BAKI ALİ NEFT MƏKTƏBİ
BAKU HIGHER OIL SCHOOL

Mobile development and security

Session 13

Karim Karimov
Lecturer

3G Network

The third generation (3G) proposal for cellular communications aimed at providing global roaming for mobile users, high transmission bandwidths, and protection to sophisticated services such as the global positioning systems and multimedia on the demand of mobile users. In the mid-1980s, the International Telecommunications Union (ITU) challenged the communication community to produce a single and worldwide standard capable of offering high speed communication, better QoS support, and enhanced security compared to 2G cellular networks. Ten years later, the concept of International Mobile Telecommunications 2000 was established and a series of technical specifications has been approved under the identification **IMT-2000 (ITU, 1997)**. This specification was meant to be a unifying description that is able to attract various technologies covering many frequency bands, channel bandwidths, modulation formats, and network operators.

3G Network

The following is a (non-exhaustive) list presenting the major objectives related to the communication features that IMT-2000 intends to provide:

- To make it easy to offer mobile subscribers a wide range of services, **regardless of their location**; and to offer the best possible quality of service by providing a large radio coverage and transport higher bandwidth.
- To make larger the number of services that can be offered, **regardless of limiting constraints** such as radio transmission, spectrum efficiency, and system economics.
- To offer **high speed packet data rates** such as:
  - 2Mbps provided for fixed environments;
  - 384 Kbps for pedestrian;
  - 144 Kbps for vehicular traffic.

3G Network

- To **maintain user mobility** based on the registration of mobile terminals and the provision of the mobile subscribers with individual cards (such as the subscriber identity module cards used in GSM).
- To **enhance on the security** of the second generation systems, by addressing and correcting real and perceived weaknesses in GSM and other 2G networks.
- To permit and support **international operation and roaming** of mobile subscribers.

Retention of 2G Robust Features

Several security mechanisms have been shown to be robust and useful in 2G communication systems. 3GPP standards have to build on these mechanisms and retain their advantages. These mechanisms rely on four major issues:
(a) the SIM-based authentication;
(b) the confidentiality of user traffic on the air interface;
(c) the radio interface encryption; and
(d) the confidentiality of user identity on the radio interface.

