Security functions in mobile communication systems

Dr. Hannes Federrath
University of Technology Dresden

- Security demands
- Security functions of GSM
- Known attacks on GSM
- Security functions of UMTS
- Concepts for hiding locations of mobile users
Security deficits of existing mobile networks

• Example of security demands: Cooke, Brewster (1992)
  – protection of user data
  – protection of signaling information, incl. location
  – user authentication, equipment verification
  – fraud prevention (correct billing)

• Security deficits of GSM (selection)
  – Only symmetric cryptography (algorithms no officially published)
  – Weak protection of locations (against outsiders)
  – No protection against insider attacks (location, message content)
  – No end-to-end services (authentication, encryption)

• Summary
  – GSM provides protection against external attacks only.
  – “…the designers of GSM did not aim at a level of security much higher than that of the fixed trunk network.” Mouly, Pautet (1992)
Security functions of GSM

• Overview
  – Subscriber Identity Module (SIM, smart card)
    • Admission control and crypto algorithms
  – Authentication (Mobile station → network)
    • Challenge-Response-Authentication (A3)
  – Pseudonymization of users on the air interface
    • Temporary Mobile Subscriber Identity (TMSI)
  – Link encryption on the air interface
    • Generation of session key: A8
    • Encryption: A5
**Challenge-Response-Authentication**

- **When initialized by the mobile network?**
  - Location Registration
  - Location Update when changing the VLR
  - Call Setup (both directions)
  - Short Message Service

- **Protocol**

```
MS

max. 128 Bit

Ki

A3

MSC/VLR/AuC

128 Bit

Authentication Request

RAND

32 Bit

Authentication Response

SRES

Random Generator

Ki

A3

Authentication Result
```
**Challenge-Response-Authentication**

- **Algorithm A3**
  - Implemented on SIM card and in Authentication Center (AuC)
  - Cryptographic one way function A3:
    \[ SRES' = A3(Ki, RAND) \quad (Ki: \text{individual user key}) \]
  - Interfaces are standardized, cryptographic algorithm not standardized

- **Specific algorithm can be selected by the network operator**
  - Authentication data (RAND, SRES) are requested from AuC by the visited MSC
  - visited MSC: only compares \( SRES = SRES' \)
  - visited MSC has to trust home network operator

![Diagram of Challenge-Response-Authentication process]
Attacks – Telephone at the expense of others

• **SIM cloning**
  – Weakness of authentication algorithm

• **Interception of authentication data**
  – Eavesdropping of internal communication links

• **IMSI catcher**
  – Man-in-the-middle attack on the air interface
**SIM cloning**

- **Scope**
  - Telephone at the expense of others
  - Described by Marc Briceno (Smart Card Developers Association), Ian Goldberg and Dave Wagner (both University of California in Berkeley)
  - [http://www.isaac.cs.berkeley.edu/isaac/gsm.html](http://www.isaac.cs.berkeley.edu/isaac/gsm.html)
  - Attack uses a weakness of algorithm COMP128, which implements A3/A8
  - SIM card (incl. PIN) must be under control of the attacker for at least 8-12 hours

- **Effort**
  - Approx. 150,000 calculations to determine Ki (max. 128 bit)
  - 6.25 calculations per second only, due to slow serial interface of SIM card
Interception of authentication data

• **Scope**
  – Telephone at the expense of others
  – Described by Ross Anderson (University of Cambridge)
  – Eavesdropping of unencrypted internal transmission of authentication data (RAND, SRES) from AuC to visited MSC

• **Weakness**
  – GSM standard only describes interfaces between network components.
  – They forgot the demand for internal encryption.
  – **Microwave links** are widely used for internal linkage of network components.
No encryption of internal links

originator device → radio transmission (encrypted) → BTS → fixed network

domain of network operator 1

Gateway-MSC

Database

terminating device → radio transmission (encrypted) → BTS → fixed network (not encrypted)

domain of network operator 2
**Interception of authentication data**

- **faked mobile station**
  - (any message)
  - TMSI
  - Auth. Request RAND
  - Auth. Response SRES
  - Ciphering Mode Cmd.
  - Start Ciphering
  - Ciphering Mode Compl.

