unit-1

* Introduction to cybercrime

cybercrime (or) computer-oriented crime is a crime that includes a computer and a network. is called cybercrime.

-> The computer may have been used in the execution of a crime (or) it may be the target.

-> cybercrime is a major issue in 21st century

-> some examples of cybercrime.

- Identity theft
- phishing
- child pornography
- Ransomware

* cybercrime and Information security

cybercrime cybercrime also known as computer crime or digital crime, refers to any criminal activity that involves any use of computers devices, networks, (or) internet is called cyber crime.

Information security

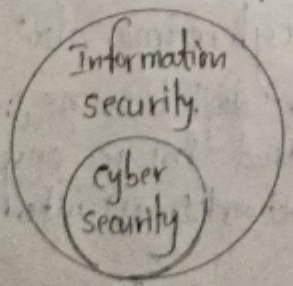
Def: Information security is a board term that includes cybersecurity, as well as other security measures to protect information from unauthorized access, use (or) destruction is called Information security.

-> Information security protects sensitive information from unauthorized activities.

-> The goal of info sec is to ensure the safety and privacy of customer details and financial data.

-> Some common threats to (Info sec):

- Information extortion.
- Sabotage
- Theft of information
- Theft of Identity.
- Theft of intellectual property.



* Difference b/w cybersecurity and Infor security

cybersecurity	Information security
-> protects only digital Information.	-> protects physical and digital Information
-> cybersecurity deals with the danger in cyberspace.	-> Information security deals with protection of data from any form of threat
-> cybersecurity strikes against cyber crimes, cyber frauds etc.,	-> Information security strikes against unauthorized access etc.
-> Act as first line of defence.	-> comes into play when security is breached
-> It primarily addresses external threats.	-> It primarily addresses internal threats.
-> It emphasize technical measures.	-> It emphasize non-technical measures.

* who are cyber criminals

cyber criminals : cybercriminals are individuals (or) groups who use digital devices (or) networks to commit illegal activities such as
- Identity theft
- Fraud
- Malware
- Data breaches etc.

-> cybercrimes are done by cybercriminals
-> cybercriminals are categorized into three groups
- Type-I : cybercriminals - not hungry for recognition
  - Hobby hackers
  - IT professionals
  - politically motivated hackers
  - terrorist organizations
- Type-II : cybercriminals - not hungry for recognition
  - psychological perverts
  - financially motivated hackers
  - organized criminals
- Type III : cybercriminals - the insiders
  - disgruntled
  - competing companies using employes to gain economic advantage

* cybercrime
* The legal perspectives

-> cybercrime possess a mammoth challenge in 1979.
-> computercrime criminal justice Resource Manual (1979)
-> The legal perspective on cybercrime in india is primarily governed by the Information Technology (IT) Act. 2000.
-> The IT Act was enacted to provide legal recognition and electronic transactions and facilitate governance
-> cybercrime - The legal perspectives
- Defining cybercrime legally
- cybercrime legislation
- International cooperation

- Privacy and dataprotection laws
- law enforcement and Investigation challenges
- legal challenges with Eeg Emerging cybercrimes
- cyberatime and civil liability
- preventive legal measures

* The Indian perspectives :

-> cybercrime has became a significant concern in India, affecting individuals businesses, and government Institutions

-> key cybercrime trends in India
- Financial frauds
- social Engineering and phishing
- Identity theft and Dat Breaches :
- Ransomware Attacks
- cyber harassment and cyberbullying
- cryptojacking

-> legal framework in India
India has established a legal and regulatory framework to address cybercrime.
- Information Technology Act, 2000 (IT Act)
- Indian penal code (IPC)
- CERT-In
- data protection and privacy

India faces complex cybercrime landscape that demands concerted efforts from the government, private and public sectors.

* cybercrime and the Indian ITA 2000

cybercrime def :

-> The Information Technology Act (ITA) 2000, implemented in India, was a landmark piece of legislation addressing.

-> Here an overview of how ITA 2000 tackles cybercrime.

-> The Information Technology Act 2000 is also known as IT Act.

-> IT Act proposed by the Indian parliament reported on 17 oct 2000.

-> This IT Act was based on united Nations.

-> It is the most important law in india dealing with cybercrime.

-> The IT Act 2000 has two schedules.
  - First schedule: Deals with the documents.
  - second schedule: deals with the electronic signature.

-> key features in ITA 2000:
  - Digital signatures.
  - Electronic governance.
  - cybercrime prevention.
  - Data protection.
  - Electronic contracts.

-> key sections
  - section 43: compensation for unauthorized access (or) damage.
  - section 66: Hacking, penalty, imprisonment.
  - section 67: publishing obsence Information.
  - section 72: Breach of privacy.
  - section 79: Intermediary liability.

-> Amendments.
  - ITA-2008.
  - ITA-2011.

* A global perspctive on cybercrime:-

cybercrime is a global issue that has been increasing day by day due to rapid development of the internet and computer technology.

-> Global cybercrime damage costs this year are expected to breach us $6 trillion an annum.

-> cybercrime is estimated to cause over $9 trillion in damages globally in 2024.

-> cybercrime makes more money than human trafficking, illegal drug trafficking etc.

-> cybercrime is expected to increase in the coming years globally.

-> New methods for illegal operations such as the use of artificial intellegence (AI) and Internet of things (IOT).

-> AI and IOT will make harder for authorities to detect cyber criminals.

-> cybercrimes which happens globally are:-

- Hacking
- phishing
- Identity theft.
- online harassment.
- Ransomeware.
- Data breaches

-> Global cybercrime statistics are:-

- 2020 : 4.8 billion malware attacks.
- 2019 : 3.5 billion data breaches.
- 2020 : $6 trillion global crime cost.

-> globally Emerging issues:

- AI and machine learning based cybercrime.
- IOT
- cryptocurrency-related crimes.
- social media based cybercrimes
- cyber security and data protection.

-> Now a days cybercrimes are rapidly inareases globally, AI and IOT makes more helpful for the cyber criminals for making crimes.

unit 2

* cyber offences

Introduction :

-> cyber crimes (or) cyber offenses are a range of criminal activities that can involve the use of technology to steal, destroy (or) misuse data is called cyber offence.