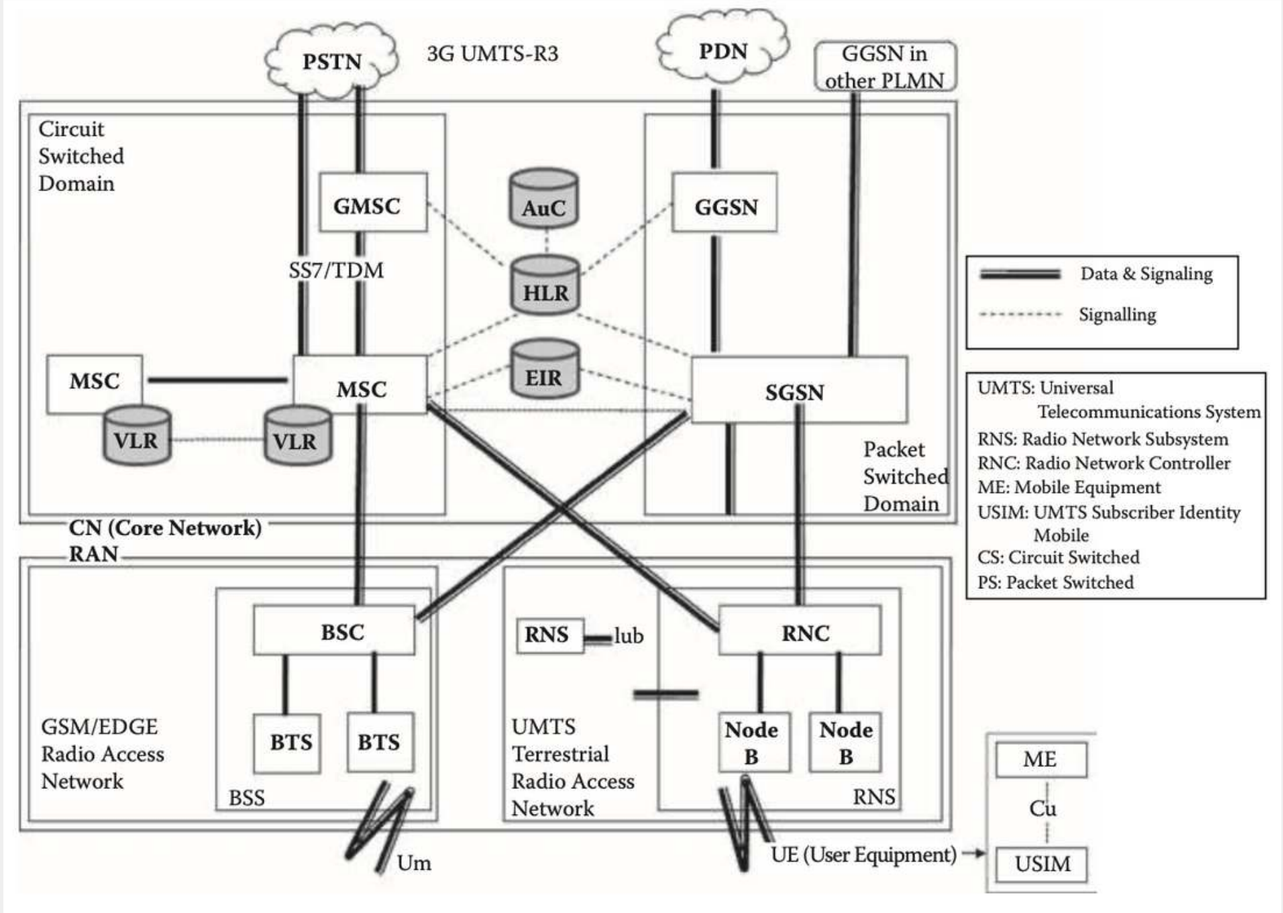
The 3G networks

Wireless network evolution can be characterized by an increase in functionality and its support for a growing number of services. However, this also means that the 3G networks are becoming increasingly complex in terms of architecture. 3G networks are likely to share the same major components within their communication architecture.

3G Network Architecture

UMTS network presents an implementation of 3G-mobile systems, which is compatible in some way with the Global System for Mobile communication and the General Packet Radio Services networks. The fundamental difference between GSM/GPRS and UMTS is that the latter supports higher access rates. This is achieved through a **Wideband Code Division Multiple Access** radio interface for the land-based communication system, named **UMTS Terrestrial Radio Access Network** (**UTRAN**). Recent versions introduce new concepts and advanced features including the shift to an all-IP network architecture and the integration of an open service architecture, which aims at allowing network operators to offer third party access to their UMTS service architecture.

3G Network Architecture



3G Network Architecture

A UMTS network is logically divided into two parts, which are referred to as **the Core Network (CN)** and **the Generic Radio Access Network (GRAN)**. The core network reutilizes several elements already present in GPRS and GSM networks (3GPP, 900). It consists of two overlapping domains: **the Circuit-Switched (CS) domain** and the **Packet-Switched (PS) domain**. The CS domain is made up of entities that **allocate dedicated resources to the user traffic**, control the signals when the connections are established, and release them when the sessions terminate. Often, voice calls are handled by the functions developed within the CS domain. The entities in the PS domain are responsible for **transporting the user data** in the form of autonomous packets, which are routed independently of each other. This attempts to overcome the limitations of 2G networks to transmit data efficiently. The user can set up a connection to and from external packet data networks and other wireless networks.

The Mobile Station (MS)

Similar to GSM, a MS is defined as a device allowing a user access to network services and the Universal Subscriber Identity Module (USIM). It is involved in any major UMTS procedures, call setup and management, handoff procedures, and mobility management. The USIM contains the functions and data needed to identify and authenticate users, as well as a copy of the user's service profile and the security elements needed for confidentiality and integrity services. UMTS mobile stations can operate using one of the three modes:

1. **The circuit switching mode of operation**, which allows the MS to be only attached to the CS domain and which can only operate services of the CS domain;
2. **The packet switching mode of operation**, which allows the MS to be only attached to the PS domain and which may only operate services of the PS domain, while not preventing CS-like services to be offered over the PS domain; and
3. **The PS/CS mode of operation**, where the MS is attached to the PS and CS domains and is capable of simultaneously operating PS services and CS services.