- **air interface**
  - Lookup
  - store auth. info
  - Kc
  - A5

- **visited network**
  - mapping TMSI–IMSI
  - store auth. info
  - SRES’
  - auth. res.
  - Kc
  - A5

- **microwave link (not encrypted)**
  - Provide Auth. Info
  - IMSI
  - Authentication Information
  - RAND, SRES, Kc

- **home network**
  - RAND Ki
  - A3+A8

Interception of Authentication Triplets RAND, SRES, Kc
**IMSI-Catcher**

- **Scope**
  - Identities of users of a certain radio cell
  - Eavesdropping of communications
  - (Telephone at the expense of others)

- **Man-in-the-middle attack (Masquerade)**

- **Weakness**
  - No protection against malicious or faked network components

Note: The IMSI Catcher sends its “location area identity” with a higher power than the genuine.
Universal mobile telecommunication system (UMTS)

• Security functions of UMTS ...
  ... have been »inspired« by GSM security functions

• From GSM
  – Subscriber identity confidentiality (TMSI)
  – Subscriber authentication
  – Radio interface encryption
  – SIM card (now called USIM)
  – Authentication of subscriber towards SIM by means of a PIN
  – Delegation of authentication to visited network
  – No need to adopt standardized authentication algorithms

• Additional UMTS security features
  – Enhanced UMTS authentication and key agreement mechanism
  – Integrity protection of signaling information (prevents false-base-station attacks)
  – New ciphering / key agreement / integrity protection algorithms
    … and a few minor features
UMTS Security Architecture

Ciphertext/integrity protection
- cipher key CK, integrity key IK
- ciphering function f8
- integrity function f9

User authentication
- authentication key K,
- authentication function f1, f2

Network authentication
- key generation function f3, f4, f5
- sequence number management SQN

USIM  UMTS Subscriber Identity Module
MS   Mobile Station
RNC  Radio Network Controller
VLR  Visitor Location Reg.
SGSN  SG Serving Network
HLR  Home Location Register
AuC  Authentication Centre
Generation of authentication vectors

\[ \text{AUTN} := \text{SQN} \oplus \text{AK} \parallel \text{AMF} \parallel \text{MAC} \]

\[ \text{AV} := \text{RAND} \parallel \text{XRES} \parallel \text{CK} \parallel \text{IK} \parallel \text{AUTN} \]

SQN  Sequence number
RAND  Random number
AMF  Authenticated Management Field
K  Secret Key
MAC  Message authentication code
XRES  Expected response
CK  Cipher key
IK  Integrity key
AK  Anonymity key
AUTN  Authentication token
AV  Authentication vector

[...]  # of bits
Authentication function in the USIM

Verify MAC == XMAC

Verify that SQN is in the correct range

SQN  Sequence number
RAND Random number
AMF  Authenticated Management Field
K Secret Key
MAC  Message authentication code
XMAC Expected MAC
RES  Response
CK Cipher key
IK Integrity key
AK Anonymity key
AUTN Authentication token

[...] # of bits
Security mode setup procedure

- **User Identity (IMSI or TMSI), KSI**
- **Decision about AKA**
- **AKA (optional)**
- **Allowed security algorithms, CK, IK**
- **Select sec. algorithms**
- **Start Integrity Protection**
- **Security Mode Command (incl. UE Sec. Cap., selected alg., FRESH)**
- **Control of UE Sec. Cap. Integrity check Start Integrity Protection Start Ciphering**
- **Security Mode Complete**
- **Integrity check**
- **Start Ciphering**
- **Security Mode Complete**

- **Prevents Replay attacks**

Abbreviations:
- MS: Mobile Station
- RNC: Radio Network Controller
- VLR: Visitor Location Reg.
- SGSN: SG Serving Network
- UE: ?
- STARTCS: Start circuit switched
- STARTPS: Start packet switched
- KSI: Key Set Identifier
- AKA: Authentication and Key Agreement
- CK: Ciphering Key
- IK: Integrity Key
- FRESH: prevents Replay attacks
Cipher algorithm f8

- Combination of Output Feedback mode (OFB) and counter mode
- First encryption under CK’ prevents chosen plaintext attacks (initialization vector is encrypted, KM: key modifier)

Key stream is XORed with MESSAGE block
**Integrity algorithm f9**

- ISO/IEC 9797-1 (MAC algorithm 2)
- Sender and receiver use f9
- Receiver verifies $\text{MAC} == \text{XMAC}$

Diagram:

COUNT || FRESH

MESSAGE[0]…MESSAGE[63]

MESSAGE[64]…MESSAGE[127]

Final Message Block (padded)

IK → KASUMI

IK → KASUMI

IK → KASUMI

IK → KASUMI

IK' → KASUMI

MAC or XMAC (left 32 bits)
**Protection of locations**

- **Mobile user**
  - wishes to be reachable at his current location.
  - He won’t be localizable by outsiders and the network operator unless the explicitly gives his permission.

