EXPLORING LTE SECURITY WITH OPEN-SOURCE TOOLS, TESTING PROTOCOL EXPLOITS AND ANALYZING THEIR POTENTIAL IMPACT ON 5G NETWORKS

Roger Piqueras Jover
rpiquerasjov@bloomberg.net
ABOUT ME

● Recent dad who goes to a lot of live music shows, plays and watches too much soccer, and does some security research on the side
● Security Researcher (aka Senior Security Architect), Office of the CTO at Bloomberg
● Formerly (5 years) Principal Member of Technical Staff at AT&T Security Research
● Mobile/wireless network security research
  – Mostly LTE PHY and upper layers
● If it communicates wirelessly, I am interested in its security
  – BLE
  – 802.11
  – Zigbee, Zigwave
  – LoRaWAN
● More details
  – http://rogerpiquerasjover.net/  
  – @rgoestotheshows
The first mobile networks were not designed with a strong security focus (no support for encryption in 1G!!)

- "Old" encryption
  - No BS authentication

- Strong encryption
  - Mutual authentication

- Stronger encryption
  - Mutual authentication

- PKI for IMSI protection
  - More secure (?)
LTE BASICS
LTE CELL SELECTION AND CONNECTION

- System configuration
  - Decode Master Information Block (MIB) from PBCH
  - Decode System Information Blocks (SIBs) from PDSCH

- Power on
- Decode PBCH
- Extract System Configuration
- Idle timer
- RACH
- RACH
- Mobile connection

- Idle state
  - Random Access
  - Connected state
  - Radio Access Bearer + (Attach)
MOBILE NETWORK USER/DEVICE IDENTIFIERS

IMEI – “Serial number” of the device

IMSI – secret id of the SIM that should never be disclosed
TMSI – temporary id used by the network once it knows who you are

MSISDN – Your phone number.

XYZ-867-5309
LTE (IN)SECURITY RATIONALE
### LTE (IN)SECURITY RATIONALE

<table>
<thead>
<tr>
<th>Name</th>
<th>Start Time</th>
<th>Dur</th>
<th>Cell</th>
<th>Cell ID</th>
<th>Frame</th>
<th>Subf</th>
<th>RCE</th>
<th>Power</th>
<th>Length</th>
<th>Errs</th>
<th>Retrans</th>
<th>Decr</th>
<th>Valid</th>
<th>SF RSSI</th>
<th>SINR</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACH</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>440</td>
<td>1</td>
<td>-16.64</td>
<td>-57.98</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16.54</td>
<td></td>
</tr>
<tr>
<td>MAC Random Access Response</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>440</td>
<td>5</td>
<td>-16.41</td>
<td>-45.73</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16.41</td>
<td></td>
</tr>
<tr>
<td>RRC Connection Request</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>441</td>
<td>1</td>
<td>-23.89</td>
<td>-51.14</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>23.85</td>
<td></td>
</tr>
<tr>
<td>RRC Connection Setup</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>442</td>
<td>5</td>
<td>-14.21</td>
<td>-26.21</td>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>26.21</td>
<td></td>
</tr>
<tr>
<td>RRC Connection Setup Complete</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>445</td>
<td>0</td>
<td>-25.25</td>
<td>-48.36</td>
<td>53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>25.25</td>
<td></td>
</tr>
<tr>
<td>Attach Request</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>445</td>
<td>0</td>
<td>-25.25</td>
<td>-48.36</td>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>25.25</td>
<td></td>
</tr>
<tr>
<td>PDN Connectivity Request</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>446</td>
<td>0</td>
<td>-25.25</td>
<td>-48.36</td>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>25.25</td>
<td></td>
</tr>
<tr>
<td>DLTInformationTransfer</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>453</td>
<td>5</td>
<td>-15.00</td>
<td>-41.33</td>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-38.44</td>
<td>15.30</td>
</tr>
<tr>
<td>Authentication Request</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>467</td>
<td>2</td>
<td>-20.80</td>
<td>-52.66</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20.80</td>
<td></td>
</tr>
<tr>
<td>DLTInformationTransfer</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>467</td>
<td>2</td>
<td>-20.80</td>
<td>-52.66</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20.80</td>
<td></td>
</tr>
<tr>
<td>Security Protected NAS Message</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>471</td>
<td>4</td>
<td>-15.52</td>
<td>-44.04</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15.52</td>
<td></td>
</tr>
<tr>
<td>Security Mode Command</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>471</td>
<td>4</td>
<td>-15.52</td>
<td>-44.04</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-39.22</td>
<td>15.52</td>
</tr>
<tr>
<td>DLInformationTransfer</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>473</td>
<td>2</td>
<td>-22.49</td>
<td>-52.16</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>22.49</td>
<td></td>
</tr>
<tr>
<td>Unknown NAS</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>473</td>
<td>2</td>
<td>-22.49</td>
<td>-52.16</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>22.49</td>
<td></td>
</tr>
<tr>
<td>DLInformationTransfer</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>477</td>
<td>4</td>
<td>-14.73</td>
<td>-45.60</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14.73</td>
<td></td>
</tr>
<tr>
<td>Security Protected NAS Message</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>477</td>
<td>4</td>
<td>-14.73</td>
<td>-45.60</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-39.27</td>
<td>14.73</td>
</tr>
<tr>
<td>Unknown NAS</td>
<td>01:23:05.45999</td>
<td>U</td>
<td>477</td>
<td>2</td>
<td>-21.36</td>
<td>-53.39</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>21.36</td>
<td></td>
</tr>
<tr>
<td>ULInformationTransfer</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>479</td>
<td>2</td>
<td>-21.36</td>
<td>-53.39</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>21.36</td>
<td></td>
</tr>
<tr>
<td>Ciphered RRC</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>491</td>
<td>3</td>
<td>-16.41</td>
<td>-45.73</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16.41</td>
<td></td>
</tr>
<tr>
<td>Ciphered RRC</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>491</td>
<td>3</td>
<td>-16.41</td>
<td>-45.73</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16.41</td>
<td></td>
</tr>
<tr>
<td>Ciphered RRC</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>491</td>
<td>3</td>
<td>-16.41</td>
<td>-45.73</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16.41</td>
<td></td>
</tr>
<tr>
<td>Ciphered RRC</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>491</td>
<td>3</td>
<td>-16.41</td>
<td>-45.73</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16.41</td>
<td></td>
</tr>
<tr>
<td>Ciphered RRC</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>491</td>
<td>3</td>
<td>-16.41</td>
<td>-45.73</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16.41</td>
<td></td>
</tr>
<tr>
<td>Ciphered RRC</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>491</td>
<td>3</td>
<td>-16.41</td>
<td>-45.73</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16.41</td>
<td></td>
</tr>
<tr>
<td>Ciphered RRC</td>
<td>01:23:05.45999</td>
<td>D</td>
<td>491</td>
<td>3</td>
<td>-16.41</td>
<td>-45.73</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16.41</td>
<td></td>
</tr>
</tbody>
</table>

