BAKI ALİ NEFT MƏKTƏBİ
BAKU HIGHER OIL SCHOOL

Mobile development and security

Session 12

Karim Karimov
Lecturer

GSM

The **Global System for Mobile Telecommunication** (**GSM**) has become one of the most popular systems for mobile communication. GSM provides terminal mobility and allows users to roam seamlessly from one GSM network to another. It is characterized by a special feature, the separation of the user identity from the terminal phone equipment. In fact, the subscriber identity is inserted in a **Subscriber Identity Module** (**SIM**) that can be added to any GSM mobile terminal. The SIM carries sensitive data that are utilized to authenticate the subscriber and provide confidentiality of the exchanged messages.

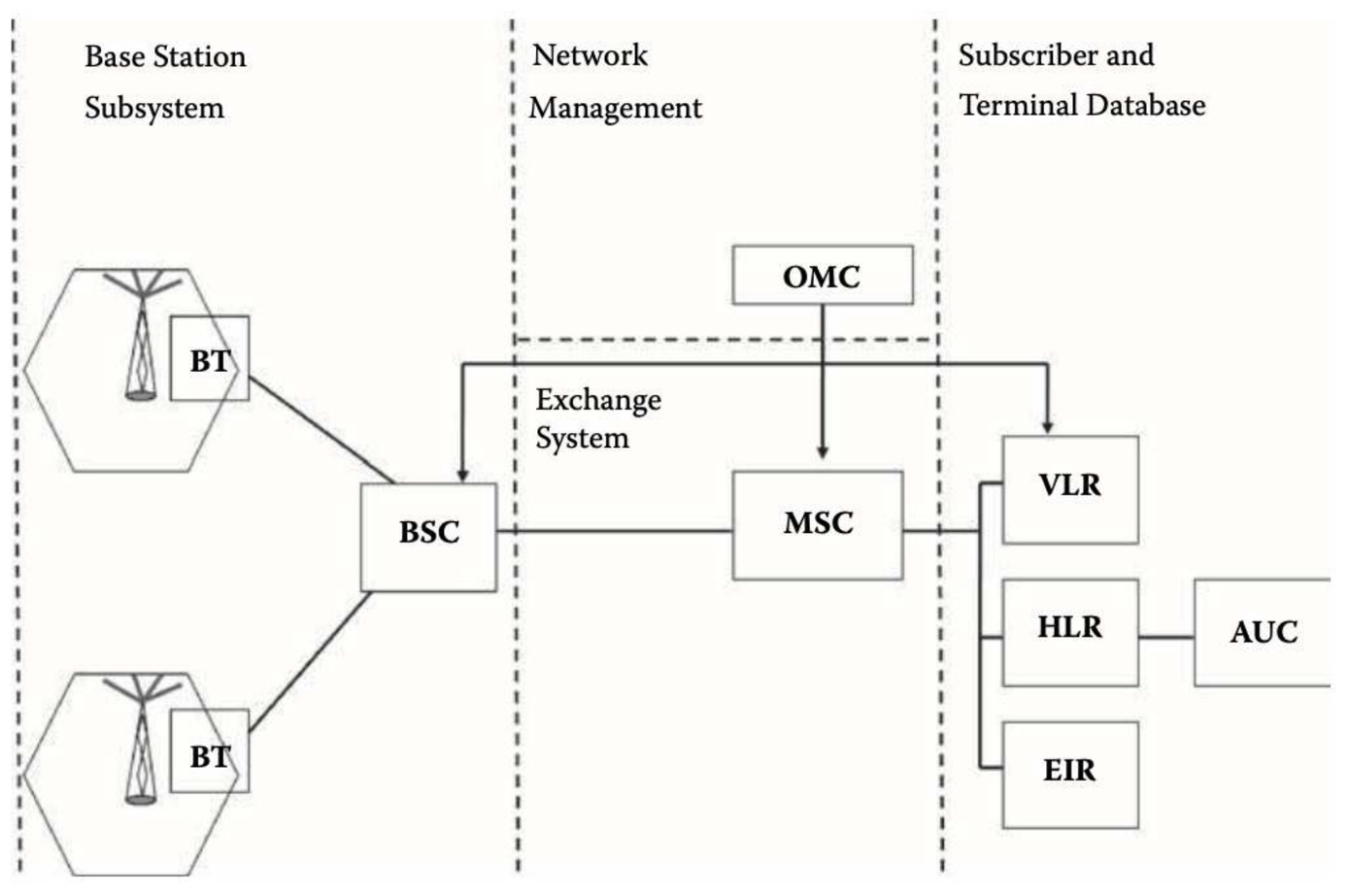
GSM

Security in GSM is an important issue because the mobile users are likely to transmit sensitive data over a network infrastructure that is not truly secure. The security weaknesses of GSM system from some trust-related hypotheses made by the developers, including the lack of node authentication and some design flaws in the security protocols. The most important threat for the GSM is, however, linked to the fact that the subscriber may believe that the entire structure is secure and may erroneously trust it to exchange confidential information. Nonetheless, since all wireless networks suffer from multiple exposures posed by the wireless environment, the security and confidentiality in GSM were some of the reasons for which this standard was considered superior to other mobile communication systems.

GSM

However, some security problems have occurred with the GSM operation. These problems include, but are not limited to, the following:
(a) **security is obscure**, meaning that none of the security algorithms used by GSM is available to the public;
(b) **the GSM provides only access security**, which means that all communications between the user's mobile terminal and the base transceiver are encrypted. However, all communications and signaling messages are generally transmitted in clear text in the GSM network;
(c) the cryptographic mechanisms are **difficult to upgrade**; and
(d) the mobile subscriber **visibility is missing**.

GSM Infrastructure



GSM Infrastructure

