Privacy Leaks on 4G/LTE networks

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

Ravishankar Borgaonkar
Oxford University

N. Asokan
Aalto & Uni. of Helsinki

Valtteri Niemi
Uni. of Helsinki

12 March 2016

Nullcon, Goa

UNIVERSITY OF HELSINKI

Outline

- Evolution of security in mobile networks
  - ✓ 2G/GSM, 3G/UMTS, 4G/LTE
- Practical attacks against 4G/LTE
  - ✓ Location and identity leaks
  - ✓ Denial of service
- Vulnerabilities and attacks
- Impact

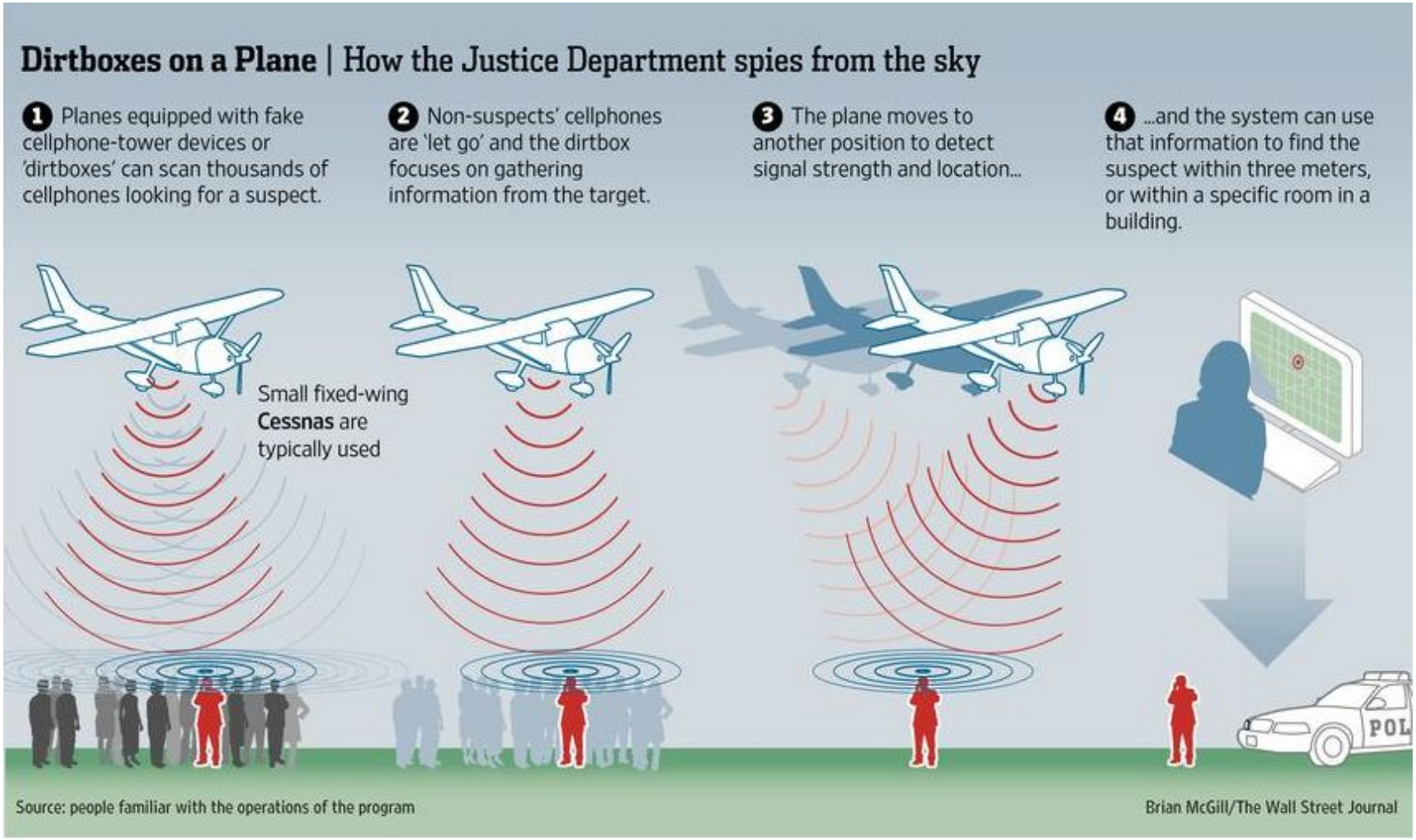
Motivation

- Baseband - GPS access rights (no android or iOS)
  - user is unaware
- Platform for practical security research in LTE/4G
  - closed source telco industry
  - 2G, 3G open source available - osmocom

Fake base-stations..1

- Used for: IMSI/IMEI/location tracking, call & data interception
- Exploit weaknesses in 2G & 3G (partially)
- Knows as IMSI Catchers, very expensive
- Difficult to detect on normal phones (Darshak, Cryptophone or Snoopsnitch)