- **RACH handshake between UE and eNB**
- **RRC handshake between UE and eNB**
- **Connection setup (authentication, set-up of encryption, tunnel set-up, etc)**
- **Encrypted traffic**

© Portions Copyright 2018 Bloomberg L.P.
Unencrypted and unprotected. I can sniff these messages and I can transmit them pretending to be a legitimate base station.

Other things sent in the clear:
- Base station config (broadcast messages)
- Measurement reports
- Measurement report requests
- (Sometimes) GPS coordinates
- HO related messages
- Paging messages
- Etc
Regardless of mutual authentication and strong encryption, a mobile device engages in a substantial exchange of unprotected messages with *any* LTE base station (malicious or not) that advertises itself with the right broadcast information.

**Spoiler alert** – This also potentially applies to 5G. No viable solution proposed in the specifications yet.

*(more on this later)*
EXPLORING LTE SECURITY WITH SOFTWARE-RADIO
TOOLSET

- LTE open source implementation (eNB+UE)
  - Modified srsLTE – https://github.com/srsLTE
    - First available UE stack implementation!!!!!!
    - LTE sniffer
  - Modifications to source for protocol exploit experimentation
- HW setup
  - USRP B210/USRP mini for active rogue base station
  - BUDGET: USRP B210 ($1100) + GPSDO ($625) + LTE Antenna (2x$30) = $1785
  - Machine running Ubuntu 16

All LTE active radio experiments MUST be performed inside a faraday cage!!!
SNiffing Base Station Configuration

- Base station configuration broadcasted in the clear in MIB and SIB messages.
- `srsLTE + AirScope`
  - Dump everything on pcap
- Very useful information that could be leveraged by an adversary
  - Optimal tx power for a rogue base station
  - High priority frequencies to force priority cell reselection
  - Tracking Area of the legitimate cell (use a different one in your rogue eNodeB to force TAU update messages)
  - Mapping of signaling channels
  - Paging channel mapping and paging configuration
- Broadcast message scanning tools available in both `srsLTE` and openLTE

