UNIT-5

Activity No. Date :

Topic :

Aim/Objective :

Syllabus → Wireless Security
- ✓ Authentication & confidentiality
- ✓ Cell phone & GSM security
- ✓ Security in UMTS
- ✓ Wireless LAN vulnerabilities / Phising
- ✓ Buffer overflows
- ✓ Format String attacks, ✓ Cross-Site Scripting
- ✓ SQL injection
- Virtual Election

⑧ Types of WLAN

WLAN stands for wireless local area network. It uses radio communication to provide mobility to network users, while maintaing the connectivity to the wired ntw.

1) Wireless LAN : technology provide internet access within a building or limited outdoor area. uses in offices, homes, restaurants etc.

2) Wireless MAN : Wirless metropolitan area network has been installed in cities worldwide to provide access for people outside office, homes.

3) Wireless PAN : W personal area network covers a very limited area, typically a maximum 10 metre for most applications like Bluetooth, Zigbee.

4) Wireless WAN : use cellular technology use to provide access outside the range of WLAN or WMAN. Ynese network enables to make call to each other.

Wired ntw : In many organization wired ntw is an Ethernet LAN with an existing security infrastructure that includes an authentication Server (AS).

Principle of WLANs : 1) Adhoc N/w : where stations communicate directly with each other. (learn in NRA).

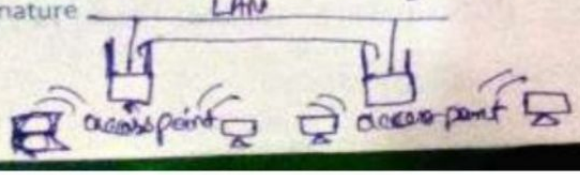
2) Infrastructure WLANs : which uses an access point (AP).

A Station first send a frame to an AP, then AP deliver it to its final destination.

→ Destination may be another wireless station or may be a station on the wired ntw that the AP is connected to.

→ Then AP serves as a bridge blw WAN and existing wired n/w.

Teacher's Signature



(*) Security issues in wireless Networks

WLANs transmit and receive data using radio wave rather than wires. This lack of physical barrier makes WLAN vulnerable to unlawful interception, hacking, a range of other cyber security issues.

→ Denial of Service attack: When the intruder flood the n/w with req. affecting the availability of n/w resource. (Matlb hackers attack karke ha our available resource use karke hain illegally)

→ Spoofing & session hijacking: attackers gain access to n/w data & resources by assuming identity of valid user (kisi person ka id login password churaa ke resource use kr lete hain).

→ Eavesdropping – when unauthorised third party intercept the data being transferred over secure network.

(**) WLAN, IEEE 802.11 Architecture (Imp) Components:

1) (STA) Stations: Station comprises all devices & equipments that are connected to wireless LAN.

Two types Station:

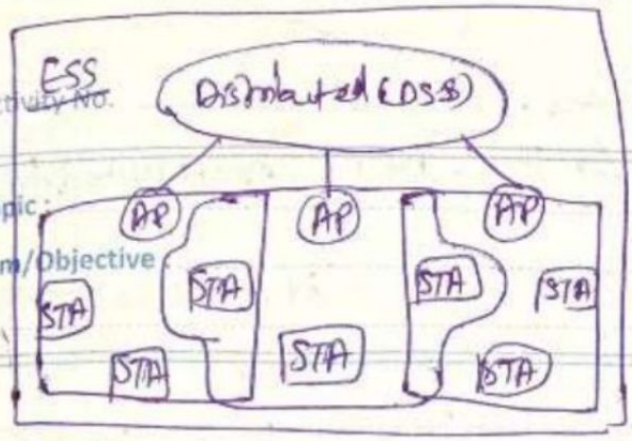
- (wireless Access point) WAP: WAP are generally wireless router that forms base stations or access.
- Client: Clients are workstations, PC, laptop, printer, cellphones

2) Basic Service Set (BSS): A grp of station communicating at physical layer level: BSS can be 2 categories:

- Independent BSS: device communicate with other dev. through AP.
- Infrastructure BSS: devices communicate in peer-to-peer basic in adhoc manner.

