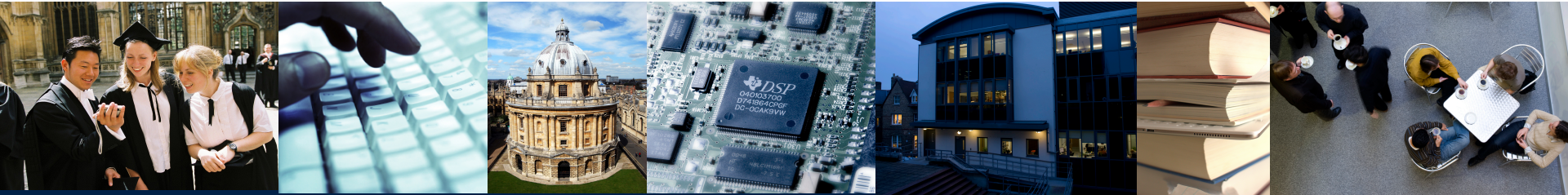




DEPARTMENT OF
**COMPUTER
SCIENCE**



Don't connect to my 4G base station: investigating info leaks in 4G basebands

Ravishankar Borgaonkar, Oxford University
Altaf Shaik, TU Berlin

TelcoSecDay Troopers 2016

15 March 2016

Outline

- Research Motivation
- 4G/LTE security
- Experiment setup
- Vulnerabilities
- Attack examples
- Conclusion

Motivation

- Location of mobile equipment over-the-air (GPS coordinates)
 - Passive and active attack
 - Like in GSM & UMTS – RRLP, diagnostic reports, etc
 - LPP (LTE Positioning Protocol)
- IMSI catcher (tracking)
 - When user is using only data connection
 - CSFB

RRLP – Radio Resource Location Protocol
CSFB – Circuit Switched Fallback

How to do..

- Read the big set of 3GPP documents
 - Informative documents but difficult :/
 - Wish there is an easy way to track changes in every release
- Build some infrastructure to analyze over-the-air protocol messages
 - Implementation issues baseband?
 - Confidence booster – eye brow raising bug!

**CONNEXION LTE SANS CONTRÔLE D'INTÉGRITÉ
(MODE EIAO)**
ATTACHEMENT D'UN MOBILE À UN FAUX RÉSEAU LTE

- Demand for network false:
 - reuse the previous authentication vector
 - use EEA0 modes (without encryption) and EIA0 (without integrity check)