(or)

-> cyber offences are cyber crimes, refers to any criminal activity using computer devices (or) networks is called cyber offence.

-> cyber offence is also called as cyber crime.

-> Examples of cyber offence.

- Identity theft
- phishing
- Data breaches
- Malware
- Ransomware
- online harassment
- money laundering
- social media fraud

* How criminals plan the Attacks :

-> cybercriminals plan attacks by developing a detailed strategy towards target.

o Researching the target

-> Attackers identify a ~~tro~~ target and research their systems, people and vulnerabilities.

-> This can include collecting IP addresses, scanning of software and hardware.

o choosing Attack methods

-> Attackers may use a variety of methods, including

- social engineering
- custom exploits
- Network penetration tests.

o. Carrying out the Attack

-> The Attack often happens in stages,

-> starting with compromise and then executing full attack.

-> stealing data, hijacking etc.

o covering their attacks

-> Attackers may use command and control to make it look like there's no threat or DOS to distract security systems.

o some common types of cyber Attacks include :

- Ransomware.
- phishing
- credential attacks
- Hijacked websites.

* cybercafe and cybercrimes :

cybercafe : A cybercafe, is also known as an internet cafe, is a public place where people can access the internet, computers, and other digital technologies. is called cybercafe.

-> cybercafes are popular with students and travellers, people who don't have their own computers (or) internet connection.

-> cybercafe is a safe and secure enviroment for all users.

-> The term "cybercafe" was first used in 1994 when Ivan pope opened one in London.

-> cybercafes ensures that provides security.

-> A cybercafe is a type of business where computers are provided for accessing the internet, playing games, chatting with friends, doing other computer related tasks.

-> There are many cyber cafes located worldwide.

-> A cybercafe is also known as Internet cafe.

-> cyber cafes are far less expensive than personal ownership of computer.

-> Most cybercafes have printers, scanners and other peripherals for customer use.

-> cyber cafes provides fast internet speed

-> cyber cafes are a target for cyber criminals because they are public internet access points.

-> cybercriminals prefer cyber cafes to carry out their activities.

-> cyber criminals may install key loggers on computers in cyber cafes.

* Botnet - The fuel for cybercrime

Botnet : A botnet is a network of compromised computers, devices, or servers controlled remotely by an attacker is called Botnet.

(or)

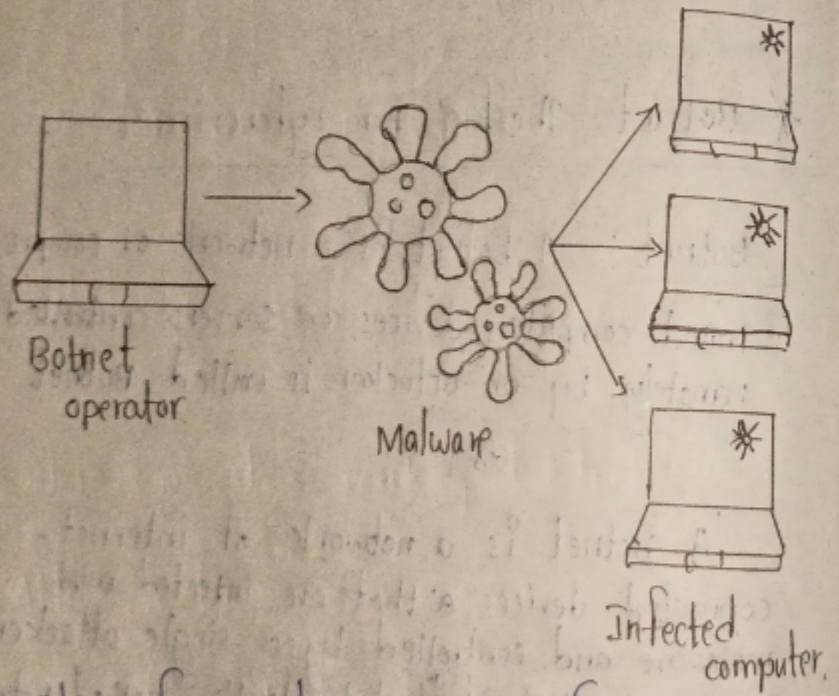
A botnet is a network of internet-connected devices that are infected with malware and controlled by a single attacker known as ~~botnet~~ "bot-herder", is called Botnet.

-> The term botnet is a combination of "robot" and "network".

-> Botnets can be used for malicious purposes such as.

- cyber attacks
- spam.
- Data theft.
- click fraud.

-> "Botnet"



-> Above figure shows overview of Botnet.

-> Botnet consist of Botnet operator, Malware, Infected computer.

-> Here Malware is Malicious software.

Types of Botnet

-> There are three types of Botnets are there.

1. Internet Relay chat (IRC) Botnet

-> IRC botnet act as the c&c channel

-> Bots receive commands

-> A command is in the form of a normal chat message.

-> The limitation of the IRC Botnet, entire botnet can be collapsed by simply shutting down the IRC server.

2. peer-to-peer Botnet :-

-> It is formed using the P2P protocols.

-> It is very difficult to shut down due to it's structure.

-> Each p2p bot can act as the client and server.