3) Extended system Set (ESS): It is Set of all connected BSS.

4) Distributed System: It connects access point (AP) in ESS.



Activity No.
Date:
Topic:
Aim/Objective:

Advantage of WLAN

- equipment, setup cost reduced.
- Easy to install
- LAN are scalable in nature.
- provide clutter free homes, offices.

Disadvantage of WLAN

- WLANs are slower than LAN.
- greater care is needed for encryp. information.
- Signal are noiser and more inference from nearby system.

IEEE 801.11 : It is a protocol that support authentication at link layer.

→ It involved three entities : Supplicant, authenticator, authentication Server.

→ different authentication mechanism are defined by (EAP) Extensible authentication Protocol standardized by IETF.

→ EAP is a framework upon which authentication protocol supported,

→ EAP exchanges mostly comprised request, responses.

(*) Frame format of IEE.801.11

- frame control : 2 byte starting field of 11 subfield, control info of frame.
- Duration : 2 byte field that specifies the time period for which the frame and its ack occupy channel.
- Address field : 6 byte field contains address of source, destination.
- Sequence : 2 byte field store frame no.
- Data : variable size field that carries data from the upper layer.
- Check sequence : 4 byte field containing error detection info.

diagram IEEE8M. frame format

WLAN security features

1) (SSIDs) Service set identifier : prevent connection to access point unless a device uses a given identifier correctly.

2) Media access point (MAC) : involves using address attach to each device to limit connection to access point.

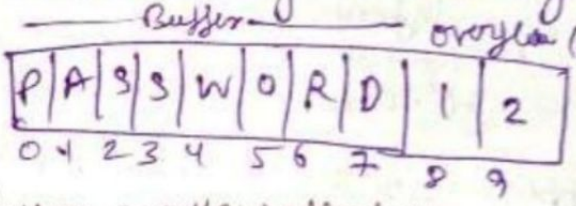
3) (WEP) Wired equivalent privacy : uses encryption keys, so device with correct key can communication with (AP).

Teacher's Signature

75

⊛ Buffer overflow

→ Buffer are memory storage regions.
→ It hold data temporarily while it is being transferred from one place to another
→ Buffer overflow occurs when volume of data exceeds storage capacity of memory buffer.
→ As a result program attempting to write data to the buffer overwrite adjacent memory locations.



⊛ Buffer overflow attacks:
→ attackers exploit Buffer overflow issue by overwriting the memory of an application
→ this changes the execution path of the program
→ triggering a response that damage files or expose private info.

⊛ Types of Buffer attack

1) Stack based buffer overflow: leverage taking stack memory that only exist during execution time of function.
2) Heap based attacks: involve flooding the memory space allocated for pgms.

⊛ Prevent Buffer overflow:

1) (ASLR) Address space randomization: randomly moves around the address space locations of data regions.
2) Data execution prevention: flags certain areas of memory as executable or non-executable.
3) Structured exception handler overwrite protection (SEHOP): helps stop malicious code from attacking Structured Exception Handling (SEH), a system ranging HW & SW exceptions

Activity No. Date:

Topic

Aim/Objective :

(*) Cross site scripting (XSS)

→ It is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website.

→ The actual attack occurs when the victim visits the web application that execute malacious code.

→ A web page or web application is vulnerable to XSS if it use unsanitized user input

→ The user input must then be parsed by victim's browsers.

→ XSS attacks are possible in VBScript, flash, even CSS. common in Javascript.

Two Stages of typical XSS attacks.

(1) → To run malicious Javascript code in a victim browser, an attacker must first find a way to inject malicious code into a web page that the victim visits.

(2) → After that, victim must visit the web page with malacious code. If the attack is directed at particular victims, the attacker can use social engineering to send a malicous URL to victim.

(*) SQL injection

→ It is code injection technique that might destroy the database.

→ It is most common web hacking technique, allow hackers to view data that are not able to retrieve.

→ SQL injection is the placement of malacious code in SQL statements via web page input

→ SQL injection occurs when you ask user input like username, id.