A GSM network involves nine major components: the **Mobile Station (MS)**, the **Subscriber Identity Module (SIM)**, the **Base Station Subsystem (BSS)**, the **Base Station Controller (BSC)**, the **Transcoding Rate and Adaptation Unit (TRAU)**, the **Mobile Services Switching Center (MSC)**, the **Home Location Register (HLR)**, the **Visitor Location Register (VLR)**, and the **Equipment Identity Register (EIR)**. Together, all these components constitute a **Public Land Mobile Network (PLMN)**.

The Mobile Station (MS)

The MS is carried by the subscriber. It is constituted by the mobile equipment (ME) and a smart card referred to as the Subscriber Identity Module (SIM). The typical ME is the mobile phone. Inserted into the ME, the SIM card allows the subscriber to receive calls at the ME and make calls from that ME. The SIM stores sensitive data that are protected by the subscriber’s personal identity number (PIN).

Subscriber Identity Module (SIM)

Particularly, the SIM card contains the following subscriber related information:

- **The International Mobile Subscriber Identity (IMSI)**: This number uniquely identifies a subscriber. Its provision is necessary to access the GSM services. IMSI is used by the network for purposes including universal identification and roaming.
- **The cryptographic algorithms A3 and A8 and a secret subscriber authentication key Ku**: They provide security functions for authenticating the mobile user via his SIM card, and generating the session keys for confidentiality needs, respectively.
- **The temporary network related data**: The temporary data mainly include the Temporary Mobile Subscriber Identity (TMSI), which is an identifier assigned to the subscriber for a limited interval of time, the Location Area Identifier (LAI), and the forbidden Public Land Mobile Networks (PLMN).
- **The Card Holder Verification Information (CHVI)**: The information authenticates the user to the card and provides protection against the use of stolen cards.

The Base Station Subsystem (BSS)

The BSS controls the radio related tasks and provides connectivity between the network and the mobile stations via the radio interface. It consists of the **Base Transceiver Station** (**BTS**) and the **Base Station Controller** (**BSC**). The BTS sets up the radio transceivers that handle the radio link with the MS and covers a radio cell identified by the BTS. The BSC manages the radio communication and takes care of all the needed control functions. It also controls a set of BTSs.

