Cybersecurity Unit 1 & 2

cyber security (Dr. A.P.J. Abdul Kalam Technical University)

CLASSTIME Pg. No.
Date 14 / 09 /2023

Unit-1

→ The technique of protecting internet connected systems such as computers, server, mobile phone from virus attack is known as Cyber Security.

⇒ We can divide Cyber Security into 2 parts Cyber and Security.
- Cyber means system, network, program, and data.
- Security means protection.

Sometimes cybersecurity is called Electronic Information Security

Types of Security

1. Network Security
2. Application Security
3. Information or Data Security
4. Identity Management
5. Operational Security
6. Mobile Security
7. Cloud Security
8. Disaster Recovery & Business continuity planning

Network Security

It involve implementing the hardware and software to secure a computer network from unauthorised access.

Application Security

* It involve protecting the software and devices from unwanted threats.
* The protection can be done by regular update of the Application.

Information or Data Security

It involves implementing a strong data storage method.

Identity Management

It deals with the procedure for determining the level of access that is an individual has within the organization.

Operational Security

It involves processing and decision making for handling the secure data.

Mobile Security

It involves securing the organizational and personal data store on mobile devices such as cell phones, computers and tablets.

Cloud Security

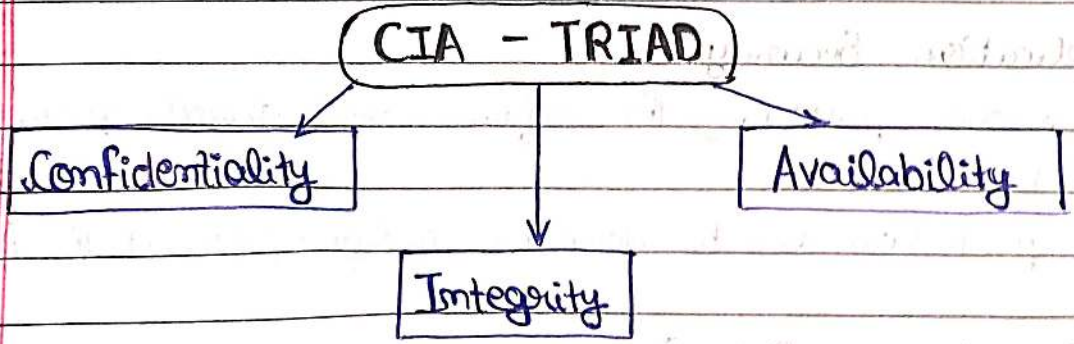
It involve protecting the information store in cloud architecture.

Example: Amazon Web service

Disaster Recovery & Business Continuity Planning

It deal with the process, monitoring, alerts and plans how an organization from any attack.

Cyber Security Goals



Date / /

① Confidentiality

* It is equivalent to privacy that avoid unauthorised access of information.
* It involve ensuring that data is accessable by those who are allowed to use it.

② Integrity

* It ensure that data is authentic, accurate and safe from unauthorized modification. If any modification occurs, certain action should be taken.

③ Availability

This principle makes the information to be available and useful for authorised person always.

Cyber Crime

It is any criminal activity that involve a computer, common network devices or a network.

- Cyber means computer and things.
- Crime means illegal and unfair.

US department of Justice divide the cyber crime into 3 categories :

① Crime in which the computing device is the target.
Eg: To gain network access.

② Crime in which the computers is used as a weapon.
Eg: Virus attack

③ Crime in which the computer is used to steal sensitive useful data.

CLASSTIME Pg. No.
Date 20 / 09 /2023

Various Cyber Crimes

i) **Cyber Fraud** – This refers to an act of stealing e-data or gaining unlawful use of any computer system without the permission.
This involves
- Hacking of computer
- Send malicious code such as virus
- Installing spyware
- Sending Hoax (like a good but in reality are not)

ii) **Cyber Terrorism** – This term was coin ... by Barry Collin in 1997. The act of terrorism is executed using computer technology and computer resources by the terrorist group called Cyber Terrorism.

iii) **Ad Fraud** – Ad Fraud refers to a scam that are used to sending amazing offers to user.

iv) **Computer as a Target** – A computer can be targeted when the criminal has the technical knowledge and know how to hack the system and steal the data.

v) **Computer as a Tool** – When criminals use their system to attack the user target it is called Computer as a tool No technical knowledge are needed in this case.

vi) **Drug Trafficking** – Dark Web or Darknet Market are used to buy and sell drugs online. Criminal use encrypted message for communication.

"Silk Road" was the first online market of drug trafficking

CLASSTIME/Pg. No.
Date / /

* History Of Cyber Crime

Technically, first cyber crime attack happened in France in 1834 before the internet was invented. Attackers stole financial market information by accessing french telegraph system.

1962 - Allen Scherr launched a cyber attack against MIT computer to steal password from database by the help of punch card

1971 - First computer virus was created for research purpose by Bob Thomas at BBN Technologies. The name was "Creeper Virus". and detect on ARPANET.

1981 - Ian Murphy was the first person who committed a cyber crime after successfully hacking the AT&T computers

1992 - Cowboy and Kuji was 16 years old british scholar who launched password sniffer and performed series of attack.

1995 - Vladimir Levin was the first known hacker to attempt Rob a Bank.

2005 - In US data leak of 1.24 million users of HSBC bank.

Cybernetics

It deal with the information and its use. Cybernetics is the science that overlap information theory, computing and

Date / /

automation.

Phishing

Phishing is the form of online identity theft the main aim of phishing is to steal sensitive information such as online banking password and credit card information.

Cyber Space

Cyber Space was coin by William Gibson in 1984.
Cyber Space is a worldwide network of computer technology that use TCP/IP for communication and exchange of data.

Cyber Squatting

* Squatting means occupy an abandoned / unoccupied space that the user does not own, rent, or has permission.

* Cyber Squatting means registering, selling a domain name without permission

Cyber Punk

Cyber Punk was coin by Bruce Bethke, this means anarchy (disorder) by a machine or a computer

Cyber Warfare

This means attack against unsuspecting opponent, computer network destroy and paralyse the nation.

CLASSTIME | Pg. No.
Date / /

Who are Cyber Criminals ?

Types of Cyber Criminals

- **Need Recognition**
  - Hobby Hackers
  - IT professionals
  - Politically motivated hackers
  - Terrorist organizations
- **Don't Need Recognition**
  - Psychological perverts (workers)
  - Motivated Hackers
  - State Sponsored hackers
  - Organized criminals
- **Insiders**
  - Disgruntled (angry) Employees
  - Competitor
  - Spy

27/09/2023

Cyber Crime Classification

Cyber Crime

- **Against Individual**
  - Email Spoofing
  - Phishing
  - Spamming
  - Computer Storage
  - Malware
  - Cyber Defamation
- **Against Property**
  - Intellectual Property Crime [IPC]
  - Cyber Squatting
  - Cyber Vandalism
  - Hacking Computer System
- **Organization**
  - Hacking
  - Password
  - DOS
  - Virus Attack
  - Email Bombing
  - Logic Bomb
  - Salami Attack
  - Trojan Horse

Date / /

Cyber Crime against individual

Email Spoofing

The spoof email is one that appear to originate from one source but actually sent from another source

Phishing

It is a process of collecting your personal information through email or websites.

Spamming

The person who create electronic spam are called Spammer. Spam is the abuse of electronic messaging system to send unrequested bulk messages.

Cyber Deflamation

It is a offense either spoken or sign by someone with visible representation.