---

SNIFFING BASE STATION CONFIGURATION

LTE PDSCH SIB1 packet

Mobile operator
Cell ID
RX power to select that cell
SNIFFING BASE STATION CONFIGURATION

Wireless Packet - capture_sample_12202016

[Transport channel: DL-SCH (4)]
LTE Radio Resource Control (RRC) protocol
BCCH-DL-SCH-Message
message: c1 (0)
  c1: systemInformation (0)
  systemInformation
  criticalExtensions: systemInformation-r8 (0)
  systemInformation-r8
  sib-TypeAndInfo: 2 items
  item 0:
  "sib-TypeAndInfo item: sib2 (0)"

RACH config
Paging config
RRC timers

LTE PDSCH SIB2/3 packet
SNiffing Base Station Configuration

- MIB/SIB messages are necessary for the operation of the network
  - Some things must be sent in the clear (i.e. a device connecting for the first time)
  - But perhaps not everything
- Things an attacker can learn from MIB and SIB messages
  - Optimal tx power for a rogue base station (no need to set up your USRP to its max tx power)
  - High priority frequencies to force priority cell reselection
  - Mobile operator who owns that tower
  - Tracking Area of the legitimate cell (use a different one in your rogue eNodeB to force TAU update messages)
  - Mapping of signaling channels
  - Paging channel mapping and paging configuration
  - Etc
LOW-COST LTE IMSI CATCHER (STINGRAY)

- Despite common assumptions, in LTE the IMSI is always transmitted in the clear at least once
  - If the network has never seen that UE, it must use the IMSI to claim its identity
  - A UE will trust *any* eNodeB that claims it has never seen that device (pre-authentication messages)
  - IMSI can also be transmitted in the clear in error recovery situations (very rare)

- Implementation
  - USRP B210 + Ubuntu 16 + gnuradio 3.7.2
  - LTE base station – srsLTE (slightly modified)
    - Added feature to record IMSI from Attach Request messages
  - Send attach reject after IMSI collection
  - Very simple to implement
IMSI CATCHERS (STINGRAY)
IMSI CATCHERS (STINGRAY)

Extract IMSI from these messages

Unauthenticated messages

© Portions Copyright 2018 Bloomberg L.P.
LOW-COST LTE IMSI CATCHER (STINGRAY)

- AttachRequest message processing
  - s1ap_nas_transport.cc

```cpp
//Get attach type from attach request
if (attach_req.eps_mobile_id.type_of_id == LIBLTE_NME_EPS_MOBILE_ID_TYPE_IMSI)
{
    m_slap_log->console("Attach Request -- IMSI-style attach request\n");
    m_slap_log->info("Attach Request -- IMSI-style attach request\n");
    handle_nas_imsi_attach_request(enb_ue_slap_id, attach_req, pdn_con_req, reply_buffer, reply_flag, enb_sri);
}
else if (attach_req.eps_mobile_id.type_of_id == LIBLTE_NME_EPS_MOBILE_ID_TYPE_GUTI)
{
    m_slap_log->console("Attach Request -- GUTI-style attach request\n");
    m_slap_log->info("Attach Request -- GUTI-style attach request\n");
    handle_nas_guti_attach_request(enb_ue_slap_id, attach_req, pdn_con_req, nas_msg, reply_buffer, reply_flag, enb_sri);
}
else
{
    m_slap_log->error("Unhandle Mobile Id type in attach request\n");
    return false;
}
```
LOW-COST LTE IMSI CATCHER (STINGRAY)