Fake base-stations..2



LTE/4G

- Widely deployed, 1.37 billion users by end of 2015
- More secure than previous generations
- High speed data connection and quality of service

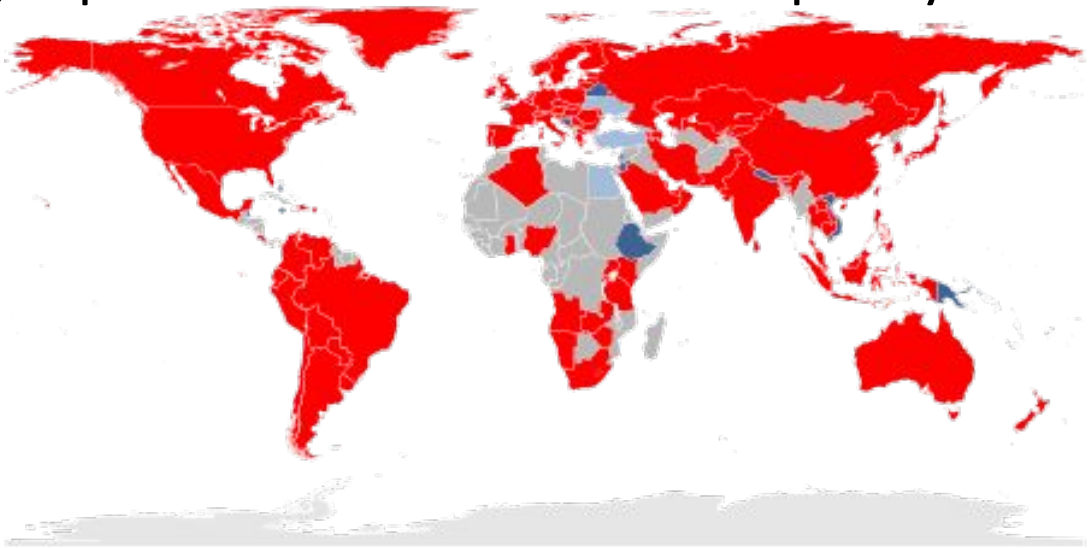
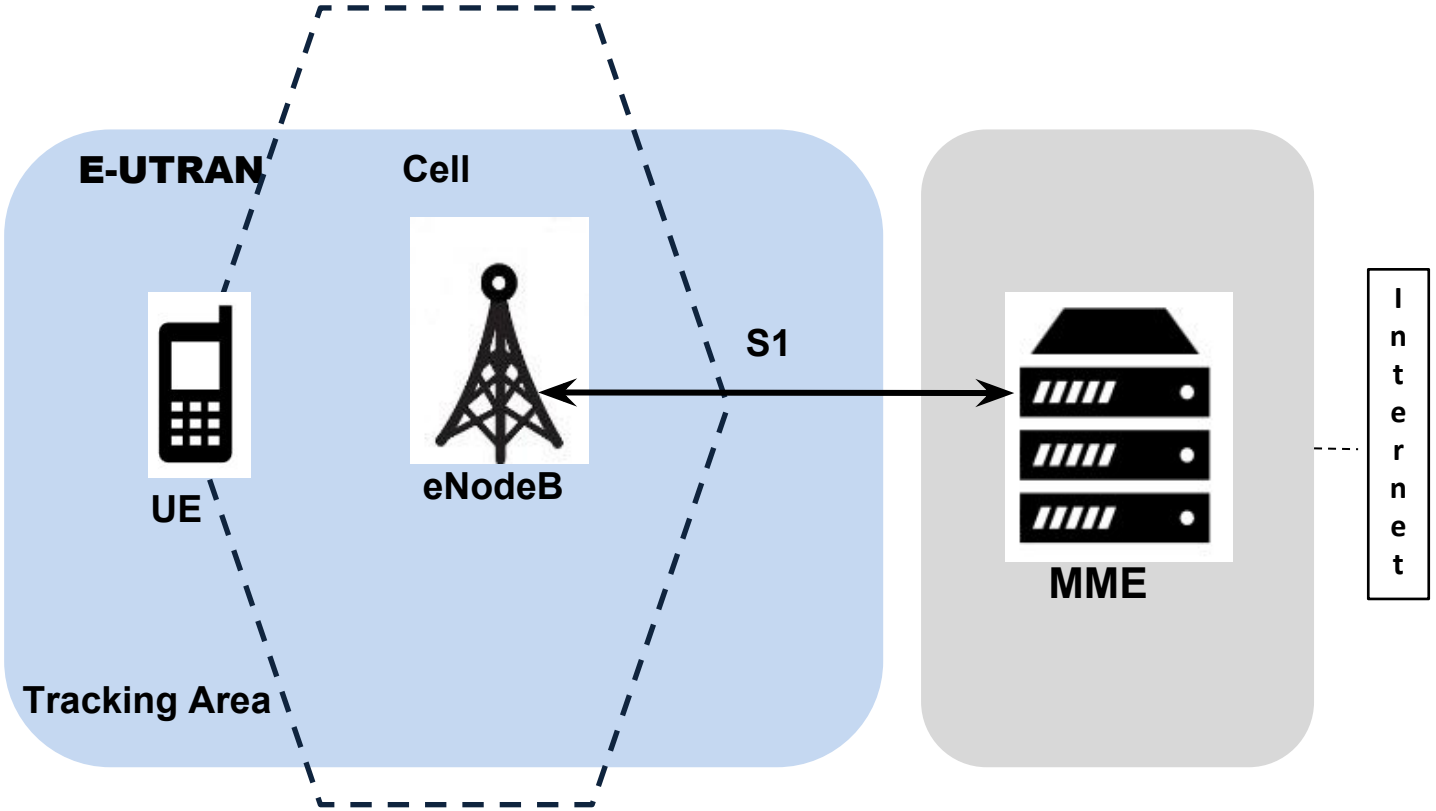


