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

(*) 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 nw.

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. These network enables to make call to each other.

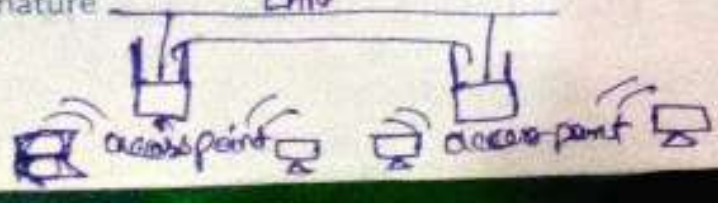
Wired nlw : In many organization wired nlw is an Ethernet LAN with an existing security infrastructure that includes an authentication Server (AS).

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 ~~station~~ wireless station or may be a station on the wired nlw that the AP is connected to.

→ Then AP serves as a bridge blw WAN and existing wired nlw.



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 issue

→ Denial of Service attack: When the intruder flood the nlw with msg affecting the availability of nlw resource. (Mtlb hackers attack karke ha our available resource use karke hain illegaly)

→ Spoofing & session hijacking: attackers gain access to nlw data & resources by assuming identity of valid user (kisi person ka id login password churna ka 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:

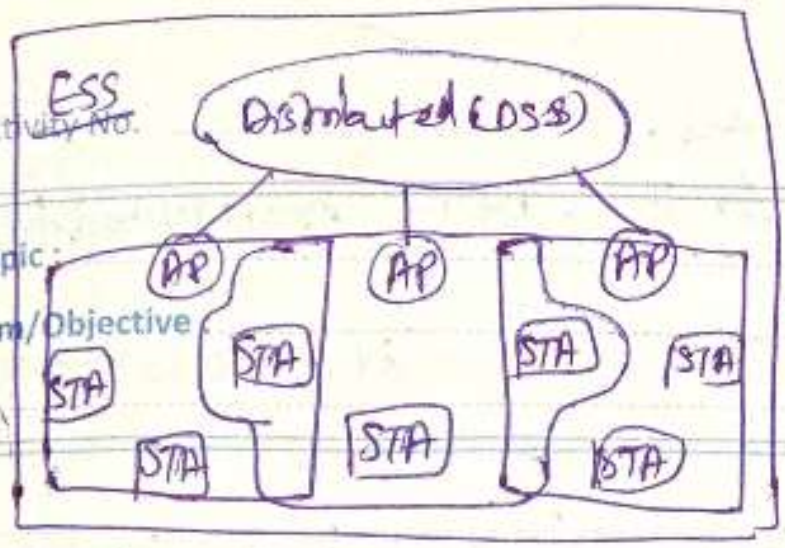
- (wireless Access point) WAP: WAP are generally wireless router that forms base stations or access.
- Client: Clients are workstations, PC, laptop, printer, cellphone

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.



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

Advantages of WLAN

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

Disadvantage of WLAN

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

→ 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 IEEE 801.11 frame format

WLAN Security features

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

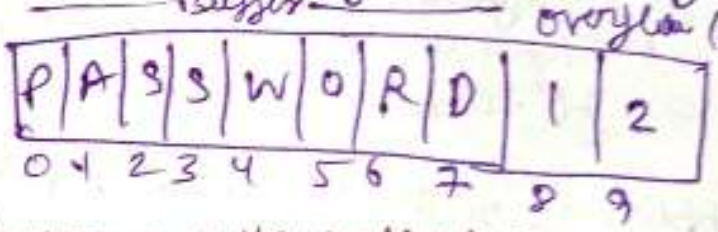
2) Media access point (MAC): Involves using address attach to each device to limit connection to access point.

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

Teacher's Signature

⊛ 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 attack:
→ 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

(*) Cross Site scripting (XSS)

Activity No. Date :

Topic

Aim/Objective :

→ It is an attack in which an attacker injects malacious 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 be then be parsed by victim's browser.

