Mobile Network Security

ACN / Mobile Security 2020

Johannes Feichtner
johannes.feichtner@iaik.tugraz.at
Outline

- **Theory**
  - Architecture of 2G / 3G networks, Evolution of 2G, 3G, 4G
  - GSM encryption

- **Attacks**
  - Active: IMSI Catchers, Passive: Cracking A5/1
  - Signaling System 7, LTE Security

- **Protection Mechanisms**
  - Are you protected? How to defend yourself?
Introduction

Goals

● Protect business models and operational services
● Privacy for user identity, data confidentiality
● Regulatory issues → legal interception

How to apply security?

● Minimize number of security threats
● Remember: Cost efficiency & high performance (load balancing)
● Interoperability with legacy systems (GSM <-> UMTS)
● Practical issues, e.g. end-to-end vs. hop-by-hop security?
Introduction

Technical objectives

● Authentication of user and network
● Confidentiality
  – User data & signaling data
  – User & device identity
  – User location
● Signaling data integrity
● User untraceability (?)

→ Need strong algorithms for enciphering and integrity,
→ Need algorithm extensibility for future proofness
Some theory...
3G/4G Network Structure

Legend
- Node B
  UMTS Base Station
- RNC
  Radio Network Controller
- SGSN
  Serving GPRS Support Node
- GGSN
  Gateway GPRS Support Node
- MSC
  Mobile Switching Center

Source: https://goo.gl/V98GB5
3G/4G Network Workflow

1) **Node B**
   - Minimum functionality base station in UMTS networks
   - Typically located near the antenna (but not necessarily)
   - Controlled by RNC using a „lub“ interface

2) **RNC**
   - Main task: Manage connected Node Bs and radio resources
     - Channels, signal strength (power), cell handover
   - Can build Mesh networks with other RNCs

3a) **Speech:** MSC (Mobile Switching Centre) $\rightarrow$ routing voice / SMS
3b) **Data:** SGSN $\rightarrow$ routing data

**GSM equivalent:** Base Transceiver Station (BTS)
3G/4G Network Components

SGSN
- Data delivery from/to mobile station in defined geographical service area
- (De-)tunnel packets from/to GGSN (*Downlink*, *Uplink*)
- Handover → phone moves from **Routing Area A** to **Routing area B**
- User data billing

GGSN
- Inter-networking between internal network and external packet switched networks (Internet)
- Keeps your connections alive while moving around
- User authentication, IP pool management, QoS
GSM Encryption

How? Stream ciphers to encrypt traffic on air interface

Set of algorithms

- A5/0: Unencrypted, no cracking needed 😊
  → broken (and partly banned, e.g. by T-Mobile Austria)
- A5/1: Combination of 3 linear feedback shift registers (LFSRs)
  → 64-bit key, broken using rainbow tables in 2009
- A5/2: export version of A5/1
  → broken in 1999, banned since 2006
- A5/3 + A5/4: Backport of Kasumi UMTS cipher (current standard)
  - 128-bit key, 64-bit input / output
GSM Encryption A5/1

Key size: 64 bits(!)

Avoid replay attacks

Diagram:
- Kc (64 bits)
- Frame number (22 bits)
- A5 key stream generator
- Pseudorandom key stream (114 bits)
- Plaintext message (114 bits)
- XOR
- Encrypted message (114 bits)
Evolution: 2G Networks

- Commerical launch in 1992
- User authentication based on per-subscriber secret key in SIM
- TDMA-based, circuit switching
  - "Time Division Multiple Access"
  - Share same frequency channel for multiple users by dividing signal into different time slots

Versions

- 2.5G: GPRS (added in 2000)
  - Theoretical speed: 171 kbps down, 40 kbps up
- 2.7G: EDGE
  - Theoretical speed: 384 kbps down, 108 kbps up
Evolution: 3G Networks

