GSM Security

What is GSM?

- Global System for Mobile Communications
  - originally Groupe Spécial Mobile
- Standard for 2G digital celleur networks.
- Developed by European Telecommunications Standards Institute (ETSI) in the late 1980's.
- First GSM call was made in 1991
- As of 2014, it has 90% market share

GSM Infrastructure [1]

- Mobile Station (MS)
  - Consists of mobile equipment (ME) (e.g: phone) and a Subscriber Identity Module (SIM) smart card, which contains:
    - International Mobile Subscriber Identity (IMSI): Unique identification for a subscriber.
    - Cryptographic algorithms A3 and A8 and a secret subscriber authentication key K_i.
    - Temporary network-related data. May include for example Temporary Mobile Subscriber Identity (TMSI) which is an identifer associated with a subscriber temporarily.
    - Card Holder Verification Information (CHVI) - authenticates the user to the card; protects against theft of the card.

GSM Infrastructure [1]

- Base Station Subsystem
  - Consists of Base Transceiver Station (BTS) and Base Station Controller
    - BTS: handles radio transceivers and radio communication with the MS. Covers its associated cell.
    - BSC: manages control functions; controls a set of BTSs.
- Mobile Services Switching Center (MSC)
  - Main component of GSM network.
  - Controls large number of BSCs.
  - Takes care of the routing of incoming and outgoing calls.
  - Handles management functions such as authentication, registration, location, handover and call routing.

GSM Infrastructure [1]

- Operation and Maintenance System (OMC)
  - Connected to all entities in the switching system and to the BSC.
  - Some of its functions include [2]:
    - Administration and operations such as subscription, charging and statistics.
    - Security Management.
    - Network configuration and performance management.
    - Maintenance tasks.
- Home Location Register (HLR)
  - Database that stores information on mobile subscribers including
    - subscriber's IMSI
    - subscriber's location
    - authentication data
  - A subscriber is assigned to a unique HLR.
  - Plays an important role in roaming to foreign networks.

GSM Infrastructure [1]

- Visitor Location Register (VLR)
  - Contains subscriber information like the HLR.
  - Information is stored only for subscribers who roam in the area associated with the VLR.
  - When a subscriber roams to another network, information is forwarded from the subscriber's HLR to the new network's VLR.
    - One reason this is done is so that authentication can be performed.
  - When a subscriber roams away from an area associated with a VLR, the HLR manages the relocation of the information from the old to the new VLR.
  - An MSC is assigned to only one VLR but a VLR may be associated with multiple MSCs.

