4G to 5G : New Attacks

Altaf Shaik
(Technische Universität Berlin, Germany)

Ravishankar Borgaonkar
(SINTEF Digital, Norway)

HITB GSEC 2019, Singapore
5G?

[Image of incorrect option: Human Communication (X)]

[Image of correct option: Machine Communication (√)]
5G Sec.?

New Services (Use Cases)

LTE Security Requirements + Enhancements

New Networking Technologies NFV/SDN

5G Security Requirements

Source: https://www.informationsecuritybuzz.com/articles/security-challenges-next-generation-5g-mobile-networks/
5G Security Elements

- Device identifiers/Credentials/
- Authentication+/
- Encryption/
- Integrity+/
- Privacy+/
- Resilience+

Cell

Edge Cloud

Network Slicing Security/
NFV/SDN Security/

Mobile Edge Computing/

Central Cloud
Security Evolution (OTA)

- **2G**: no mutual authentication
- **3G**: mutual authentication, integrity protection
- **4G**: mutual authentication, deeper mandatory integrity protection
- **5G**: mutual authentication++, deeper mandatory protection features++

Phone ➔ Base Station
IMSI Catchers in 5G?
5G Security

- 5G Security >> 4G? (What’s new)
- Similar security protocols and algorithms?
- Attacks in 4G/LTE fixed?
  - Downgrade attacks, DoS attacks, Location tracking
- What’s not fixed in 4G – copy paste to 5G
Another** IMSI catcher or fake base station attacks in 5G?

https://eprint.iacr.org/2018/1175
Capabilities?

UE Capabilities

- Core network Capabilities¹
  (Security algorithms, voice calling support, V2V)
- Radio access Capabilities²
  (frequency bands, Rx & Tx features, MIMO, CA, Category)

1. 3GPP TS 24.301, 23.401, 24.008
2. 3GPP TS 36.331
Core Capabilities

Non-Access-Stratum (NAS)PDU

0000 .... = Security header type: Plain NAS message, not security protected (0)
 .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
 NAS EPS Mobility Management Message Type: Attach request (0x41)
0... ..... = Type of security context flag (TSC): Native security context (for KSIasme)
 .111 ..... = NAS key set identifier: No key is available (7)
 .... 0... = Spare bit(s): 0x00
 .... .010 = EPS attach type: Combined EPS/IMSI attach (2)

- EPS mobile identity
- UE network capability
- ESM message container
- DRX Parameter
- MS Network Capability
- TMSI Status
- Mobile station classmark 2
- Mobile station classmark 3
- Supported Codec List - Supported Codecs
- Voice Domain Preference and UE's Usage Setting
- MS network feature support
Capabilities 5G

- V2X: Connected Cars
- Prose (D2D): Location services
- CIoT: IoT specific
Radio Capabilities

- UE-Capability RAT-Container
  - rat-Type: eutra (0)
  - ueCapability RAT-Container: c9a000024c
  - UE-EUTRA-Capability
    - accessStratumRelease: rel10 (2)
    - ue-Category: 4
    - pdcp-Parameters
    - phyLayerParameters
    - rf-Parameters
    - measParameters
    - featureGroupIndicators: 7f4ffe92
    - interRAT-Parameters
  - nonCriticalExtension
    - phyLayerParameters-v920

- interRAT-Parameters
  - GERAN-v920
  - UTRA-v920
  - csg-ProximityIndicationParameters-r9
  - neighCellSI-AcquisitionParameters-r9
  - son-Parameters-r9
  - nonCriticalExtension
    - lateNonCriticalExtension: 8c000000
      - UE-EUTRA-Capability-v9a0-IEs
        - featureGroupIndRel19Add-r9: c
      - nonCriticalExtension
        - ue-Category-v1020: 6
          - rf-Parameters-v1020
          - measParameters-v1020
          - featureGroupIndRel110-r10: 68240
          - ue-BasedNetwPerfMeasParameters-v920
          - nonCriticalExtension
            - rf-Parameters-v1060
LTE Registration

- UE Capabilities
  - sent to network while registration
  - stored at network for long periods
  - visible in plain-text over-the-air
  - Passive and active attacks
Issue?

