

UNIK 4250 - Mobile Network Security

Sindre

Tor

Iñaki

Seray

Nils

Andreas

Endre

Andre

Frik

slides:

(wi.unih.no/wiki/UNIK4250)



Mobile Network Security

Josef

Polygon Real Presence
Desktop

GSM: Cell size $< 15\text{km}$

UMTS: Cell size $3\text{km} \rightarrow 1.5\text{km}$

Mobile systems

The generation game

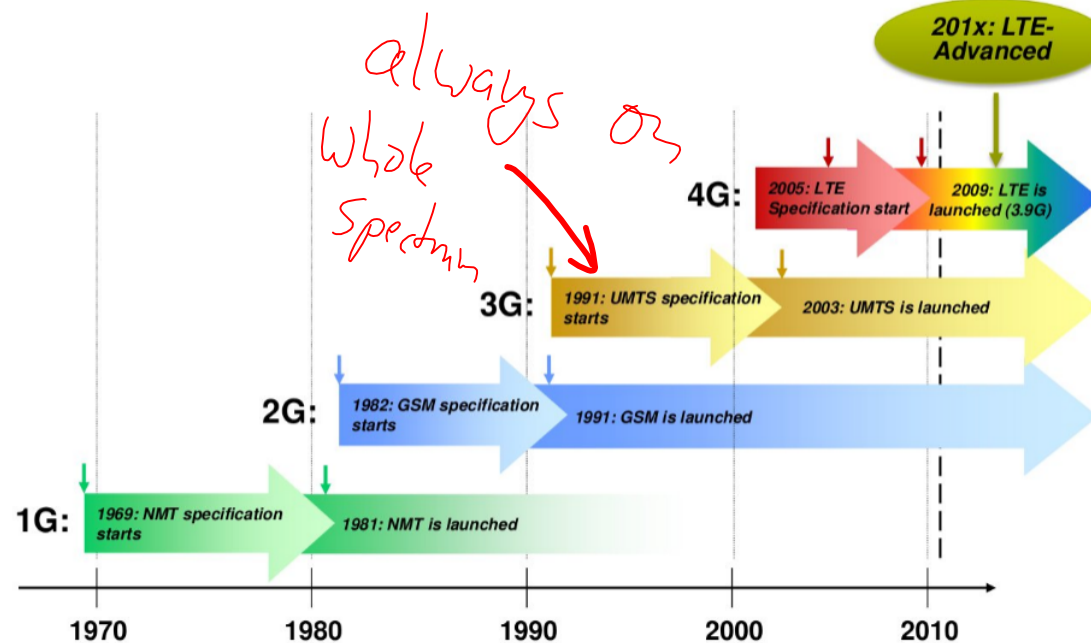


Figure from P. Lehne, Telenor Chapter 19:

Firefox UNIK4250-MobileSecurity.key - UNIK... UNIK4250-MobileSecurity.key - UNIK... UNIK4250 Mobile Network Security
cw.unik.no/images/c9/UNIK4250-L7-MobileSecurity.pdf
Side: 14 av 103 Automatisk zoom
[source: Lars Strand, 2011] Chapter 19:

Security Goals

- Protect against interception of voice traffic on the radio channel:
 - Encryption of voice traffic.
- Protect signalling data on the radio channel:
 - Encryption of signalling data.
- Protections against unauthorised use (charging fraud):
 - Subscriber authentication (IMSI, TMSI).
- Theft of end device:
 - Identification of MS (IMEI), not always implemented.

split of signalling & traffic
SIM
Temporary

Chapter 19:

Firefox UNIK4250-MobileSecurity.key - UNIK... UNIK4250-MobileSecurity.key - UNIK... UNIK4250 Mobile Network Security

cwi.unik.no/images/c9/UNIK4250-L7-MobileSecurity.pdf

Side: 15 av 103 Automatisk zoom Vis mine bokmerker

Chapter 19:

GSM – Components

- MS (Mobile Station) = ME (Mobile Equipment) + SIM (Subscriber Identity Module);
 - SIM gives personal mobility (independent of ME)
- BSS (Base Station Subsystem) = BTS (Base Transceiver Station) + BSC (Base Station Controller)
- Network Subsystem = MSC (Mobile Switching Center, central network component) + VLR, HLR, AUC, ...
- HLR (Home Location Register) + VLR (Visitor Location Register) manage Call Routing & Roaming Information
- AUC (Authentication Center) manages security relevant information
- ...

