

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

Altaf Shaik & Jean Pierre Seifert
TU Berlin & T-Labs

Ravishankar Borgaonkar
University of Oxford

N. Asokan
Aalto & Uni. of Helsinki

Valtteri Niemi
Uni. of Helsinki

23 February 2016
NDSS 2016 San Diego USA



UNIVERSITY OF HELSINKI

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..1

- 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 or 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

4G/LTE

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

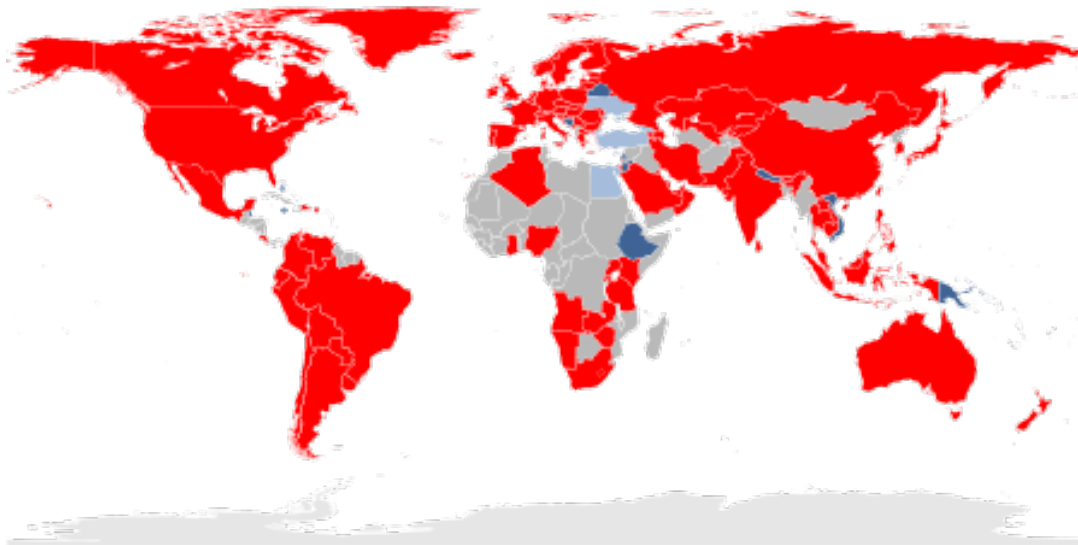
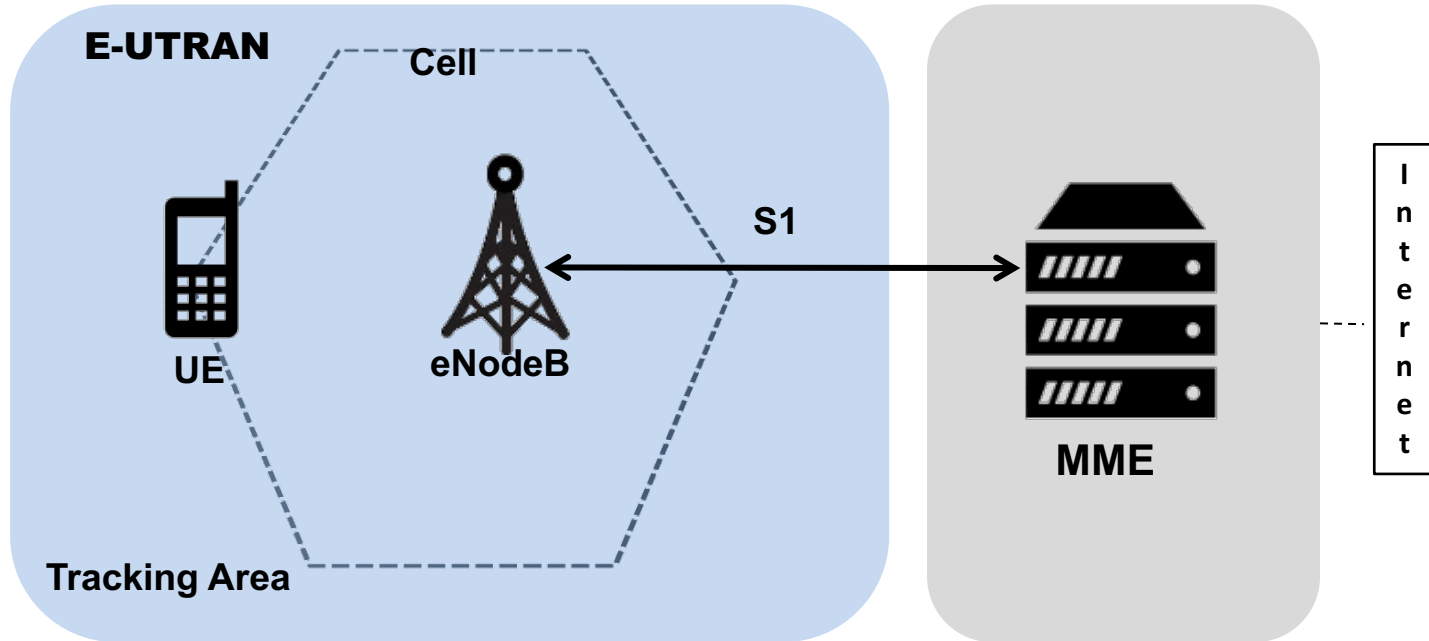


