Network Security

Chapter 16

Security of GSM and UMTS Networks
GSM Overview (1)

- The GSM standards:
  - Acronym:
    - formerly: Groupe Spéciale Mobile (founded 1982)
    - now: Global System for Mobile Communication
  - Pan-European standard (ETSI)
  - Simultaneous introduction of essential services in three phases (1991, 1994, 1996) by the European telecommunication administrations (Germany: D1 and D2) → seamless roaming within Europe possible
  - Today many providers all over the world use GSM (more than 130 countries in Asia, Africa, Europe, Australia, America)

- Characteristics:
  - True mobile, wireless communication with support for voice and data
  - Worldwide connectivity and international mobility with unique addresses
  - Security functions:
    - Confidentiality on the air interface
    - Access control and user authentication
GSM Overview (2)

- GSM provides the following security features [ETSI93a, ETSI94a]:
  - **Subscriber identity confidentiality:**
    - Protection against an intruder trying to identify which subscriber is using a given resource on the radio path (e.g., traffic channel or signaling resources) by listening to the signaling exchanges on the radio path
    - Confidentiality for signaling and user data
    - Protection against the tracing of a user's location
  - **Subscriber identity authentication:**
    - Protection of the network against unauthorized use
  - **Signaling information element confidentiality:**
    - Non-disclosure of signaling data on the radio link
  - **User data confidentiality:**
    - Non-disclosure of user data on the radio link

- However, only eavesdropping attacks on the radio link between the mobile and the base stations are taken into account!
## GSM Overview (3)

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUC</td>
<td>Authentication center</td>
</tr>
<tr>
<td>BSC</td>
<td>Base station controller</td>
</tr>
<tr>
<td>BTS</td>
<td>Base transceiver station</td>
</tr>
<tr>
<td>IMSI</td>
<td>International mobile subscriber identity</td>
</tr>
<tr>
<td>HLR</td>
<td>Home location register</td>
</tr>
<tr>
<td>LAI</td>
<td>Location area identifier</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile station (e.g. a mobile phone)</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile switching center</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile subscriber international ISDN number</td>
</tr>
<tr>
<td>TMSI</td>
<td>Temporary mobile subscriber identity</td>
</tr>
<tr>
<td>VLR</td>
<td>Visitor location register</td>
</tr>
</tbody>
</table>
Authentication in GSM (1)

Involved in Authentication:
- MS
- BSS/MSC/VLR
- HLR/AUC
Authentication in GSM (2)

Kᵢ: Individual Subscriber Authentication Key
SRES: Signed Response

A3

MSC

RAND

128 bit

128 bit

SRES* =? SRES

32 bit

SIM

Mobile Network

© Dr.-Ing G. Schäfer

The basic (initial) authentication dialogue:

1.) MS → VLR: (IMSI\textsubscript{MS})
2.) VLR → AUC: (IMSI\textsubscript{MS})
3.) AUC → VLR: (IMSI\textsubscript{MS}, K\textsubscript{BSC,MS}, R\textsubscript{AUC}, SRES\textsubscript{AUC})
4.) VLR → MS: (R\textsubscript{AUC:1})
5.) MS → VLR: (SRES\textsubscript{AUC:1})
6.) VLR → MS: (LAI\textsubscript{1}, TMSI\textsubscript{MS:1})

Remarks:

- SRES\textsubscript{AUC} = A3(K\textsubscript{AUC,MS}, R\textsubscript{AUC}); A3 is an algorithm
- K\textsubscript{BSC,MS} = A8(K\textsubscript{AUC,MS}, R\textsubscript{AUC}); A8 is an algorithm
- R\textsubscript{AUC}, SRES\textsubscript{AUC} are arrays of multiple values
Authentication in GSM (4)

