ON LOW-COST PRIVACY EXPOSURE ATTACKS IN LTE MOBILE COMMUNICATION

Ruxandra F. Olimid*,** and Stig F. Mjølsnes*

* Dept. of Information Security and Communication Technology, NTNU, Norway

** Dept. of Computer Science, University of Bucharest, Romania

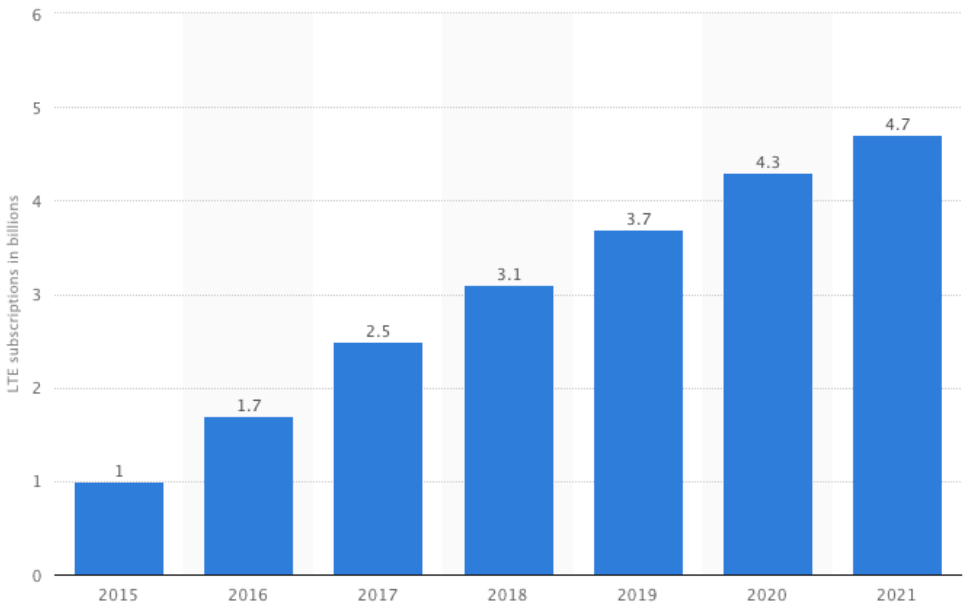
Norwegian University of Science and Technology

