LTE and IMSI catcher myths

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

Blackhat EU, Amsterdam, Netherlands

13 November 2015

A! Aalto University

berlin

UNIVERSITY OF HELSINKI

Outline

- Fake base stations in GSM/3G
- LTE/4G Security
- Types of vulnerabilities in practice
- Building LTE/4G base station
- Attacking methods/demos
- Impact & Analysis

Motivation

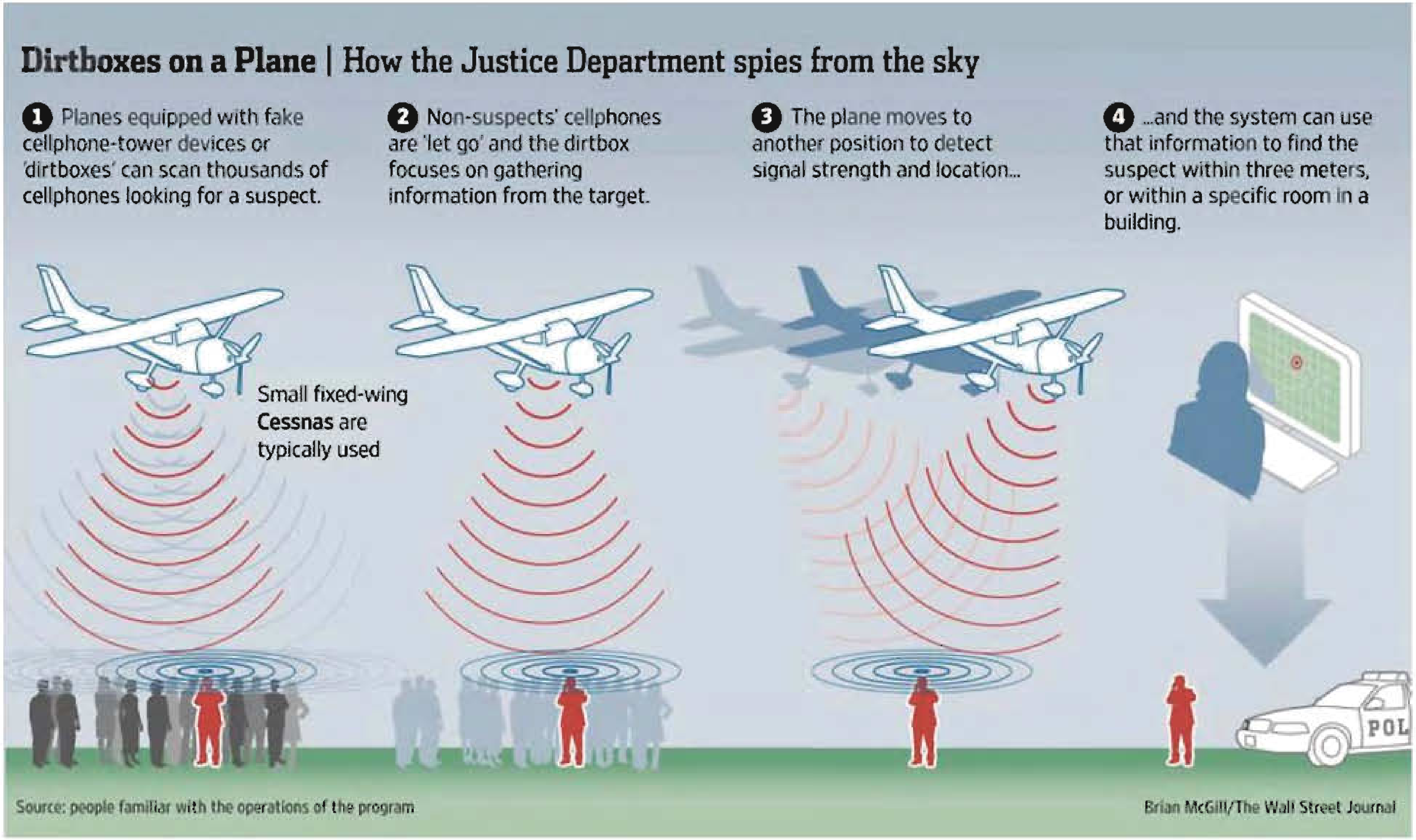
- Baseband story
- Platform for practical security research in LTE/4G
- Attacking cost VS security measures (defined in 15 years back)

Fake base-stations..1

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

© Erik Tham/Corbis

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.

