NS Unit-5

* Wireless LAN security :-

Some of the key factors contributing to the higher security risk of wireless n/w compared to wired n/ws include the following :-

(i) Channel :- Eavesdropping (~~security/privacy~~) than wired n/ws. Wireless n/ws are also more vulnerable to active attack that exploit

(ii) Mobility :- Mobility results in number of risks.

(iii) Resources :- Limited memory & resources with which to counter threats, including DOS and malware.

(iv) Accessibility :- Greatly increases their vulnerabilities to physical attacks.

* Wireless Security Threats (1)

(i) Accidental association :- A user intended to connect to one LAN might accidently/unintentionally lock on to a wireless access point in the neighbour.

(ii) Malicious association :- A wireless devices is configured to be a legitimate acess point enabling the operator to steal password ~~from~~ and penetrate a wired n/w.

(iii) Adhoc n/w :- peer-peer n/ws bet° wireless computer with no access point bet° them.

(iv) Non-traditional n/w :- Bluetooth devices, barcode readers pose a security risk. ~~is term~~

* Wireless Security Threat (2)

(i) Identity theft (MAC spoofing) :- When attacker is able

eavesdropping ⇒ when a hacker intercepts, deletes or modifies data transmission bet² two devices.

to eavesdrop on n/w traffic and identify MAC address of a computer with n/w privileges.

(ii) Man-in-middle attack :- In this communication is going through an intermediate attacking device. wireless n/ws are particularly vulnerable to such threats.

(iii) DOS :- It is easy for the attacker to easily attack to the direct wireless messages at the target.

(iv) Network injection :- A n/w injection attack targets wireless access point that are exposed to non-filtered n/w traffic such as routing protocol messages or n/w management messages.

* Wireless Security Measures (1)

→ Securing wireless Transmission principal threats to wireless transmission are eavesdropping, altering or inserting messages and disruption

- Signal-Hiding techniques :-
Organisations take a no. of measures to make it more difficult for an attacker to locate their wireless access point, including turning off services set identifier (SSID) broadcasting by wireless access points.
Reducing signal strength to the lowest that still provides requisite coverage and locating wireless access point in the interior of the building.

- Encryption :- Encryption of all wireless transmission is effective against eavesdropping to the extent that encrypted keys are secured.

* Wireless Security Measures (2) Securing wireless Access Point
→ The main threat involving wireless access point is unauthorized access to the n/w.
→ The principal approach for preventing such access is IEEE 802.1X standard for port-based network access control.
→ Securing wireless n/ws :-
(i) Use encryption :- Wireless routers are typically equipped with built-in-encryption mechanism for router-to-router traffic.
(ii) Use antivirus and antispyware and a firewall.
(iii) Change your router pre-set password for administration
(iv) Allow only specific computers to access your wireless network.

* Authentication in Wireless LAN :-
→ 802.11 authentication is the first step in n/w attachment. 802.11 authentication requires a mobile device (station) to establish its identity with an access point.
No data encryption or security is available at this page.
→ The Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard defines 2 link-level types of authentication.
• open system • shared key.
(i) Open system authentication :-
→ Consists of two communication
(i) First, an authentication request is sent from the mobile device that contains the station ID (typically MAC address)

AP → Access Point

(3) Next, an authentication response from AP/router with a success or failure message.

2. Shared key authentication :-

→ With shared key authentication ~~response from AP/router~~ is a shared key, ~~or~~ is manually set on both the mobile device and the router

* Authentication and Confidentiality Wireless Security

Confidentiality attack :-

→ The role of attacks targeting the confidentiality of information, is simply to break the encryption model used in the wireless deployment

• Recommendations for security models :-

WEP encryption

(i) ~~Non~~ encryption :- These are not very secure approaches and should not be used under any circumstances.

(ii) TKIP encryption :- This encryption model is used in WPA deployments. TKIP is not considered as strong mean of encryption.

(iii) CCMP encryption :- This is used with WPA2. So far, it is considered as safest encryption model that is based on not breakable AES algo.

* Wireless Security Authentication attack :-

→ Authentication is the method of verifying the presented identity and credentials. Most of the schemes used in wireless setups are secured with proper encryption.

→ The EAP authentication used in WPA/WPA2 with PSK authentication. By sniffing the 4-way handshake betⁿ the client & the authenticator (AP) one may perform a brute-force attack to break the encryption and derive PSK value.