USIM vs SIM

The USIM is an application stored in a removable smart card, which interoperates with the mobile equipment to provide access to 3G services. Similar to the SIM card, USIM has the following features:

- it unambiguously **identifies** a unique mobile subscriber;
- it **stores** subscription related information;
- it **authenticates** itself to the network and vice-versa (mutual authentication);
- it provides **security functions**;
- and finally, it **stores information elements** such as the preferred language, international mobile subscriber identity (IMSI), and cipher key.

The Access Network (UTRAN)

The UTRAN manages all the functions related to the radio resources and air interface management. The UTRAN consists of two types of components, **the Node-Bs** and **the radio network controllers**, which play roughly equivalent roles to those performed in GSM by the base transceiver stations and the base station controller, respectively.

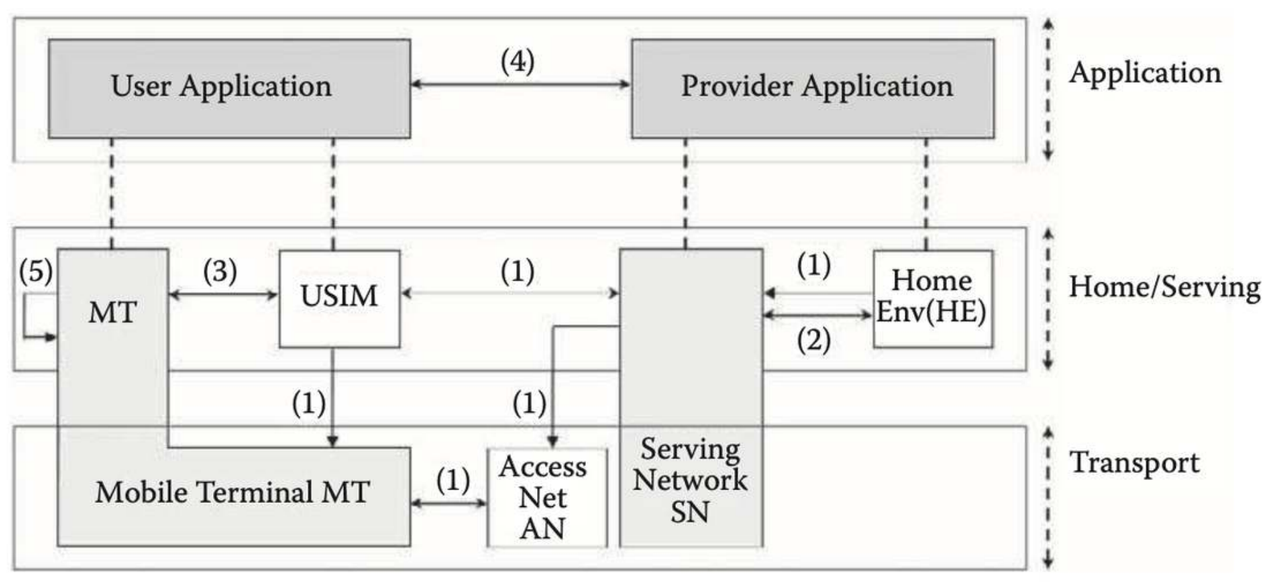
1. **Node B:** This is the physical unit for radio transmission/reception with mobile stations located within their radio cells. The base transceiver station of the UTRAN serves one or more radio cells. The main tasks of Node B are the air interface transmission/reception and CDMA physical channel coding.
2. **Radio Network Controller (RNC):** This component manages the radio resources of each of the Node Bs that are under its control. The RNC connects Node B to the transport network. It is responsible for handoff decisions that require signaling to the MS. The Node B resources are controlled from the RNC.

The Core Network (CN)

The CN is the structure responsible for transporting the user's data to its destination. It involves the use of a number of switching entities and gateways (such as the MSC, the Gateway MSC, the SGSN, and the GGSN) to the **external networks** (such as the Internet). It also maintains information regarding the user's access **authorizations** (involving the AuC and the EIR). Therefore, the CN also includes **databases** that store user profiles, and mobility management information (e.g., ***HLR*** and ***VLR***).

UMTS Security Architecture

The security generic architecture of UMTS networks is built on a set of security characteristics and protection mechanisms. **A security characteristic** is a service capability that complies with one or more security requirements. **A security mechanism** is a process that is used to carry out a security function. Figure below depicts the way security functions are organized together in five classes.