LTE/4G

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

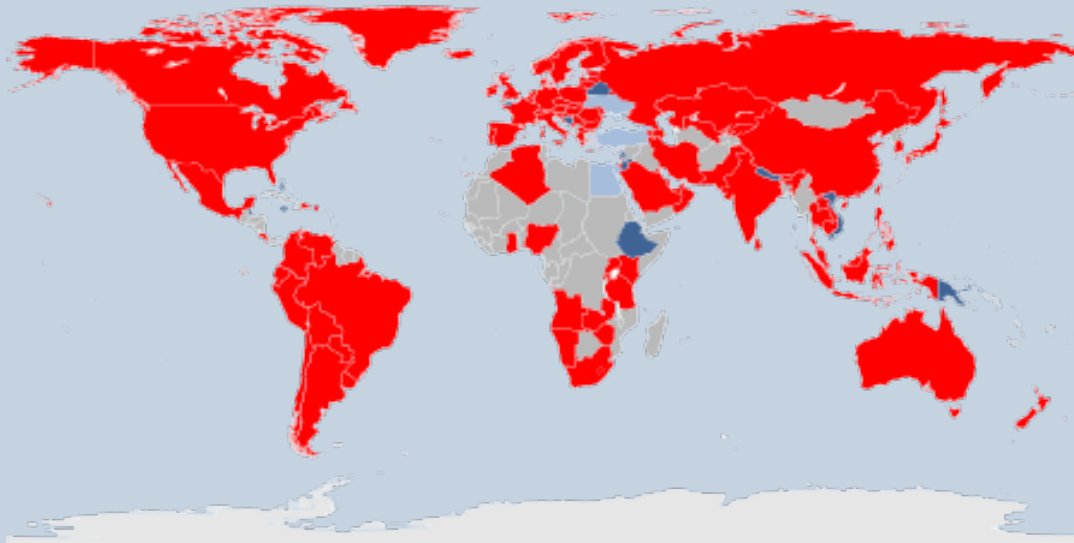
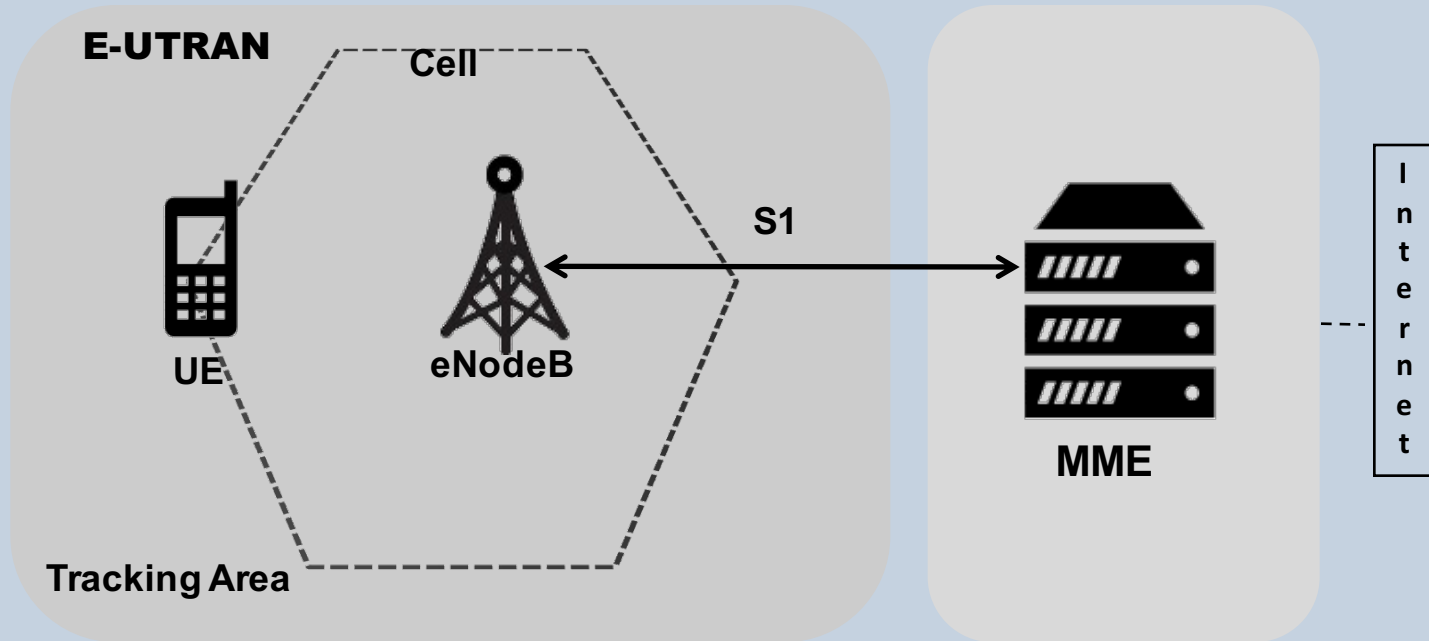


Fig. source: Wikipedia

LTE Architecture



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

UE: User Equipment
S1 : Interface

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



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

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

Looking into specifications

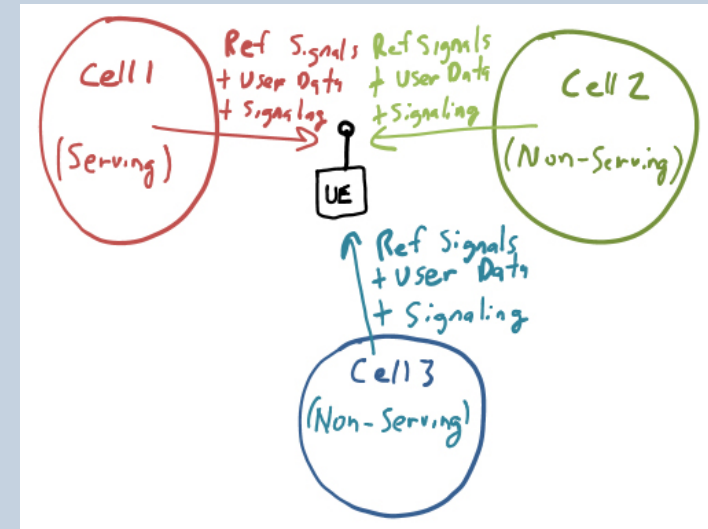


DEPARTMENT OF
**COMPUTER
SCIENCE**



3GPP Specification issues (1)

