http://cwi.unik.no/wiki/UNIK4250

http://cwi.unik.no/wiki/Mobile_network_security

Pensum (read before)	
References (further info)	Dieter Gollmann, "Computer Security", Ch. 19. http://www.wiley.com/college/gollmann
Keywords	NMT, GSM, UMTS, LTE, Network Security, Mobile Security

this page was created by Special:FormEdit/Lecture, and can be edited by Special:FormEdit/Lecture/Mobile network security.

Lecture slides

- Media:UNIK4250-L7-MobileSecurity.pdf - slides
- Media:Dabrowski_ISMI_Catch_me_Catchers.pdf
- Remote connection through Video_conference, Call UNIK at room IP 301: IP adresse 193.156.97.18;

Josef Nolli Chris 1st

Kyrre

Joakim Sergej

Tuan

Liv

Torjus (NTNU) Mats Olav

Endre

USA

IS95 → WCDMA 70%

no ~~SIM~~

CDMA 2000

Economics

3G

2G

1G

300%

Europe

GSM 2G → WCDMA 90%

SIM 3G

SIM Card

The SIM card

is the major security element for mobile systems. It carries a.og. a secret subscriber key *Ki*, the algorithms A3 and A8, and the international mobile subscriber identity (IMSI), and a tempory mobile subscriber identity (TMSI). All these elements are used in the subscriber identification to the network and the encryption of the communication with the network.

During purchase of the SIM a link between the *Ki* and the *IMSI* is performed in the authentication center (AUC), allowing to decouple the *phone number of the user* from the identity of the SIM.

A modern SIM card, including the near-field-communication (NFC) pin and a high-speed (8-12 Mbit/s) USB interface, can act as *(i)* payment and access card and *(ii)* decrypt multimedia content on the SIM card.

Major Security Algorithms

The main functionality of the three major security algorithms A3, A5 and A8

A3 is used as an authentication algorithm, authenticating the SIM card (*the user*) to the network. This is done through generating a response based on a random *RAND* number from the network and combine it with the *Ki* key through the A3 algorithm. The resulting *SRES* is then sent back to the network to check if the results calculated in the network matches the result calculated in the SIM.

A5 for signalling data and user data encryption. The A5/1 algorithm is a stream cipher and was kept confidential, not even exported to regions in Eastern Europe.

A8 is a ciphering key generating algorithm and is used to generate the session key used by the A5 algorithm to encrypt communication between a mobile phone and the base station.

Biometric passport

1. pass #
2. creation date
3. ...

decryption key

digital info of pass

fingerprint / biometrics

Secret?

Threat environment

GSM

1. Vulnerability: Cloning
   - GSM security service: Authentication
   - GSM security mechanism: Authentication mechanism
2. Vulnerability: Content (voice) sent in clear
   - GSM security service: Call content confidentiality
   - GSM security mechanism: A5/1, A5/2, A5/3, A5/4
3. Vulnerability: Spying (subscriber location tracking)
   - GSM security service: Identity confidentiality
   - GSM security mechanism: Location security (TMSI)