Teacher's Signature (77)

SQL eg: textUserID
getRequestString("UserId");
1st SQL : "Select * from User where
Userid = " + txtUserID;

(*) Common SQL injections

→ Retrieving hidden data : where we can modify SQL query to return add" result.

→ Union attack : where we can retrieve data from diff" DB tables.

→ Examine the DB where we extract info abt version/structure of db.

→ Blind SQL injection : where the result of query we control & not retrieved in application response.

How to detect SQL injection vulnerabilities ?
It can be found using web vulnerability scanner & manually by using a systematic set of test against entry point in the application.

(*) Format string attack

→ format string exploit occurs when the submitted data of an input string is evaluated as a command by application.

→ attackers can easily insert malicious code into string & access stack.

→ It exploit the programing language

→ format of format string attacks :

```
char * user_input = "foobar";
printf (user_input);
```

Activity No. Date :

Topic :

Aim/Objective :

⊛ Damages for a string format cause:-

1) Crash the prgm.
2) View data on the stack.
3) Views memory at arbitrary locations
4) Execute arbitrary code
5) Write data in arbitrary location.

⊛ Preventing format string attacks

1) If possible make format string constant
2) always specify a format string as a part of program rather than as input.
3) Use format guard, It is a small patch to glibc that provide general protections against format bugs.

⊛ UMTS

UMTS, universal mobile telecommunications system/framework

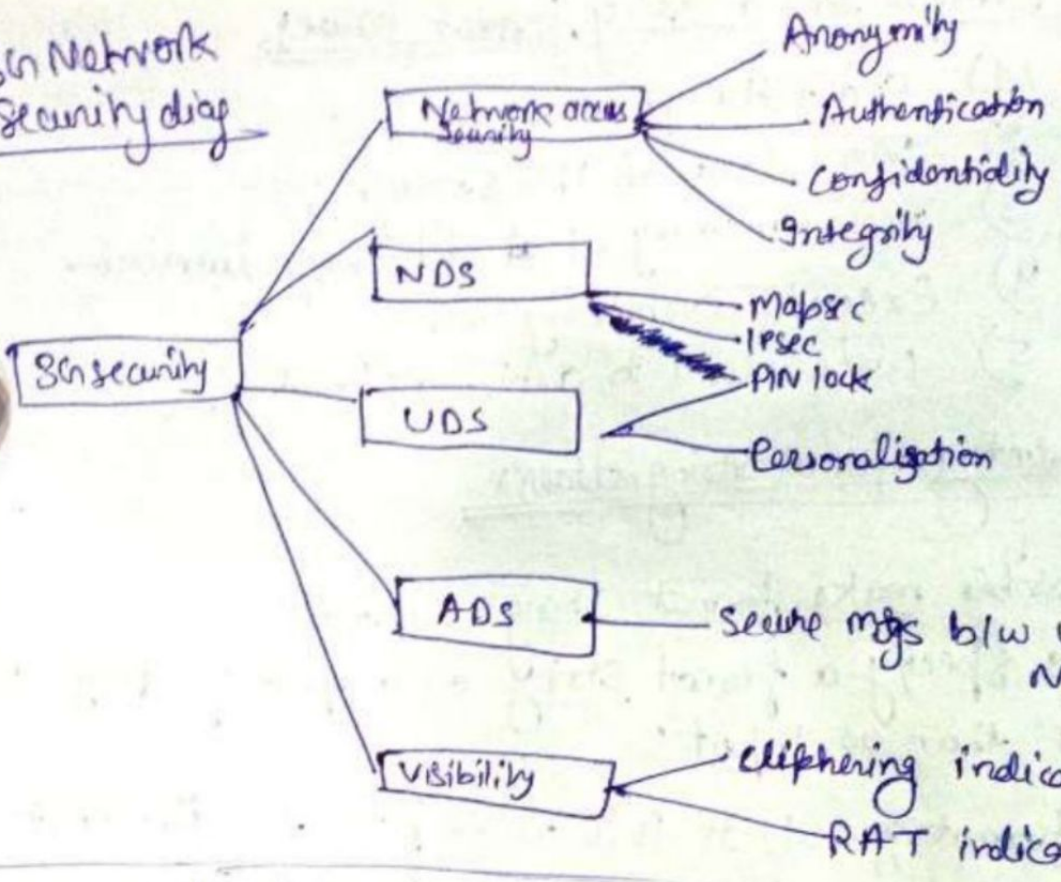
→ It is the 3g successor to the GSM family of measures counting GPRS and EDGE.
→ UMTS employments a completely diverse radio interface.
→ UMTS is designed to interoperate with GSM network
→ to protect GSM network against man-in-middle attacks.
→ UMTS security also referred as 3G security.
→ In UMTS authentication 'key' is shared blw network.