- Re-authentication dialogue with the same VLR:
  1.) MS → VLR: \((\text{LAI}_1, \text{TMSI}_{\text{MS}:n})\)
  2.) VLR → MS: \((\text{R}_{\text{AUC};i})\)
  3.) MSC → VLR: \((\text{SRES}_{\text{AUC};i})\)
  4.) VLR → MS: \((\text{LAI}_1, \text{TMSI}_{\text{MS}:n+1})\)

- Remarks:
  - The *location area identification* LAI\(_1\) allows to detect an MS “coming in” from another area
  - After successful authentication a new temporary mobile subscriber identity TMSI\(_{\text{MS}:n+1}\) is assigned
Authentication in GSM (5)

- Re-authentication dialogue with handover to new VLR₂:
  1.) MS → VLR₂: (LAI₁, TMSIₘₛₙ)
  2.) VLR₂ → VLR₁: (LAI₁, TMSIₘₛₙ)
  3.) VLR₁ → VLR₂: (TMSIₘₛₙ, IMSIₘₛ, Kₜₜ, Rₐᵤｃ, SRESₐᵤｃ)
  4.) VLR₂ → MS: (Rₐᵤｃⁱ)
  5.) MS → VLR₂: (SRESₐᵤｃⁱ)
  6.) VLR₂ → MS: (LAI₂, TMSIₘₛₙ₊₁)

- Remarks:
  - Only unused Rₐᵤｃ, ... are transmitted to VLR₂
  - This scheme can not be used and an initial dialogue is needed:
    - If TMSIₘₛₙ is unavailable at VLR₁, or
    - If VLR₂ is not able to contact VLR₁
  - If VLR₁ and VLR₂ belong to different network operators the handover can not be performed and the call is disconnected
Conclusion on Authentication in GSM (6)

- Only the mobile authenticates itself to the network
- Authentication is based on challenge-response:
  - The AUC in the home network generates challenge-response pairs
  - The MSC/VLR in the visited network checks them
  - Challenge-response vectors are transmitted unprotected in the signaling network
- The permanent identification of the mobile (IMSI) is just sent over the radio link when this is unavoidable:
  - This allows for partial location privacy
  - As the IMSI is sometimes sent in clear, it is nevertheless possible to learn about the location of some entities
    - An attacker may impersonate a base station and explicitly demand mobiles to send their IMSIs!
- Basically, there is trust between all operators!
General Packet Radio Service (GPRS)

- **GPRS (General Packet Radio Service):**
  - Data transmission in GSM networks based on packet switching
  - Using free slots of the radio channels only if data packets ready to send
    (e.g., 115 kbit/s using 8 slots temporarily)

- **GPRS network elements:**
  - **GGSN (Gateway GPRS Support Node)**
    - Interworking unit between GPRS and PDN (Packet Data Network)
  - **SGSN (Serving GPRS Support Node)**
    - Supports the MS (location, billing, security, basically equivalent to MSC)
  - **GR (GPRS Register)**
    - Handles user addresses (equivalent to HLR)

(general GPRS description taken from [Sch03a])
GPRS Logical Architecture
GPRS Protocol Architecture (Transmission Plane)

MS
apps.
IP/X.25
SNDCP
LLC
RLC
MAC
radio

BSS
UM
RLC
MAC
radio
BSSGP
FR

SGSN
SNDCP
LLC
UDP/TCP
BSSGP
IP
FR
L1/L2

GGSN
GTP
IP
UDP/TCP
IP
L1/L2

G:

SNDCP: Subnetwork Dependent Convergence Protocol
GTP: GPRS Tunnelling Protocol
GPRS Security

- Security objectives:
  - Guard against unauthorised GPRS service usage (authentication)
  - Provide user identity confidentiality (temporary identification and ciphering)
  - Provide user data confidentiality (ciphering)

