Mobile Security

Network Security - Lecture 6

Ruxandra F. Olimid

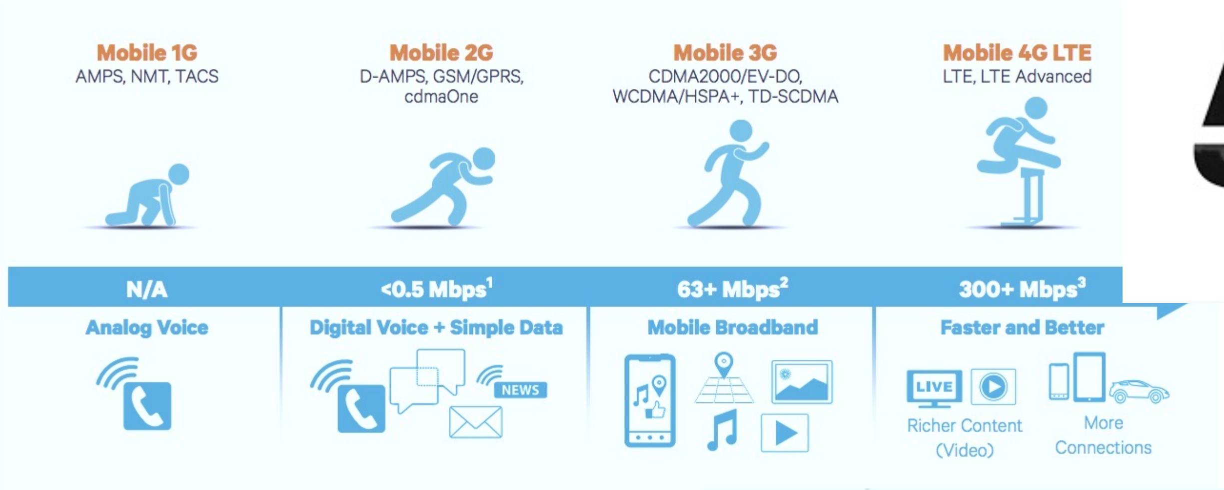
Faculty of Mathematics and Computer Science, University of Bucharest

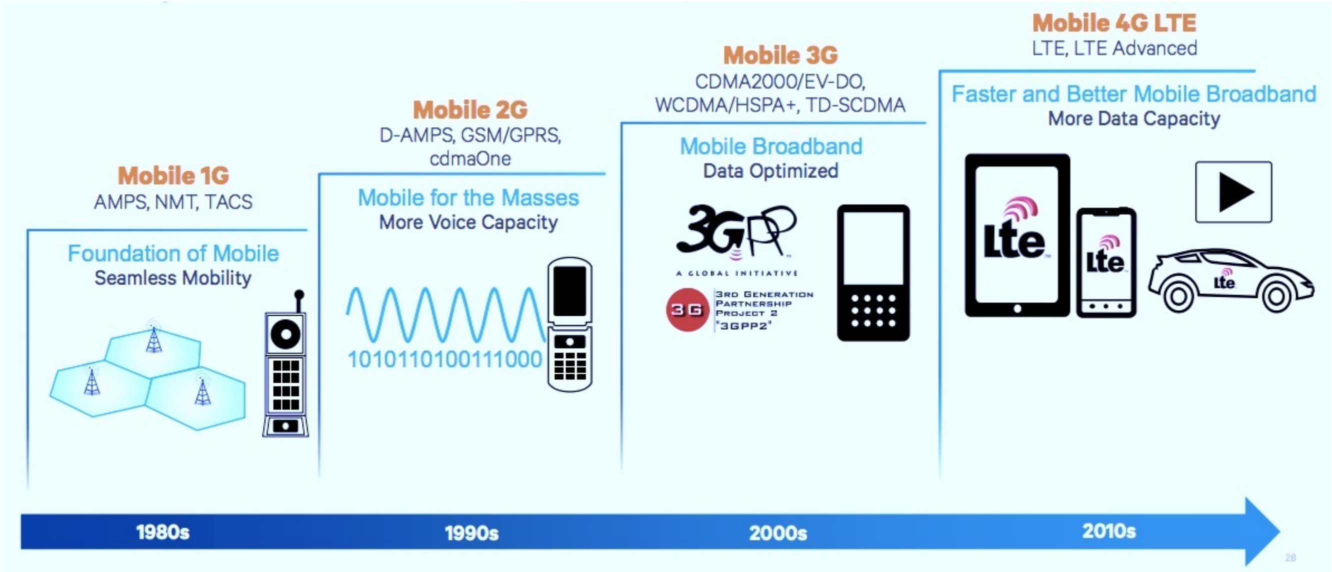
*slides adapted from the course TTM4137 thought at NTNU

Outline

- Intro to Mobile Security
- GSM Architecture
- GSM Security Requirements / Principles
- Vulnerabilities and Attacks