→ Another ex. can be LEAP (Light weight Extensible Authentication Protocol). It was used in olden times as mechanism to generate dynamic WEP keys.

→ A short description of the authentication attack that may be applied to LEAP would consist of following step.

- The username is sent in a clear text
- There is a challenge text in clear text
- The response text is hashed
- Office dictionary attack, that can be used here to try all the combinations of password inside "function (password, challenge) : response" mathematical formula to find right password

* Cell phone Security :-

→ Mobile security is a concept that 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 :-

① Loss of mobile device :- This is a common issue that can put at risk not only you but your contacts by possible phishing.

(11) Application hacking or breaching :-

→ Most of us have downloaded and installed phone appl^{n}. Some of them request extra access or privileges such as access to your location, contact, browsing history and, the site provides access to other contacts too.
other factors of concern are Trojans, virus etc.

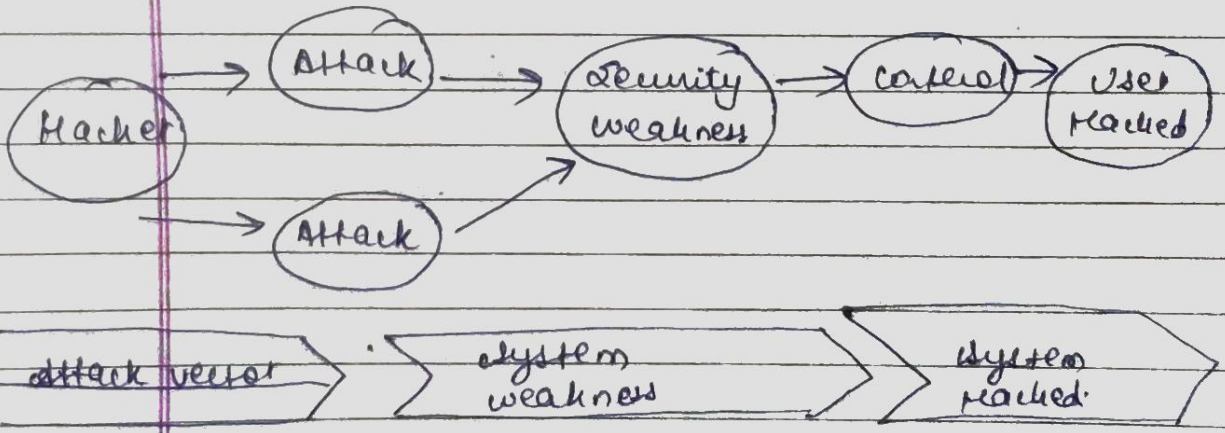
* Mobile Security - Attack Venders :-

→ Attack vender is a method or technique that a hacker use to gain access to other computing devices or n/w in order to inject a "bad code" often called payload.

→ This vector helps attackers to exploit system vulnerabilities.

→ Many of these attacks takes adv. of human element as it is the weakest point of the system.

→ Following is the representation of attack vectors process which can be many at the same time used by a hacker.



→ Some of the mobile attacks vectors are :-

- Malware
  - Virus and Rootkit
  - Appl^n modification
  - OS "
- Data Exfiltration
  - Data leaves the organization
  - Print screen
  - Copy to USB and backup loss
- Data Tampering
  - Modification by another appl^n
  - Undetected tamper attempts
  - Jail-broken devices.
- Data loss
  - Device loss
  - Unauthorized device access
  - Appl^n vulnerabilities

* Consequences of attack vendors :-

(i) Losing your data :- All the mobile data stored is lost and taken by the attacker [when mobile is hacked]

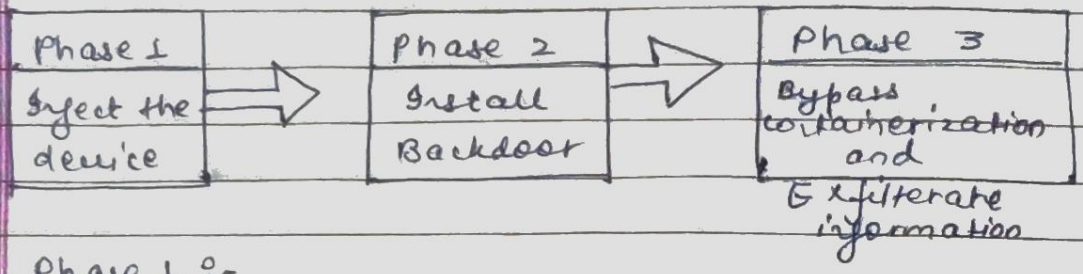
(ii) Bad use of your mobile resources :- which means that your n/w or mobile device can go in overload so you are unable to access your genuine services.