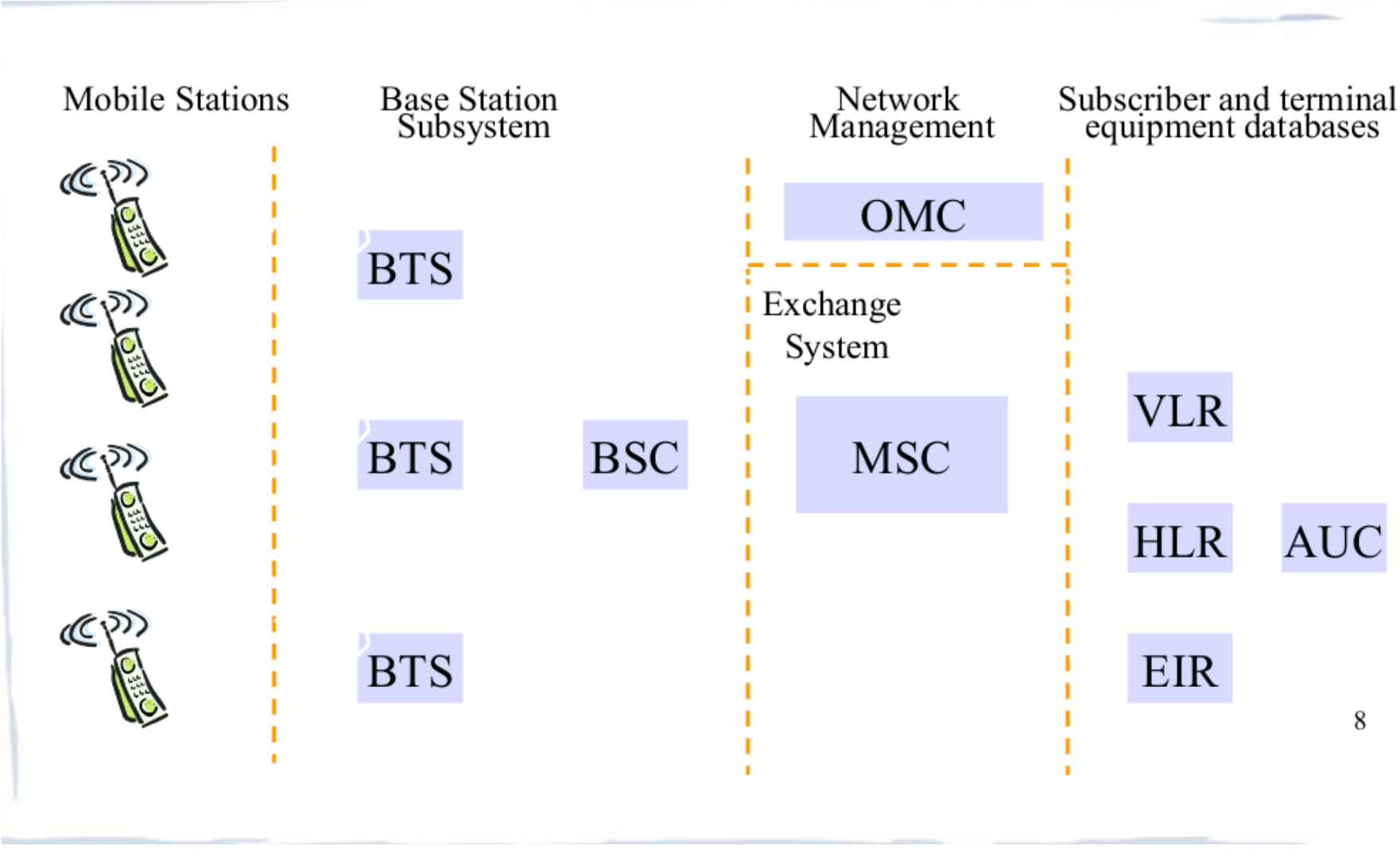
GSM Infrastructure

- Authentication Center (AuC)
  - Authenticates a SIM card that attempts to connect to the GSM network.
    - if authentication is successful, the HLR can manage the SIM.
  - Generates an encryption key for encryption of commmunication between phone and GSM network.
  - The SIM and AuC share a key K_i.
    - never transmitted
    - used in challenge/response protocol for authentication.

GSM Infrastructure

- Equipment Identity Register (EIR)
  - Used to detect whether mobile equipment is valid.
    - Mobile phone is identified by an International Mobile Equipment Identifier (IMEI)
    - An IMEI is independent of the SIM.
  - The EIR has three lists which are used to check status of IMEI [3]:
    - White List: valid mobiles
    - Black List: stolen or non-type mobiles
    - Gray List: local tracking mobiles

GSM Infrastructure



Source: [3].

GSM Security Features [3]

- Key management is independent of equipment
- Subscriber identity protection
- Detection of compromosed equipment
- Subscriber authentication
- Signaling and user data protection

Subscriber Identity Protection [3]

- A Temporary Mobile Subscriber Identity (TMSI) is used instead of an IMSI to temporarily identity the subscriber.
  - Prevents an eavesdropper from identitying the subscriber.
- TMSI is assigned on the first phone switch on when IMSI is sent to the AuC.
- When the subscriber's location is updated, a new TMSI assignment occurs.
- The MS reports to the network using the TMSI.
- Network uses TMSI to communicate with the MS.
- When the MS is switched off, the TMSI is saved to the SIM card for reuse next time.
- TMSI is assigned by the VLR.

Detection of compromised equipment [3]

- Each handset has a unique International Mobile Equipment Identifier (IMEI).
- This can be used to identity stolen or compromised handsets.
- The EIR is used to lookup an IMEI to check whether it has been compromised (i.e. on the black list).
- A Central EIR (CEIR) consolidates the black lists of several operators.
  - If a device's IMEI is listed on the CEIR it is not supposed to work on any network operator that is a member of the CEIR.