UMTS Security Architecture

- **Network access security (Class I):** The functions of this class provide secure access to 3G services and protect against attacks on the radio link.
- **Network domain security (Class II):** This class contains functions that allow the nodes in the operator’s network to securely exchange signaling messages, and protects against attacks on the wired network targeting UMTS.
- **User domain security (Class III):** This class of functions aims at securing the access of mobile stations to the UMTS network and services.
- **Application domain security (Class IV):** The functions belonging to this class aim at enabling applications implemented at the user domain and the provider domain to securely exchange messages.
- **Visibility and configurability of security (Class V):** This class of functions allows the user to get information about the security functions that are in operation for him. The class also allows the user to check whether the provision of a service depends on the activation of some security features.

Mitigating 2G Weaknesses

The 3G objectives have addressed the mitigation of the following weaknesses observed in the security of 2G networks:

- active attacks using a rogue BTS are launchable in 2G networks;
- the cipher keys and authentication data are transmitted in clear between and within networks;
- the encryption is only performed on the wireless link. This may result in the transmission of user and signaling data in a non-crypted form across micro-wave links (from the BTS to the BSC, in the case of GSM);
- the data integrity is not provided. Data integrity defeats certain rogue BTS attacks and provides protection against channel hijack;
- the IMEI is an unsecured identity;
- the 2G systems do not have the flexibility to upgrade and improve security functionality over time.

Denial of Service

DoS attacks launched using request spoofing have been made unfeasible for 3G networks by simply providing integrity and non-replay of signaling requests. Such attacks include the following:

- **User de-registration request spoofing:** This attack requires a modified MS and exploits the weakness that the 2G network cannot authenticate the messages it receives over the radio interface. The intruder may spoof a deregistration request (IMSI detach) to the 2G network. Then the network de-registers the user from the visited location area and instructs the HLR to do the same.
- **Location update request spoofing:** An attack that requires a modified MS and exploits the weakness that the 2G network cannot authenticate the messages it receives over the radio interface. The user spoofs a location update request in a different location area from the one in which the user is roaming. The network registers in the new location area and the target user will be paged in that new area. The user is subsequently unreachable (where he is actually) for mobile terminated services.

Identity Catching

Several attacks can be launched against the user identity confidentiality in 2G networks. The following attacks have been counteracted in 3G networks:

- **Passive identity catching:** This is a passive attack that requires a modified MS and exploits the weakness that the GSM network may sometimes request the user to send his identity in a clear form. In 3G use of temporary identities allocated by the serving network makes passive eavesdropping inefficient since the user must wait for a new registration or a mismatch in the serving network database before he can capture the user's permanent identity in plaintext.
- **Active identity catching:** This is an attack that requires a modified BS and exploits the weakness that the 2G network may request the MS to send its permanent user identity in a clear form. An intruder attracts the target user to camp on his false BS and consequently requests the target user to send his permanent identity in cleartext (by forcing a new registration or claiming a temporary identity mismatch due to database failure). The identity confidentiality mechanism provided in UMTS networks counteracts this attack by using an encryption key shared by a group of users to protect the user identity.

Impersonation of the Network Attacks

These attacks aim at impersonating a legitimate network. The ultimate objective of the attacks is to eavesdrop on user data or send to a user information that is subsequently thought to be initiated from an authentic network or a mobile user. Three attacks can be distinguished.

- **Impersonation of the network by suppressing encryption between the target user and the intruder:** The 3G network provides a mandatory cipher mode command with message authentication and replay inhibition to allow the mobile to verify that the encryption has not been hidden by an attacker.
- **Impersonation of the network by suppressing encryption between the target user and the legitimate network:** To protect against these attacks, 3G networks set up a mobile station class-mark with message authentication and replay inhibition to allow the network to verify that the encryption has not been suppressed by an attacker.
- **Impersonation of the network by forcing the use of a compromised cipher key:** The 3G networks are still vulnerable to attacks using compromised authentication vectors that have been intercepted between generation in the authentication center and their use.

Eavesdropping on User Data

These attacks aim at eavesdropping on user data that is transmitted through the legitimate network to the intended recipient. Three different attacks can be launched in the GSM network.