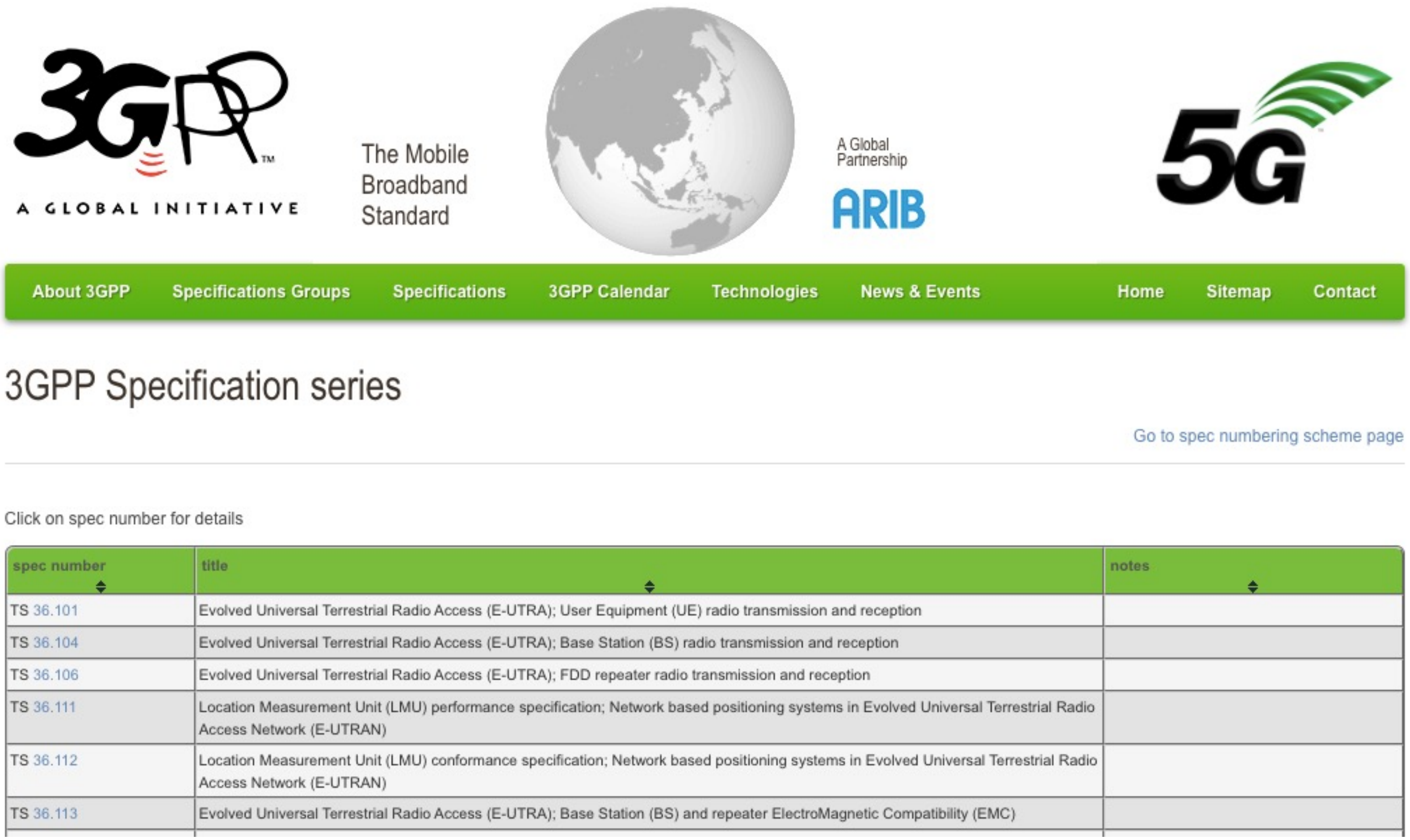
Evolution





[Source: Qualcomm – The Evolution of Mobile Technologies, '14]

3GPP - Specifications



3GPP A GLOBAL INITIATIVE

The Mobile Broadband Standard

A Global Partnership ARIB

5G

About 3GPP | Specifications Groups | Specifications | 3GPP Calendar | Technologies | News & Events | Home | Sitemap | Contact