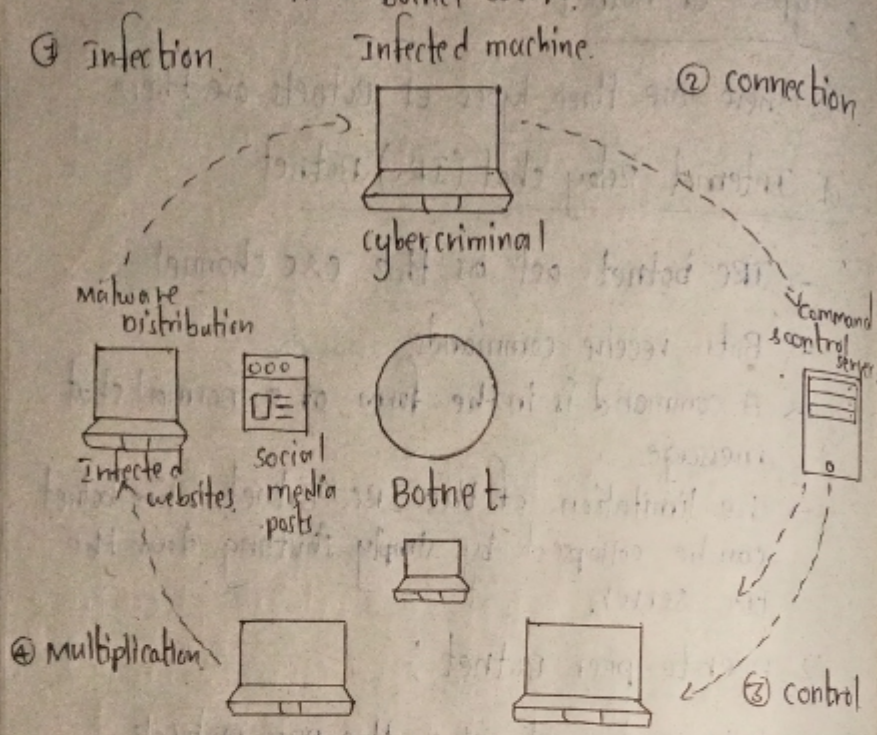
-> limitation is high latency.

3. Hyper text transfer protocol (HTTP) Botnet

-> Bots uses specific URL's and IP addresses.

-> unlike IRC and HTTP bots periodically visit c&c server.

"How Botnet works"



-> Above figure shows working of Botnet.

◦ Attack vector

-> A botnet attack vector is a method that cybercriminals use to gain access to a network.

- ◦ phishing
- ◦ Social Engineering.
- ◦ Infected Firmware.
- ◦ Insider Threats.
- ◦ Exploit kits.
- ◦ Drive by downloads.

◦ cloud computing

Botnets are serious threats to cloud computing, because they can be built using cloud Infrastructure.

- ◦ sending spam.
- ◦ stealing data.
- ◦ Ransomware.
- ◦ DDoS.
- ◦ credential stuffing.

-> Botnet can be used in cloud computing.

- ◦ silent infection.
- ◦ phishing emails
- ◦ C&C architecture.
- ◦ Targeting vulnerabilities.

Unit - 3

* proliferation of mobile and wireless devices

Def The proliferation of mobile and wireless devices in cybersecurity refers to the rapid increase in the production of these devices and resulting security threats

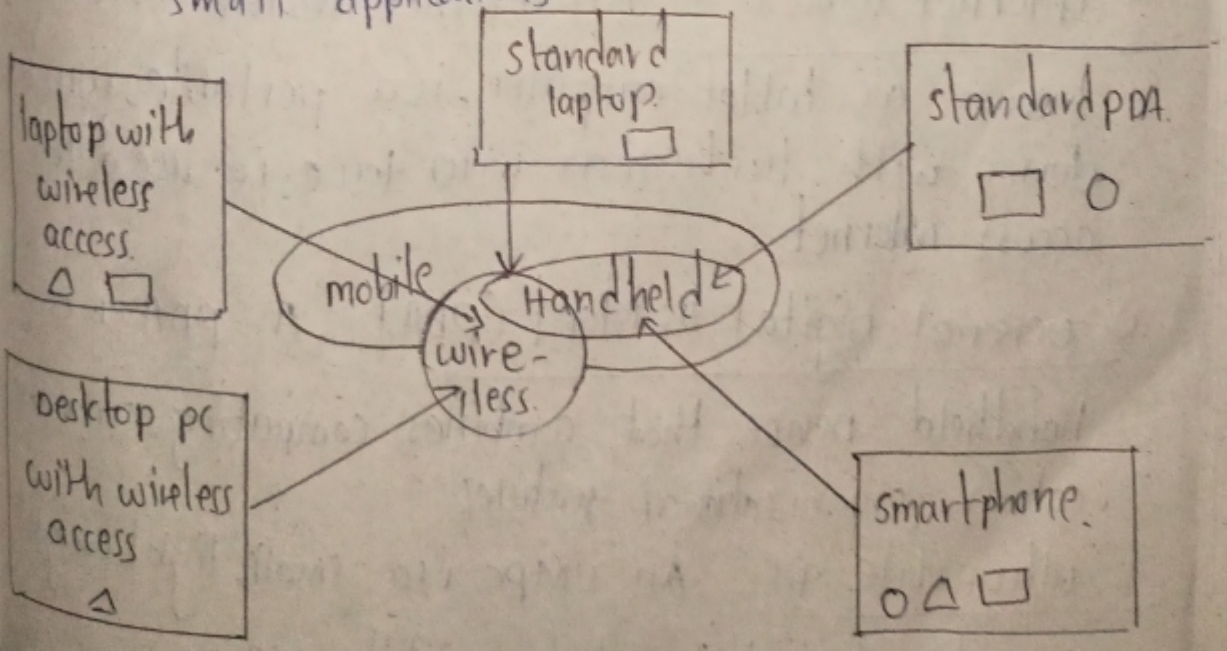
-> The increase in mobile devices has led to a rise in cybercrime.

-> Today incredible advances are being made for mobile devices.

-> The trend is for smaller devices.

-> A few years ago, the ~~chio~~ choice was between a wireless phone and PDA

-> A simple hand-held mobile enough to compute small applications



-> Above block diagram shows mobile, wireless, hand-held devices.

-> Here PDA means personal Digital Assistant.

-> □ mobile devices
△ wireless devices
○ Handheld devices

-> Many type of mobile computers have been introduced since 1990's, They are as follows.

○ portable computer It is a general-purpose computer that can be moved from one-place to another, it requires Ac power source.

○ Tablet PC : Tablet pc is also known as tablet computer (or) tablet, is a portable wireless computer with a touchscreen interface.

○ Internet tablet An internet tablet is also known as tablet computer, is a portable, wireless device with touchscreen interface, ie used to access internet.