- Accessible by fake base stations
- Sent plain-text over the air
- Standard + Implementation bugs
Attacks?

- MNmap (active or passive)
- Bidding down (MITM)
- Battery Drain (MITM)
Setup – LTE MitM attacker

- **Hardware**
  - 2 X (USRP B210 + Laptops)
  - Phones, Quectel modems, cars, IoT devices, trackers, laptops, routers,....

- **Software**
  - SRSLTE

- **Attacks tested with real devices and commercial networks**
1. MNmap

- (Mobile Network Mapping)
- similar to IP Nmap

- Maker
- Model
- OS
- Applications
- Version
1. MNmap

Identify any cellular device in the wild

Chip Maker, Device Model, Operating System, Application of device, Baseband Software Version
Identification – How

**Baseband vendors implement capabilities differently**

- For e.g., Qualcomm Chipsets always Disable EAI0
- Many Capabilities are **optional**, (disabled/enabled)

**Each target application requires different set of UE Capabilities**

- V2V for automated car
- Voice calling and codec support for phone
- GPS capability for tracker
- Data only support for routers, USB data sticks (SMS only)
## Devices Under Tests

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>Baseband Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung</td>
<td>Galaxy Alpha</td>
<td>Intel XMM7260</td>
</tr>
<tr>
<td>Samsung</td>
<td>Galaxy S6</td>
<td>Samsung Exynos Modem 333</td>
</tr>
<tr>
<td>Samsung</td>
<td>Galaxy S7</td>
<td>Samsung Exynos 8890</td>
</tr>
<tr>
<td>Samsung</td>
<td>Galaxy S8</td>
<td>Samsung Exynos 8895</td>
</tr>
<tr>
<td>Huawei</td>
<td>Honor 7</td>
<td>Kirin 935</td>
</tr>
<tr>
<td>Huawei</td>
<td>P20</td>
<td>Kirin 970</td>
</tr>
<tr>
<td>Huawei</td>
<td>One E9</td>
<td>MediaTek X10</td>
</tr>
<tr>
<td>HTC</td>
<td>G Flex 2</td>
<td>Qualcomm MSM8994</td>
</tr>
<tr>
<td>LG</td>
<td>Xperia Z5</td>
<td>Qualcomm MSM8994</td>
</tr>
<tr>
<td>Sony</td>
<td>Xperia X</td>
<td>Qualcomm MSM8956</td>
</tr>
<tr>
<td>Sony</td>
<td>Gemini</td>
<td>MediaTek X27</td>
</tr>
<tr>
<td>Planet Computer</td>
<td>iPhone 6</td>
<td>Qualcomm MDM6255</td>
</tr>
<tr>
<td>Apple</td>
<td>iPhone 8</td>
<td>Intel XMM7480</td>
</tr>
<tr>
<td>Apple</td>
<td>iPhone 8 (US)</td>
<td>Qualcomm MDM6555</td>
</tr>
<tr>
<td>Apple</td>
<td>iPhone X (US)</td>
<td>Qualcomm MDM6555</td>
</tr>
<tr>
<td>Google</td>
<td>Nexus 5X</td>
<td>Qualcomm MSM8992</td>
</tr>
<tr>
<td>Nokia</td>
<td>8110 4G</td>
<td>Qualcomm MSM8905</td>
</tr>
<tr>
<td>Asus</td>
<td>ZenFone 2E</td>
<td>Intel XMM7160</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>Baseband Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huawei</td>
<td>E3372</td>
<td>Huawei</td>
</tr>
<tr>
<td>Samsung</td>
<td>GT-B3740</td>
<td>Samsung CMC220</td>
</tr>
<tr>
<td>Sierra Wireless</td>
<td>EM7455</td>
<td>Qualcomm MDM9635</td>
</tr>
<tr>
<td>Fibocom</td>
<td>L850-GL</td>
<td>Intel XMM7360</td>
</tr>
<tr>
<td>Telit</td>
<td>LN930</td>
<td>Intel XMM7160</td>
</tr>
<tr>
<td>AVM</td>
<td>FritzBox LTE</td>
<td>Intel XMM7160</td>
</tr>
<tr>
<td>Huawei</td>
<td>B310s</td>
<td>Huawei</td>
</tr>
<tr>
<td>Netgear</td>
<td>Nighthawk</td>
<td>Qualcomm MDM9250</td>
</tr>
<tr>
<td>GlocalMe</td>
<td>G2</td>
<td>Qualcomm MSM8926</td>
</tr>
<tr>
<td>Quectel</td>
<td>BC68</td>
<td>Huawei NB-IoT</td>
</tr>
<tr>
<td>Quectel</td>
<td>BC66</td>
<td>MediaTek NB-IoT</td>
</tr>
<tr>
<td>Quectel</td>
<td>BG69</td>
<td>Qualcomm MDM9206</td>
</tr>
<tr>
<td>Audi</td>
<td>A6</td>
<td>Qualcomm MDM9635</td>
</tr>
<tr>
<td>Samsung</td>
<td>SM-V110K</td>
<td>Qualcomm MDM9206</td>
</tr>
<tr>
<td>Mobile Eco</td>
<td>ME-K60KL</td>
<td>Qualcomm MDM9206</td>
</tr>
<tr>
<td>Apple</td>
<td>Watch Series 3</td>
<td>Qualcomm MDM9635M</td>
</tr>
<tr>
<td>Huawei</td>
<td>MediaPad M5</td>
<td>Kirin 960</td>
</tr>
<tr>
<td>Apple</td>
<td>iPad 5th gen</td>
<td>Qualcomm MDM9625M</td>
</tr>
</tbody>
</table>
Ref model

