infrastructures

When it comes to web attacks one term is used instead of internet or web attack that is cyber attack. Cyber is a word used for internet usually to enhance its meaning. So internet attacks or threats are same as cyber attacks and threats. Currently almost every person use internet on daily basis and also using social media for communication or making friends etc. There are lots of benefits of using these technologies as well as there are many disadvantages of that as well. Because every good invention and advantage limits us with different-different threats and attacks and it is usual to have an attack by any attacker on our infrastructure.

Attacks on the internet can have a lot of bad effects. An attack can lead to a variety of issues, including data breaches, data loss, and data manipulation. Associations endure deficiency of cash, loss of client certainty and harm to notoriety. In order to control or limit Internet attacks, internet security is implemented. Networks, computer systems, and their parts or components must be protected from unauthorized digital access through internet security. Attacks on the internet can also be serious, resulting in numerous issues; some of them are as per the following:

1. Malware Attack:

Malware, which includes worms, spyware, ransomware, adware, and Trojans, is the most common type of attack on the Internet. Malicious software viruses are also known as malware.

The Trojan virus takes on the appearance of legitimate software. Spyware, on the other hand, is a type of software that steals all of your confidential personal data without your knowledge or consent. Ransomware prevents access to key network components. Adware is software that puts banners and other advertising content on the user's screen.

Vulnerability in a network flaw that allows malware to enter in the system if a user clicks on a malicious link, downloads an email attachment, or uses an infected pen drive.

To prevent a malware attack:

- Use antivirus software for example: Avast Antivirus, Norton Antivirus, and McAfee Antivirus etc.

- Use firewalls. Firewalls filter and control the traffic that is trying to come into your computer system. There are built-in firewalls such as Windows Firewall and Mac Firewall.
- Avoid clicking on any doubtful links and staying alert.
- Regularly update your Operating system and browsers.

2. Phishing Attack:

The most common, famous and fast spreading types of internet attacks is called Phishing attack. Social engineering technique is used in this attack, when an attacker pretends to be a trusted contact and sends fake emails to the victim and when victim opens the email and malicious link in the attachment of email is clicked by victim. By that attackers can get access to confidential private information and details of account credentials.

To prevent from Phishing attacks:

- Check the received emails. There are some significant errors in most of the phishing emails such as spelling mistakes and legitimate sources format changes.
- Install and use an anti-phishing toolbar.
- Regularly change your passwords.

3. Password Attack:

This is kind of attack in which a hacker cracks your password by using different-2 programs and password cracking tools for example Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. These password attacks can be of many types like dictionary attacks, brute force attacks and key logger attacks.

To prevent password attacks:

- Always choose a strong passwords containing alphanumeric with special characters.
- Avoid using the same password for many multiple websites or accounts.
- Change your passwords on regular basis.
- Don’t write or show your password hints.

4. Man-in-the-Middle Attack:

Eavesdropping attack is another name for a Man-in-the-Middle Attack (MITM). In this attack, If two parties are communicating with each other then attacker comes in between to hijack the session between a client and host by which hackers steal and manipulate data.

To prevent from MITM attacks:

- Use encryption on your devices as well as on website for security.
- Avoid using different public Wi-Fi networks.

5. SQL Injection Attack:

A database-driven website can be attacked on by a Structured Query Language (SQL) injection attack when a standard SQL query is manipulated by the hacker. It is done by injecting any malicious code into search box of a weak website to reveal all the confidential information of the server.

As a result, an attacker is able to view, edit and delete tables in the databases. Administrative rights can also be taken by attackers by this.

To prevent a SQL injection attack:

- To detect unauthorized access to a network, use an Intrusion detection system.
- The user-supplied data needs to be validated with a validation process, to keep the user input checked.

6. Denial-of-Service Attack:

A significant threat many companies are facing is a Denial of Service Attack. Here, systems, networks or servers are targeted by the attackers to be flooded with traffic to limit their resources and bandwidth.

(Distributed Denial-of-Service) attack is also known by DDoS. To launch this attack attackers use many multiple compromised systems.

To prevent a DDoS attack:

- To recognize malicious traffic by executing a traffic analysis.
- Network slowdown, website shutdowns etc. are kind of warning signs need to understand. At that time, the necessary steps must be taken by the organization without delay.

- Make a checklist; execute an incident response plan to make sure your team and data center can easily control and stop a DDoS attack.
- Cloud-based services providers must be preventing from outsource DDoS.

7. Insider Threat:

As its name says Insider means inside the organization doesn't involve third party that's called an insider threat. That insider person can be an individual person from within company or the organization. That has access to whole data of company and who knows everything about the organization. It has potential threat to cause tremendous damages.

In small businesses, it is out of control when it comes to Insider threats. As the employees or staff in company has access to multiple accessing accounts with data. Reasons behind insider threat can be malice, greed or even carelessness. Insider threats are very tricky and very difficult to predict.

To prevent the insider threat attack:

- Cyber security awareness should be known to organizations in a good culture.
- Depending on job roles for IT resources staff companies must limit their access.
- Training about insider threat must be provided by organizations to employees so that they can prevent and help to stop this insider threat if any occurs.

8. Cryptojacking:

Cryptocurrency is the most popular term relates closely to the term Cryptojacking. Cryptojacking occurs when someone else's computer is accessed and used by attackers for mining cryptocurrency.

By infecting a website or manipulating victim's mind to click any malicious link cryptojacking can be executed by attackers. Online ads with JavaScript code are also used by this. As the Crypto mining code works in the background of system so victims are unaware of this while system also gets slow down.

To prevent from cryptojacking:

- As cryptojacking can infect the most unprotected systems, software and all the security apps must be updated time to time.
- To help detecting cryptojacking threats, need to provide cryptojacking awareness training for the employees.

- To block cryptojacking scripts, an ad blocker should be installed on system. An extension can also be installed like MinerBlock that is used to detect, identify and block crypto mining scripts.

9. Zero-Day Exploit:

A zero-day exploit can follow the announcement of a network vulnerability, and in most cases, there is no solution. As a result, the vendor informs users of the vulnerability. However, the attackers may also be affected by this information.

Before a patch or solution is implemented, attackers target the disclosed vulnerability.

To prevent Zero-day exploits:

- Patch management processes of organizations should be well-communicated. To automate the procedures, can use management solutions.
- To help you deal with a cyber attack by using an incident response plan. On zero-day attacks focus to keep a strategy to reduce and avoid damage completely.

10. Watering Hole Attack:

A specific region, group, or organization may be affected. The websites that are frequently accessed by the target group are also the targets of this kind of attack. Websites can be identified by either guessing or closely following the individual or the group.

To prevent the watering hole attack:

- By updating your software, the risk of an attacker exploiting vulnerabilities is reduced. Regularly confirm to check for security patches.
- To spot watering hole attacks, should use your network security tools. When it comes to detecting such suspicious activities Intrusion prevention system (IPS) works well.
- Check your online activities, use a VPN and use your browser’s private browsing feature. It works as a shield for your browsing activity.

9.8 Social Media Attacks on Critical Infrastructures:

To connect with people all around the world, social media has been a great platform, with millions of operators and users using internet online every day. However, many criminals have found social media to be the great easy way to collect private data details to promote cyber attacks such as phishing attacks or brand imitation.

Although you are known of it or not, attacks to the security and integrity of many business and personal accounts are a constant issue. That's why everyone should be cautious to social media safety. At first, you can save yourself by learning about the dangers of social media.

9.8.1 Social Media Threats: A social media attack can do anything that negotiations the security of any account. It's easy to attack so many people mostly provide their private data on social media websites or apps. Attackers gather these details easily and misuse it for their benefit.

Phishing scams are such another type of some social media threats. This defines that the attacker has gathered private data details successfully via social media and misused this details to send any message in email to his victim. Such messages usually prompt the person to click on an attached link which can send sensitive information to the attacker, which can be use by attackers for blackmail.

9.8.2 Prevention from Social Media Attacks:

Successfully bridling the troubles of social media substantially dishonesty in enlightening the people. Businesses require prioritizing conducting educational forums on cyber security to update their workers regarding the implicit pitfalls in cyberspace. In situation of private individualities, they can understand writing on internet manuals related to problem.

Second method to check the troubles of social media is to use announcement blockers. These blockers can block vicious advertisements from appearing on your screen. However, try to avoid clicking on strange advertisements while browsing the Internet, if that is not possible. You can also change your watchwords regularly to insure the sequestration of your accounts.

Another forestallment tip is to filter the friend requests you admit on all social media platforms. Unfortunately, not everyone is your friend on social media. However, it's stylish to ignore it, If you are doubtful about the person transferring you friend requests. Incipiently, avoid using social media spots in public Wi- Fi hotspots as these are more accessible to bushwhackers.

9.8.3 Cyber Security Role in Social Media:

Cyber security is an important matter to be taken seriously. Any threat to an individual's social media account should be dealt with promptly, with the user's safety in mind. If you believe you have received an email containing malicious links and attachments, it is best to ignore it and block the user who sent it. Companies should also invest in providing appropriate educational seminars to their employees and consider hiring the services of brand protection companies to ensure a safe work environment.