Fig. source: Wikipedia

4G Architecture



eNodeB: Evolved Node B ("base station")
E-UTRAN: Evolved Universal Terrestrial Access Network
MME : Mobility Management Entity

UE: User Equipment
S1 : Interface

Security evolution in mobile networks



no mutual authentication **2G**

mutual authentication
integrity protection **3G**

mutual authentication
deeper mandatory integrity protection **4G**

decides encryption/authentication
requests IMSI/IMEI



Base Station



Research Motivation

- Analysis of access network protocols and integrity protection in practice
- 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 4G Security: Experiment Set-up

Set-up cost - little over 1000 Euros!

- Hardware – USRP, 4G dongle, 4G phones
- Software – OpenLTE & srsLTE



Thanks to OpenLTE and srsLTE group!

Results

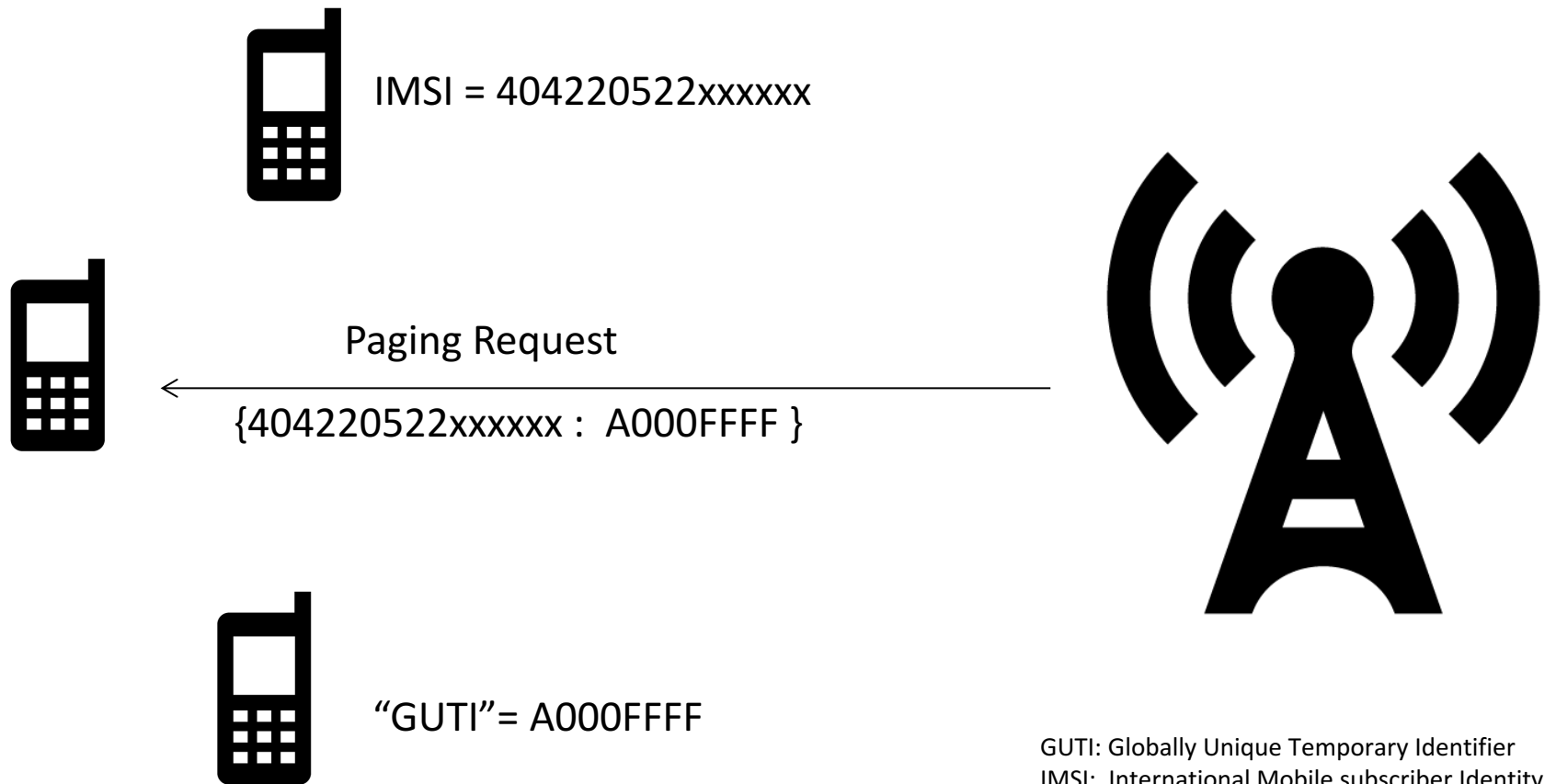
- Vulnerabilities in 4G specifications and networks
- Demonstrating impact by practical attacks
 - ✓ Location leaks
 - ✓ Denial-of-service

Relevant 4G Features

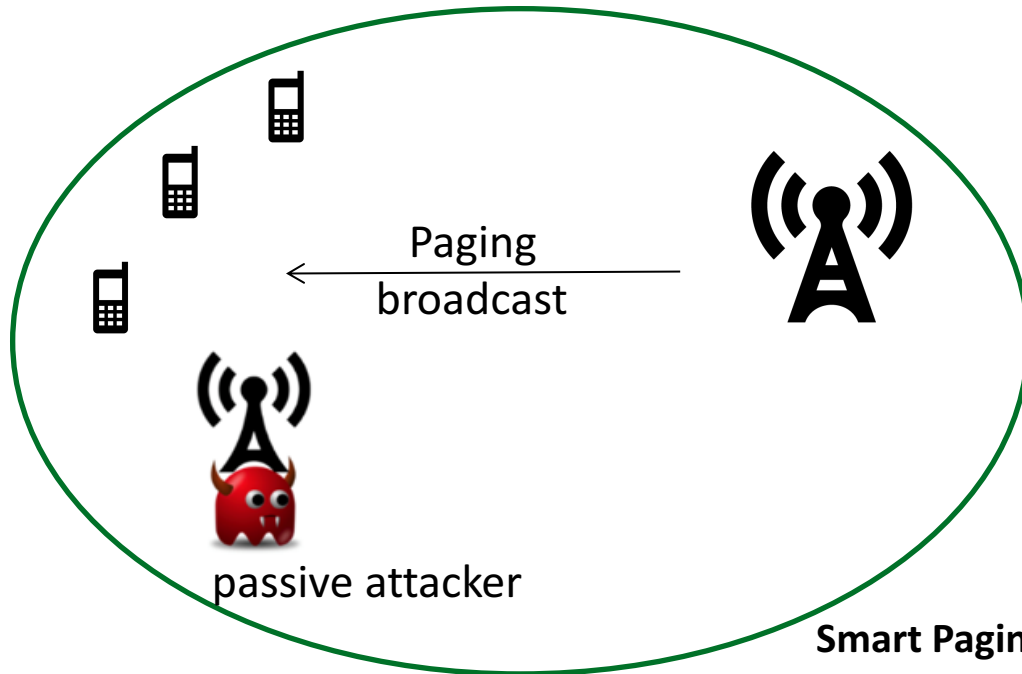
- (Smart) Paging
- Diagnostic Reports from UE
- Mobility Management