→ 5 security group exist in 3G network :

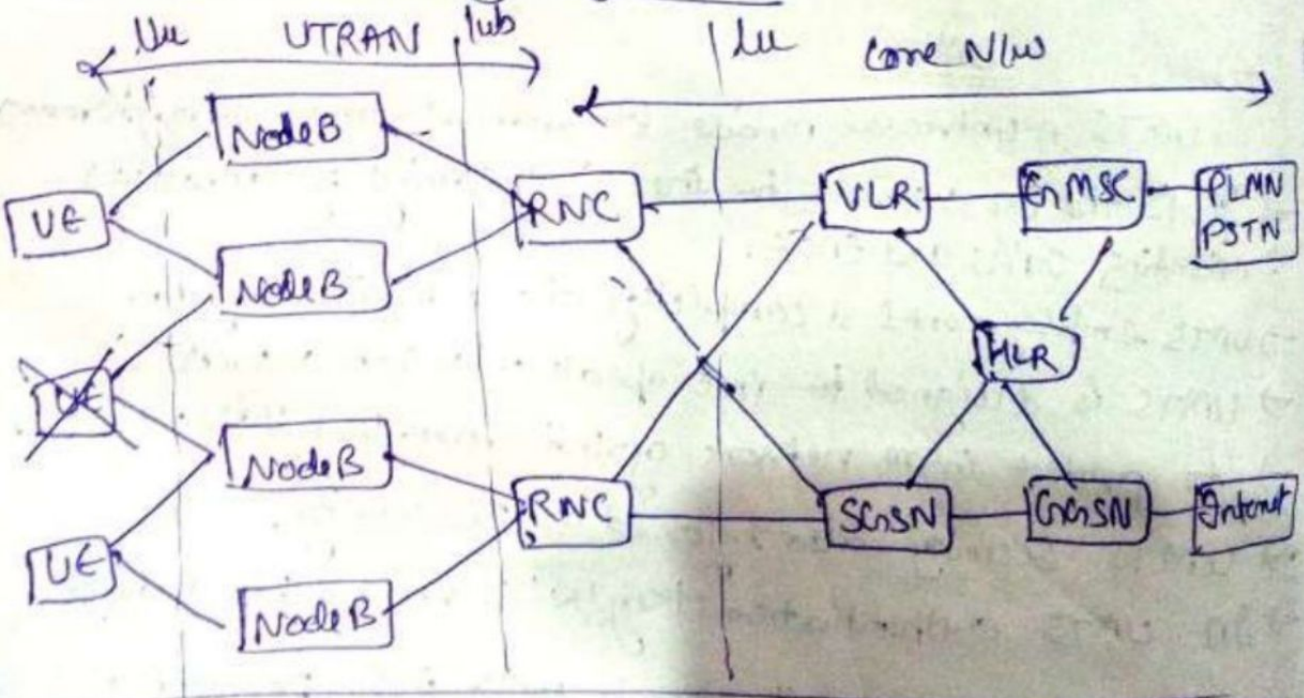
- Network access security
- Network domain security
- User domain Security
- Application domain
- Visibility, configuration of security

Teacher's Signature

3G Network Security diag



Architecture diagram of UMTS



→ (UE) User Equipment : is the name given to what was previously termed the mobile or cell phone

→ (RNS) Radio network subsystem : also known as

UMTS radio access network, it provide & manage air interface in n/w.