Devices
- Baseband vendor
- Application
- Chipset name
- 3GPP release
### Fingerprint

#### Implementation differences among Baseband vendors

<table>
<thead>
<tr>
<th>Capability</th>
<th>Huawei</th>
<th>Samsung</th>
<th>Intel</th>
<th>Mediatek</th>
<th>Qualcomm</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM Service Prompt</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>EIA0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Access class control for CSFB</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Extended Measurement Capability</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Half-way

1. Baseband Maker
2. Baseband Model
3. List of supported devices for the chipset
4. Identify the right device and application
## Fingerprints

### Difference b/w phone and other devices

<table>
<thead>
<tr>
<th>Capability</th>
<th>Phone</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE’s Usage setting</td>
<td>Voice or Data</td>
<td>Not present</td>
</tr>
<tr>
<td>Voice domain preference</td>
<td>CS Voice or PS Voice</td>
<td>Not present</td>
</tr>
<tr>
<td>UMTS AMR codec</td>
<td>Present</td>
<td>Not</td>
</tr>
</tbody>
</table>

### Difference b/w iOS and Android

<table>
<thead>
<tr>
<th>Capability</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS assisted GPS</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Voice over PS-HS-UTRA-FDD-r9</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

### Phone and preferred Baseband

<table>
<thead>
<tr>
<th>Phone</th>
<th>Baseband</th>
</tr>
</thead>
<tbody>
<tr>
<td>Huawei</td>
<td>Huawei</td>
</tr>
<tr>
<td>Samsung</td>
<td>Samsung</td>
</tr>
<tr>
<td>Apple</td>
<td>Intel or QCT</td>
</tr>
</tbody>
</table>

### Difference b/w cellular and cellular IoT

<table>
<thead>
<tr>
<th>Capability</th>
<th>Cellular IoT</th>
<th>Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSM Timer</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>T3412 ext period TAU timer</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
MNmap issues