Feature: Paging in 4G

Why: locate subscriber to deliver calls/messages



Paging configuration vulnerabilities



F7	10	17EF
F7	11	17EF
F7	1B	17EF
F7	14	17EF
F7	16	17EF
F7	18	17EF
F7	12	17EF
F7	11	17EF

e03a5b73
e03a5bda
e03a5be2
e03a5bed
e03a5bfs

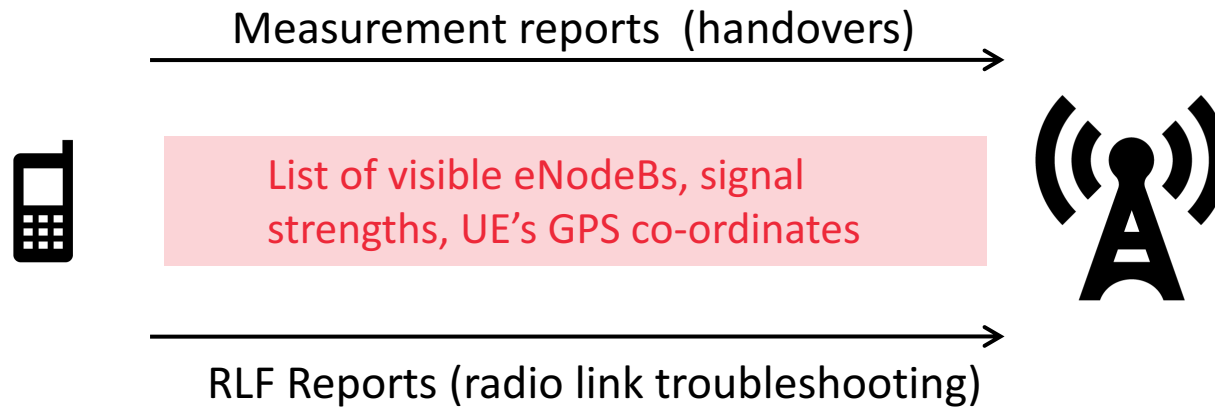
Smart Paging

- ✓ sent onto a small cell instead of a big tracking area
- ✓ Allows attacker to locate 4G subscriber in a cell