RCD 2017

Bucharest, September 18

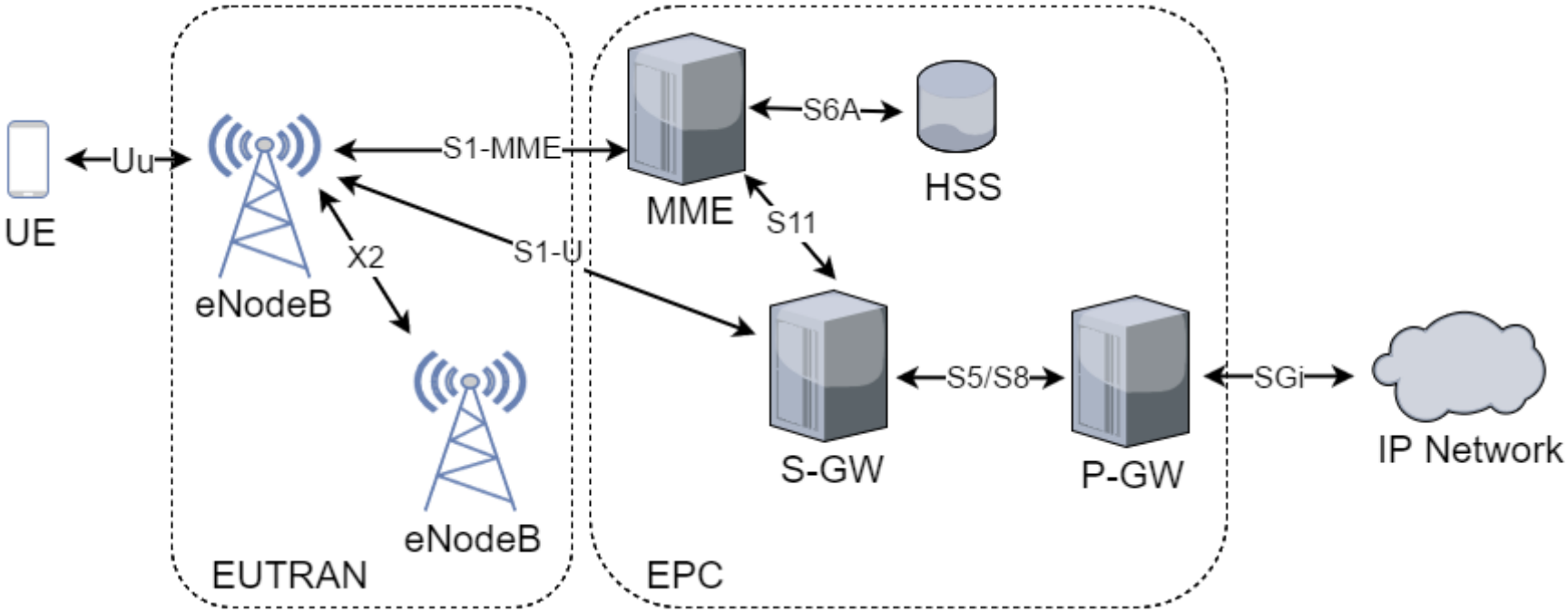
Motivation

Number of LTE subscriptions worldwide from 2015 to 2021 (in billions)*



[https://www.statista.com/statistics/206615/forecast-of-the-number-of-global-hspa-lte-subscriptions-up-to-2014]

LTE - Architecture



LTE - Identification

User side (UE):

- SIM (2G), USIM(3G/4G)
- Stores subscriber permanent ID (IMSI) and private keys

Network side (HSS):

- Stores identification and authentication parameters of the subscribers

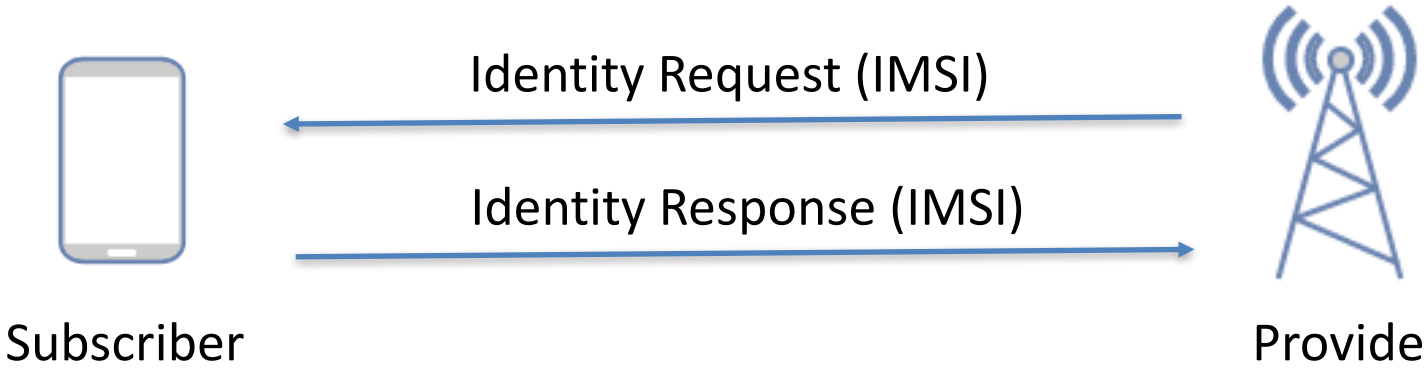
IMSI (International Mobile Subscriber Identity)

MCC (Mobile Country Code)	**MNC** (Mobile Network Code)	**MSIN** (Mobile Subscriber Identification Number)