- Export/save IMSI when processing AttachRequest message
## Table

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Delta</th>
<th>Direction</th>
<th>Length</th>
<th>Temporary C-RNTI</th>
<th>RNTI</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0.0780931</td>
<td>0.028845</td>
<td>Uplink</td>
<td>188</td>
<td></td>
<td></td>
<td>70 LTE RR. RRCConnectionSetupComplete, Attach request, PDN connectivity request</td>
</tr>
<tr>
<td>5</td>
<td>0.071905</td>
<td>0.000947</td>
<td>Downlink</td>
<td>34</td>
<td></td>
<td></td>
<td>70 LTE RR. [DL] [AM] SRB1 [CONTROL] ACK_SN=1, DLInformationTransfer, Attach reject (EPS services not allowed)</td>
</tr>
<tr>
<td>6</td>
<td>113.975051</td>
<td>113.975051</td>
<td>Downlink</td>
<td>15</td>
<td></td>
<td></td>
<td>MAC-LTE RACH Preamble chosen for UE 0 (RAPID=0, attempt=0)</td>
</tr>
<tr>
<td>7</td>
<td>113.985023</td>
<td>0.009722</td>
<td>Uplink</td>
<td>22</td>
<td></td>
<td></td>
<td>71 LTE RR. RRCConnectionRequest</td>
</tr>
<tr>
<td>8</td>
<td>114.006054</td>
<td>0.024301</td>
<td>Downlink</td>
<td>86</td>
<td></td>
<td></td>
<td>71 LTE RR. RRCConnectionSetup</td>
</tr>
<tr>
<td>9</td>
<td>114.031227</td>
<td>0.022173</td>
<td>Uplink</td>
<td>188</td>
<td></td>
<td></td>
<td>71 LTE RR. RRCConnectionSetupComplete, Attach request, PDN connectivity request</td>
</tr>
<tr>
<td>10</td>
<td>114.031054</td>
<td>0.000172</td>
<td>Downlink</td>
<td>76</td>
<td></td>
<td></td>
<td>116.295064 32.361110 Downlink 15</td>
</tr>
<tr>
<td>11</td>
<td>116.295064</td>
<td>32.361110</td>
<td>Downlink</td>
<td>15</td>
<td></td>
<td></td>
<td>126.385024 0.010160 Downlink 22</td>
</tr>
<tr>
<td>12</td>
<td>13.328095</td>
<td>0.023734</td>
<td>Downlink</td>
<td>86</td>
<td></td>
<td></td>
<td>146.351086 0.022108 Downlink 188</td>
</tr>
<tr>
<td>13</td>
<td>146.351086</td>
<td>0.022108</td>
<td>Downlink</td>
<td>188</td>
<td></td>
<td></td>
<td>156.351086 0.000002 Downlink 76</td>
</tr>
</tbody>
</table>

### 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)

00 = Type of security context flag (TSC): Native security context (for KSIasme)

01 = NAS key set identifier: No key is available (7)

0000 = Spare bit(s): 0x00

010 = EPS attach type: Combined EPS/IMSI attach (2)

### EPS mobile identity

- Length: 8
- Odd/even indication: Odd number of identity digits
- Type of identity: IMSI (1)

**IMSI:** 

```
+--------------------+
| ...               |
| ...               |
| ...               |
| ...               |
| ...               |
| ...               |
| ...               |
| ...               |
+--------------------+
```

---

Frame (189 bytes)

Unaligned OCTET STRING (197 bytes)

International mobile subscriber identity (IMSI) (e21.2 imsie), 8 bytes

Packets: 25 - Displayed: 25 (100.0%) - Lead time: 0.02s

Profile: Default
DEVICE AND SIM TEMPORARY LOCK

- Attach reject and TAU (Tracking Area Update) reject messages not encrypted/integrity-protected
- Spoofing this messages one can trick a device to
  - Believe it is not allowed to connect to the network (blocked)
  - Believe it is supposed to downgrade to or only allowed to connect to GSM

These are not the droids we are looking for. I am not allowed to connect to my provider anymore, I won't try again.
SOFT DOWNGRADE TO GSM

- Use similar techniques to “instruct” the phone to downgrade to GSM
  - Only GSM services allowed OR LTE and 3G not allowed

- Once at GSM, the phone connects to your rogue base station
  - Bruteforce the encryption
  - Listen to phone calls, read text messages
  - Man in the Middle
  - A long list of other bad things...

I will remove these restraints and leave this cell with the door open... and use only GSM from now on... and I’ll drop my weapon.

(Much more dangerous) rogue GSM base station

REQUEST

REJECT

You will remove these restraints and leave this cell with the door open... and use only GSM from now on.

Attach reject (EPS services not allowed)
DEVICE TEMPORARY LOCK AND SOFT DOWNGRADE

● Some results
  – The blocking of the device/SIM is only temporary
  – Device won’t connect until rebooted
  – SIM won’t connect until reboot
  – SIM/device bricked until timer T3245 expires (24 to 48 hours!)
  – Downgrade device to GSM and get it to connect to a rogue BS

● If the target is an M2M device, it could be a semi-persistent attack
  – Reboot M2M device remotely?
  – Send a technician to reset SIM?
  – Or just wait 48 hours for your M2M device to come back online…
OTHER ATTACH/TAU REJECT EXPLOITS

- 3GPP defines a number of possible EMM Cause Codes
  - Let’s try them all and see what happens…
FUZZING MOBILE NETWORK PROTOCOLS