Small fixed-wing **Cessnas** are typically used

Source: people familiar with the operations of the program

Brian McGill/The Wall Street Journal

Why in GSM & 3G

- GSM - lack of mutual authentication between base station and mobiles

- 3G – no integrity protection like in LTE, downgrade attacks

- GSM/3G – power is to base station, decides when and how to authenticate/encrypt

© Erik Tham/Corbis

- IMSI/IMEI can be requested any time

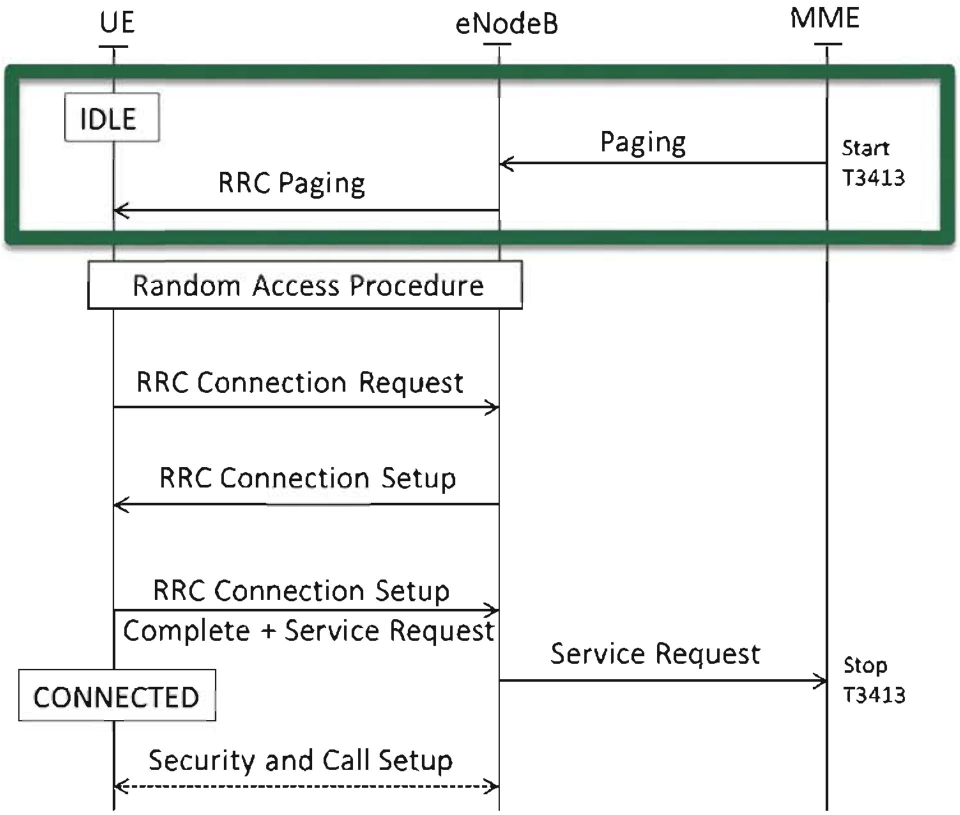
LTE/4G networks

- Widely deployed, 1.37 billion users at the end of 2015
- Support for VoLTE
- High speed data connection and quality of service
- More secure than previous generations
- Best effort to avoid previous mistakes