Mobile Services Switching Center (MSC)

The MSC is the main component of the GSM network management system. It controls a large number of BSCs and acts like a switching node. It also provides all the management functions for terminal mobility including ***registration***, ***authentication***, ***location***, ***handover***, and ***call routing***. Similar to a digital telephone exchange, a router, or a switch, it is responsible for the routing of incoming and outgoing calls. In addition, it handles the assignment of user channels on the air-interface.

The Operation and Support System (OMC)

The OMC is connected to all equipments in the switching system and to the BSC, as well. The purpose of the OMC is to offer the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network. It also provides a network overview and supports the operational maintenance activities.

Home Location Register (HLR)

The HLR is a database that stores and manages the mobile subscriber specific parameters (or administrative information) of a large number of registered subscribers along with their current location. The parameter values stored for a subscriber are permanent. The most important parameter of a subscriber stored in the HLR is the shared authentication key **Ku** and the **IMSI**. Every user is assigned to a unique HLR. A unique HLR is usually assigned to a PLMN. The HLR plays an important role in various tasks such as the roaming of mobiles to foreign networks.

Visitor Location Register (VLR)

The VLR component is a database designed to off-load the HLR of user database related functions. Like the HLR, the VLR contains subscriber information, with the difference that it relates only to the subscribers who roam in the area assigned to the VLR. When a subscriber roams away from his/her own network, information is forwarded from the subscriber's HLR to the VLR of the serving network, in order to perform the authentication process. Typically, when a subscriber moves out of a VLR area, the HLR takes care of the relocation of the subscriber information from the old to the new VLR. Notice that a VLR may be associated with several MSCs; but, a MSC is always assigned to only one VLR.

Authentication Center (AuC)

The AuC contains a database that is used to store the identification and authentication information related to each subscriber. Typically, the AuC is an important part of the HLR. The attributes in this database include the subscriber's **IMSI**, **secret key K**, **LAI**, and **TMSI**. The AuC is responsible for generating triplets of values consisting of a random field, called **RAND**, an **assigned response** (denoted by and SRES), and **session key K**, which are stored in the HLR for each subscriber and a call made by the subscriber.

Equipment Identity Register (EIR)

Since the subscriber identity and the mobile equipment (ME) are processed independently by the GSM system, it is possible to operate any GSM ME with any valid SIM card. This makes cellular terminal theft an attractive task for hackers. To protect against thefts, the **Equipment Identity Register** (**EIR**) was introduced in the GSM system. Every GSM terminal has an internationally unique identifier, called the International **Mobile Station Equipment Identity (IMEI)**, which cannot be altered without destroying the terminal. IMEI contains a serial number and a type identifier. The EIR is a repository that maintains three lists: ***the white list***, ***black list***, and ***grey list***. The white list contains all number series of equipment identities that are permitted for communication. The Black list contains all equipment identities that need to be disqualified. Mobile equipments appearing in the grey list are not disqualified (unless they are on the black list or out of the white list), but are tracked by the network for specific purposes.

Security Requirements

GSM, like many other cellular networks that serve a large number of users, contains many valuable assets that may constitute serious vulnerability sources and need protection against misuse and malicious attacks. Two classes of requirements are valuable for GSM: the requirements for **mobile user's privacy** and the requirements for **data integrity protection**. A subscriber to a GSM network necessitates protection in the following activities: ***call setup***, ***voice-based services protection***, ***privacy of location***, ***privacy of calling patterns***, ***privacy of user identity***, and ***protection of data***.

Protection of Call-Setup Information and Communication Services

During the call-setup process, the mobile terminal transmits important call-setup information to the GSM network. This information contains the ***calling party number***, the ***calling card number***, and the ***service type requested***. This information must be protected and secured against eavesdroppers. In addition, all communication services (including spoken communication) must be properly encrypted by the cryptographic system, when requested, so that it cannot be intercepted by any malicious user listening to the radio interface or other interfaces of the system.

Privacy of User-Location, Calling Patterns, and User-Data

Any out-leaking of signaling information on the GSM network may enable a hacker to approximately locate the position of a subscriber and reduce the subscriber's privacy. Information related to traffic generated by a particular user and his/her calling patterns (such as the caller-id) should not be made available to attackers. Therefore, measures should be taken to protect the mobile subscriber from attacks against his/her privacy of location, to keep calling patterns inaccessible to eaves-droppers, and to protect subscriber identification information against hackers. In addition to securing the transmitted data, there must be a provision in the network and the terminal to check whether the data it receives has been altered. This property is traditionally called **Data Integrity**.