→ 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 views 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");
fstSQL: "Select *from User where
Userid = "+txtUserID;

⊛ Common SQL injections

→ Retrieving hiddendata: where we can modify SQL query to return addⁿ result.
→ Union attack: where we can retrieve data from diffⁿ DB tables.
→ examine the DB where we extract Infs abt version/structure of db.
→ Blind SQL injection: where the result of query use 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 fan a string format cause:-

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

⊛ Preventing format string attacks

1) It 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

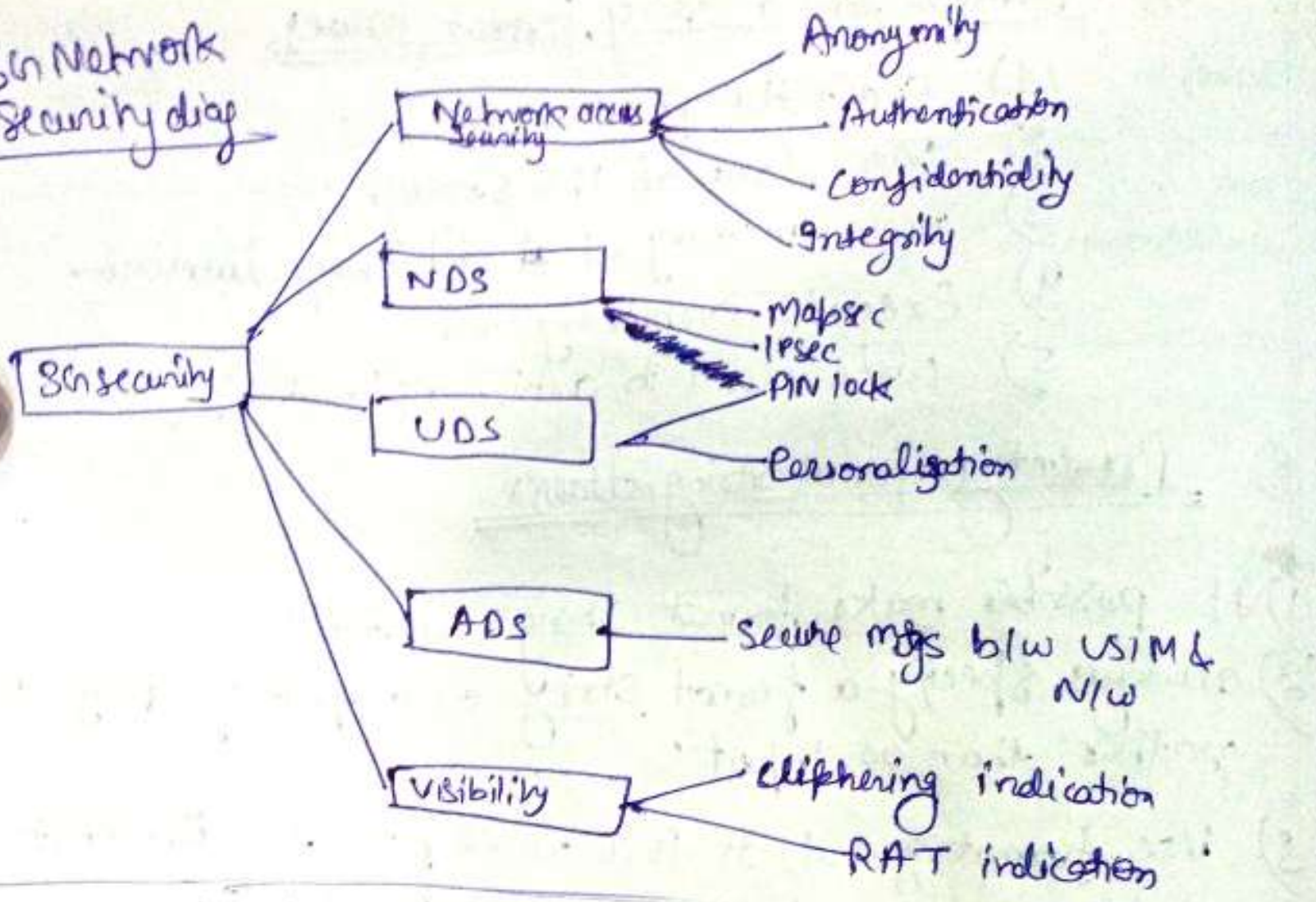
→ It is the 3g successor to the GSM family of measures counting GPRS and EDGE.
→ UMTS employments a completely diverse radio interface.
→ UMTS is designed to interoperate with GSM network
→ to protect GSM network against man-in-middle attacks.
→ UMTS security also referred as 3G security.
→ In UMTS authentication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