(iii) Reputation loss :- In case your facebook or business email account is hacked, the hacker can send fake messages to your business partners & other contacts this might damage your reputation

Jailbreaking ⇒ gaining unauthorized access root access to OS by modifying the iOS.

- Identity theft :- There can be a case of identity theft such as photo, name, address, credit card etc and same can be used for crime.

* Anatomy of Mobile attack :-



* Phase 1 :-

Injecting the device :-

→ Performed differently for mobile users & iOS

→ Android :-

- Users are tricked to download an app from the market or 3rd party appl^n generally by using social engineering attack.
- Remote injection can also be performed through a man-in-the-middle (MiTM) attack, where an active adversary intercepts the user's mobile communication to inject the malware

→ iOS :-

iOS injection requires physical access to the mobile

* Phase 2 [Installing a Backdoor]

→ To install a backdoor requires administrator privileges by rooting android devices and jailbreaking Apple devices.

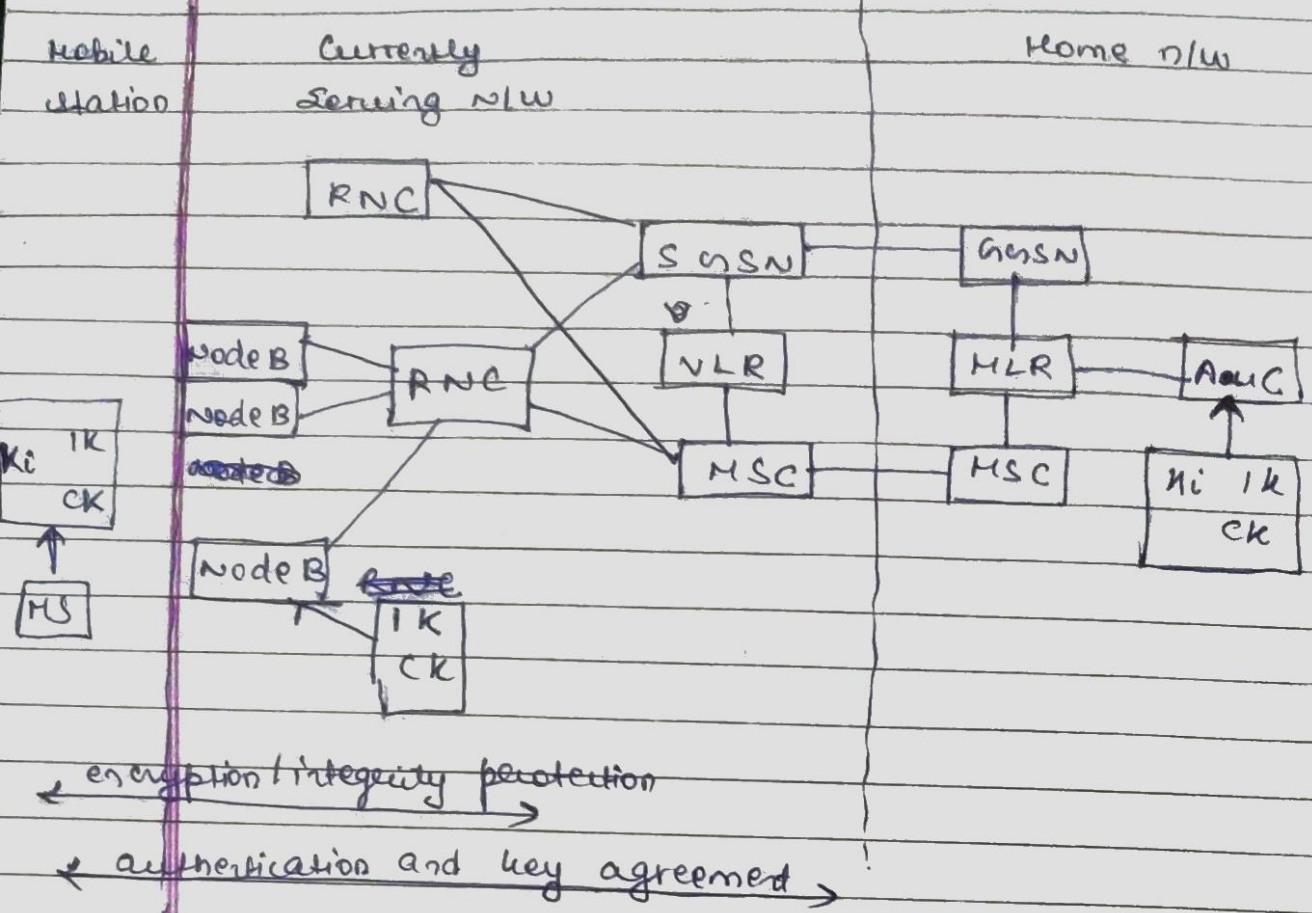
→ Despite devices manufacturers placing rooting / jailbreaking detection mechanism, mobile spyware