● LTEFUZZ v0.1
  – Try each value of EMM Reject Cause one by one
  – Rinse and repeat

● Some observed interesting behaviors
  – Cellular modem in UE stops working (crash?)
  – Weird reconnection + reattach attempt
  – IMSI + IMEI disclosure
  – Constant retransmission/reattempt
    • Battery drain substantially fast but I need to test more
  – Induction of handover attempts to secondary eNB

● Currently triaging and reliably reproducing results

● Collaboration with 2 academic labs (any students interested?)
CONNECTION HIJACKING IN LTE

- LTE layer 2 encryption and integrity protection
  - Packets with known structure
  - AES Counter Mode (AES-CTR)
  - 16 bit checksum in the IP-UDP DNS request packets

- Protocol exploit
  - Track user (RNTI)
  - Identify DNS requests
  - MitM DNS requests (some “radio” challenges)
  - Apply mask to flip bits on destination IP address
  - Forward DNS requests to malicious DNS server
EXPLORING UPLINK PROTOCOL SECURITY
SRSUE

- First open-source implementation of the mobile device stack
  - https://github.com/srsLTE/srsLTE/tree/master/srsue
  - First commit May 2017

- Platform to experiment with UL pre-authentication messages

- Now researchers can analyze exploits in the eNodeB and the mobile core network
  - eNodeB and core network (MME+HSS) fuzzing!
CONNECTION DETACH HANDSHAKE

● Procedure through which the UE disconnects from the network
  – Switch off UE
  – Airplane mode
  – Remove SIM

● Can be UE initiated and does not require ACK from network (!!!)

● Authentication/integrity protection (???)

3GPP TS 24.301 V13.7.0 (2016-09). Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS);
CONNECTION DETACH HANDSHAKE

- NAS detach request message
  - Includes EPS mobile identity
  - Can be GUTI or IMSI
  - It can even be the IMEI

- In some cases it does not require integrity protection
  - It can be spoofed!

4.4.4.3 Integrity checking of NAS signalling messages in the MME

Except the messages listed below, no NAS signalling messages shall be processed by the receiving EMM entity in the MME or forwarded to the ESM entity, unless the secure exchange of NAS messages has been established for the NAS signalling connection:

- EMM messages:
  - ATTACH REQUEST;
  - IDENTITY RESPONSE (if requested identification parameter is IMSI);
  - AUTHENTICATION RESPONSE;
  - AUTHENTICATION FAILURE;
  - SECURITY MODE REJECT;
  - DETACH REQUEST;
  - DETACH ACCEPT;
  - TRACKING AREA UPDATE REQUEST.

NOTE 1: The TRACKING AREA UPDATE REQUEST message is sent by the UE without integrity protection, if the tracking area updating procedure is initiated due to an inter-system change in idle mode and no current EPS security context is available in the UE. The other messages are accepted by the MME without integrity protection, as in certain situations they are sent by the UE before security can be activated.

3GPP TS 24.301 V13.7.0 (2016-09). Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS);
CONNECTION DETACH HANDSHAKE

- In some cases it does not require integrity protection
  - It can be spoofed!

In mobile protocol security it only takes finding one single security edge case supported by the standard to make the entire house of cards fall apart.
Once a current EPS security context exists, until the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving EMM entity in the MME shall process the following NAS signalling messages, even if the MAC included in the message fails the integrity check or cannot be verified, as the EPS security context is not available in the network:

- ATTACH REQUEST;
- IDENTITY RESPONSE (if requested identification parameter is IMSI);
- AUTHENTICATION RESPONSE;

3GPP

Release 13 48 3GPP TS 24.301 V13.7.0 (2016-09)

- AUTHENTICATION FAILURE;
- SECURITY MODE REJECT;
- DETACH REQUEST (if sent before security has been activated);
- DETACH ACCEPT;
REMOTE DEVICE DETACH

- Set up
  - Test smartphone (victim)
  - Linux box #1
    - USRP B210 running srsUE (adversary)
  - Linux box #2
    - USRP B210 running srsENB
    - Open source LTE EPC

- Run RRC handshake and spoof Detach Request message with victim’s identity

- Knock out victim from network remotely
  - Though in the lab it is not “remotely”

- Testing it in a real network would be easy
  - But not legal
  - Next tests → commercial picocell

- Might not work in a real network if inter-layer integrity checks are well implemented
LTE LOCATION LEAKS
LOCATION LEAKS AND DEVICE TRACKING - RNTI