(Example: Someone published defamation matter about someone on the website.)

Computer Storage

The use of internet to stop the normal functioning of a computer and attack on computer data.

Cyber Crime against Property

Intellectual Property Crime

Intellectual Property Crime is stealing copyright software piracy trade & and patent using internet.

Cyber Squatting

Date / /

It is an act of registering or using a domain name to profit from a trademark, corporate name of personal name of an Individual.

Cyber Vandalism

Cyber Vandals are individuals who damage information infrastructure only for their enjoyment.

(Example: In the year 2016, US presidential election the wikipedia Donald Trump was damaged many times.)

Cyber Crime against Organisation

Password Sniffing

Password sniffing is an attack on internet that is used to steal user name and password of user from the network.

DOS

DOS stands for Denial of Service also known as Brute Force Attack. It is usually triggered by an intruder flooding large amount of traffic on a website. The main aim of DOS attack is bring down website infrastructure.

⇒ DOS attack may do the following :

1. Flood a large traffic on the network.
2. Start an action between two systems.
3. Disturb service to a specific system.

Virus Attack

Computer virus is a program that infects software and applications without the knowledge and permission of the User.

Date / /

Email Bombing

It is also known as **Mail Bomb**. It refers to sending a large number of email to the victims email account and crash victim's email account.

Logic Bomb

Logic Bomb is a piece of malicious code that is inserted into software. It is activated when certain conditions are fulfilled.

(Example: Log on and Log off condition)

~~Salami Attack~~

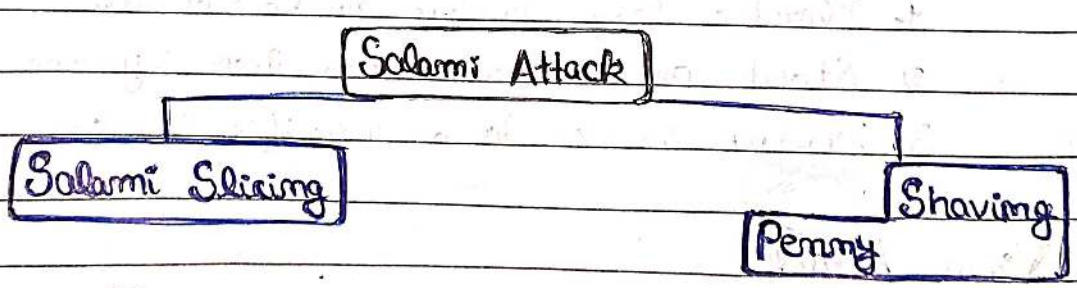
Protection Against Logic Bombs

1. Always use latest version of antivirus software.
2. Scan all the files.
3. Stop unauthorized access of computer.

Salami Attack

These techniques are used for financial crime the idea is here to make alter the information that is completely unnoticed.

(Example: A bank employee insert a program into the bank server that deduct small amount of money Rs. 1 from every account. No account holder will ~~no~~ probably notice this.)



Salami Slicing

Salami Slicing occurs when the attacker get personal information like Bank detail, credit card detail but no amount

Date / /

will deducted from the account.

Penny Shaving

When the attacker steal small amount of money it is ~~fully~~ called Penny Shaving.

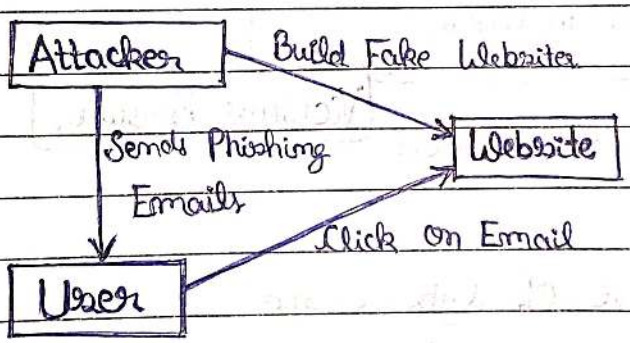
Trojan Horse

Trojan Horse gets its name from the well-known story of Trojan War. It is a malicious code of program with the entity of to take the control of the system. It is used for steal the information or damage the system.

25/09/2023

* Data Diddling

Data Diddling is a type of cybercrime that ~~includes~~ involves Alter the raw data before the processing and changing it back after the processing.



Protection from Data Diddling

1. Access Control
2. Authentication
3. Data Encryption
4. Regular Backup
5. Monitoring & Auditing
6. Employee Training
7. Continuous Assessment of Security

Date / /

Cyber Crime against Society

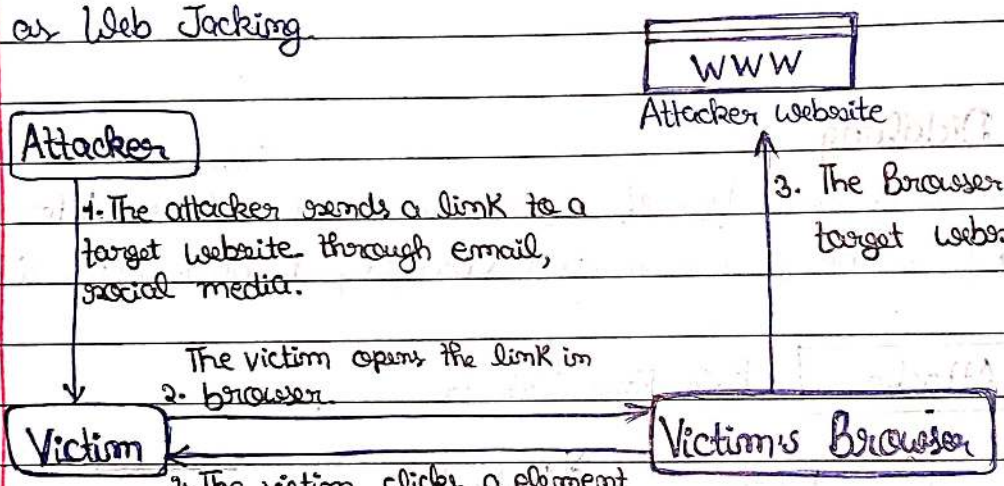
① Forgery (8 November 2016, at 8pm Notebandi started in India to put a stop in fake note-making supplies)

- Counterfeit currency notes, postage, stamps & marksheets can be printed printed with the help of computer, printer & scanner.

② Cyber Terrorism

③ Web Jacking

- Illegal control of a website while taking over a domain is known as Web Jacking.



☆ A Global perspective of Cyber crime

* In Australia, cyber crime has a narrow meaning.
* In India, cyber crime act 2001, it is a offense against computer data and system.
* In the council of europe, cyber crime is used as umbrella term to refer many of the criminal activities including offense against computer & system.
* August 4, 2006 the US senate rectifies cyber crime separate from normal crime, so every country have different rules against cyber crime.

CLASSTIME Pg. No.
Date / /

☆ Cyber Crime Era
Survival Mantra for Netizens.

* The term Netizen was coined by Michael Haubem. The netizens are internet users who is spending their ~~time~~ time online.

⇒ There are 5P mantra's for online security of netizens.

5P
- ① Precaution
- ② Prevention
- ③ Protection
- ④ Preservation
- ⑤ Perseverance (fixer)

For ensuring Cyber Safety, the moto for the netizens should be "Stranger is Danger!"

