Security of Mobile Systems

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de
Contents

- Introduction
- Security functions of GSM
  - Basics and architecture of GSM
  - Security functions
  - Mobility management functions
  - Location based systems
  - Call management
- Security functions of further mobile Systems
  - UMTS
  - Bluetooth
  - WLAN
- Protection of locations in mobile systems
  - GSM
  - Mobile IP

(extended slide set only)
Introduction
Mobile network communication vs. fixed networks

- Users are moving / roaming

- On air interface:
  - Limited bandwidth
  - Errors (bit failures, burst errors)
  - Communication breaks (lost connectivity)

- New threads
  - Sniffing / eavesdropping of wireless communication
  - Location finding (direction-finding, sense-finding)
Sensors

- Sensors in mobile devices make new apps possible
  - GPS
  - WiFi
  - Bluetooth
  - Microphones
  - Cameras
  - Motion sensors
  - Adapters for more sensors
    - Personal: heart rate monitors
    - Environmental
      - Cars: CAN bus adapters
      - Houses: smart meter, heater, alarm system

... and new tracking possibilities
Mobile communication – Classification

1. Types of Mobility

- Terminal Mobility:
  - Example: Mobile Phone
    - Wireless communication
    - Mobile device

- Personal Mobility:
  - Example: Public Terminals
    - Mobile user
    - Location-independent address
  - Special kind of personal mobility: Session Mobility:
    - «Session Freezing» and reactivation in other location and/or device
Mobile communication – Classification

2. Wave lengths
   – Radio [waves] (f = 100 MHz up to several GHz)
   – Light [waves] (infrared)
   – Sonar [waves] (e.g. acoustic coupler)

3. Cell sizes
   – Pico cells d < 100 m
   – Micro cells d < 1 km
   – Macro cells d < 20 km
   – Hyper cells d < 60 km
   – Overlay cells d < 400 km

Further classifications
   – Point-to-point communication, Broadcast (paging services)
   – Analogue, Digital systems
   – Simplex, Duplex communication channels
Examples for mobile Systems

- Speech communication = mass market
  - 1. Generation: analogue
    - C-Netz, Cordless Telephone, AMPS
  - 2. Generation: digital
    - GSM, DCS-1800, DECT
  - 3. Generation: service integration
    - UMTS/IMT-2000/FPLMTS

- Satellite services
  - Iridium, Inmarsat, Globalstar, Odyssey
  - GPS (Global Positioning System), Galileo (European satellite navigation system), GLONASS

- Internet (Mobile IP)
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)

- General security demands
  - Confidentiality
  - Integrity
  - Availability

- Mobile network cannot be considered trustworthy
The attacker model defines the maximum strength of an adversary regarding a specific security mechanism.

- Protection against an omnipotent attacker is impossible.

Aspects of an attacker model:

- Roles of attacker (Outsider or Insider, ...)
  - combined roles also
- Dissemination of attacker
  - Which stations or channels can be controlled?
- Behavior of attacker
  - passive / active, observing / modifying
- Computing power of attacker
  - unlimited: information theoretic
  - limited: complexity theoretic
Attacker model (concrete)

- **Outsiders**
  - Passive attacks only (confidentiality)
- **Insiders**
  - Passive and active data modification attacks (integrity)
- **Insiders and outsiders**
  - Denial of Service attacks on air interface

- **Mobile device**
  - Trustwothy
- **Network components**
  - Safe against outsiders, but not against insiders
- **Air interface**
  - Location-finding (insiders and outsiders)
Global System for Mobile Communication (GSM)
Global System for Mobile Communication (GSM)

- Key features of Global System for Mobile Communication
  - Very high international mobility
  - Worldwide caller ID
  - High geographic coverage
  - High user capacity
  - High speech quality
  - Advanced error correction mechanisms
  - Advanced resource allocation strategies (e.g. FDMA, OACSU)
  - Priority emergency call service
  - Built-in Security functions
    1. Subscriber Identity Module (SIM, smart card)
    2. Authentication (Mobile station → network)
    3. Pseudonymization of users on the air interface
    4. Link encryption on the air interface
Architecture of GSM

OMC: Operation and Maintenance Center
HLR: Home Location Register
AuC: Authentication Center
EIR: Equipment Identity Register
MSC: Mobile Switching Center
GMSC: Gateway MSC to fixed network
VLR: Visitor Location Register
BSS: Base Station Subsystem
BSC: Base Station Controller
BTS: Base Transceiver Station
MS: Mobile Station
LA: Location Area
Location Management in GSM

- **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

![Diagram showing HLR, VLR, and LA with LAI and MSISDN connections](image)
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)
Data bases (registers) in GSM

- **Home Location Register (HLR):** Semi permanent data
  - **IMSI (International Mobile Subscriber Identity):** max. 15 numbers
    - Mobile Country Code (MCC, 262) + Mobile Network Code (MNC, 01/02) + Mobile Subscriber Identification Number (MSIN)
  - **MSISDN (Mobile Subscriber International ISDN Number):** 15 numbers
    - Country Code (CC, 49) + National Destination Code (NDC, 171/172) + HLR Number + Subscriber Number (SN)
    - Number porting: translation table
  - Subscriber data (name, address, account etc.)
  - Service profile (priorities, call forwarding, service restrictions, e.g. roaming restrictions)
Data bases (registers) in GSM

- **Home Location Register (HLR):** Temporary data
  - VLR address, MSC address
  - MSRN (Mobile Subscriber Roaming Number)
    - CC + NDC + VLR number
      - VLR number = MSC number + SN
  - Authentication Set, consists of several Authentication Triplets:
    - RAND (128 Bit),
    - SRES (32 Bit),
    - Kc (64 Bit)
  - Billing data later on transferred to Billing Centres
Data bases (registers) in GSM

- **Visitor Location Register (VLR)**
  - TMSI (Temporary Mobile Subscriber Identity)
  - LAI (Location Area Identification)
  - MSRN
  - IMSI, MSISDN
  - MSC-address, HLR-address
  - Copy of Service profile
  - Billing data later on transferred to Billing Centres
Data bases (registers) in GSM

- **Equipment Identity Register (EIR)**
  - **IMEI** (International Mobile Station Equipment Identity): 15 numbers
    - serial number of mobile station
      - white-lists (valid mobiles, shortened IMEI)
      - grey-lists (mobiles with failures are observed)
      - black-lists (blocked, stolen mobiles)
  - **USSD** (Unstructured Supplementary Service Data) code for showing IMEI: *#06#
Security functions of GSM

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

- Data stored on SIM:
  - IMSI (International Mobile Subscriber Identity)
  - individual symmetric key Ki (Shared Secret Key)
  - PIN (Personal Identification Number): admission control
  - TMSI (Temporary Mobile Subscriber Identity)
  - LAI (Location Area Identification)

- Cryptographic algorithms:
  - A3: Challenge-Response-Authentication
  - A8: Session Key generation: Kc
Challenge-Response-Authentication

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

- 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](image-url)
Pseudonymization on air interface

- **TMSI (Temporary Mobile Subscriber Identity)**
  - hides from traceability of mobile users by outsiders
  - on air interface: all (unencrypted) transactions from and to mobile user is addressed with TMSI
  - algorithm for TMSI generation is network individual (not standardized)

- **Identity Request**
  - first contact (home network)
  - after failure
    - IMSI is requested by serving network
**First contact Failure**

**Identity Request**

Diagram:

- **MS**
  - alte TMSI im SIM
  - IMSI aus SIM
  - Kc
  - A5
  - TMSI Reallocation Command
    - cipher(TMSI new)

- **Netz**
  - VLR: keine Zuordnung TMSI — IMSI möglich
  - VLR: Neuvergabe TMSI
  - Speicherung TMSI new
  - BSC: Chiffr. A5