easily bypass them -
Android :- Rooting detection mechanism do not apply to intentional rooting.
iOS :- The Jailbreaking community is motivated.

* Phase 3 :- (Bypass encryption mechanism and exfiltrating info.)
→ 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 breaks the data at the point where the user pulls up data from secure container in order to read it.
→ At that stage, when the content is decrypted for user's usage, the spyware takes control of the content and sends it on.

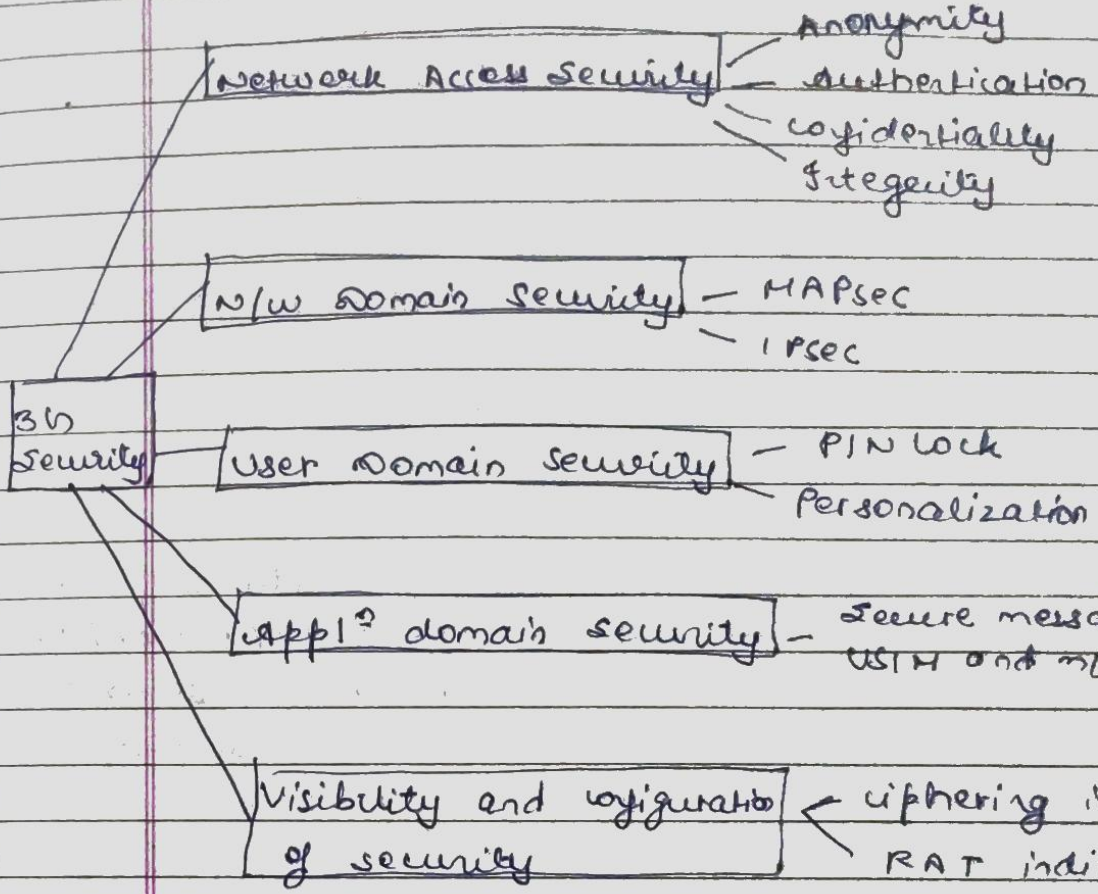
* Security in UMTS (3G)
→ Universal Mobile Telecommunication system (UMTS)
→ UMTS is designed to interoperate with GSM networks.
→ To protect GSM n/w against man-in-middle attacks, 3GPP [Third Generation Partnership Project) is considered to add a structure RAND [Random number development] authentication challenge.
→ In UMTS, security mechanism is developed to take care of all the GSM security shortfalls.
→ UMTS security is also referred to as 3G security