Identifiers & Parameters

User Equipment	**IMSI**	International Mobile Subscriber Identity
	IMEI	International Mobile Equipment Identifier
	IMEISV	IMEI Software Version
	TMSI **GUTI** **GUMMEI**	Temporary Mobile Subscriber Identity Globally Unique Temporary Identity Globally Unique Mobility Management Entity Identifier
	K	The shared cryptographic key
Network Operator	**MCC**	Mobile Country Code
	MNC	Mobile Network Code
	TAC	Tracking Area Code
	EARFCN	EUTRA Absolute Radio-Frequency Channel Number

Motivation



[. . .] requests the user to send its permanent identity. The user's response contains the IMSI in cleartext. This represents ***a breach in the provision of user identity confidentiality****.*

[ETSI TS 133 401 V10.3.0 (2012-07)]

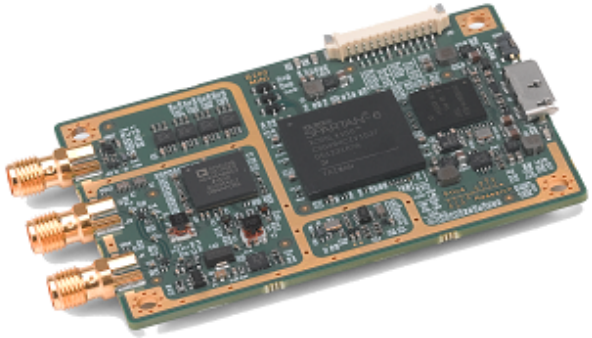
Our contribution

Question: *What is the effect of identities and parameters **leakage** in LTE mobile communication systems w.r.t. **security and privacy** of the subscribers?*

2 scenarios:

1. Physical access to the user equipment
   - apps, built-in codes
2. Attack the radio link
   - passive & active attacks

Tools: **Hardware**



- Software radio peripherals (USRPs)
  - **Ettus B200mini** + antennas
  - **HackRF One** + antenna

[https://www.ettus.com/product/details/USRP-B200mini]

- Computers
  - Standard desktops or laptops: Intel NUC D54250WYK (i5-4250U CPU@1,30GHz), Lenovo ThinkPad T460s (i7-6600U CPU@2,30GHz)

[https://greatscottgadgets.com/hackrf/]

- Mobile phones:
  - LG Nexus 5 Android v6.0.1
  - LG Nexus 5X Android v7.0
- SIM cards:
  - mobile operators in Norway and Romania

Tools: **Software**

- LTE Emulators and tools:
  - **Open Air Interface (OAI),** an open source software that provides a (partially) standard compliant implementation of LTE

    [http://www.openairinterface.org/]
  - **LTE Cell Scanner and Tracker**

    [https://github.com/0x90/sdr-arsenal/tree/master/LTE-Cell-Scanner]

- Mobile phones:
  - Service Mode, built-in codes for mobile devices
  - Apps

Table 1: Applications

Application	Author
SIM Reader	Jaemin Kim
SIM Card Info	Harry Gonzalez
SIM Card Information and IMEI	Trusted App Developers, Inc.
G-NetTrack Lite	GyokovSolutions
LTE Discovery	Simply Advanced

Physical Access to the UE

Table 2: Information Disclosure - User Equipment

Handset	Operation System	IMSI	IMEI	IMEISV
Nexus 5	Android v6.0.1	-	Phone Status Menu	Phone Status Menu
		-	*#*#4636#*#*	-
		-	*#06#	-
		SIM Reader	SIM Reader	SIM Reader
		SIM Card Info	SIM Card Info	SIM Card Info
		SIM Card Information and IMEI	SIM Card Information and IMEI	-
Nexus 5X	Android v7.0	-	Phone Status Menu	Phone Status Menu
		-	*#*#4636#*#*	-
		-	*#06#	-
		SIM Reader	SIM Reader	SIM Reader
		SIM Card Info	SIM Card Info	SIM Card Info
		SIM Card Information and IMEI	SIM Card Information and IMEI	-