Prior to the arrival of social media, we had to go out to meet people with our associates in scary time. Now, almost everyone (and their nanny) has a social media account. We utilize it to show off our creativeness, inform friends about our daily life and as a full preparation board for our welfare.

Whichever stage you have built house online, that’s sure: Many persons get social media security not as much critically as they do. They do upload, share and then re-tweet it without taking permission of privacy.

9.9 Cyber Attacks on Critical Infrastructures:

The types of infrastructure are divided into many sectors by the Cyber Security and Infrastructure Security Agency (CISA) considered critical according to their security needs for unique vulnerabilities.

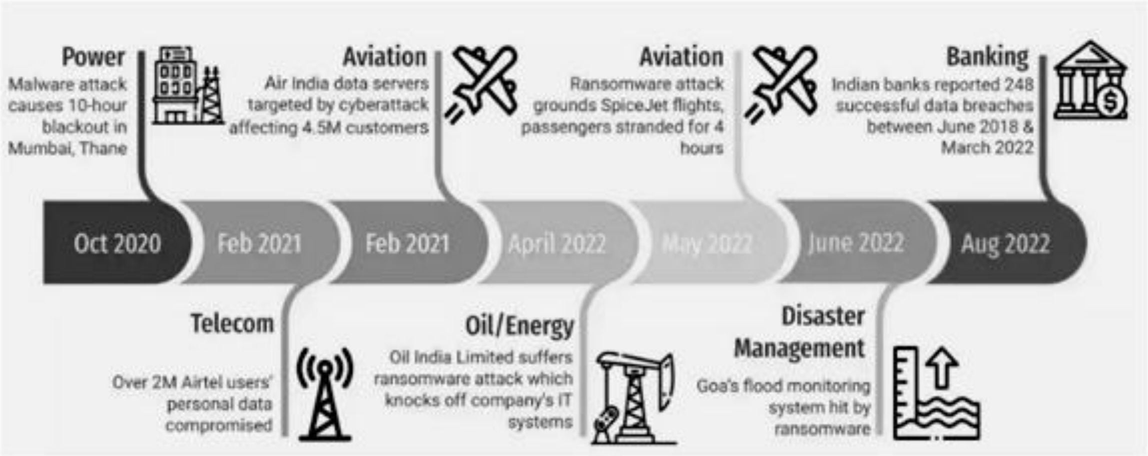
9.9.1 Why Cyber Attacks are increasing on Critical Infrastructures:

Infrastructure and people are increasingly using connectivity and that also leads rising accordingly to their vulnerability to attack and development. In the previous years to ensure continuity, Organizations were forced by World-changing events to adapt and depend heavily on remote access.

It takes a lot of price because in the US, over half of industry professionals trust networks of industries without the essential security controls to function safely. Three-quarters in security staff of IT field pays much attention regarding critical infrastructure performs attacks than enterprise data breaches. Obviously for better funding and awareness to protect these critical infrastructure sectors, recently it has been pushed by governments, regulators, other public and private actors.

9.9.2 Worldwide Leading Cyber Attacks:

Critical Infrastructure in India: Recent Cyber attacks and Security Incidents


Power
Malware attack causes 10-hour blackout in Mumbai, Thane
Aviation
Air India data servers targeted by cyberattack affecting 4.5M customers
Aviation
Ransomware attack grounds SpiceJet flights, passengers stranded for 4 hours
Banking
Indian banks reported 248 successful data breaches between June 2018 & March 2022
Oct 2020
Feb 2021
Feb 2021
April 2022
May 2022
June 2022
Aug 2022
Telecom
Over 2M Airtel users' personal data compromised
Oil/Energy
Oil India Limited suffers ransomware attack which knocks off company's IT systems
Disaster Management
Goa's flood monitoring system hit by ransomware

(fig. 9.3)

Apart from these recent cyber attacks, critical information infrastructure faced large number of cyber attacks worldwide. Some of cyber attacks resulting great extent on critical infrastructure entities are described as under:

1. **AIIMS ATTACK 2022:**

   Most recent Ransomwarecyber attack is executed on India's biggest healthcare infrastructure unit AIIIMS, Delhi on November'22 hacked its servers. Millions of patient's medical history database, including VVIP persons has been hacked by the attackers. All online services of All India Institute of Medical Science (AIIMS) put on hold for many weeks, impacted most of the services to the patients. A case of extortion and cyber terrorism was registered by the Intelligence Fusion and Strategic Operations (IFSO) unit.

2. **Triton Malware Attack 2017:**

   Potentially, one of the most devastating and unsafe cyber attacks in the past several years on Industrial Control Systems (ICS) was the Triton malware attack in 2017. This malware sponsored by state assault exposed first at petrochemical plant in Saudi, which allowed attackers for getting over SIS- Safety Instrument System of the plant.

The malicious code has the ability to ignite and release poisonous gas, and this is the first time an attack of this kind has been planned in advance and resulted in the loss of life and property. According to the findings of this investigation, spear phishing was the initial method by which the plant's internal network was breached; despite the fact that others accept it was a mis-configured firewall.

3. Nippon Telegraph and Telephone (NTT):

NTT Communications, the world's fourth largest telecommunications corporation, rules and helps data centres in more than 21 countries. Lately, they were got data infringe that uncovered by lot of preparation and many attack at front. The data infringe leaked the data of around 621 company customers and fusion in nature.

This type of attack can be prevented by running regular security checks and supplementary controls of security. Those improvements can stop entrance of perceptive personal data by equally solutions of company, employees and prevention of inappropriate facts or system usage.

4. Israeli Water System:

Israeli water frameworks were digital gone after a few times during the 2020s. The attacks were designed to communicate with the ICS command and control Israel's pumping stations, wastewater plants, sewer systems, and agricultural pumping systems.

Although attackers eventually unsuccessful, the threats were intended at attempting to increase chlorine in water and some other dangerous chemicals into the water to injurious stages and interrupt water supplies during heat waves and COVID-19. The people group still used the old-fashioned systems and enforced inadequate password guidelines on those facilities.

5. Taiwan's state-owned energy company, CPC Corp.

CPC Corp, a property of nation in command of oil distribution and liquefied natural resources of gas imports in Taiwan was aimed as target with an attack of ransomware previous year. Although creation of energy kept unaffected, the hackers threw the payment system of corporate into problems.

CPC gas stations customers were not capable in utilizing the expense stick VIP cards and apps for payment were there but of no use, although credit and cash still worked. A flash drive i.e. compromised is believed to be an unverified offender, and officials have not legitimately named the criminal, although hacker group Vinti suspects it.

6. **Moderna:**

Assumed hackers of China-backed investigated Moderna, a corporation that was at front position development of Covid-19 vaccine. They discovered the weaknesses of site and alienated users among extended security authority within the system network in their efforts of hacking.

Exploiting software flaws in well-known web repair software was the hackers' primary mode of operation. However, the hackers conducted some research but were unable to obtain confidential information. Even worse, over the past ten years, hackers have terrorized hundreds of government and corporate organizations.

7. **Unnamed US Natural Gas Operator:**

A natural resourced gas capability in the U.S.A. that has not been named got under attack with a strange ransomware that disrupted infrastructure and be in charge of property. Cybercriminals firstly utilized phishing spear links to get rights to IT networks prior to hiring ransomware within networks of OT. The fields dealt with built-in Human Machine Interface (HMI) and storage of data.

Luckily, the gas plant never "lost control" of functions yet was enforced in closing down for two days in anticipation of substitute tools could be got and programmed again. The need of division between IT networks and OT networks was the main loose point of facility.

8. **Ukraine's Power Grid:**

The power facility of Ukraine PrykarpattyaOblenergo in 2016 was one more example of a deliberate, enough fatal attack in cyberspace. Half of the population (700,000 peoples) of the IvanoFrankivsk area in Ukraine was surviving without electricity in middle of December because of an assault of malware.

A dangerous malware called "BlackEnergy 3" was used in the attack, reportedly by the notorious Russian hacker group Sandworm. On the other hand, the attack was not so simple. The hackers also work on the hard drive killer KillDisk, credential theft, spear phishing, VPNs, DoS telephony attacks, remote access exploits and other tricks.

9. San Francisco's MUNI Light-Rail System:

A strange jolt struck the San Francisco working class one morning in 2016, affected more than two thousand office systems.

The public (customers) were prompted to type the messages "out of order" and "get a free ride" as a result of this threat, which forced the company to close the ticketing structure for four days. The attack did not alter any personal or transactional customer data, and Backupify accepted the transfer rights to the recover objective on most systems as soon as the attack was discovered.

Even though backups were a good idea, they needed to be done more often and cover all important system parts at least. Running security audits on a regular basis and upgrading security software will help identify and address ransomware-related vulnerabilities earlier.