3GPP Specification series

Go to spec numbering scheme page

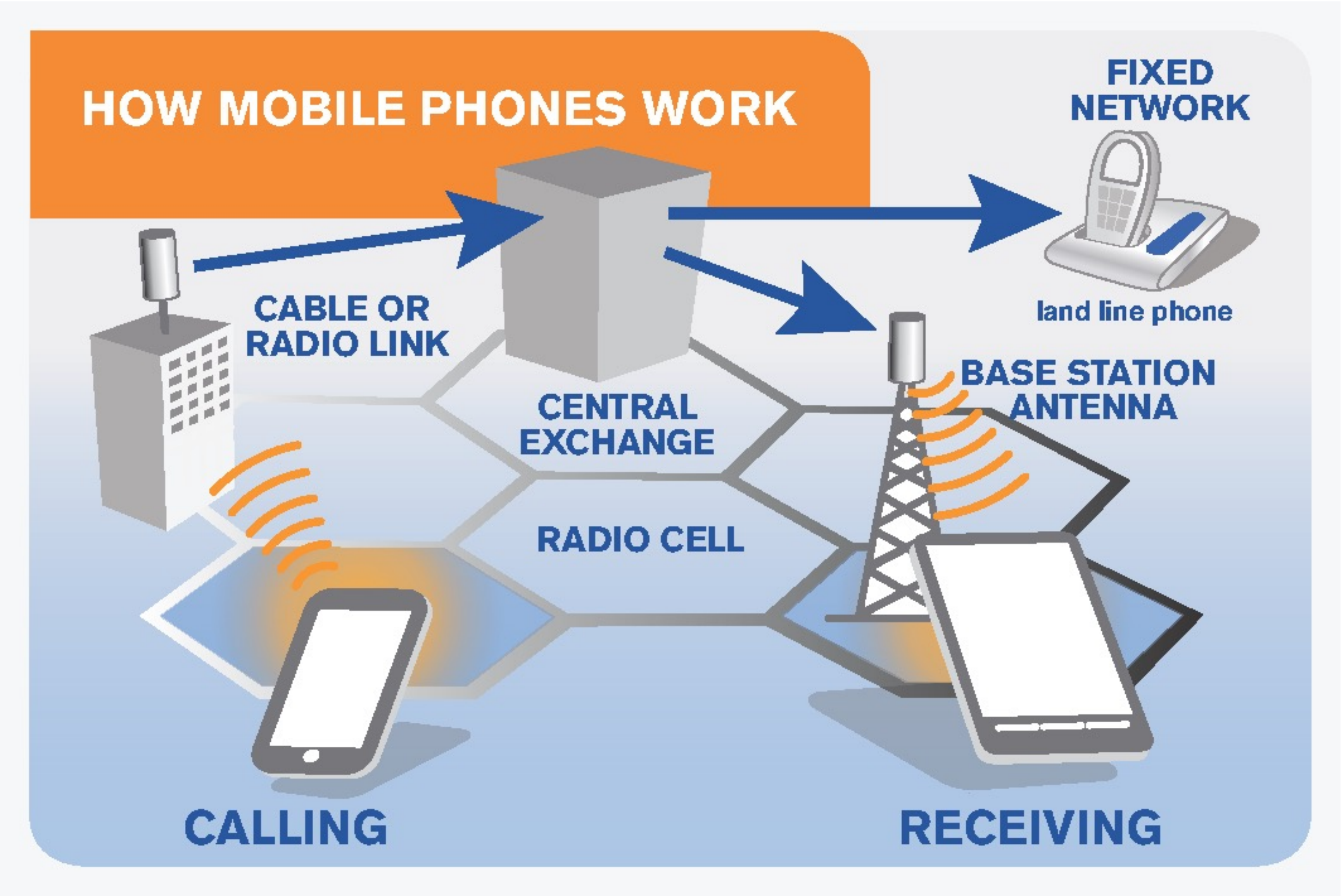
Click on spec number for details

spec number	title	notes
TS 36.101	Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception	
TS 36.104	Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception	
TS 36.106	Evolved Universal Terrestrial Radio Access (E-UTRA); FDD repeater radio transmission and reception	
TS 36.111	Location Measurement Unit (LMU) performance specification; Network based positioning systems in Evolved Universal Terrestrial Radio Access Network (E-UTRAN)	
TS 36.112	Location Measurement Unit (LMU) conformance specification; Network based positioning systems in Evolved Universal Terrestrial Radio Access Network (E-UTRAN)	
TS 36.113	Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) and repeater ElectroMagnetic Compatibility (EMC)	

https://www.3gpp.org/

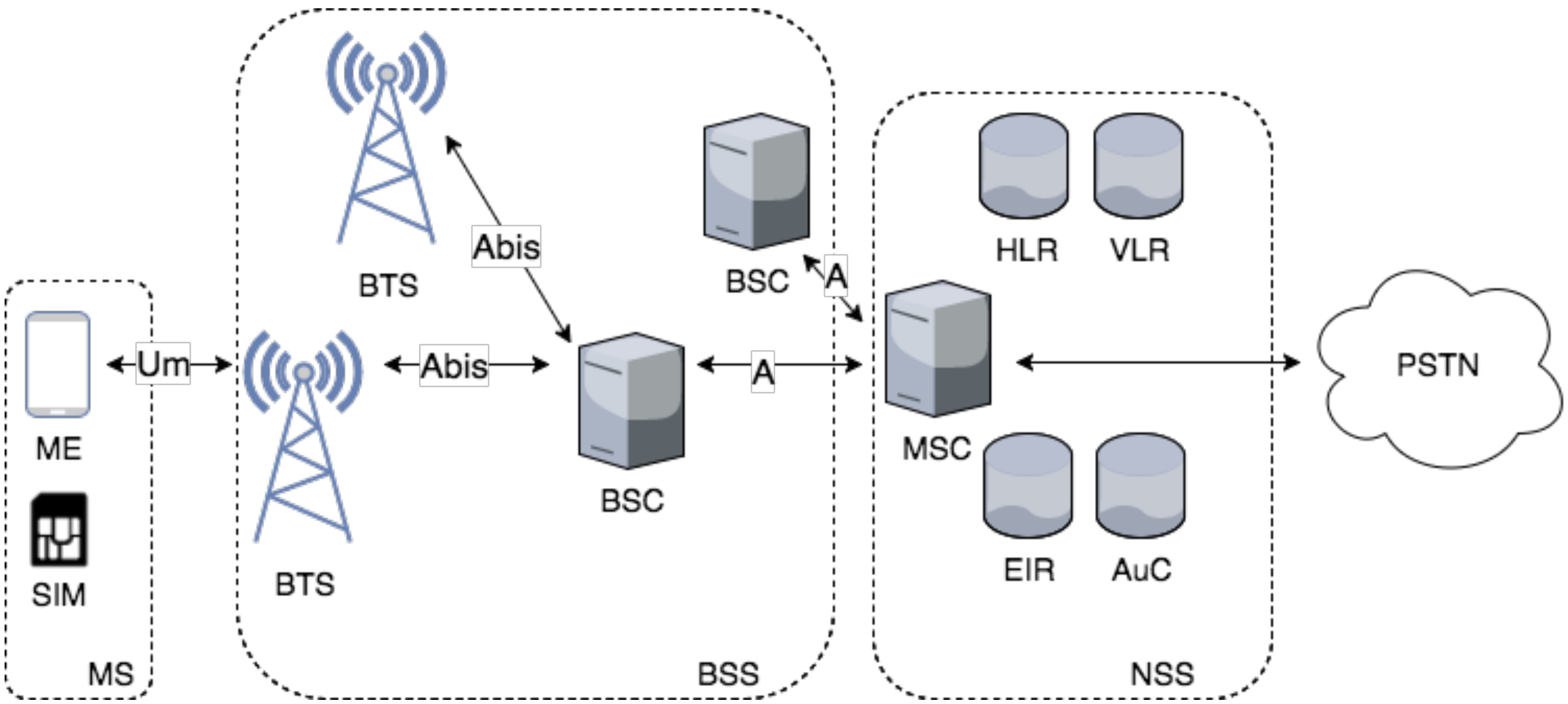
Overview

- User device
- Access network
  - Radio link
- Core network



[Source: ITU EMF Guide http://emfguide.itu.int/emfguide.html]

GSM - Architecture



MS: Mobile Station
ME: Mobile Equipment
SIM: Subscriber Identity Module

BSS: Base Station Subsystem
BTS: Base Transceiver Station
BSC: Base Station Controller