Fig. source: Wikipedia

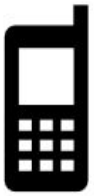
4G Architecture



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



Phone

no mutual authentication **2G**

mutual authentication
integrity protection **3G**

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

Base Station

decides encryption/authentication
requests IMSI/IMEI

Enhanced security in LTE

- Mutual authentication between base station & mobiles
- Mandatory integrity protection for signaling messages
- IMEI is not given in non-integrity messages
- Fake base-stations fail (partly)
- Stronger security algorithms (AES)

Challenge

- 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
- Base station and sniffer

Thanks to OpenLTE and srsLTE group!

Results

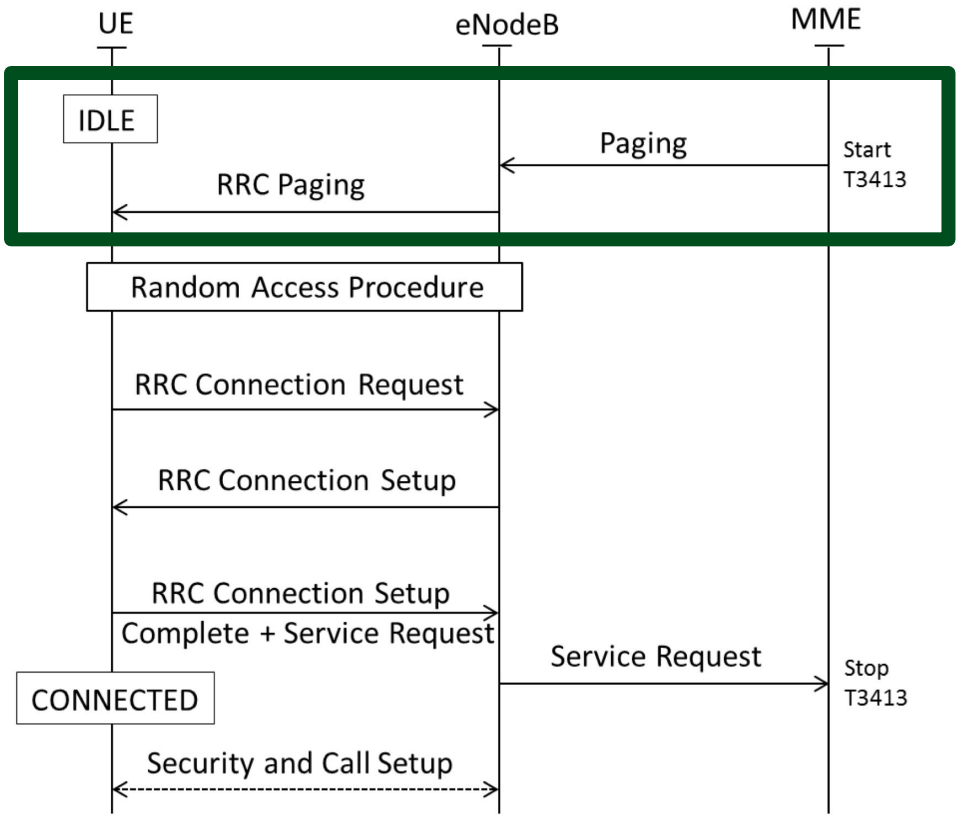
- Vulnerabilities in 4G specifications and networks

- Demonstrating impact by practical attacks
  - ✓ Location and identity leaks
  - ✓ Denial-of-service

Relevant 4G Features

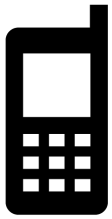
- (Smart) Paging
- Diagnostic Reports from UE
- Mobility Management