- RRC protocol – 3GPP TS 36.331
- ‘UE Measurement Report’ messages
- Necessary for handovers & troubleshooting
- No authentication for messages
- Reports not encrypted



MeasurementReport	+	-	-	Justification for case “P”: RAN2 agreed that measurement configuration may be sent prior to security activation
-------------------	---	---	---	---

P...Messages that can be sent (unprotected) prior to security activation

A - I...Messages that can be sent without integrity protection after security activation

A - C...Messages that can be sent unciphered after security activation

3GPP Specification issues (2)

- EMM protocol – 3GPP TS 36.331
- ‘Tracking Area Update Reject’ messages
- Necessary for UE mobility
- No integrity protection for reject messages
- Recovery mechanism not effective

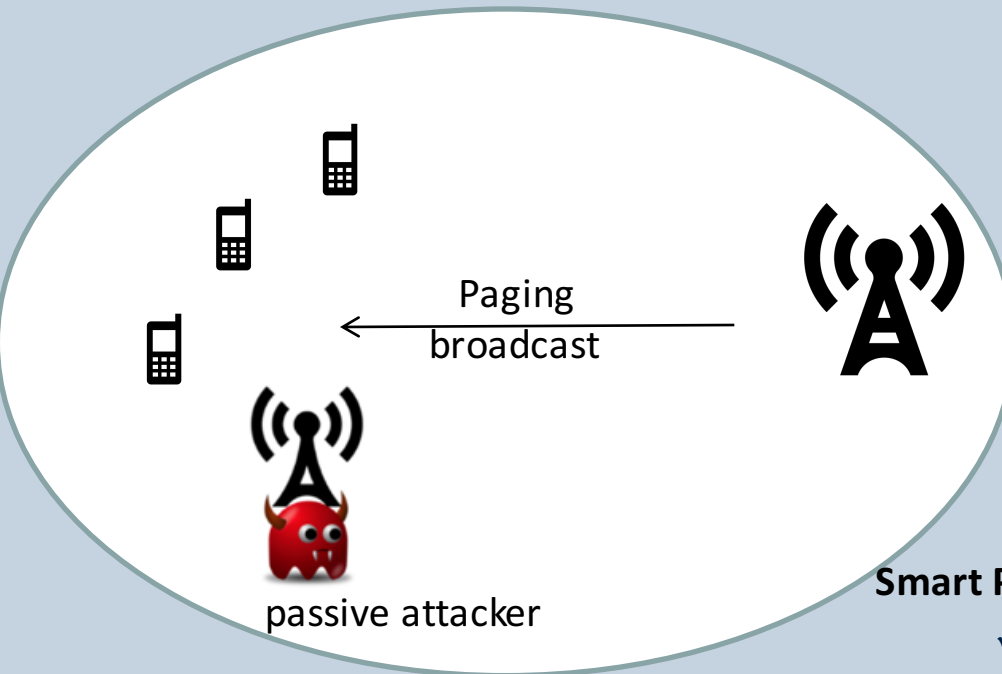
3GPP TS 24.301 version 10.3.0 Release 10

55

ETSI TS 124 301 V10.3.0 (2011-06)

Upon expiry of the timer T3245, the UE shall erase the "forbidden PLMN list", the "forbidden PLMNs for GPRS service" list, and the "forbidden PLMNs for attach in S1mode" list and set the USIM to valid for non-EPS and EPS services.