○ personal Digital Assistant (PDA) : A PDA is a handheld device that combines computing, communication, organizational features.

○ ultramobile pc : An UMPC is a small, light weight computer. ~~def~~ designed for mobile use.

○ Smartphone A smartphone is a portable personal device that combines features of a computer, phone, advanced computing capabilities is called smartphone.

* Trends in Mobility

Def Trends in mobility refers to the latest developments, advancements in the way people and devices move in the society.

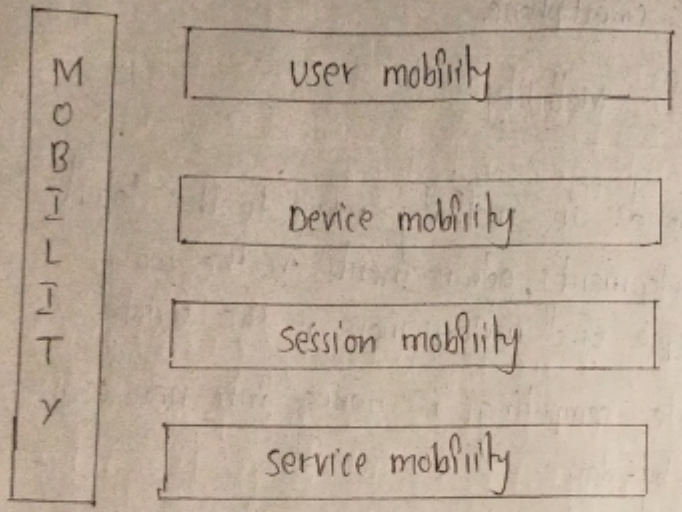
-> mobile computing is moving into new era, day-by-day.

-> "iphone" from Apple and google-led from "Android phones" are the best examples of trend.

-> The smart mobile technology rapidly gaining popularly

-> Below block diagram shows mobility types and implications.

Types of mobility and it's Implications



-> 3G or 3rd generation, is a cellular network technology that allows mobile devices to connect to the Internet.

-> 3G networks offers faster data transfer than previous generations

-> popular types of attacks against 3G mobile networks and worms

o Malwares, viruses and worms many users still using 2G, 3G, it is need to educate community people.

-> Here some examples of malwares

- o skull Trojan
- o caliri worm
- o Mosquito Trojan
- o Brador Trojan
- o Lasco coorm

o Denial of service (DOS) The Denial of service is a cyber Attack that is to make a website, network with the aim of degrading it's performance etc

o overbilling Attack: overbilling attack is a cyber attack, that results in customers being charged for data they didn't use.

o spoofed policy development process

There are attacks in the GTP (General packet Radio service, (Tunneling protocol.

* credit card frauds in mobile and wireless computing era

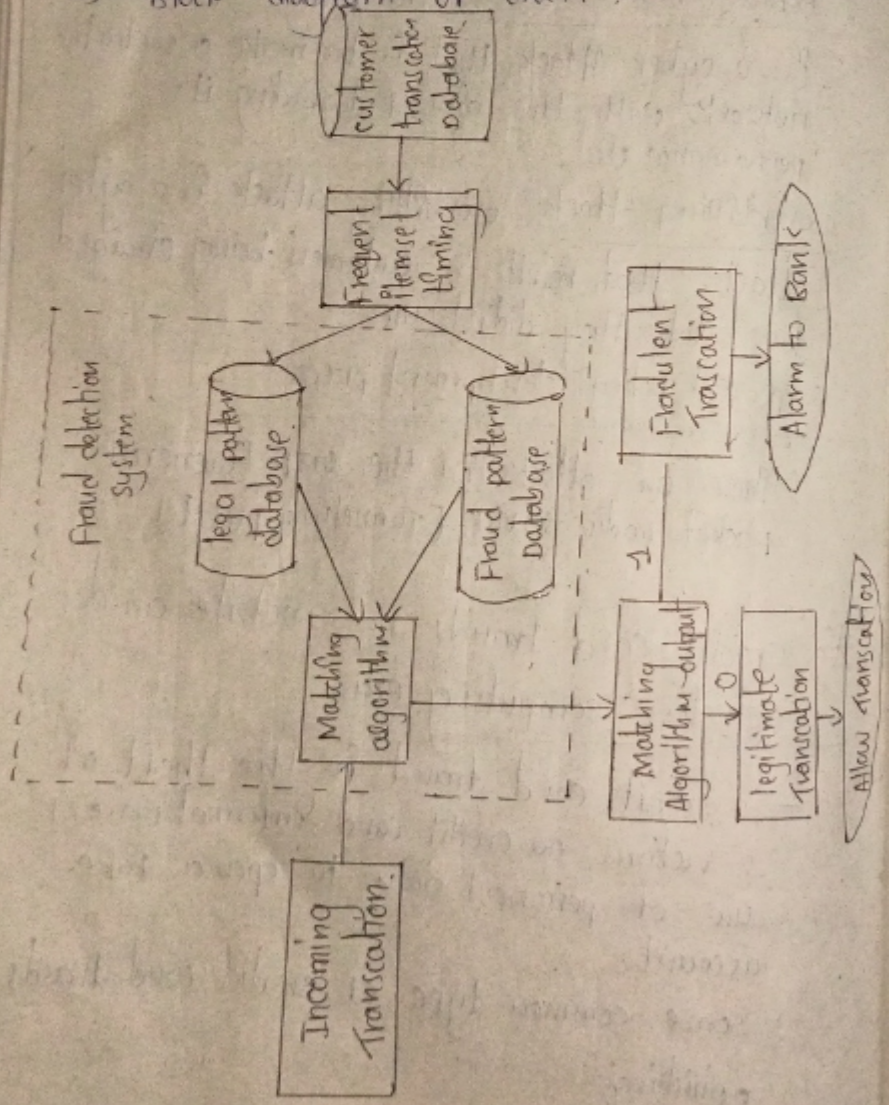
-> credit card fraud is the theft of a victims ~~ea~~ credit card information or use of personal data to open a fake account.

-> some common type of credit card frauds

o phishing.