GUTI persistence

- ✓ MNOs don't change GUTI sufficiently & frequently

Feature: Reports from UE to eNodeB



Vulnerabilities in the feature



Specification

UE measurement reports

- ✓ Requests not authenticated
- ✓ Reports are not encrypted



← Send me
Measurement/RLF report



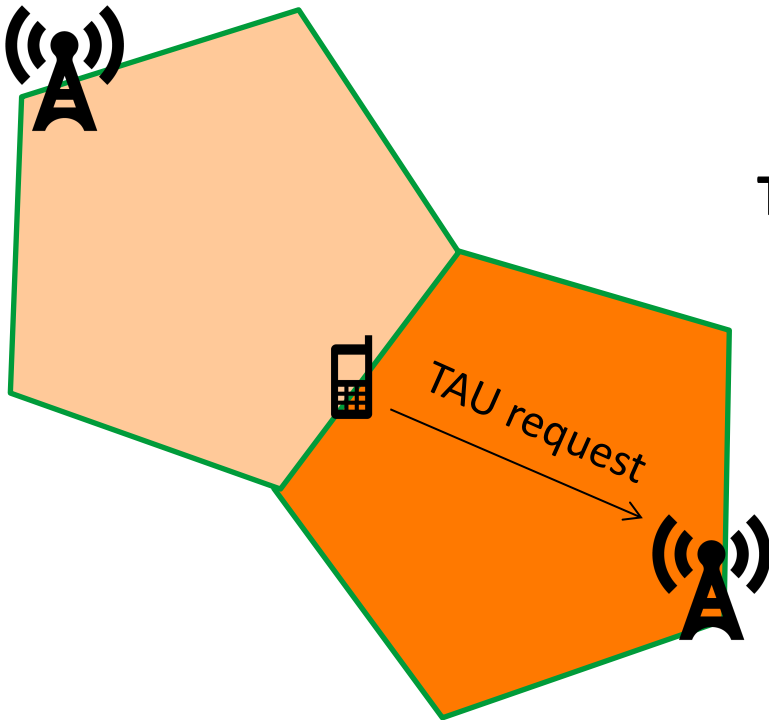
active attacker

Implementations

RLF reports

- ✓ Requests not authenticated
- ✓ Reports are not encrypted
- ✓ All baseband vendors

Feature: Mobility Management in 4G

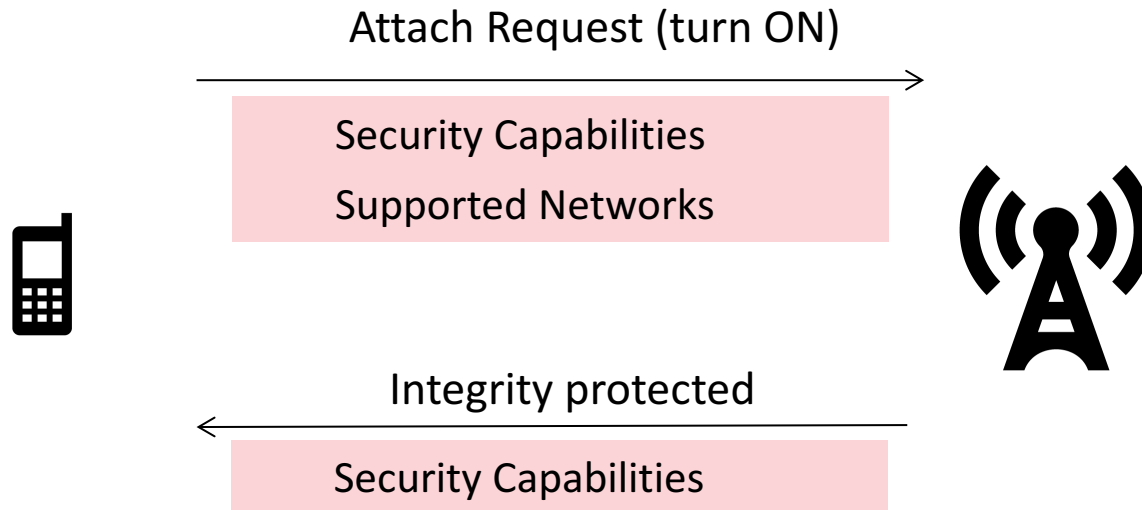


Tracking Area Update (TAU) procedure

- ✓ 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

Feature: Mobility Management in 4G



Specification vulnerability:
Network capabilities not protected - bidding down attacks