10
2/~~09~~/2023

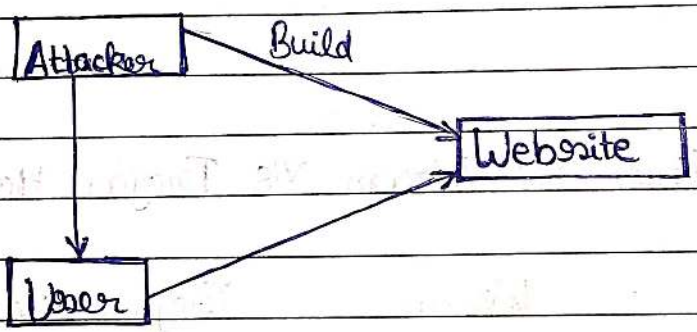
Comparison Virus V/S Worm V/S Trojan Horse

Feauture	Virus	Worm	Trojan Horse
① Definition	Viruses are the computer program that connect to other softwares of programs and harm the computer.	Worm is a malware program similar to virus that does not interact with other system applications only slow down the performance.	A Trojan Horse is a type of malware that steals sensitive data from the user and deliver it to different locations.
② Replication	It replicates itself.	It also replicates itself.	It does not replicate itself.
③ Execution	It relies on the transfer	It replicate itself without human action.	It is downloaded as software and executed.

④ Remotely controlled	It could not be remotely controlled.	It may be remotely controlled.	Totally remotely controlled.
⑤ Infection	Spread through executable files.	Worm take the advantage of flaws.	The trojan horse run as a program and interpretated as unitary software.

Data Diddling

Data Diddling is a type of cyber crime that involve alter raw data just before it is processed by a computer and then changing it back after reprocessing is completed.



* Protection from Data Diddling

① Access Control
② Authentication
③ Data Encryption
④ Regular Backup
⑤ Monitoring & Auditing
⑥ Employee Training
⑦ Continuous Assessment of Security

CLASSTIME Pg. No.
Date / /

★ Cyber Offenses – How criminals plan

Following phases are involved in planning of cyber crime.

① **Reconnaissance** – It means information gathering that is called Passive attack.

② Scanning the gathered information for the validity of the information.

③ Launching an cyber attack.

Passive Attack

Passive Attack involves gathering the information about the target without the knowledge of user.

Active Attack

An active attack involve acquiring the network to discover the confirmation of information [IP address, operating system types, applications and services]

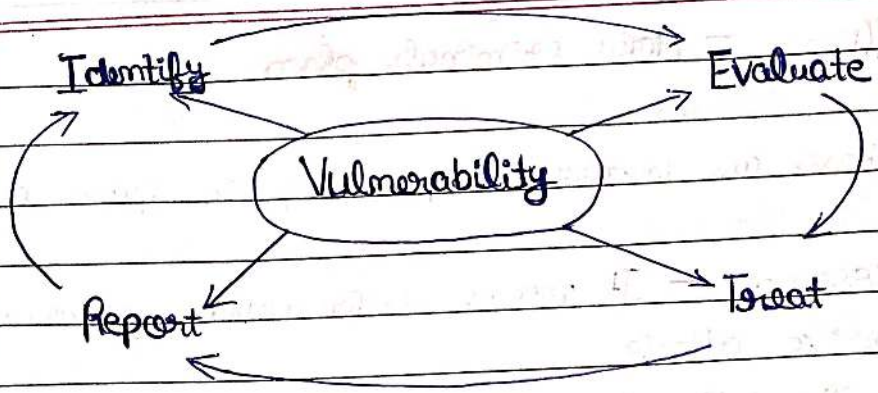
* Scanning the gathered information

Scanning is the key to examine the gathered information is correct or not, The objective of scanning are :-

1) Port Scanning
   Identify open and closed port of network.

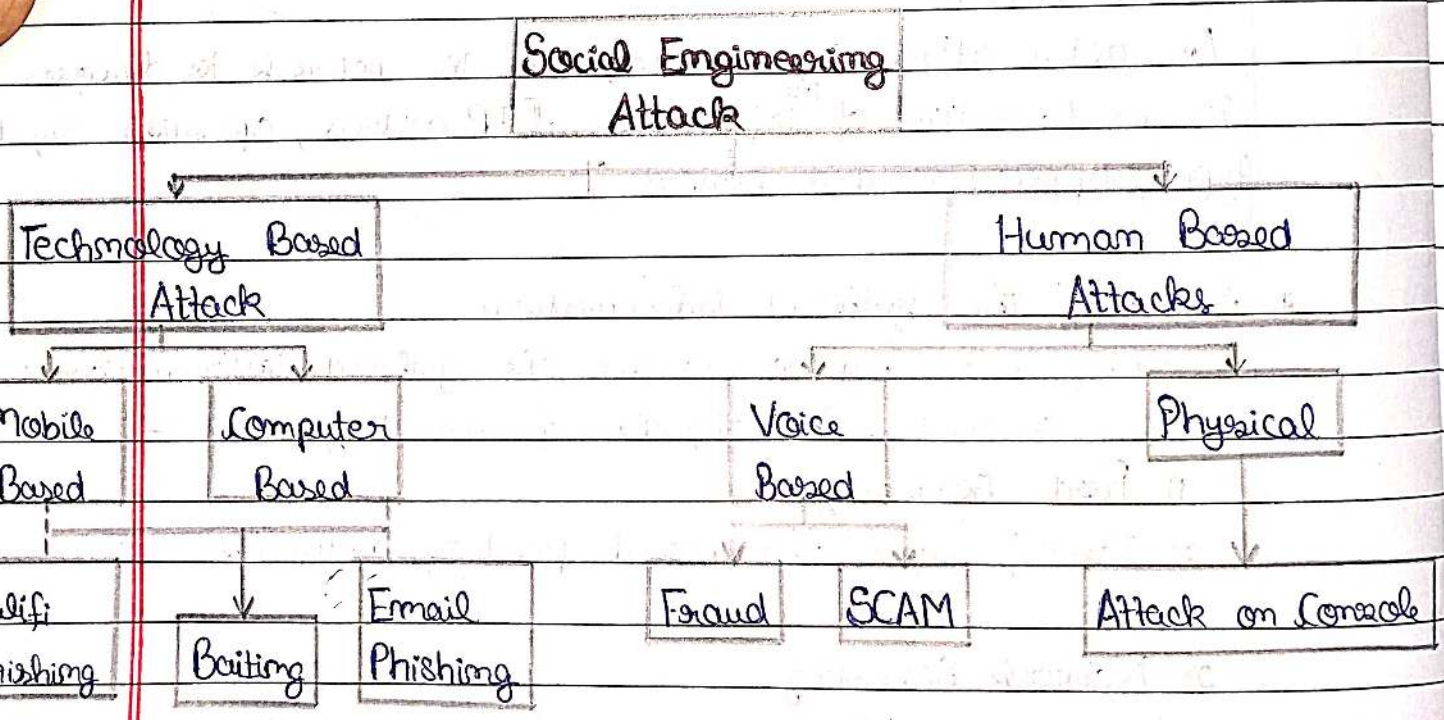
2) Network Scanning
   Understand IP address and related information about the computer network.

3) Vulnerability Scanning
   Understand the existing weakness of the system with following phases :-



Social Engineering

* Social Engineering is the technique to influence the people to obtain the information for some action.
* Social Engineers exploit the natural tendency of persons
* The goal of social engineers are to make a fool of someone and provide methods for accessing their confidential information.