**Identity Request**

**Identity Response**

-beliebige Nachricht, in der TMSI verwendet wird)

LAI old, TMSI old
**TMSI Reallocation Command**

**alte TMSI im SIM**

LAI old, TMSI old

**VLR: Zuordnung TMSI — IMSI**

**Netz**

**TMSI Reallocation Command**

cipher(TMSI new)

**BSC: Chiffr. A5**

**Speicherung TMSI new**

**VLR: Neuvergabe TMSI**

**Löschung TMSI old**

**Normal case**

**TMSI used**
Link encryption on air interface

- **Session key generation: Algorithm A8**

![Diagram](image.png)
Link encryption on air interface

- Session key generation: Algorithm A8
  - implemented on SIM and in Authentication Centre (AuC)
  - cryptographic one-way function
  - interfaces are standardized
  - COMP128: well-known implementation of A3/A8
Link encryption on air interface

- Link encryption: Algorithm A5

![Diagram](image-url)
Link encryption on air interface

- **Link encryption: Algorithm A5**
  - implemented in mobile station (not SIM!)
  - standardized algorithms:
    - A5 or A5/1
    - A5* or A5/2 «weak variant» of A5 — (deprecated)
    - [A5/3 based on KASUMI (UMTS) with length(Kc)=64 bit]
    - [A5/4 same as A5/3 with length(Kc)=128 bit]

- **Security of A5/1 and A5/2**
  - Cipher is based on non-linear shift registers
  - Algorithms considered insecure today
    - A5/1 broken by Nohl 2010
      - Attack uses ≈ 2 TByte of pre-calculated rainbow tables
Link encryption on air interface

- **Ciphering Mode Command (GSM 04.08)**

  
<table>
<thead>
<tr>
<th>TI flag</th>
<th>TI value</th>
<th>Protocol discriminator</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>N(SD)</td>
<td>Message type</td>
</tr>
</tbody>
</table>

  Ciphering Mode Command

  SC=0: No ciphering
  SC=1: Start ciphering

- **Cipher mode setting information element**

<table>
<thead>
<tr>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>SC=0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SC=1</td>
</tr>
</tbody>
</table>

  Ciph mode set IEI
  Spare
  Spare
  Spare
Active Man-in-the-Middle Attack on A5/3

MS
- Authentication Request
  - RAND
- Authentication Response
  - SRES
- Ciphering Mode Command
  - Start Ciphering with A5/1
- Ciphering Mode Complete
  - A5/1 Encrypted
    - «Communication»

Attacker
- Crack Kc in realtime

BTS
- Authentication Request
  - RAND
- Authentication Response
  - SRES
- Ciphering Mode Command
  - Start Ciphering with A5/3
- Ciphering Mode Complete
  - A5/3 Encrypted
    - Communication

Knows Kc
GSM security functions overview

Location Updating Request
TMSI
Authentication Request
RAND

Authentication Response
SRES

Ciphering Mode Command
Start Ciphering

Ciphering Mode Complete
TMSI Reallocation Command
TMSI new

Location Updating Accept

TMSI Reallocation Complete
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
  - Determine Ki in SIM card

- **Attack 1**
  - 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
  - Needs $2^{17}$ RAND values ($\approx 150,000$ calculations) to determine Ki (max. 128 bit)
  - 6,25 calculations per second only, due to slow serial interface of SIM card
SIM cloning

- **Scope**
  - Telephone at the expense of others
  - Determine Ki in SIM card

Source: http://www.ccc.de/gsm/
SIM cloning

**Scope**
- Telephone at the expense of others
- Determine Ki in SIM card

**Attack 2**
- Side Channel Attack on SIM card
- Measurement of chip power consumption during authentication reveals Ki
- Attack on the implementation of COMP 128, not the algorithm itself
- Very fast: 500-1000 random inputs used for practical attack

- More reading:
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, Kc) 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

- Mobile station
- BTS
- Microwave link (not encrypted)
- (Gateway)-MSC

Air interface (encrypted)

Fixed network (not encrypted)
Interception of authentication data

**faked mobile station**

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

**air interface**

- *(any message)*
  - TMSI
  - Auth. Request
    - RAND
  - Auth. Response
    - SRES
  - Ciphering Mode Cmd.
    - Start Ciphering
  - Ciphering Mode Compl.
    - A5

**visited network**

- mapping TMSI–IMSI
  - store auth. info
  - SRES'
  - auth. res.
  - Kc
  - Ciphering Mode Compl.
    - 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

- **EP 1 051 053 B1**
  - April 2000 by Rohde & Schwarz
IMSI-Catcher

Pictures: Verfassungsschutz,
IMSI-Catcher: Getting IMSI and IMEI

Note: The IMSI-Catcher sends its «location area identity» with a higher power than the genuine BTS.

Only relevant for eavesdropping.
IMSI-Catcher: Eavesdropping Mobile Originated Calls

IMSI-Catcher opens a call on a second phone with suppressed or faked caller ID

Not encrypted

Encrypted
IMSI-Catcher: Eavesdropping Mobile Terminated Calls

MS camps on cell of IMSI-Catcher

- Paging Request
- Authentication Request (RAND)
- Authentication Response (SRES)
- Ciph. Mode Cmd. ([No Ciphering])

IMSI-Catcher

- suppress ciphering
- Ciph. Mode Cmd. ([Start Ciphering])
- Ciphering Mode Complete ([Fault])
- Ciph. Mode Cmd. ([No Ciphering])

Mobile network

- Incoming call
- Authentication Request (RAND)
- Authentication Response (SRES)
- Ciph. Mode Cmd. ([No Ciphering])

Not encrypted
IMSI-Catcher (1)

- All BTS' send a list of frequencies of BCCHs of their neighboring cells and the own LAI

- Examples:
  - BTS 7: f4, f5, f8; LA 2
  - BTS 8: f7, f4, f5, f6, f9; LA 2
**IMSI-Catcher (2)**

- **IMSI-Catcher**
  - receive from BCCH of current cell (5)
    - BTS 5: f1, f2, f3, f4, f6, f7, f8, f9; LA 1
  - select any frequency (e.g. f4) and receives from BCCH on f4
    - BTS 4: f1, f2, f5, f8, f7; LA 1
  - choose any LAI which differs from actual LAIs in neighborhood (e.g. LA 9)
  - send on f4 with high power
    - IMSI-C.: f1, f2, f5, f8, f7; LA 9

<table>
<thead>
<tr>
<th>BTS 1: f1 / LA 1</th>
<th>BTS 4: f4 / LA 1</th>
<th>BTS 7: f7 / LA 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>BTS 2: f2 / LA 3</td>
<td>BTS 5: f5 / LA 1</td>
<td>BTS 8: f8 / LA 2</td>
</tr>
</tbody>
</table>

- **IMSI-Catcher**

---

51
IMSI-Catcher (3)

- **MS (camps on cell 5)**
  - monitors BCCHs of cells 1-9
  - finds best signal on f4 (transmitted by IMSI-Catcher) and learns that cell belongs to a new LA
  - send a LUP request to IMSI-Catcher

- **IMSI-Catcher**
  - responds with a Identity Request

- **MS**
  - answers with IMSI and IMEI

---

**Diagram:**

- **BTS 1:** f1 / LA 1
- **BTS 4:** f4 / LA 1
- **BTS 7:** f7 / LA 2
- **BTS 2:** f2 / LA 3
- **BTS 5:** f5 / LA 1
- **BTS 8:** f8 / LA 2
- **BTS 3:** f3 / LA 3
- **BTS 6:** f6 / LA 3
- **BTS 9:** f9 / LA 2