Activity No: Date:

→ VLR: visitor location Register; used to keep track of all mobile station that are currently connected to N/w.

Aim/Objective:

→ (HLR): Home location Register keep track of the current location of all home network subscriber.

→ (GGSN): gateway GSN

→ (SGSN): serving GPRS support node

Difference in FDMA, CDMA, TDMA, SDMA

Technique	FDMA	TDMA	CDMA	SDMA
Concept	divide the freq. band into disjoint subband	Divide the time into non-over lapping time slots.	Spread the signal with orthogonal codes.	Divide the space into sectors.
Active termination	all terminals active on their specified frequency	Terminal active in their specified slots.	all terminals active on same frequency	no of terminals per beam depend on FDMA/TDMA.
Handoff	Hard	Hard	Soft	Hard & soft
Advantage	Simple, Robust	flexible	Flexible	very simple inc. system capacity.
Current application	Radio, TV analog cellular	GSM & PDC	2.5G 3G	Satellite Systems.

Teacher's Signature

65

⊛ GSM Intro

→ Global system for mobile communication is a digital cellular communication system.

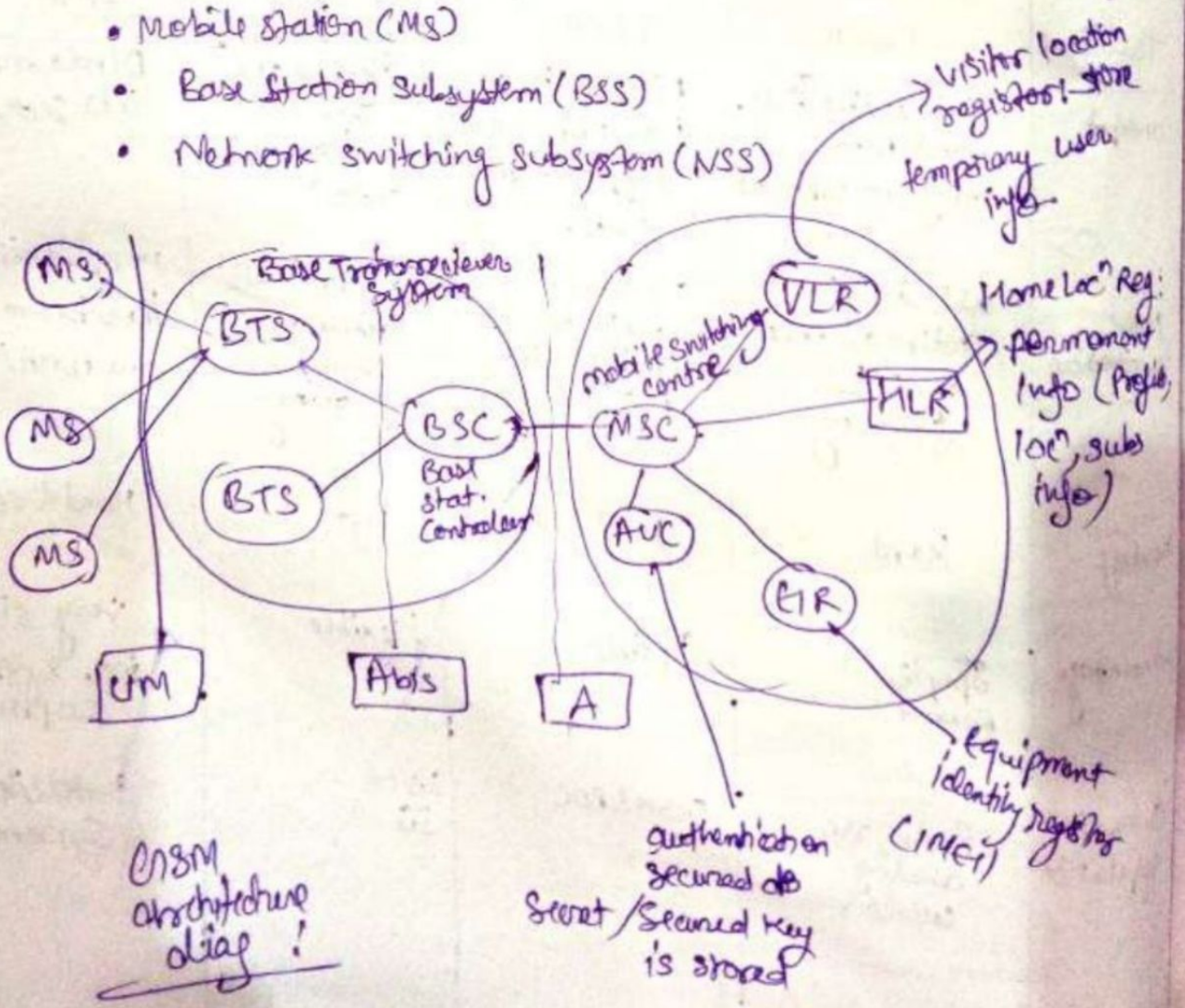
→ Based on digital technology

→ Standardized system had to meet certain Criteria's;

- International roaming
- Low mobile & base station costs.
- Spectrum efficiency
- ability to support new services.

⊛ GSM system architecture;

- Mobile station (MS)
- Base station subsystem (BSS)
- Network switching subsystem (NSS)



GSM architecture diag!

→ Cell size in GSM network :

- Macro : BS antenna is installed
- micro : antenna height < avg roof level
- Pico : small cells indoor.
- umbrella : cover shadowed region
  - → fill in gaps b/w cells.

GSM features :

- International roaming
- Good voice quality
- Low service cost
- New feat
- ISDN compability

NSS : Network switching System

component	function
BTS	encoding, encryption, decoding, decryption, multiplexing, modulation
BSC	frequency helping control, Traffic management, Power management Handoff management
MSC	Registration, authentication, loc^{n} update, call routing call setup, supervision

Cellphone Security

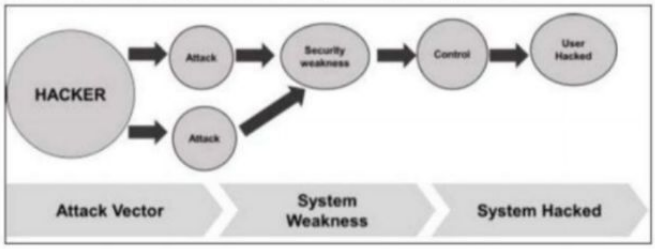