[source: Lars Strand, 2011] Chapter 19: 13

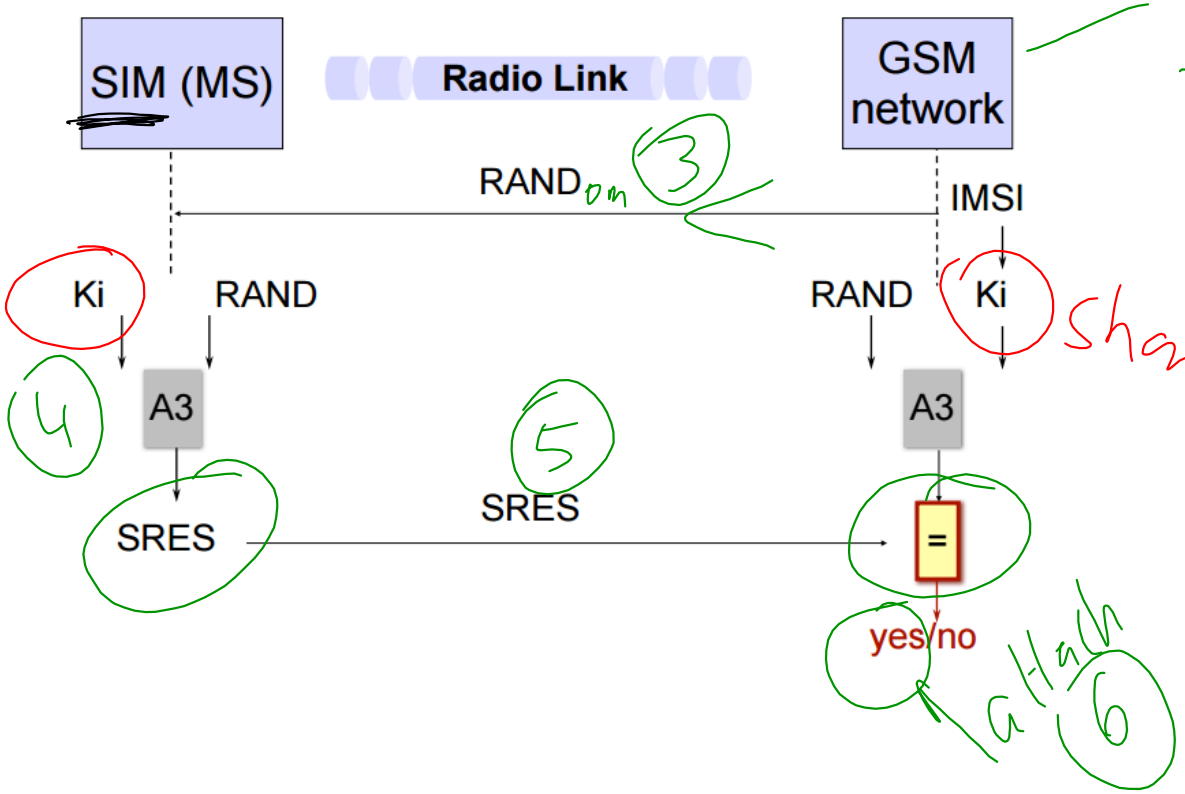
SIM: Subscriber Identity Module

- 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
  - ...

Cryptography in GSM

- A3 authentication algorithm
- A5 signalling data and user data encryption algorithm
- A8 ciphering key generating algorithm

GSM authentication



1) broadcast
2) Mobile "I want to connect"
3
4
5
6
shared secret

GSM – Summary

- Voice traffic encrypted over the radio link (A5)
  - but calls are transmitted in the clear after the base station.
- Optional encryption of signaling data
  - but ME can be asked to switch off encryption.
- Subscriber identity separated from equipment identity.
- Some protection of location privacy (TMSI).
- Security concerns with GSM:
  - No authentication of network: IMSI catcher pretend to be BTS and request IMSI.
  - Undisclosed crypto algorithms.

Security architecture: UMTS

Main tasks of the security architecture (Køien, 2004):