**IMSI-Catcher**
**IMSI-Catcher (4)**

- IMSI-Catcher
  - sends junk (non-decodable data) on Paging Channel (PCH) and
  - sends a frequency list of BTS which do not send the frequency of IMSI-Catcher (f4) in their frequency lists
    - IMSI-C.: f3, f6, f9; LA 9

![IMSI-Catcher Diagram]
MS

- receives junk on PCH and (according to GSM05.05) does a cell reselection:
- MS monitors signal strengths of f3, f6, f9
- changes to the best cell (LUP)
IMSI-Catcher (5)

- **Result**
  - MS is back in the network again
  - because BTS 3, 6 and 9 do not send f4 in their frequency lists, the MS does not recognize the powerful IMSI-Catcher signal again (and subsequently does not change back to it)
IMSI-Catcher detectors

- **AIMSICD**
  - [https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector](https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector)

- **SnoopSnitch**
  - from SRLabs (Karsten Nohl)

- **Darshak**
  - TU Berlin

- **GSMK CryptoPhone**
  - special Smarthone

- **IMSI-Catcher-Catcher (ICC)**
  - SBA Research (Adrian Dabrowski)

Sources: [https://www.privacy-handbuch.de/handbuch_75.htm](https://www.privacy-handbuch.de/handbuch_75.htm)
Location Management

- **Centralized approach**
  - Change of Location Area (LA), i.e. Location Updating, needs communication with HLR (far away from LA)
  - Efficiency: Good at low Location Updating rates

- **Used in Mobile IP**
  - HLR = Home Agent

Diagram:
- **incoming call:**
  - MSISDN
  - A

- **HLR**
  - MSISDN, LAI
  - speichert Adresse des LA zusammen mit der MSISDN

- **MSISDN enthält Nummer des HLR**

- **Datenbankabfrage**

- **Vermittlung des Rufes ins LA**

- **BTS**

- **Broadcast im LA**

- **besuchtes LA**
Location Management

- 2-staged approach
  - Change of Location Area (LA) changes VLR entry
  - VLR serves geographically limited area (VLR-Area)
  - Rare changes of VLR-Area changes HLR entry
  - Reduced signaling costs in wide area network
  - Tradeoff: Delayed call setup (mobile terminated)
Location Management

- **Multi-staged storage**
  - Many proposals for 3rd Generation Systems (UMTS), never realized in the field
  - **Variations**: Hierarchical storage, Forwarding strategies
Legend:

a) Change of radio cell
b) Change of LA
c) Change of VLR/MSC area
d) Change of MSC area

LA 1 (belongs to MSC 1 and VLR 1)
LA 2 (belongs to MSC 2 and VLR 2)
LA 3 (belongs to MSC 2 and VLR 2)
LA 4 (belongs to MSC 3 and VLR 2)

Movement of MS

Radio cell
Location Updating: New LA

- New LA, old VLR (TMSI found)
  - Location Updating Request (TMSI, LAI)old
  - Security management
    - Authentication
    - Ciphering Mode
    - TMSI Reallocation
  - Location Updating Accept
Location Updating: New VLR area

- **MSC/VLR new**
  - **Location Updating Request**: TMSI old, LAI old
  - **Location Updating Accept**
  - **Update Location**: IMSI, MSC/VLR new
  - **Update Location Result**
  - **De-Allocation**: TMSI old

- **MSC/VLR old**
  - **TMSI old, LAI old**

- **MS**
  - **Sicherheitsmanagement**: Authentikation, Verschlüsselungsmodus setzen, Zuweisung TMSI new
  - **Bestätigung TMSI new**
  - **Löschen TMSI old**

- **HLR**
  - **Cancel Location**
Mobile Terminated Call Setup (MTCSU)

- **Incoming Call**
  - MSISDN-B enthält Routing-Information zum gebuchten GSM-Netz des Mobilfunkteilnehmers B
  - liest den Datenbankeintrag für MSISDN/IMSI-B und vermittelt zum entsprechenden MSC weiter

- **Gateway MSC**
  - send routing information
  - MSISDN/IMSI-B
  - MSC2 (eigentlich MSRN)

- **Visited MSC2**
  - send info for incoming call
  - LA1, TMSI-B
  - IMSI-B

- **BroadcastNachricht im LA1**
  - LA1
  - Station erkennt Verbindungswunsch Nachricht an ausgestrahlter TMSI-B

- **VLR2**
  - IMSI-B, LA1, TMSI-B
  - IMSI-C, LA3, TMSI-C

- **HLR**
  - MSISDN/IMSI-A
  - MSC3
  - MSISDN/IMSI-B
  - MSC2
  - MSISDN/IMSI-X
  - MSC4
  - MSISDN/IMSI-Y
  - MSC1
  - MSISDN/IMSI-Z
  - MSC2
Mobile Originated Call Setup

- Kanalanforderung an BSS
- CM Service Request
- Sicherheitsmanagement: Authentikation, Verschlüsselungsmodus
- Kanalzuweisung bei early-TCH-Assignment
- Setup
- Alert
- Kanalzuweisung bei OACSU
- Connect
- Initial Address Message
- Adress Complete Message
- Answer Message
- Data
- Disconnect
- Release
Message format GSM 04.08

- **Protocol discriminator**

  4 3 2 1  bit number
  0 0 1 1  call control, packet-mode, connection control and call related SS msgs
  0 1 0 1  mobility management messages
  0 1 1 0  radio resources management messages
  1 0 0 1  short message service messages
  1 0 1 1  non call related SS messages
  1 1 1 1  reserved for tests procedures

  All other values are reserved
Transaction identifier (TI)
- Used for distinction of parallel activities of MS
  - TI flag:
    - 0: message sent from the originated TI side
    - 1: message sent to the originated TI side

TI value
- Number 000…110 (bin: 0…6)
- 111 reserved
Message format GSM 04.08

- **3 Classes:**
  - Radio resources management
  - Mobility management
  - Call control

- **N(SD)**
  - Sequence number or Extension Bit

<table>
<thead>
<tr>
<th>octet 1</th>
<th>octet 2</th>
<th>octet 3</th>
<th>octet 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>TI flag</td>
<td>TI value</td>
<td>Protocol discriminator</td>
<td>Message type</td>
</tr>
<tr>
<td>0</td>
<td>N(SD)</td>
<td>Data</td>
<td>...</td>
</tr>
</tbody>
</table>
Message type (1)

- Radio resources management (1)

<table>
<thead>
<tr>
<th>8 7 6 5 4 3 2 1</th>
<th>bit number</th>
</tr>
</thead>
<tbody>
<tr>
<td>----------------</td>
<td>------------</td>
</tr>
</tbody>
</table>

0 0 1 1 1 — — — Channel establishment messages
- 0 1 1 ADDITIONAL ASSIGNMENT
- 1 1 1 IMMEDIATE ASSIGNMENT
- 0 0 1 IMMEDIATE ASSIGNMENT EXTENDED
- 0 1 0 IMMEDIATE ASSIGNMENT REJECT

0 0 1 1 0 — — — Ciphering messages
- 1 0 1 CIPHERING MODE ASSIGNMENT
- 0 1 0 CIPHERING MODE COMPLETE

0 0 1 0 1 — — — Handover messages
- 1 1 0 ASSIGNMENT COMMAND
- 0 0 0 ASSIGNMENT COMPLETE
- 1 1 1 ASSIGNMENT FAILURE
- 0 1 1 HANDOVER COMMAND
- 1 0 0 HANDOVER COMPLETE
- 0 0 0 HANDOVER FAILURE
- 1 0 1 PHYSICAL INFORMATION

0 0 0 0 1 — — — Channel release messages
- 1 0 1 CHANNEL RELEASE
- 0 1 0 PARTIAL RELEASE
- 1 1 1 PARTIAL RELEASE COMPLETE

...
## Message type (1)

