NTNU

Experimental Assessment of Private Information Disclosure in LTE Mobile Networks

Stig F. Mjølsnes and Ruxandra F. Olimid

Department of Information Security and Communication Technology,
NTNU - Norwegian University of Science and Technology

Passive Attacks

Tools

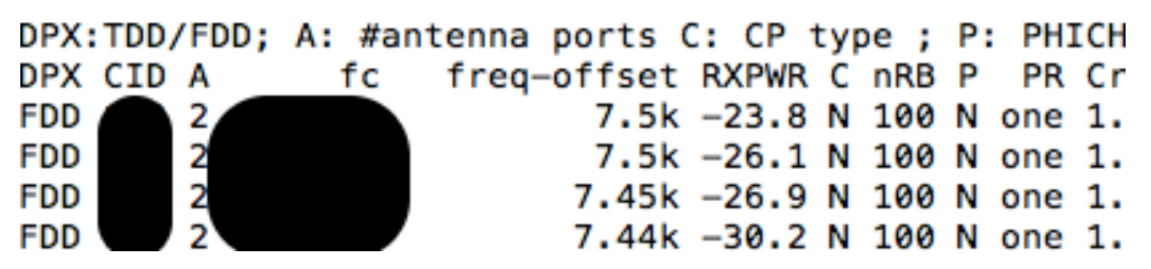
- Hardware: *Hack RF One* [1]
- Software: *LTE Cell Scanner and Tracker* [2]

Figure 2. HackRF One [1]

Results

We sniffed the radio interface and intercepted parameters of a commercial mobile network in the Trondheim NTNU campus area:

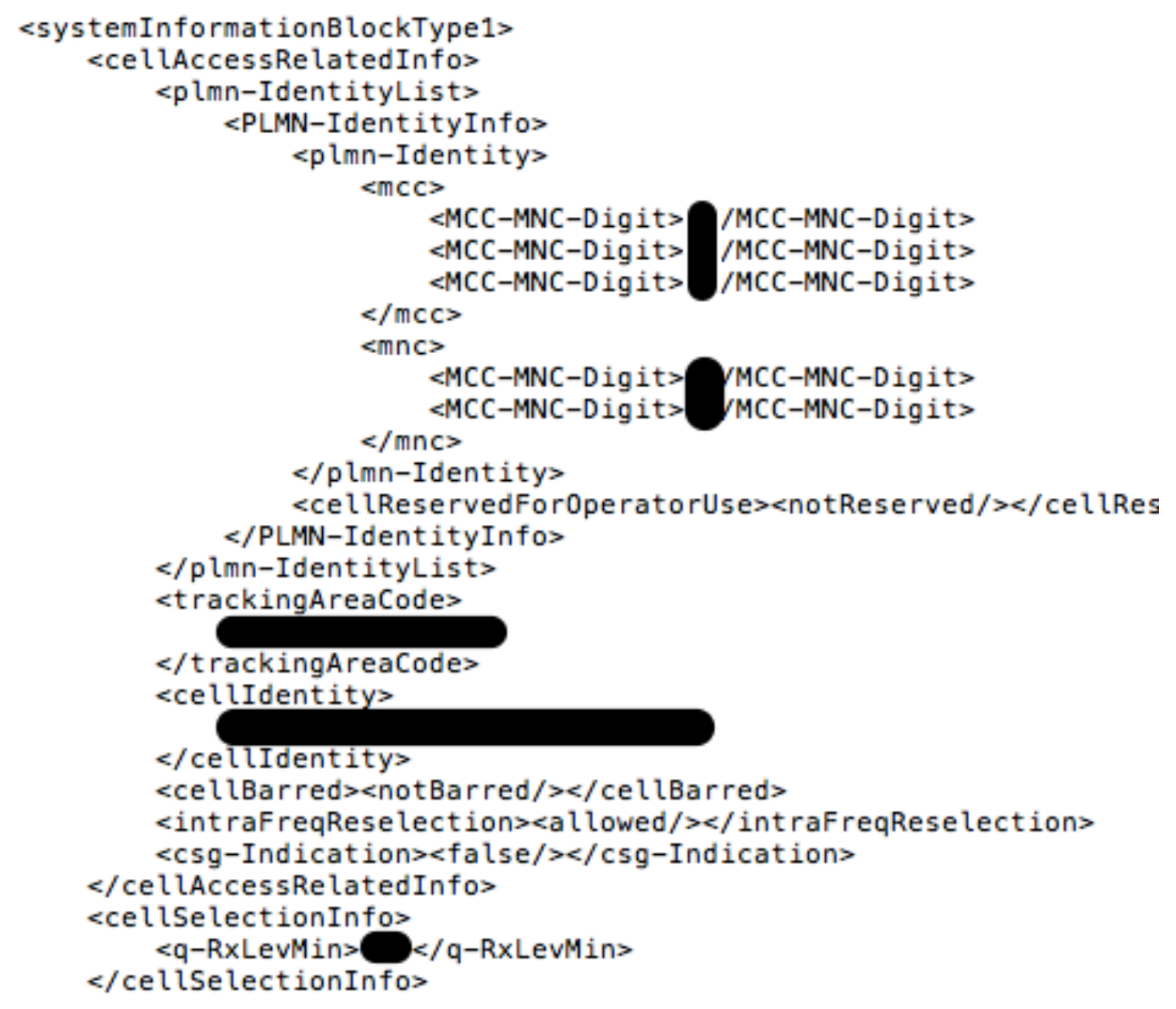
- Figure 3 shows an example of cell search on a given frequency, listing cells that correspond to commercial eNodeBs in the area



```
DPX:TDD/FDD; A: #antenna ports C: CP type ; P: PHICH
DPX CID A       fc    freq-offset RXPWR C nRB P  PR Cr
FDD [redacted] 2 [redacted]   7.5k -23.8 N 100 N one 1.
FDD            2              7.5k -26.1 N 100 N one 1.
FDD            2             7.45k -26.9 N 100 N one 1.
FDD            2             7.44k -30.2 N 100 N one 1.
```