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

e03a5b	73
e03a5b	da
e03a5b	e2
e03a5b	ed
e03a5b	fs

Smart Paging

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

MME issues

GUTI persistence

- ✓ MNOs don't change GUTI sufficiently & frequently

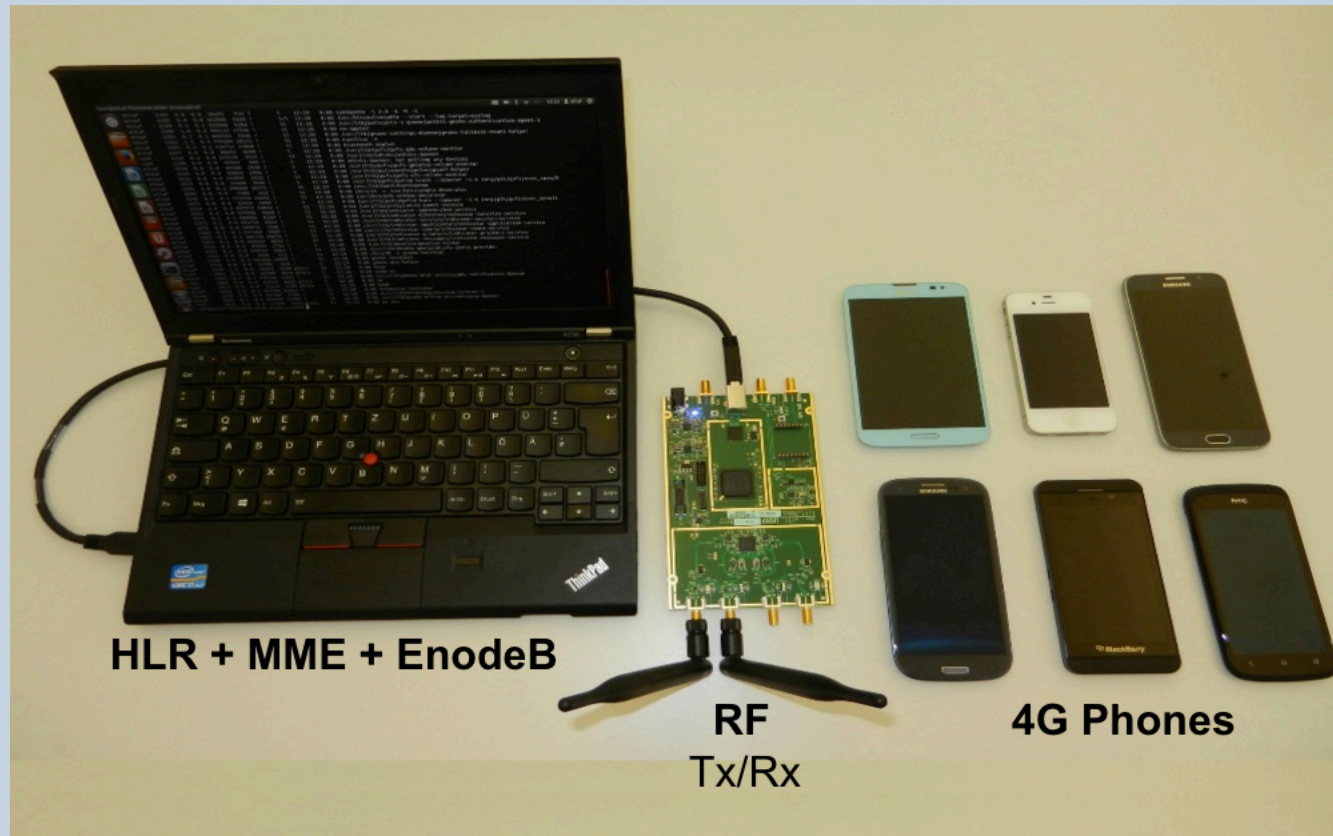
Building minimal functional network

Goal – to be able to communicate with LTE phones and perform AKA

- Open Air LTE interface – Not fully supported
- Amarisoft – expensive for academic research
- **OpenLTE**
- **srsLTE**
- **USRP B210**

<http://www.openairinterface.org/>
<http://amarisoft.com/>

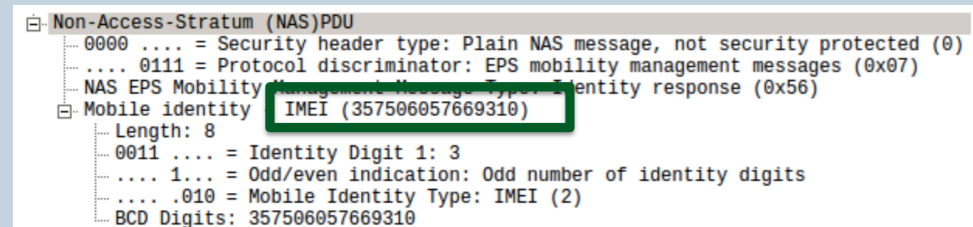
Building minimal functional network



IMEI leak

LTE attempts to prevent IMEI transfer in clear text!