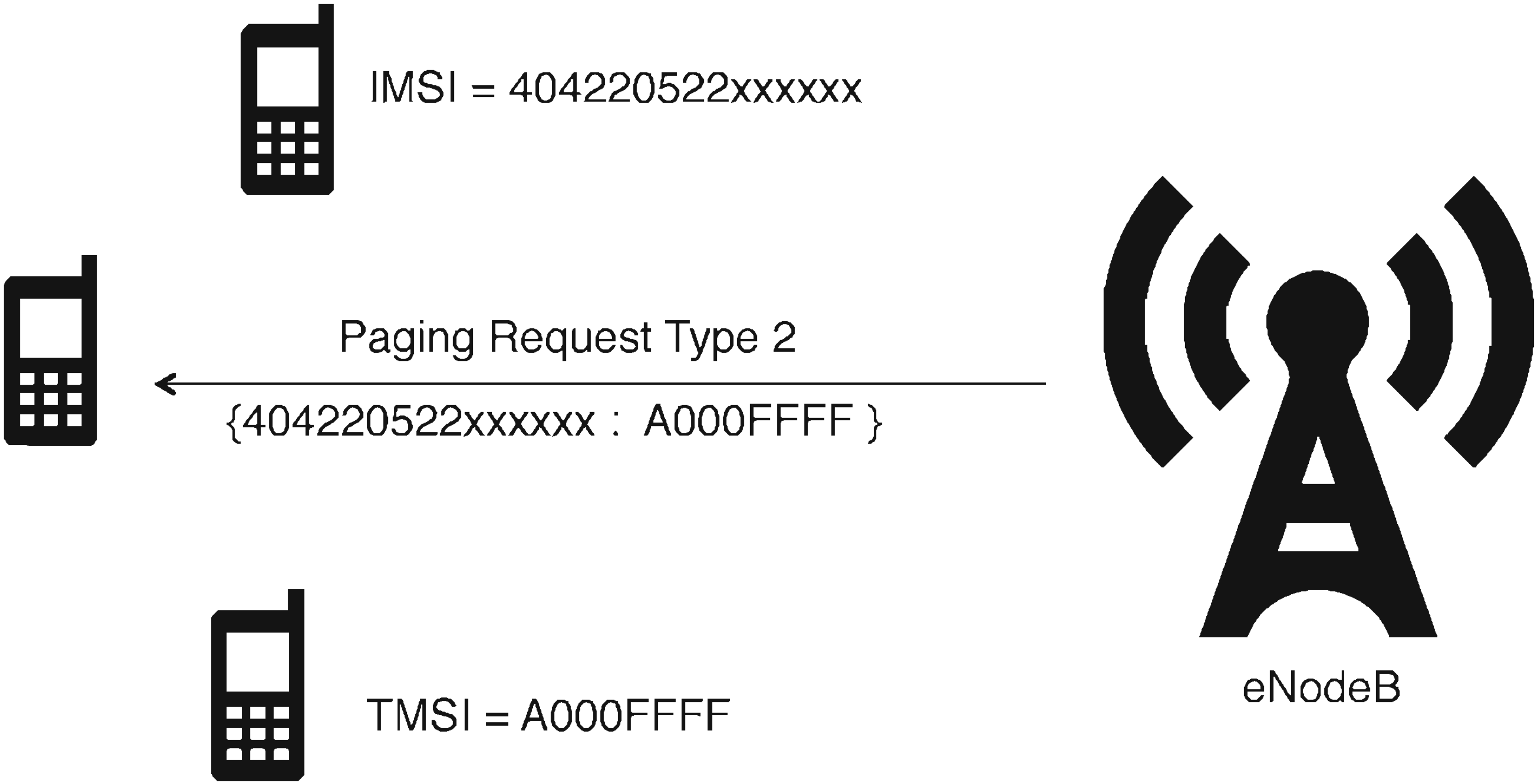
Enhanced security in LTE

- Mutual authentication between base station & mobiles
- Mandatory integrity protection for signaling messages
- Extended AKA & key hierarchy
- Security algorithms
- Other features (not relevant for this talk)