Figure 3. Commercial LTE Cells

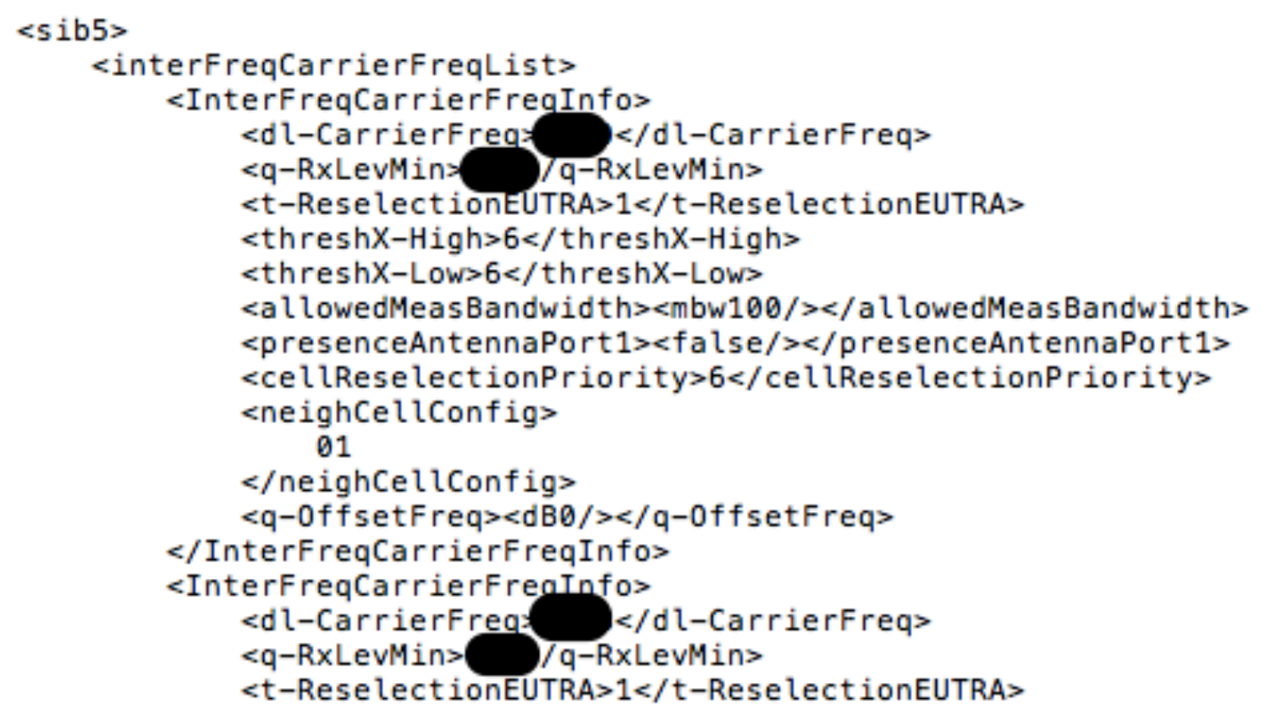
- Figure 4 shows a successfully decoded SIB1 (System Information Block 1) message. Notice the network identification parameters MCC (Mobile Country Code) and MNC (Mobile Network Code), the location area identifier and the cell identity. The cell is not barred and allows intra frequency reselection



```
<systemInformationBlockType1>
    <cellAccessRelatedInfo>
        <plmn-IdentityList>
            <PLMN-IdentityInfo>
                <plmn-Identity>
                    <mcc>
                        <MCC-MNC-Digit>[redacted]/MCC-MNC-Digit>
                        <MCC-MNC-Digit>          /MCC-MNC-Digit>
                        <MCC-MNC-Digit>          /MCC-MNC-Digit>
                    </mcc>
                    <mnc>
                        <MCC-MNC-Digit>[redacted]/MCC-MNC-Digit>
                        <MCC-MNC-Digit>          /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>
```

Figure 4. Real capture of SIB1 (fragment)

- Figure 5 shows a successfully decoded SIB5 (System Information Block 5) message. Notice the frequencies used in the area and their associated priorities



```
<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>
```

Figure 5. Real capture of SIB5 (fragment)

Abstract

*Open source software running on SDR (Software Defined Radio) devices now allow building a full-fledged mobile network at low cost. These novel tools open up for exciting possibilities to analyse and verify by experiments the behaviour of existing and emerging mobile networks in new lab environments, for instance at universities. We use **SDR equipment** and **open source software** to analyse the feasibility of **disclosing private information** that is sent over the LTE access network. We verify by experiments that **identity information** can be obtained both **passively,** by listening on the radio link**, and actively,** by running considerable low detectable rogue base stations to impersonate the commercial network. Moreover, we implement a **downgrade attack** (to non-LTE networks) with minimal changes to the open source software.*

Motivation & Contribution

- Disclosure of sensitive information in mobile networks has important consequences for both the privacy of subscribers and the security of commercial services
- New tools have opened up the possibility to analyse by experiment the behaviour of all generations of cellular networks
- We investigate, by experiment, information disclosure in LTE in 2 scenarios: ***passive attacks*** and ***active attacks***

Experimental Setup

General setup: computers running open source software, attached with SDR (Software Defined Radio) devices and antennas

- Computers: Intel NUC D54250WYK (i5-4250U CPU@1.30GHz) andLenovo ThinkPad T460s (i7-6600U CPU@ 2,30GHz), running 64-bit Kubuntu 14.04 kernel v.3.19.0-61-low latency
- Handsets: Nexus 5 (Android v6.0.1) and Nexus 5X (Android v7.0)