Feature: Paging in LTE

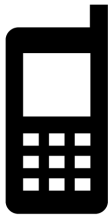


Paging from base station

Why: locate subscriber to deliver calls/messages

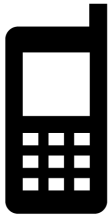


IMSI = 404220522xxxxxx



Paging Request

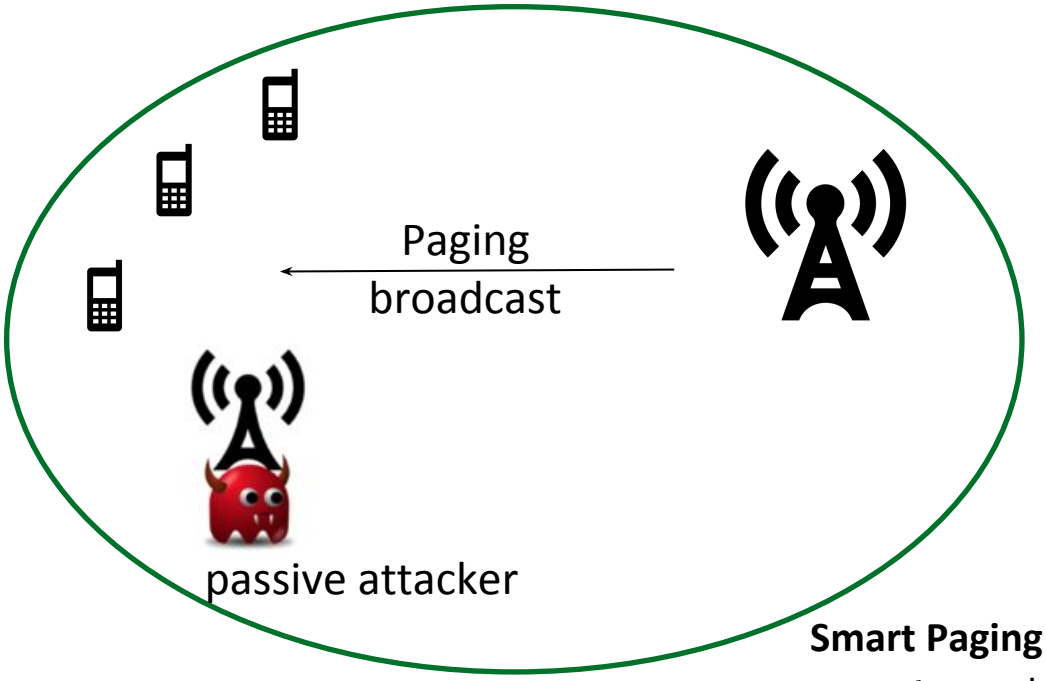
{404220522xxxxxx : A000FFFF }

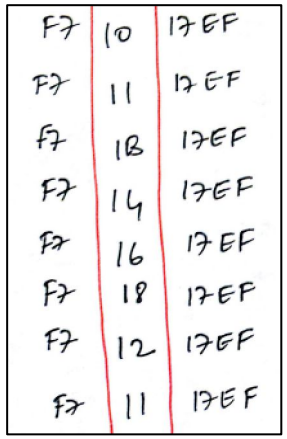


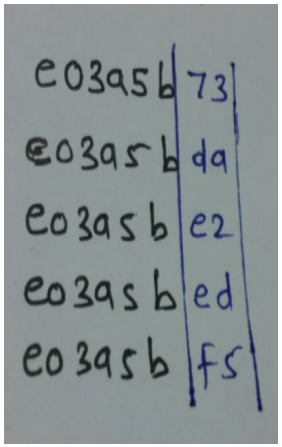
"GUTI"= A000FFFF

GUTI: Globally Unique Temporary Identifier
IMSI: International Mobile subscriber Identity