- Identity theft
- Account takeover
- card-not-present fraud
- skimming
- Application fraud

-> Block diagram of credit card fraud.



-> wireless credit card processing is very desirable system.

-> As above figure shows
  - Incoming Transcation reaches to matching algorithm.

-> legal and fraud pattern databases are given to matching algorithm.

-> matching algorithm is in fraud detection system.

-> if the matching algorithm output is 0, ie. not a fraud.

-> If the matching algorithm output is 1 i.e a fraud transcation.

* security challenges posed by mobile devices

-> Mobility gives two main challenges to cybersecurity

-> first, on the hand-held devices, information is being taken outside the physically controlled enviroment.

-> second, access to back to the protected enviroment.

-> As the no. of mobile users increases two challenges are presented.

- one at the device level called "micro challenges" and another all the organizational level called "macro challenges"

-> Some well known technical challenges in mobile security are:
- LDAP security
- RAS "
- media player control security
- cryptography security
- Authentication service security.

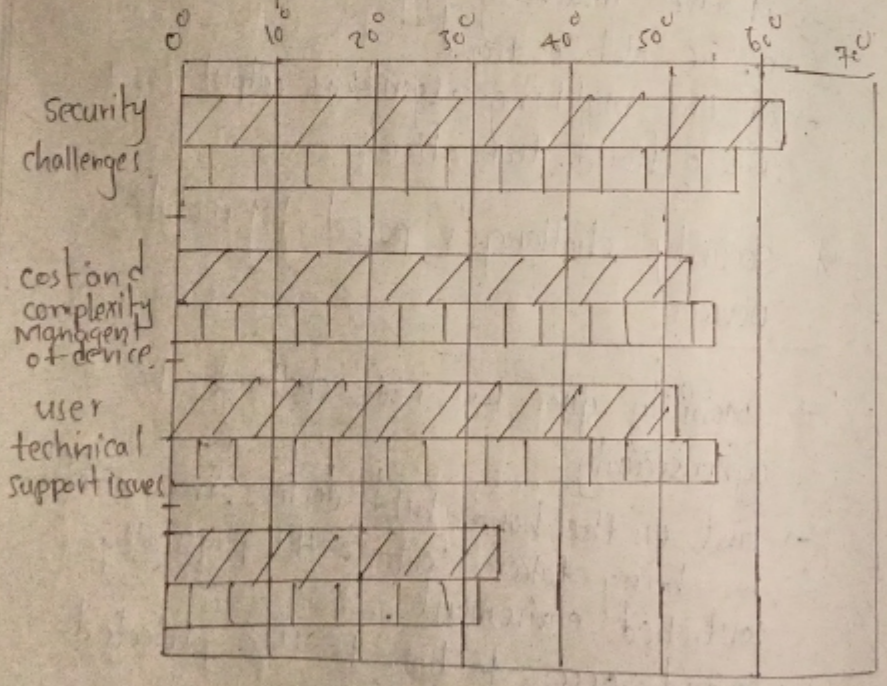


Fig Important issues for managing mobile devices

* Registry settings for mobile devices

Def Registry settings are a key part of the windows operating system that store configuration information for hardware devices, software applications and system settings

* Authentication service security

-> Authentication is a vital part of cyber security that verifies the Identity of a user (or) device before they can access a system (or) resource

-> only authorized persons can access sensitive information and systems

-> Here some things to consider about authentication service security.

-> Authentication methods (passwords, biometrics, the most basic 1 is username and password).

-> password Authentication protocol.

-> Authentication services.

-> stolen user credentials

* Attacks on mobile-cell phones:-

-> mobile phones have become an integral part of everybody's life.
-> The mobile phone being a luxury to everyone.
-> Mobile phone uses rapidly increasing day-by-day.

o Mobile phone theft: Mobile phone theft has been big issues from last few years.
-> India is a huge populated country, so public transport, bus stops, railway stations, traffic signals etc.
-> Mostly mobile theft occurs in above mentioned places.

o Mishing: Mishing is a type of cyber Attack that involves sending fradulent text messages a trick people.
-> mishing is combination of sms and phishing.
-> Deceptive messages
-> Links and numbers
-> social Engineering
-> Malware

o Vishing: vishing or voice phishing is a cybercrime where scammers use phone calls to trick people get information.

o Smishing: smishing is a type of cybercrime that involves sending fake messages to trick people to get sensitive information.
-> smishing is also known as sms phishing.
-> smishing is a social Engineering Attack

o Bluetooth-Hacking: Bluetooth hacking refers to unauthorized access and manipulation of Bluetooth enabled devices by exploiting vulnerabilities in the Bluetooth protocol.
-> Hackers take advantage of security weakness in Bluetooth connections.
-> Types of Bluetooth hacking
  - o Bluejacking
  - o Blue bugging
  - o Blue borne

* organizational measures for mobile devices

-> Here are some organizational measures for handling mobile devices:-

- o Mobile policy create a policy for mobile at the organizational level.
- o Access control : only authorized employees have access to corporate data on their mobile device.
- o user training Educate all employees who use mobile devices, about security and privacy
- o policies
  - o mobile device policy (MDP)
  - o Bring your own device (Byod) policy)
  - o Mobile Application management policy
  - o Data protection policy
  - o Incident Response policy.
- o policy Reviews Regularly review and update mobile device policies.

Identity management use mobile Identity management to ensure that users are who they claim to be.

* Security Implications for organizations

Security Implications for organizations in cybersecurity are the potential risks and consequences that can arise from vulnerabilities.

-> Here are some cybersecurity implications for organizations:-

Ransomware A major cyber threat to businesses of all sizes, ransomware attacks lock down data and system until ransom paid

IOT security As no. of IOT devices increases, so do the risks of cyberattacks and data breaches.

cloud security cloud computing provides a secure platform for storing data and protecting against cyber threats.

Data security Data security ensures that data cannot be accessed by unauthorized parties.

o phishing

phishing attacks can display malware (or) steal sensitive information from an organization.

Unit 4

Introduction

→ cybercriminals use a variety of tools and methods to commit cybercrime

- Social Engineering
- Malware
- Bots

→ cybercrime investigators use a variety of tools and techniques to gather evidence and indentify suspects including.