UMTS architecture and storage of Secret keys



MS → Mobile station
Node B → Base Transceiver Station
RNC → Radio N/W controller
SGSN → Serving GPRS support Node
MSC → Mobile Switching Center
VLR → Visitor location Register
HLR → Home location Register
GGSN → Gateway GSN
AuC → authentication center
Ki → Secret for subscriber key
CK → Encryption key
IK → Integrity key.

* Five security group exist in 3G n/ws as shown in figure.



→ N/w Access security helps protect air interface and also provides 3G subscribers to access 3G n/w securely.

→ In UMTS authentication, key 'K' is shared bet? n/w and UE [user equipment].

→ The n/w transmits a random generated no. 'RAND' and 'AUTN' [Aeronautical Telecommunication Network] in the message authentication challenge to the UE.

→ AUTN makes it possible for UE to authenticate the 3G n/w.

→ USIM generates response back to the n/w with integrity keys. this helps n/w authenticate the UE.

→ Major difference bet^n GSM security & 3G security

GSM	3G security
(i) N/w authentication was not possible with GSM compliant UE.	(i) Possible in UMTS compliant UE
(ii) Cipher key (Kc) is 64-bits in GSM	(ii) 128 bits
(iii) Ciphering is provided only to air interface and ciphering bet^n MS and BTS is not provided.	(iii) Security is provided bet^n UTRAN and RNC. Hence, 3G security is extented bet^n UE and RNC

* Wireless LAN vulnerabilities :-

→ Below are the most common threats to wireless networks.

1. Configuration problem :-

→ Simple configuration problem are often cause of many vulnerabilities because many customers or SOHO (Small office / Home office) - grade access point ship with no security configuration at all.

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

2. Denial of Service :-

→ Simplest n/w attack and can be done by placing viruses or worm program on your n/w or by sending a large amount of traffic at a specific ~~traffic~~ target with the intent of causing a slowdown / shutdown of wireless services this allows attackers to hijak resources, view unauthorized information.

→ For wireless n/w it can be much easier, as the signal can be interferred with through a no. of different techniques.
When a wireless LAN is using 2.4 GHz band, interference can be caused by something as simple as a microwave oven.

3. Passive capturing :-

→ Passive capturing (eavesdropping) is performed simply by getting within range of a target wireless LAN and then 'listening in' and capturing data which can be used for breaking existing security settings and analyzing non-secure traffic.
Such info can be "heard" include SSIDs, packet exchanges and files.

→ Consider the following scenarios that make passive capturing possible :-

① Your office building has multiple tenants, above or below you on diff. floors.
② You have lobby just outside your office
③ Your parking lot is close to the building

④ There is a street that passes nearby.
⑤ There are adjacent buildings.

→ Passive capturing is possible anywhere. There are also some go-arounds when an attacker can't be within normal broadcast range, such as using big antennas or a wireless repeater device to extend range by miles.
→ It is impossible to completely prevent this attack coz of the nature of wireless n/w what we can do is use high security st. and using complex parameters.

4. Rogue or Unauthorized / Ad-hoc Access Point
→ Attackers set up rogue access point within the range of existing wireless LAN.
→ The idea is to 'fool' some of the authorized device in the area to associate with false access point.
→ This requires some amount of physical access
→ If a user associate with a rogue access point then is unable to perform any of their normal duties. The vulnerabilities will be short-lived and not that effective.
→ The exception to this barrier is when the wireless LAN being targeted only provides internet access.
→ Some steps you can take such access point are
① Use proper WLAN authentication technique and encryption methods.

(5) Make it easier for employees to gain access to legitimate (and secure) wireless access points.
(3) Regularly walk around your office with a wireless-equiped device to search for rogue access point.
(4) Install a WIPS (Wireless Intrusion Prevention System) to scan radio spectrums, searching for access points with configuration error.