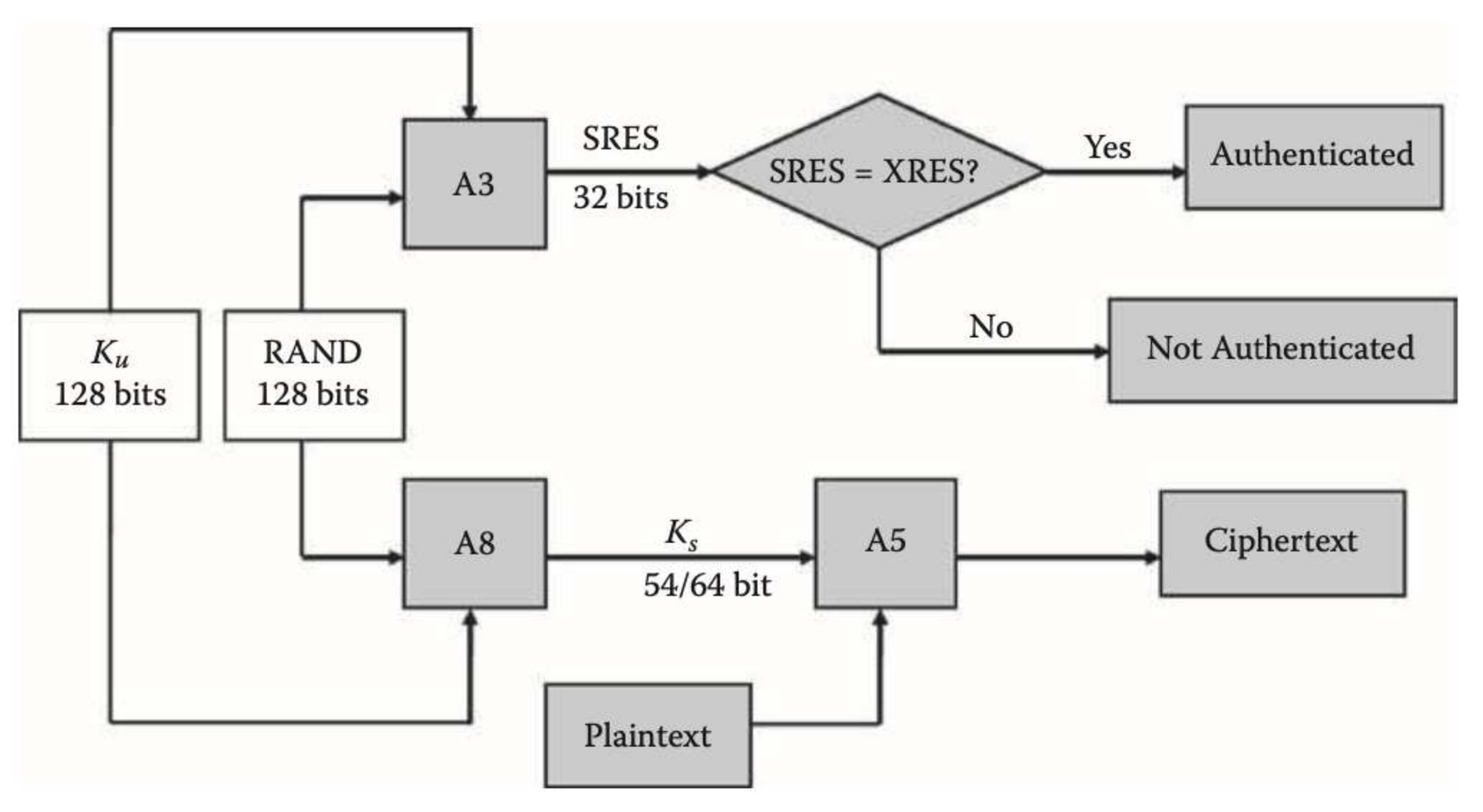
Replication and Clone Resistant Design

Replication is a damaging attack in GSM communication systems. Cloning refers to the ability of an intruder to determine information about a personal mobile terminal and duplicate it, meaning that the intruder creates a duplicate copy of it using the collected information. This kind of fraud can be easily accomplished by legitimate network users, since they have all the information they need to clone their own personal information stored in the SIM in the terminal. Doing so, ***multiple users can use one account*** by cloning personal equipment. It also could be done by an external user who desires to get benefit of services on the expense of legitimate users. The cryptographic protection for the GSM network must include some tools for clone-resistance. Security must be provided for the radio-interface, the network databases, and the network interconnections so that personal equipment information can be kept secure.

Equipment Identifiers

In GSM systems, where the account information is logically and physically separated from the terminal, stealing personal equipments could be an attractive and lucrative business for attackers. To avoid such a threat, personal equipments must have unique (worldwide) identification information that reduces the potential of stolen equipment to be re-used. The identifiers may take the form of tamper-resistant values that are permanently integrated into the mobile terminals.

GSM Security Model



GSM Security Model

Authentication and confidentiality are achieved by giving the mobile user and the network a **shared secret**, which is a **128-bit value Ku**, stored in the SIM card. This key is not directly accessible to the user. Each time the user connects to the network, the network authenticates the user by sending a random number **RANDG** to the MS. The SIM card then uses the random number and the secret key to run an authentication algorithm, provide a value **SRES**, and create a session key **Ks**. The user is authenticated if the provided **SRES** matches the value of **SRES that is computed separately by the GSM network** using the same parameters and algorithms. The encryption is performed using key **Ks**. The mechanisms used in GSM networks to provide anonymity, authentication, and confidentiality to the mobile users are detailed in the following. The security model aims at providing a solution that satisfies, to a certain extent, the aforementioned security requirements. Security services provided by GSM include anonymity, user authentication, and confidentiality. Unfortunately, this model does not provide any security features such as network authentication.