- **Radio resources management (2)**

<table>
<thead>
<tr>
<th>Bit Number</th>
<th>Message Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 7 6 5 4 3 2 1</td>
<td>bit number</td>
</tr>
<tr>
<td></td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>

0 0 1 0 0 — — — Paging messages
- 0 0 1 PAGING REQUEST TYPE 1
- 0 1 0 PAGING REQUEST TYPE 2
- 1 0 0 PAGING REQUEST TYPE 3
- 1 1 1 PAGING RESPONSE

0 0 0 1 1 — — — System information messages
- 0 0 1 SYSTEM INFORMATION TYPE 1
- 0 1 0 SYSTEM INFORMATION TYPE 2
- 0 1 1 SYSTEM INFORMATION TYPE 3
- 1 0 0 SYSTEM INFORMATION TYPE 4
- 1 0 1 SYSTEM INFORMATION TYPE 5
- 1 1 0 SYSTEM INFORMATION TYPE 6

0 0 0 1 0 — — — Miscellaneous messages
- 0 0 0 CHANNEL MODE MODIFY
- 0 1 0 RR-STATUS
- 1 1 1 CHANNEL MODE MODIFY ACKNOWLEDGE
- 1 0 0 FREQUENCY REDEFINITION
- 1 0 1 MEASUREMENT REPORT
- 1 1 0 CLASSMARK CHANGE
**Message type (2)**

- **Mobility management**
  - Bits 7 and 8 (value: 00) reserved as extension bits
  - Bit 7: mobile originated only: 1, if sequence number is sent

<table>
<thead>
<tr>
<th>bit number</th>
<th>Registration messages</th>
<th>Security messages</th>
<th>Connection management messages</th>
<th>Connection management messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 x 0 0</td>
<td>0 0 0 1 IMSI DETACH INDICATION</td>
<td>0 0 0 1 AUTHENTICATION REJECT</td>
<td>0 x 1 0 CM SERVICE ACCEPT</td>
<td>0 x 1 1 CM SERVICE REQUEST</td>
</tr>
<tr>
<td></td>
<td>0 0 1 0 LOCATION UPDATING ACCEPT</td>
<td>0 0 1 0 AUTHENTICATION REQUEST</td>
<td>0 0 1 0 CM SERVICE REJECT</td>
<td>0 0 1 0 CM REESTABLISHMENT REQUEST</td>
</tr>
<tr>
<td></td>
<td>0 1 0 0 LOCATION UPDATING REJECT</td>
<td>0 1 0 0 AUTHENTICATION RESPONSE</td>
<td></td>
<td>0 1 0 0 CM SERVICE REQUEST</td>
</tr>
<tr>
<td></td>
<td>1 0 0 0 LOCATION UPDATING REQUEST</td>
<td>1 0 0 0 AUTHENTICATION RESPONSE</td>
<td></td>
<td>1 0 0 0 CM REESTABLISHMENT REQUEST</td>
</tr>
<tr>
<td>0 x 0 1</td>
<td>0 0 0 1 LOCATION UPDATING REQUEST</td>
<td>0 0 0 1 AUTHENTICATION REJECT</td>
<td>0 x 1 0 CM SERVICE ACCEPT</td>
<td>0 x 1 1 CM SERVICE REQUEST</td>
</tr>
<tr>
<td></td>
<td>0 0 1 0 LOCATION UPDATING REJECT</td>
<td>0 0 1 0 AUTHENTICATION REQUEST</td>
<td>0 0 1 0 CM SERVICE REJECT</td>
<td>0 0 1 0 CM REESTABLISHMENT REQUEST</td>
</tr>
<tr>
<td></td>
<td>0 1 0 0 LOCATION UPDATING REQUEST</td>
<td>0 1 0 0 AUTHENTICATION RESPONSE</td>
<td></td>
<td>0 1 0 0 CM SERVICE REQUEST</td>
</tr>
<tr>
<td></td>
<td>1 0 0 0 LOCATION UPDATING REQUEST</td>
<td>1 0 0 0 AUTHENTICATION RESPONSE</td>
<td></td>
<td>1 0 0 0 CM REESTABLISHMENT REQUEST</td>
</tr>
<tr>
<td>0 x 1 0</td>
<td>0 0 0 1 CM SERVICE ACCEPT</td>
<td>0 0 0 1 MM STATUS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Message type (3)

- Call control (1)
  - Bits 7 and 8 (value: 00) reserved as extension bits
  - Bit 7: mobile originated only: 1, if sequence number is sent

- Nationally specific messages: next octets contain message

```
  8 7 6 5 4 3 2 1  bit number
-----------------------------
0 x 0 0 0 0 0 0 0  Escape to nationally
                      specific message types

0 x 0 0  Call establishment messages
0 0 0 1  ALERTING
1 0 0 0  CALL CONFIRMED
0 0 1 0  CALL PROCEEDING
0 1 1 1  CONNECT
1 1 1 1  CONNECT ACKNOWLEDGE
1 1 1 0  EMERGENCY SETUP
0 0 1 1  PROGRESS
0 1 0 1  SETUP

0 x 0 1  Call information phase
   messages
0 1 1 1  MODIFY
1 1 1 1  MODIFY COMPLETE
0 0 1 1  MODIFY REJECTED
0 0 0 0  USER INFORMATION
...```
Message type (3)

- **Call control (2)**
  - Bits 7 and 8 (value: 00) reserved as extension bits
  - Bit 7: mobile originated only: 1, if sequence number is sent

<table>
<thead>
<tr>
<th>8 7 6 5 4 3 2 1</th>
<th>bit number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td>0 x 1 0 – – – –</td>
<td>Call clearing messages</td>
</tr>
<tr>
<td>0 1 0 1</td>
<td>DISCONNECT</td>
</tr>
<tr>
<td>1 1 0 1</td>
<td>RELEASE</td>
</tr>
<tr>
<td>1 0 1 0</td>
<td>RELEASE COMPLETE</td>
</tr>
<tr>
<td>0 x 1 1 – – – –</td>
<td>Miscellaneous messages</td>
</tr>
<tr>
<td>1 0 0 1</td>
<td>CONGESTION CONTROL</td>
</tr>
<tr>
<td>1 1 1 0</td>
<td>NOTIFY</td>
</tr>
<tr>
<td>1 1 0 1</td>
<td>STATUS</td>
</tr>
<tr>
<td>0 1 0 0</td>
<td>STATUS ENQUIRY</td>
</tr>
<tr>
<td>0 1 0 1</td>
<td>START DTMF</td>
</tr>
<tr>
<td>0 0 0 1</td>
<td>STOP DTMF</td>
</tr>
<tr>
<td>0 0 1 0</td>
<td>STOP DTMF ACKNOWLEDGE</td>
</tr>
<tr>
<td>0 1 1 0</td>
<td>START DTMF ACKNOWLEDGE</td>
</tr>
<tr>
<td>0 1 1 1</td>
<td>START DTMF REJECT</td>
</tr>
</tbody>
</table>
Movement profiling in GSM

- **Variants:**
  - Access HLR and VLR data (insiders only)
  - Direction finding (German: «Peilung»)

- **Protection:**
  - Privacy protection of database entries
  - Direct Sequence Spread Spectrum
Access HLR and VLR data

OMC

HLR

kennt VLR bzw. MSC

MBR

kennt LA

bei existierender Verbindung:
kennt Zelle

BSS

MSC

kennt Frequenzsprungparameter
(Hopping Parameters)

BSC

kennt Frequenzsprungparameter
(Hopping Parameters)

BTS ... BTS

LA
Direction finding with directional antennas

Richtantennen notwendig
Measurement of signal delay times
Location Based Services

- Terminal-based locating
  - Global Positioning System (GPS)
    - Accuracy: 10...100 m
    - Location time: up to 30 sec
  - Assisted-GPS (A-GPS)
    - GPS signals re-broadcasted by BTS
    - Increased location speed (and accuracy)
  - Observed Time Difference (OTD)
    - BTS1 ... BTS3 send a location signal
    - Received after $\Delta t_1$, $\Delta t_2$ and $\Delta t_3$ by MS
    - If $\Delta t_i == \Delta t_j$ then OTD=0
Assisted-GPS (A-GPS)

1. MS and A-GPS Server receive same satellite signals

2. Calculates support information for fast localization (doppler shift, pseudo random noise phase)

3. Support information

4. Performs exact measure and transmits values to A-GPS server

5. Exact measure values

6. Calculates exact location
Location Based Services

- **Network-based locating**
  
  - Time of Arrival (TOA)
    - Mobile station sends signal
    - BTS receive signal after $\Delta t_i$ (i=1,2,3)
  
  - Cell of Origin (COO)
    - Cell-ID is associated with geographic location
    - Accuracy: 100 m ... 35 km
Spread Spectrum Systems

- Radio communication between military divisions
  - Sender sends on frequency $f_0$ with bandwidth $B$

- Problems:
  - Spectrum analyzer detects energy around $f_0$ and directional antennas locate source of signal
  - Jammer may interfere communication
Transmision model Spread Spectrum Systems

Sender