Features

- Same core network as 2G
  - Still circuit-switched (GSM) & packet-switched hybrid (UMTS)
- No integrity protection (like LTE) → Downgrade attacks possible
- Almighty base station → Decides if, when, and how to authenticate / encrypt

Versions

- **3G** UMTS max. 2 Mbps down, 384 kbps up
- **3.5G** HSDPA max. 14.4 Mbps down, 2 Mbps up
- **3.6G** HSUPA max. 14.4 Mbps down, 5.76 Mbps up
- **3.75G** HSPA+ max. 21 Mbps down, 5.8 Mbps up
- **3.8G** HSPA+ Enhanced max. 84 Mbps down, 20 Mbps up
- **3.9G** LTE (pre 4G!) max. 100 Mbps down, 50 Mbps up
Evolution: 4G Networks

Currently: LTE Advanced (LTE-A) max. 1 Gbit down, 500 Mbit up

Features

- Only IP-based communication (also voice → VoLTE), no more circuit switching
  - Fallback support for circuit-switched calls
- **Mutual authentication** between base station & mobiles
- **Mandatory integrity protection** for signaling messages
- IMEI ciphered to protect user equipment privacy

- New algorithms and extensibility
  - Word-oriented stream cipher (128 bit key): SNOW 3G
  - Integrity, confidentiality: AES-GCM
(Recent) Attacks
Scenarios

**Intercept**
- Adversary records calls & SMS
  - Decryption in real time or batch process (after recording)

**Impersonation**
- Calls or SMS spoofed
- Received using stolen mobile identity

**Tracking**
- Tracing mobile subscribers
  - a) using Internet-leaked information
  - b) locally by repeated TMSI pagings
Active Attack: Fake Base Stations

= IMSI Catchers

- Partially exploit weaknesses in GSM & 3G networks
- Used for
  - Tracking users (IMEI, IMSI, location)
  - Eavesdropping calls, data, SMS, etc.
  - Man-in-the-Middle
  - Attack phone using operator system messages,
    - e.g. Management Interface, re-program APN, HTTP proxy, SMS/WAP server, ...
  - Attack SIM or phone baseband
  - Geo-targeting ads (SMS)
  - Intercept TAN, mobile phone authentication, ...
How does it work?

- Advertise base station on beacon channel
- Phone sends IMSI / TMSI (sort of secret)
- MCC: Mobile Country Code (232 for .at)
  - Country-specific tuple with MCC, e.g. 232-01 for a1.net

→ Phones will connect to *any* base station with spoofed MNC/MCC
  - If you claim it, they will come because strongest signal wins 😊
  - Crypto optional (until 4G) and set by base station!
## IMSI Catchers in Practice

<table>
<thead>
<tr>
<th>User identification</th>
<th>Traffic Man-in-the-middle</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Retrieve IMSI / IMEI / TMSI</td>
<td></td>
</tr>
<tr>
<td>- Reject location update</td>
<td></td>
</tr>
<tr>
<td>- Tracking</td>
<td></td>
</tr>
<tr>
<td>- Hold user in cell</td>
<td></td>
</tr>
<tr>
<td>- Actively intercept traffic</td>
<td></td>
</tr>
<tr>
<td>- Relay to real network</td>
<td></td>
</tr>
<tr>
<td>- Active or passive decryption</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UMTS Downgrade</th>
<th>Hold but intercept passively</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Blocking UMTS transmission</td>
<td></td>
</tr>
<tr>
<td>- Spoofing system messages</td>
<td></td>
</tr>
<tr>
<td>- Imprison in cell</td>
<td></td>
</tr>
<tr>
<td>→ Phone not lost to neighbor cell</td>
<td></td>
</tr>
</tbody>
</table>
Fake Base Stations

**Dirtboxes on a Plane**
How the Justice Department spies from the sky

1. Planes equipped with fake cellphone-tower devices or ‘dirtboxes’ can scan thousands of cellphones looking for a suspect.
2. Non-suspects’ cellphones are ‘let go’ and the dirtbox focuses on gathering information from the target.
3. The plane moves to another position to detect signal strength and location...
4. ...the dirtbox will ‘let go’ of the suspect’s phone once officers move into position nearby. Those officers then use their handheld device to connect to the phone and zero in on the suspect.