Cyber Stalking

The use of information and communication technology to harass a person/people of globe are called as Cyber Stalking

⇒ There are few examples of cyber stalking :-

CLASSTIME Pg. No.
Date / /

① Posting offensive or rude comments online.
② Releasing victims confidential information online.
③ Tracking all online movement of victim.
④ Use technology for Blackmailing
⑤ Creating Fake profiles on social media.
⑥ Posting or Distributing real or fake photo of victim.

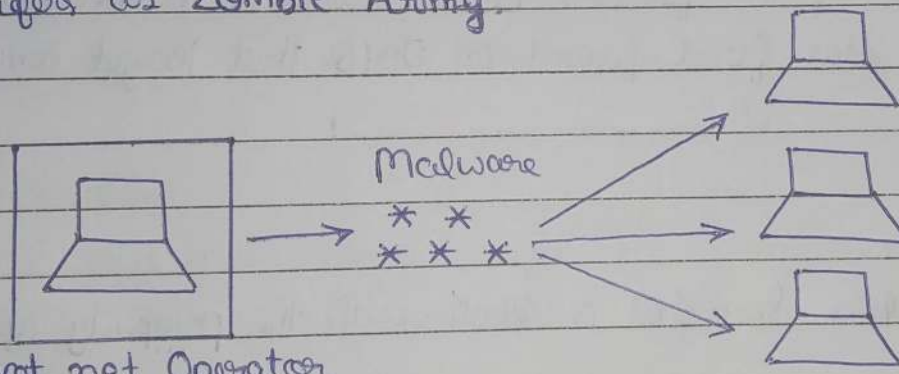
Date / /

① Posting offensive or rude comments online.
② Releasing victims confidential information online
③ Tracking all online movement of victim.
④ Use technology for Blackmailing
⑤ Creating Fake profiles on social media.
⑥ Posting or Distributing real or fake photo of victim.

11/10/2023

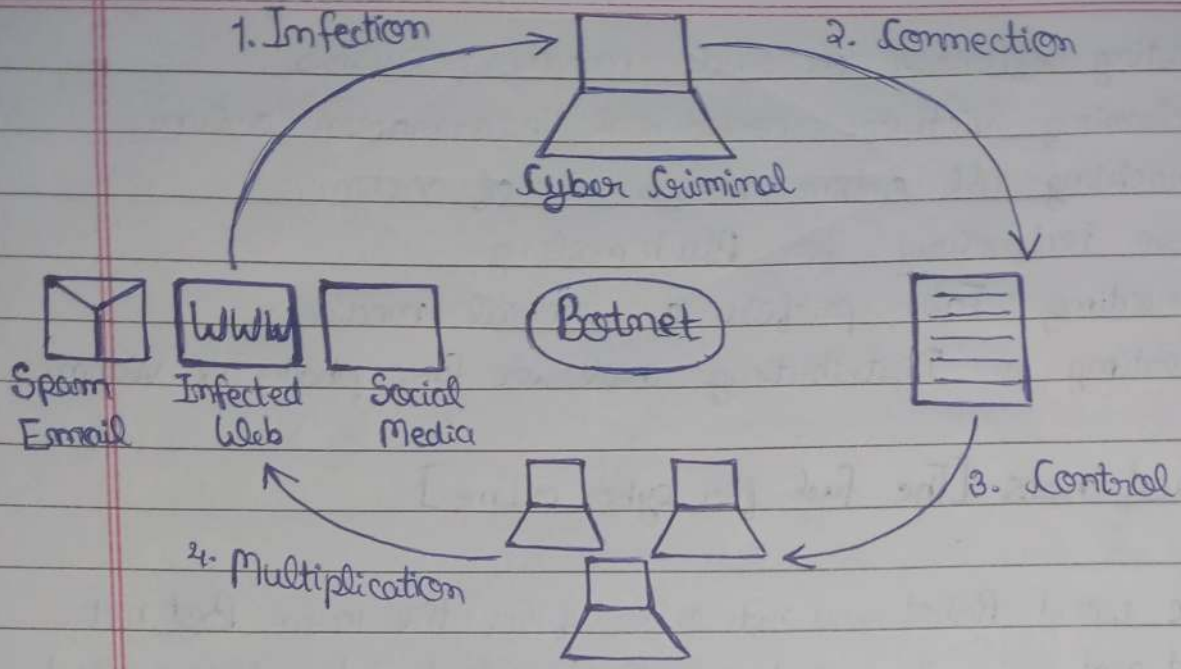
Bot nets [The fuel for cyber crime]

The word Robot and network defines the term Bot net. Bot net refers to a network of hijacked internet connected devices that are installed with malware code. Infected device are known as Bots and hacker is known as Bot Herder. A Bot is also called Zombie and Bot net refers as Zombie Army.



How Botnet works

Bot net works under the cycle and there are 4 phases of Botnet working.



Famous Botnets Attacks

① **Mirai**

Mirai is one of the famous Botnet attack associated with IoT devices. It was first found in 2016 that target online consumers.

② **Mariposa**

This attack was launched in 2009 with the property of DDOS.

③ **3Ve**

This attack was launched in 2016. It generate fake clicks on online advertisement. Hosted by fake websites.

Attack Vector

Attack vector is a path by which an attacker or hacker can gain access to a computer or network in order to deliver malicious code.

Attack vector include viruses e-mail attachments web pages and chat rooms.

CLASSTIME Pg. No.
Date / /

Comma Attack Vector

1. Poor Encryption
2. Phishing
3. Trust Relationship
4. DDOS attack
5. Weak Password
6. Software Vulnerabilities

Malware

It is a malicious software designed to damage a computer system without the information of user.

Types of Malware are :

- Spyware
- Virus
- Trojan Horse
- Worm
- Keylogger

Adware

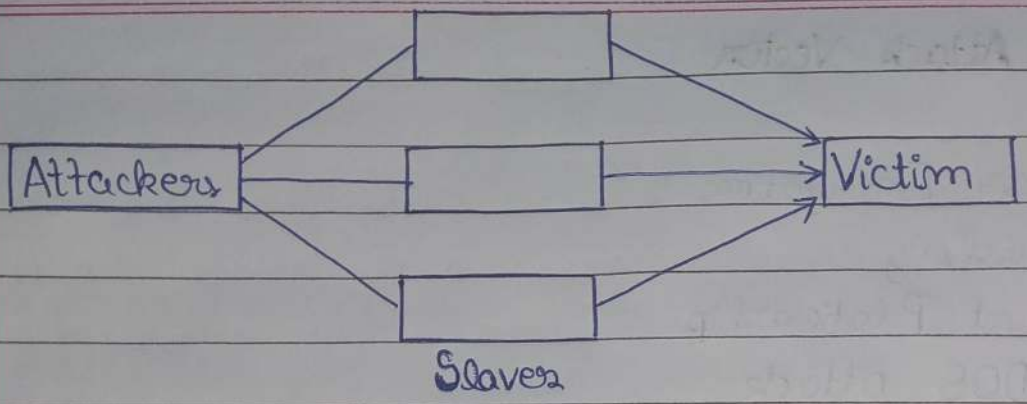
It is a advertising supporting software which automatically play, display or download to your computer.

Spam dexing

It is also known as Search Spam or search engine spam. It involve no. of method such as repeating a task.

DDOS

DDOS stands for distributed denial of service when multiple systems flood the bandwidth of a resources of target system from the multiple ~~beams~~ places it is called DDOS.



Foistware (Sneakware)

Foistware is a software that adds hidden component to the system without the user information and knowledge. Spyware is a example of Foistware.