Paging configuration vulnerabilities







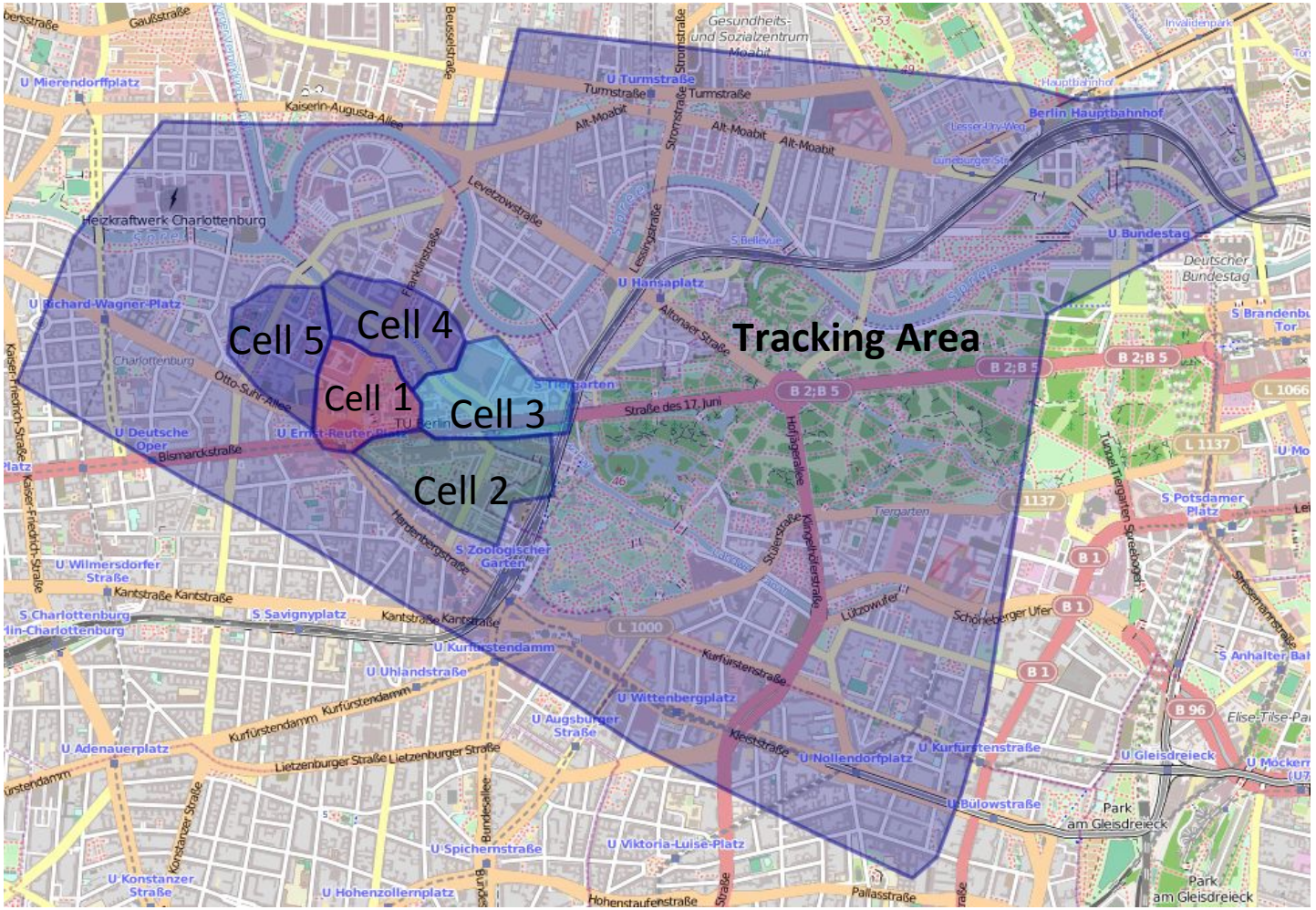
Smart Paging

- ✓ 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
- ✓ MME configuration issues

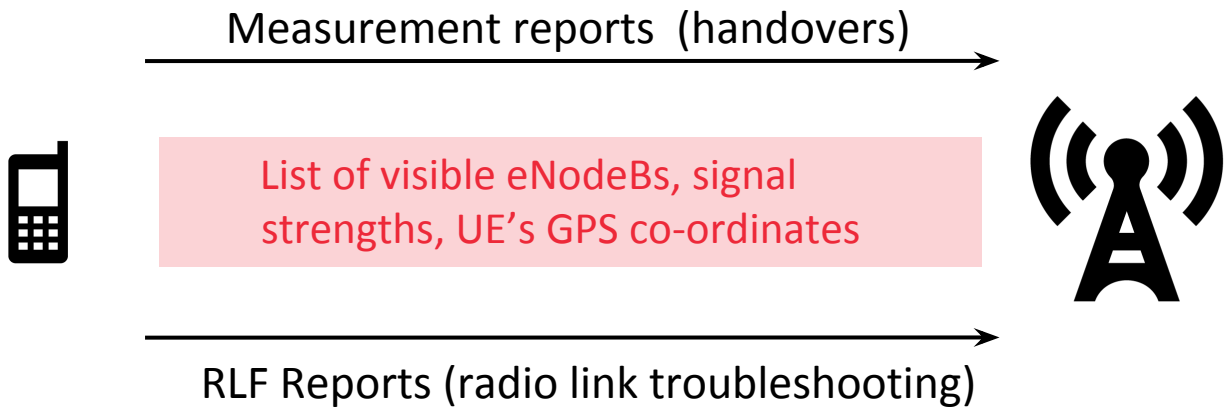
LTE Smart Paging



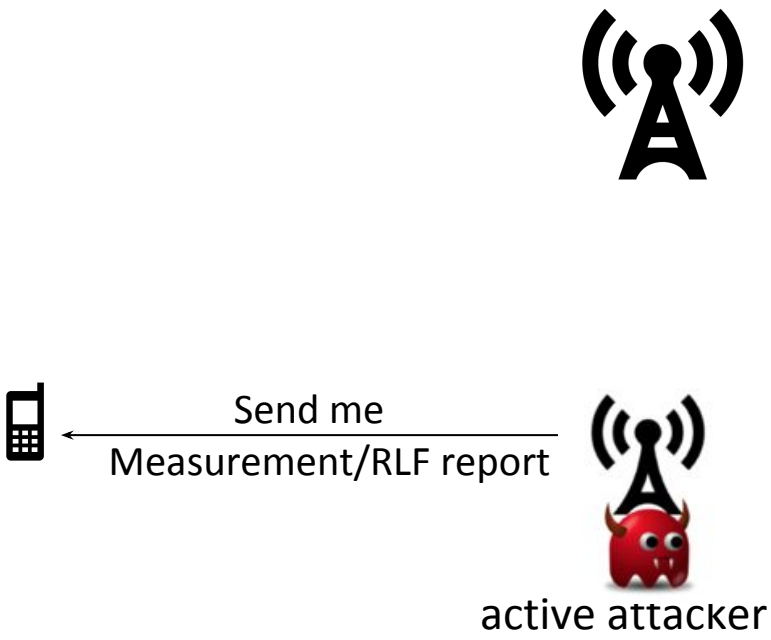
Feature: Reports from UE to eNodeB

- 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: Reports from UE to eNodeB