- Device rejects when requested via eNodeB
- But send TAU reject message (cause: 'UE Identity cannot be derived')
- Device deletes existing sessions
- Now ask for IMEI and given 😊
- Popular vendor affected & vulnerability fixed
- However not patched by the OEMs yet ☹️

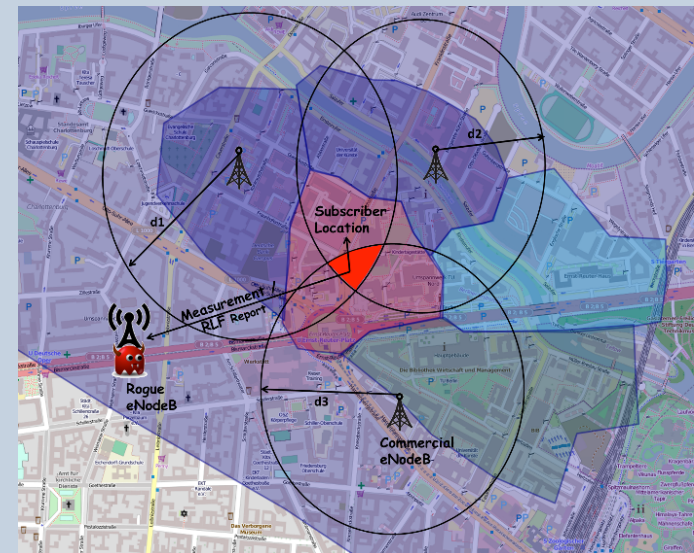


```
Non-Access-Stratum (NAS)PDU
  0000 .... = Security header type: Plain NAS message, not security protected (0)
  .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
  NAS EPS Mobility Management Message Type: Identity response (0x56)
  Mobile identity
    Length: 8
    0011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

Fine-grained location leak

Precise location using trilateration or GPS !

- RLF report
 - ✓ Two rogue eNodeBs for RLF
 - ✓ eNodeB1 triggers RL failure: disconnects mobile
 - ✓ eNodeB2 then requests RLF report from mobile
- Almost all baseband vendors affected
- But no GPS co-ordinates (optional feature)




RLF report contains

```
└─ LTE Radio Resource Control (RRC) protocol
  └─ UL-DCCH-Message
    └─ message: c1 (0)
      └─ c1: ueInformationResponse-r9 (11)
        └─ ueInformationResponse-r9
          └─ rrc-TransactionIdentifier: 0
            └─ criticalExtensions: c1 (0)
              └─ c1: ueInformationResponse-r9 (0)
                └─ ueInformationResponse-r9
                  └─ rlf-Report-r9
                    └─ measResultLastServCell-r9
                      └─ rsrpResult-r9: -78dBm <= RSRP < -77dBm (63)
                        └─ rsrqResult-r9: -3dB <= RSRQ (34)
                    └─ measResultNeighCells-r9
                      └─ measResultListEUTRA-r9: 1 item
                        └─ Item 0
                          └─ MeasResult2EUTRA-r9
                            └─ carrierFreq-r9: 1300
                              └─ measResultList-r9: 1 item
                                └─ Item 0
                                  └─ MeasResultEUTRA
                                    └─ physCellId: 28
                                      └─ measResult
                                        └─ rsrpResult: -102dBm <= RSRP < -101dBm (39)
                                          └─ rsrqResult: RSRQ < -19.5dB (0)
                    └─ failedPCellId-r10: pci-arfcn-r10 (1)
                      └─ pci-arfcn-r10
                        └─ physCellId-r10: 101
                          └─ carrierFreq-r10: 1300
                        └─ connectionFailureType-r10: rlf (0)
```

Fine-grained location leak..

Results finally 😊 😊 😊