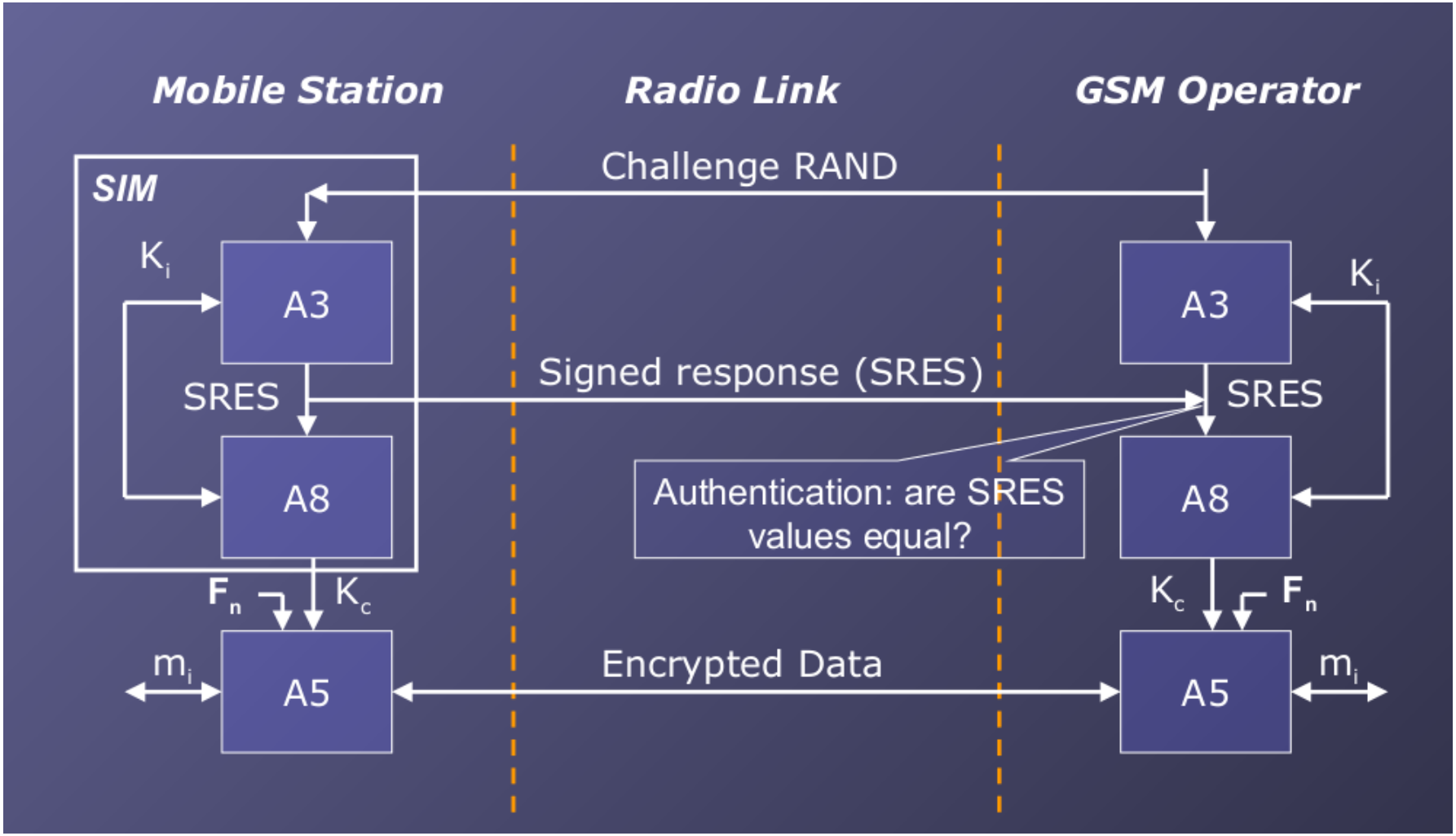
Authentication [3]

- Authentication Goals
  - Subscriber authentication.
  - Protection of the network against unauthorized use.
  - Establish a session key.
- Authentication Scheme
  - Subscriber identification: IMSI or TMSI
  - Challenge-Response protocol run between subscriber and operator.

Air Interface Security [4]

- Three main algorithms
  - A3 algorithm used for authentication
  - A8 for generation of a cipher key
  - A5 for enciphering data.
- All security operations based on a 128-bit key K_i shared between the SIM card and the AuC.

Authentication



Source: [3].

Authentication [3]

- The AuC supplies triples (parameters for authentication and encryption) of the form $(\mathrm{RAND}, \mathrm{RES}, K_c)$.
- The HLR gives the triples to the MSC.
- When a subscriber is not in his/her home network, the VLR stores the triples.

