Security in cellular-radio access networks

Ravishankar Borgaonkar, Oxford University

5G Security Workshop
Stockholm, Sweden
11 May 2016
Outline

- Radio Access Network
- Layered Security
- Emerging low cost attacks
- From 5G perspective
- Conclusion
Radio Access Network

- Connects mobile devices to the serving network
  - Allow legitimate devices only
  - Energy efficient
  - Establish secure communication channel

- Needs protocol with tradeoff decisions
  - Security vs availability vs performance vs functions

- Availability is vital – critical services in recent Brussels attack
Radio Access Network 2G/3G/4G

Note: picture provides an abstract view only
LTE Architecture

- **eNodeB**: Evolved Node B ("base station")
- **E-UTRAN**: Evolved Universal Terrestrial Access Network
- **MME**: Mobility Management Entity
- **UE**: User Equipment
- **S1**: Interface

**Diagram Details**:
- **E-UTRAN**: Evolved Universal Terrestrial Access Network
- **Cell**: The area covered by a single eNodeB
- **UE**: User Equipment
- **eNodeB**: Evolved Node B ("base station")
- **MME**: Mobility Management Entity
- **S1**: Interface
- **Tracking Area**: The area where a UE can be tracked

**Internet**
Security evolution in mobile networks

Phone

Base Station

2G
- no mutual authentication

3G
- mutual authentication
- integrity protection

4G
- mutual authentication
- deeper mandatory integrity protection

decides encryption/authentication
requests IMSI/IMEI
Security aspects

Authentication
Availability
Confidentiality
Integrity
Security aspects and attacks

Security tradeoffs play essential role in protocol design.
Low cost attacking infrastructure

- 2G/3G/4G* network setup cost < 1000 USD
  - Open source software & hardware
  - USRP, Osmocom, OpenBTS, OpenLTE, etc
- IMSI catcher device problem
- Targeted attacks from illegal actors
- Almost no detection capabilities for the end-users
Emerging attack examples
Implementation issues on RAN

From TS 124.008 v11.8.0: If MAC failure, then phone should not communicate with BTS (2G)

Table 2. Baseband behavior on MAC failure

<table>
<thead>
<tr>
<th>Phone</th>
<th>Vendor</th>
<th>Version</th>
<th>Call in/out</th>
<th>SMS in/out</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 5</td>
<td>Qualcomm</td>
<td>10b350 3.04.25</td>
<td>OK/OK</td>
<td>OK/OK</td>
</tr>
<tr>
<td>iPhone 4</td>
<td>Qualcomm</td>
<td>MC605IP/A 04.12.09</td>
<td>OK/OK</td>
<td>OK/OK</td>
</tr>
<tr>
<td>Galaxy S2</td>
<td>Infineon</td>
<td>I9100BOLP5</td>
<td>OK/OK</td>
<td>OK/OK</td>
</tr>
<tr>
<td>Galaxy SIII</td>
<td>Infineon</td>
<td>I9300BOLF1</td>
<td>OK/OK</td>
<td>OK/OK</td>
</tr>
<tr>
<td>Samsung corby pro</td>
<td>unknown</td>
<td>B5310AEJ1</td>
<td>OK/OK</td>
<td>OK/OK</td>
</tr>
<tr>
<td>Google nexus 1 (HTC)</td>
<td>Qualcomm</td>
<td>32.41.00.32U 5.08.00.04</td>
<td>OK/OK</td>
<td>OK/OK</td>
</tr>
<tr>
<td>Geekphone</td>
<td>Qualcomm</td>
<td>unknown</td>
<td>OK/OK</td>
<td>OK/OK</td>
</tr>
<tr>
<td>Keon</td>
<td>Qualcomm</td>
<td>unknown</td>
<td>OK/OK</td>
<td>OK/OK</td>
</tr>
<tr>
<td>Nokia N900</td>
<td>Nokia</td>
<td>20.2010.36-2</td>
<td>blocked</td>
<td>blocked</td>
</tr>
</tbody>
</table>