Date 13 / 12 /2023

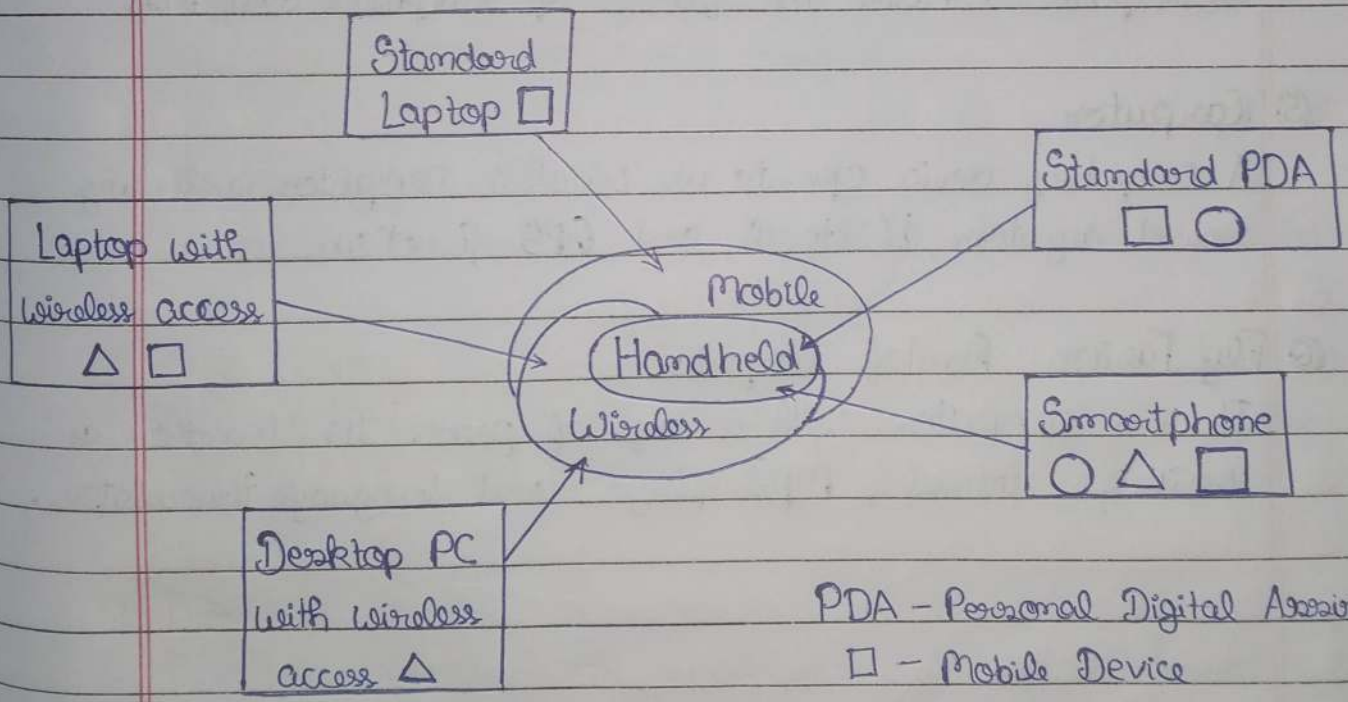
Unit-II

Mobile & Wireless Device Introduction

In the modern era the rising importance of electronic gadgets that is integral part of business provide the connectivity with office using internet. The use of laptop, PDA (Personal Digital Assistant) has been grow.
Smart phone combine the features of mobile and PDA.
In November 2007, there was 3.3 Billions of mobile phone users.

★ Proliferation (expansion) of Mobile & Wireless Devices

Today the advancing are being made for mobile devices that trends are smaller devices with more processing power



Mobile Computing is taking a computer and on necessary fields and files with software into the outside the word.

Date / /

Many of the Mobile computers has been introduced since 1990's

① Portable Computer
It is a general purpose computer that can be easily moved from one place to another place.

② Tablet PC
Tablet PC inbuilt Keyboard with feature of touch screen.

③ PDA
PDA stands for Personal Digital Assistant. It is a packet sized computer with limited functions.

④ Smartphone
Smartphone combine the features of cellphone and PDA

⑤ Computer
A computing device operate as wireless computer including sound system, bluetooth, and GPS function.

⑥ Fly Fusion Pentaf Computer
It is a computer with a size of pen. Its function as writing utensil, mp3 player and language translator.

CLASSTIME Pg. No.
Date 18/ 10 /2023

★ Type of Mobility & its implication

What is Difference

MOBILITY

- User Mobility → User Interaction Model
- Device Mobility → Smaller, Battery Devices, Multiple Heterogeneous network.
- Session Mobility → Issues in Data Distribution
- Service Mobility [code mobility] → Distributed life cycle, security issue

Popular Type of attack over 3G & 4G Mobile Network

① Malware, Viruses, Worm
These are the common attacks on the mobile network these perform harmful activities on Mobile Network.

② Skull Trojan
It targets series 60 phones [NOKIA] with symbian mobile OS.

③ Cabir Worm
It is the first dedicated mobile phone worm that's running on symbian mobile OS (operating system).

④ Mosquito Trojan
It affects the series 60 smartphones and this virus work with mobile phone games.

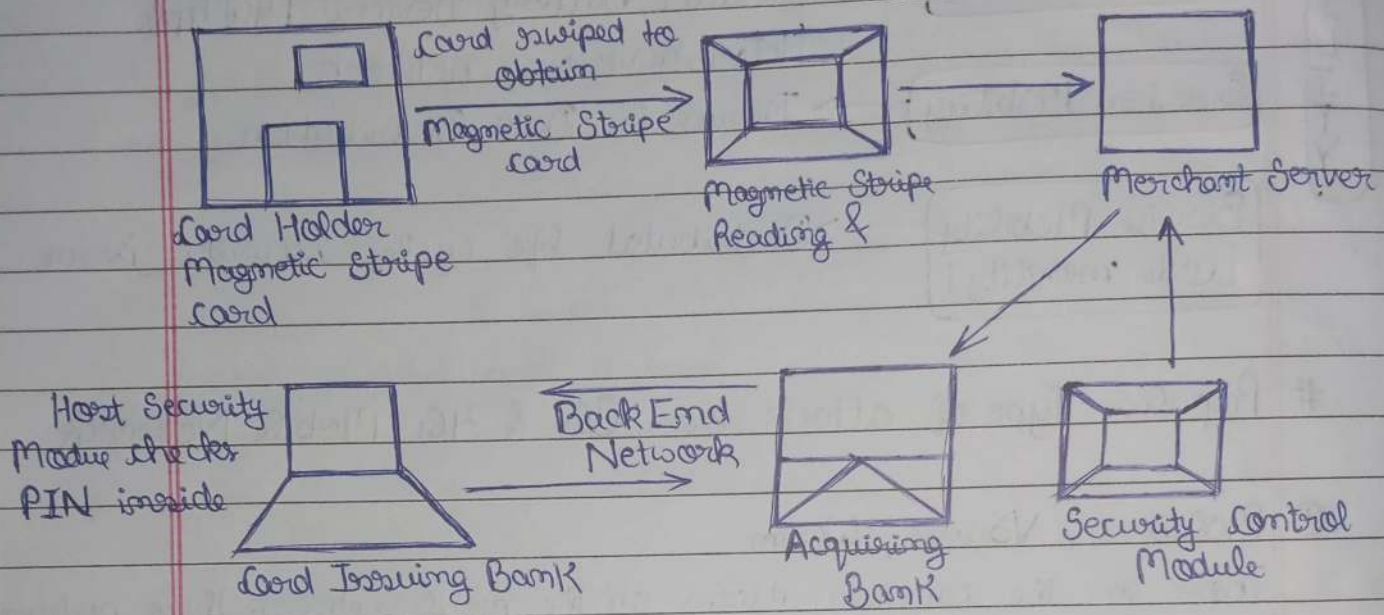
⑤ DOS (Denial of Service)

⑥ Overbilling Attack
Overbilling involve an attacker hijack the subscriber IP address and

use it.