- Digital forensics
- Collaboration

* proxy server

Def A proxy server is a tool in cyber-security that can protect user's privacy and security while browing the Internet is called proxy server.

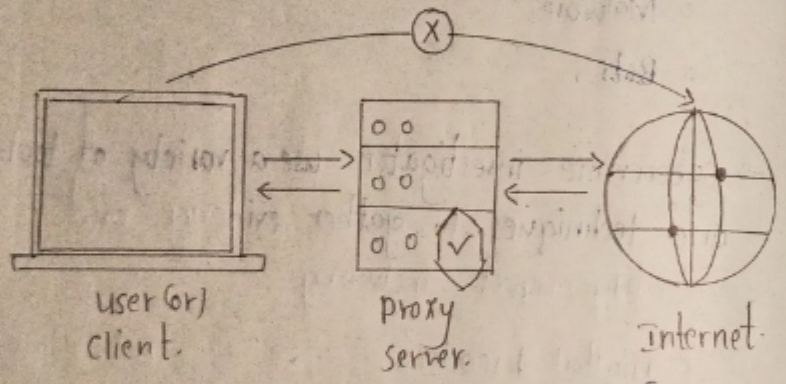
→ It acts as Intermediate blw a user's device and Internet

-> proxy server prevents cyber attackers.

-> There are many proxy providers in the market that provides services to both individuals and businesses.

-> proxy server prevents the identification of user's IP address.

-> The proxy server operation:



-> Above Block diagram show working of proxy server.

-> Every computer has unique ip address, which uses to communicate with other node.

-> similarly proxy server has it IP address.

-> when you send request, your request goes to the proxy server first, and then forward it to internet, and collects data from internet and send back to you.

-> proxy server can
  - o Improve your privacy
  - o improves " online security
  - o web scarping
  - o providing faster speed

-> There are different types of proxy servers
  - o Forward proxy server.
  - o Reverse " "
  - o Transperent " "
  - o Non- " " "
  - o split " "
  - o Forced " "

Advantages

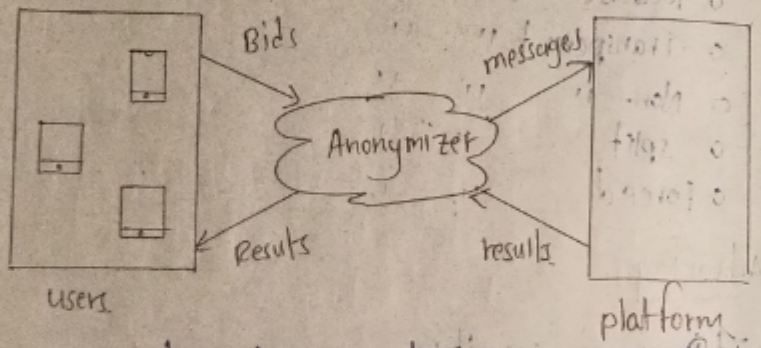
-> It improves security
-> It hides the Identity of the user.
-> protects from malware.

* Anonymizers

Def: A anonymizer is a tool that helps to make users internet activity untraceable is called Anonymizer.

-> It is also known as anonymous proxy.

-> Anonymizers are crucial part of cybersecurity
-> They protect sensitive information
-> An anonymizer act as intermediate b/w user and internet.
-> A anonymizers hides IP address from website.
-> Block diagram



-> Above block diagram shows working of anonymizer.
-> Here platform means central processing unit.
-> Types of anonymizers
  o VPN (virtual private Network)
  o 'proxy' servers
  o Tor Network

Advantages
-> Secure browsing
-> protected Identity
-> Enhanced privacy

Disadvantages
-> slow internet speed.
-> Limited Accessibility.

* phishing

Def phishing is a form of online fraud in which hackers attempt to get your private information such as passwords credit cards, bank account etc. is called phishing.

-> This is usually done by sending false emails (or) messages.
-> phishing is another type of cyber attack.
-> phishing got it's name from "phish"
-> The most common mode of phishing is sending spam emails.
-> The main motive of attacker behind phishing
  o password
  o Date of Birth
  o credit card details
-> The attackers uses original logo of email to

make phishing.

-> Bte. Below mentioned are ways through which phishing generally occurs

- clicking on unknown file.
- using free wifi hotspot.
- Responding to social media.
- clicking on unknown links.

Types of phishing

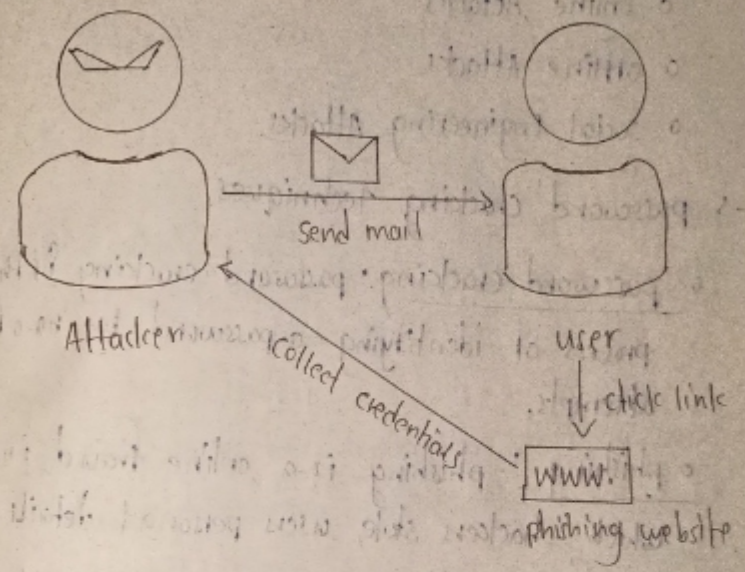
-> There are many types of phishing Attacks.

- Email phishing
- spear phishing
- Smishing
- whailing
- clone phishing
- vishing.

impact of phishing

- Financial loss
- Identity theft
- spread of malware

-> Block diagram of phishing



* password cracking:

Def: password cracking is the process of attempting to find the password by many possible combinations is called password cracking.

