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, Trondheim, Norway

Keywords: 4G/LTE Security, Mobile Networks Security, IMSI Catcher, Privacy, Software Defined Radio.

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 subscriber 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.

1 INTRODUCTION

Disclosure of sensitive information in mobile communications networks has important consequences for both the privacy of subscribers and the security of commercial services. Although LTE (Long Term Evolution) implements improved mechanisms and protocols that provide better protection than previous generations of mobile networks, nevertheless 4G has turned out susceptible too. LTE was proved directly vulnerable to privacy exposure, location tracking, DoS (Denial of Service), or communication eavesdropping (Jover, 2013; Shaik et al., 2016; Jover, 2016; Lichtman et al., 2016; Rupprecht et al., 2016; The Register, 2016; Mjølsnes and Olimid, 2017).

Open source software running on SDR (Software Defined Radio) devices allow the emulation of mobile networks at low cost. These tools have opened up the possibility to analyse by experiment the behaviour of all generations of cellular networks. Usage of such devices in academia leads to a better understanding of the standards and research results that would have been previously possible in industrial environments only. Making use of available SDR equipment and open source software, we analyse the feasibility of gathering sensitive information exchanged by radio communication in the access network in LTE. Disclosure of private identifiers and parameters is the first step to take advantage of security breaches in 4G. More precisely, the adversary usually first reconnoiters the network operation in the eavesdropped area of attack and then use the gathered information to configure a rogue base station for an active attack that might severely damage the privacy of the user (e.g.: interception of personal communication) or the credibility of the network operator (e.g.: DoS attacks).

1.1 Related Work

Academic works implement IMSI Catchers - active attack devices against the radio link protocols in mobile networks with the main goal of collecting IMSIs - by modifying the code of open-source software projects, such as OpenLTE (OpenLTE, 2017), srsLTE (srsLTE, 2017; Gomez-Miguelez et al., 2016), or gr-LTE (gr-LTE, 2017). We have very recently showed that Open Air Interface (OAI) (Open Air Interface, 2017) can be used to build an out-of-the-box IMSI Catcher (Mjølsnes and Olimid, 2017). The attack requires no changes to the software, making the IMSI Catcher accessible to adversaries with absolutely no programming skills, but only publicly accessible software and COTS (Commercial-out-of-the-Shelf) hardware at an affordable price. Rupprecht et al. have also used OAI, but for another purpose: to test compliance of some UE (User Equipment) with the LTE standard with respect to encryption mechanisms, under the assumption that the UE automatically tries to connect

Mjølsnes, S. and Olimid, R.
Experimental Assessment of Private Information Disclosure in LTE Mobile Networks.
DOI: 10.5220/0006462305070512
In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT*, pages 507-512
ISBN: 978-989-758-259-2

to the rogue base station by re-selection (Rupprecht et al., 2016). New vulnerabilities arise continuously, LTE being a hot topic for top security conferences (Borgaonkar et al., 2017). A theoretical analysis has been conducted to understand the threats in LTE networks (Bhattarai et al., 2014). Some work has been done to detect or mitigate IMSI Catchers, both at the subscriber (Dabrowski et al., 2014) and at the network level (Dabrowski et al., 2016).

1.2 Motivation and Contribution

We investigate, by experiment, information disclosure in LTE, which has important consequences on the privacy of subscribers and the security of commercial networks. We analyse disclosure of sensitive information by both passive and active attacks:

Passive Attacks. We exemplify by experiment how the adversary can sniff parameters that are broadcasted in clear by the commercial network. These data give an overview of the network operation that is valuable in implementing more advanced attacks (e.g.: the list of cells in a given area, the uplink and downlink frequencies used in the area and their associated priority). All experiments were performed in the wireless security lab at the university and the measurements were conducted on commercial mobile networks. To succeed our goals, we used open source software (LTE Cell Tracker) running on SDR device (Hack RF One). We performed minimal changes to the Matlab scripts of the open source software to allow correct decoding of the captured messages. This required basic programming skills, such as reading and understanding the Matlab code. Previous work describes similar passive attacks, but the authors use changes in the software of other LTE tools (Jover, 2016). Our attacks proves how easy it is to gather information about commercial networks, without any specialised hardware or software.

Active Attacks. The out-of-the box IMSI Catcher built by Mjølsnes and Olimid generates a DoS attack (the UE will only allow reconnection to the commercial network after rebooting), which makes the attack easily detectable by the end user (Mjølsnes and Olimid, 2017). We now make the UE reconnect to the commercial network immediately after disclosing the IMSI to the rogue base station. This mitigates the detection of the attack at the subscriber level, because UE loses connectivity for a very short time only. Moreover, we show how to deny LTE services to the subscriber, by performing a downgrade attack to previous generation mobile networks. Both results are obtained with minimal changes in the OAI open source software, running on SDR device (Ettus B200mini). To the best of our knowledge, we are the first to verify by experiment the feasibility of low-detectable IMSI Catchers and downgrade attacks using the OAI open source software. Moreover, in the same experimental settings, we test compliance to standard with respect to IMEI (International Mobile Equipment Identifier) disclosure. We find that the test devices are standard compliant, in the sense that they do not send the IMEI over the network. To get the desired behaviour, we performed small changes to the code. These changes must be performed by an attacker to launch the attack, but require only some familiarity with the LTE standard and basic C programming skills.