→ 5 security group exist in 3G network :

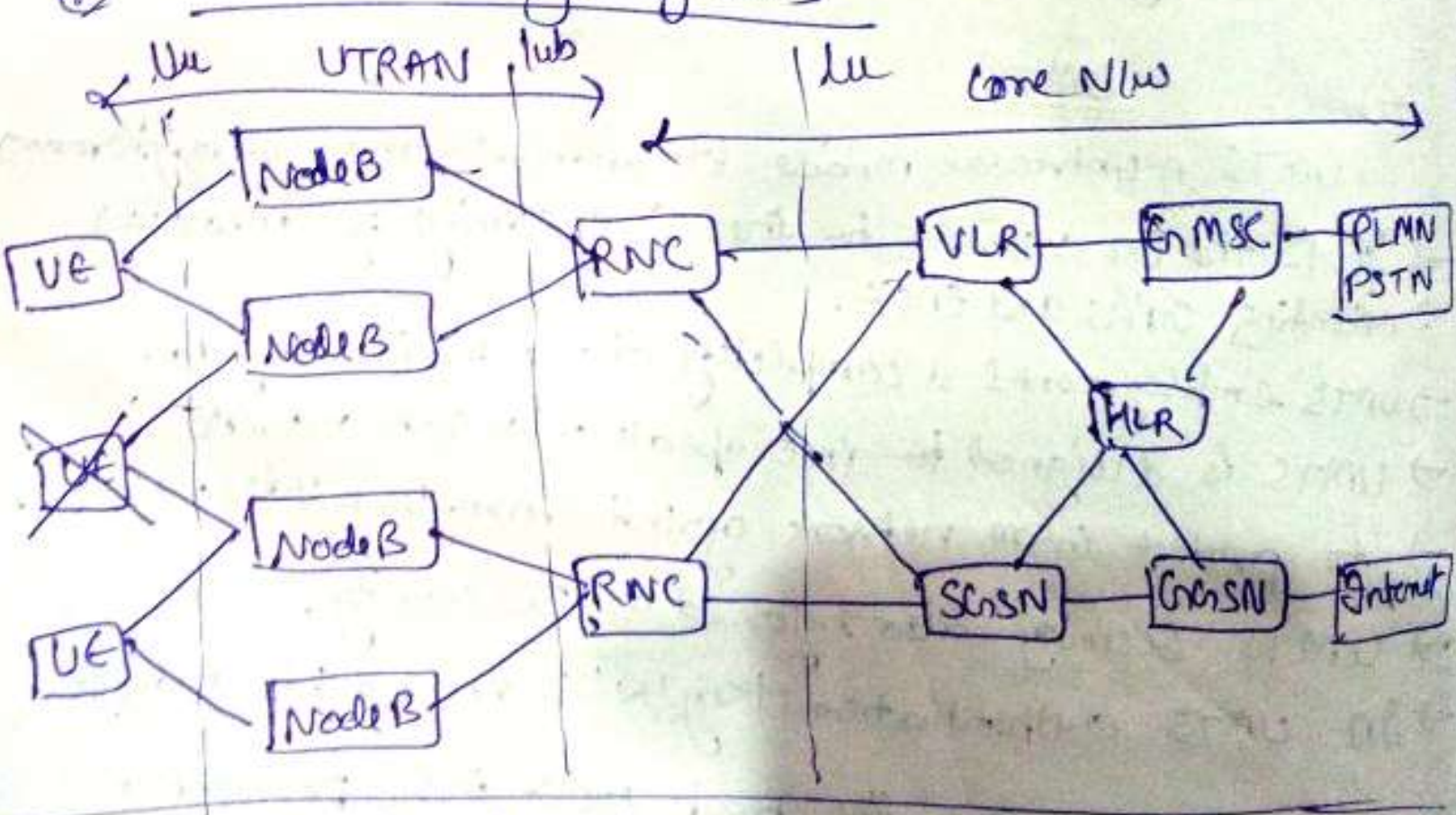
- Network access security
- Network domain security
- User domain Security
- Application domain "
- Visibility, configuration of security

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 provides & 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.

