

Cwi.unih.no/wiki/LINK4250

Security Architecture

- “The design artifacts that describe how the security controls (= security countermeasures) are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system’s quality attributes, among them confidentiality, integrity, availability, accountability and assurance.”
- – Open Security Architecture (OSA)

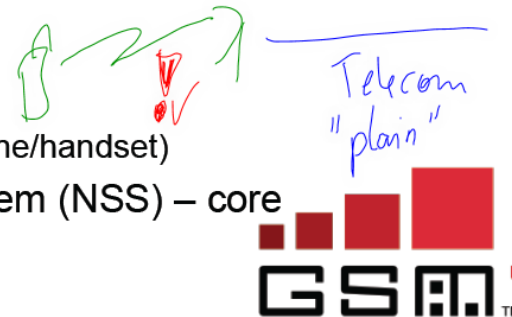
99.9%
parameter
85%
70%

[source: Lars Strand, 2011]

Chapter 19:

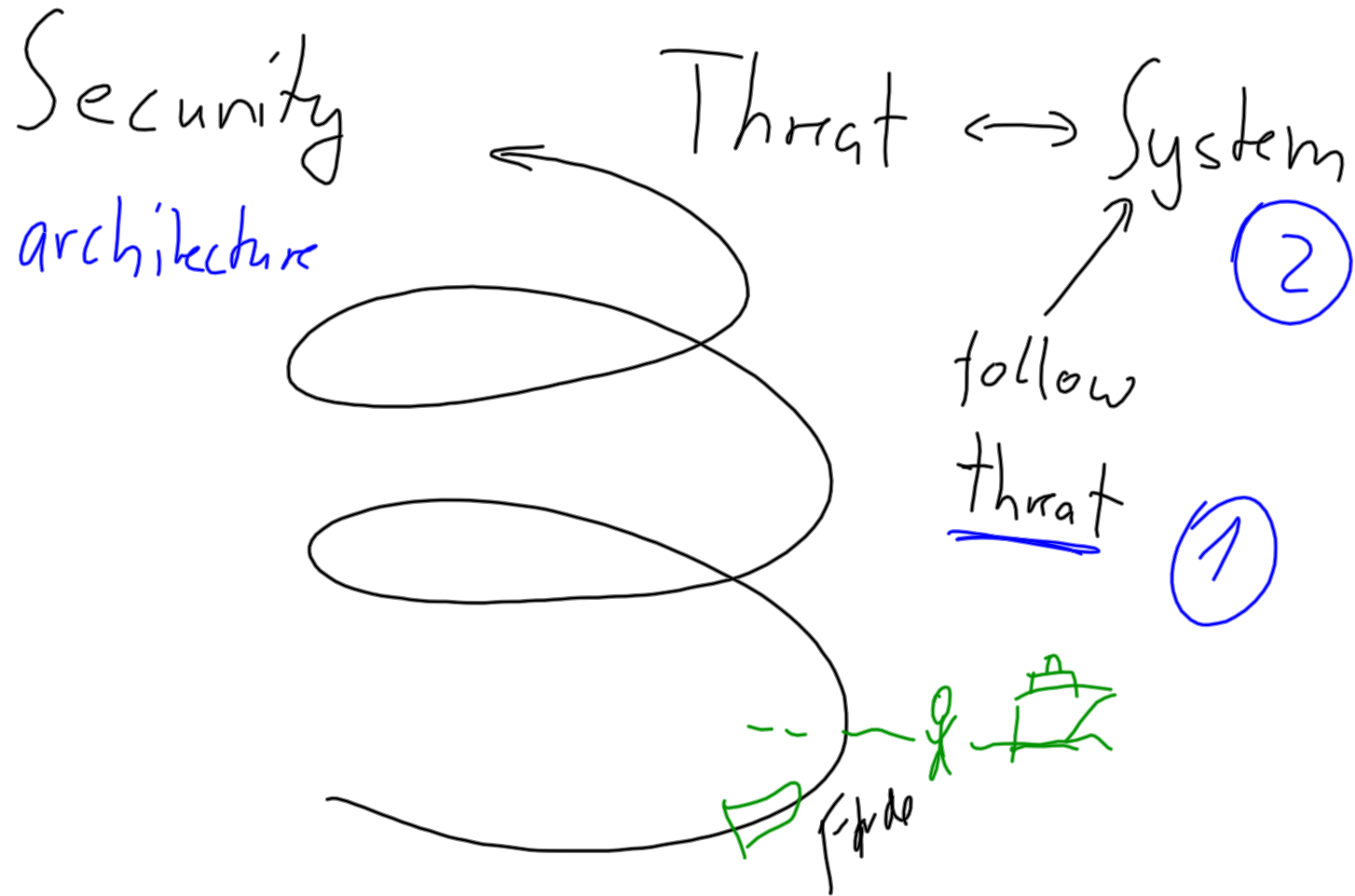
Mobile systems: GSM

- Developed in the late 1980s, deployed 1992.
 - Norway a key developer and inventor
- Today: Cover 80% of world population (5+ billion users!), gsmworld.com.
- GSM security goal: “as secure as the wire”
- GSM network consists of several network elements
 - Radio Subsystem (RSS)
 - Base station Subsystem (BSS)
 - Mobile Equipment (ME) (cell phone/handset)
 - Network and Switching Subsystem (NSS) – core network
 - Operation Subsystem (OSS)



[source: Lars Strand, 2011]

Chapter 19:

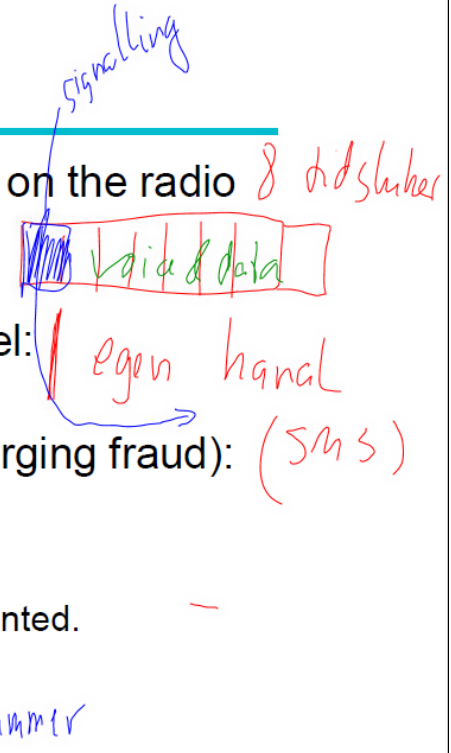


Security Goals

- 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). *Western Europe*
 - Subscriber authentication (IMSI, TMSI).
- Theft of end device:
 - Identification of MS (IMEI), not always implemented.

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): (SMS)
 - Subscriber authentication (IMSI, TMSI).
- Theft of end device:
 - Identification of MS (IMEI), not always implemented.



IMT 2G $\longleftrightarrow$ GSM, IS 95
3G $\longleftrightarrow$ UMTS

IMT-A
ITU 3.9G
Brand 4G

100 Mbit/s
1 Gbit/s

high mobility
low mobility, stationary

LTE

4G "saig"
Winmax
802.16e

Family of radio
interfaces

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
- ...

Trusted Element
nono SIM
virtual SIM

utlandet

GSM: Problems

- Focus on *access security*
 - Confidentiality terminated at the base stations
 - Weak operator network protection
 - Example: Traffic to/from BS and AuC should be protected!
- “Security through obscurity” - A3/A5/A8 eventually leaked
- Algorithms not resistant to cryptanalysis attack
 - A5/1 can “easily” be broken – today gradually replaced by A5/3
 - No public scrutiny during development
- Lack of user visibility
 - User do not know if/what encryption is used
- Difficult to upgrade cryptographic algorithms
 - But not in theory? Resides on the SIM card
- Authentication: One-way authentication only
 - Only MS to BS and not BS to MS.
- + many more..