★ **Credit Card Fraud in Mobile & Wireless Computing**

Credit Card Fraud is the new trends in cyber crime with mobile computing using the mobile commerce and mobile banking.



★ **Tips to prevent Credit Card Frauds**

Do's

1. Put your signature on the card immediately after receiving.
2. Make a photocopy or scan copy both side of your card & store it at the safe.
3. Change the PIN (Personal Identification Number) regularly.
4. Always carry customer care number for emergency.
5. Keep your eyes on during the transaction.
6. Store all the receipts to compare with invoice.
7. Report to the Bank in the case of lost the card & block the transaction.

Don't's

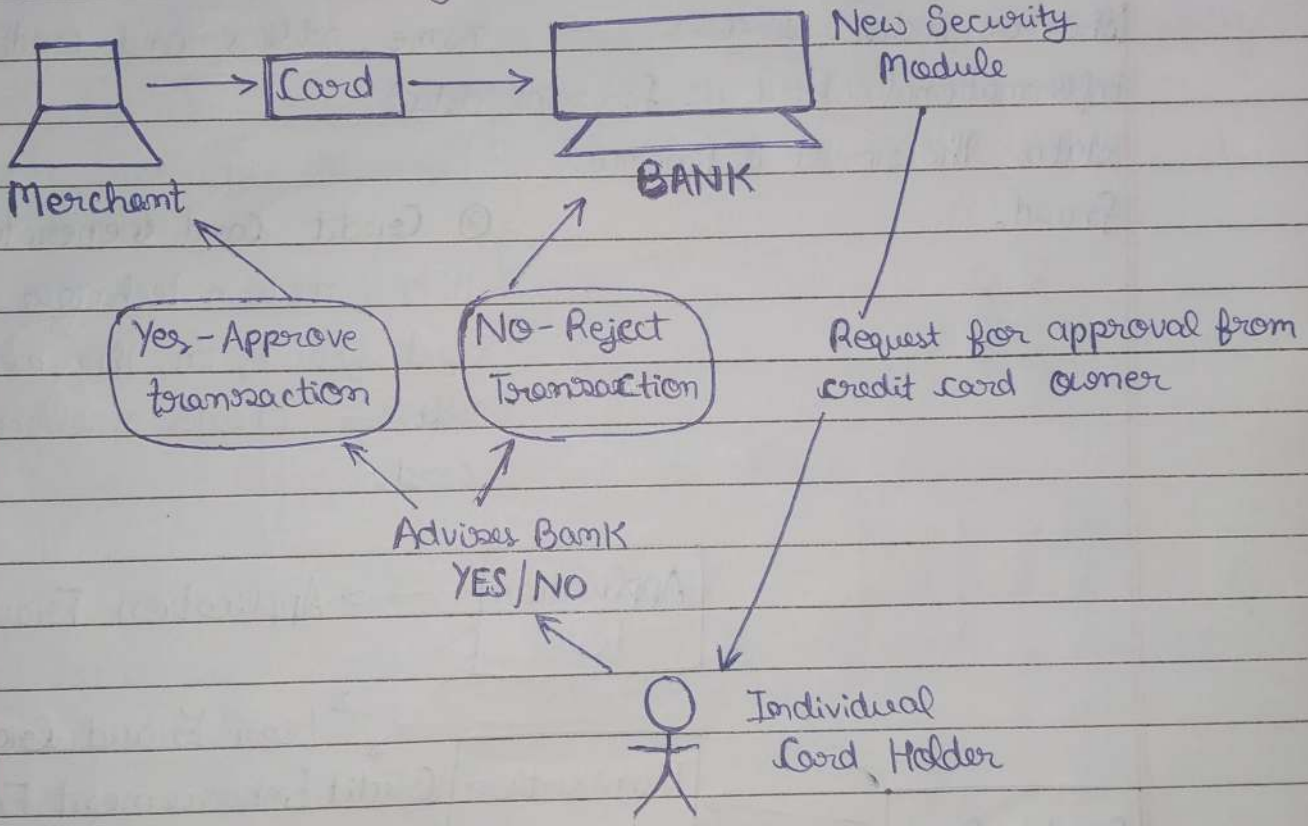
1. Never store your card number and PIN in your cell phone.

Date / /

② Never transfer your card to other person.
③ Don't share OTP or PIN to anyone.
④ Avoid phishing ~~scams~~ scams.
⑤ Avoid public wifi.
⑥ Don't shop on unsecured websites.

CLEW

CLEW stands for Closed Loop environment for wireless. This system was developed by australian company Alacrity for online transaction system.



18/10/2023

⇒ Steps of CLEW

1. Merchant send a transaction to the bank.
2. The bank transmit the request to authorised ~~and~~ card holder.
3. Card holder approve or reject the request using OTP.
4. Bank notify to customer about transaction using SMS or email.
5. Transaction is completed.

Date / /

* Types & Techniques of Credit Card Frauds

Traditional Technique

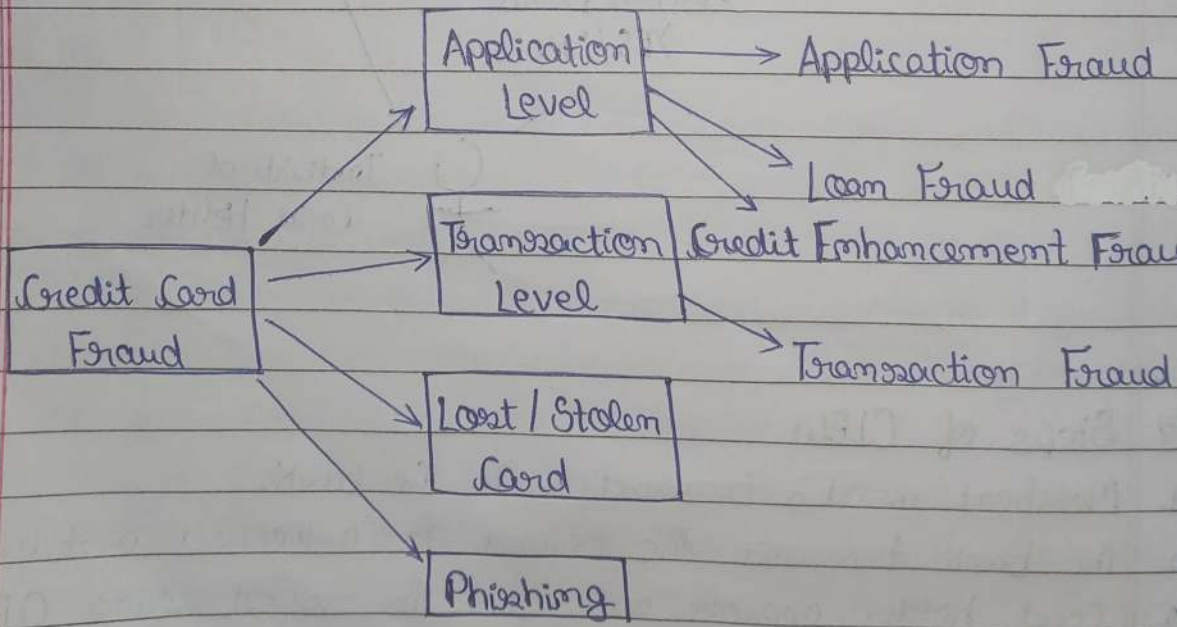
① ID Theft
Where an individual pretends to be someone else.