10. Iranian Cyber Attack on New York Dam:

Iranian hackers sponsored by state, Team the ITSec or Mersad Company, ruined in Supervisory manage of Bowman Dam and SCADA - Data Acquisition systems in New York. The system was associated to a cellular modem but was under maintenance at the moment in time of the attack.

The hackers took benefit of insecure modem connections and the lack of security controls for the dam's systems. Fortunately, the hackers simply gained access to a little sluice gate, but were capable of manipulating SCADA controllers efficiently. The attack was not of necessity of a composite environment, but was considered as a dissemination investigation to check for vulnerabilities.

11. Anonymous US Water Authority:

The US Water Authority's cellular network was hacked and taken over by the hackers, whose identity has not been disclosed. However, his goals were slightly distinct from those of many others. The hackers used cellular routers to inflate cellular data bills by 15,000 percent, from $300 per month to $50,000 over a two-month period, rather than attempting to disrupt the water supply or poison potable water.

The crucial fact was the facility's Sixnet BT router's old, factory-installed password firmware. Soon thereafter, a shortcoming in the switch's hard-coded certifications was found by the DHS, which programmers took advantage of to take advantage of organization weaknesses.

12. Colonial Oil Pipeline:

Ransomware struck Colonial's oil pipeline on May 7, 2021, making it the largest cyber attack on infrastructure in recent memory. The primary general pipeline in the United States, Pipeline, which supplies the East Coast with more than 45% of its gas, diesel, and jet fuel, was shut down completely. By May 18, they were able to restore the system's functionality, but approximately 11,000 gas stations were still without gas.

9.10 Check Your Progress

1. A bidirectional relationship between two infrastructures by which each infrastructure state affects or depends on the state of the other is called__________________________________.
2. When it comes to internet attacks one term is used instead of internet attack that is ____________________________.
3. The __________________converts itself seems like legitimate software.
4. _________________is software to show advertising content like banners on a user's screen.
5. __________________ is kind of attack in which a hacker cracks your password by using different-2 programs and password cracking tools
6. MITM stands for ____.

7. __________________________ as a form of abuse has become a feature of social media which many organizations and networks actively use over the past few years for combating.
8. CISA refers to ____.
9. __________________________ is a technique where someone is sending a message with a link seems real like a trustworthy company or make contact with in order to trick victim to disclose personal information such as passwords or credit card numbers.
10. ______________are a type of malware that duplicates itself to extend into more and more computers.

9.11 Summary

Defining Critical Infrastructures:

Critical infrastructure (CI) includes a group of systems and assets, whether it is physical or virtual, necessary to a nation. Any interruption of its services may have a serious impact on the economic, national security, public health or interests of any large group etc.

Over the time, Critical infrastructure has been defined in different ways, but usually consist "the physical or cyber-based systems essential for the minimal operation of the economy and government." Since the major cyber attack events around the globe start occurring to result a large extent of damage, the definition of critical infrastructure has been further expanded, "all critical national entities that may result a wide weakening effect on the national security, economic security and national public health or safety security from the destruction or getting inaccessible after any cyber attack."

Critical Information Infrastructure:

The term ‘Information Infrastructure’ usually refers to define inter-connected computers and networks, and any information passing through them. A big chunk of such Information Infrastructure could be used for managing and controlling of critical infrastructure providers’ such as Power Grids, Oil and Gas pipelines, or assist any national economy or national fabric such as Telecom and Banking, Emergency Communication systems, Financial Systems, Defense Systems and Air Traffic Control

Networks. These infrastructures assist major services and more importantly, the effect of any immediate failure or outage on our National well being or Security defines them as being Critical. It also ensures large scale processes throughout the economy by facilitating individuals, organizations and systems across worldwide networks for business and economic needs.

Key Assets of Critical Infrastructure: Energy, Information communication technology (ICT), Water, Food and Agriculture, Health care and public health, Financial Systems, Civil Administration, Public, legal order and security, Transportation system, Chemical industry, Nuclear industry, Space.

Critical Infrastructure Sectors: Chemical Sector, Commercial Comfort Zone, Communications Sector, Transportation System Sector, Food and Agriculture Sectors Dam area, Defense Industrial Base Sector, Important Manufacturing Sectors, Emergency Service Area, Information Technology Sector, Financial Services Sector, Energy sector, Government comfort zone, Health care and public health sector, Water and Wastewater Systems Sector, Nuclear reactors, materials and waste areas.

Critical Infrastructure Interdependencies: A bidirectional relationship between two infrastructures by which each infrastructure state affects or depends on the state of the other is called interdependency.

Interdependency Classes:

The nature of the system and the resources transmitted between the systems level of interaction has possibility to differentiate four classes dependency and interdependency.

Physical interdependency, Cyber interdependency, Geographic Interdependency and Logical Interdependency.

Internet Attacks on Critical Infrastructures

When it comes to internet attacks one term is used instead of internet attack that is cyber attack. Cyber is a word used for internet usually to enhance its meaning. So internet attacks or threats are same as cyber attacks and threats. Currently almost every person use internet on daily basis and also using social media for communication or making friends etc. There are lots of benefits of using these technologies as well as there are many disadvantages of that as well. Because every good invention and advantage limits us with different-different threats and attacks and it is usual to have an attack by any attacker on our infrastructure.

1. Malware Attack
2. Phishing Attack
3. Password Attack
4. Man-in-the-Middle Attack
5. SQL Injection Attack
6. Denial-of-Service Attack
7. Insider Threat
8. Cryptojacking
9. Zero-Day Exploit
10. Watering Hole Attack

Social Media Attacks on Critical Infrastructures:

To connect with people all around the world, social media has been a great platform, with millions of operators and users using internet online every day. However, many criminals have found social media to be the great easy way to collect private data details to promote cyber attacks such as phishing attacks or brand imitation.

Social Media Threats

A social media attack can do anything that negotiations the security of any account. It's easy to attack so many people mostly provide their private data on social media websites or apps. Attackers gather these details easily and misuse it for their benefit.

Cyber Attacks on Critical Infrastructures:

The types of infrastructure are divided into many sectors by the Cyber Security and Infrastructure Security Agency (CISA) considered critical according to their security needs for unique vulnerabilities.

Worldwide Leading Cyber Attacks:

1. **AIIMS ATTACK 2022**
2. **Triton Malware Attack 2017**

3. **Nippon Telegraph and Telephone (NTT)**
4. **Israeli Water System**
5. **Taiwan's state-owned energy company, CPC Corp.**
6. **Moderna**
7. **Unnamed US Natural Gas Operator**
8. **Ukraine's Power Grid**
9. **San Francisco's MUNI Light-Rail System**
10. **Iranian Cyber Attack on New York Dam**
11. **Anonymous US Water Authority**
12. **Colonial Oil Pipeline**

9.12 Keywords

- Critical Infrastructure
- Key Assets of Critical Infrastructure
- Critical Infrastructure Interdependencies
- Physical interdependency
- Cyber interdependency
- Geographic Interdependency
- Logical Interdependency
- Internet Attacks
- Malware Attack
- Phishing Attack
- Password Attack
- Man-in-the-Middle Attack
- SQL Injection Attack
- Denial-of-Service Attack
- European Program for Critical Infrastructure Protection (EPCIP)
- Information communication technology (ICT)
- Industrial Control Systems (ICS)
- Supervisory Control and Data Acquisition (SCADA)
- Structured Query Language (SQL)
- Insider Threat
- DDoS - istributed Denial-of-Service
- Cryptojacking
- Zero-Day Exploit
- Watering Hole Attack
- Likejacking/Clickjacking
- Counterfeit Cheap
- Malware as Unbelievable News
- Affiliate Scams
- Fake friends or followers

- Phishing attempt with fake link
- Catfishing/Dating Scams
- Cyberbullying and Abuse
- Identity Theft
- Virus-loaded fake apps
- Cryptocurrency
-

9.13Self Assessment Test

Q.1 Define Critical Infrastructure, its key assets and sectors?

Q.2 What are critical infrastructure interdependencies, its classes and how can we analyze critical infrastructure interdependency?

Q.3 Describe Critical Information Infrastructure.

Q.4 What is a social media platform? How social media attacks can affect critical infrastructure and what preventions can be applied to avoid such attacks?

Q.5 Discuss cyber attacks happened on critical infrastructure in past many years.