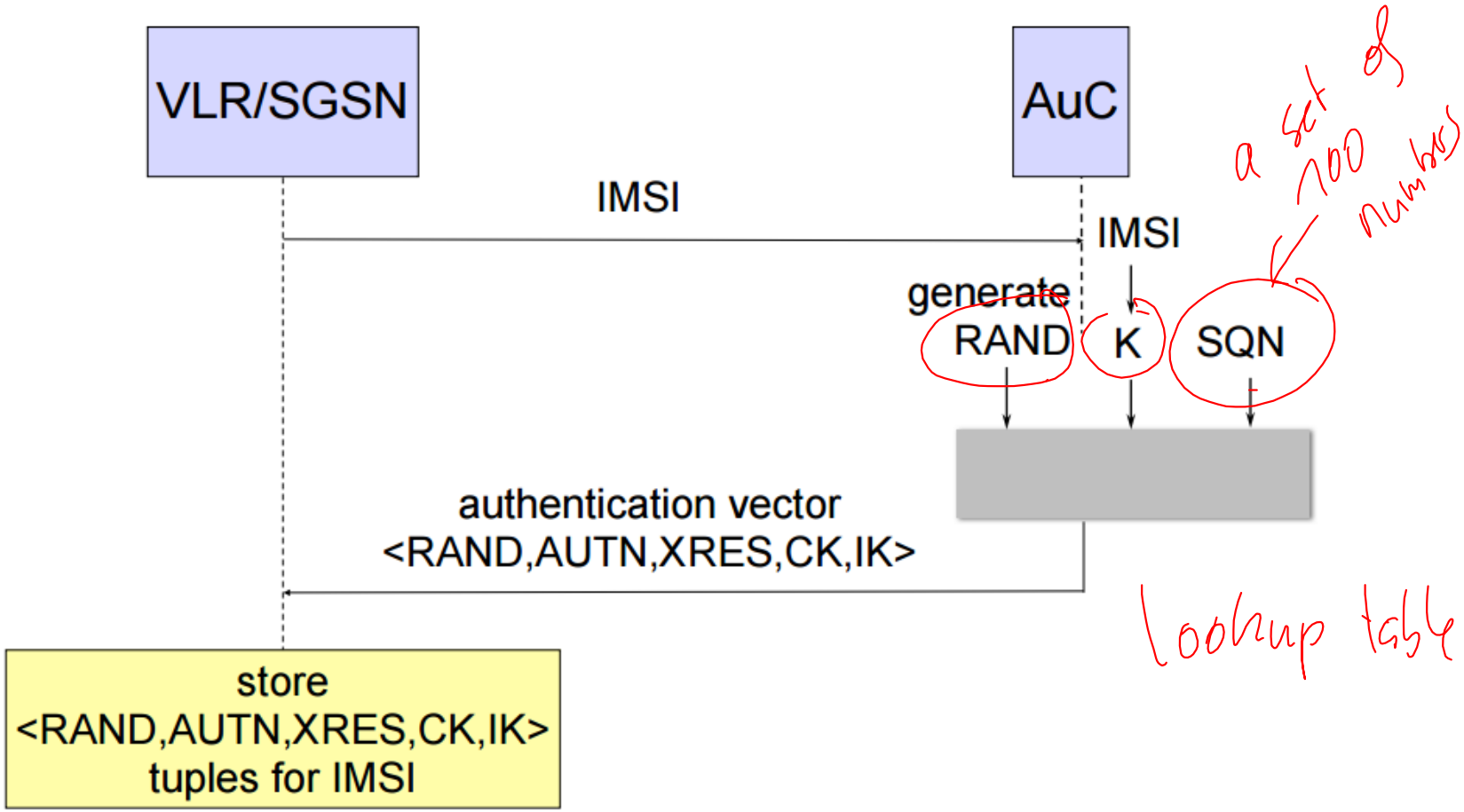
1) Authentication
   - GSM vulnerability: False BST
   - UMTS: Mutual authentication, new algorithm (MILENAGE)
2) Replace algorithms/New key generation
   - GSM vulnerability: Inadequate algorithm
   - UMTS: New algorithm (KASUMI)
3) Encryption/integrity protection
   - GSM vulnerability: Cipher keys and auth data sent in clear in operator network
   - UMTS: Extend confidentiality and integrity service to the operator network

UMTS AKA

"Authentication and Key Agreement"

- Home network (AuC) and USIM (Universal Subscriber Identity Module) in user equipment (UE) share secret 128-bit key K.
- AuC can generate random challenges RAND.
- USIM and AuC have synchronized sequence numbers SQN available.
- Key agreement on 128-bit cipher key CK and 128-bit integrity key IK.
- AMF: Authentication Management Field.

(ISIM) → SQN


VLR/SGSN
AuC
IMSI
IMSI
generate
RAND
K
SQN
a set of 100 numbers
authentication vector
<RAND,AUTN,XRES,CK,IK>
lookup table
store
<RAND,AUTN,XRES,CK,IK>
tuples for IMSI

- 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

- 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

IPsec

[source: Lars Strand, 2011]