Paging in LTE



Paging in LTE



IMSI = 404220522xxxxxx

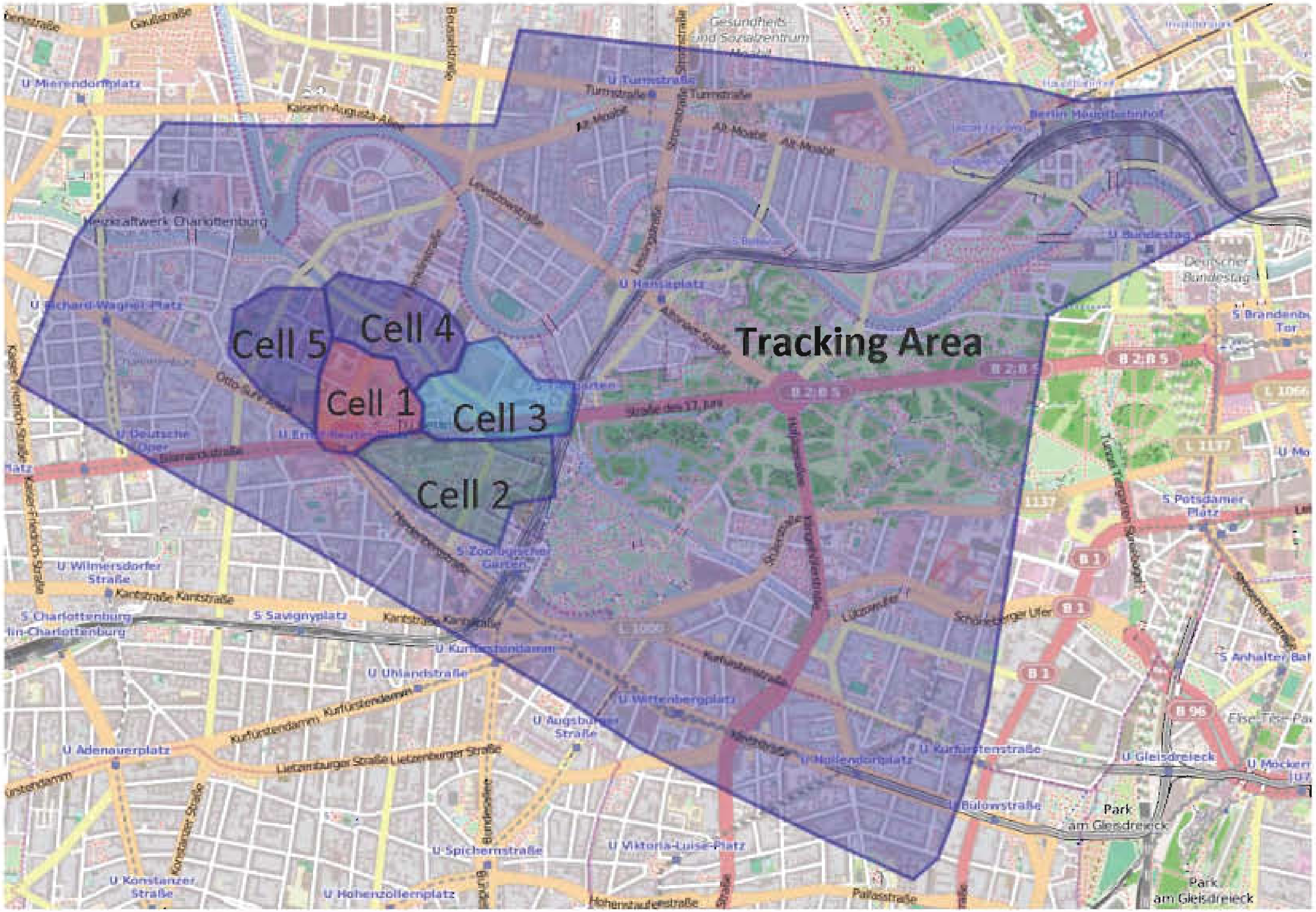
Paging Request Type 2

{404220522xxxxxx : A000FFFF }

TMSI = A000FFFF

eNodeB

LTE Smart Paging



Aalto University

UNIVERSITY OF HELSINKI

Enhanced security w.r.t fake base station

- Mutual authentication between base station & mobiles
- Mandatory integrity protection for signaling messages
- IMEI is not given in non-integrity messages
- Complexity in building LTE fake base station*
- But in practice:
  - ✓ implementations flaws, specification/protocol deficiencies?

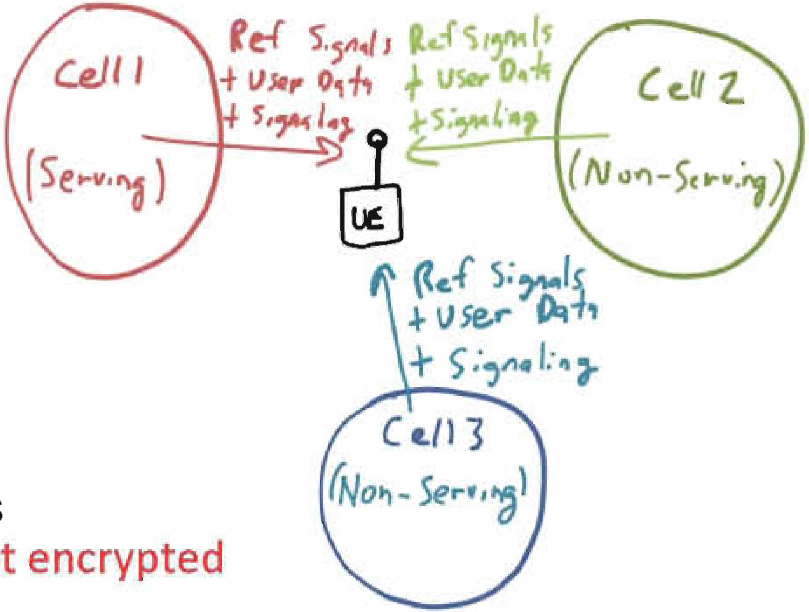
* https://insidersurveillance.com/rayzone-piranha-lte-imsi-catcher/

Specification Vulnerabilities

LTE RRC protocol* : specification vulnerability

RRC protocol – setup & manage over-the-air connectivity!