```
  data
  Spreading modulator
    Spreading sequence (high bandwidth)
  HF modulator
    High frequency bearer
```

Receiver

```
  HF demodulator
    High frequency bearer
  Spreading demodulator
    Spreading sequence (high bandwidth)
  data
```
Spreading

- Data is modulated with high-bandwidth spreading sequence:
  - Walsh functions (orthogonal codes)
  - Pseudo-Noise-Sequence (PN-Code)
Data is modulated with high-bandwidth spreading sequence:
- Walsh functions (orthogonal codes)
- Pseudo-Noise-Sequence (PN-Code)

- Spectral spreading of signal
- Dispersion of energy on a large frequency spectrum
De-Spreading

- Spread data interfered by (random) noise
De-Spreading

- Spread data interfered by (random) noise
- Spectral spreading of noise
- De-spreading of data
Missing end-to-end-Services in GSM

- Speech channels of GSM are not bit transparent channels
  - Lossy compression of speech channels

- Use data channel for additional end-to-end encryption
  - As an external add-on (e.g. GSM TopSec Med)
  - As integrated service (e.g. GSM TopSec GSM)

- Both is not GSM standards conform add-on
- Users need compatible devices or software on MS
Signaling of channel type (speech, data) in GSM

**MS-A (sendet)**
- type: =data
- A/D
- CODEC
- A5
- TX/RX

**MS-B (empfängt)**
- A/D
- CODEC
- A5
- TX/RX

**BSS**
- TX/RX
- A5
- TRAU
- Rate Adaption
- Transcoder

**MSC**
- Logik
- IF type=data
  THEN Rate Adaption
- ELSEIF type=speech
  THEN Transcoder

**IF type=speech**

**MSC**
- Logik
- Rate Adaption
- Transcoder
- TRAU

**MSC**
- Mobile Station
- Base Station Subsystem
- Analog-Digital-Converter
- Speech Coder/Decoder
- Terminal Adaption

**A5**
- GSM Link Encryption
- Transmitter/Receiver
- Transcoder/Rate Adaption Unit
- Mobile Switching Centre
Bit transparent data channel for end-to-end speech encryption

Example:

*TopSec MED* (Rohde&Schwarz): external device bluetooth connected to mobile phone
Bit transparent data channel – internal use for end-to-end enc.

Example:
TopSec GSM
(Rohde&Schwarz): modified Siemens S35i with Crypto processor, 128 bit encryption
Software solutions for end-to-end encryption

- Example: SecureGSM · http://www.securegsm.com
  - For Windows Mobile Smartphones
  - Bit transparent data channel used
  - Asymmetric key agreement («4Kbit»)
  - Triple encryption with AES, Serpent and Towfish with triple 256 bit session keys
Summary of security problems in GSM

- **Hard**
  - Weak link encryption «protects» against outsiders only
  - No bit transparent speech channels → no end-to-end encryption
  - Location finding for insiders possible
  - Mutual authentication is missing

- **Further**
  - Symmetric encryption
  - No anonymous network usage possible
  - Trust into accounting is necessary
Security functions of further mobile Systems

UMTS and LTE
Bluetooth security
WiFi security
Universal mobile telecommunication system (UMTS)

- Security functions of UMTS -> «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

USIM  UMTS Subscriber Identity Module
MS    Mobile Station
RNC   Radio Network Controller
VLR   Visitor Location Reg.
HLR   Home Location Register
AuC   Authentication Centre

Node B (Base Station)  Serving Network  Home Environment

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

User authentication

Network authentication
- authentication key K,
- authentication function f1, f2
- key generation function f3, f4, f5
- sequence number management SQN
Generation of authentication vectors (network side)

\[
\text{AUTN} := \text{SQN} \oplus \text{AK} || \text{AMF} || \text{MAC} \\
\text{AV} := \text{RAND} || \text{XRES} || \text{CK} || \text{IK} || \text{AUTN}
\]
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQN</td>
<td>Sequence number</td>
</tr>
<tr>
<td>RAND</td>
<td>Random number</td>
</tr>
<tr>
<td>AMF</td>
<td>Authenticated Management Field</td>
</tr>
<tr>
<td>K</td>
<td>Secret Key</td>
</tr>
<tr>
<td>MAC</td>
<td>Message authentication code</td>
</tr>
<tr>
<td>XRES</td>
<td>Expected response</td>
</tr>
<tr>
<td>RES</td>
<td>Response</td>
</tr>
<tr>
<td>CK</td>
<td>Cipher key</td>
</tr>
<tr>
<td>IK</td>
<td>Integrity key</td>
</tr>
<tr>
<td>AK</td>
<td>Anonymity key</td>
</tr>
<tr>
<td>AUTN</td>
<td>Authentication token</td>
</tr>
<tr>
<td>AV</td>
<td>Authentication vector</td>
</tr>
</tbody>
</table>

False-base-station attacks possible if attacker can eavesdrop AV on network internal communication lines

\[ \ldots \] \ # of bits
Authentication function in the USIM (user side)

Verify MAC == XMAC, then verify that SQN is in the correct range.
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 MAC == XMAC
Own base station in UMTS

- Example: Vodafone SuperSignal
  - base station connected via IP with UMTS network
  - femto cell at home, not a repeater

Long Term Evolution (LTE) Architecture

USIM  UMTS Subscriber Identity Module
ME    Mobile Equipment
E-UTRAN Evolved UMTS Terrestrial Radio Access Network
MME   Mobility Management Entity
HSS   Home Subscriber Service
S-GW  Serving Gateway
P-GW  Packet Data Network Gateway
IP    Internet Protocol
Long Term Evolution (LTE)

- **Characteristics**
  - Traffic channels: Data services only, Speech is realized via Voice-over-IP
  - SMS is realized via signalling messages (similar to GSM)

- **Security: inspired and closely related to UMTS**
  - Individual symmetric key at USIM and HSS
  - Authentication vector
    - Calculated at USIM and HSS
    - Checked at MME
  - Pseudonymization on air interface:
    - Globally Unique Temporary Identity (GUTI)
  - Data encryption
    - Air interface: Advanced Encryption Standard (AES)
    - Network internal communication: IPSec
      - False-base-station attacks: impossible
Bluetooth security
Bluetooth

- **Development**
  - Initiated by Ericsson
  - Bluetooth Special Interest Group (SIG)
    - Ericsson, Nokia, IBM, Toshiba, Intel and many other

- **Standard**
  - IEEE 802.15.1

- **Benefits**
  - Low energy consumption
  - Low interference sensibility (spread spectrum techniques)

- **Disadvantages**
  - Low Bandwidth
  - Limited signal coverage (radius)
  - Limited number of users
Technical Details

- **Physical Layer**
  - License free ISM-Band: 2.4GHz (ISM: Industrial, Scientific, Medical)
  - 2402 to 2480 MHz
  - 79 channels per 1 MHz bandwidth
  - Frequency-Hopping with 1600 chips (changes per second)

- **Link Layer (DLL)**