9.14 Answers to Check Your Progress

1. Interdependency
2. Cyber Attack
3. Trojan Virus
4. Adware
5. Password Attack
6. Man-in-the-Middle Attack
7. Cyber bullying
8. Cyber Security and Infrastructure Security Agency
9. Phishing
10. Worms

9.15 References

1. Thomas A. Johnson, “Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, CRC Press, ISBN:978-1-4822-3923-2, 2015.
2. Nina Godhole and SunitBelapure, Cyber Security, Wiley India, 2011
3. https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/
4. https://uk.norton.com/blog/online-scams/11-social-media-threats-and-scams-to-watch-out-for

SUBJECT: Cyber Security	
COURSE CODE: MCA-34 CHAPTER NO. 10	AUTHOR: DR. ABHISHEK KAJAL

Cyber Attacks and Security of Critical Infrastructure

(Cyber Threat Spectrum- Cyberspace Attacks and Weapons, Framework for improving Critical Infrastructure Cyber security)

INDEX **Page No.**

Protecting Critical Infrastructure

The Cyber Threat Spectrum

Cyberspace Attacks and Weapons

Framework for Improving Critical Infrastructure Cyber Security

Lesson-10

(Cyber Threat Spectrum- Cyberspace Attacks and Weapons, Framework for improving Critical Infrastructure Cyber security)

The Cyber Threat Spectrum

10.1 Introduction to the Spectrum of Cyber Attack:

Regardless of broad undeniable level direction from pioneers in the internet, the gamble of key disappointment and squandered assets in hostile the internet activities stays high. Since evolution of the internet, our dependent on computers and data flow driven technologies has greatly increased our potential for vulnerability if our system face any cyber attack. Information systems around the globe nowadays receive huge attempts of intrusion and this trend seems to be exponentially increased after breakdown of COVID-19 pandemic, when most crucial services go online nowadays. It is paramount that developing any appropriate defensive or preventive mechanism to systematically counter the cyber attacks in near future. The important part in countering any type of cyber attack is to instantly discern the form of attack and respond appropriately. In account of fighting the Islamic State of Iraq and Syria (ISIS) from 2015 to 2017, the former Defense Secretary Ash Carter reflected on these failures: Cyber Command's effectiveness against ISIS disappointed me a lot. It never really developed any technological or effective cyber weapons. In a nutshell, none of our agencies performed exceptionally well in cyber warfare.

10.2 The Framework of cyber attack spectrum:

In recent decades, a lot of stress has been given to expedite the field of cyber attack developments and its defense mechanisms. Even today, India is lagging far behind when discussions go around the capabilities of encountering cyber attacks.

Leaders and planners around the globe at the operational level attempts to outline the objectives to be pursued, describe the anticipated end-states, and articulate the various trade-offs between methods if they understand the cyber attacks at each level of the spectrum. This makes it possible to give a specific goal the right amount of time, effort, and resources. In the end, commanders will be able to offer a variety of strategies for achieving strategic goals, each of which comes with its own set of risks, rewards, and commitments to resources.

In the relatively short history of cyber warfare, actors at all levels have carried out a wide range of attacks. Notwithstanding contrasts between people, these assaults can be separated into five levels or classifications that expand on one another to shape a range: Network denial can take many forms, including mission denial, enterprise denial, mission denial, and mission manipulation.

The three levels of the namespace that are included in the "spectrum" are based on the definition of denial of cyberspace operations found in Joint Publication (JP) 3-12, which states that it "prevents the access, operation, or availability of the targeted operation." is an online attack I tumbled.

Denial Attacks: "control or change...deception, trickery, conditioning, creates a physical denial effect by using spoofing and other similar techniques" is added as an attack on manipulation in Denial of the Network, Enterprise, and Mission by JP.

The names of the remaining levels are: Enterprise manipulation and mission manipulation. In this definition, "physical" simply refers to the fact that manipulation takes place outside of cyberspace. The physical systems themselves as well as the cognitive level of those using those systems are included in this definition. It explains how to manipulate the human component of a system to change or influence it. More intrusive network access is required for deeper manipulation attacks, which necessitate a deeper comprehension of the systems involved. This knowledge and access are required to successfully manipulate, deceive, or otherwise influence the behavior of users within the target organization.

Level 1: Network Denied

A network is unable to communicate with other networks as a result of this kind of cyber attack. The first level of attack is utilized the most because it is the easiest to launch and the most difficult to stop. The information itself is not the target of Level 1 Network Denial; rather, it is its transmission. These assaults can go after the whole organization or a piece of it. They can be carried out in a number of different ways, many of which are very difficult to stop. Level 1 attacks compromise the target's ability to communicate with the other organization, but internal processes are largely unaffected.

Example: A straightforward illustration of a network denial is when an attacker attempts to transfer data by forcing entry and intercepting routers at the organization's network boundary. This state prevents the target organization from using the computer network or sending any information outside of it for a time period and isolates it from all network traffic. This kind of network isolation will have an impact on the operations of any organization, but only as long as the target is unable to restore proper functionality.

Level 2: Enterprise Denial

A digital assault brings about the clients of the association being denied admittance to their information. In the event that a cyber attack occurs at a later stage, it may even render an organization inoperable while also interfering with end users' day-to-day activities. Enterprise refers to the systems and applications that users use every day. One example of a daily activity that is affected by Level 2 attacks is the ability to log in. Level 2 attacks, in contrast to Level 1 network denial, specifically conceal information with which an organization's users directly interact.

Example: Ransomware Malware, or "ransomware" as it is presently alluded to by cybercriminals, is the most normal illustration of a Level 2 assault. Without the use of ransomware, users encrypt and access their data, making it impossible for an organization to identify the threat before it has accomplished its intended goal. Files that need to be encrypted are essential to the system and users due to the fact that malicious software attacks all files, historical records, activity records, daily tasks, and any other files used for company work are significant. Businesses suffer greatly as a result of attacks of this kind.

Level 3: Enterprise Manipulation

A cyber attack in which users of an organization are coerced into making decisions without being identified. The first level of manipulation is manipulation with the goal of changing the opponent's behavior rather than preventing them from carrying out business operations. Level 2 Enterprise Denial attacks target the same computer systems as these attacks, but they use a deep understanding of the organization to affect or contaminate normal organizational processes without denying them. In addition, a level 3 attack's primary goal is to carry it out without the user's knowledge. The primary distinction between level 3 and the other two levels is based on this.

Example: Despite the fact that data manipulation has only recently been openly discussed. It is not difficult to imagine the ongoing chaos. "Mr. Robot" has captivated producers of television shows like these attacks and series. These attacks can be as simple as deleting important emails, locking out particular accounts of customers, or altering important records of customers. Attacks that are more local and potentially widespread can be devastating because they can control data on finances or human resources, for example.

Level 4: Mission Denied

A cyber attack that specifically prevents an organization from carrying out its mission-critical processes or systems. The scope of frameworks and cycles essential for an association to satisfy its center mission is the sole focal point of the last two levels of the digital assault range. Examples of this focus include the destruction of mission-critical data or, in very specific circumstances, the physical destruction of hardware by manipulating industrial control systems. Level 4, Mission Denial, is more accurate than Level 2, Enterprise Denial.

Example: The 2015 Russian attack on Ukraine's power grid is a prime example of a level 4 cyber attack. Russia gained crucial, undetected access to three primary Ukrainian power companies during this attack. Once inside the network, the malicious actors immediately targeted the internal operator's power generation control system. As workers evaluated the system, operators had to spend a lot of time learning which interfaces were used to control the power generators. When they were discovered, the intruders systematically shut down the generators and disabled the computers' remote controls. Each generator had to be manually restarted by technicians, which took six hours. By allowing power generator operators to restore the system remotely, this was prevented.

Level 5: Mission Manipulation

A cyber attack that alters processes or systems that is crucial to an organization's mission, both intentionally and unintentionally. Mission manipulation is the cyber attack spectrum that is the most advanced and strategically complex. Repeated and persistent mission manipulation can disrupt an organization's fundamental mission.

The primary distinction between Level 5 and Level 4 attacks is that they are carried out undetected. Even though this is a minor difference, achieving it is extremely difficult.

Example: tampering with and destroying systems that are essential to a mission. To date, only one cyber attack has been made public, demonstrating the necessity of concealing those actions: Stuxnet. Stuxnet is well known for the actual obliteration it caused to Iranian rotators between April 2009 and June 2010. However, Stuxnet's true genius lies in its clever deception. Stuxnet systematically destroyed these mission-critical centrifuges and manipulated monitoring components to inform engineers that they were operating properly.

Cyberspace Attacks and Weapons

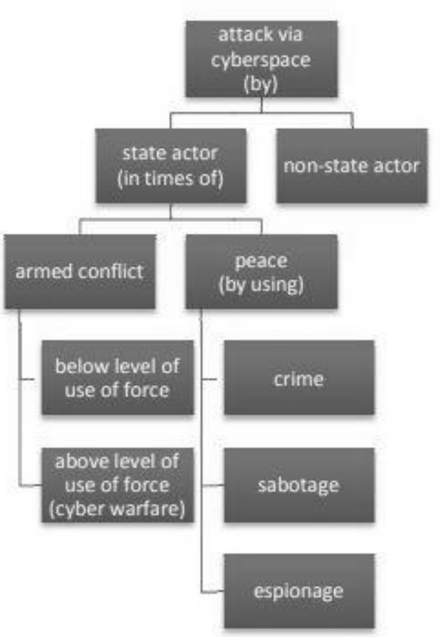
10.3 Cyber Space:

In the past few years, the concept of cyberspace has received a lot of attention. Digital technologies are becoming more and more important to people. Virtually everyone and everything is affected by cyberspace. Because of this interdependence, targeted attacks on or through cyberspace have the potential to have a significant impact on society: large-scale cyber attacks on vital infrastructure like energy supplies, communication systems, financial markets, and military infrastructure have the potential to cause harm.