- Realization of security services:
  - Authentication is basically identical to GSM authentication:
    - SGSN is the peer entity
    - Two separate temporary identities are used for GSM/GPRS
    - After successful authentication, ciphering is turned on
  - User identity confidentiality is similar to GSM:
    - Most of the time, only the Packet TMSI (P-TMSI) is send over the air
    - Optionally, P-TMSI “signatures” may be used between MS and SGSN to speed up re-authentication
  - User Data Confidentiality is realized between MS and SGSN:
    - Difference to GSM which just ciphered between MS and BTS
    - Ciphering is realized in the LLC protocol layer
GPRS supports an “optimized handover” including re-authentication (however, this might inhibit a weakness → P-TMSI “signature”)
Overview over the UMTS Security Architecture

(I) **Network access security**: protect against attacks on the radio interface

(II) **Network domain security**: protect against attacks on the wireline network

(III) **User domain security**: secure access to mobile stations

(IV) **Application domain security**: secure message exchange for applications

(V) **Visibility and configurability of security**: inform user of secure operation
Current State of the UMTS Security Architecture

- **Network Access Security:**
  - Currently the most developed part of UMTS security (see below)

- **Network Domain Security:**
  - This part is mainly to be done (in specifications up to Release 5)

- **User Domain Security:**
  - Basically requires that the user authenticates himself to his user services identity module (USIM), e.g. by entering a PIN
  - Optionally, a terminal can require authentication of the USIM

- **Application Domain Security:**
  - Defines a security protocol to be used between applications running in the terminal / USIM and some system in the network (3GPP TS 23.048)
  - Somewhat out of the scope of mobile communications security

- **Visibility and configurability of security:**
  - Defines requirements so that the user will be in control of security features

→ In the following, we will concentrate on network access security
UMTS Network Access Security Services (1)

- **User identity confidentiality:**
  - *User identity confidentiality:* the property that the permanent user identity (IMSI) of a user to whom a service is delivered cannot be eavesdropped on the radio access link.
  - *User location confidentiality:* the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link.
  - *User untraceability:* the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

- **Entity authentication:**
  - *User authentication:* the property that the serving network corroborates the user identity of the user.
  - *Network authentication:* the property that the user corroborates that he is connected to a serving network that is authorized by the user's HE to provide him services; this includes the guarantee that this authorization is recent.
UMTS Network Access Security Services (2)

- **Confidentiality:**
  - *Cipher algorithm agreement:* the property that the MS and the SN can securely negotiate the algorithm that they shall use subsequently
  - *Cipher key agreement:* the property that the MS and the SN agree on a cipher key that they may use subsequently
  - *Confidentiality of user data:* the property that user data cannot be eavesdropped on the radio access interface
  - *Confidentiality of signaling data:* the property that signaling data cannot be eavesdropped on the radio access interface

- **Data Integrity:**
  - *Integrity algorithm agreement*
  - *Integrity key agreement*
  - *Data integrity and origin authentication of signaling data:* the property that the receiving entity (MS or SN) is able to verify that signaling data has not been modified in an unauthorized way since it was sent by the sending entity (SN or MS) and that the data origin of the signaling data received is indeed the one claimed
### Overview of the UMTS Authentication Mechanism (1)

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AK</td>
<td>Anonymity Key</td>
</tr>
<tr>
<td>AMF</td>
<td>Authentication management field</td>
</tr>
<tr>
<td>AUTN</td>
<td>Authentication Token</td>
</tr>
<tr>
<td>AV</td>
<td>Authentication Vector</td>
</tr>
<tr>
<td>CK</td>
<td>Cipher Key</td>
</tr>
<tr>
<td>HE</td>
<td>Home Environment</td>
</tr>
<tr>
<td>IK</td>
<td>Integrity Key</td>
</tr>
<tr>
<td>RAND</td>
<td>Random challenge</td>
</tr>
<tr>
<td>SQN</td>
<td>Sequence number</td>
</tr>
<tr>
<td>SN</td>
<td>Serving Network</td>
</tr>
<tr>
<td>USIM</td>
<td>User Services Identity Module</td>
</tr>
<tr>
<td>XRES</td>
<td>Expected Response</td>
</tr>
</tbody>
</table>
Overview of the UMTS Authentication Mechanism (2)