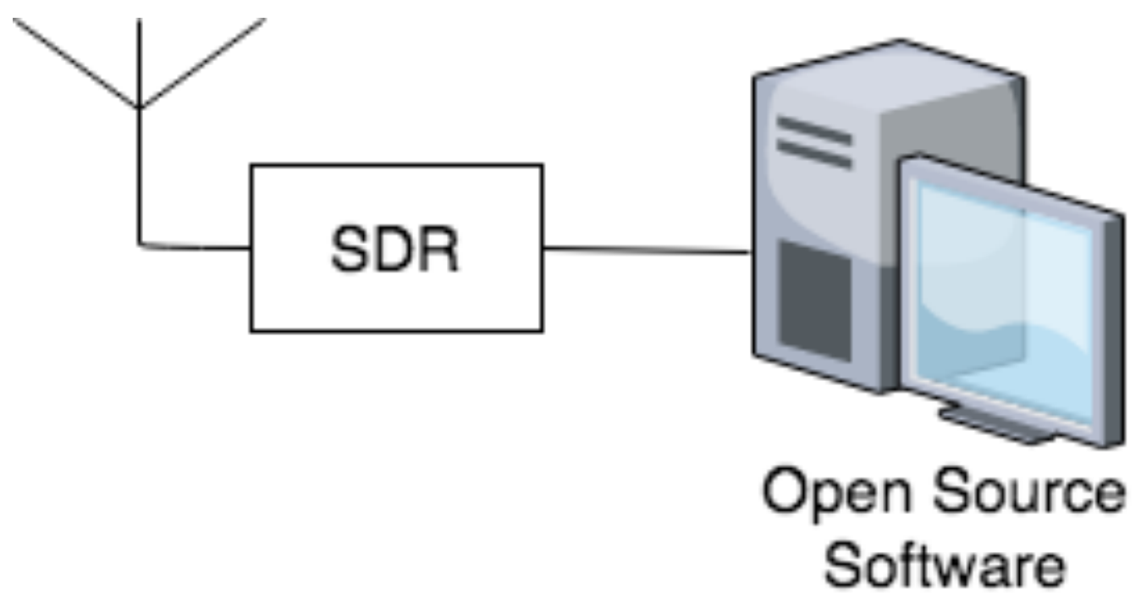


Figure 1. Experimental Architecture using SDR

Acknowledgements

The authors would like to thank post doc David Palma at our department for providing some of the equipment necessary for the experiments and master students Christoffer E.Ottesen and Christian Sørseth for their help with some of the experiments.

Active Attacks

Tools

- Hardware: *USRP B200 mini* [3]
- Software: *Open Air Interface (OAI)* [4]