Consequently, cyber security is practically ingrained in today's national and international security politics. The German Interior Minister, Thomas de Maiziere, issued a caution regarding the high potential of IT-security threats in Germany in a recent report. In addition, the Obama administration's security strategy has placed a significant emphasis on cyber security ever since 2009. "One of the most serious economic and national security challenges," according to the White House, is cyber security. Cyberspace, on the other hand, not only poses a threat to national security but also opens up new avenues for war. In point of fact, the military regards cyberspace as a fifth battlefield.

10.4 Cyber Attacks

The issue of how to respond to a Cyber Attack is so contentious because the definition and nature of cyber attacks is rapidly changing. The cyber attack response will first be determined by the identified perpetrator (state actor or non-state actor, as shown in the figure). Though non-state actors must be prosecuted, while an attack by a state actor can occur in either armed conflict or peace. The most important question is whether Cyber Attacks during armed conflicts fall under international humanitarian law. The kind of attack (cybercrime, cyber espionage, or cyber sabotage) and its consequences (such as access, manipulation, disruption, damage, or destruction) during peacetime.


attack via cyberspace (by)
state actor (in times of)
non-state actor
armed conflict
peace (by using)
below level of use of force
above level of use of force (cyber warfare)
crime
sabotage
espionage

(fig. 10.1)

In light of this, a globally accepted definition of cyber attacks is clearly required. However, international actors have not been able to agree on anything at this time. In point of fact, the various actors' definitions of a cyber attack vary significantly. Listed below are a few definitions that may illustrate various approaches to cyber attacks: NATO is taken into consideration after Germany and the United States due to the military alliance's approach to cyber attacks. It might be fascinating to look into. The Tallinn Manual provides a legal and non-governmental viewpoint once more.

(Four definitions of cyber attacks and their specifics)

CYBER ATTACK	Germany	USA	NATO	Tallinn Manual
Attacker	Cyber espionage: launched/ by foreign intelligence service only state actors Cyber sabotage: unspecified	Unspecified	Unspecified	Predominantly state actors
Context	Peace (and armed conflicts)	Peace (and armed conflicts)	Peace (and armed conflicts)	Armed conflicts

Type of attacks	Cyber espionage and cyber sabotage	cyber sabotage	cyber sabotage	Cyber-attacks in armed conflicts
Level of impact	Confidentiality, integrity and/or availability	Integrity and/or availability	Integrity and/or availability	Injury or death to persons or damage or destruction to object

(Cyber-attacks in peace and armed conflict in legal studies)

CYBER ATTACK	**Executed in times of peace**	**Executed in armed conflicts**
Actors	Mainly by state actors	Mainly by state actors
Legal issue	Application of jus ad bellum	Application of jus in bello
Main dispute	(When) does a cyber attack justify a use of force so that the right of self-defense applies for the attacked state?	(When) does a cyber-attack reach the level of a use of force so that IHL applies?
Viewpoints in research	Consensus that a categorization of the effects of cyber attacks is needed, and that internationally accepted definitions for the terms cyber attack, cyber space and cyber weapon are also needed	2 different approaches: permissive (allowing a wide range of cyber attacks against the civilian population) vs. restrictive approach (restricting cyber attacks as a matter of law)
Legal papers	Charter of the United Nations	Tallinn Manual, IHL (Additional Protocol of the Geneva Convention of 1949)

10.5 Cyber Weapons:

10.5.1 Introduction:

The new field of warfare known as "cyber space" is accepted in the age of information technology, but its definition is still disputed worldwide. The situation with cyber weapons is similar. Recent war between Ukraine and Russia is the latest instance where initially large extent of cyber attacks made before beginning of physical military confrontation in February, 2022. Richard A. Clarke, a security expert for the US government, defines cyber warfare in his book as significant actions to gain access to another nation state's computer or network within one nation state's computer or network with the intention of causing damage or disruption. Cyber weapons are tools for fighting between nations.

Weapons essentially mean and are considered as "instruments of mischief". Man has used weapons to hunt, show off, or gain power since the beginning of time. As a result of the need to deter the perceived threat and the advancement of modern technology, the variety of weapons, as well as their range, power, and accuracy, have significantly increased. Therefore, weaponry has evolved over time. The amount of time it takes to turn a concept or material into a product or weapon has decreased due to the rapid pace of technology development and its engineering into production. As predictable weapons, cyber weapons are also developing at a very rapid rate. With the help of technology, new threats can emerge in the cyberworld in days or even hours. The most significant development of cyber weapons, such as the demonstration in the real world, has occurred as a result of the Stuxnet attack on an Iranian nuclear facility.

10.5.2 Definition:

We must define cyber weapons as such because of the significant specific political, security, and legal issues involved. Both the level of threat posed by a cyber attack and the responsible characterization of political and legal issues and the associated political and legal responsibilities for the attacker must be addressed. As a result, there may be two definitions, one provided by a security expert and the other by lawyers, as shown below:

A cyber weapon is a piece of computer code that is used to cause problems, harm, or threaten any structure, system, or living thing physically, mentally, or functionally.

"When any device, computer command, or set of instructions is intended to destroy or damage a system, its data, programs, or information that serves as a critical infrastructure, or even interrupts, in whole or in part, or is intended to facilitate the updating of its operations."

There is a gigantic scope of conceivable outcomes that digital weapons rely upon and could on a fundamental level expand: from "tailored" malware like Stuxnet, which has a high level of infiltration and collateralization, to denial-of-service attacks, which typically involve a low level of penetration characterized by a low damage rate., It can be difficult to evaluate cyber weapons based on their importance in cyberspace because of their distinct potential to cross effective boundaries and into the real world.

10.5.3 Categories of Cyber Weapons:

Cyber weapons can be classified on basis of four parameters:-

(a)Precision: This is a parameter of capability for targeting the specific objective only and to decrease possibility of damages of security.

(b) Intrusion: It is about penetration level to get inside target.

(c) Visibility: It is capability to make us undetectable.

(d) Ease of Implementation: To develop the particular cyber weapon, it’s a measurement needed for that.

10.5.4 Need of Cyber Weapons:

Straight military strikes are very opposite to the use of cyber weapons. It has possibilities of:-

(a) Destroying adversary defenses critical structure by supporting obnoxious operations.

(b) Check the special abilities of the antagonist by assessing the ability of the agent to infect the antagonist's system.

(c) Cyber weapons are more effective and less costly.

(d) The attack is carried out at the speed of light.

(e) Cyber weapons are low noise (covert munitions) - no one wants to admit the sins of their system.

(f) Criterion is veritably delicate- working undercover makes cyber likely veritably seductive armament.

(g) Cyber munitions are obnoxious and ideal munitions for asymmetric warfare- 21st century warfare.

(h) It's easy to hide the medication phase of cyber munitions from prying eyes and it’s delicate to identify the development of cyber munitions.

With these advantages, small states have been very attracted by cyber weapons that even if they have decreased funds for military expenditure and budget just to compete with the most powerful countries in the new type of field or area. The development of cyber warfare capability is engaged in nearly 140 countries in the world so far at present.

10.5.5 Targets of Cyber Weapons and Impact on Cyberspace:

Cyberspace-based spread of malicious program agents can result in significant human loss of life and damage to vital infrastructure. Cyber weapons have been developed to deal with these situations because they are extremely serious and have a direct impact on the system. However, security systems also suffer as a result of the uncontrolled flow of cyber weapons. Cyber attacks can cause damage to civilians comparable to that of a direct attack. The area of the spectrum is very high and wide. The critical system or infrastructure of any nation can generally be protected from cyber weapons like:-

- **National Defense Electronic System:** Hacking can be used to gain control of a nation's weapons by entering that nation's defense system. For instance, the state or other concerned nations are likely to hack any missile and launch it. Controlling, intercepting, or disrupting the enemy's defense communication networks can similarly degrade large-scale command and control systems.
- **Hospitals:** If hospital and health center electronic systems can be remotely compromised or misused, cyber attacks can cause serious issues.
- **Critical facility programmable logic controllers (PLCs) or industrial control systems like supervisory control and data acquisition (SCADA) systems:** Any cyber attack that compromises the control or management system of a dam can have a significant impact on chemical plants, power generation facilities, or nuclear sites by altering production procedures and exposing large areas.
- **Water Supply:** Water is one of the population's most valuable resources for life. In large areas without water, stopping the flow of water supplies can result in serious

issues. Changing anything in the water supply's control system may work, but a gradual attack can be very bad, like water poisoning.

