Case Study: security in GSM and UMTS

Security in Networked Computing Systems
GSM and UMTS security

GSM
System model

Mobile Device

Currently Serving Network

Home Network

MD: Mobile Device
BTS: Base Transceiver Station
BSC: Base Station Controller
MSC: Mobile Switching Center
BSS: Base Station System

VLR: Visitor Location Register
HLR: Home Location Register
AuC: Authentication Center
Ki: Secret per subscriber key
SIM: Subscriber Identity Module
IMSI: International Mobile Subscriber Identity

Ki
A3
A8
A5
IMSI

A5

A5

Ki
A3
A8
IMSI

09/05/16
GMS and UMTS security
Security model

• What is supported
  – Mobile device authentication
  – Encryption of the air interface between MD and BTS

• What it is NOT supported
  – Network authentication
  – Integrity
Registration

• Each user (subscriber) registers for a Home Provider (Network)

• HP associates the user with IMSI and Ki (128 bit)
  – IMSI: International Mobile Subscriber Identity

• IMSI and Ki are stored on HN’s AuC and SIM
  – SIM: Subscriber Identity Module
Security algorithms

• Authentication and Key agreement
  – A3: Authentication algorithm
  – A8: Key generation algorithm
  – Provider specific

• Encryption algorithms
  – A5/0 (no encr), A5/1 (standard), A5/2 (weaker that A5/1),
    A5/3 (similar to KASUMI)
  – A5/0, A5/1 and A5/2 are mandatory
  – Standardized, no provider-specific

• Implemented by MD and BTS
GSM authentication: simplified

MD                  FN                  HN
|                  |        REQ, IMSI        |                  |
|+––––––––––––––––––––––––>‌                                                          |
|                  |                         |                  |
|                  |  RAND, RES, Kc          |                  |
|                  |<––––––––––––––––––––––––+                  |
|                  |                         |                  |
|                  |          RAND           |                  |
|                  |                  <–––––––––––––––––––––––––‌|
|                  |                         |                  |
|                  |          RES*           |                  |
|                  |+––––––––––––––––––––––––>‌                  |

\[
Kc = A8(Ki, RAND)
\]

\[
RES = A3(Kc, RAND)
\]

if (RES == RES*)
    return true;
else return false;

HN: Home Network; FN: Foreign Network

Pre-defined secure channel
Analysis

\[ MD, HN \models MD \leftrightarrow HN \]
\[ FN \models FN \leftrightarrow MD \]
\[ FN \models \#(RAND) \]
\[ FN \models \#(FN \leftrightarrow MD) \]
\[ FN \models MD \models (FN \leftrightarrow MD) \]

Registration

By virtue of the secure channel between FN and HN

Final belief

\[ MN \text{ achieves no beliefs} \]
GSM authentication

Figure 7.2: GSM Authentication, Key Agreement, and Security-Mechanism Negotiation

- IMSI
- TMSI
- Authentication challenge
- Authentication response
- Encryption key
- GSM cipher mode command
- Start deciphering and start encryption
- Any correctly deciphered message
- Start encryption

RRC connection establishment including:
- Security capabilities
- Encryption mechanisms

MD → BTS → MSC/HLR → MSC/VLR

Kc, K_i, A8 / A3, RES, RAK

RES = RES

RAND, A8 / A3

K_i, Kc

A8 / A3

RES, RAND, K_i, Kc

In particular, it is unclear what happens if the new BTS does not support the A5 algorithm used between the source BTS and MD.

Most networks can be expected to support the same algorithms on every BTS throughout the network, such that the same algorithm can be used before and after handover. However, e.g. due to a sequential upgrade of BTSs, this is not necessarily the case.
Negotiation and policies

- Negotiation
  - MD sends its security (encryption capabilities)
    - FN drops connection if MD does not enforce mandatory algorithms
  - FN chooses one of the encryption algorithms and acknowledges its choice to MD
    - Even A5/0 or A5/2
    - HN has no influence
    - MD cannot enforce the use of A5/1 or A5/3
Anonimity

- In order to protect anonymity, IMSI is sent in the clear over the ai interface as rarely as possible

- Upon first connection FN associates a TIMSI to MD
  - Upon next connection, MD presents its TIMSI to the FN
  - If FN is not able to resolve the TIMSI, it requests MD its IMSI and a new TIMSI is allocated
Intra-provider roaming