-> password cracking is the one of the technique used by hackers to steal users data.

-> password cracking is unauthorized access

-> By using password cracking technique, a hacker can gain access to a system by cracking the password.

-> password cracking can be done by;
- online Attacks
- offline Attacks
- social Engineering Attacks.

-> password cracking Techniques.

- password cracking: password cracking is the process of identifying a password by no.of attempts.
- phishing: phishing is a online fraud, in which hackers stole, users personal details etc.
- Brute force m Attack It is one of the method for password cracking, in which trail and error method involves.

Strategies for preventing password cracking

- setting up strong and unique password.
- Multi-factor Authentication.
- password updating.
- common passwords should be Avoided.
- Never use repeating strings for password.
- Never use DOB (or) personal names.
-> Do not ruse passwords

X Dos and DDos Attacks

Dos Attack

Def: A Dos Attack is a type of cyberattack where, an attacker overwhelms a computer system, network, (or) website is called Dos, Attack.

-> Dos stands for Daniel of Denial of service.
-> characteristics of Dos Attacks
- single source.
- Traffic volume.
- Traceability
- Blockability.

DDos Attack

Def. A DDos Attack is a type of cyber attack where multiple compromised devices flood a targeted system, network (or) website is called DDos Attack.

-> DDos- distributed Denial of service.
-> characteristics of DDos.
- multiple sources
- Traffic volume.

- Difficulty in Tracing
- Difficulty in Blocking.

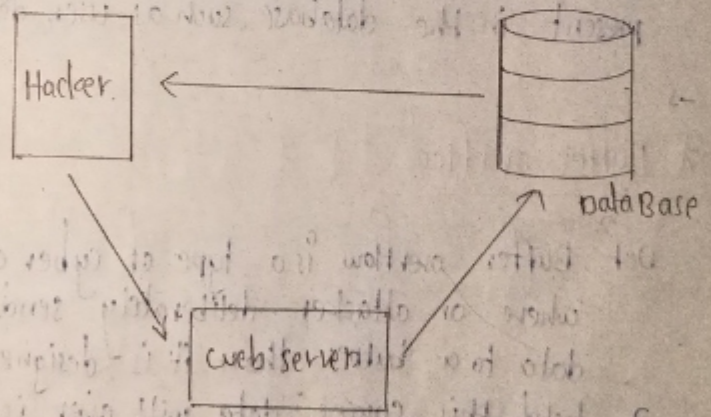
DOS	DDOS
-> DOS- Denial of service	-> DDOS- Distributed Denial of service.
-> In DOS single system targets the victims system.	-> In DDOS multiple systems targets the victims system.
-> It is slower	-> It is faster.
-> It is easy to blocke this attack	-> It is difficult to this attack.
-> Easy to trace this.	-> Difficult to trace this.
-> Easy to operate and manage	-> Not easy to operate and manage.
-> low threat level	-> High threat level
-> There is malware involvement.	-> There is no malware involvement.

X SQL injection

Def: SQL injection is a type of web application security vulnerability that allows an attacker to inject malicious SQL code into a web applications is called SQL injection.

-> SQL injection is a security flaw in web applications, where attackers insert harmful SQL code through user inputs.

-> Example of SQL injection.



-> Above figure shows schematic layout of SQL injection.

-> It consist of Hacker, webserver, database etc.

-> A successful SQL injection attack can have

Severe consequences.

-> Attackers may manipulate (or) delete crucial data.
-> This can leads to identity theft, financial loses.

Types of SQL injection

- In-band SQL injection.
- Error based SQL injection.
- Blind SQL injection.
- out-band SQL injection.
- Inference based SQL injection.

-> The hacker can retrive all the user data present in the database. such as user details.

->

* Buffer overflow

Def: Buffer overflow is a type of cyber attack where an attacker deliberately sends more data to a buffer than it is designed to hold, this causes data spill over is called buffer overflow.

-> A buffer is a temporary area of data.
-> when more data gets placed by a program the extra data overflows.

-> There are two types of buffer flows in
- stack based buffer overflow.
- Heap " " " "

* Steganography :-

Def: steganography defined as caching of secret information.

-> This word is derived from greek 'stegos' means 'cover and grayfiya means writing, covered writing (or) hidden writing.
-> with the help of steganography we can hide any digital thing like, textbook, image, video etc.

different types of steganography

- Text steganography: Text steganography in which involves caching secret information within a textbook document.
- Image steganography: Image steganography in which involves caching secret information with digital images.
- Audio steganography: Audio steganography in which involves caching ~~secret~~ secret information within audio lines.

- video steganography

-> video steganography in a which involves caching secret information within digital videotape lines.

- Network steganography

-> Network steganography in which involves caching secret information within network protocols.

Advantages

-> It offers better security for data sharing.
-> data hiding.
-> secure communication.

* Trojan Horse and Back door

Trojan Horse: Trojan horse or simply Trojan is a type of malicious software that disguises itself as legitimate software, allowing unauthorized access to a computer.

-> Disguisess itself as legitimate software.
-> Hides within legitimate software.
-> Executes Malware code.
-> Allows unauthorized access.
-> difficult to detect.

Backdoor: A 'back door' is a hidden entry point in a computer system or software, that allows unauthorized access. is called Backdoor.

-> Back door is a known as Trap door.
-> Backdoor allows anyone to gain access to any system. with going through usual security access.
-> Back door are quite difficult to detect
-> programmers use a back door legally to debug and test programs.

* virus and worms

- Virus: A computer virus is a malicious program that can infect a computer or network router without user's knowledge or permission.

-> A virus can attach itself to the other programs and spread to other devices.
-> virus can't be controlled by remote.
-> It is more harmful.
-> It's spreading speed is slow.

○ Worms

Def A worm is a type of malicious software that replicates itself and spread to other devices without user's permission is called worm.

-> worm is similar to virus.
-> It replicates itself more and more to slow down computer system.
-> worms can be controlled by remote.