- **Civil And Military Air Traffic Control As Well As Fully Automated Transport Control Systems:** Cybercriminals can profit from numerous transportation systems that do not require conductors or drivers and do not require any human resources to operate. or grant access control and operation of transport. Consider the potential consequences of such an attack on the air traffic management system or train control system.
- **System for Controlling the Electricity Grid:** A nation's fundamental system is electricity. It is also a serious problem if these systems are attacked and the power supply is disrupted, which could result in a complete power outage for services like hospitals, computers, and telecommunications. Digital assaults can track down an obvious objective and their digital system is principal to their guard.
- **Networks for Data and Communication:** Financial platforms and banking systems: Blocking the transfers of money can cause serious issues because financial systems are the foundation and essential assets of almost every national system. A nation's financial system can be disrupted or blocked for all economic operations by a cyber attack, even if no human lives are directly lost. Since a single state's financial system is connected to the nation's economy, problems in one state's economy can cause serious and unpredictability in the entire financial system.

10.5.6 Limitations of Cyber Weapons:

There are so many dangerous effects of using a cyber weapon because of unpredictability of its issues when it’s out of control since cyber space has no boundaries. Some of the limitations are as follows:-

(a) There are numerous flighty manners by which digital weapons can influence different frameworks and organizations that are not really targets. It can likewise represent a serious danger to the host country's frameworks from the going after innovation in a kind of "boomerang style impact".

(b) Some vindictive individual can utilize digital weapons in the internet to figuring out any programming code and opens up a great deal of potential outcomes. Hacktivists, foreign governments, cybercriminals, and cyber terrorists may be able to spread new cyber threats and detect, isolate, and analyze existing ones in problematic systems.

(c) Cyber weapons have self life limitation because they are just developed to misuse a particular weakness of system instead of entire system.

(d) The complexity of the cyber weapon can relate to expansion of attack and level of damage is inversely proportional.

10.5.7 Generations of Cyber Weapons:

Like other weapon frameworks, there are three ages of digital weapons as indicated by time, innovation and danger mindfulness as follows:

Generation 1: Weapons that can blind, kill, degrade, or incapacitate through physical attack or conventional electronic warfare (or (anti-)radiation). These are effective weapons for command and control. The basis is the degree of appropriated impact. Downgrading, very tightly controlled deployment, and disruption of communication are the usual effects of targeting. The 1982 explosion of the Siberian oil pipeline is one example utilizing carbon fiber to short the electric grid in order to dismantle the power grid in Iraq; blowing up the phone system in Baghdad during the Gulf War, for example.

Generation 2: Implementations of technology that are derived from hardware and software and enable specific targets to exploit vulnerabilities in a system or systems. These are distinguished by the requirement that the system design, configuration, or software implementation contain an exploitable feature. It is additionally portrayed by a weighty dependence on network framework, despite the fact that they may not be the essential system of double-dealing. There are various levels of entry barriers. Traditional features like espionage and sabotage have varying degrees of sophistication and deployment control. Estonia7 and Georgia8 will qualify the occasion.

Generation 3: After that, weapons of Generations 1 and 2 transform into point-and-shoot weapons that are able to degrade, disrupt, or destroy an adversary's systems without needing to take advantage of vulnerabilities. The adversary is no longer required to make errors. These sorts of weapons annihilate the order and control, (correspondence and coordination) conduct of the digital framework. Speed of deployment and selective targeting are two new features.

Weapons of Generation 1 primarily hinder the availability of systems and the infrastructure on which they operate. Weapons of Generation 2 target protocols and applications running on top of the network at the logical layers. At last, Age 3 weapons seem bound to work against whole framework foundation, including people.

According to their threat level, cyber weapons fall into three main categories:

(a) Destroyers: The purpose of these programs is to erase entire databases and information. These are known as "logic bombs," and they are firstly pre-installed in the systems of the enemy and then activated at a predetermined time or immediately during a targeted attack. The most well-known example of this kind of malware is Wiper.10

(b) Spying applications: These groups include cyber weapons (malware) like Pegasus, Gauss11, DQ12, and MiniFlame13. This kind of malware is used to collect as much data as possible, particularly to access data that is highly specialized.

(c) Cyber Sabotage Tools: Cyber sabotage tools, in which threats cause physical harm to the intended outcomes, are the ultimate form of cyber weapons. The Stuxnet worm naturally falls into this category.

These unique threats necessitate significant intelligence and R&D resources. In addition to defending themselves against these threats, many developed and networked nations are actively developing them.

10.5.8 Cyber Weapons:

The New WMDs:-

As the Information Age ushers in a new, low-cost alternative, a type of cyber warfare for strategic defense in general and cyber weapons in particular, the Industrial Revolution brought about a fundamental shift in warfare. After that, the majority of strategic objectives could now be accomplished with the ever-important nuclear or air superiority capability. The circumstances are comparable to those of early nuclear theory, which attempted to comprehend cyber weapons by addressing the same kinds of issues.

(a) As an anti-coercive weapon (power projection capability at a low cost), some important issues are as follows: If long-range strike has the potential to be as effective as cyber warfare, then it could be very useful.

(b) A strong cyber capability is a deterrent that significantly reduces external interference in domestic and regional affairs.

(c) Cyber weapons, which require a fraction of the forward investment or strategic air power of nuclear weapons but can still carry out similar missions with minimal or no collateral damage, could form a force that is comparable to nuclear weapons. The cyber weapon's intended duration of operation may result in an entire electrical grid blackout that can be reversed with a single switch click!

(d) These weapons could have been used to launch a devastating cyber attack with the speed and accuracy of a warning shot. This attack could cost trillions of dollars and cause unexpected inconvenience to people.

Framework for Improving Critical Infrastructure Cyber Security

There is no one-size-fits-all strategy for managing cyber security risks to critical infrastructure that is based on a framework. The framework's practices will continue to be implemented in a variety of ways, and organizations will continue to face their own unique set of risks with varying risk tolerances, vulnerabilities, and threats. In order to get the most out of each dollar spent, organizations can prioritize investments and identify activities that are essential to providing essential services. The framework's ultimate objective is to lessen and manage cyber security risks more effectively. This framework is a living document that will be improved and updated as industry feedback on its implementation is received.

10.6 Framework Introduction:

The public and financial security of any nation relies upon the dependable working of basic security framework.

In view of rising cyber attacks and threats, Indian Government introduced an amendment in Section 70A of the IT Act, 2000 (amended 2008), through a gazette notification on 16 January 2014 to lay down the creation of new organization National Critical Information Infrastructure Protection Centre (NCIIPC) for securing India’s critical information infrastructure. NCIIPC further will be accountable for all measures, including R&D of new framework for cyber security in relating to the protection of critical information infrastructure.

On February 12, 2013, US President Obama issued Executive Order, "Improving Critical Infrastructure Cyber Security," to improve this infrastructure's resilience. A voluntary cyber security framework—the "Framework"—that provides a "prioritized, flexible, repeatable, perform-based, and cost-effective approach" to the delivery of critical infrastructure services is required by this executive order. An organization can get direction for managing cyber security risk thanks to the framework, which was developed in conjunction with the industry.

To ensure extensibility and facilitate technological innovation, the framework is technology neutral. The framework builds on a variety of existing standards, guidelines, and practices to make it possible for providers of critical infrastructure to achieve flexibility. By relying on global standards, their guidelines, and evolving practices that are updated by management and industry, the tools and methods available to achieve the Framework's outcomes will cross borders, acknowledge the global nature of cyber security risks, and acknowledge technological advancements as well as grow with the business requirements. Through the use of existing and new standards, it will be easier to create effective products, services, and processes that meet identified market needs.

The Framework provides organizations with a general classification and mechanism for building on those standards, guidelines, and practices:

1) Describe their current approach to cyber security.

2) Describe the state they want to have the best cyber security in.

3) Identifying opportunities for improvement and giving them priority in the context of a process that is continuous and repeatable.

4) Evaluate the progress made toward the goal state;

5) Discuss cyber security risk with stakeholders both internal and external.

An organization's cyber security program and risk management process are complemented, not substituted, by the Framework. The framework and the organization's existing procedures can be used to identify opportunities for communication and improve cyber security risk management in accordance with industry standards. Alternately, the Framework can be used as a reference to establish a cyber security program for an organization that does not already have one.

In the same way that the Framework is not industry-specific, the Framework's general classification of standards, guidelines, and practices is not country-specific. Organizations outside of the any nation can use the Framework to boost their own cyber security efforts and contribute to the development of a common language for international cooperation on critical infrastructure cyber security.

10.7 Overview of the Framework:

The following sections make up the framework, which is an approach to network security risk monitoring that is based on gamification: Profile, Core, and the implementation level of the Framework. Each part of the framework reinforces the connection between cyber security activities and business drivers. These components are as under:

- **The Framework Core**
- **A Framework Profile**

10.8 Risk Management and the Cyber Security Framework:

The continuous process of identifying, evaluating, and responding to risks is known as risk management. Organizations must comprehend the likelihood of an event occurring and its impact in order to manage risk. With this data, associations can decide a satisfactory degree of chance for the conveyance of administrations and express this concerning their gamble resistance.