NSS: Network Subsystem
MSC: Mobile Services Switching Center
HLR: Home Location Register
VLR: Visitor Location Register
EIR: Equipment Identity Register
AuC: Authentication Center

PSTN: Public Switched Telephone Network

GSM - Arhitecture

- MS (Mobile Station):
  - Consists in a Mobile Equipment (ME) and the Subscriber's Identity Module (SIM)
- BSS (Base Station Subsystem):
  - Consists in several BTSs and BSCs
  - The BSC is a central element that controls the radio network, maintaining radio connectivity with several BTSs and providing connection to the NSS
  - BTS is the element to which the MS connects to in the GSM network via radio link; its functions include signal processing, signaling, ciphering
- NSS (Network SubSystem):
  - MSC is the main element of the NSS with respect to call functions, being responsible for call control, BSS control, and interconnecting to the external networks (PSTN)

GSM - Arhitecture

- VLR (Visitor Location Register):
  - Stores information about subscribers that are served by the MSC (it maintains copies of the data from HLR, increasing efficiency: decreases the number of messages that are exchanged between the MSC and the HLR)
  - Usually is not independent hardware, but a software component of the MSC
- HLR (Home Location Register):
  - It is the main database in GSM
  - Maintains information for each subscriber: IMSI, phone no. - MSISDN (Mobile Station International Subscriber Directory Number), available services for the subscriber, location, etc.
- AuC (Authentication Center):
  - For each subscriber, stores the permanent key K_i that is also stored in the SIM
  - Generates the authentication vectors (RAND, SRES, K_C) in the authentication phase

GSM - Arhitecture

- EIR (Equipment Identity Register):

  - Keeps inventory of the devices in the mobile network, which are identified by their IMEI

  - Keeps up to date 3 lists:

    - *__White list__:* contains the equipment that are compliant to the operator and can access the mobile network without any restriction

    - *__Black list__:* contains the equipment that have been reported as stolen or that have been proved to affect the network functionality, and that are restricted to access the mobile network

    - *__Gray list__:* contains the equipment that are not fully compliant to the operator, and are allowed to access the network but there are under surveillance

GSM – Security Principles

We will find a similar limitation for LTE, where for example 3GPP did not considered PKI to be a feasible solution

Goal: GSM should be as secure as the wired network (PSTN) …
…but, security mechanisms should not have a negative impact on the usability of the system

- Security requirements in GSM:

- *Access control to the MS:* provide authenticated user access to the mobile station
- *Anonymity of subscribers (privacy):* keep the identity of the subscribers (and their location, possibility of linking calls, etc.) hidden to external parties
- *Authentication of subscribers*: subscribers must prove their identity and their right to access mobile services
- *Confidentiality:* maintain the confidentiality <u>on the radio link</u>

GSM – Security Principles

Weaknesses in GSM security:

- *Breaking Kerckhoffs' principle*: cryptographic algorithms were kept confidential (e.g.: A5/1, A5/2), and their strength was not publicly tested
- *Short keys;* cryptosystems are vulnerable to *exhaustive search attack*
- *Limited encryption:* data is encrypted on the radio link only
- *Unilateral authentication:* The mobile station does not authenticate the network (only the network authenticates the mobile station)
- No specification about the *integrity of the data*
- *Active attacks are possible*; e.g.: IMSI Catchers, when an adversary masquerades a legitimate BTS
- *Users are (usually) not notified about the level of security used*

Mobile Equipment (ME)

- Identification:
  - **IMEI** (International Mobile Equipment Identity), a number used to identify the mobile phone; it is printed on the device, and it can be displayed by dialing *#06#
  - **IMEISV** (IMEI Software Version) discards the check digit from the IMEI and adds 2 digits SVN (Software Version Number)

- Access control:
  - IMEI can be used to deny connectivity to the network for stolen phones based on a blacklist stored by the operator
  - Biometric authentication; e.g.: fingerprint recognition, voice recognition
  - Screen unlock mechanisms; e.g.: codes, patterns

SIM Card

- Identification:
  - **IMSI** (International Mobile Subscriber Identity), a global unique identifier for the subscriber (≅15 digits)
  - **ICCID** (Integrated Circuit Card ID) it is the identifier of the SIM itself and printed on the SIM card
- Access control:
  - **PIN** (Personal Identification Number), a sequence of numbers required to unlock the SIM card
  - **PUK** (Personal Unlocking Key), a code required when the PIN has been introduced incorrectly several times

IMSI (International Mobile Subscriber Identity)

MCC (Mobile Country Code) - 3 digits -	**MNC** (Mobile Network Code) - 2 digits (EU) / 3 digits (US) -	**MSIN** (Mobile Subscriber Identification Number)
242 (Norway)	01 (Telenor) / 02 (Telia)	XXXXXXXXXX
226 (Romania)	01 (Vodafone) / 10 (Orange)	XXXXXXXXXX

List of MCCs and MNCs: http://mcc-mnc.com/

SIM Card

Authentication and Confidentiality:

- **IMSI** (International Mobile Subscriber Identity)
- **TMSI** (Temporary Mobile Subscriber Identity), a temporary identity used to restrict the sending of IMSI over the air and mitigate eavesdrop attacks
- **K_i** a 128-bits permanent key
- Cryptographic mechanisms: a *challenge-response mechanism* that uses the permanent key for the authentication of the subscriber and a *key generation mechanism* for confidentiality of communication

SIM cards must be *tamper-resistant* (i.e. an adversary should not be able to read / modify the security information stored on the SIM card). Otherwise, SIM cards become vulnerable to *cloning attacks*, for which the attacker creates copies of the SIM card to use in different purposes (eavesdropping on the victim, making calls on the victim behalf, etc.)