Mobile Security as a concept deals with the protection of our mobile devices from possible attacks by other mobile devices, or the wireless environment that the device is connected to.

Following are the major threats regarding mobile security −

- Loss of mobile device. This is a common issue that can put at risk not only you but even your contacts by possible phishing.
- Application hacking or breaching. This is the second most important issue. Many of us have downloaded and installed phone applications. Some of them request extra access or privileges such as access to your location, contact, browsing history for marketing purposes, but on the other hand, the site provides access to other contacts too. Other factors of concern are Trojans, viruses, etc.
- Smartphone theft is a common problem for owners of highly coveted smartphones such as iPhone or Android devices. The danger of corporate data, such as account credentials and access to email falling into the hands of a tech thief is a threat.

Mobile Security - Attack Vectors

By definition, an **Attack Vector** is a method or technique that a hacker uses to gain access to another computing device or network in order to inject a "bad code" often called **payload**. This vector helps hackers to exploit system vulnerabilities. Many of these attack vectors take advantage of the human element as it is the weakest point of this system. Following is the schematic representation of the attack vectors process which can be many at the same time used by a hacker.



Some of the mobile attack vectors are −

- Malware
  - Virus and Rootkit
  - Application modification
  - OS modification
- Data Exfiltration
  - Data leaves the organization
  - Print screen

[redacted]

  - Copy to USB and backup loss
- Data Tampering
  - Modification by another application
  - Undetected tamper attempts
  - Jail-broken devices
- Data Loss
  - Device loss
  - Unauthorized device access
  - Application vulnerabilities

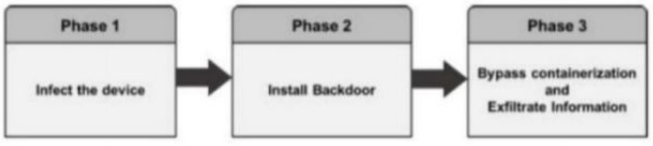
Consequences of Attack Vectors

Attack vectors is the hacking process as explained and it is successful, following is the impact on your mobile devices.