Discovered Vulnerabilities in 4G

Specification

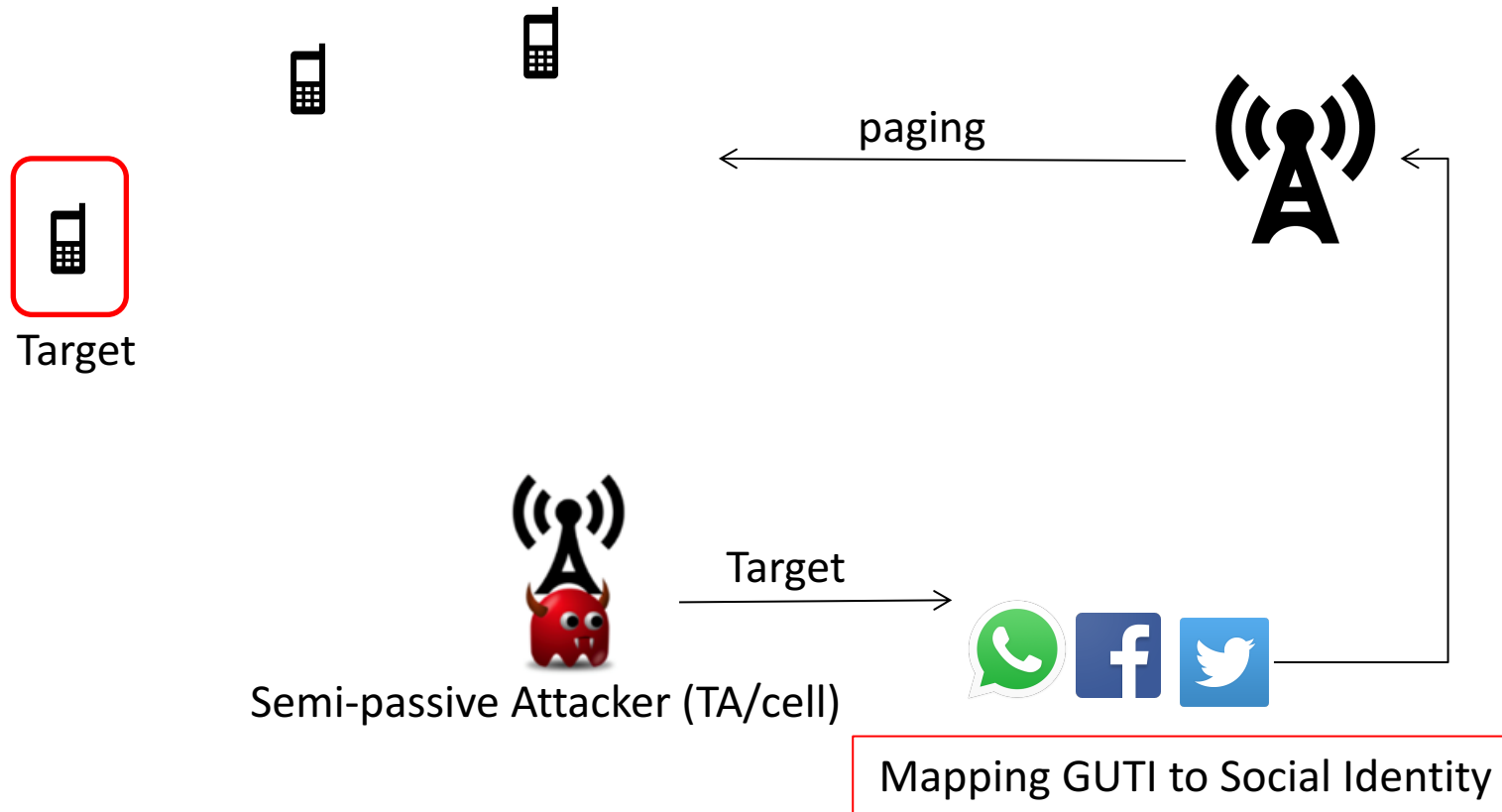
- UE measurement reports
 - ✓ Requests not authenticated: reports are not encrypted
- Tracking Area Update (TAU) procedure
 - ✓ Reject messages are not integrity protected
- Attach procedure
 - ✓ Network capabilities are not protected against bidding down attacks

Implementations: (all baseband vendors)