→ (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-overlapping 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

⊛ GSM Intro

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

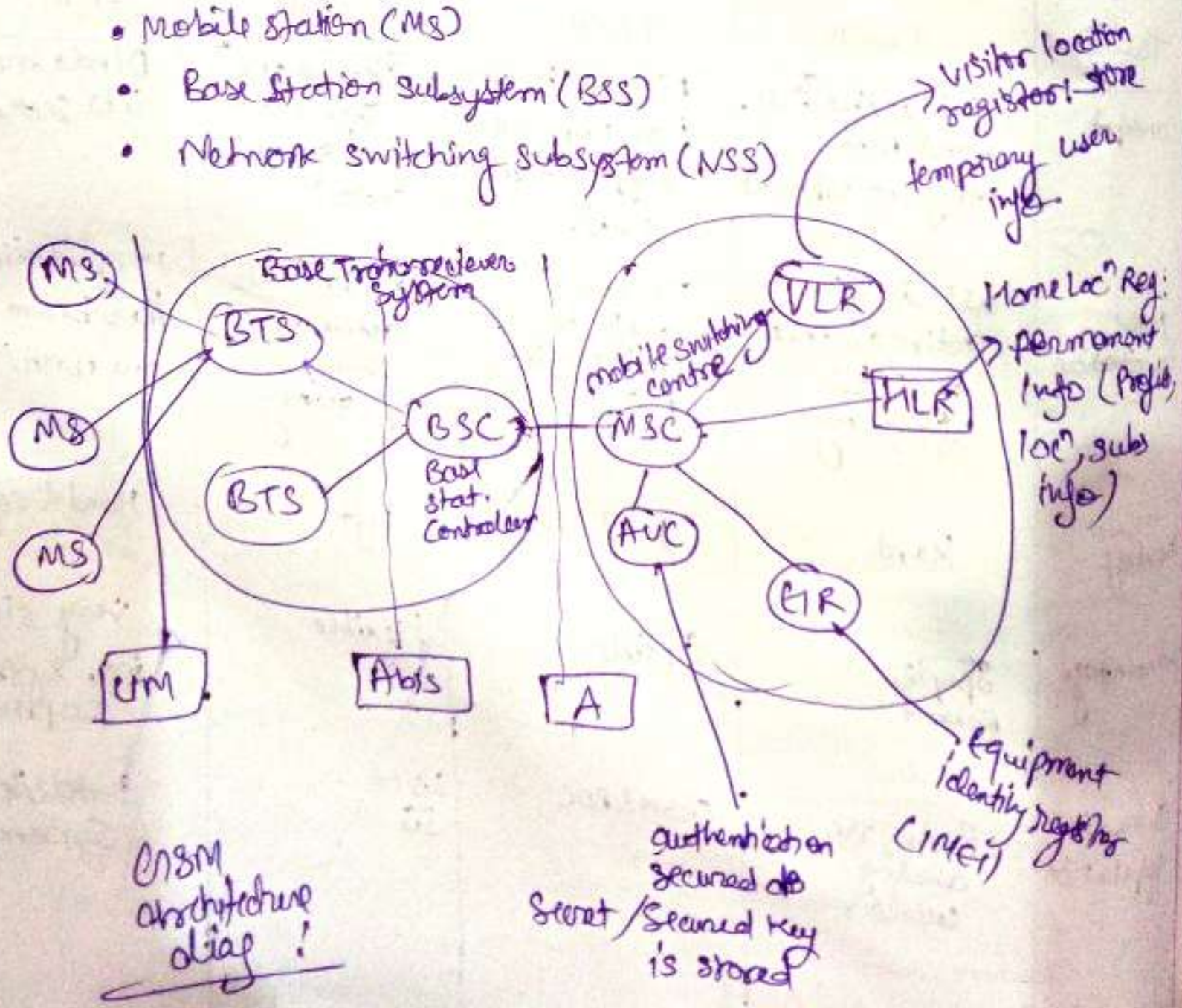
→ Based on digital technology

→ 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 compatibility

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