- Broadcast information
  - ✓ UE identities
  - ✓ Network information (SIB) messages
  - ✓ Neither authenticated nor encrypted
- UE measurement reports
  - ✓ Necessary for smooth handovers
  - ✓ UE sends "Measurement Report" messages
  - ✓ Requests not authenticated: reports are not encrypted

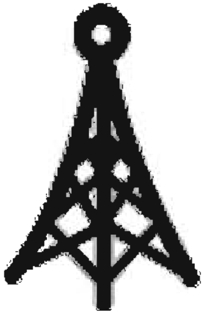


*3GPP TS 36.331 : E-UTRA; RRC protocol
Fig. source: http://lteuniversity.com/

LTE RRC protocol* : specification vulnerability

RRC protocol – setup & manage over-the-air connectivity!

- Broadcast information
- UE Identities – IMSI, TMSI
- Network information messages (SIB)
- Neither authenticated nor encrypted



eNodeB

*3GPP TS 36.331 : E-UTRA; RRC protocol
SIB : System Information Blocks

EMM protocol* : specification vulnerability

EMM protocol - Controlling UE mobility in LTE network!

- Tracking Area Update(TAU) procedure
  - ✓ UE sends "TAU Request" to notify TA
  - ✓ During TAU, MME & UE agree on network mode
  - ✓ "TAU Reject" used to reject some services services (e.g., LTE services) to UE
  - ✓ However, reject messages are not integrity protected

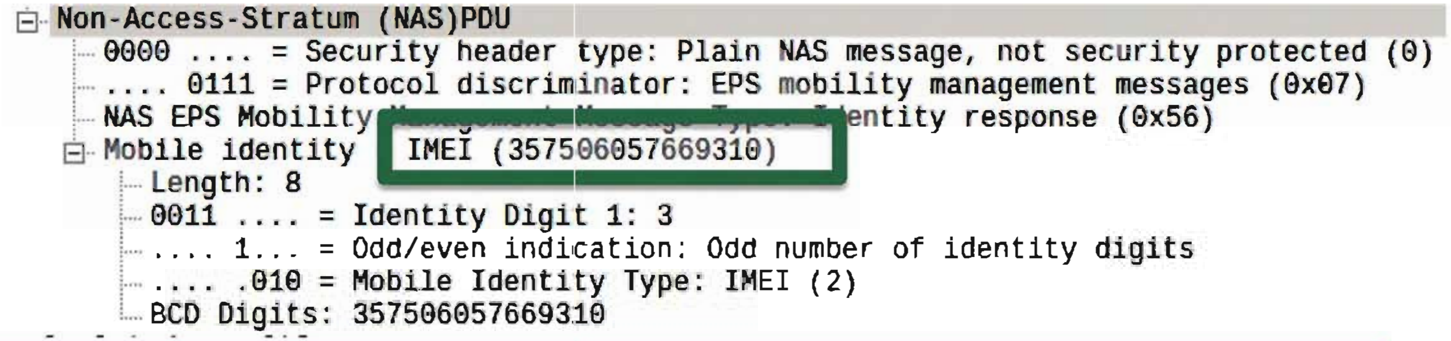
- LTE Attach procedure
  - ✓ UE sends its network capabilities
  - ✓ Unlike security algorithms, no protection
  - ✓ Network capabilities are not protected against bidding down attacks