2 PRELIMINARIES

2.1 LTE Architecture

The LTE architecture consists of the EUTRAN (Evolved Universal Terrestrial Radio Access Network) and the EPC (Evolved Packet Core). The user terminal, called UE (User Equipment), communicates with an eNodeB (enhanced NodeB), which is the access point to the operator's core network. To identify itself, authenticate and establish secure communication to the network, UE makes use of unique identifiers and keys stored in the USIM (Universal Subscriber Identity Module) and at the mobile operator side. Table 1 lists identifiers that we will refer to later in the paper. Some of these identifiers are sent in clear, before the secure communication is established. The mobile operator broadcasts some configuration information in clear also, such as the SIB (System Information Blocks) messages. Examples of SIB messages include SIB1 that contains cell access related parameters, and SIB5 that contains information regarding inter-frequency reselection.

2.2 Experimental Setup

The experimental setup consists of computers running open source software, attached with SDR and antennas (Figure 1). We used 2 computers: one Intel NUC D54250WYK (i5-4250U CPU@1.30GHz) and one Lenovo ThinkPad T460s (i7-6600U CPU@ 2,30GHz), both running 64-bit Kubuntu 14.04 kernel version 3.19.0-61-low latency and 2 types of handsets: Nexus 5 (Android v6.0.1) and Nexus 5X (Android v7.0).

Table 1: Identities and Parameters.

UE (User Equipment)		
IMSI	International Mobile Subscriber Identity	A unique long-time identifier for the USIM.
IMEI	International Mobile Equipment Identifier	A unique identifier for the user hardware device (e.g.: phone, modem).
Mobile Network		
MCC	Mobile Country Code	A unique identifier for the country a mobile subscriber belongs to.
MNC	Mobile Network Code	A unique identifier for the network a mobile subscriber belongs to.
TAC	Tracking Area Code	A code for a geographical region of a network operator served by the same Mobile Management Entity.
EARFCN	EUTRA Absolute Radio-Frequency Channel Number	A uniquely identifier for the LTE band and carrier frequency.

In the passive attacks scenario (Section 3.1), we used HackRF One (Great Scott Gadgets, 2017) as SDR and LTE Cell Tracker (Jiao Xianjun, 2017) software to sniff cells and decode broadcast messages. In the active attacks scenario (Section 3.2), we used B200mini (Ettus Research, 2017b) as SDR and OAI software (Open Air Interface, 2017) to build the rogue eNodeBs. Detailed information about the hardware and software for each of the two scenarios follows.

2.2.1 Passive Attacks

Hack RF One is a SDR (Software Defined Radio) peripheral capable of transmission and reception of radio signals from 1 MHz to 6 GHz, communicating in half duplex. The technical specifications of the HackRF One are available at (Great Scott Gadgets, 2017). We used HackRF One to sniff information about the target mobile network (Section 3.1). Our reason for using a HackRF device is that it is compatible with existing open-source software LTE Cell Tracker that allows to capture and decode unencrypted LTE traffic.

LTE Cell Scanner and Tracker is an open source software that can be used to sniff an LTE mobile access network and obtain information on the network topology and design (Jiao Xianjun, 2017). We used this software for scanning cells and capture traffic at selected frequencies. The LTE Cell Tracker uses Matlab scripts to decode the 20MHz bandwidth downlink LTE messages sent in clear, thus revealing important information sent in SIB messages.

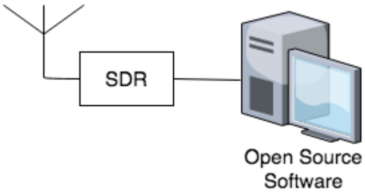


Figure 1: Experimental Architecture using SDR.

2.2.2 Active Attacks

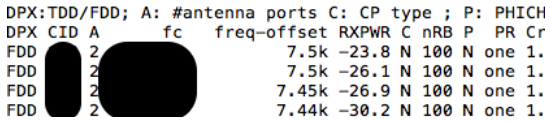
USRP B200mini is a USRP (Universal Software Radio Peripheral) from Ettus Research (Ettus Research, 2017a). The B200mini device is capable of transmission and reception of radio signals from 70MHz to 6GHz, communicating in full duplex. The technical specifications of the B200mini are available at (Ettus Research, 2017b). B200mini can be used for all LTE frequency bands, which allows high flexibility. It is easy to handle with (due to its small dimensions), affordable in price for academic experiments and satisfies all the technical requirements for our experiments, being compatible with the OAI software.