② Financial Frauds
When an individual gives informational about its financial status the result is financial fraud.

Modern Technique

① Triangulation
The criminal offers the goods with heavy discount through a website hosted by criminal. The customer registers on this website with his name, address and credit card detail.

② Credit Card Generators
It is a modern technique of credit card fraud, in this method a software creates a clone of the card.



Security Challenges Posed by Mobile Devices
↓
Generated

CLASSTIME Pg. No.
Date / /

Mobility bring 2 main challenges of Cyber Security.

1. On the handheld devices information is taken outside the environment.
2. Remote access provide access to your computer from anywhere.

As the number of mobile device increases the main challenges are :-

1. At the device level - Microchallenges.
2. At the organizational level - Macrochallenges.

★ Some well known technical challenges in mobile security are :-

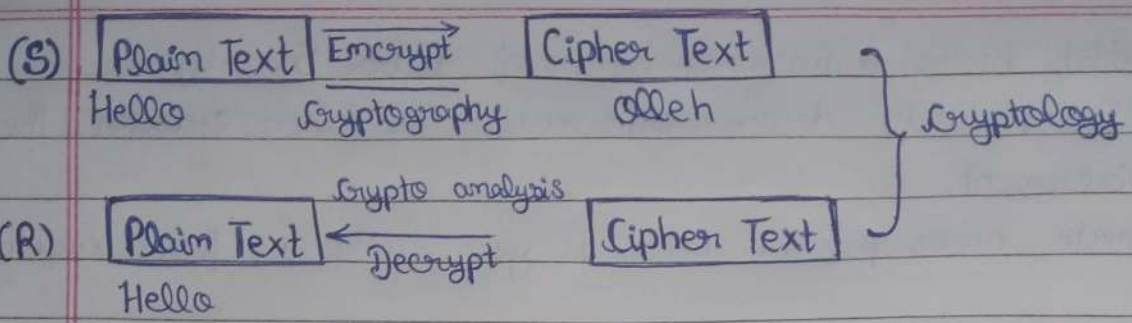
① Cryptography Security
② RAS Security
③ Media player control security
④ Network Application security

★ Overcome security challenges on mobile devices.

① Turn off Bluetooth.
② Encrypt your phone using Password and other method.
③ Back up of your data.
④ Update OS. (Operating System)
⑤ Download Anti-malware (Anti-virus)
⑥ Use public wifi with caution.

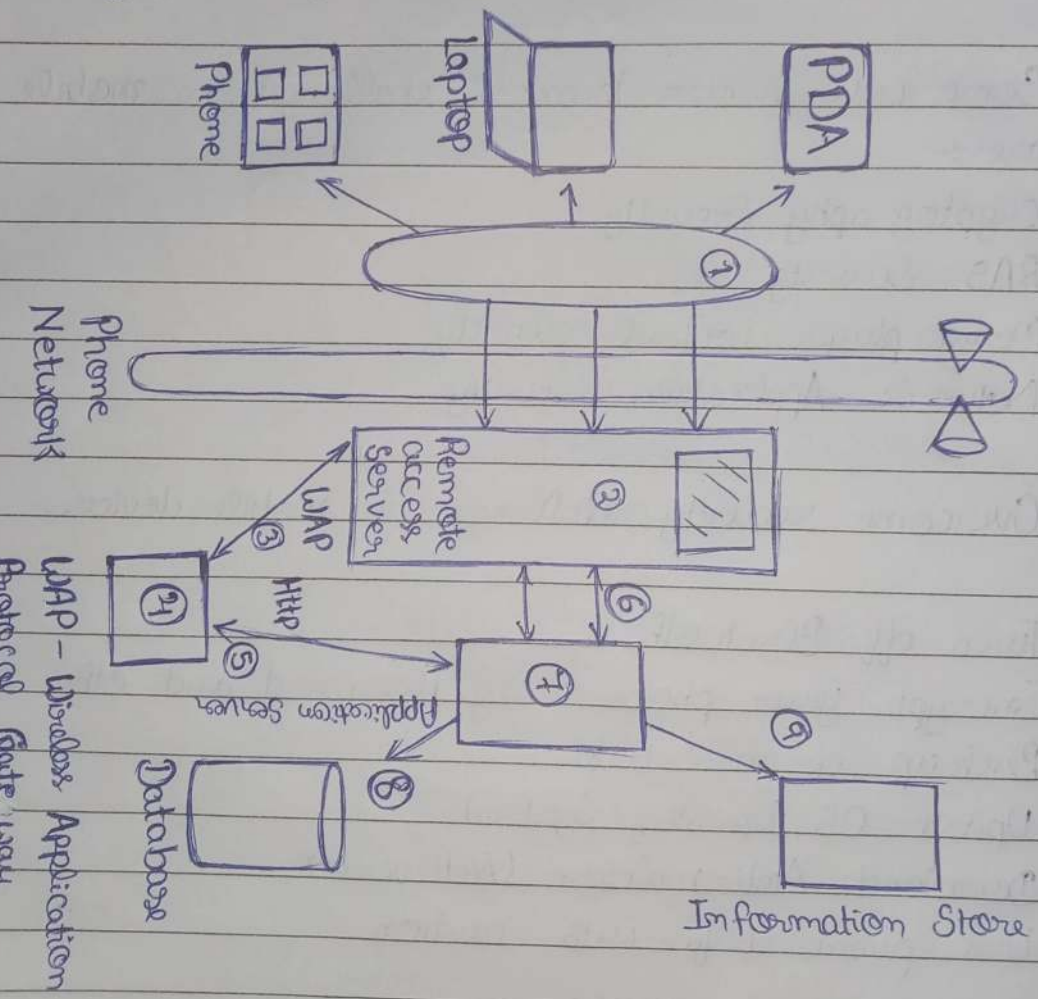
CRYPTOGRAPHY SECURITY

⇒ Cryptographic generated address IPV6 (Internet Protocol Version 6) address.
That can address upto 64 bits.



- RAS – (Remote Access Service)

⇒ It is a combination of Hardware and software that are used remotely access of mobile network.



- Media Player control security

Various software development organisation provide the warning text to user using the media player control.

- Network Application Security

CLASSTIME Pg. No.
Date / /

It provide various software and protocol for connecting the system to others.

E.g. :- 802-11, Wifi, IR (infrared)

It provide various software and protocol for connecting the system to others.
E.g. :- 802-11, Wifi, IR (infrared)

25/10/2023
Repeat

Media Player Control Security

Various Software development organisation provide the warning text to user using the media player control.