*Terminology: Initially, the card itself was also called a SIM, later the card itself was called UICC (Universal Integrated Circuit Card) and the SIM was considered the application running on the card

Anonymity of Subscribers

- Goal: Keep the identity (presence/absence in an area, location, etc.) of the subscriber private to unauthorized parties

- A subscriber can identity itself by one of the following identifiers:
  - **IMSI** - permanent identity
  - **TMSI** - temporary identity

- Principles:
  - Introduce the TMSI as a way to avoid IMSI exposure on the radio interface
    - e.g.: IMSI uniquely identifies a subscriber, and if it intercepted it suffice to prove the presence of the subscriber in a location
  - TMSI is assigned to the MS when authenticates to the network, and it is local in the visiting network (VLR keeps the IMSI – TMSI correspondence); the MS stores the TMSI in the SIM to use it even after rebooting
  - TMSI must be renewed at specific intervals (tradeoff with efficiency); a TMSI that is not changed often enough can break privacy too

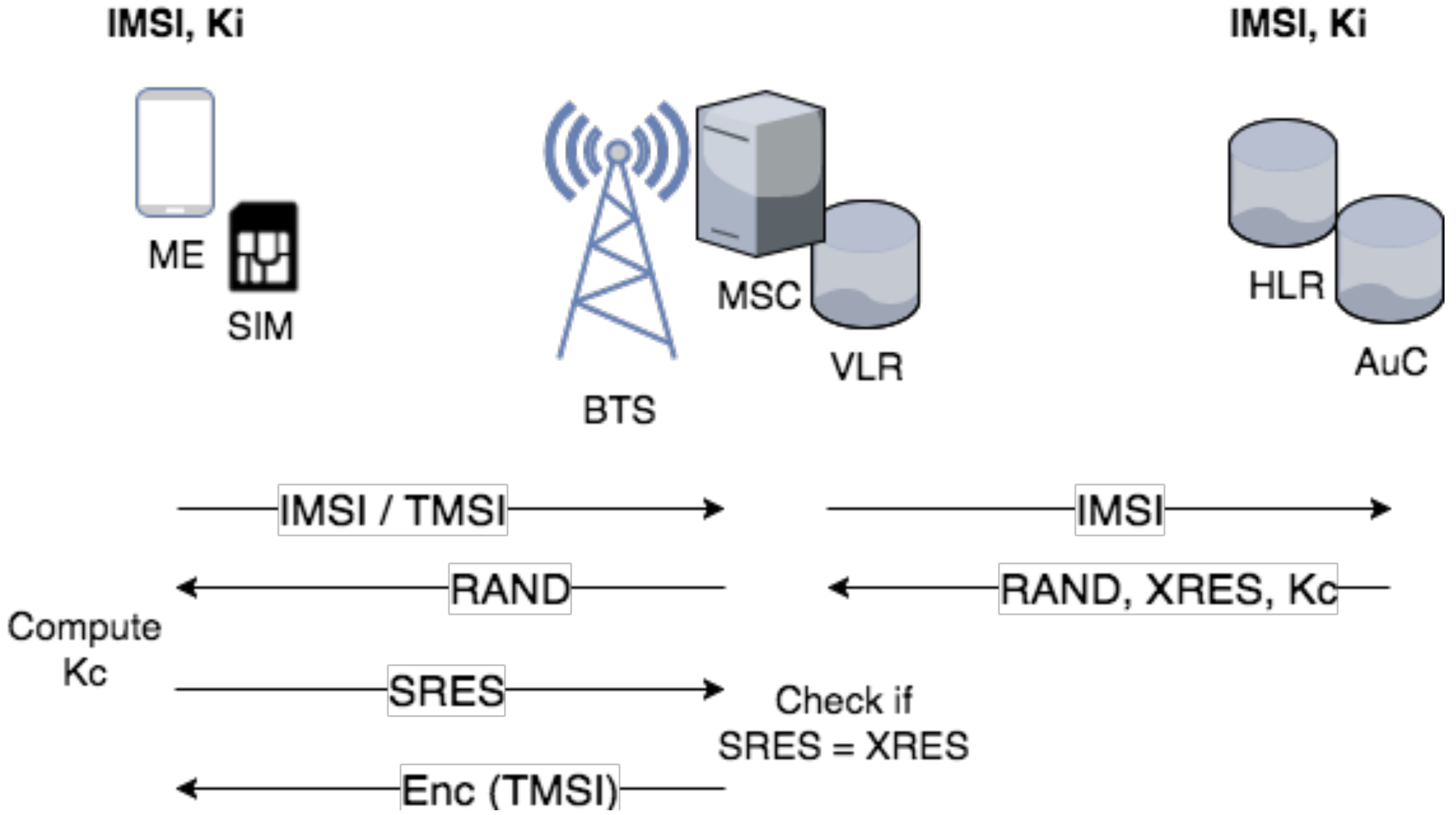
Authentication of Subscribers

- Goal: Prove the identity of the subscriber to the mobile network, and avoid unauthorized parties to access the mobile services

- The authentication mechanism uses:
  - The permanent key $\mathbf{K_i}$, unique for each subscriber, that is stored:
    - in the SIM card (**subscriber's side**)
    - in the AuC (**network operator's side**)
  - Cryptographic algorithms: **A3** (subscriber authentication), **A8** (key generation)

- Principles:
  - K_i does never leave the 2 locations (SIM, AuC);
  - Authentication consists in checking if the subscriber knows the correct key K_i by using a *challenge-response mechanism*
  - The serving network does not have access to the key K_i, so it cannot perform authentication without help from the home network
  - During authentication phase, is derived a key K_c that will be later used for encryption

Authentication of Subscribers



$Kc = A8(K_i, RAND)$

$SRES / XRES = A3(K_i, RAND)$

Authentication Triplets

- Goal: Allow the visiting network to authenticate the MS without knowing K_i and improve efficiency by using batches of triplets

- A triplet used for authentication is

$$(\text{RAND}, \text{XRES}, K_c)$$

where $\text{XRES} = \text{A3}(K_i, \text{RAND})$ and $\text{Kc} = \text{A8}(K_i, \text{RAND})$

- Operation:
  - AuC produces batches of triplets for each MS, each with a different RAND and sends them to the HLR
  - For a single request, the VLR receives a batch of triplets from the HLR (to avoid often communication between the VLR and the HLR)
  - If the network runs out of triplets, it should request more from the HLR, but if not it is allowed to reuse triples

Encryption

- Goal: Encrypt all communication between the mobile station and the BTS (both phone calls and sensitive signaling information such as TMSI, MSISDN, etc.)