Table 3: Information Disclosure - Network Operator

Handset	Operation System	MCC	MNC	TAC	EARFCN
Nexus 5	Android v6.0.1	*#*#4636#*#*	*#*#4636#*#*	*#*#4636#*#*	-
		G-NetTrack Lite	G-NetTrack Lite	G-NetTrack Lite	-
		LTE Discovery	LTE Discovery	LTE Discovery	
Nexus 5X	Android v7.0	*#*#4636#*#*	*#*#4636#*#*	*#*#4636#*#*	*#*#4636#*#*
		G-NetTrack Lite	G-NetTrack Lite	G-NetTrack Lite	G-NetTrack Lite
		LTE Discovery	LTE Discovery	LTE Discovery	LTE Discovery

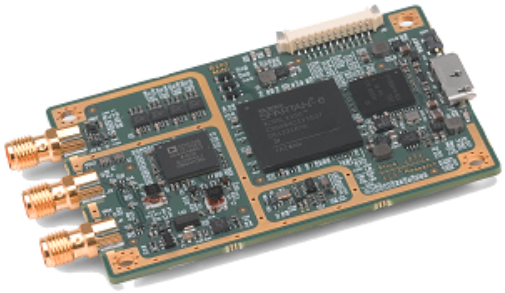
Passive Attacks

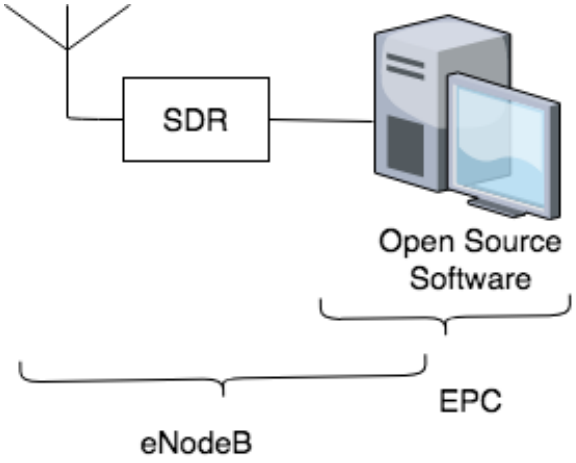

```
<systemInformationBlockType1>
    <cellAccessRelatedInfo>
        <plmn-IdentityList>
            <PLMN-IdentityInfo>
                <plmn-Identity>
                    <mcc>
                        <MCC-MNC-Digit>[redacted]/MCC-MNC-Digit>
                        <MCC-MNC-Digit>[redacted]/MCC-MNC-Digit>
                        <MCC-MNC-Digit>[redacted]/MCC-MNC-Digit>
                    </mcc>
                    <mnc>
                        <MCC-MNC-Digit>[redacted]/MCC-MNC-Digit>
                        <MCC-MNC-Digit>[redacted]/MCC-MNC-Digit>
                    </mnc>
                </plmn-Identity>
                <cellReservedForOperatorUse><notReserved/></cellRes
            </PLMN-IdentityInfo>
        </plmn-IdentityList>
        <trackingAreaCode>
            [redacted]
        </trackingAreaCode>
        <cellIdentity>
            [redacted]
        </cellIdentity>
        <cellBarred><notBarred/></cellBarred>
        <intraFreqReselection><allowed/></intraFreqReselection>
        <csg-Indication><false/></csg-Indication>
    </cellAccessRelatedInfo>
    <cellSelectionInfo>
        <q-RxLevMin>[redacted]</q-RxLevMin>
    </cellSelectionInfo>
```

```
<sib5>
    <interFreqCarrierFreqList>
        <InterFreqCarrierFreqInfo>
            <dl-CarrierFreq>[redacted]</dl-CarrierFreq>
            <q-RxLevMin>[redacted]/q-RxLevMin>
            <t-ReselectionEUTRA>1</t-ReselectionEUTRA>
            <threshX-High>6</threshX-High>
            <threshX-Low>6</threshX-Low>
            <allowedMeasBandwidth><mbw100/></allowedMeasBandwidth>
            <presenceAntennaPort1><false/></presenceAntennaPort1>
            <cellReselectionPriority>6</cellReselectionPriority>
            <neighCellConfig>
                01
            </neighCellConfig>
            <q-OffsetFreq><dB0/></q-OffsetFreq>
        </InterFreqCarrierFreqInfo>
        <InterFreqCarrierFreqInfo>
            <dl-CarrierFreq>[redacted]</dl-CarrierFreq>
            <q-RxLevMin>[redacted]/q-RxLevMin>
            <t-ReselectionEUTRA>1</t-ReselectionEUTRA>
```