[source: Lars Strand, 2011]

Chapter 19:

SIM: Subscriber Identity Module

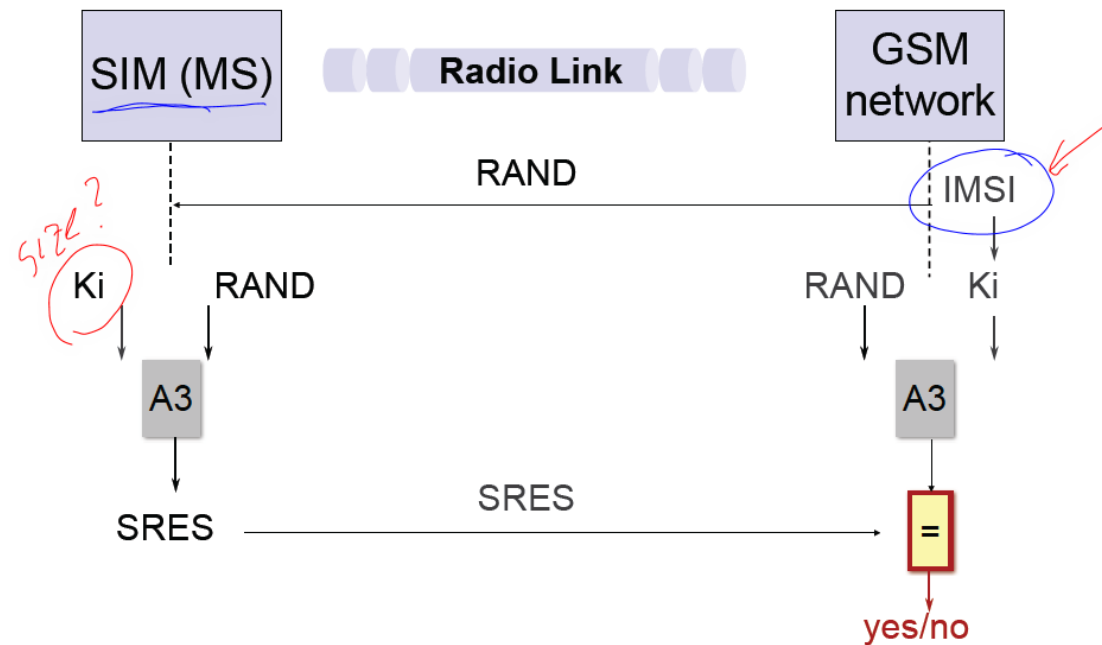
- Smart card (processor chip card) in MS:

- Current encryption key Kc (64 bits)
- Secret subscriber key Ki (128 bits)
- Algorithms A3 and A8
- IMSI
- TMSI
- PIN, PUK
- Personal phone book
- SIM Application Toolkit (SIM-AT) platform
- ...

Chapter 19:

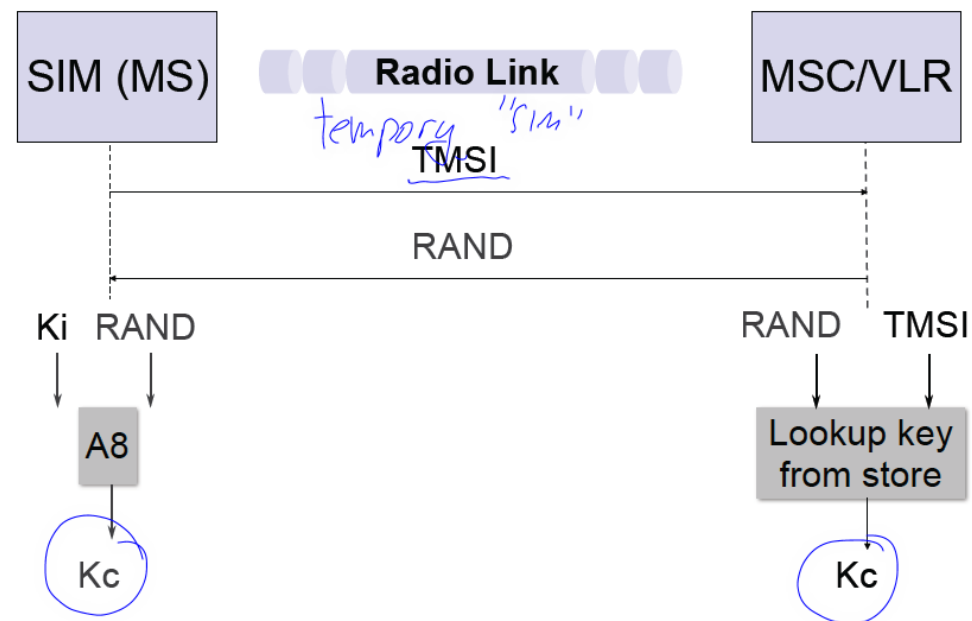
GSM Subscriber Authentication

Trusted



Chapter 19:

GSM Subscriber Authentication



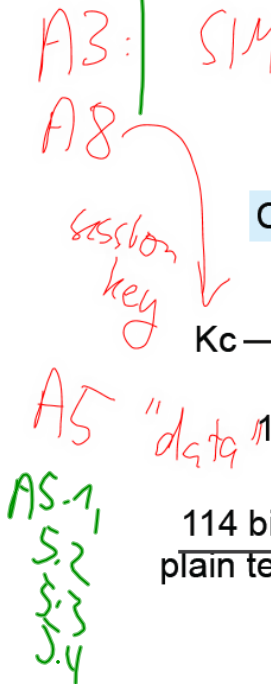
Chapter 19:

Cryptographic Algorithms: A3/A8

- Algorithms A3 and A8 shared between subscriber and home network; thus each network could choose its own algorithms.
 - Algorithms A3 and A8 at each PLMN operator's discretion.
 - GSM 03.20 specifies only the formats of their inputs and outputs; processing times should remain below a maximum value (A8: 500 msec).
- COMP128: one choice for A3/A8; attack to retrieve Ki from the SIM (→ cloning) possible; not used by many European providers.

Chapter 19:

standard
MSA



Chapter 19:

Bio metric passport

"legal"
= papir

RFID

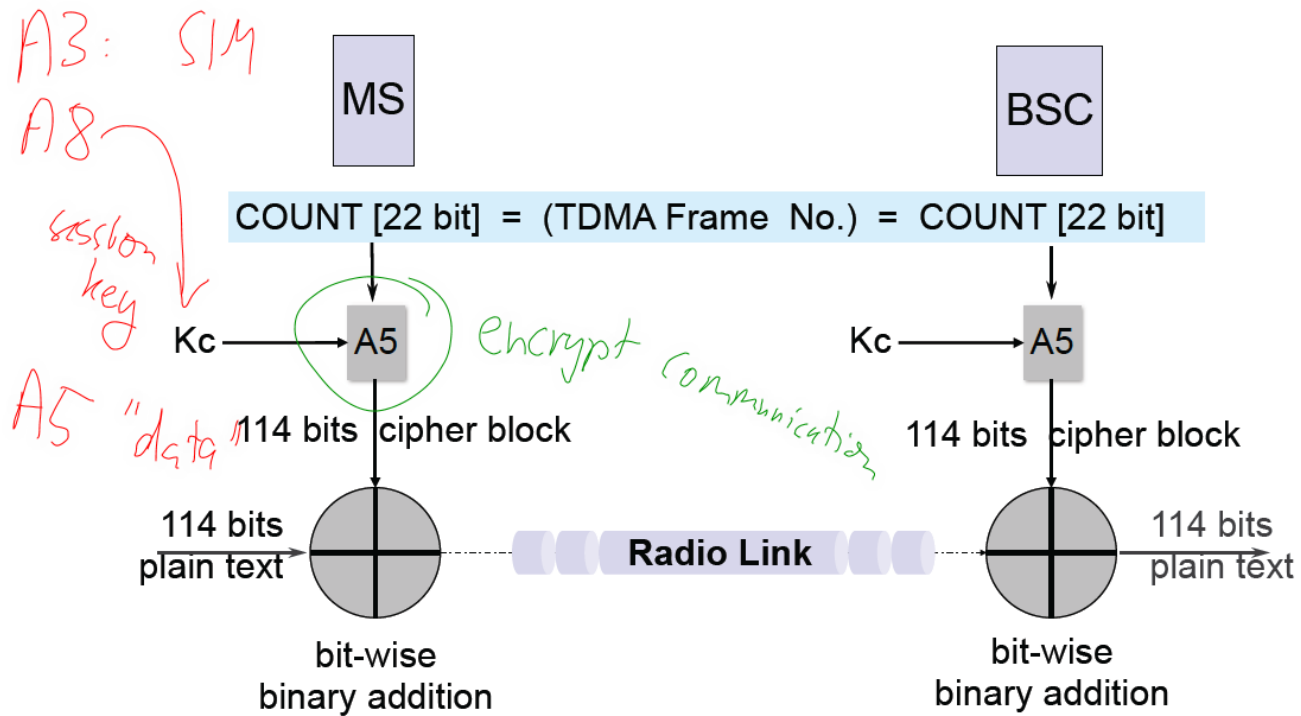
lev 1: passport data

pass nr + u/tørsket + fødselsdato
| | |
pass nr + u/tørsket + fødselsdato

lev 2: biometric (fingerprint)

ingen enighet! - personvern

MS/BSC Encryption



Chapter 19:

UMTS – Introduction

- Work on 3rd generation mobile communications systems started in the early 1990s; first release of specifications in 1999.
- Standards organization: 3G Partnership Project (3GPP).
 - ETSI (Europe)
 - ARIB (Japan)
 - TTC (Japan)
 - T1 (North America)
 - TTA (South Korea)
 - CCSA (China)
- Mission: Drive forward standardization of 3G systems.

Handwritten notes:

- 2012 (green)
- 2002 (red)
- IS95 - CDMA 2000 60% (blue)
- CDMA (blue)
- UTR SIM (red)
- med SIM (red)
- GSM X (blue)
- UMTS (blue, circled)
- LTE (green)
- 40% (green)
- SIM (red, underlined)

Chapter 19:

Unik.no
cwi.unik.no/images/UNIK
Zwipe | Biometric Card
cwi.unik.no/images/UNIK4250-L7-MobileSecurity.pdf

Security architecture: UMTS

Threats/attacks	Security services	Security mechanisms
False BST	Authentication	Mutual authentication mechanism (challenge-response with a shared secret)
Eavesdropping (Poor GSM encryption)	Confidentiality	Encryption of signaling and call content
Data sent in clear in the operator network	Confidentiality	Encryption and integrity protection of data, to also cover operator network

Conclusion: UMTS has a decent security architecture

- * Extensive threat and attack analysis
- * Open development
- * Modular (“flexible”) security mechanisms
 - “cryptographic core” can be replaced by operator
- * Target: End-user, Operators and law enforcements

[source: Lars Strand, 2011]

Chapter 15:

LTE Advanced (4G)

(26 | 36)

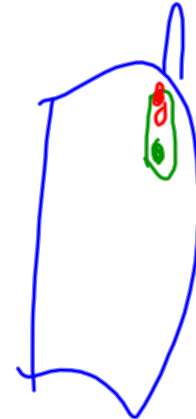
GSM & UMTS

umts 5m
GSM: 900, 1800 MHz
UMTS: 1900, 2100
LTE: 2600

stör
sänd

WCDMA + TD-SCDMA i UMTS

dårlig säkerhet



Unik.no x cw.uni.no/images/UNIK x Zwipe | Biometric Card x

cwi.uni.no/images/UNIK4250-L7-MobileSecurity.pdf

Security architecture: LTE

Threats/attacks	Security services	Security mechanisms
Eavesdropping	Data confidentiality	IPSec
Modification of content	Data integrity	IPSec
Impersonation	Authentication	EAP-AKA
Denial of service, roaming, performance	Availability service	?, fast re-authentication? different access network?

Security Architecture
Mobile → IP

Conclusion: LTE has a decent security architecture

- * Built on and improved over UMTS
- * All-IP architecture a challenge
- * ~~Untrusted non-3GPP~~ access a challenge
- * Performance might be an issue

50

[source: Lars Strand, 2011]