- The GSM encryption uses:
  - The key $\mathbf{K_c}$, derived in the authentication mechanism
  - Encryption algorithm: **A5** (radio encryption)

- Principles:
  - Encryption is only performed on the radio link (!)
  - The encryption algorithm uses as input the session ley K_c derived from the authentication phase

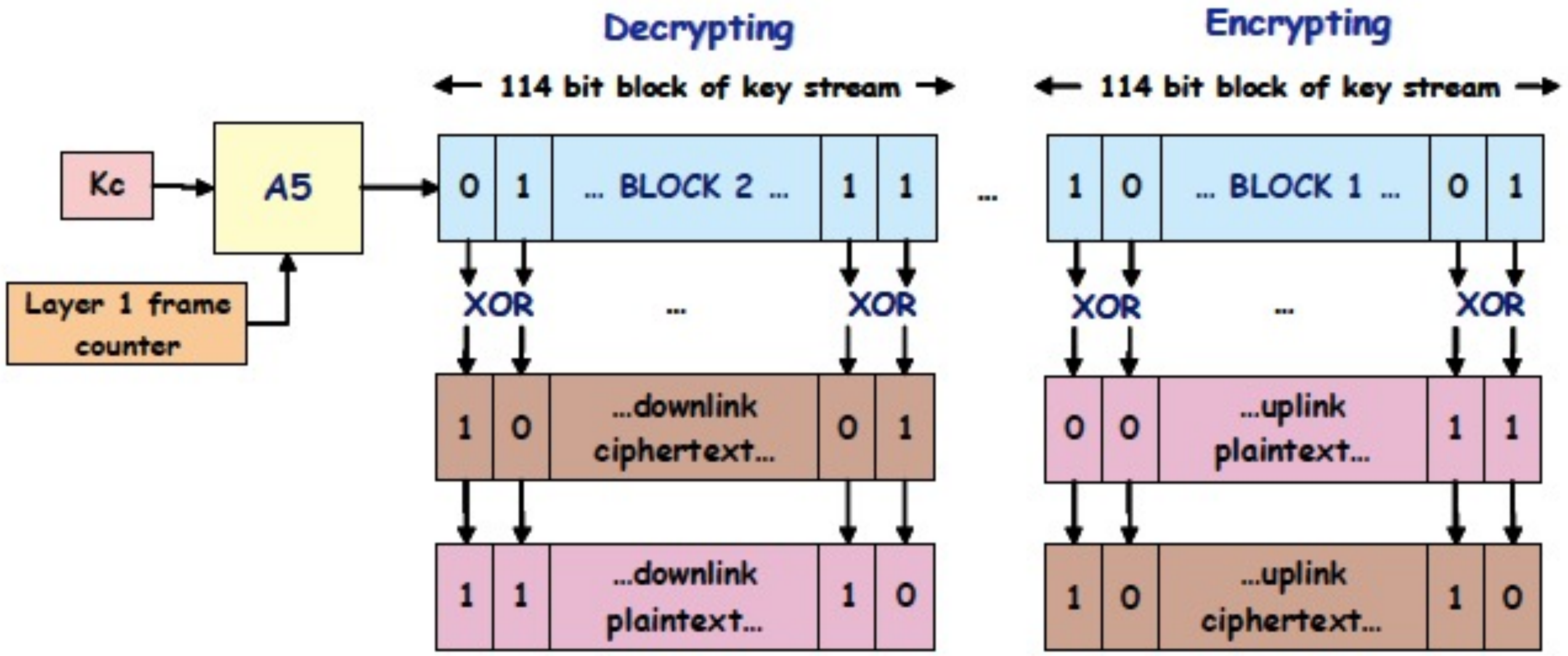
- Operation:
  - The key K_c is used as the encryption key for a stream cipher (LFSR-based):