- **Losing your data** − If your mobile device has been hacked, or a virus introduced, then all your stored data is lost and taken by the attacker.
- **Bad use of your mobile resources** − Which means that your network or mobile device can go in overload so you are unable to access your genuine services. In worse scenarios, to be used by the hacker to attach another machine or network.
- **Reputation loss** − In case your Facebook account or business email account is hacked, the hacker can send fake messages to your friends, business partners and other contacts. This might damage your reputation.
- **Identity theft** − There can be a case of identity theft such as photo, name, address, credit card, etc. and the same can be used for a crime.

Anatomy of a Mobile Attack

Following is a schematic representation of the anatomy of a mobile attack. It starts with the infection phase which includes attack vectors.



Infecting the device

Infecting the device with mobile spyware is performed differently for Android and iOS devices.

Android − Users are tricked to download an app from the market or from a third-party application generally by using social engineering attack. Remote infection can also be performed through a Man-in-the-Middle (MitM) attack, where an active adversary intercepts the user's mobile communications to inject the malware.

iOS − iOS infection requires physical access to the mobile. Infecting the device can also be through exploiting a zero-day such as the JailbreakME exploit.

Installing a backdoor

To install a backdoor requires administrator privileges by rooting Android devices and jailbreaking Apple devices. Despite device manufacturers placing rooting/jailbreaking detection mechanisms, mobile spyware easily bypasses them −

Android − Rooting detection mechanisms do not apply to intentional rooting.

iOS − The jailbreaking "community" is vociferous and motivated.

Bypassing encryption mechanisms and exfiltrating information

Spyware sends mobile content such as encrypted emails and messages to the attacker servers in plain text. The spyware does not directly attack the secure container. It grabs the data at the point where the user pulls up data from the secure container in order to

Below are seven of the most common threats to wireless networks.

- Configuration Problems (Misconfigurations or Incomplete Configurations) ...
- Denial of Service. ...

7

- Passive Capturing. ...
- Rogue (or Unauthorized/Ad-Hoc) Access Points. ...
- Evil Twin Attacks. ...
- Hacking of Lost or Stolen Wireless Devices. ...
- Freeloading.

Network Threats (and How to Protect Against Them)

While deceitful actions do commonly occur, there are also many accounts of innocent, yet careless, actions are often the cause of a major security breach. Below are seven of the most common threats to wireless networks.

1. Configuration Problems (Misconfigurations or Incomplete Configurations)

Simple configuration problems are often the cause of many vulnerabilities because many consumer/SOHO-grade access points ship with no security configuration at all. Other potential issues with configuration include weak passphrases, feeble security deployments, and default SSID usage.

A novice user can quickly set up one of these devices and gain access, or open up a network to external use without further configuration. These acts allow attackers to steal an SSID and connect without anyone being the wiser.

To mitigate the risk, use a centrally managed WLAN that features periodic audits and coordinated updates.

2. Denial of Service

Anybody familiar with network security is aware of the concept of denial of service (DoS), also referred to as a "spoiler." It is one of the simplest network attacks to perpetrate because it only requires limiting access to services. This can be done by placing viruses or worm programs on your network, or by simply sending a large amount of traffic at a specific target with the intent of causing a slowdown or shutdown of wireless services. This allows attackers to hijack resources, view unauthorized information disclosures, and introduce backdoors into the system.

For wireless networks it can be much easier, as the signal can be interfered with through a number of different techniques. When a wireless LAN is using the 2.4 GHz band, interference can be caused by something as simple as a microwave oven or a competing access point on the same channel. Because the 2.4 GHz band is limited to only three non-overlapping channels (in the U.S.), an attacker just needs to cause enough interference into these to cause service interruption.