- SIM card can have affect on capabilities
  - enabled/disabled – operator setting, e.g., bands

- IoT applications LTE-M vs NB-IoT
  - Timer values (low for smart meters, high for asset trackers)

- Success and failures in detecting (close to round off, multiple options)
Zero Encryption for IoT

- Integrity protected and partially ciphered
- EEA0 for NAS by some X operator
- IoT devices depend on Air interface security
- Device details in clear
What next

- Passive MNmap also works (active base station not required)

- Privacy
  - Link IMSI to device capabilities on 4G
    - (associate device fingerprints to people)

- Launch target specific attack

- Open source MNmap : share traces and automated tool
2. Bidding down

- Hijacking
  - Radio Capabilities
  - MitM relay before OTA Security
  - Network/Phone cannot detect
Bidding down

- Radio Capabilities are modified
  - UE Category changed (Cat 12 -> Cat 1)
  - CA and MIMO are disabled
  - Frequency Bands are removed
  - VoLTE mandatory requirements are disabled
  - V2V capabilities can be removed
Tests with real networks

- LTE service downgrade (with elite USIM)
  - Iphone 8 and LTE Netgear router (Qualcomm Basebands)
  - Data Rate (downlink) 48 Mbps to 2 Mbps (USA and Europe)
  - VoLTE calls are denied to UE (CSFB used)
  - Handovers to 2G/3G due to lack of band support – downgraded
Impact

▪ **22 out of 32** tested LTE networks worldwide (Europe, Asia, NA) are affected (USA, Switzerland, France, Japan, Korea Netherlands, UK, Belgium, Iceland etc.)

▪ Persistent for 7 days
  ▪ Capabilities are **cached** at the Core Network components
  ▪ **Restart** device for normal operation

▪ **Radio is a bottleneck for high-speed data services**
Why without/before Security

3GPP TR 33.809 V0.2.0 (2019-02)

5.1 Key Issue #1: Security of unprotected unicast messages

5.1.1 Key issue details

This key issue covers both the uplink and downlink unicast message which could be sent unprotected. An example of unprotected uplink message is RRC UECapabilityInformation, and examples of unprotected downlink messages are RRC UECapabilityEnquiry, and REJECTs in RRC/NAS layers.

In current 3GPP standards, it has been a design choice to allow RRC UECapabilityEnquiry and RRC UECapabilityInformations messages to be sent unprotected "before" AS security activation. The reason for allowing that is to enable the network to do early optimization for better service/connectivity. It means that during the RRC

***To do early optimization for better service/connectivity***
3. Battery Drain

- **NB-IoT** (Narrow Band)
- Power Saving Mode (PSM)
  - OFF when not in use
Tests

- PSM disabled (UE and network don’t detect)

- Continuous activity - Neighbor cell measurements
  - drains battery (10 year battery??)

- Experiment with NB-IoT UE (Quectel BC68 modem)
  - Reconnects after 310 hours (13 days)
  - Battery lifetime reduced by 5 times

- Persistent attack: restart required to restore
Vulnerability Status & Impact

- Responsibly reported to GSMA, 3GPP SA3, & other affected operators/vendors
- Thanks to GSMA: findings verified (CVD-2019-0018) & SA3 to add fixes
- Core network capabilities are still unprotected
  - MNmap still possible on 5G: passive, active
Fixes for Deployed 4G/5G Networks

✓ Fixes in LTE release 14 for NB-IoT will appear commercially soon in the devices

✓ UE Capabilities should be security protected: accessible only after mutual authentication
  • Operators eNodeB implementation/configuration should be updated

✓ Capabilities should be replayed to UE after NAS security setup for verification – Hash of them
  • V2V, Voice calling features, PSM timers, etc.
Thank you

altaf329@sect.tu-berlin.de
ravi.borgaonkar@sintef.no
Director@kaitiaki.in