With a comprehension of chance resilience, associations can focus on network safety exercises, permitting associations to settle on informed conclusions about digital protection spending. Organizations can quantify and communicate changes to their cyber security programs through the implementation of risk management programs. Depending on the potential impact on the delivery of essential services, organizations may choose to manage risk in a variety of ways, including mitigating risk, shifting risk, avoiding risk, or accepting risk.

Organizations can use the Framework's risk management procedures to better inform and prioritize decisions about cyber security. In order to assist businesses in selecting target states for cyber security activities that reflect desired outcomes, it supports recurring risk assessments and validates business drivers. As a result, the Framework gives businesses the ability to choose and direct changes to cyber security risk management for IT and ICS environments in a dynamic way.

10.9 Framework Basics:

The Framework provides a common language for understanding, managing, and expressing Cyber Security risk both internally and externally. It can be used to help identify and prioritize actions for reducing Cyber Security risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage Cyber Security risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

10.9.1 Framework Core:

The Framework Core provides a set of activities to achieve specific Cyber Security outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key Cyber Security outcomes identified by industry as helpful in managing Cyber Security risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in Figure 1:

10.9.2 The Framework Core elements:

The following is how the core components of the framework interact with one another:

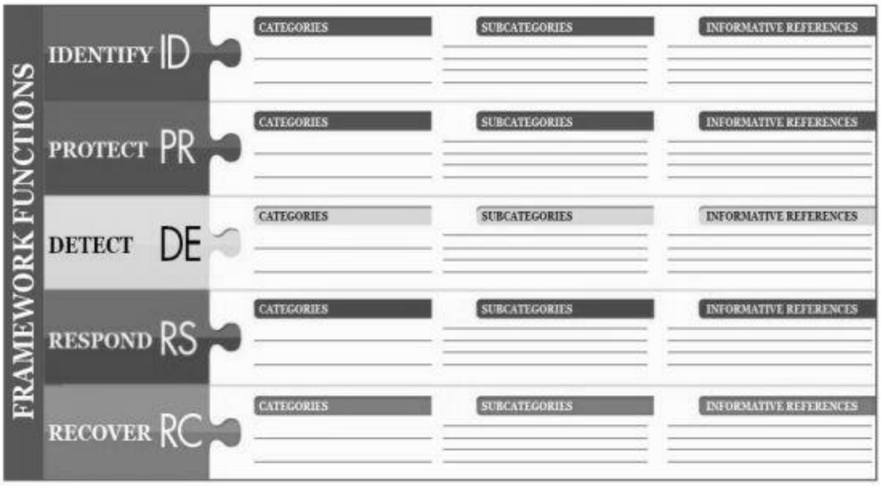
- **Function:** The functions organize fundamental cyber security activities at the highest level. Identifying, protecting, detecting, responding, and recovering are all examples of these functions. By organizing information, facilitating risk management decisions, addressing threats, and making improvements through learning from previous activities, they assist an organization in articulating the management of cyber security risk.
- **Categories:** Cyber security outcomes that are closely linked to program requirements and particular activities are grouped into categories of a function. "Management of Asset," " Controlling of Access," and " Process of Detection " are good examples of categories.
- **Subcategories:** further gap a classification into explicit consequences of specialized or potentially the board exercises. They give a bunch of results that, while not thorough, assist with

supporting the accomplishment of results in every classification. "External information systems enlisted," "Data-at-rest protected," and "Informations from detection systems screened" are examples of subcategories.

- **Informative References:** Specific sections of critical infrastructure sector standards, guidelines, and practices that provide a method for achieving the outcomes associated with each subcategory are referred to as informative references. The Framework Core's informational references are merely examples and not comprehensive. Throughout the framework development process, cross-sector guidance is frequently cited as their foundation.

10.9.3 Framework Core Functions:

The definitions of the five following functions do not have the intention of leading to a stable desired end position or creating a serial path. Instead, an operational culture that addresses dynamic cyber security risk can be created through the simultaneous and continuous execution of tasks.



(fig. 10.4)

- **Identify:** Develop an understanding of cyber security risk management for the organization's systems, assets, data, and capabilities. The Identify function's activities are crucial to the Framework's efficient use. An organization can focus and prioritize its efforts in accordance with its risk management strategy and business requirements if it comprehends the business context, the resources that support essential functions, and the cyber security risks that are associated with them.

- **Protect:** Create and execute proper safety efforts to guarantee the conveyance of basic foundation administrations. The Safeguard capability upholds the capacity to restrict or control the effect of a potential digital protection episode. Instances of result classifications under this capability include: Control of access; training and awareness; data safety; procedures and processes for information security; maintenance; and safety equipment.
- **Detect:** Identify the occurrence of a cyber security incident by planning and carrying out appropriate activities. The detect function makes it possible to quickly find cyber security incidents. Instances of result classifications inside this capability include: irregularities and episodes; Continuous Security Monitoring; and test methods.
- **Respond:** To respond to a cyber security incident that has been identified, develop and carry out appropriate actions. The ability to control the effects of a possible cyber security incident is supported by the Respond function. This function's result categories include the following: planning for response; Communications; analysis; Mitigation; and advance.
- **Recover:** In order to maintain plans for resilience and restore any capabilities or services that may have been impacted by a cyber security incident, develop and carry out the appropriate actions. The recuperation capability upholds ideal recuperation to ordinary tasks to limit the effect from a digital protection episode. This task's result categories include, among others: planning for recovery; Improvement; and interaction.

10.10 Framework Profile

The alignment of the organization's functions, categories, and subcategories with its business requirements, risk tolerance, and resources is referred to as the Framework Profile (or Profile). A profile lets businesses make a plan for reducing cyber security risk that is in line with the goals of the company and the industry, takes into account legal and regulatory requirements and industry best practices, and reflects priorities for risk management. They can select from a variety of profiles, combine them with specialized elements, and determine their individual requirements in light of the complexity of many organizations.

Specific cyber security activities' current or desired target states can be described with the help of framework profiles. The cyber security outcomes that are currently being achieved are depicted in the current profile. The outcomes needed to achieve the desired cyber security risk management goals are shown in the Goal Profile. Profiles facilitate risk communication within and between organizations and support the requirements of the business or mission. Flexibility in implementation is provided by the absence of a profile template in this framework document.

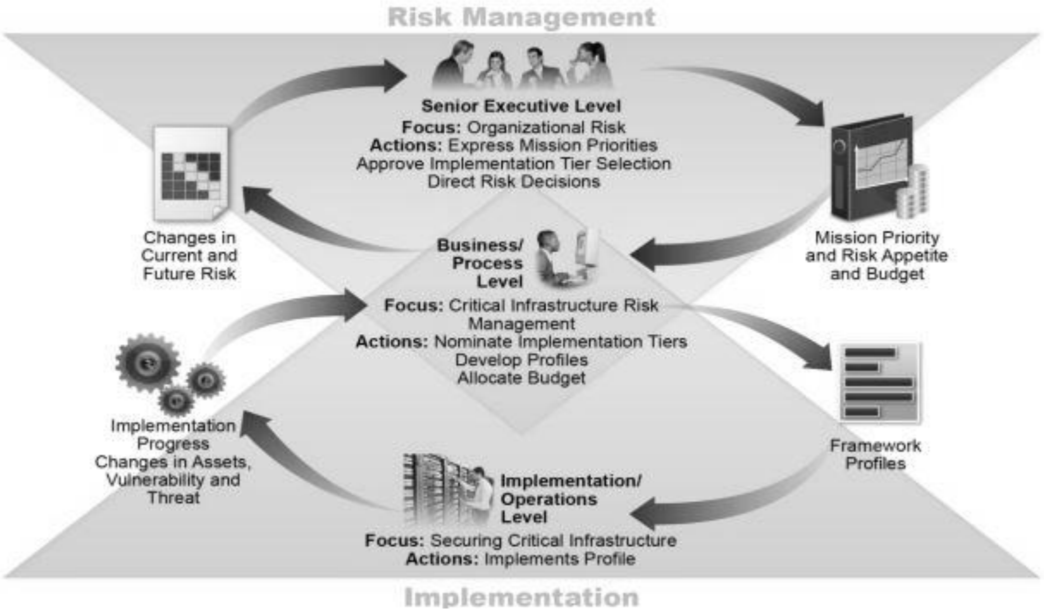
Cyber security risk management objectives may not be met if profiles are compared, such as the current profile and the target profile. The aforementioned road map might benefit from an action plan to fill in these gaps. The need of whole decrease is driven by the association's business needs and chance administration processes. An organization can scale resource projections, such as funding and staffing, using this risk-based strategy to achieve cyber security goals in a cost-effective and prioritized manner.