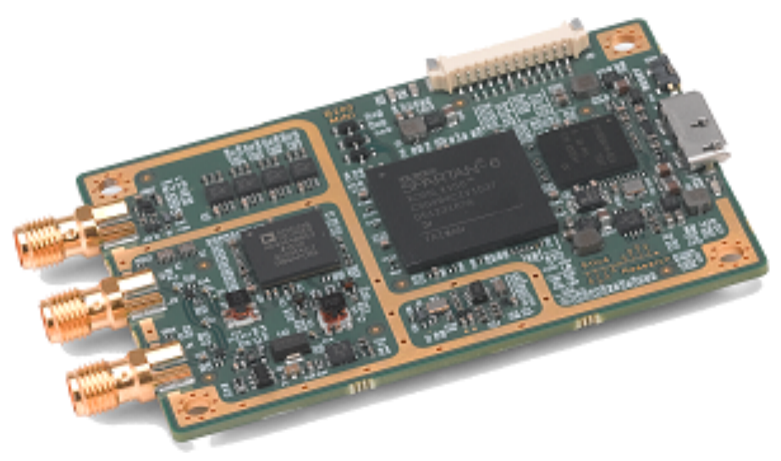
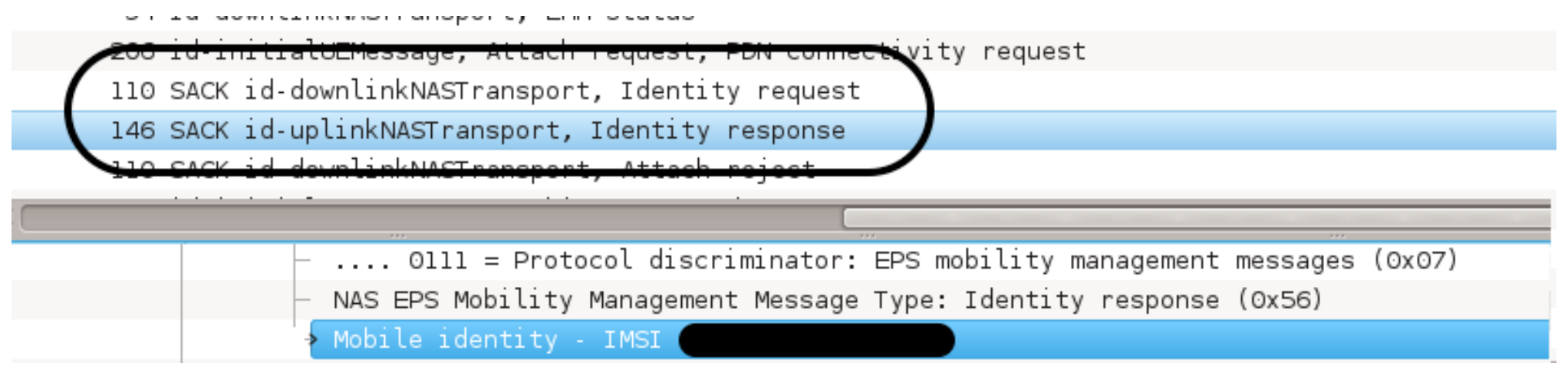


Figure 6. B200mini [3]

Results

We built an IMSI Catcher that collects subscribers' identifiers (IMSI) in the area of NTNU and then makes the phone reconnect to the commercial network in 2 ways:

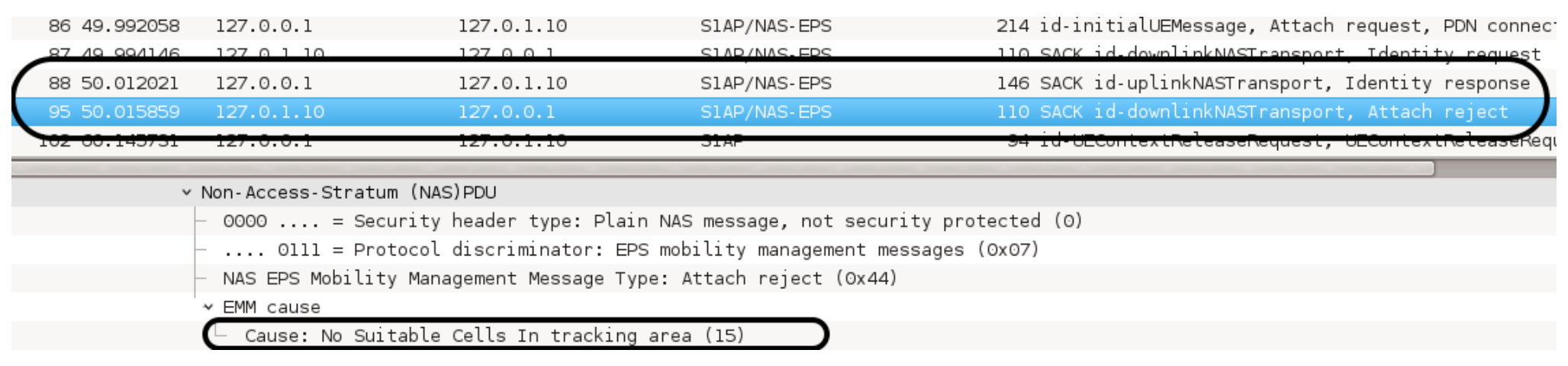
- Figure 7 exemplifies an `Identity Response` message (displayed in Wireshark) that contains the IMSI as a response of an `Identity Request` (based on our previous results in [5])



```
200 id-initialUEMessage, Attach request, PDN connectivity request
110 SACK id-downlinkNASTransport, Identity request
146 SACK id-uplinkNASTransport, Identity response
110 SACK id-downlinkNASTransport, Attach reject

    .... 0111 = Protocol discriminator: EPS mobility management messages (0x07)
    NAS EPS Mobility Management Message Type: Identity response (0x56)
  > Mobile identity - IMSI [redacted]
```