- **RNTI**
  - PHY layer id sent in the clear in EVERY SINGLE packet, both UL and DL
  - Identifies uniquely every UE within a cell
    - Changes infrequently
    - Based on several captures in the NYC and Honolulu areas
  - No distinguishable behavior per operator or per base station manufacturer
  - Assigned by the network in the MAC RAR response to the RACH preamble

(C-RNTI assignment + timing advance)
LOCATION LEAKS AND DEVICE TRACKING - RNTI
### LOCATION LEAKS AND DEVICE TRACKING - RNTI

<table>
<thead>
<tr>
<th>Name</th>
<th>Start time</th>
<th>D/UI</th>
<th>Cell ID</th>
<th>Frame</th>
<th>RNTI</th>
<th>UE Identity</th>
<th>Length</th>
<th>Errs</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACH</td>
<td>00:22:6830866</td>
<td>U</td>
<td>988</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Random Access Response</td>
<td>00:22:6834866</td>
<td>D</td>
<td>989</td>
<td>8</td>
<td></td>
<td>7</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>RRCCConnectionRequest</td>
<td>00:22:6840866</td>
<td>U</td>
<td>989</td>
<td>19841</td>
<td></td>
<td>6</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>RRCCConnectionSetup</td>
<td>00:22:6853866</td>
<td>D</td>
<td>991</td>
<td>19841</td>
<td></td>
<td>24</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6855868</td>
<td>D</td>
<td>991</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6855868</td>
<td>D</td>
<td>991</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6857868</td>
<td>D</td>
<td>991</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6857868</td>
<td>D</td>
<td>991</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6858868</td>
<td>D</td>
<td>991</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Unknown Data</td>
<td>00:22:6871868</td>
<td>D</td>
<td>992</td>
<td>12381</td>
<td></td>
<td>52</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Unknown Data</td>
<td>00:22:6871868</td>
<td>D</td>
<td>992</td>
<td>12381</td>
<td></td>
<td>109</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>RRCCConnectionSetupComplete</td>
<td>00:22:6874866</td>
<td>U</td>
<td>993</td>
<td>19841</td>
<td></td>
<td>7</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Service Request</td>
<td>00:22:6874866</td>
<td>U</td>
<td>993</td>
<td>19841</td>
<td></td>
<td>3</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6894868</td>
<td>D</td>
<td>995</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6895868</td>
<td>D</td>
<td>995</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6895868</td>
<td>D</td>
<td>995</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6895868</td>
<td>D</td>
<td>995</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6900868</td>
<td>D</td>
<td>995</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6901868</td>
<td>D</td>
<td>995</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6902868</td>
<td>D</td>
<td>995</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6903868</td>
<td>D</td>
<td>995</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>SecurityModeCommand</td>
<td>00:22:6909868</td>
<td>D</td>
<td>996</td>
<td>19841</td>
<td></td>
<td>3</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6911868</td>
<td>D</td>
<td>996</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6911868</td>
<td>D</td>
<td>996</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>SecurityModeComplete</td>
<td>00:22:6929866</td>
<td>U</td>
<td>998</td>
<td>19841</td>
<td></td>
<td>2</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6933868</td>
<td>D</td>
<td>999</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6934868</td>
<td>D</td>
<td>999</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6935868</td>
<td>D</td>
<td>1000</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6935868</td>
<td>D</td>
<td>1000</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6953868</td>
<td>D</td>
<td>1001</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6954868</td>
<td>D</td>
<td>1001</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6955868</td>
<td>D</td>
<td>1001</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6955868</td>
<td>D</td>
<td>1001</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>RRCCConnectionReconfiguration</td>
<td>00:22:6957866</td>
<td>D</td>
<td>1004</td>
<td></td>
<td>84</td>
<td>OK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RRCCConnectionReconfigurationComplete</td>
<td>00:22:6972866</td>
<td>U</td>
<td>1002</td>
<td>19841</td>
<td></td>
<td>2</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>IP Data (IPv4 UDP)</td>
<td>00:22:6972866</td>
<td>U</td>
<td>1002</td>
<td>19841</td>
<td></td>
<td>70</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6974868</td>
<td>D</td>
<td>1003</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:6975868</td>
<td>D</td>
<td>1003</td>
<td>19681</td>
<td></td>
<td>1280</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>MAC Random Access Response</td>
<td>00:22:6984868</td>
<td>D</td>
<td>1004</td>
<td>19681</td>
<td></td>
<td>7</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>RRCCConnectionSetup</td>
<td>00:22:7003866</td>
<td>U</td>
<td>1006</td>
<td>19841</td>
<td></td>
<td>24</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Unknown Data</td>
<td>00:22:7020868</td>
<td>D</td>
<td>1007</td>
<td>19841</td>
<td></td>
<td>1428</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Ciphered data</td>
<td>00:22:7017868</td>
<td>D</td>
<td>1007</td>
<td>19841</td>
<td></td>
<td>2</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>
### RNTI TRACKING WITH OPEN-SOURCE TOOLS