Table from the paper “Implementing an Affordable and Effective GSM IMSI Catcher with 3G Authentication”
IMSI catchers (1)

• Exploit weakness in authentication methods
• Location tracking and interception
• Protection for ‘active attacks’ not considered
• Lack of security indicator implementation
3G AKA vulnerability(2)

• Linkability attack by Arpanis et al

• Affects in 4G as well
4G Feature: Reports from UE to eNodeB (3)

RRC protocol – 3GPP TS 36.331

- Measurement reports (handovers)
  - List of visible eNodeBs, signal strengths, UE’s GPS co-ordinates
- RLF Reports (radio link troubleshooting)
Vulnerabilities in the feature

**Specification**

- UE measurement reports
  - Requests not authenticated
  - Reports are not encrypted

**Implementations**

- RLF reports
  - Requests not authenticated
  - Reports are not encrypted
  - All baseband vendors
3GPP Specification issues (1)

• RRC protocol – 3GPP TS 36.331

• ‘UE Measurement Report’ messages

• Necessary for handovers & troubleshooting

• No authentication for messages

• Reports not encrypted

<table>
<thead>
<tr>
<th>MeasurementReport</th>
<th>+</th>
<th>-</th>
<th>-</th>
<th>Justification for case “P”: RAN2 agreed that measurement configuration may be sent prior to security activation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>P...Messages that can be sent (unprotected) prior to security activation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A - I...Messages that can be sent without integrity protection after security activation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A - C...Messages that can be sent unciphered after security activation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4G Feature: Mobility Management (4)

EMM protocol – 3GPP TS 36.331

Tracking Area Update (TAU) procedure
- During TAU, MME & UE agree on network mode (2G/3G/4G)
- “TAU Reject” used to reject some services (e.g., 4G) to UE

Specification vulnerability: Reject messages are not integrity protected
3GPP Specification issues (2)

- EMM protocol – 3GPP TS 36.331
- ‘Tracking Area Update Reject’ messages
- Necessary for UE mobility
- No integrity protection for reject messages
- Recovery mechanism not effective

Upon expiry of the timer T3245, the UE shall erase the "forbidden PLMN list", the "forbidden PLMNs for GPRS service" list, and the "forbidden PLMNs for attach in S1mode" list and set the USIM to valid for non-EPS and EPS services.
Practical Attacks
Location Leaks: tracking subscriber coarse level

Target

Semi-passive Attacker (TA/cell)

Mapping GUTI to Social Identity

Location Accuracy: 2 Sq. Km
DoS Attacks

Exploiting specification vulnerability in EMM protocol!

• Downgrade to non-LTE network services (2G/3G)
• Deny all services (2G/3G/4G)
• Deny selected services (block incoming calls)
• Persistent DoS
• Requires reboot/SIM re-insertion
Reasons for vulnerabilities

Trade of between security and

• Performance
  • Phone restricts to connect to network- saving power
  • Saving network signaling resources (avoid unsuccessful attach)
  • Operator do not refresh temporary identifiers often

• Availability
  • Operators require unprotected reports for troubleshooting

• Functionality
  • Smartphone apps on generic platforms not mobile-network-friendly

• Attacking cost
  • Active type of IMSI catcher attacks thought to be expensive
5G Networks Perspective

Authentication

- Asymmetric keys for IMSI protection
- Improve AKA protocols

Availability

- Remove unnecessary protocol messages
- Effective recovery mechanisms
5G Networks Perspective

Confidentiality & Integrity

- Encryption
- Indicators & APIs

- Dynamic Policies
Conclusions

• **Specification & implementation vulnerabilities**

• **Lead to attacks:**
  - Silent tracking
  - DoS attacks are persistent & silent to users

• **Design trade-offs made a decade ago no longer effective**

• **For 5G Networks:**
  - New trade-offs to tackle emerging attacks
  - Protection for active type of fake BTS attacks
  - Study for removing unwanted protocol messages from 2G/3G/4G
Thank You.

Questions?

Pic ref: https://twitter.com/zahidtg