Authentication Service Security

There are two components of Security in mobile computing :-

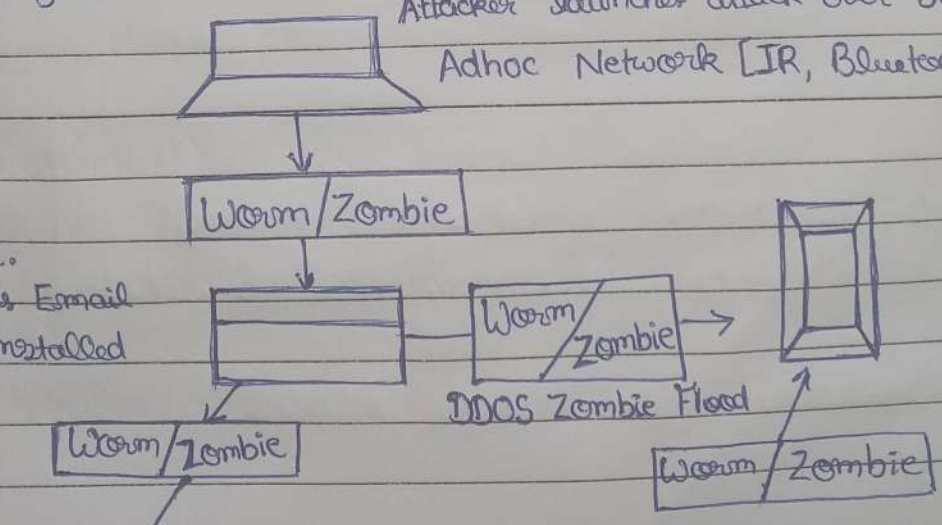
1) Security of devices
2) Security of network

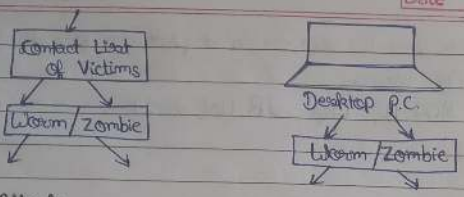
A secure network access involve mutual authentication between the device and the base station.
Some kind of attack on mobile devices are :-

1. PUSH attack
2. PULL attack
3. CRASH attack

1. PUSH attack

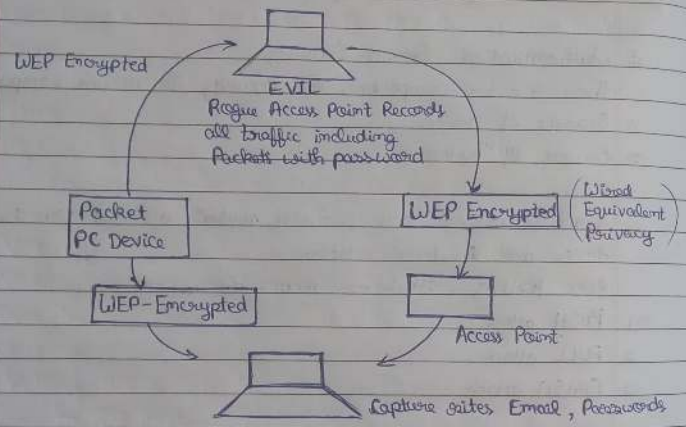
In PUSH attack, attacker create malicious code for gaining the access of system.





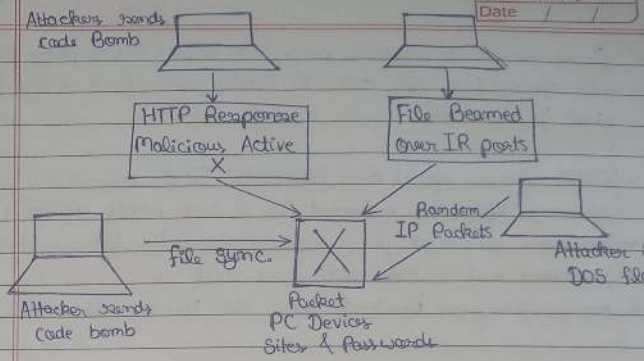
2. PULL Attack

In case of PULL attack, attacker control the device and handle it according to need.



3. CRASH Attack

In case of crash attack, attackers stops the services and crash the system and servers.



Attacks on Mobile Phone

① Mobile Phone Theft

They are the integral part of the life, Theft of mobile phones has rise in over the past few years. So many company's stop the mobile phone insurance due to large no. of claims.

⇒ Following factors contribute for mobile phone thefting :-

Ⓐ Enough Target Terminals (June 2004)

Discovered by an organization "O Jam" this virus send SMS to the organization without the user knowledge.

Ⓑ Enough Functionality

Mobile Phones devices have large no. of functions so it is easy to attack on mobile devices.

Ⓒ Enough Connectivity

Smart phone offers multiple communication options such as SMS, IR, and Bluetooth for connection.

② Mobile Viruses

It is similar to computer virus that target mobile phone data and its applications. Till date 40 mobile virus families are found and 300+ mobile viruses are identified.

Mobile Viruses spread over Bluetooth, SMS, IR.
Following tips are measured to protect mobile devices:-
1) Download or accept program only from trusted source.
2) Download and install anti-virus software
3) Always put your bluetooth into Non-Discoverable mode.

11/2023

Mishing

It is a combination of mobile & phishing. Attackers are very creative about to handle the user to try the personal information

Vishing

Vishing is a criminal practice of using social engineering over the telephone system. It is the combination of voice plus phishing.

⇒ Vishing attack include :
- ID Theft
- Purchasing luxury goods & services
- Transferring money
- Monitoring the victims bank accounts
- Making applications for loans

Phishing	Email
Smishing	SMS/Text message
Vishing	Phone, Voice call, VOIP

Protection from Vishing Attacks

① Be suspicious about unknown callers.
② Do not trust on caller ID.
③ Report incident for cyber police.

Protection from Smishing Attacks

① Do not answer a text message that you have received that is asking for your personal information.
② Never click ~~on~~ unknown link received on your mobile phones.

☆ Hacking Bluetooth

Bluetooth is an open wireless technology standard used for communication and exchanging the data with the frequency of 2.0 GHz (GigaHertz). Various tools are used for hacking a bluetooth device.

	Name of Tool	Description
①	Blue Scanner	This tool serves for bluetooth enabled device and will try to extract as much as information as possible.
②	Blue Sniff	It is a GUI base utility for finding discoverable and hidden bluetooth device
③	Blue Bugger	This tool exploit the vulnerability of the device and access the image phone book and messages from the mobile.
④	Blue Snoofer	If a ~~branch~~ bluetooth device is switched ON, then blue snoofer try to connect the phone without the permission of mobile phone user.
⑤	Blue Diving	It is used for testing a entrails for implementation of a attack.

CLASSTIME | Pg No.
Date / /

- **Blue Jacking**
  Jacking is the short form of Hijacking. It means hijack a bluetooth device.

- **Blue Bugging**
  It allows attackers to remotely access a user mobile phone without the knowledge of user.

- **Car Whisperer**
  It is a piece of software that allow attacker to send and receive audio from bluetooth enabled car stereo.

* Mobile Devices : Security Implications for Organizations

① Managing Diversity & Proliferation of hand held devices

Cyber security is the primary concern of the organization. Mobile Devices of the employee should be registered and monitor these device time to time.

② Unconventional / Stealth Storage Devices

Compact Disk and USB Drives used by the employee play a key role against cyber attacks because technology are advanced and these devices change their size & shape.

⇒ Following factors are involved against storage devices :-

1) Not only can viruses, worm and trojan but it can also destroy valuable data.
2) Organization have the policy to block all the codes.
3) Using Device Lock software stops Plug and Play devices.