• Inter-provider roaming always causes roaming authentication
• This is not the case if MD is in idle-mode and moves within the same network
• Kc is moved to the next BTS or MSC, as needed
• If encryption between MD and BTS was disabled, it is not re-enabled after roaming to the next BTS
• Standard say nothing if the next BTS does not support the A5 alg chosen by the previous one
Impersonation attack

- **One-dide MiM** An attacker impersonates a fake base station to MD
  - The attacker makes MD to connect to the fake base station
  - The attacker requests MD to turn encryption off
  - The attacker can eavesdrop on all mobile traffic
  - Unless the attacker cannot impersonate MD to a real network as well, MD will be unreachable for incoming traffic
    - The attacker need Kc!
Impersonation attack

- **Two-sided MiM** An attacker can impersonate a MD during authentication by simply forwarding the authentication traffic
  - It’s not easy for the adversary to turn encryption off because of mandatory algorithms
- The attacker succeeds if (s)he knows that a network always uses A5/0
  - Actually the attacker can make MD to connect to a network that disables encryption
GSM and UMTS security

UMTS
System model

MD: Mobile Device
Node B: Base Transceiver Station
RNC: Radio Network Controller
VLR: Visitor Location Register
UTRAN: UMTS Terrestrial Radio Access Network

MSC: Mobile Switching Center
HLR: Home Location Register
AuC: Authentication Center

K\textsubscript{U}: Secret per subscriber key
f1–f5: key generation functions
f8: encryption mechanism
f9: integrity protection mechanism

GMS and UMTS security
Security model

• Mobile device and visited network mutual authentication
• Integrity
• Encryption of the air interface between MD and BTS
Registration

• Each user (subscriber) registers for a Home Provider (Network)

• HP associates the user with IMSI and Ku (128 bit)
  – IMSI: International Mobile Subscriber Identity

• IMSI and Ki are stored on HN’s AuC and SIM
  – USIM: Universal Subscriber Identity Module
  – USIM implements crypto-functions f1, f2, f3, f4, f5 (MILENAGE)
  – These functions are provider-dependent
Confidentiality and integrity

• End-to-end confidentiality and integrity between MD and RNC
  – Encryption and integrity algorithms are implemented on the MD
• No mechanism to restrict $K_c$ lifetime
• Encryption
  – Up to 16 encryption algs
  – Currently UEA0 (no encryption) and UEA1 (stream cipher built on KASUMI)
• Integrity
  – Up to 16 integrity algs
  – Currently UIA0 built on KASUMI
UMTS authentication: simplified

Security capabilities
Selected algorithms
RES = f2(Ku, RAND)
CK = f3(Ku, RAND)
IK = f4(Ku, RAND)
AUTN = SQN xor f5(Ku, RAND) || AMF || f1(Ku, SQN||AMF)

if (RES == RES*)
    return true;
else return false;

Pre-defined secure channel
Analysis

Assumptions

\[ KD, \; HN \models MD \leftrightarrow HN \]

\[ KN \models (MD \leftrightarrow HN, MD \leftrightarrow HN) \]

Goals

\[ FN \models MN \models (FN \leftrightarrow MD) \]

\[ IK \]

\[ MD \models HN \models (MD \leftrightarrow HN) \]

\[ MD \models HN \models (\text{security capabilities}) \]

Mutual authentication
UMTS Authentication

**RRC connection establishment**
- including: security capabilities
- integrity/encryption mechanisms

**TMSI**
- try to resolve TMSI

**IMSI**
- identity request

**authentication challenge**
- RAND, AUTN

**authentication response**
- RES

**verify AUTN**
- compute RES, CK, IK

**verify RES**
- decide allowed mechanisms
- CK, IK

**allowed mechanisms**
- decide mechanisms
- start integrity protection

**security mode command**
- selected algorithms, security capabilities
- protected with IK

**verify sec. cap. and integ. protection on sec. mode command**

**generate auth. vector**
- RAND, AUTN, IK, CK, RES

**authentication vector**
- RAND, AUTN, IK, CK, RES

**authentication data request**
- generate auth. vector

**UMTS**
- Node B / RNC
- SGSN/MSC/VLR
- GSN/MSC/HLR
Negotiation and policies

- MD and FN negotiate encryption-/integrity-algs
- After authentication of MD, FN selects a pair of algs
  - MD is mandated to implement *no-encryption* (UEA0)
  - Neither MD nor HN can enforce encryption to be enabled
- UMTS uses the same TIMSI mechanism as GSM
- Intra-provider roaming is similar to GSM
Impersonation attack

By means of \textit{secap}' the adversary could claim to support only the mandatory encryption algorithms (security capabilities)