Figure 7. IMSI Capture

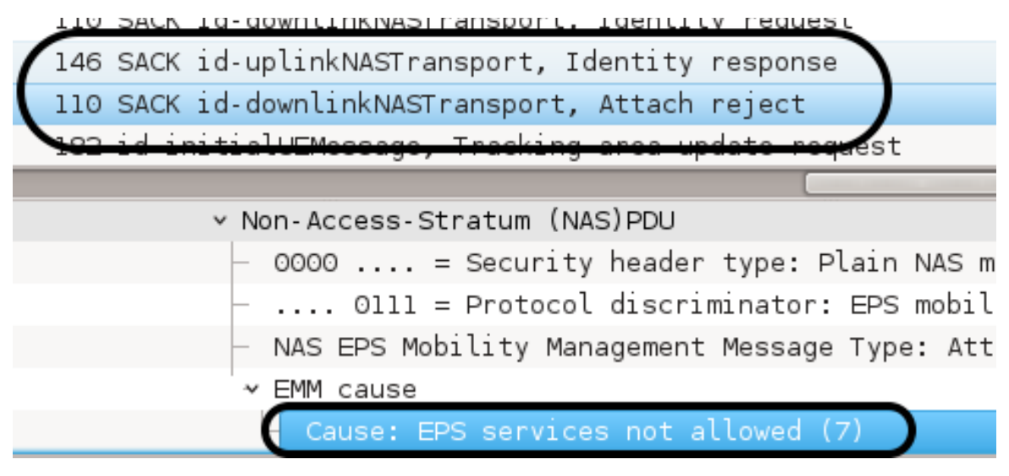


```
 86 49.992058  127.0.0.1    127.0.1.10   S1AP/NAS-EPS   214 id-initialUEMessage, Attach request, PDN connec
 87 49.994146  127.0.1.10   127.0.0.1    S1AP/NAS-EPS   110 SACK id-downlinkNASTransport, Identity request
 88 50.012021  127.0.0.1    127.0.1.10   S1AP/NAS-EPS   146 SACK id-uplinkNASTransport, Identity response
 95 50.015859  127.0.1.10   127.0.0.1    S1AP/NAS-EPS   110 SACK id-downlinkNASTransport, Attach reject
102 60.145731  127.0.0.1    127.0.1.10   S1AP            94 id-UEContextReleaseRequest, UEContextReleaseRequ

 v 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: Attach reject (0x44)
  v EMM cause
      Cause: No Suitable Cells In tracking area (15)
```

Figure 8. Trigger reconnection to commercial network

- Figures 8 and 9 show the EMM causes that trigger reconnection to the commercial network, respectively downgrade to non-4G services (*downgrade attack*). To obtain the results, we performed minimal changes in the OAI source code.