- ***Eavesdropping on user data by suppressing encryption between the target user and the intruder*:** A mandatory cipher mode command with message authentication and replay inhibition allows the mobile to verify, in the 3G networks, that the encryption has not been suppressed by an attacker.
- ***Eavesdropping on user data by suppression of encryption between the target user and the legitimate 2G network*:** Message authentication and replay inhibition of the mobile's encryption capabilities allows the 3G network to verify that the encryption has not been suppressed by an attacker.
- ***Eavesdropping on the user data by forcing the use of a compromised cipher key*:** similar to the preceding attack, the architecture does not protect against force use of compromised authentication vectors, which have not yet been used to authenticate the USIM.

Classification of Attacks on 3G Networks

A classification of attacks on the 3G network can be approached using three dimensions. They are
(a) the attack categories;
(b) the attack means; and
(c) the physical access dimension,
where attacks are classified based on the level of physical access the attacker has to the 3G wireless telecommunication network.

Classification by their type

1. ***Interception*:** The attacker intercepts information or reads signaling messages on a cable, but does not modify or delete them. Such attacks affect the privacy of the subscriber and the network operator. The attacker may use the data obtained from interception to analyze traffic. The attacker may use the data obtained from interception to analyze traffic.
2. ***Fabrication/Replay*:** In this case the attacker may insert spurious objects into the system. These objects depend on the target means and physical access type. The attacker may insert false signaling messages, fake service logic, or fake subscriber data into the communication system. The effects could result in the attacker masquerading as an authority, for example.
3. ***Modification of Resources*:** The attacker causes damage by modifying system resources, meaning that he may modify signaling messages in and out of the cable. He may modify the service logic or modify the subscriber data in the entity.

Classification by their type

4. ***Denial of Service*:** The attacker causes an overload or a disruption in the resources or applications connected to the 3G system, forcing the network to operate in an abnormal manner. The abnormal behavior may include a legitimate subscriber not receiving service, an illegitimate subscriber receiving service, or the entire network to be disabled.
5. ***Interruption*:** The attacker can cause an interruption of operation by destroying resources. He may delete signaling messages from and to the cable. He may delete a subscriber data in an entity, such as an HLR, and he may stop the delivery of a service to a mobile user.

Classification by their mean

1. ***Data-based attacks*:** The attacker targets the data stored in the 3G communication system. The damage can be caused by modifying, inserting, and/or dropping the data stored in the system.
2. ***Messages-based attacks*:** The attacker launches attacks against the 3G communication system targeting the signaling messages. The attacker may insert, modify, replay, and drop the signaling messages flowing to and from the network.
3. ***Service Logic attacks*:** The attacker causes important damages by simply attacking the service logic running in the various 3G network entities. An example of damage would be a complete deletion of logic running on the MSC.

Classification by their physical access

1. **Physical Access attacks I (the attacker obtains access to the air interface using a physical device):** Typically, the attacker has access to an inexpensive off-the-shelf equipment that he uses to impersonate some parts of the network. He may build a part of a rogue base station. Victims camping on the rigue base station are subject to various attacks. Attackers may also use modified mobile stations to broadcast at a high frequency, eavesdrop, and execute man-in-the-middle attacks.
2. **Physical Access attacks II (the attacker obtains access to the cables connecting the 3G network switches):** Typically, only the authorized personnel can access the 3G switches; but, if an attacker has access to cables connecting these switches, they may cause considerable damage by disrupting the normal transmission of signaling messages.

Classification by their physical access

3. *Physical Access attacks* III (the attacker has access to some sensitive components of the 3G network): In this case, the attacker may be a displeased employee who has managed to obtain access to the 3G node switch. The attacker can cause important impairments by editing the service logic or modifying the subscriber data (related to the user's profile, security, and services) stored in the 3G network entity.

4. *Physical Access attacks* IV (the attacker has access to some links connecting the Internet to the 3G network): This is a cross infrastructure cyber attack, where the attacker can cause a certain harm by disrupting the transmission of signaling messages flowing between the link and inserting some signaling messages into the link between the two networks.

5. *Physical Access attacks* V (the attacker has access to Internet servers or cross network servers providing services to mobile subscribers connected to the 3G network): This is a cross infrastructure cyber attack, where the attacker can cause harmful damage by editing the service logic or modifying subscriber data (profile, security, and services) stored in the cross network servers.

End of the session