Source: people familiar with the operations of the program
Source: [https://goo.gl/C2GUCK](https://goo.gl/C2GUCK)
Active Attack: DoS

Fake base station sending messages

- "You are an illegal cellphone"
- "Here is no network available. You could shut down your 2G/3G/4G modem."

Attach Request message can include cause for reject

→ Some special causes result in no service...
Passive Attack: Key Cracking

- A5/1 vulnerable to generic pre-computation attacks
  - Goal: Break session key for communication between base station and phone

How to?
1. Intercept GSM call with reprogrammed 20 euro phone
   - Idea: Cluster multiple phones for wide-scale capture
2. Crack A5/1 session key using rainbow tables (1-2 TB)
   - Done in a few seconds using GPU power

Note: Also A5/3 uses only 64 bit key on SIM & USIM
- According to „Intercept“ broken by NSA
- GSM A5/4 and UMTS UEA/1 considered secure with USIM (128 bit key)
Signaling System 7

- Protocols used by most Telcos to identify network elements, clients, ...
- Share session key in case of **roaming** (but works also without roaming!)

**Problem:**
- Walled-garden approach → we trust each other, need no auth
- Getting access is easy
  - Buy from telcos for < 1000 euro / month
  - Find equipment unsecured on internet (Shodan)

**Attacker’s playground**
- Track any phone using a variety of signaling messages, e.g.
  - Phone number → **AnytimeInterrogation** → Get subscriber location (Cell ID)
Send from any international SS7 inter-connection → abuse legitimate messages

Abuse Scenario
- Local passive intercept: SendIdentification
  → Easily blockable at network boundary
- 3G IMSI catcher: SendAuthenticationInfo
- Rerouting attacks: UpdateLocation
  → Message required for operations

Source: https://goo.gl/YBhvXw
## Signaling System 7

### How to intercept 3G (A5/3)?

1. Use software-defined radio (SDR) to capture 3G transactions
2. Query SS7 SendIdentification to get decryption key

*Note*: For many networks no SS7 needed for 3G interception!

<table>
<thead>
<tr>
<th>Network</th>
<th>Encrypts</th>
<th>Authenticates calls / SMS</th>
<th>Protects integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cambodia</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>India</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>South Korea</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Russia</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>

Source: [https://goo.gl/YBhvXw](https://goo.gl/YBhvXw)
LTE Security

Cipher & USIM improvements

→ No known ways to break used crypto, recover key from SIM, break authentication, encryption, or integrity protection

But...

● Not everything is encrypted
  – E.g. null encryption supported → Data is simply (unencrypted) plaintext

● Several messages allowed without integrity protection
  – E.g. null integrity for emergency calls, broadcast system, cell handover
Low-cost IMSI catcher for 4G/LTE networks tracks phones’ precise locations

$1,400 device can track users for days with little indication anything is amiss.

What?
Exploiting LTE specification flaws

Problems?

- RRC Protocol
  - Measurement reports for handover
    - Not authenticated, not encrypted

- EMM Protocol
  - Control device mobility
    - Not integrity protected

Attacker can

- Track user location / movements
- Downgrade to non-LTE

The attacks target the LTE specification, which is expected to have a user base of about 1.37 billion people by the end of the year, and require about $1,400 worth of hardware that run freely available open source software. The equipment can cause all LTE-compliant phones to leak their location to within a 32- to 64-foot (about 10 to 20 meter) radius and in some cases their GPS coordinates,