A denial of service attack can also be used in conjunction with a rogue access point. For example, one could be set up in a channel not used by the legitimate access point. Then a denial of service attack could be launched at the channel currently being used, causing endpoint devices to try and re-associate onto a different channel that is used by the rogue access point.

3. Passive Capturing

Passive capturing (or eavesdropping) is performed simply by getting within range of a target wireless LAN, then 'listening to' and capturing data which can be used for breaking existing security settings and analyzing non-secured traffic. Such information that can be "heard" include SSIDs, packet exchanges, and files (including confidential ones).

Consider the following scenarios that make passive capturing possible:

8

- Your office building has multiple tenants, including immediately above or below you on different floors.
- You have a lobby just outside your office.
- Your parking lot is close to the building.
- There is a street that passes nearby.

4. Rogue (or Unauthorized/Ad-Hoc) Access Points

One method often used by attackers involves setting up a rogue access point within the range of an existing wireless LAN. The idea is to 'fool' some of the authorized devices in the area to associate with the false access point, rather than the legitimate one.

To really be effective, this type of attack requires some amount of physical access. This is required because if a user associates with a rogue access point, then is unable to perform any of their normal duties, the vulnerability will be short-lived and not that effective. However, if an attacker is able to gain access to a physical port on a company network and then hook the access point into this port, it's possible to get devices to associate and capture data from them for an extended period of time.

The exception to this barrier is when the wireless LAN being targeted only provides internet access. A rogue access point can also offer simple internet access and leave the user unaware of their vulnerability for an extended amount of time.

Part of the same idea of rogue access points is unauthorized, non-malicious access points and ad-hoc networks. In these situations, a legitimate user sets up an access point or ad-hoc network for their own use, but does not implement proper security techniques. This provides an opening for watching attackers.

Some steps you can take to prevent such access points are to:

- Use proper WLAN authentication techniques and encryption methods.
- Establish and communicate a policy prohibiting employees from using their own wireless access points.

- Make it easier for employees to gain access to legitimate (and secured) wireless access points.
- Regularly walk around your office with a wireless-equipped device to search for rogue access points, looking in every network outlet.
- Install a WIPS (wireless intrusion prevention system) to scan radio spectrums, searching for access points with configuration errors.

5. Evil Twin Attacks

An attacker can gather enough information about a wireless access point to impersonate it with their own, stronger broadcast signal. This fools unsuspecting users into connecting with the evil twin signal and allows data to be read or sent over the internet.

Server authentication and penetration testing are the only tools that will aid in ending evil twin attacks.

6. Hacking of Lost or Stolen Wireless Devices

Often ignored because it seems so innocent, but if an employee loses a smartphone, laptop, etc., that is authorized to be connected to your network, it's very easy for the finder or thief to gain full access. All that's necessary is to get past the password, which is quite simple to do.

Make it a policy and practice to have employees immediately report a misplaced or stolen device so that it can be remotely locked, given a password change, or wiped clean.

7. Freeloading

Sometimes unauthorized users will piggyback on your wireless network to gain free access. Usually this is not done maliciously, but there are still security ramifications.

1. Your internet service may slow down.
2. Illegal content or spam can be downloaded via your mail server.
3. "Innocent" snooping may take place.

Additionally, employees sharing files with unrecognized networks, or giving permission for a friend or family member to use their login credentials for computer access, both seriously disrupt security measures.

Phishing:-

Phishing is a type of Social Engineering attack in which the victims are psychologically manipulated to provide sensitive information or install malicious programs. It is similar to 'fishing.' While in fishing, the fishermen use the fish food as the bait to trap fishes into fishing-net or fishing rod, in Phishing the cyber attackers use fake offers, warnings as bait to trap users into their scam.

The attackers can perform Phishing through emails, SMS, phone call, fake websites, and even face to face.

We will now discuss how Phishing is performed through different mediums.

How is Phishing Performed through Emails

For performing Phishing through emails, Cybercriminals follow these steps −

- At first, the targets are finalized, and details about them are collected. The target can be an individual, group of people or an organization.