Vulnerabilities in baseband chipset

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
```

LTE RRC* : implementation vulnerability

RLF reports – network troubleshooting!

- When Radio Link Failure happens
- Informs base station of RLF
- UE sends “RLF report” message
- Privacy sensitive information in RLF report
- Request not authenticated: reports are not encrypted

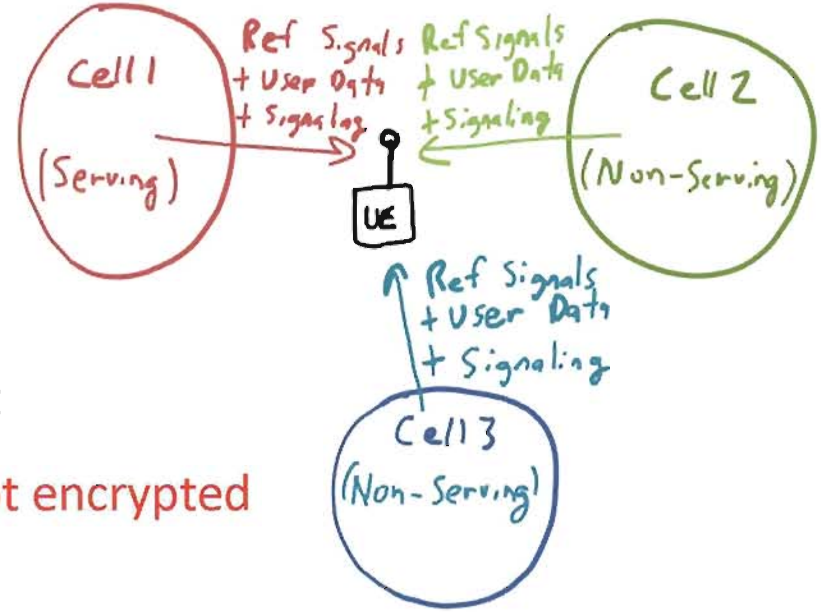
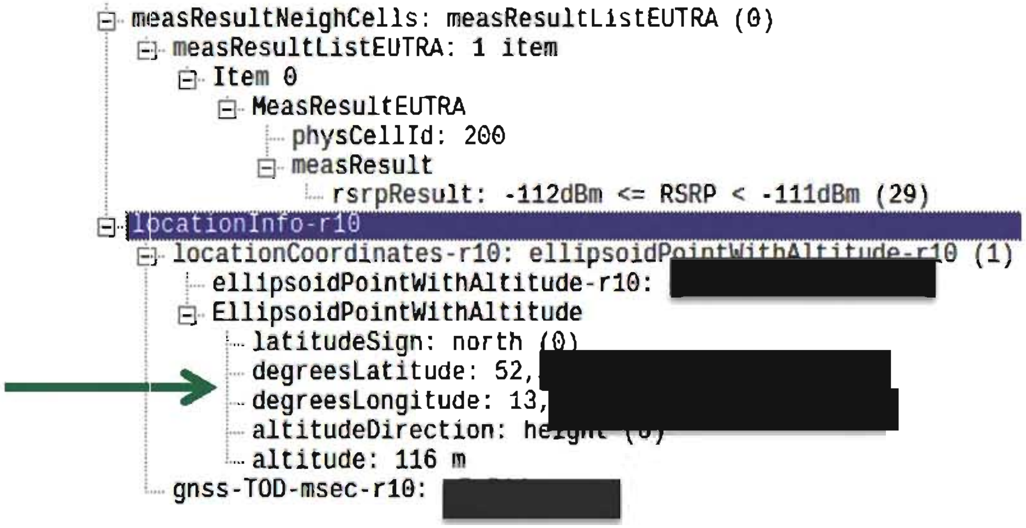


Fig. source: http://lteuniversity.com/

LTE RRC* : implementation vulnerability

Measurement reports – GPS co-ordinates!

- For handover
- Privacy sensitive information in the report
- Request not authenticated
- reports are not encrypted