Vulnerabilities in the feature



Specification

UE measurement reports

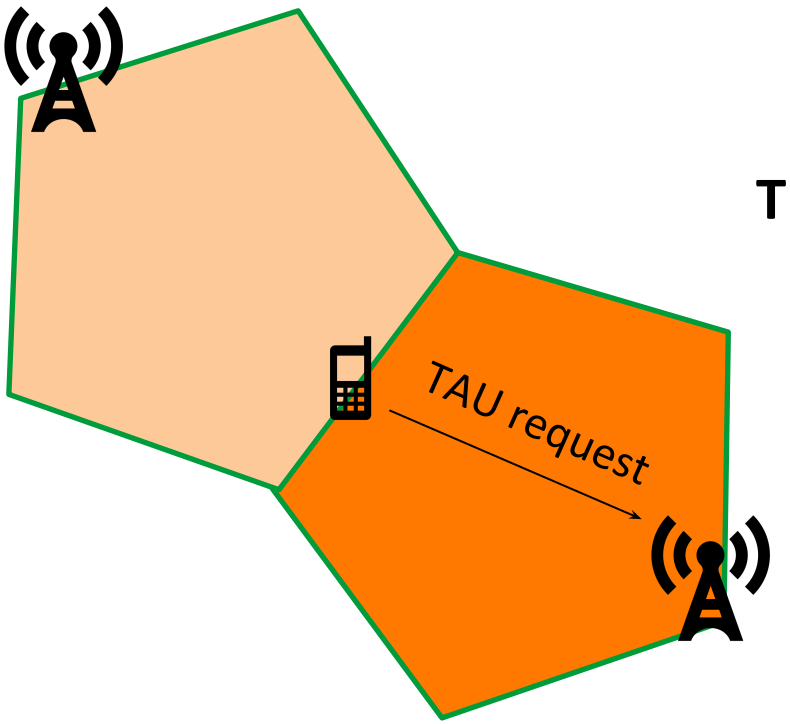
- ✓ Requests not authenticated
- ✓ Reports are not encrypted

Implementations

RLF reports

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

Feature: Mobility Management in 4G

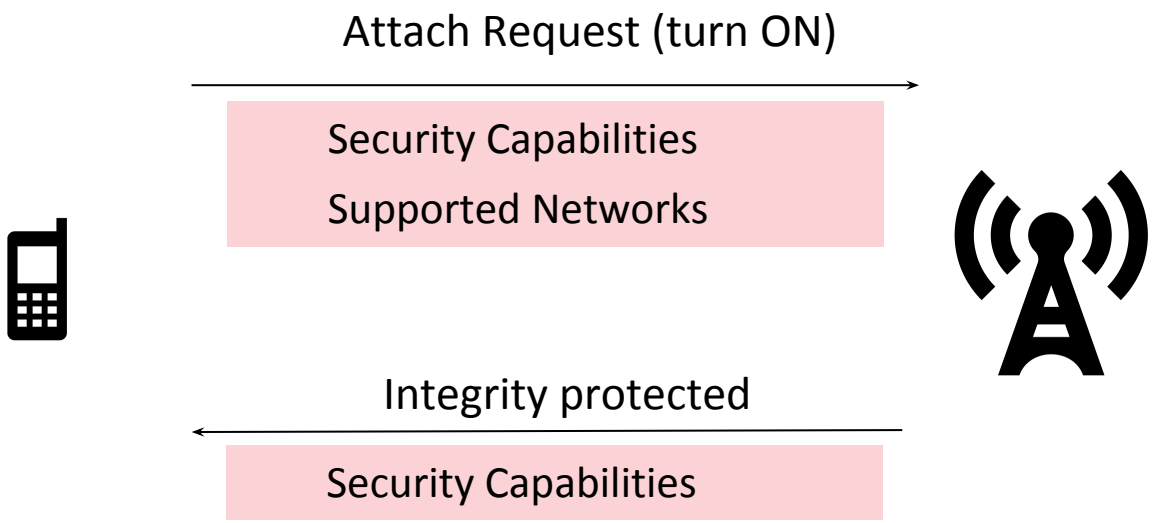


Tracking Area Update (TAU) procedure

- ✓ During TAU, MME & UE agree on network mode (2G/3G/4G)
- ✓ "TAU Reject" used to reject some services services (e.g., 4G) to UE

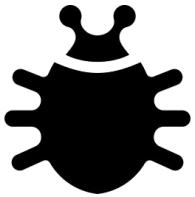
Specification vulnerability: Reject messages are not integrity protected

Feature: Mobility Management in 4G



Specification vulnerability: Network capabilities not protected

IMEI leak : implementation vulnerability



TAU reject – special cause number!