8. Evil Twin Attacks :-
→ An attacker gather enough info. about wireless access point to impersonate it with their own stronger broadcast signal.
This fools the user into connecting with the evil twin signal and allows data to be read or sent over the internet.
→ Remedy :- Server authentication
Penetration testing.

6. Hacking of Lost or Stolen Wireless Devices :-
→ If an employee loses a smartphone, laptop that is authorized to be connected to your nlw, it is very easy for the attacker to gain full access.
→ Remedy :- Making a policy where employees immediately report a misplaced or stolen device so that it can be remotely locked, given a password change.

ANKIT
Date
Page

7. Freeloading :-

→ Sometimes unauthorized users will piggyback on your wireless n/w to gain your access.

→ Internet service may slow down.

→ Illegal content or spam can be downloaded w/o your mail server.

* Phishing :-

→ Type of social engineering attack in which the victims are ~~forgot~~ psychologically manipulated to provide sensitive info. or install malicious programs.

→ In Phishing the cyber attackers use fake offers, warnings as bait to trap users into their scam.

→ The attacker can perform Phishing through emails, SMS, phone calls, fake websites and even face to face.

How Phishing is performed through Email

- At first target is finalized and details about them are collected. The target can be group of people, individual or an organization.
- Now, email message is framed based on the details gain from previous step. For ex. a fake banking email is prepared by knowing in which bank the target's account is.
- The mail is sent with catchy subject line

and pictures. The email is sent to thousand people so that atleast 100 of them get into this trap.

- after getting response from few people, the Phisher now collects sensitive info.. ~~or mal~~
- The info. obtained is used conduct activities like stealing money from account, hacking social media sites etc.

* Buffer Overflow :-

→ A buffer overflow arises when a program tries to store more data in a temporary data storage area (buffer) than it was intended to hold.

→ Since, buffer are created to contain a finite amount of data, the extra info. can overflow into adjacent buffers, thus corrupting files in them.

* Format string attacks :-

PAGE NO.
DATE / /

GSM (Global System for Mobiles) — C, A, I

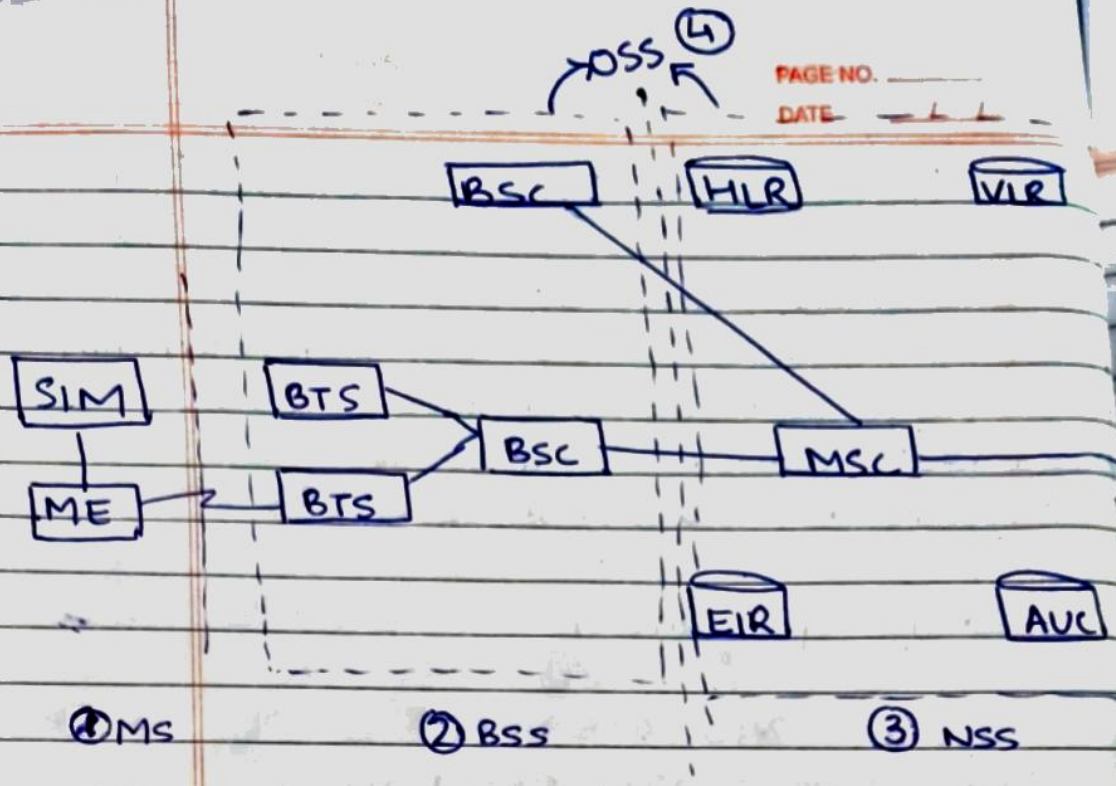
→ It is a 2G Network
→ Developed in 1991 by European telecomm
→ Supports voice and data services
→ GSM introduced sim card
→ 2G handset (low cost, size)