Anonymity

Limited anonymity is provided in GSM by the use of **temporary identifiers**. When a mobile user powers on his/her mobile terminal, the real identity (IMSI) is used to identify the MS to the network and then a temporary identifier **Temporary Mobile Subscriber Identity** (**TMSI**) is allocated as a temporary local identifier of the MS to the network in future sessions. The TMSI has significance only within a given location area. According to the ETSI specification, the network always encrypts TMSI before sending it to the MS.

Authentication

Since any malicious user is able to overhear a communication on the radio medium, authentication, which aims to prove that users are who they claim to be, is an essential element of a mobile network. Authentication involves two functional components, the **SIM card** in the mobile and the **Authentication Center (AuC)**. One of the most important security functions of the SIM is to authenticate the subscriber to the network. This process guarantees that the MS requesting service is a legitimate subscriber and not an intruder or a cloned user. The GSM network verifies the identity of the subscriber through a **challenge-response** process. When a MS requests a service, the network randomly generates the real number **RAND** and challenges the MS by sending it RAND. The MS should answer correctly the challenge before being granted access by sending back the expected value of **SRES**.

Confidentiality

In addition to the information needed for the authentication of subscribers, the SIM card also provides the information needed to encrypt the radio connection between the MS and the covering BTS. More specifically, an algorithm called **A8** is used to generate a session key **Ks** with each accepted connection. Key **Ks** is utilized for voice and data encryption before transmission on the radio link. The algorithm used for computing the 64-bit Ks is invoked.
On the other hand, since the GSM network uses the **time division technique** to share the radio channel with **up to eight other users**, each user takes its turn using the common radio channel, sending and receiving information only during one of the eight available time slots in every frame. A GSM conversation uses two frames, one going from the base station to the MS (i.e., on the **downlink**) and the other going from the MS back to the base station (**uplink**). Each of these frames contains 114 bits of user information, which is often digitized and compressed speech. Therefore, every 4.615 milliseconds the MS receives 114 bits of information from the base station and transmits another 114 bits to the base station. These 228 bits require encryption to protect it from hackers.