  - Modulation method:
    - Gaussian Frequency Shift Keying
  - Forward Error Correction (FEC)
  - Cyclic Redundancy Check (CRC)
Technische Details

Specifications

- 1.0: First spec, still immature, ca. 732 kbps data rate
- 1.1: Broadly used
- 1.2: Adaptive Frequency Hopping, improved error correction
- 2.0 (Nov 2004): Data rates up to 2 Mbps
- 3.0 (Apr 2009): Data rates up to 24 Mbps
- 4.0 (Dec 2009): Bluetooth Low Energy

Classification

- Pico-Bluetooth
  - 2.5 mW / 1 mW transmission power (Class 2 and 3)
  - Radius up to 50 m / 10 m
- Mega-Bluetooth
  - 100 mW transmitting power (Class 1)
  - Radius up to 100 m
Development of networks

a) Point-to-Point

b) Pico-Network: 1 Master, up to 7 active slaves

c) Scatter-Network: various overlapping Pico-Networks
Protocols


<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBEX</td>
<td>Object EXchange protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>SDP</td>
<td>Service Discovery Protocol</td>
</tr>
<tr>
<td>RFCOMM</td>
<td>Serial cable emulation protocol</td>
</tr>
<tr>
<td>AT-Commands</td>
<td></td>
</tr>
<tr>
<td>TCS</td>
<td>Telephony Control protocol Specification</td>
</tr>
<tr>
<td>LMP</td>
<td>Link Manager Protocol</td>
</tr>
<tr>
<td>L2CAP</td>
<td>Logical Link Control and Adaption Protocol</td>
</tr>
<tr>
<td>OBEX (vCard,vCal)</td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td></td>
</tr>
<tr>
<td>PPP</td>
<td></td>
</tr>
<tr>
<td>L2CAP</td>
<td></td>
</tr>
<tr>
<td>RFCOMM</td>
<td></td>
</tr>
<tr>
<td>AT-Commands</td>
<td></td>
</tr>
<tr>
<td>TCS</td>
<td></td>
</tr>
<tr>
<td>Audio</td>
<td></td>
</tr>
<tr>
<td>Voice</td>
<td></td>
</tr>
<tr>
<td>Baseband</td>
<td></td>
</tr>
<tr>
<td>Bluetooth Radio</td>
<td></td>
</tr>
</tbody>
</table>
Protocols (2)

- Bluetooth Radio
  - Air Interface
- Baseband
  - Functions for Link connection, Frequency-Hopping, etc.
- Link Manager Protocol (LMP)
  - Security features, clock synchronisation
- Logical Link Control and Adaption Protocol (L2CAP)
  - Interface for higher protocol layers to access baseband
- Service Discovery Protocol (SDP)
  - Information about device types, services, etc.
- RFCOMM (Serial cable emulation protocol)
  - Based on ETSI TS 07.10; for universal use (Modem, IP, ...)
- Telephony Control protocol Specification (TCS)
  - For device control
Security

- **Security functions**
  - Secure device pairing
  - Symmetric authentication (one sided and mutual)
  - Symmetric encryption

- **Basic algorithm for pairing and authentication**
  - SAFER+
    - Publicly known
    - 1 of 15 candidates for AES (Advanced Encryption Standard)
  - Characteristics of SAFER+
    - Block cipher with 128 Bit block length
    - 8 rounds
    - Key length 128 Bit
  - Used in E21, E22, E1 und E3
Pairing

- **Objectives**
  - Identification of two devices A and B
  - Generates a symmetric key $K_{AB}$

- **Pairing Procedure**
  1. Exchange of device addresses BD_ADDR$_A$ and BD_ADDR$_B$
  2. Generate Initialization key $K_{init}$ (intermediate step)
  3. Generate $K_{AB}$
Pairing (1)

- Generate Initialization key $K_{init}$ (Algorithm E22)

- Input:
  - Device address (BD_ADDR$_B$, 48 Bit)
  - PIN (8-128 Bit, typ. at least 4 digits)
  - Random number (IN_RAND, 128 Bit)

- Output:
  - $K_{init}$ (128 Bit)
Pairing (2)

- **Generate** $K_{AB}$ (Algorithm E21)

**Input:**
- Random numbers ($LK_{RAND_{A/B}}$, 128 Bit)
- Device address ($BD_{ADDR_{A/B}}$, 48 Bit)
- Initialization key $K_{init}$

**Output:**
- $K_{AB}$ (128 Bit)
Authentication (one sided or mutual)

- **Algorithm E1**

- **Input:**
  - Random number AU_RAND
  - $K_{AB}$
  - Device address A BD_ADDR_A

- **Output:**
  - true or false
  - ACO (Authenticated Chiphering Offset, 96 Bit)
Encryption

- 2 Steps
  - Generate key $K_c$ with algorithm E3
  - Data encryption with stream cipher E0

- Algorithm E3

- Input:
  - Random number ($\text{EN\_RAND}_A$, 128 Bit)
  - Ciphering Offset Number (COF, 96 Bit) = ACO (from Authentication)
  - $K_{AB}$ (128 Bit)

- Output:
  - $K_c$ (8-128 Bit, manufacturer specific)
Encryption (2)

- Algorithm E0
  - Linear Feedback Shift Register
  - Stream cipher with variable block length up to 64 Bit

- Input:
  - $K_c$
  - Device address (BD_ADDR$_A$)
  - Clock (counter)
  - Plaintext or Ciphertext

A and B identical:

- $K_c$
- BD_ADDR$_A$
- Clock

Payload key generator → Payload key → Key stream generator

EO

Plaintext/Ciphertext

Ciphertext/Plaintext
Encryption (3)

Device A

BD_ADDR_A → E0
Clock_A → E0
K_C → E0
Data_{A-B} → E0
K_cipher → E0

Device B

EN_RAND_A → «start encryption»

BD_ADDR_A → E0
Clock_A → E0
K_C → E0

Encrypted data → Air interface → Encrypted data
Summary: Safety functions

- **Initialization (Pairing)**
  - Generate symmetric key $K_{AB}$ between devices
  - $K_{AB}$ saved
  - $K_{init}$ no longer needed

- **Authentication**
  - Challenge-Response based on $K_{AB}$

- **Encryption**
  - Session key $K_c$ generated from $K_{AB}$
  - Pseudo-One-Time-Pad
  - $K_c$ can be changed automatically while being connected
Vulnerabilities

- **Used PIN with Pairing**
  - Often too short (4 digits)
  - Fixed in the device (1234 or 0000)
  - Often one for all devices used by user (convenience)
  - Some devices can only process max. 16-digit PINs

- **Location finding is easy**
  - BD_ADDR used to discover devices
  - Service Discovery Protocol (SDP)
  - Generating route profiles

- **Device address can be faked**

- **High level of vulnerability to DoS-attacks**
  - Repeated refused queries
    - Result: battery is discharged
Known attacks (selection) 1/2

- **Range:** with antenna up to 2 km
  - Salzburg research, August 2004

- **BlueBug: Uses implementation errors**
  - Marcel Holtmann, Sept 2003
  - BlueSnarf: change phone book, send SMS, ...
  - Chaos-Attack: initiate unnoticed calls, possibilities like BlueSnarf
  - No pairing necessary

- **BlueSmack:**
  - DoS-Attack (use echo-requests)
Known attacks (selection) 2/2

- **PIN Cracking**
  - Yaniv Shaked and Avishai Wool, Juni 2005
  - Brute-force attack on $K_{\text{init}}$ (and $K_{\text{AB}}$)
  - Passive attack
    - Pairing process is sniffed by attacker
  - Active Attack
    - Attacker provokes Re-Pairing and hopes for weak PIN
  - Not possible, if PIN $>$ 64 Bit $\approx$ 19 digits

<table>
<thead>
<tr>
<th>PIN lengths</th>
<th>Time in s</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0.063</td>