MS | VLR/SGSN | HE/HLR

- Distribution of authentication vectors from HE to SN
- Authentication data request
- Generate authentication vectors AV(1..n)
- Authentication data response AV(1..n)
- Store authentication vectors
- Select authentication vector AV(i)
- User authentication request
  - RAND(i) || AUTN(i)
  - Verify AUTN(i) || AUTN(i)
- Compute RES(i)
- User authentication response
  - RES(i)
  - Compare RES(i) and XRES(i)
- Compute CK(i) and IK(i)
- Select CK(i) and IK(i)
- Authentication and key establishment

(Source [3GPP00a])
Generation of UMTS Authentication Vectors (1)

- Generate SQN
- Generate RAND

SQN
AMF
K

f1
f2
f3
f4
f5

MAC
XRES
CK
IK
AK

AUTN := SQN \oplus AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

(Source [3GPP00a])
Generation of UMTS Authentication Vectors (2)

- The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND
  - For each user the HE/AuC keeps track of a counter SQN_{HE}
- An authentication and key management field AMF is included in the authentication token of each authentication vector
- Subsequently the following values are computed:
  - a message authentication code \( MAC = f_1_K(SQN || RAND || AMF) \) where \( f_1 \) is a message authentication function
  - an expected response \( XRES = f_2_K(RAND) \) where \( f_2 \) is a (possibly truncated) message authentication function
  - a cipher key \( CK = f_3_K(RAND) \) where \( f_3 \) is a key generating function
  - an integrity key \( IK = f_4_K(RAND) \) where \( f_4 \) is a key generating function;
  - an anonymity key \( AK = f_5_K(RAND) \) where \( f_5 \) is a key generating function
- Finally the authentication token AUTN = SQN \( \oplus \) AK \( || \) AMF \( || \) MAC is constructed.
UMTS User Authentication Function in the USIM (1)

Verify MAC = XMAC
Verify that SQN is in the correct range

(Source [3GPP00a])
UMTS User Authentication Function in the USIM (2)

- Upon receipt of RAND and AUTN the USIM:
  - computes the anonymity key $AK = f_5^K(RAND)$
  - retrieves the sequence number $SQN = (SQN \oplus AK) \oplus AK$
  - computes $XMAC = f_1^K(SQN || RAND || AMF)$ and
  - compares this with MAC which is included in AUTN.
  - If they are different, the user sends *user authentication reject* back to the VLR/SGSN with an indication of the cause and the user abandons the procedure.
  - If the MAC is correct, the USIM verifies that the received sequence number $SQN$ is in the correct range:
    - If the sequence number is not in the correct range, the USIM sends *synchronisation failure* back to the VLR/SGSN including an appropriate parameter, and abandons the procedure
    - If the sequence number is in the correct range, the USIM computes:
      - the authentication response $RES = f_2^K(RAND)$
      - the cipher key $CK = f_3^K(RAND)$ and the integrity key $IK = f_4^K(RAND)$. 

Conclusions on Security in UMTS Release ‘99

- UMTS Release ‘99 security is quite similar to GSM security:
  - The home AUC generates challenge-response vectors
  - The challenge-response vectors are transmitted unprotected via the signaling network to a visited network that needs to check the authenticity of a mobile
- Unlike in GSM, the network also authenticates itself to the mobile
- The IMSI which uniquely identifies a user:
  - is still revealed to the visited network
  - can still be demanded by an attacker which impersonates a base station, as there is no network authentication in this case!
- The security model still assumes trust between all network operators
- Confidentiality is only provided on the radio link

Concluding, UMTS Release ‘99 is designed to be just as secure as an insecure fixed network
Additional References


[3GPP02b] 3GPP. Security Mechanisms for the (U)SIM application toolkit; Stage 2. 3GPP TS 23.048, V5.5.0, December 2002.