RNTIs being tracked within this cell (srsLTE)

<table>
<thead>
<tr>
<th>Index</th>
<th>RNTI</th>
<th>DL (kb)</th>
<th>MCS</th>
<th>PRB (from 0-15)</th>
<th>UL (kb)</th>
<th>MCS</th>
<th>PRB (from 0-15)</th>
<th>Timeout (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.7</td>
<td>21.0</td>
<td>4.0</td>
<td>116</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>2.7</td>
<td>2.6</td>
<td>12.4</td>
<td>8.6</td>
<td>3.8</td>
<td>3.8</td>
<td>90</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>0.9</td>
<td>17.0</td>
<td>18.0</td>
<td>8.0</td>
<td>0.0</td>
<td>0.0</td>
<td>621</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>1.6</td>
<td>11.0</td>
<td>8.0</td>
<td>8.0</td>
<td>0.0</td>
<td>0.0</td>
<td>85</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>0.1</td>
<td>7.0</td>
<td>3.0</td>
<td>8.6</td>
<td>0.0</td>
<td>0.0</td>
<td>589</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>0.6</td>
<td>2.0</td>
<td>4.0</td>
<td>8.6</td>
<td>0.0</td>
<td>0.0</td>
<td>451</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>0.2</td>
<td>7.0</td>
<td>3.0</td>
<td>8.6</td>
<td>0.0</td>
<td>0.0</td>
<td>481</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>0.6</td>
<td>2.0</td>
<td>4.0</td>
<td>8.6</td>
<td>0.0</td>
<td>0.0</td>
<td>481</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>0.0</td>
<td>921</td>
</tr>
</tbody>
</table>

© Portions Copyright 2018 Bloomberg L.P.
- Unprotected RRC Connection Reconfiguration message for handover should not occur
  - eNBs that used to have this issue have since been configured correctly

- According to 3GPP TR 33.899 V1.3.0 (2017-08)
  - RNTI tracking is not a privacy issue because RNTI is not a long lived id
    - But I keep seeing in the lab the RNTI of my devices not changing for hours…
  - TMSI can be mapped to RNTI, but TMSI is also short lived id
    - But the TMSI changes rather infrequently as well…

- LTE hijacking paper shows it is indeed possible!
  - https://alter-attack.net/media/breaking_lte_on_layer_two.pdf
OTHER POTENTIAL LTE LOCATION LEAKS

- Paging messages sent in the clear
  - Known location tracking techniques based on sniffing paging messages
  - Silent text message to target IMSI/TMSI/MSISDN
  - If a paging is sniffed, the UE is in the same Tracking Area as the sniffer
  - If connection establishment is sniffed, the UE is in the same cell as the sniffer
Wireshark - Packet 24 - capture_sample_12202016

Frame 24: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
DLT: 147, Payload: mac-lte-framed (mac-lte-framed)
MAC-LTE PCH PDU (13 bytes)
[Context (RNTI-65534)]
LTE Radio Resource Control (RRC) protocol
PCCH-Message

- PagingRecord
  - ue-Identity: s-TMSI (0)
  - s-TMSI
  - cn-domain: ps (0)

- PagingRecord
  - ue-Identity: s-TMSI (0)
  - cn-domain: ps (0)
OTHER POTENTIAL LTE LOCATION LEAKS

- Simple location inference
  - Eavesdrop MAC RAR messages
  - Time Advance → distance from eNodeB
  - Very low resolution unless one captures MAC RARs from multiple base stations

Tri-lateralation of user’s location with eavesdropped MAC-RAR messages
5G SECURITY
5G STANDARDS

- 5G largely a marketing buzz word
  - But there’s some actual very interesting technology behind
  - First deployments and tests already happening

- Release 15 of the 3GPP standards
  - December 2017
  - First release of 5G – New Radio + 5G System

- Most changes at the PHY layer
  - mmWave
  - Massive MIMO

- Work to address some protocol exploits
  - IMSI obfuscation and encryption
  - PKI for IMSI concealing