GSM 02

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

ects

- The authentication of the GSM PLMN subscriber identity may be triggered by the network when the subscriber applies for:
 - change of subscriber-related information element in the VLR or HLR (including some or all of: location updating involving change of VLR, registration or erasure of a supplementary service); or
 - access to a service (including some or all of: set-up of mobile originating or terminated calls, activation or deactivation of a supplementary service); or
 - first network access after restart of MSC/VLR; or in the event of cipher key sequence number mismatch.

HLR
SMS
voice
data
"data"
signalling

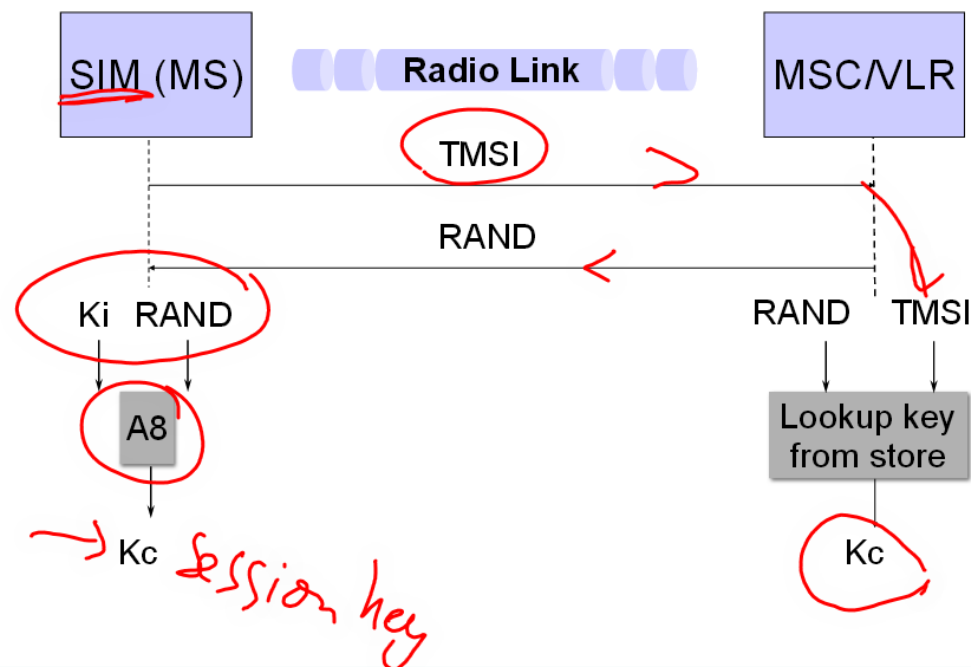
Chapter 19:

GSM Security

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

Authentication



Chapter 19:

UMTS (3G)

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

open security algorithms

- Universal Mobile Telecommunications System (UMTS)
- Security mechanisms in GSM used as starting point for UMTS
- UMTS objectives, specified in 3G TS 33.120, 3G Security, *Security Principles and Objectives*:
 - UMTS security will **build on** the security of 2G systems
 - UMTS security will **improve** on the security of 2G systems
 - UMTS security will **offer new** security features [services]
- Threat/risk analysis for 3G systems performed
 - 3G TS 21.133, 3G Security, *Security Threats and Requirements*
- The objectives + threat environment became basis for
 - 3G TS 33.102, 3G Security, *Security Architecture*