10.11 Coordination of Framework Implementation

Figure 10.5 depicts a normal progression of data and choices at the accompanying levels inside an association:

- **Executive**
- **Business Process**
- **Implementation/Operation**

At the business/process level, the executive level determines the mission priorities, available resources, and overall risk tolerance. The information is used as input into the risk management process by the business/process layer, which then works with the implementation/operational layer to communicate business requirements and make a profile. The progress of the implementation at the business/process level is recorded in the Implementation/Operational Level profile. Impact assessment is carried out with this information at the business/process level. The results of that impact assessment are presented by business/process level management to the executive level for use in the organization's overall risk management procedure and to the implementation/operational level for awareness of the impact on the business.


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress
Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

(fig. 10.5)

10.12 Check Your Progress

1. ____________________________is a kind of cyber attack that stops a network communication for connecting with external network.
2. ____________________________________ is a cyber attack in which users of an organization are coerced into making decisions without being identified.
3. In this Information technology Age, the new domain of warfare is accepted and referred to as_________________________________.
4. A computer code that is used to cause problems or to harm or threaten any structures, systems or living beings physically, mentally or functionally is known as____________________________________.
5. NCIIPC refers to as ____ and
6. PLC refers to as ____.

7. WMD stands for ____.

8. There are ________________ stages of Cyber Triad.

9. The ______________________ is a set of Cyber Security actions, desired results and references to apply that are common sectors of critical infrastructure.

10. The ______________________________ can be utilized by an organization as an essential component of its systematic method for identifying, evaluating, and managing cyber security risk.

10.13 Summary

Introduction to the Spectrum of Cyber Attack:

. Since evolution of the internet, our dependent on computers and data flow driven technologies has greatly increased our potential for vulnerability if our system face any cyber attack. Information systems around the globe nowadays receive huge attempts of intrusion and this trend seems to be exponentially increased after breakdown of COVID-19 pandemic, when most crucial services go online nowadays. It is paramount that developing any appropriate defensive or preventive mechanism to systematically counter the cyber attacks in near future.

The Framework of cyber attack spectrum:

In recent decades, a lot of stress has been given to expedite the field of cyber attack developments and its defense mechanisms. Even today, India is lagging far behind when discussions go around the capabilities of encountering cyber attacks.

Leaders and planners around the globe at the operational level attempts to outline the objectives to be pursued, describe the anticipated end-states, and articulate the various trade-offs between methods if they understand the cyber attacks at each level of the spectrum. This makes it possible to give a specific goal the right amount of time, effort, and resources. In the end, commanders will be able to offer a variety of strategies for achieving strategic goals, each of which comes with its own set of risks, rewards, and commitments to resources.

Level 1: Network Denied

Level 2: Enterprise Denial

Level 3: Enterprise Manipulation

Level 4: Mission Denied

Level 5: Mission Manipulation

Cyber Space:

In the past few years, the concept of cyberspace has received a lot of attention. Digital technologies are becoming more and more important to people. Virtually everyone and everything is affected by cyberspace. Because of this interdependence, targeted attacks on or through cyberspace have the potential to have a significant impact on society: large-scale cyber attacks on vital infrastructure like energy supplies, communication systems, financial markets, and military infrastructure have the potential to cause harm.

Cyber Attacks

The issue of how to respond to a Cyber Attack is so contentious because the definition and nature of cyber attacks is rapidly changing. The cyber attack response will first be determined by the identified perpetrator (state actor or non-state actor).Non-state actors must be prosecuted, while an attack by a state actor can occur in either armed conflict or peace.

Cyber Weapons:

The new field of warfare known as "cyber space" is accepted in the age of information technology, but its definition is still disputed worldwide. The situation with cyber weapons is similar. Richard A. Clarke, a security expert for the US government, defines cyber warfare in his book as significant actions to gain access to another nation state's computer or network within one nation state's computer or network with the intention of causing damage or disruption. Cyber weapons are tools for fighting between nations.

Targets of Cyber Weapons and Impact on Cyberspace:

Cyberspace-based spread of malicious program agents can result in significant human loss of life and damage to vital infrastructure. Cyber weapons have been developed to deal with these situations because they are extremely serious and have a direct impact on the system. However, security systems also suffer as a result of the uncontrolled flow of cyber weapons.

Hospitals, industrial control systems like SCADA systems or programmable logic controllers (PLCs) for critical facilities, water supply, fully automated transportation control systems, civil and military air traffic control, power grid management systems, and communication and data networks are all examples of electronic national defense systems.

Generations of Cyber Weapons:

Like other weapon frameworks, there are three ages of digital weapons as indicated by time, innovation and danger mindfulness as follows:

Weapons of Generation 1 primarily hinder the availability of systems and the infrastructure on which they operate. Weapons of Generation 2 target protocols and applications running on top of the network at the logical layers. At last, Age 3 weapons seem bound to work against whole framework foundation, including people.

Framework for Improving Critical Infrastructure Cyber Security:

There is no one-size-fits-all strategy for managing cyber security risks to critical infrastructure that is based on a framework. The framework's practices will continue to be implemented in a variety of ways, and organizations will continue to face their own unique set of risks with varying risk tolerances, vulnerabilities, and threats. In order to get the most out of each dollar spent, organizations can prioritize investments and identify activities that are essential to providing essential services. The framework's ultimate objective is to lessen and manage cyber security risks more effectively. This framework is a living document that will be improved and updated as industry feedback on its implementation is received.

Overview of the Framework:

The following sections make up the framework, which is an approach to network security risk monitoring that is based on gamification: Profile, Core, and the implementation level of the Framework. Each part of the framework reinforces the connection between cyber security activities and business drivers. These components are as under:

- **The Framework Core**
- **A Framework Profile**

Framework Core:

The Framework Core provides a set of activities to achieve specific Cyber Security outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key Cyber Security outcomes identified by industry as helpful in managing Cyber Security risk.

The Framework Core elements:

The following is how the core components of the framework interact with one another:

Function: At the highest level, functions organize basic cyber security activities. These tasks include identifying, protecting, detecting, responding, and recovering.

Categories: Cyber security outcomes that are closely linked to program requirements and particular activities are grouped into categories of a function.

Subcategories: further gap a classification into explicit consequences of specialized or potentially the board exercises. They give a bunch of results that, while not thorough, assist with supporting the accomplishment of results in every classification.

Informative References: Specific sections of critical infrastructure sector standards, guidelines, and practices that provide a method for achieving the outcomes associated with each subcategory are referred to as informative references. The Framework Core's informational references are merely examples and not comprehensive.

Framework Core Functions:

The definitions of the five follow. These functions do not have the intention of leading to a stable desired end position or creating a serial path. Instead, an operational culture that addresses dynamic cyber security risk can be created through the simultaneous and continuous execution of tasks.

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

Framework Profile:

The alignment of the organization's functions, categories, and subcategories with its business requirements, risk tolerance, and resources is referred to as the Framework Profile (or Profile). A profile lets businesses make a plan for reducing cyber security risk that is in line with the goals of the company and the industry, takes into account legal and regulatory requirements and industry best practices, and reflects priorities for risk management. They can select from a variety of profiles, combine them with specialized elements, and determine their individual requirements in light of the complexity of many organizations.

Coordination of Framework Implementation

Figure depicts a normal progression of data and choices at the accompanying levels inside an association:

- Executive
- Business/Process
- Implementation/Operations

10.14 Keywords

- Cyber Threat Spectrum
- Critical Infrastructure
- Cyber Space
- Cyber Attacks
- Cyber Weapons
- Need of Cyber Weapons
- Generations of Cyber Weapon
- Framework for improving critical infrastructure Cyber Security
- Risk Management
- Framework Basics
- Cyber Security Framework
- Framework Core

- Framework Implementation Tiers
- Framework Profile
- Cyber Security Practices
- Cyber Security Program
- Cyber Security Risk

10.15 Self Assessment Test

Q.1 Describe Cyber Threat Spectrum and its framework.

Q.2 Explain Cyber Space, Cyber Attacks and Cyber Weapons.

Q.3 What are the categories of Cyber Weapons, its need, limitations and generations?

Q.4 Define Framework for improving Critical Infrastructure Cyber Security.

Q.5 Explain Framework Basics – Framework core, its elements and functions.

Q.6 Describe Framework Implementation Tiers.

Q.7 How to use the Framework? Please describe it.

Q.8 Explain methodology to protect privacy and civil liberties.

10.16 Answers to Check Your Progress

1. Network Denial
2. Enterprise Manipulation
3. Cyber Space
4. Cyber Weapon
5. National Critical Information Infrastructure Protection Centre
6. Programmable Logic Controllers
7. Weapons of Mass Destruction
8. Three
9. Framework Core
10. Framework

10.17 References

1. Thomas A. Johnson, "Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare", CRC Press, ISBN:978-1-4822-3923-2, 2015.
2. Nina Godhole and SunitBelapure, Cyber Security, Wiley India, 2011
3. https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
4. https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/
5. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-4/V-Musielewicz.pdf
6. https://usiofindia.org/publication/usi-journal/cyber-weapons-the-new-weapons-of-mass-destruction

NOTES

NOTES

NOTES