- Security standards published in March 2018
  - 3GPP TS 33.501 V1.0.0 (2018-03)
IMSI PROTECTION

- IMSI encrypted (concealed) with public key of home operator
  - Probabilistic asymmetric encryption
  - Same IMSI encrypted multiple times results in different ciphertexts (to avoid tracking)

- IMSI catching much harder

- Challenges
  - What happens if private key of home operator is “lost” or needs to be rotated?
    - New SIM?
    - New public key burned in SIM?
    - “Outside of the scope of the 3GPP specifications"
SUPI – THE NEW IMSI

- SUPI – Subscription Permanent Identifier
  - New IMSI in 5G
  - SUCI (SUbscription Concealed Identifier) – Encrypted SUPI

- Challenges
  - “If the home network has not provisioned the public key in USIM, the SUPI protection in initial registration procedure is not provided. In this case, the null-scheme shall be used by the ME.”
    - Null cipher still supported
  - “In case of an unauthenticated emergency call, privacy protection for SUPI is not required.”
    - Can a rogue base station fool a UE to initiate such an emergency call?
PROTOCOL EXPLOITS IN 5G

- Most LTE protocol exploits caused by implicit trust in pre-authentication messages
  - RRC, MAC, NAS layers

- 5G aims to tackle known exploits in LTE
  - E.g. AttachReject DoS and downgrade to GSM mentioned explicitly

- Leverage public key of home operator?
  - Does not work with roaming devices
  - Public key from all operators?
    - Not scalable
    - Unrealistic

- How are the 5G security specifications preventing exploiting pre-authentication messages?
  - As of now, 5G appears to be vulnerable to pre-authentication message protocol exploits
PROTOCOL EXPLOITS IN 5G

- I am not the only one claiming this…

Fake 5G Base Station may still Exist

DoS attack examples:
- You are an illegal cellphone!
- Here is NO network available. You could shut down your modem.

The root cause is the initial broadcasting message from network can not be proved to be trustable.

NO PKI infrastructure solution reaches agreement in 3GPP.

“OUT OF SCOPE”

This works for most wireless security specifications:

Ctrl+F for {“scope”,”out of scope”,”out of the scope”, etc}

In mobile communication standard documents

● 5.2.5 – Subscriber privacy
  – “The provisioning and updating of the home network public key is out of the scope of the present document. It can be implemented using, e.g. the Over the Air (OTA) mechanism.”

● 12.2 – Mutual authentication
  – “The structure of the PKI used for the certificate is out of scope of the present document.”

● C.3.3 – Processing on home network side
  – “How often the home network generates new public/private key pair and how the public key is provisioned to the UE are out of the scope of this clause.”
NULL CIPHERING

- Supported ciphering modes
  - **NEA0 - Null ciphering algorithm**
  - 128-NEA1 - 128-bit SNOW 3G based algorithm
  - 128-NEA2 - 128-bit AES based algorithm
  - 128-NEA3 - 128-bit ZUC based algorithm

- **Null ciphering** is a supported option
  - **Same for null integrity**
  - Potential security edge cases
  - Bidding down attacks
    - Public key of home operator burned in SIM
    - How to authenticate a bidding down request at a foreign (roaming) network?

- Note null ciphering support often a requirement for Lawful Interception
POTENTIAL SECURITY EDGE CASES

- “In case the UE registers for Emergency Services and receives an Identifier Request, the UE shall use the null-scheme for generating the SUCI in the Identifier Response.”

- “If the UE receives a NAS security mode command selecting NULL integrity and ciphering algorithms, the UE shall accept this as long as the IMS Emergency session progresses.”

- “If the authentication failure is detected in the AMF then the UE is not aware of the failure in the AMF, but still needs to be prepared, according to the conditions specified in TS 24.301, to accept a NAS SMC from the AMF requesting the use of the NULL ciphering and integrity algorithms.”

- “If the AMF cannot identify the subscriber, or cannot obtain authentication vector (when SUPI is provided), the AMF shall send NAS SMC with NULL algorithms to the UE regardless of the supported algorithms announced previously by the UE.”

- …
NAS integrity activation:
“Replay protection shall be activated when integrity protection is activated, except when the NULL integrity protection algorithm is selected.”

Are we there yet? The long path to securing 5G mobile communication networks“
https://www.linkedin.com/pulse/we-yet-long-path-securing-5g-mobile-communication-piqueras-jover
Q&A

http://rogerpiquerasjover.net ---- @rgoestotheshows
FURTHER READING

FURTHER READING

**FURTHER READING**