</tr>
<tr>
<td>5</td>
<td>0.75</td>
</tr>
<tr>
<td>6</td>
<td>7.609</td>
</tr>
<tr>
<td>7</td>
<td>76.127</td>
</tr>
</tbody>
</table>

Results with Pentium IV 3GHz
Security

- **In general**
  - no use of Bluetooth, as far as possible
  - if not used, switch it off
  - disable visibility of device

- **Pairing**
  - no pairing in the public
  - pairing with other technology (e.g. NFC = Near Field Communication)
  - use (more than 18 digits) non-trivial PINs
  - multiple devices must have different PINs

- **Hope for good implementation**
  - firmware update if necessary
WiFi security
**WLAN: Wireless Local Area Networks**

- **Wireless connection of systems**
  - increased mobility
  - no physical (wired) connections

- **Topologies**
  - Ad-hoc mode: peer-to-peer connections (client-to-client)
  - Infrastructure mode: via Access Point (AP)

- **IEEE 802.11 standard**
  - IEEE: Institute of Electrical and Electronics Engineers
  - defines layer 1 and parts of layer 2 of OSI ref. model
  - has Logical Link Control (802.2) together with other 802 standards
IEEE 802.11 Standard

- Mobile terminal
- Access point
- Infrastructure network
- Fixed terminal

Application stack:
- TCP
- IP
- LLC
- 802.11 MAC
- 802.11 PHY

- Application
- TCP
- IP
- LLC
- 802.3 MAC
- 802.3 PHY
IEEE 802.11 Protocol family

- Well-known WLAN-standards:
  - IEEE 802.11:
    - Infrared (IR)
    - 1 or 2 Mbps via radio in 2.4-GHz ISM band
  - IEEE 802.11b: 11 Mbps in 2.4-GHz ISM band
  - IEEE 802.11a: 54 Mbps in 5-GHz ISM band
  - IEEE 802.11g: 54 Mbps in 2.4-GHz ISM band
  - IEEE 802.11n: 600 Mbps in 2.4-GHz and 5-GHz ISM band
  - IEEE 802.11p: 27 Mbps around 5-GHz Car-to-Car

- Security
  - IEEE 802.11i: Security (WPA2)
  - Outdated:
    - WEP (Wired Equivalent Privacy)
    - WPA (WiFi Protected Access) and others
WLAN

- **Security demands**
  - Confidentiality:
    - Protection against eavesdropping
  - Integrity:
    - Protection against modification of messages
    - Protection against unauthorized access
  - Availability
    - Protection against denial-of-service attacks
Protection against unauthorized access

- Weak protection: MAC addresses
  - Limit access to specific MAC addresses on the network

Problem:
- Management of valid MAC addresses
- MAC addresses can be spoofed (MAC spoofing)
WEP: Wired Equivalent Privacy

- **General**
  - Optional sub-protocol of IEEE 802.11
  - Encryption, integrity protection and authentication
  - Implemented in virtually all WLAN devices

- **Encryption**
  - Symmetric encryption with 40 or 104 bit keys, based on RC4

- **Integrity protection**
  - CRC (Cyclic Redundancy Check)

- **Authentication**
  - Method 1: «Open»: no authentication
  - Method 2: «Shared Key»: Challenge-Response-Authentication
WEP: Encryption

- **Symmetric stream cipher**
  - Plaintext XORed with key stream

- **Generation of key stream**
  - Initialization vector (IV, 24 bit)
  - Key (K, 40 or 104 bit)
  - RC4 algorithm used as Pseudo Random Number Generator (PRNG)

- IV is send in clear

- **Decryption**
  - Receiver generates same key stream
  - Ciphertext XORed with key stream
  - Cipher text and key stream linked again with XOR
WEP: Encryption and Integrity protection

Initialization vector IV 24 Bit

Key K
40 or 104 Bit

seed
64 or 128 Bit

RC4 (PZZG)

Key stream

Plaintext M

CRC

ICV

Integrity Check Value

concatenation

XOR

IV || (M || CRC(M)) ⊕ RC4(IV || K)

Or shorter:

IV, (M,CRC(M)) ⊕ RC4(IV,K)
WEP: Decryption and integrity protection

K → || → seed → RC4 (PZZG)

IV

Ciphertext C

concatenation

XOR

Reverse function of ||

CRC

ICV

ICV' ?= OK

NO → HALT

M
WEP: Authentication

- **Two options**
  - Open and Shared Key

- **Open (= no authentication)**
  - disable authentication (only SSID, Server Set ID)

- **Shared Key**
  - Challenge-Response-Authentication
  - Access Point sends unencrypted challenge value
  - Client sends challenge value back as encrypted response
  - Access to network, if challenge is encrypted correctly
WEP: Vulnerabilities

1. Initialization vector
   - IV too short, repeated usage of equal IVs
   - Some products implement IV++ with start value IV=0
   - Results in Known-Plaintext-Attack:
     - Attacker can store a table of (IV, Key stream):
       - Ciphertext $C = (M, \text{CRC}(M)) \oplus \text{RC4}(IV,K)$
       - Attacker knows ciphertext, IV and M:
         Calculate Key stream = RC4(IV,K)
         If IV again occurs, attacker can decrypt
     - Message-related break: Break individual messages, without finding the key K

1. Key K
   - Too short key length with 40 Bit (Brute-Force-Attack)
3. Weakness in RC4 and its usage
   - «weak» IVs can be used to calculate K with statistic attack:
     - Attacker knows IV, ciphertext and beginning of plaintext
       - Beginning of plaintext: Data packets start with M=0xAAAA03 (SNAP-Header, Sub Network Access Protocol)
         -> Attacker knows first three bytes of key stream
       - Determine Key stream (output of RC4) from ciphertext and M
         \[ C = \text{Key stream} \oplus M \]
     - With knowledge of many IVs and many Key streams:
       - Possible exploitation of vulnerability from RC4: partial Linearity of RC4 allows determination of K
         \[ \text{Key stream} = \text{RC4}(\text{IV}, K) \]
3. Weakness in RC4 and its usage

Statistical analysis:
- RC4(IV₁, K) = S₁
- RC4(IV₂, K) = S₂
- RC4(IV₃, K) = S₃
- RC4(IV₄, K) = S₄

... Result of weakness:
K can be calculated
WEP: Vulnerabilities

3. Weakness in RC4 and its usage
   - Practical attack
     • 4-6 million data packets required to gather «weak» IVs: ≈5% IVs are weak (≈900,000 of $2^{24}$).
     • needs 8-12 hours (avg. net load of 1 Mbps) and up to 12 GB HDD space
     • all data packets begins with SNAP pattern 0xAAAA03
     • partial linearity of RC4 on weak IVs
   - Improvement 1:
     • Attacker can enforce usage of weak IVs to reduce network load by choosing the IV, and sending and receiving packets
   - Improvement 2:
     • Tews et al (2007) found further weakness in RC4 to improve speed of WEP attack to ≈ 1 min and no need of weak IVs

Weak IVs: Attack only possible if certain bit combinations in IV
3. Weakness in RC4 and its usage

- Literature:
  - Erik Tews, Ralf-Philipp Weinmann, Andrei Pyshkin: Breaking 104 bit WEP in less than 60 seconds. 2007
4. Weakness of CRC

- CRC and encryption are linear:
  - \( c(a \oplus b) = c(a) \oplus c(b) \)
- Modification of data packets is easy:
  - XOR a random number to (encrypted) plaintext
  - XOR a CRC to (encrypted) checksum
4. Weakness of CRC

- Let
  \[(M, \text{CRC}(M)) \oplus \text{RC4}(\text{IV}, K) = C\]
- Attacker sends a \(C \oplus X\): with \(X = (M', \text{CRC}(M'))\)
  \[X \oplus (M, \text{CRC}(M)) \oplus \text{RC4}(\text{IV}, K) = C \oplus X\]
- Recipient decrypts:
  \[X \oplus (M, \text{CRC}(M)) = (M', \text{CRC}(M')) \oplus (M, \text{CRC}(M))\]
- Because of the data format and the linearity of the encryption (or XOR) and CRC:
  \[\text{CRC}(M \oplus M') = \text{CRC}(M) \oplus \text{CRC}(M')\]

- Result: Attacker has sent a valid message \(M \oplus M'\)
  - CRC can be used to detect random errors, but not to detect modifications of data by an attacker
WEP: Vulnerabilities

4. Weakness of CRC

Ciphertext from sender:
\[ C = (M, \text{CRC}(M)) \oplus \text{RC4}(IV,K) \]

X of attacker:
\[ X = (M', \text{CRC}(M')) \]

Attacker sends \( C \oplus X \):
\[ (M', \text{CRC}(M')) \oplus (M, \text{CRC}(M)) \oplus \text{RC4}(IV,K) \]

Receiver decrypts:
\[ (M', \text{CRC}(M')) \oplus (M, \text{CRC}(M)) \]

Receiver checks CRC (always successful here),
\[ \text{CRC}(a \oplus b) = \text{CRC}(a) \oplus \text{CRC}(b) \]

\[ M \oplus M' \]

Flowchart:
- CRC
- ICV
- OK
- NO
- STOP
- CRC(M) \oplus CRC(M')
WEP: Vulnerabilities

5. No mutual authentication
   – No protection against false Access Points

6. Ineffective authentication
   – Attacker eavesdrops Challenge-Response-Pairs (x/C)
     • Knows $x=M$ and $C$ (and IV)
     • Calculates Key stream = $\text{RC4}(\text{IV}, K)$
   – Attacker opens his own Session
     • Receives a Challenge $x'$
     • Calculates: $x' \oplus \text{RC4}(\text{IV}, K)$
     • Weakness: Attacker chooses same IV
WEP: Vulnerabilities: Ineffective authentication

- Attacker monitors IV, x and $x \oplus \text{RC4}(IV,K)$
- Calculates Key stream RC4(IV,K) from x

- Knows K
- Chooses a random x

- Authorized Client
  - Knows K
  - Chooses IV

- Authorized Client
  - Knows Key stream
  - Chooses monitored IV
Development of WiFi Security

- **Evolution steps**
  - WEP128
  - WEPplus
  - Fast Packet Keying
  - WEP2
  - EAP (Extensible Authentication Protocol)
  - WPA (WiFi Protected Access)

- **IEEE 802.11i**
  - «WPA2»
  - covers some of the evolutorial extensions by one standard
## Comparison of WEP, WPA, WPA2

<table>
<thead>
<tr>
<th></th>
<th>WEP</th>
<th>WPA</th>
<th>WPA2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encryption</strong></td>
<td>RC4</td>
<td>RC4</td>
<td>AES</td>
</tr>
<tr>
<td><strong>Key length</strong></td>
<td>40 Bit</td>
<td>128 Bit</td>
<td>128 Bit</td>
</tr>
<tr>
<td><strong>IV</strong></td>
<td>24 Bit</td>
<td>48 Bit</td>
<td>48 Bit</td>
</tr>
<tr>
<td><strong>Data integrity</strong></td>
<td>CRC-32</td>
<td>Michael</td>
<td>CCM</td>
</tr>
<tr>
<td><strong>Header integrity</strong></td>
<td>–</td>
<td>Michael</td>
<td>CCM</td>
</tr>
<tr>
<td><strong>Replay attacks</strong></td>
<td>–</td>
<td>IV sequence</td>
<td>IV sequence</td>
</tr>
<tr>
<td><strong>Key management</strong></td>
<td>–</td>
<td>Based on EAP</td>
<td>Based on EAP</td>
</tr>
</tbody>
</table>
Evolutionary solutions

- **WEP128**
  - Proprietary extension of WEP standard
  - WEP with 128 bit encryption (24 Bit IV plus 104 Bit key)

- **WEPplus**
  - Another proprietary extension of WEP standard
  - Defined by Agere Systems (ORiNOCO-Chipset producer)
  - Prevent occurrence of «weak» IVs

- **Unsolved:**
  - No useful authentication
  - No cryptographic integrity
  - Replay/repetition of IVs still very likely
Fast Packet Keying

- Extension for WEP by RSA Security Inc. (Developer of RC4)
  - prevent «weak» IVs
  - prevent repeated combinations of IV and Key
  - Key stream = RC4(PHASE2(PHASE1(TK,TA),IV))

TK Temporal Key
TA Transmitter Address
PPK Per Packet Key
TTAK Key Mixing of TK and TA
Phase 1: Key Mixing
Phase 2: Generating a Per Packet Key
Fast Packet Keying

- **Functionality**
  - Symmetric key TK (Temporal Key), 128 Bit
  - Key Mixing: new key is generated from TK and device address TA (Transmitter Address), 48 Bit
  - Packet Key Generation: 24 Bit IV and WEP Key is generated from a 16 Bit IV and mixed key
  - Input of RC4 is repeated after $4 \cdot 10^{21}$ years

- **Unsolved:**
  - No useful authentication
  - No cryptographic integrity
WEP2

- Task Group i (TGi) within IEEE:
  - Objective: Improvement of WEP
  - New standards: WEP2, WPA, WPA2

- WEP2
  - Extension of IV to 128 Bit
  - Optional authentication of Access Points and Clients via Kerberos
  - Introduction of Session Keys

- Problems:
  - Replay of IVs still possible
  - Weak IVs not excluded
  - Security vulnerability in Kerberos
  - Ineffective authentication
EAP

- Extensible Authentication Protocol
  - Introduced for Remote Access with Dial-In connections
  - Part of 802.1X standard
  - Authentication and key management
  - Low implementation costs in Access Points (AP)
  - No firmware-Upgrade necessary

- Functionality
  - Three systems involved: Client, AP, Authentication server
  - AP works as a proxy between client and Authentication server
  - AP grants access to network after successful authentication
WPA is part of IEEE 802.11i

Functionality
- Authentication via EAP
- Encryption based on RC4 with 128 Bit keys
- New cryptographic integrity protection by alg. «Michael»
- Mechanism to negotiate key length and authentication procedure
- either: Session Key Distribution over RADIUS servers (Remote Authentication Dial-In User Service)
- or: without server via Broadcast/Multicast
- IV is incremented with each packet (prevent replay of IV)
WPA (WiFi Protected Access)

- WPA is part of IEEE 802.11i

- Problems
  - Broadcast/Multicast key is known to all stations
  - «Michael» is relatively weak: $O(2^{20..30})$
  - 1-minute shut-down of AP while receiving more than one wrong authenticate packet (within a given time)
    - Denial-of-Service attacks easy
    - Possible improvements:
      - Reduction of deactivation/disconnection time (ca. 100ms)
      - After n authentication errors, renegotiate Session Keys
802.11i

- **WPA2-Standard adopted in July 2004**
  - Includes WPA
  - Requires hardware upgrade of AP and Client

- **Functionality**
  - Authentication via EAP
  - AES for encryption
  - New protocol for integrity protection