$$\text{Ciphertext} = \text{A5}(K_c, \text{Plaintext})$$

Encryption

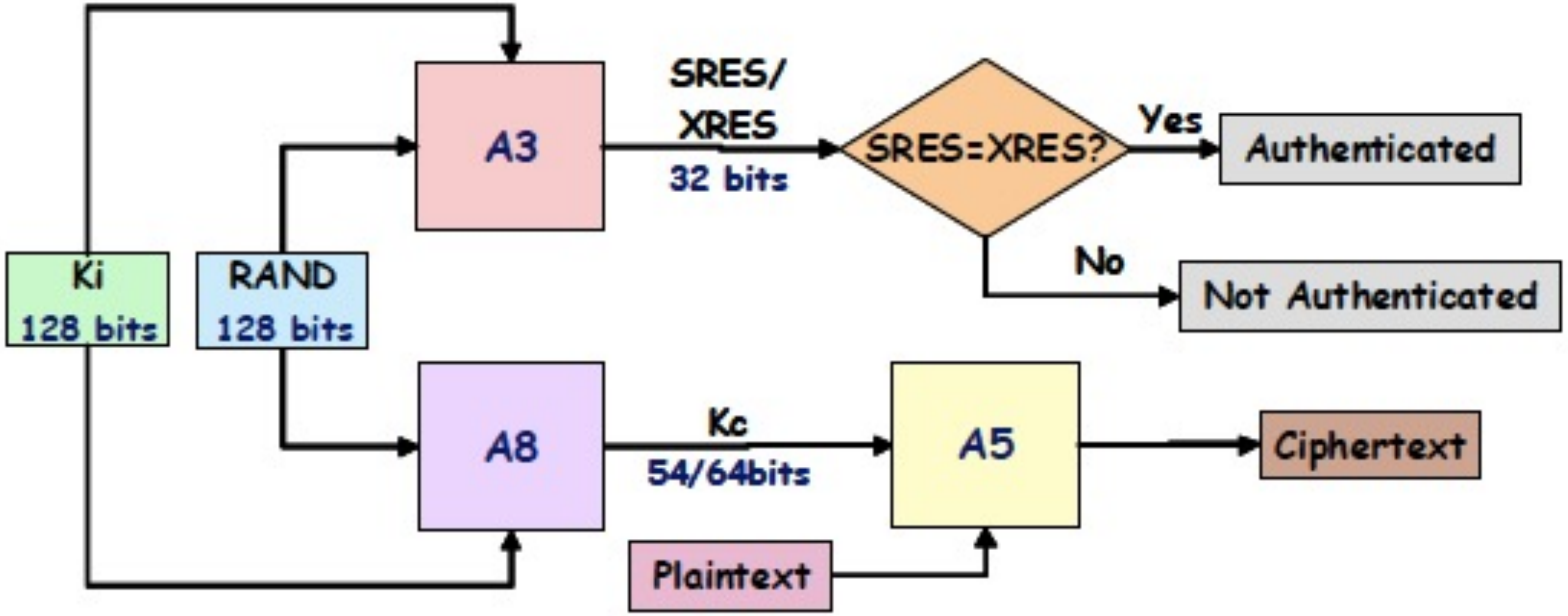
- Both A5/1 and A5/2 were not public, breaking *Kerckhoffs' principle*
- Encryption operates at the physical layer (Layer 1), which brings some advantages:
  - Maximum amount of data is encrypted (both user and signaling data)
  - The encryption algorithm can be implemented in hardware
- A5 algorithms are **stream ciphers**, so encryption is performed bit-by-bit
- A *frame counter* (22 bits) is used as an additional input together with the key K_c
- Vulnerability! The frame counter repeats every 2^{22} frames (approx. every 3.5 hours), so the key stream repeats if the K_c is not renewed meanwhile
- GSM is *full duplex*: for each frame, first 114-bit block (Block1) is used for encryption of data that is being transmitted, and the second 114-bit block (Block2) is used for decryption of data that is being received

Encryption



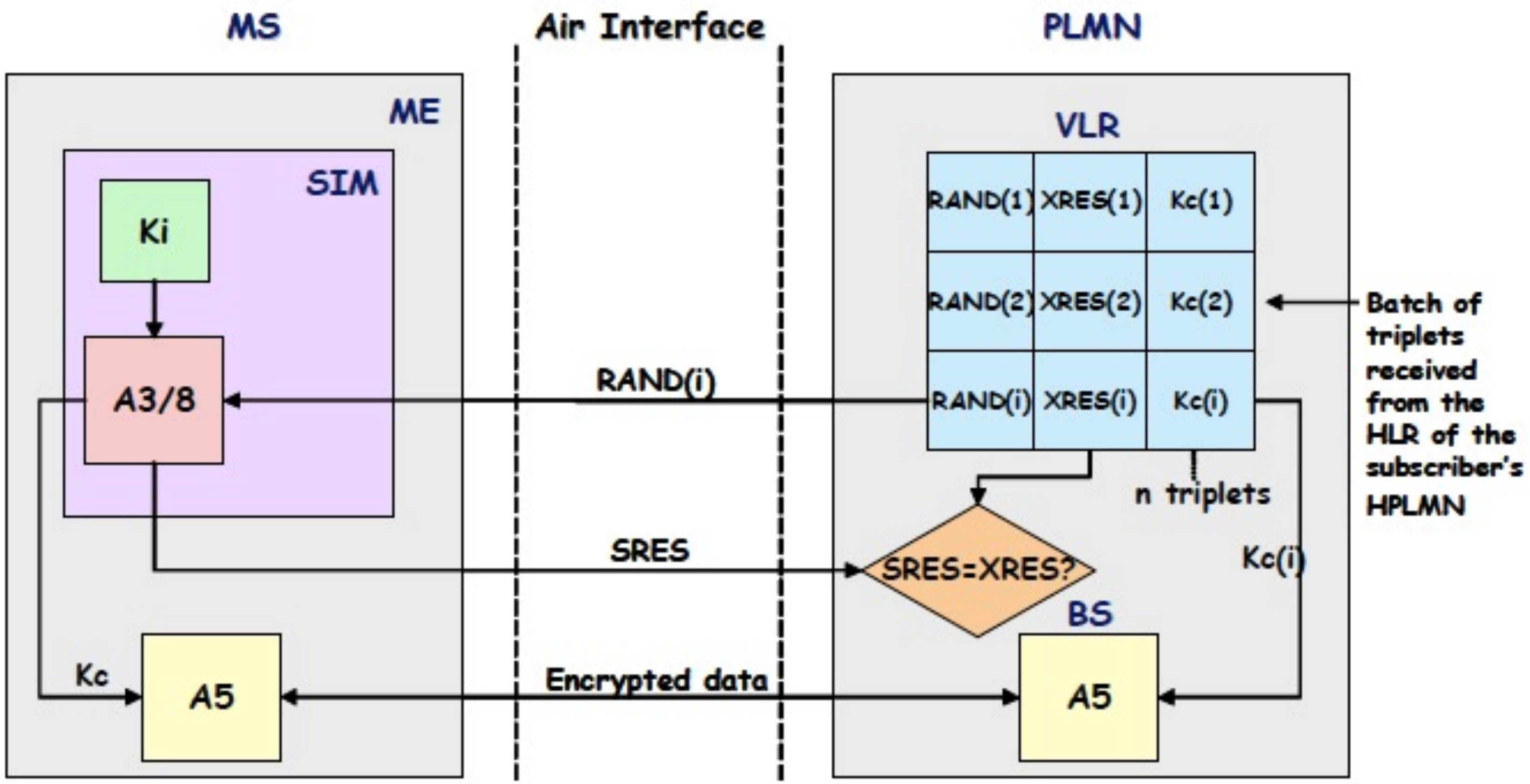
[Source: P.S.Pagliusi – A Contemporany Foreword on GSM Security, InfraSec '02]