Confidentiality

Using **RAND** and secret key **Ku**, the SIM runs the **A8** algorithm to produce the 64-bit long session key called **Ks**. Ks is transferred out of the SIM and into the MS, where it is used by a third algorithm called **A5**. Algorithm **A5** uses **Ks** and the current publicly known frame number to produce a key stream of 228 bits, decomposed into two halves. While the first half encrypts the downlink frame (dl), the second half is used to encrypt the uplink frame (ul). For each new frame to be transferred, a new 228-bit key stream is produced by the algorithm **A5** to encrypt (and decrypt) the frame. The algorithm **A5** lives in the hardware part of the terminal, and never in the SIM card. It has to operate quickly and continuously to generate a fresh set of 228 bits every 4.615 milli-seconds.

Basic attacks on GSM

GSM Security Flaws

- **No authentication of the network is provided to the user:** The authentication procedure described in the previous sections does not require the network to prove its knowledge of the user key **Ku**. Thus, it is possible for an attacker to set up a false base station (or RBS, for rogue BS) with the same mobile network code as the subscriber's network.
- **Common implementation of A3/A8 is flawed:** The most common implementations of the **A3** and **A8** algorithms use the procedure **COMP128**, which generates the 64-bit **Ks** and the 32-bit **SRES** from the 128-bit **RAND** and the **Ku** input. This algorithm is seriously flawed, in the sense that some chosen values for the input RAND will provide enough information to determine the key **Ku** in significantly less than the large number of attempts required by a brute force (of the order of 2^128).

Basic attacks on GSM

GSM Security Flaws

- **Vulnerabilities in the subscriber identity confidentiality mechanism:** GSM system has provided the **TMSI** instead of using **IMSI** in communication and maintains a database in the **VLR** mapping TMSIs to IMSIs. If the network somehow loses track of a particular **TMSI**, it **must ask the subscriber to submit its IMSI** over the radio link, using a special mechanism for identity request. Thus, the **IMSI** is sent in **plaintext**. Combined with the aforementioned flaw (stating that the network does not authenticate itself to a user), an attacker can use this **to map a TMSI to its IMSI**.
- **Over the air cracking of *Ku*:** Combined together, the aforementioned flaws can result in a serious attack.
    - The attacker can **imitate** a valid base station
    - the attacker gets the MS's **IMSI** by sending to the MS an identity request
    - The attacker collects the (**RAND**, **SRES**) pairs until he gains enough information to derive the key **Ku**.

Impersonation Attacks

In impersonation attacks, the attacker is willing to impersonate the network with respect to the MS, impersonating the MS with respect to the network, or combining both operations to perform a **man-in-the-middle attack**. A malicious adversary impersonating one of the two entities is able to perform a large spectrum of illegitimate actions, including
(a) listening to private traffic;
(b) modifying, deleting, re-ordering, or replaying messages; and
(c) spoofing and behaving as a repeater relaying signaling and user data between the two communicating parties.
The required equipments to achieve a man-in-the-middle attack are made of a **modified BTS** in conjunction with a **modified MS**. The modified BTS impersonates the network to the MS, while the modified MS impersonates the MS to the network. The term **rogue base station** (**RBTS**) will be used to refer to the modified, while BTS will mainly refer to a legitimate base station.

Attacks on the Authentication Algorithm

The difficulty in starting using an algorithm different than **COMP128** remains in the fact that the algorithm **resides inside the SIM**, meaning that the subscribers having active subscriptions (or SIM cards) algorithm are forced to keep using their SIM cards with the old algorithm on the introduction of a different algorithm even though it is stronger. It is, however, possible to include better secure versions of the procedure COMP128 in the new SIM cards that are handed to new subscribers. This unfortunately poses a **crucial problem for the efficiency** of the authentication process.

Another fact adds serious consideration: despite the decision of keeping the design of the procedure **COMP128 non-available to public**, one can find that it has been reverse engineered and crypt-analyzed. In fact, since the GSM specification for SIM cards is widely available, all that is needed to clone a SIM card is the **128-bit COMP128 secret key** and the **IMSI**, which is embedded in the SIM card.

End of the session