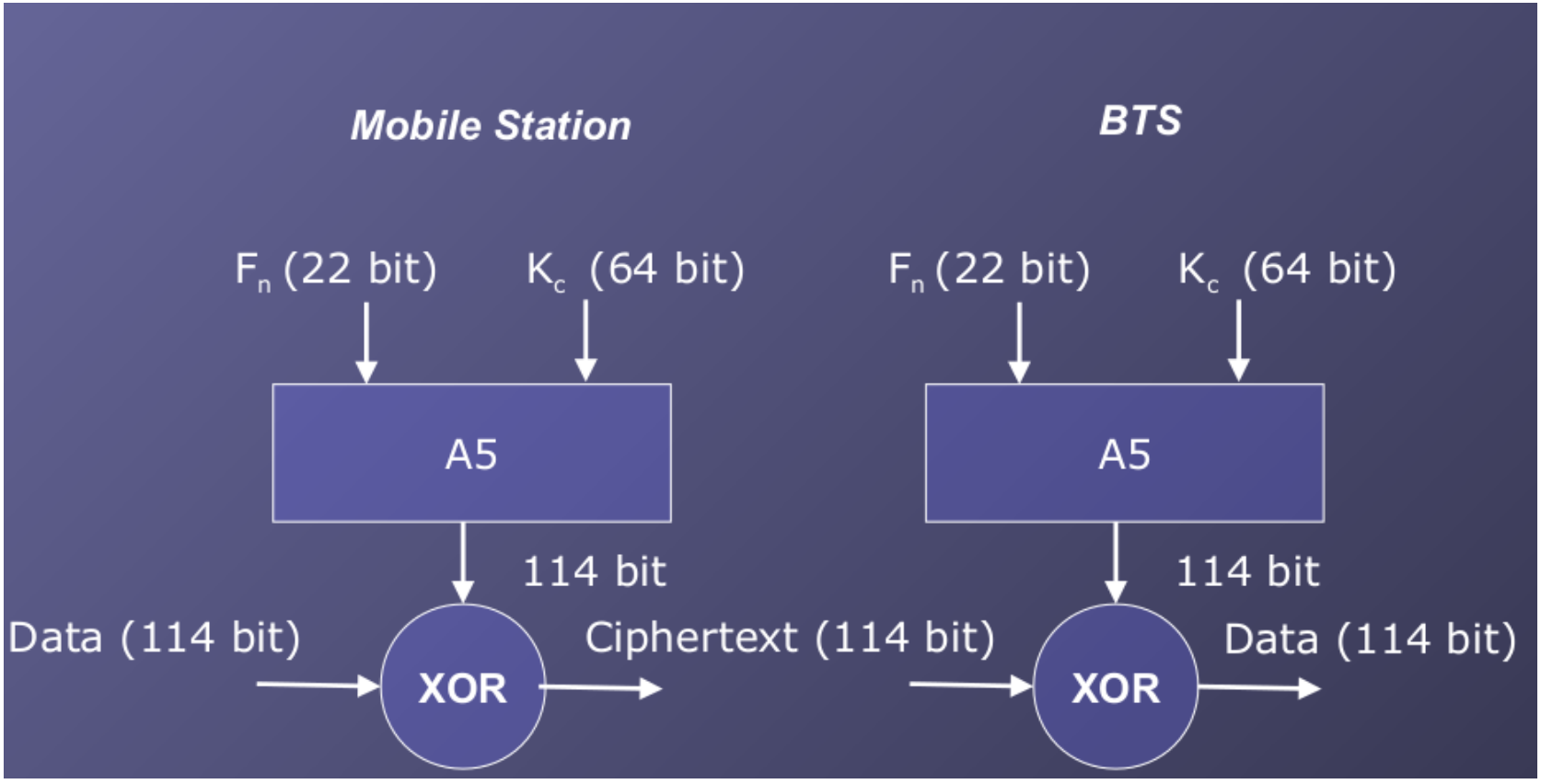
A3 and A8 [3]

- Both algorithms are implemented on the SIM
- Algorithm implementation is independent of network operators and hardware manufacturers.
- Operator can decide which algorithm to use.
- In most GSM networks, the COMP128 algorithm is used for A3 and A8.
  - COMP128 is a keyed hash function
  - Takes a 128-bit key and a 128-bit input (such as RAND) and produces a 128-bit output.
  - SRES is 32 bits and with COMP128v1 K_c is 54 bits (this weakens the encryption provided by A5). K_c is 64-bits in COMP128v2.