- mutual authentication
Mobile → BS

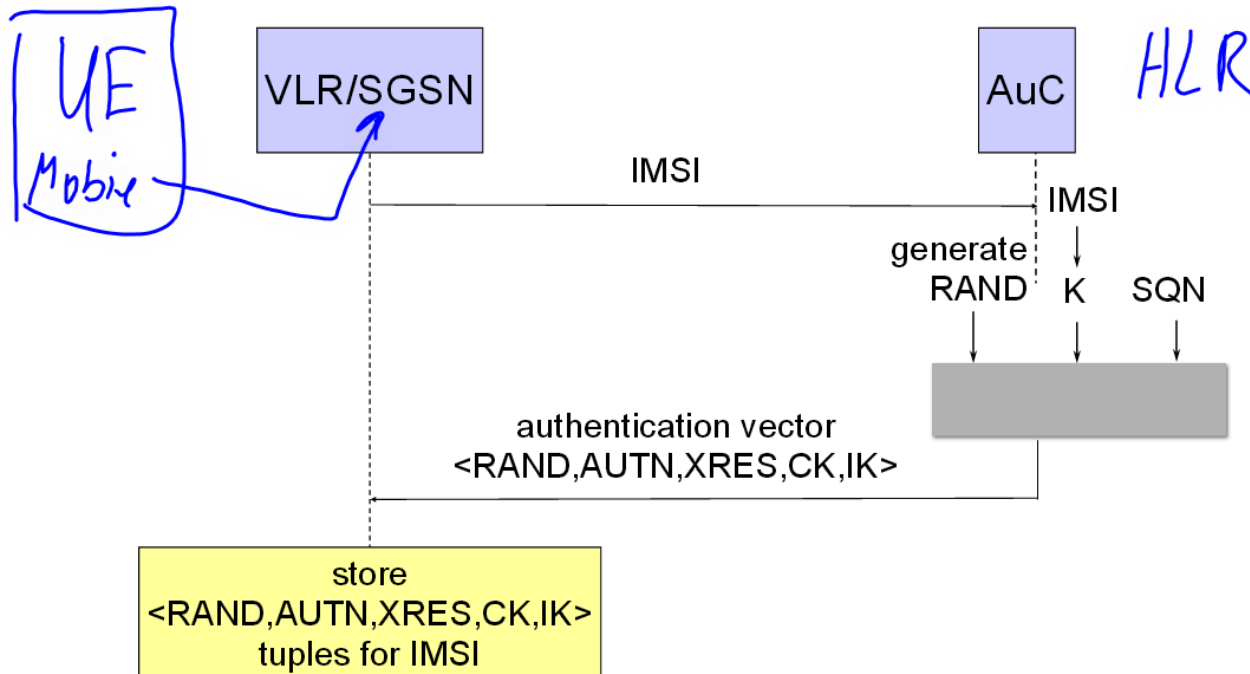
[source: Lars Strand, 2011]

Chapter 19:

UMTS

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.



Chapter 19:

UMTS

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

- Checks at USIM: *checks (Base station) network*
 - Compares MAC received as part of AUTN and XMAC computed to verify that RAND and AUTN had been generated by the home AuC.
 - Checks that SQN is fresh to detect replay attacks.
- Checks at VLR: *Checks user integrity (cached ~~ISIM~~)*
 - Compares RES and XRES to authenticate USIM.
- False base station attacks prevented by a combination of key freshness and integrity protection of signaling data, not by authenticating the serving network.

Chapter 19:

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

- Long Term Evolution (LTE/SAE) ture
- Overall architecture of Evolved Packet System (EPS) consists of:
 - 1) Access network
 - 2) Evolved Packet Core (EPC) network
 - IP Multimedia Subsystem (IMS)
- "Improved overall security robustness over UMTS"
- Major changes from UMTS:
 - All IP network (AIPN)
 - Higher bandwidth
 - May use non-3GPP access networks

only packet network
voice = "priority packet"



[source: Lars Strand, 2011]

LTE: H

pdf.js er nå i fullskjerm.

Trykk ESC når som helst for å avslutte.

works



- Non-3GPP access network include:
 - *cdma* cdm2000, WiFi (WLAN), fixed networks (Internet)
- Two classes of network access defined:
 - 1) Trusted access – has direct access to the operator network
 - Network operator decide which access technology is trusted
 - Can use EAP-AKA
 - 2) Untrusted access – everything else
 - Require IPsec with IKEv2 + EAP-AKA
 - Challenges: New threats (Internet), performance!

*EAP > 17 standards
EAP-SIM
EAP-AKA*

[source: Lars Strand, 2011]

48

EAP-SIM, EAP-AKA (1) authenticity
& federation between operators

m: +47 9083 8066 Telenor $\Rightarrow$ Josef Noll

signature & encrypted email (2)

Attack on GRX

GRX

- British Secret Service
 - looked for people Belgarons
 - "inject a virus" - faked LinkedIn
 - captured http call, inserted their LinkedIn
- insert program on all mobile
binary code update