- IMEI is leaked by popular phones
- Triggered by a special message
- Fixed now but still your device leak ;)
- IMEI request not authenticated correctly

```
Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Identity response (0x56)
    Mobile identity - IMEI (357506057669310)
        Length: 8
        0011 .... = Identity Digit 1: 3
        .... 1... = Odd/even indication: Odd number of identity digits
        .... .010 = Mobile Identity Type: IMEI (2)
        BCD Digits: 357506057669310
```

Discovered Vulnerabilities in 4G

Specification

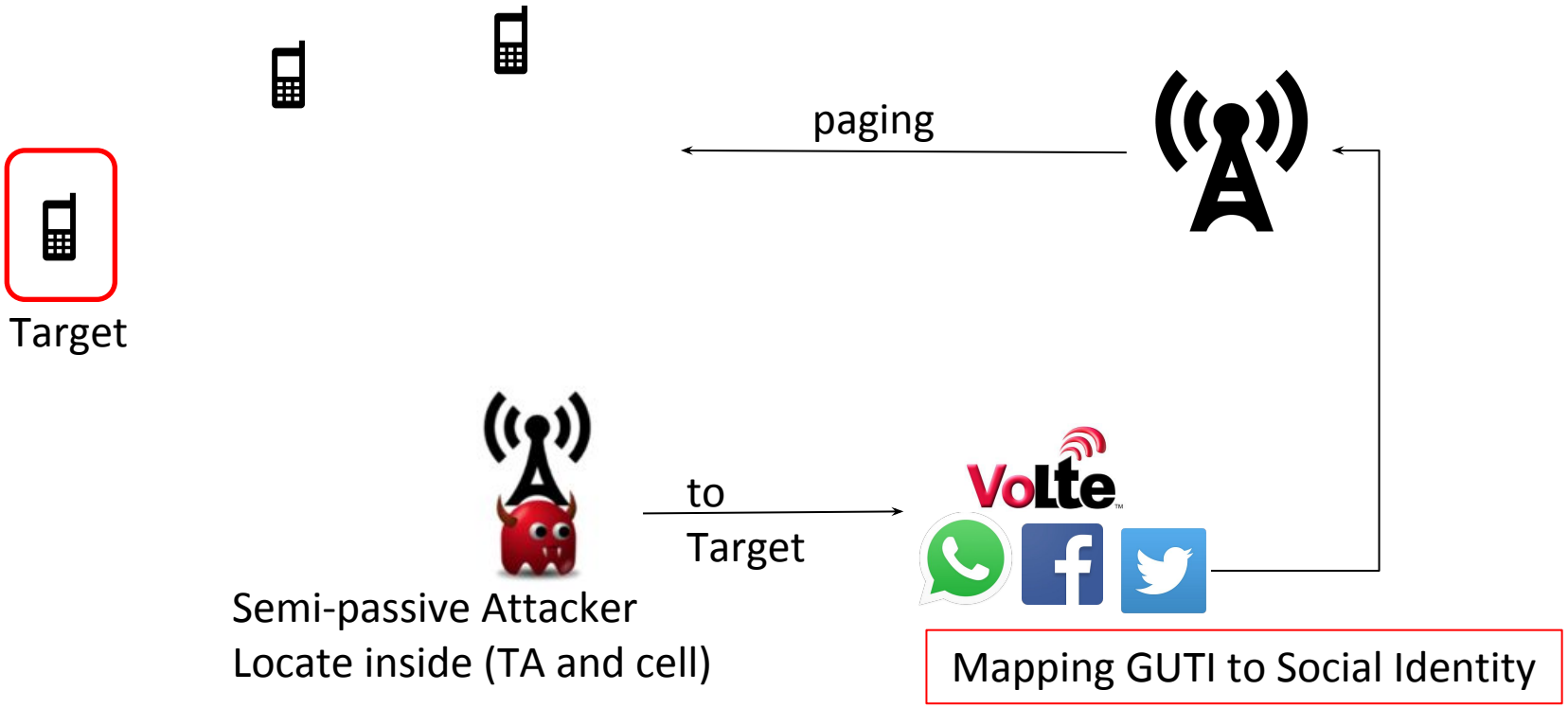
- UE measurement reports
  - ✓ Requests not authenticated: reports are not encrypted
- Tracking Area Update (TAU) procedure
  - ✓ Reject messages are not integrity protected
- Attach procedure
  - ✓ Network capabilities are not protected against bidding down attacks

Implementations: (baseband vendors)