GSM Specification

Uplink - 890-915 MHz
Downlink - 935-960 MHz
Transfer Rate - 9.6 Kbps
No. of carriers - 124
Carrier Separation - 200KHz
Modulation - GMSK
Access Method - TDMA / FDMA
Time slot - 8
GSM speed - 14.4 Kbps

GSM Architecture

1) Mobile Station (MS)
2) Basic Station Subsystem (BSS)
3) Network Switching Subsystem (NSS)
4) Operation Support Subsystem (OSS)



ME → Mobile Equipment
BTS → Base Transreceiver Station
HLR → Home location Register
VLR → Visitor Location Register
EIR → Equipment Identity Register
AUC → Authentication Centre
MSC → Mobile Service Switching Centre
BSC → Base Station Controller

(1) MS

1) MS → Mobile Station.
2) SIM → used to send & receive calls & messages

3) ME → IMEI Number.

(2) BSS

4) BTS → send and receive signal from mobile phone

5) BSC → controls group of BTS
→ Allocate Radio channels
→ Handover from one BTS to another BTS.

(3)

6) NSS

MSC → Heart of GSM Network
→ Management of mobile services like registration, authentication
→ Communicate with HLR, VLR, AUC, EIR.

EIR → Database containing all valid handset on network using IMEI number

AUC → Protected database that store copy of IMEI no, used for authentication & encryption

VLR → Subset of HLR
→ local database for user visiting location in other domain

HLR → Master database of user, current location & information.

(4)

7) OSS
→ Connected to all equipment in switching system
→ Security operation and performance management
→ Network configuration and maintenance task
→ Admin & commercial operation

PSTN - Public Switch Telephon Network
ISDN - Integrated Service Digital Network

PAGE NO. _____
DATE 1 1

Security of GSM

The main security goal in GSM is
C → Confidentiality
I → Integrity
A → Authentication

1) Confidentiality – One of the most important security is to protect user message

2) Entity Authentication – The MSC needs to be sure that the call is billed to the person making the calls.

3) Message Integrity – The receiver needs to verify that the message has be received without error

The main step in Authentication are :-
Step1 : Authentication request from cellphone

Step2 : Creation And transmission of authentication vector

Step3 : Cellphone respons
Step4 : Receipt of encryption key

Authentication and confidentiality Wireless security confidentiality attack :-

The role of attacks targeting the confidentiality of the information, is simply to break the encryption model used in the wireless deployment. Looking at variety of security models in the field the following general recommendations may be put –

- **No Encryption/ WEP Encryption** – These are not very secure approaches and should not be used under any circumstances.
- **TKIP Encryption** – This encryption model is used in WPA deployments. It has not yet been cracked, but TKIP is not considered as strong mean of encryption, due to the use of weaker RC4 algorithm.
- **CCMP Encryption** – This is used with WPA2. So far, it is considered the safest encryption model that is based on not-breakable (at least for today) AES algorithm.

The main goal of all kinds of attacks is to break the encryption and get a value of the key. This would give the attacker 2 things: broken confidentiality of other users and direct access to the wireless network.

Format String Attacks:-

How does format string attack work?

Format String attacks **alter the flow of an application**. They use string formatting library features to access other memory space. Vulnerabilities occurred when the user-supplied data is deployed directly as formatting string input for certain C/C++ functions (e.g., fprintf, printf, sprintf, setproctitle, syslog, ...).

SQL Injection:-

SQL injection is **a code injection technique that might destroy your database**. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.
What is SQL injection and how it works?

In SQL Injection, **the UNION operator is commonly used to attach a malicious SQL query to the original query intended to be run by the web application**. The result of the injected query will be joined with the result of the original query. This allows the attacker to obtain column values from other tables.