Overview



[Source: P.S.Pagliusi – A Contemporany Foreword on GSM Security, InfraSec '02]

Overview



[Source: P.S.Pagliusi – A Contemporany Foreword on GSM Security, InfraSec '02]

Crypto

Key	Length / Input + Output	Info
K_i	128 bits	Key shared between the subscriber and the network operator, stored in the SIM and AuC
K_c	54/64 bits	Secret session key, that will be used for encryption Kc = A8(K_i, RAND)
RAND	128 bits	Random challenge
SRES / XRES (Signed Response / Expected Response)	32 bits	Response to the challenge request / Expected response to the challenge request SRES / XRES = A3(K_i, RAND)
A3, resp. A8	Input: K_i, RAND Output: SRES, resp. K_c	Generic algorithms for authentication, resp. key generation (no specific algorithms) e.g.: COMP128 combines A3 and A5 and generates XRES (32 bits) and K_c (54 random bits concatenated to 10 bits of 0) Stored in the SIM
A5	Input: Kc, plaintext Output: ciphertext	Class of standardized encryption algorithms: A5/0 (no encryption), A5/1 (CEPT + USA), A5/2 (Asia), A5/3 (Kasumi, UMTS) Stored in the mobile equipment (not SIM!)

Security Principles

- Modularity:
  - GSM is modular in the sense that the cryptographic algorithms can be replaced with others, as long as maintain the same input-output structure
  - A5 refers to a family of algorithms; e.g.: A5/1, A5/2, A5/3 (64 bits key K_c); A5/0 (no encryption), A5/4 (128 bits key K_c) – some used for UMTS (e.g.: A5/3)

- Standardization:
  - A5 must be standardized (e.g.: MS must communicate to BTS in roaming)
  - A3, A8 must not necessary be standardized, because both parties involved (the SIM and the AuC) belong to the same network operator; however, 3GPP gave an example algorithm set TS55.205

[ETSI TS 155 205 V9.0.0 (2010-02): link]

Security Principles

- Use the SIM as a security module:
  - Authentication and confidentiality are performed based on a shared secret (K_i)
  - The SIM stores secret information of the subscriber (K_i, IMSI) and cryptographic algorithms (A3, A8)
  - Should be tamper-resistance
- Security in the visiting network:
  - The key K_i must not be shared to the visitor network
  - Authentication triplets allow authentication in visitor networks
- Algorithms’ requirements:
  - Statistically impossible to guess SRES
  - Statistically impossible to find K_i, K_c from the eavesdropped data
  - … (assumptions that exclude trivial attacks)

Vulnerabilities and Attacks

- Passive attacks:
  - The adversary eavesdrops on the radio link and gets the IMSI
  - The attack is possible because the IMSI is sent in clear over the radio link when the MS posses no TMSI or it cannot be identified by using the TMSI

- Active attacks:
  - The adversary requests the IMSI from the MS
  - **IMSI Catcher**: the adversary masquerades a legitimate BTS and asks the MS for the IMSI
  - The attack is possible because the MS does not authenticate the network - and cell reselection criteria is signal strength
  - We will learn more on IMSI Catchers when we will study LTE

Vulnerabilities and Attacks

- Cryptanalysis:
  - **Key length**
    - the key length of K_c (54/64 bits) is too small to provide security
    - *Exhaustive search (brute force)* can break the key in a few hours
  - **COMP128** was cracked in 1998 (by Wagner and Goldberg, but apparently known before by some operators)
    - *Chosen plaintext attack*: K_i is found when about 16000 pairs RAND-SRES are collected
    - Possible ways to connect RAND-SRES pairs:
      - Steal the SIM and connect to a phone emulator (2 to 10 hours, dependent on the phone)
      - Use a false BTS (longer in time, but does not require physical access to the SIM)

Vulnerabilities and Attacks

- Cryptanalysis:
  - **A5/1** was broken in 1999 (by Biryukov, Shamir, later the attack was improved together with Wagner)
    - *Time-memory trade-off*:
      - *Pre-processing phase*: Compute a large database of states and related keys of the stream system
      - *Attack phase*: search subsequences of the key stream in the database; if a match is found, the state is the one in the database (with high probability)
      - 2s of known plaintext (both uplink and downlink) to succeed
  - **A5/2** was cryptanalysed in 1999 (Goldberg, Wagner, Green), 2003 (Barkan, Biham, Keller), etc.

Vulnerabilities and Attacks

- Radio links:
  - BTS to BSC link is sometimes not wired, making it easily susceptible to eavesdropping
  - Possible because GSM security do NOT consider encryption beyond the BTS-BSC link (but only on the MS – BTS radio link)

- Engineering attacks:
  - Attacks against the chip card, side-channel attacks
  - Software attacks
- Optionality:
  - Encryption was introduced as an optional feature
  - Very few terminals inform the user if encryption is taking place or not

To remember!

1. Apply Kerckhoffs' principle (make crypto public!)
2. Think about the future (e.g.: do not use small cryptographic keys, think about Moore's law!)
3. Trade-off between efficiency / usability and security might expose vulnerabilities
4. Do not underestimate your adversary! (active attacks were considered infeasible)
5. New notions: security aspects in GSM network