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

Attacks: Location leaks

Location Leaks: Coarse level

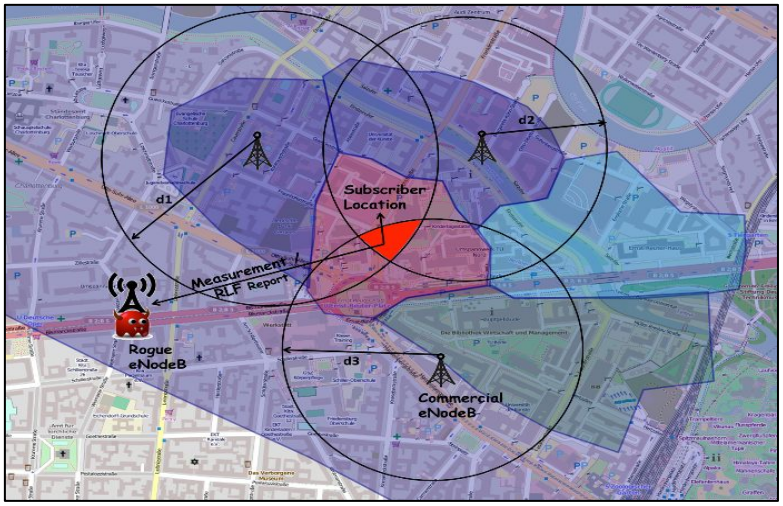


Location Accuracy: 2 Sq. Km

Location Leaks: 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]
```

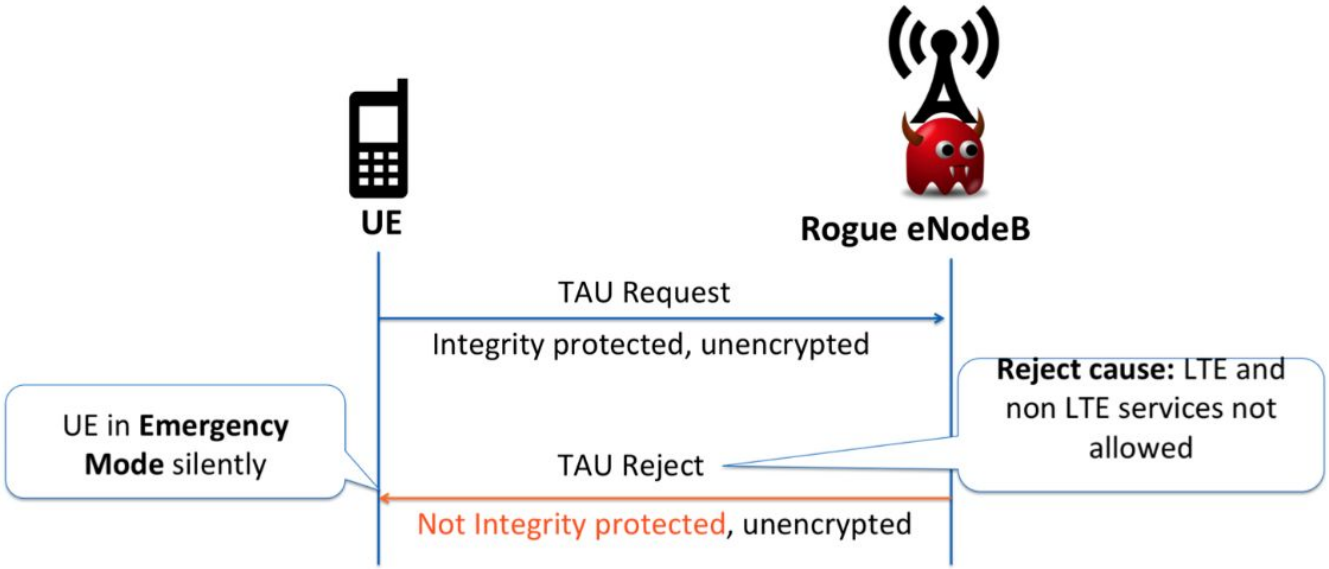
Active attacker



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

Attacks: Denial of service

DoS

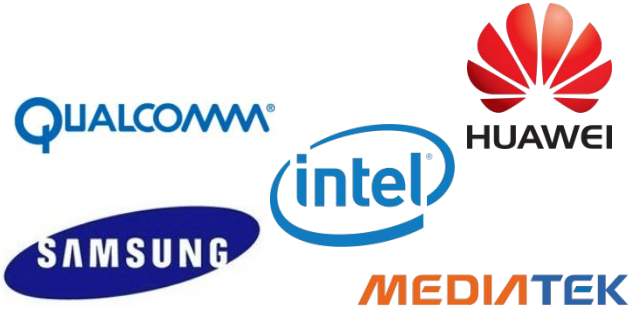

UE
Rogue eNodeB
TAU Request
Integrity protected, unencrypted
UE in **Emergency Mode** silently
Reject cause: LTE and non LTE services not allowed
TAU Reject
Not Integrity protected, unencrypted

DoS

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

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

Solution!

Use any old Nokia phone without battery and SIM card!

Thank You.

Questions?