```
⊟ 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: he[redacted] (0)
           altitude: 116 m
     gnss-TOD-msec-r10: [redacted]
```

Network Configuration Issues

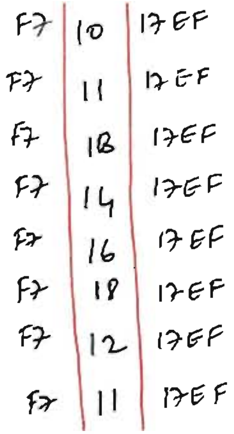
Configuration issues

Deployments all over the world!

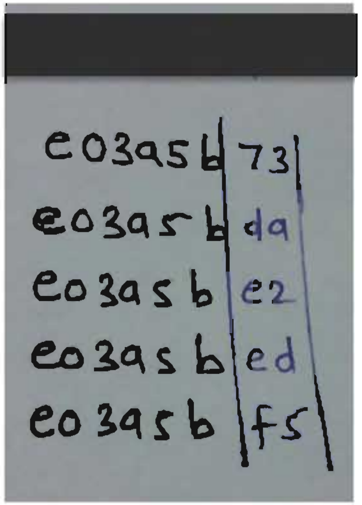
- Smart Paging
  - ✓ Directed onto a small cell rather than a tracking area
  - ✓ Allows attacker to locate LTE subscriber in a cell

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

- MME issues



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



[redacted]

e03a5b	73
e03a5b	da
e03a5b	e2
e03a5b	ed
e03a5b	f5

Building 4G fake base station and attack demos

Ethical Consideration

Experiment Set-up

Set-up cost - little over 1000 Euro!

- Hardware – USRP, LTE dongle, LTE phones
- Software - OpenLTE & srsLTE
- Implementation – passive, semi-passive, active

Thanks to OpenLTE and srsLTE folks!

Location Leak Attacks

Exploit specification/implementation flaws in RRC protocol!

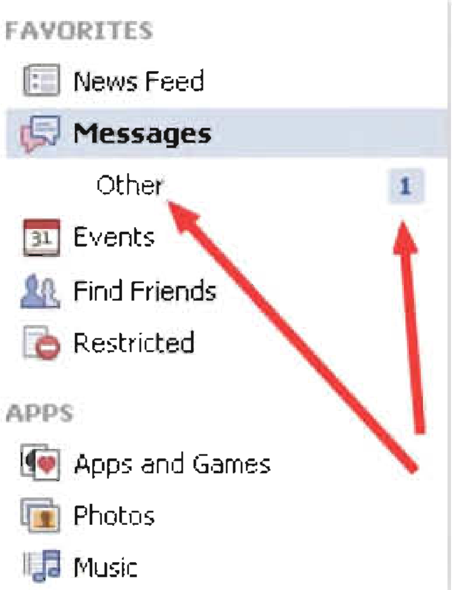
- Passive : link locations over time
  - ✓ Sniff IMSI/GUTIs at a location (e.g., Airport/home/office)
  - ✓ Track subscriber movements (same GUTI for several days)

Demo

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