A5 [3]

- A stream cipher that can be implemented efficiently on hardware.
- Design was never made public.
- Variants
  - A5/1 - strong version
  - A5/2 - weak version
  - A5/3 - Also known as KASUMI, designed by 3GPP for use in UMTS.

A5


Mobile Station
BTS
F_n (22 bit)
K_c (64 bit)
F_n (22 bit)
K_c (64 bit)
A5
A5
114 bit
114 bit
Data (114 bit)
XOR
Ciphertext (114 bit)
XOR
Data (114 bit)

Source: [3].

Attacks on GSM Security [5]

- April 1998
  - Smartcard Developer Association and researchers at UC Berkley break COMP128 and recover K_i in hours.
  - Discovered K_c is only 54 bits (not 64 bits).
- August 1999
  - A5/2 cracked using a single PC within seconds.
- December 1999
  - Biryukov, Shamir, and Wagner publish break of A5/1. Requires 2 minutes of intercepted call. Attack time is then only 1 second.
- May 2002
  - Research group at IBM extract COMP128 keys using a side-channel attack.
- August 2003
  - Barkan, Biham and Keller present instant ciphertext-only attack on A5/1 and A5/2. The attack requires only a few dozen milliseconds of encrypted communication. It finds the correct key in under a second on a PC.

Denial of Service [1]

- User de-registration request spoofing
  - Intruder spoofs a deregistration request (IMSI detach) to the 2G network.
  - The network then de-registers the user from the visited location area and tells the HLR to do the same.
  - The user is then unreachable for mobile services.
- Location update request spoofing
  - The attacker spoofs a location update request in an area different from the one the user is roaming in.
  - The network registers the user in the other area (he/she will be paged in that area).
  - The user is then unreachable in his/her actual location.

Identity Catching [1]

The following attacks can be launched against user identity confidentiality in GSM.

- Passive identity catching
- Active identity catching
  - *IMSI Catcher* acts as a fake base station (BS) and performs a man-in-the-middle attack.
  - An MS attaches to the fake BS.
  - The fake BS sends a special identity request forcing the transmission of the MS' IMSI.

Fake base stations can be built by programming software-defined radios such as USRP (Universal Software Radio Peripheral) boards.

Impersonation of the Network[1]

- suppressing encryption between target user and intruder
  - The attacker uses a modified BS to launch the attack and exploits the fact that MS cannot authenticate signaling messages received over the radio.
  - The target user is attracted to camp on the rogue BS.
  - When a service is initiated, the attacker spoofs the cipher mode command to not enable encryption.
- suppressing encryption between the target user and the legitimate network
  - The target user is attracted to camp on the rogue BS.
  - When a call is set up, the fake BS modifies the encryption capabilities of the MS to make it appear to the network that there is an incompatibility (in terms of encryption) between network and MS.
  - The network may then decide to establish an unencrypted connection.

Impersonation of the Network [1]

- forcing the use of a compromised cipher key
  - This attack requires a compromised authtentication vector.
  - The target user is attracted to camp on the rogue BS.
  - When a call is set up, the fake BS forces the use of a compromised cipher key on the MS.
  - Sequence numbers in UMTS protect against forced reuse of a compromised authentication vector.

Impersonation of the User [1]

Impersonation of the user through

- use of a compromised authentication vector
- use by the network of an eavesdropped authentication response
- hijacking incoming and outgoing calls in networks with encryption disabled

References I


Boudriga, N.:
Security of Mobile Communications. 1st edn.
Auerbach Publications, Boston, MA, USA (2009)


Pundir, A.:
Understanding gsm: The basic.
https://www.linkedin.com/pulse/understanding-gsm-basic-ashish-pundir (2015)


Stepanov, M.:
Gsm security overview.
(http://www.cs.huji.ac.il/~sans/students_lectures/GSM%20Security.ppt)


Traynor, P., McDaniel, P., La Porta, T.:
Security of Telecommunications Networks.
Springer (2008)

References II

Tague, P.:
Mobile security: Gsm security & attacks.
http://wnss.sv.cmu.edu/courses/14829/f11/files/tague_14829f11_03.pdf (2011)