- *There is no mobile network that fulfills this demand.*
Protection of locations

- **GSM (Global System for Mobile Communication)**
  - Distributed storage at location registers
    - Home Location Register (HLR)
    - Visitor Location Register (VLR)
  - Network operator has global view on location information

- **Tracking of mobile users is possible**
A. Trust into the mobile station only
   A.1 Broadcast method
   A.2 Group pseudonyms

B. Additional trust into a private fixed station
   B.1 Trusted address translation and broadcast
   B.2 Reduction of broadcast areas
   B.3 Explicit trustworthy storage of locations
   B.4 Temporary pseudonyms (TP method)

C. Additional trust into a trusted third party
   C.1 Trust Center
   C.2 Co-operating chips
   C.3 Mobile Communication-MIXing
Overview: Broadcast

- No storage of locations and global paging of mobile users
Overview: Broadcast

- No storage of locations and global paging of mobile users

- Immense costs for bandwidth...
Broadcast in general

Radio, TV, Paging services, ...

Local choice, Unobservable receiving

Broadcast srv.
Overview: Trustworthy storage

- Replace databases by trusted devices in the fixed network
**Overview: Trustworthy storage**

- Replace databases by trusted devices in the fixed network

- Every location updating needs communication with trusted station.

- Question: How can we reduce cost of location updating?
Overview: Trustworthy storage

- Tempory Pseudonyms (TP method)

Can we do this without a trusted fixed station?
Overview: Mobile Communication-MIXing

- Covered storage of location information

A MIX hides the communication relation between:
- HLR and VLR
- VLR and location area
**Implicit Addresses**

- **First contact:** Covered Implicit Address CIA
  - Recipient publishes public encryption key $c$
  - Sender creates $\text{CIA} := c(R,S,M)$
    - Redundancy $R$
    - Seed $S$ of a pseudo-random generator $\text{PRG}$
    - Message $M$ (optional, may contain symmetric key $k$)
  - Recipient decrypts *all* received messages with private key $d$
    - Finds correct $R$ for own messages only

- **Following addressing:** Open Implicit Address OIA
  - $\text{OIA}_{i+1} := \text{PRG}(i, \text{seed})$ \((i = 0,1,2,...)\)
  - Sender:
    - Calculates next $\text{OIA}$
    - Encrypts message (optional) $M$ under $k$
    - Sends $\text{OIA, M}$
  - Receiver: Associative memory of all valid $\text{OIA}s$ to recognize own messages
Broadcast method

• Performance

\[ T_v = \frac{2 \cdot \frac{B}{B} \cdot n \cdot \frac{B}{B}}{2 \cdot \frac{B}{B} \cdot (\frac{B}{B} \cdot n \cdot \frac{B}{B})} \]

\[ \frac{B}{B} = \frac{b}{B} \]

\[ T_v = 0.5 \text{ s} \]

- covered implicit address: \( B = 500 \text{ bit} \)
- open implicit address: \( B = 50 \text{ bit} \)
- minimal coding: \( B = \lceil d(n) \rceil \)
Performance: Message lengths on the air interface

- **Mobile Terminated Calls**

  GSM reference
  B.3 explicit trustworthy storage
  B.4 TP method
  C.2 cooperating chips

![Message intervals on the Air interface in bit for Mobile Terminated Calls](image_url)
Performance: Message lengths on the air interface

- **Location Update**

  GSM reference
  B.3 explicit trustworthy storage
  B.4 TP method
  C.2 cooperating chips

![Graph showing message intervals in bit for Location Updating]

- Message intervals in bit for Location Updating
  - GSM: 328
  - B.3: 328
  - B.4: 280
  - C.2: 398
Security of mobile communication

• **Conclusion**
  – Protection of locations can be technically realized
  – However, there is a demand for legal enforcement

• **More information**