- RLF reports
 - ✓ Requests not authenticated: reports are not encrypted
-

Attacks: Location leaks

Location Leaks: tracking coarse level



Location Accuracy: 2 Sq. Km

Location Leaks: tracking precise level

```
measResultNeighCells: measResultListEUTRA (0)
└─ measResultListEUTRA: 1 item
   └─ Item 0
      └─ MeasResultEUTRA
         ├── physCellId: 200
         └─ measResult
            └─ rsrpResult: -112dBm <= RSRP < -111dBm (29)
locationInfo-r10
└─ locationCoordinates-r10: ellipsoidPointWithAltitude-r10 (1)
   └─ ellipsoidPointWithAltitude-r10: [REDACTED]
      └─ EllipsoidPointWithAltitude
         ├── latitudeSign: north (0)
         ├── degreesLatitude: 52, [REDACTED]
         ├── degreesLongitude: 13, [REDACTED]
         ├── altitudeDirection: height (0)
         └─ altitude: 116 m
gnss-TOD-msec-r10: [REDACTED]
```



Active attacker



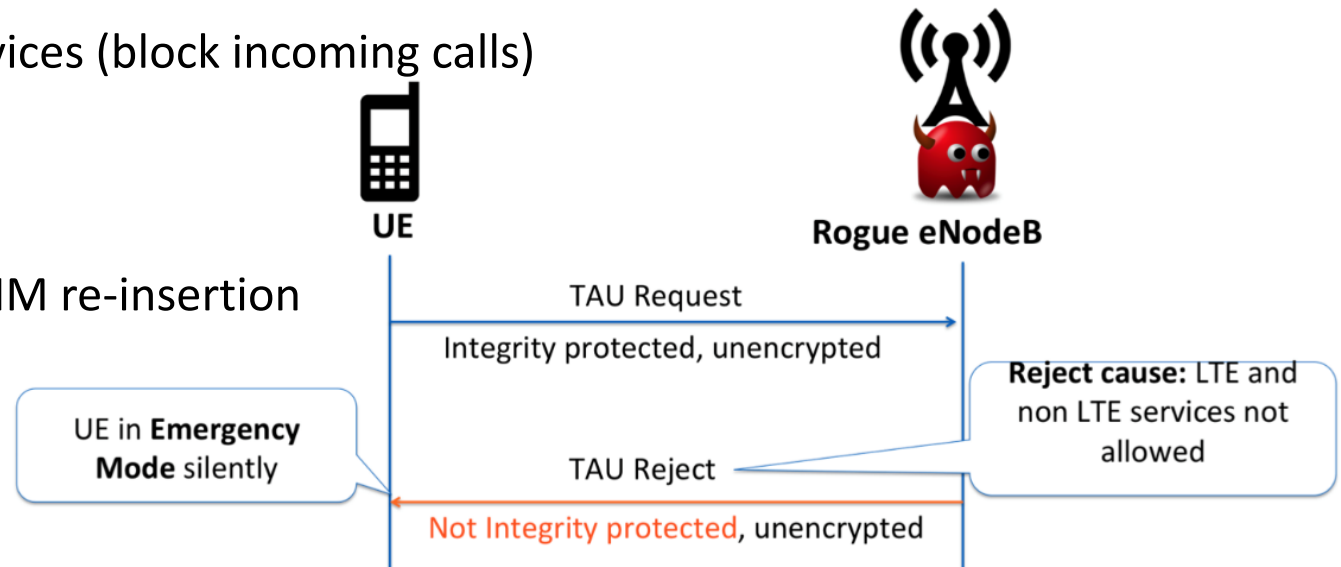
Location Accuracy: 50 meters (or) GPS co-ordinates

Attacks: Denial of service

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 Vs Security measures (defined in 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 SA3 (in Anaheim, Nov 2015) and GSMA
- ✓ Changes into LTE specifications are in progress



Social network applications

- ✓ Facebook no longer supports completely silent messages

Conclusions

- New vulnerabilities in 4G 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

Thank You.

Questions?

Shout for a demo!

This work was supported in part by the Intel Collaborative Research Institute for Secure Computing, Academy of Finland (“Cloud Security Services” project #283135), Deutsche Telekom Innovation Laboratories (TLabs), and 5G-Ensure (grant agreement No. 671562, www.5Gensure.eu).