break → 10:50

3 groups analyse paper IMSI

20min

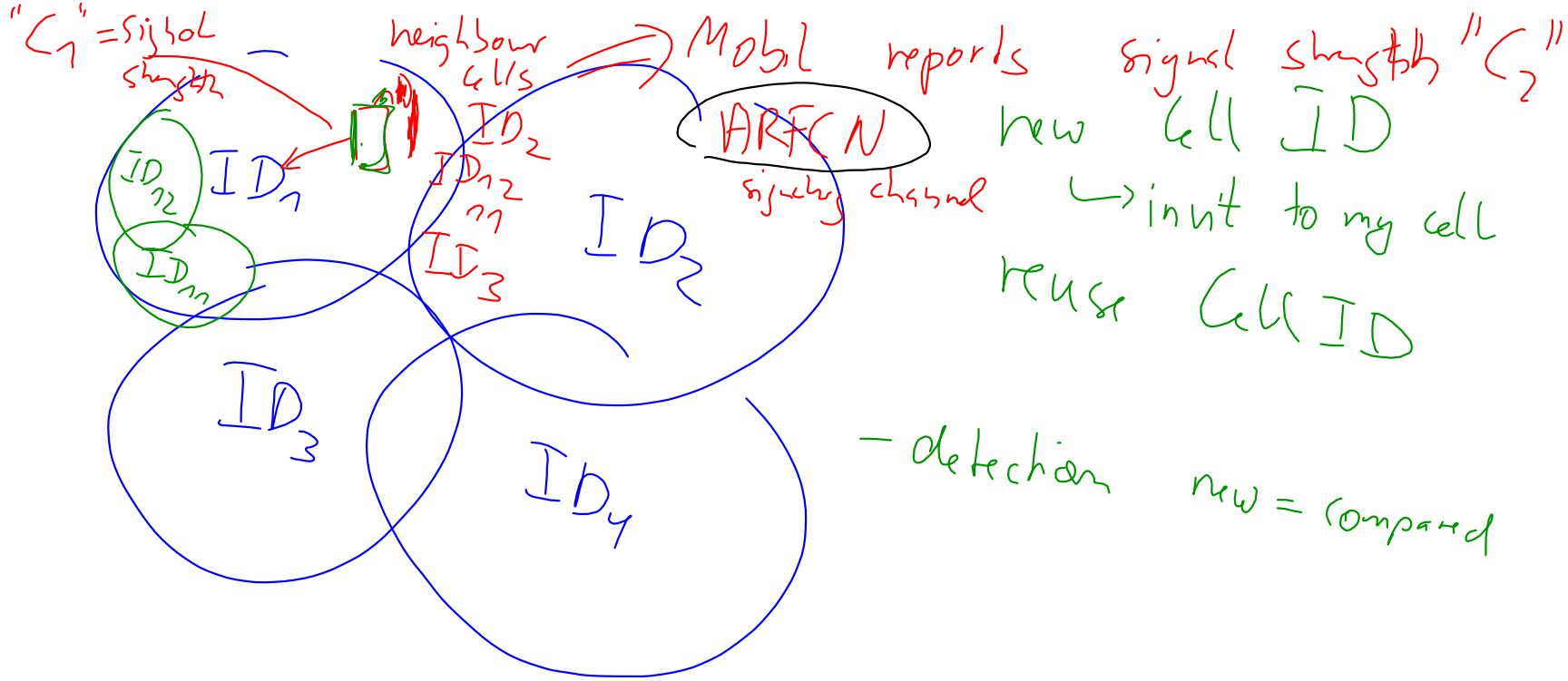
report & discuss on IMSI catcher

10 min – what information is used to identify an IMSI catcher

– Questions

- neighbour list / identification
  - selected jamming
  - denial of service
  - IMSI identification
- ARFCN = same freq
- mobile network code
- random cell ID
- mgt signal strength
- C1, C2 value modification
- geographic location, history
- base station capabilities

- anomaly detection
  no encryption


"C1" = signal strength
neighbour cells
Mobil reports signal strength "C2"
ARFCN
signaling channel
new Cell ID
↳ inst to my cell
reuse Cell ID
- detection new = compared
ID1
ID2
ID3
ID4
ID12
ID13
ID21
ID23
ID31
ID32

Identification Mode.

As a phone is lured into the fake cell, the worldwide unique identifiers such as IMSI and IMEI are retrieved and the phone is sent back to its original network via denying its original *Location Update Request* with an *Location Update Reject*-Message. This procedure typically takes less then two seconds, whereas attracting the phone can take minutes. No other information besides the identification numbers is retrieved.

A law enforcement agency can then apply for a warrant[1] and access the call- and meta information of a subject via the mobile network operator. This considerably saves the agency working hours, as no one has to operate the IMSI Catcher over the whole period of observation and follow the subject in its every move.

Other attackers can use this mode for user tracking purposes or to lookup the exact phone model based on the IMEI to better tailor future attacks.

Camping Mode.

The phone is held in the cell of the IMSI Catcher and content data is collected. Traffic is forwarded to the genuine network so that the victim stays unaware of the situation.

IMSI Catcher users that do not have time for for a warrant or can't acquire a warrant (e.g. because they operate outside the law) use this method. It will also gain importance as A5/3 and A5/4 are introduced into GSM networks, making passive snooping attacks on the broken A5/1 and A5/2 ciphers useless. In UMTS networks, phones are additionally downgraded to GSM and its less secure ciphers.

900 GSM

1800 GSM

apoi LTE

2100 UMTS 15MHz

2650 LTE