Practical attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems

Altuf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, Jean-Pierre Seifert

NDSS 2016 San Diego USA

23 February 2016
Outline

• Evolution of security in mobile networks
  • 2G/GSM, 3G/UMTS, 4G/LTE

• Practical attacks against 4G/LTE
  • Location leaks
  • Denial of service

• Potential reasons for vulnerabilities

• Impact
Fake base-stations...

- Used for: IMSI/IMEI/location tracking, call & data interception

- Exploit weaknesses in 2G & 3G (partially)

- Known as IMSI Catchers

- Difficult to detect on normal phones (Darshak, Cryptophone, Snoopsnitch)
Fake base-stations..2

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. ...and the system can use that information to find the suspect within three meters, or within a specific room in a building.

Source: people familiar with the operations of the program

Brian McGill/The Wall Street Journal
Security shortcomings in 2G & 3G

• 2G - no mutual authentication

• 3G – less pervasive, integrity protection like in LTE → downgrade attacks

• 2G/3G – power is to base station:
  • Decides when/how to authenticate/encrypt
  • Can request IMSI/IMEI at any time
LTE/4G

- Widely deployed, 1.37 billion users by end of 2015
- More secure than previous generations
- Best effort to avoid previous mistakes

Fig. source: Wikipedia
LTE Architecture

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

• Mutual authentication between base station & mobiles

• Mandatory integrity protection for signaling messages
  - Subscriber tracking is made more difficult

• Other security improvements (not relevant for this talk)

➢ LTE fake base stations: thought to be complex* and less effective

➢ But in practice:
  ✔ Implementation/configuration flaws, specification/protocol deficiencies?

* https://insidersurveillance.com/rayzone-piranha-lte-imsi-catcher/
Evaluating LTE Security: Experiment Set-up

Set-up cost - little over 1000 Euros!

- Hardware – USRP, LTE dongle, LTE phones
- Software - OpenLTE & srsLTE

Thanks to OpenLTE and srsLTE group!
Relevant LTE Features

• (Smart) Paging

• Diagnostic Reports from UE

• Mobility Management
Feature: Paging in LTE

Why: locate subscriber to deliver calls/messages

IMSI = 404220522xxxxxx

Paging Request Type 2

{404220522xxxxxx : A000FFFF }

“GUTI” = A000FFFF
Paging configuration vulnerabilities

Deployments all over the world!

• Smart Paging
  ✓ Directed onto a small cell rather than a tracking area
  ✓ Allows attacker to locate LTE subscriber in a cell

• GUTI persistence
  ✓ GUTI change – handover/attach/reallocation procedure
  ✓ MNOs tend not to change GUTI sufficiently & frequently

• MME issues
Feature: Reports from UE to eNodeB

eNodeB can demand diagnostic reports from UE
  - List of visible eNodeBs, signal strengths, UE’s GPS co-ordinates

- UE Measurements reports
  - Necessary for smooth handovers

- Radio link failure (RLF) reports
  - Necessary for troubleshooting failures
Feature: Extended Mobility Management in LTE

EMM protocol - Controlling UE mobility in LTE network!

• Tracking Area Update (TAU) procedure
  ✓ UE sends “TAU Request” to notify on moving to a new Tracking Area
  ✓ During TAU, MME & UE agree on network mode (2G/3G/4G)
  ✓ “TAU Reject” used to reject some services services (e.g., LTE) to UE

• LTE Attach procedure
  ✓ UE sends its network capabilities to eNodeB
    ✓ E.g., “supports LTE”, “supports data”
Discovered Vulnerabilities in LTE

Specification
• UE measurement reports
  ✓ Requests not authenticated: reports are not encrypted

• Tracking Area Update (TAU) procedure
  ✓ Reject messages are not integrity protected

• LTE Attach procedure
  ✓ Network capabilities are not protected against bidding down attacks

Implementations: (all baseband vendors)
• RLF reports
  ✓ Requests not authenticated: reports are not encrypted
Attacks: Location leaks
Semi-Passive: determine tracking area & cell ID

- VoLTE calls: Mapping GUTIs to phone number
  - 10 silent calls to victim’s number
  - High priority → paging to entire tracking area (TA)
  - Passive sniffer in a TA

- Social identities: Mapping GUTIs to Social Network IDs
  - E.g., 10 Facebook messages, whatsapp/viber
  - Low priority → Smart paging to a last seen cell
  - Passive sniffer in a cell
Active: leak fine-grained location

Precise location using trilateration or GPS!

- Measurement/RLF report
  - Two rogue eNodeBs for RLF
  - eNodeB1 triggers RL failure: disconnects mobile
  - eNodeB2 then requests RLF report from mobile
Attacks: Denial of service
**DoS Attacks**

Exploiting specification vulnerability in EMM protocol!

- Downgrade to non-LTE network services (GSM/3G)
- Deny all services (GSM/3G/LTE)
- 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 Vs Security measures (defined 15 years back)
Impact

All (4) affected baseband manufacturers
- Responsible disclosure of bugs: acknowledged and patches released
- But OEMs do not yet have security updates to phones

Network operators
- Configuration issues were acknowledged and fixed

Standards organizations
- Security issues presented at 3GPP SA3 (in Anaheim, Nov 2015) and GSMA
- Changes into LTE specifications are in progress

Social network applications
- Facebook no longer supports completely silent messages
Take-away messages

• New vulnerabilities in LTE standards/chipsets
• Configuration by operators do not follow best practices

• Lead to attacks:
  • Social applications used for silent tracking
  • Locating 4G devices using trilateration, GPS co-ordinates!
  • DoS attacks are persistent & silent to users

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

Questions?