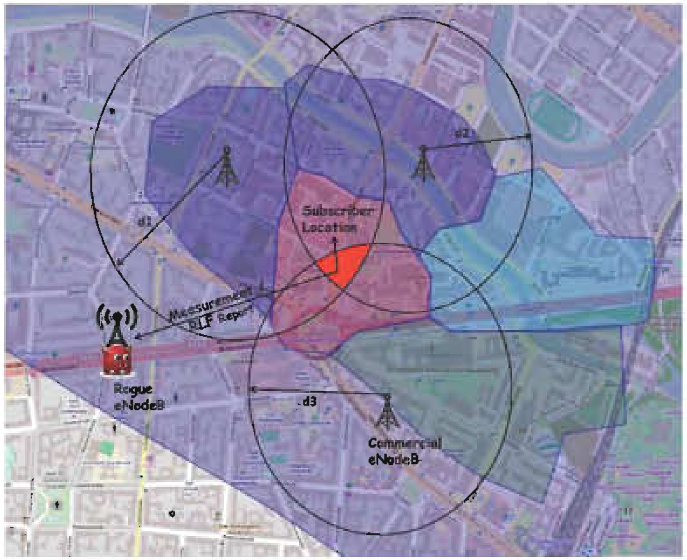


Demo

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

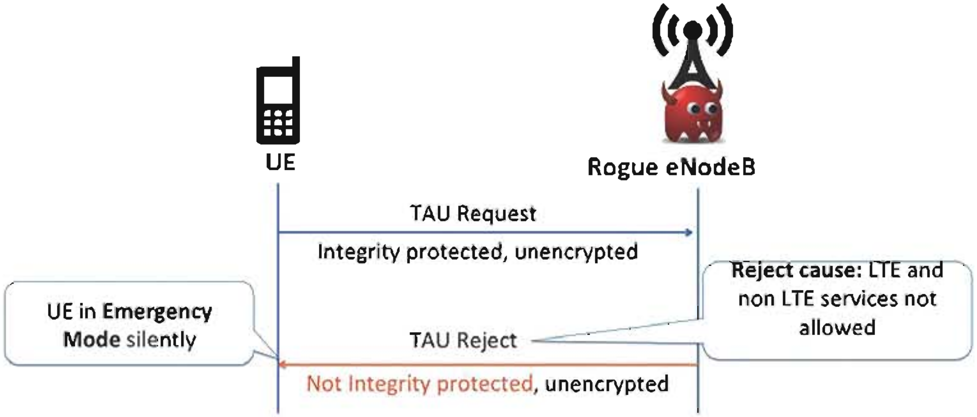


Demo

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


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

Demo

Summary

- New vulnerabilities in LTE standards/chipsets
- Social applications used for silent tracking
- Locating 4G devices using trialternation , GPS co-ordinates!
- DoS attacks are persistent & silent to users
- Configuration issues in deployed LTE networks

Solution!

Use any old Nokia phone without battery and SIM card!

Impact

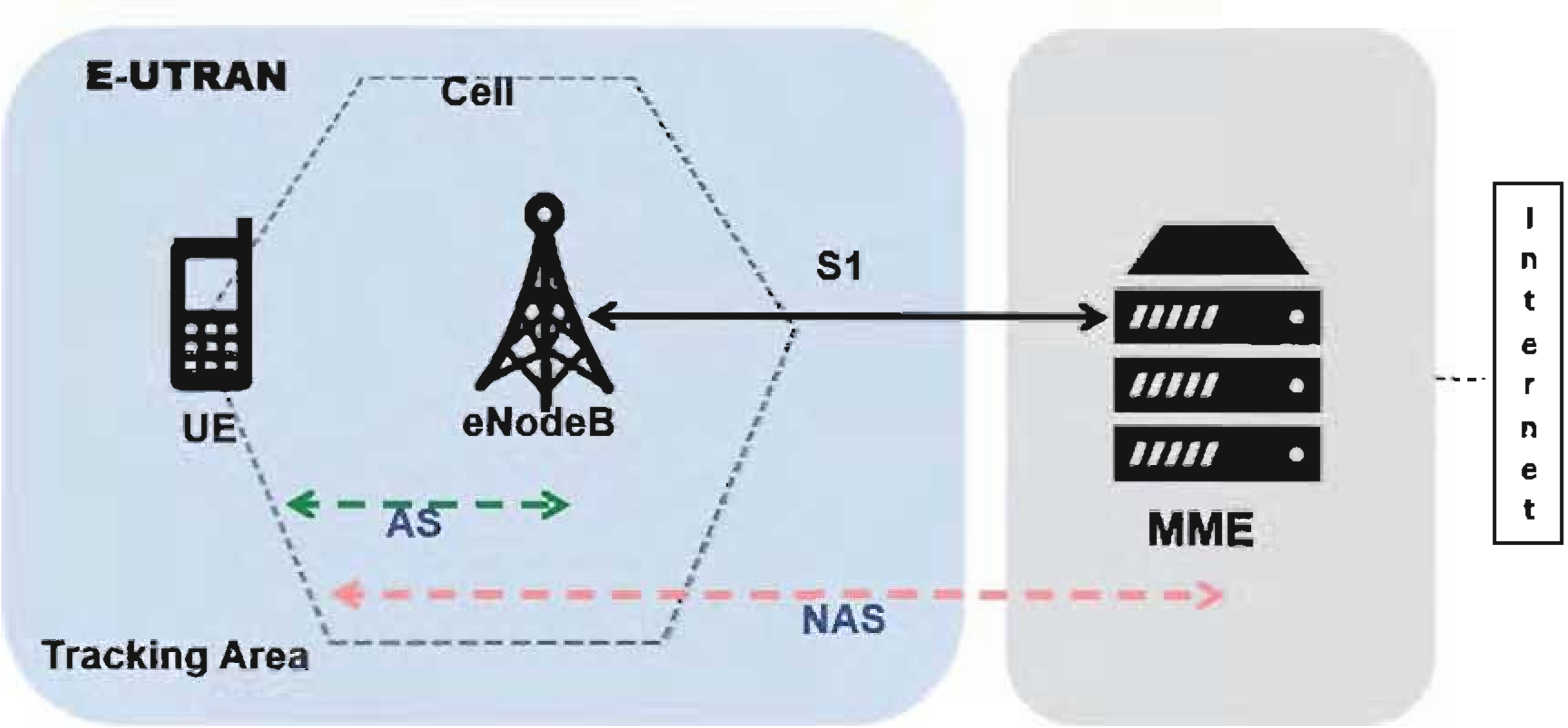
Specification vulnerabilities affect every LTE-enabled device!

- Implementation issues are (almost) fixed by baseband chip manufacturers ☺
- 3GPP/GSMA working on fixes
- However no updates from handset manufacturers yet ☹
- No response yet from MediaTek & Samsung ☹
- Mobile network operators (Germany) fixing their network configuration issues; others may affected as well ☹

Thanks

Questions?

LTE Architecture



AS : Access Stratum
NAS : Non-Access Stratum
E-UTRAN: Evolved Universal Terrestrial Access Network

UE: User Equipment
S1 : Interface
MME : Mobility Management Entity