Source: http://goo.gl/jIDjQ
Use with popular open source LTE projects

- OpenLTE  See: https://goo.gl/GEUeHV
- Open Air Interface  See: https://goo.gl/qSNrxk
Other Attack Vectors

- Branded mobile equipment
  - 3G/4G USB modems
  - Routers / Access points
  - Smartphones, femtocell, branded apps

- (U)SIM cards
  - Cracking SIM update keys, deploy SIM malware

- Radio / IP access network
  - Radio access network
  - IP access (GGSN, Routers, GRX)

See:
- http://goo.gl/kiAJpe
- https://goo.gl/WYxUTq
- http://goo.gl/c3CNZ0
Protection Mechanisms
Measures in Austria

- Numbers from 2014 (no LTE!)
- All 3G networks use A5/3 with encryption enabled
  - A1 & T-Mobile roll-out for 2G
- Unclear if networks would accept unencrypted transactions as well (subscriber-initiated)
- Call/SMS impersonation possible in all 2G networks

Source: https://goo.gl/fCqBZW
Abuse often detectable!

<table>
<thead>
<tr>
<th>Attack scenario</th>
<th>Detection heuristic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SMS Attacks</strong></td>
<td><strong>Unsolicited binary SMS</strong></td>
</tr>
<tr>
<td><strong>SS7 Attacks</strong></td>
<td><strong>Silent SMS</strong></td>
</tr>
<tr>
<td><strong>SIM OTA attacks</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Semi-lawful Tracking through silent SMS</strong></td>
<td><strong>Empty paging</strong></td>
</tr>
<tr>
<td><strong>SS7 abuse: Tracking, Intercept, etc.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Tracking or Intercept</strong> through 2G or 3G fake base station</td>
<td><strong>Unusual cell configuration and cell behavior (detailed later in this chapter)</strong></td>
</tr>
<tr>
<td><strong>Insufficient encryption leads to Intercept and Impersonation</strong></td>
<td><strong>Encryption level and key change frequency</strong></td>
</tr>
<tr>
<td><strong>Lack of TMSI updates enables Tracking</strong></td>
<td></td>
</tr>
</tbody>
</table>

Source: [https://goo.gl/jFtXYu](https://goo.gl/jFtXYu)
SnoopSnitch

Collect network traces on Android → analyze for abuse

Features

- Detection of fake base station (IMSI catcher)
  - Suspicious cell configuration / behaviour
- User tracking
- SS7 attacks

Requirements

- Rooted phone with Android >= 4.1
- Qualcomm chipset
  - Samsung Galaxy S4/S5, Sony Z1, OnePlus 2, ...

Source: https://goo.gl/KlhaZa
AIMSICD

Features

● Focus: Detecting IMSI catchers
● Check consistency of
  – Tower information
  – LAC / Cell ID
  – Signal strength
● Detect silent SMS (type 0 messages)
● Detect FemtoCells

Requirements

● Rooted Android
● Ability to send AT commands to modem

Source: https://goo.gl/mbZFgE
Network Protection Status

Austria

Source: http://gsmmmap.org
Physical Cell Locations

**Tip:** Um Standorte in Ihrer Umgebung zu finden geben Sie im Feld "Adresse, Ort oder PLZ" die Postleitzahl bzw. den Namen der gesuchten Gemeinde ein und klicken Sie anschließend auf die Taste "Suchen".

### Allgemeine Daten
- **Standortanfrage versenden**: 
- **Funkdienst**: Mobilfunk
- **Trägerstruktur**: Mast
- **Gemeinsame Nutzung (Sharing)**: Nein
- **Station1**
  - **Protokoll(e)**: GSM, UMTS, LTE, 5G
  - **Sendeleistung**: 380-400 W

**Mehr Informationen finden Sie im Kapitel Erläuterungen und Technik**

Source: https://www.senderkataster.at
Physical Cell Locations

Source: https://opencellid.org
Outlook

- 18.06.2020
  - Presentation of your results of task 2