Interception and decoding of SIB messages

Active Attacks





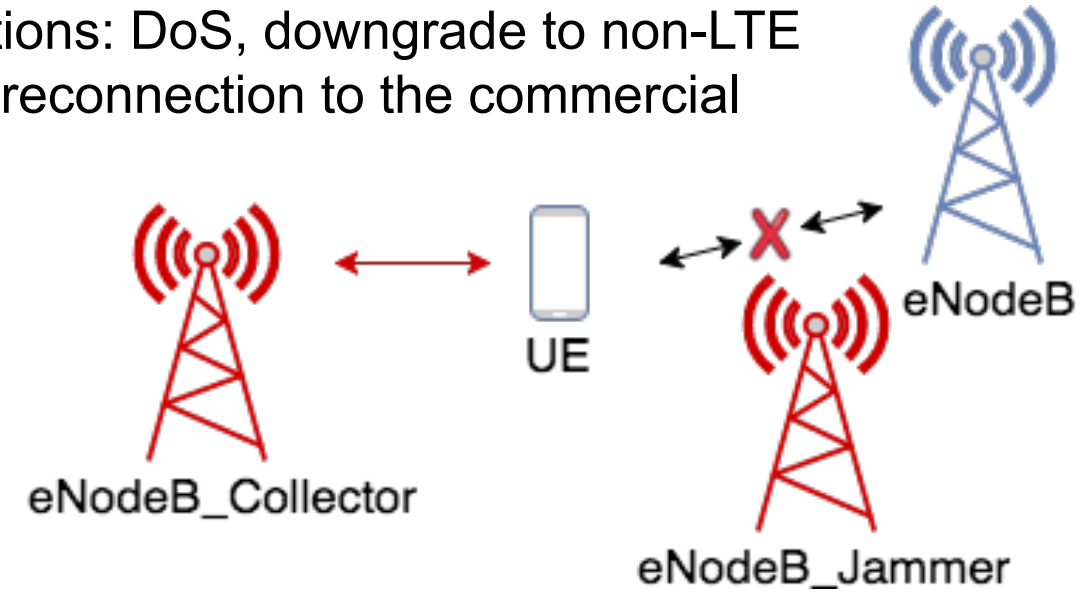

```
110 SACK id-downlinkNASTransport, Identity request
146 SACK id-uplinkNASTransport, Identity response
182 id-initialUEMessage, Tracking area update request
110 SACK id-downlinkNASTransport, Tracking area update reject
 94 id-downlinkNASTransport, EMM status
214 id-initialUEMessage, Attach request, PDN connectivity request
```

```
NAS-PDU: 17f49d7386090756082924505902830303
Non-Access-Stratum (NAS)PDU
    0001 .... = Security header type: Integrity protected (1)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    Message authentication code: 0xf49d7386
    Sequence number: 9
    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 - IMSI [redacted]
```

LTE IMSI Catchers

Our LTE IMSI Catcher

- We have built an **IMSI Catcher**:
  - Low-cost (< 3000 EUR)
  - ”Commercial of the shelf” hardware and readily available software only
  - No (or basic) changes in the source code
  - Different implementations: DoS, downgrade to non-LTE networks, immediate reconnection to the commercial network



* Results published in 2 previous papers: MMM-ACNS’17 and Secrypt’17

Thank you!