Virus	worm
-> The main objective of virus is to modify the information.	-> The main objective of worm is to eat system resources.
-> It requires a host.	-> It doesn't require host.
-> It is more harmful	-> It is less harmful
-> Antivirus software used against virus	-> Antivirus or firewall used against worm.
-> virus can't be controlled by remote.	-> worm can be controlled by remote.
-> virus generally comes from shared or downloaded files.	-> worms can be generally come from downloaded files.
-> It needs human action to replicate.	-> It doesn't need human action to replicate.
-> spreading speed is slower	-> spreading speed is faster

* keylogger

-> A keylogger is a tool that captures every single keystroke from the user to steal sensitive information etc.

-> A keylogger can either store the information on the computer or send it to the server.
-> keylogger is a very powerful cybertool.
-> Types of keyloggers

○ Hardware keylogger:

-> It is also called physical keylogger.
-> It is a hardware device that can be used for keylogging.
-> It is usually a small device.

○ Software keylogger

-> A It is a type of malicious program that records and logs keystrokes made on computer.
-> It captures sensitive information.

Spyware

Spyware is a type of malicious software that can collect and send personal information from device without user's consent is called spyware.

- spyware leads to
  - Financial loss
  - Identity theft
  - Device damage

Unit-5

cybersecurity - organizational implications

-> cyber security can have number of organizational implications, including:-

- o Dataloss
- o Financial loss
- o loss of revenue.
- o Equipment damage.
- o Reputation damage.
- o cloud migration

* cost of cybercrime

-> The cost of cybercrime has been rising rapidly as digital dependence grows globally

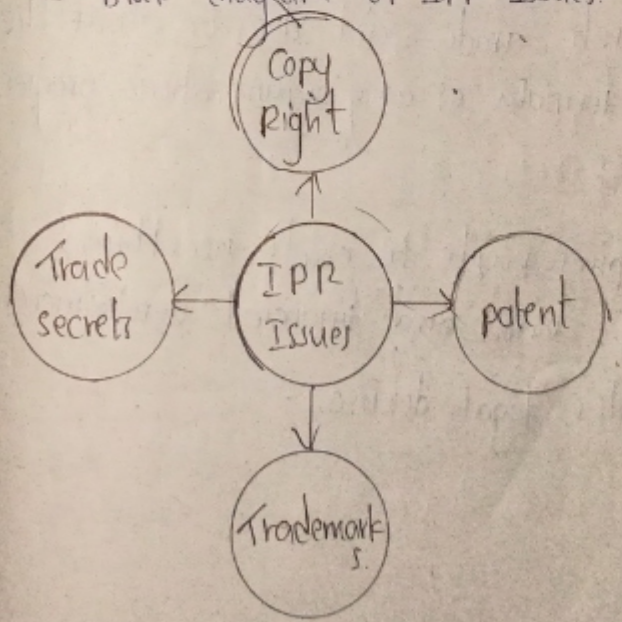
-> Here some key aspects.

o global economic Impact The global economic cost of cybercrime is $8 trillion in 2023 and it could rise ~$10.5 trillion by 2025 according to reports

- Business losses : For businesses financial losses due to data breaches, ransomware attacks,
  -> The average cost of dat breach in 2023 is $4.45 million.
- Ransomware Ransomware is a type of malware that locks (or) encrypts victim's data and demands payment to regain data.
  -> To defend ransomware you can:
  - Employee
  - updat frequently.
  - Authenticat software
  - secure backups
- cybercrime trends phishing, social Engineering, IP theft, etc.
- Types of costs
  - Direct losses This include stolen funds, ransom payments, etc.
  - Indirect losses This include loss of customer trust, reputational damage, market position erosion.

IPR Issues

-> IPR stands for Intellectual property Rights Issues. In cybersecurity.
-> cybercrime which are related to IPR includes software piracy, copyright intringement, cyber-squatting etc.
-> IPR's are rights given to each and every person for creation of new things.
-> IPR gives 'complete right over use of his/her creation for certain period of time.
-> Itellectal property Rights are legal Rights.
-> Block diagram of IPR Issues.



-> IPR issues can be classified into four types

o copyright — copyright is a term that describes ownership (or) control of the rights to use creative expression including books, videos, movies, music etc.

o patent — A patent gives it's owner the right to exclude others from making, using, selling, for limited period of time.

o Trademark — A trademark is a graphical representation that is used to distinguish the goods and services ~~of on~~ of one from others.

o Trade secrets — Trade secret describe about the general formula of any organization's progress.

o Advantages

-> It inspires people to create new things.
-> It helps social and financial development.
-> It provides legal defense.

* Security Implications :

Def: Security implications in cybersecurity are the potential risks and consequences that can arise vulnerabilities in a system is called security implications.

-> These implications can include:

Data loss: A security breach can lead to the loss of data, which can have serious financial consequences.

Data tampering: A security can allow data to be tampered.

Reputation damage: A security breach can hurt an organization's reputation and lead to loss of trust from customers.

unauthorized access: A security breach can allow unauthorized access to system, accounts, (or) data.

Service disruption: A security vulnerability can allow disrupt services (or) make network unavailable.

* privacy Implications

Def privacy implications in cybersecurity ~~are the~~ are the potential potential risks (or) consequences of unauthorized access to person information (or) data. is called privacy implications

-> These consequences can be harmful to individuals and businesses can include:

Identity theft unauthorized access to personal information can lead to Identity theft, financial fraud, and other issues

Reputational damage A business can face regulatory consequences, such as fines, lawsuits, and damage to their reputation

unwanted marketing A personal data can be sold to advertisers (or) other outside parties without user consent, which can result an unwanted marketing

list of privacy Implications

- Harr Harassment via Emails
- Hacking
- cyber-stalking
- cracking
- Intellectual property crimes
- cybersquatting
- cyber terrorism
- cyber welfare
- child pornography
- cyber Trafficking

online gambling

* Social computing

-> Social computing is also known as "Web 2.0".

-> It empowers people to use web-based products and services.

-> It helps thousands of people across the globe.

-> This would be a goldmine for a cybercriminals.

-> social computing is related to social media marketing.