```
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]
```



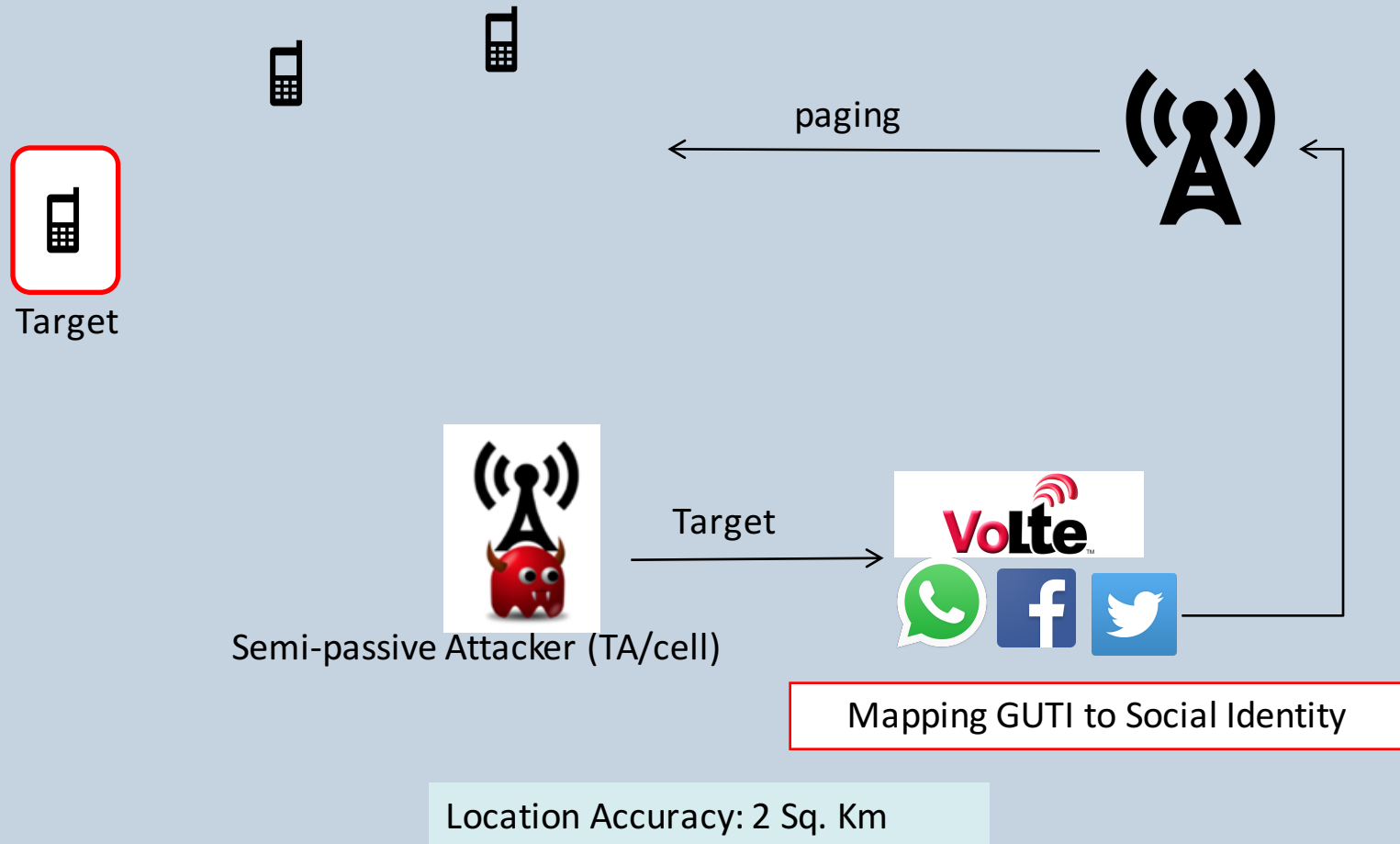
Attack Examples



DEPARTMENT OF
**COMPUTER
SCIENCE**



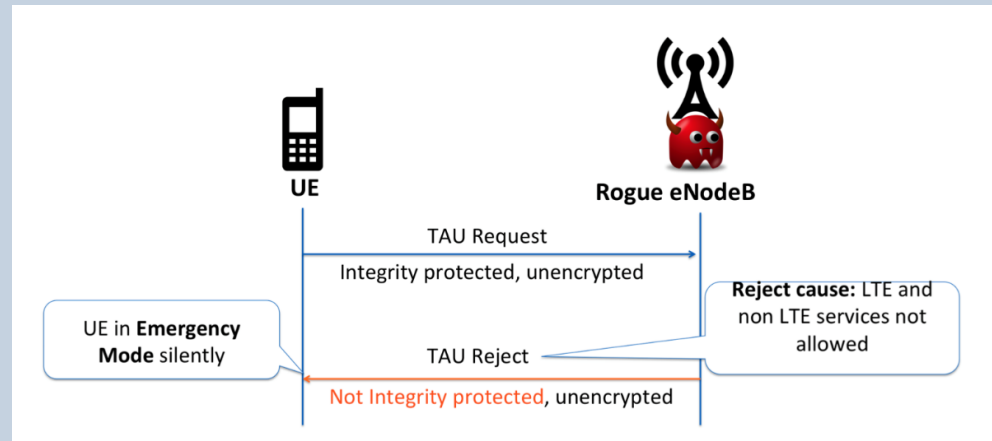
Location Leaks: tracking subscriber coarse level



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 being 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