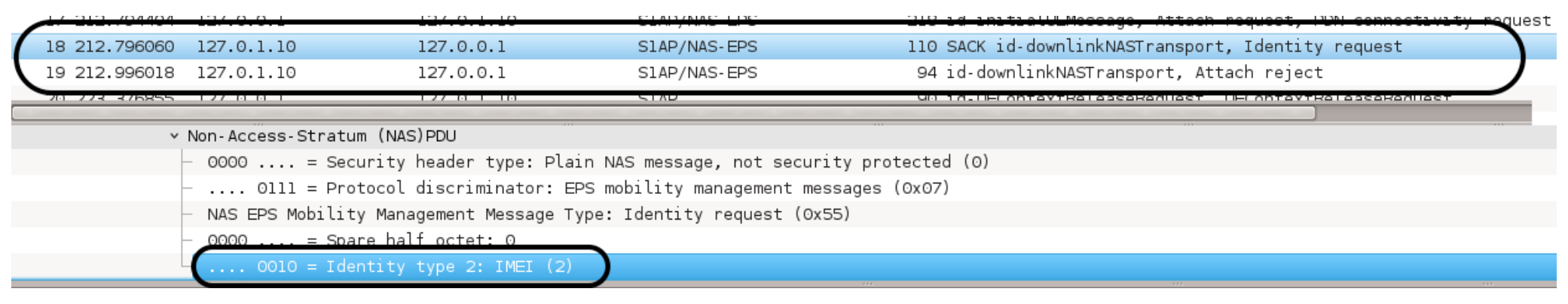


```
110 SACK id-downlinkNASTransport, Identity request
146 SACK id-uplinkNASTransport, Identity response
110 SACK id-downlinkNASTransport, Attach reject
182 id-initialUEMessage, Tracking area update request

 v Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS m
    .... 0111 = Protocol discriminator: EPS mobil
    NAS EPS Mobility Management Message Type: Att
  v EMM cause
      Cause: EPS services not allowed (7)
```

Figure 9. Trigger downgrade to non-LTE services in the commercial network

- Figure 10 exemplifies an IMEI request, followed by the `Attach Reject` message. There is no `Identity Response` message, so both devices that we tested proved to be standard compliant (they do not disclose the IMEI)



```
17 212.794404  127.0.0.1    127.0.1.10   S1AP/NAS-EPS   218 id-initialUEMessage, Attach request, PDN connectivity request
18 212.796060  127.0.1.10   127.0.0.1    S1AP/NAS-EPS   110 SACK id-downlinkNASTransport, Identity request
19 212.996018  127.0.1.10   127.0.0.1    S1AP/NAS-EPS    94 id-downlinkNASTransport, Attach reject
20 223.376855  127.0.0.1    127.0.1.10   S1AP            90 id-UEContextReleaseRequest, UEContextReleaseRequest

 v 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 request (0x55)
    0000 .... = Spare half octet: 0
    .... 0010 = Identity type 2: IMEI (2)
```

Figure 10. Identity Request (IMEI) followed by Attach Reject (no Identity Response)

Contact

Corresponding author: Ruxandra F. Olimid
Dept. of Information Security and Communication Technology
NTNU - Norwegian University of Science and Technology
Email: ruxandra.olimid@ntnu.no

References

[1] Great Scott Gadgets. HackRF One. https://greatscottgadgets.com/hackrf Last accessed: April 2017.
[2] Jiao Xianjun . Cell Scanner and Tracker. https://github.com/JiaoXianjun/LTE-Cell-Scanner Last accessed: April 2017.
[3] Ettus Research. USRP B200mini (Board only). https://www.ettus.com/product/details/USRPB200mini Last accessed: April 2017.
[4] Open Air Interface. 5G software alliance for democratising wireless innovation. http://www.openairinterface.org Last accessed: April 2017.
[5] Mjølsnes, S. F. and Olimid, R. F. *Easy 4G/LTE IMSI Catchers for Non-Programmers*. Accepted for publication at MMM-ACNS 2017.

Acronyms

EMM	EPS Mobility Management
EPS	Evolved Packet System
LTE	Long Term Evolution
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Equipment Identifier
MCC	Mobile Country Code
MNC	Mobile Network Code
OAI	Open Air Interface
SIB	System Information Block
SDR	Software Defined Radio