Open Air Interface (OAI) is an open source software that allows LTE emulation by running on a single computer with SDR attached (Open Air Interface, 2017). It is compatible with the B200mini and implements LTE control plane compliant to standard.

3 EXPERIMENTAL RESULTS

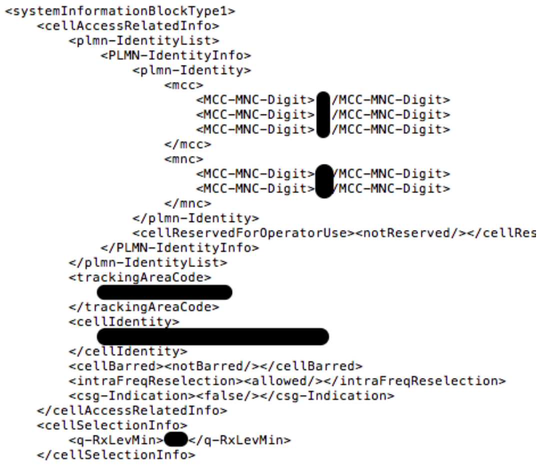
3.1 Passive Attacks

As explained in Section 2, an eNodeB broadcasts network parameters in clear. The traffic sent over the downlink channel can therefore be captured and decoded by an adversary to gain knowledge on the design of the network. We used LTE Cell Tracker to discover and track cells in the area of the university. Embedded Matlab scripts can be used to decode messages broadcast at 20MHz downlink bandwidth. However, we encountered some errors at running the scripts, so we had to perform basic corrections in the



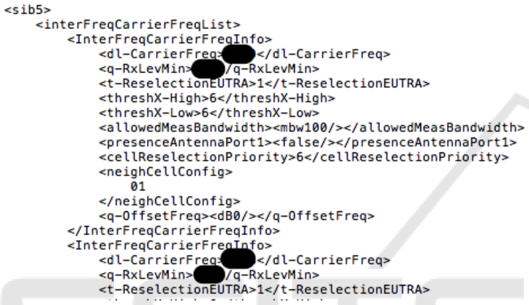
```
DPX:TDD/FDD; A: #antenna ports C: CP type ; P: PHICH
DPX CID A       fc    freq-offset RXPWR C nRB P   PR Cr
FDD [redacted] 2 [redacted]       7.5k -23.8 N 100 N one 1.
FDD        2                  7.5k -26.1 N 100 N one 1.
FDD        2                 7.45k -26.9 N 100 N one 1.
FDD        2   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

Figure 2: Commercial LTE Cells.



```
<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 3: Real capture of SIB1 (fragment).



```
<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 4: Real capture of SIB5 (fragment).

code to succeed[1]. The following examples show results of intercepting real traffic, broadcast by one of the commercial mobile operators:

- Figure 2 shows an example of cell search on a given frequency, listing cells that correspond to commercial eNodeBs in the area. Each cell is identified by a CID (Cell ID).
- Figure 3 exemplifies a successfully decoded SIB1 message. Notice the network identification parameters MCC and MNC (<MCC-MNC-Digit>), the location area identifier (<trackingAreaCode>) and the cell identity (<cellIdentity>). The cell is not barred (<cellBarred>) and allows intra frequency reselection (<intraFreqReselection>). Threshold on the signal level for cell selection is also specified (<RxLevMin>).
- Figure 4 exemplifies a decoded SIB5 message. By capturing and decoding a SIB5 message, the adversary learns the frequencies used in the area (<dl-CarrierFreq>) and their associated priorities (<cellReselectionPriority>). Hence, the adversary gains an overview of the network in the eavesdropped area and might subsequently use the gathered information to setup an active attack. More precisely, the attacker uses the results to configure the rogue base station (e.g.: setting up an IMSI Catcher by jamming the highest priority frequency and collecting IMSIs on the second highest priority frequency (Mjølsnes and Olimid, 2017)).

3.2 Active Attacks

3.2.1 IMSI Catcher

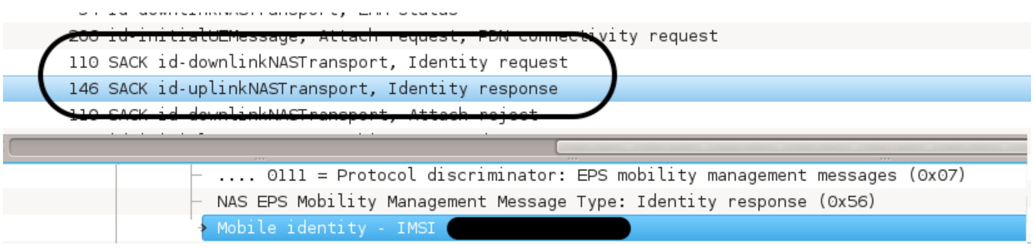
We base our work on the out-of-the box IMSI Catcher given in (Mjølsnes and Olimid, 2017). The rogue base station collects the IMSIs, but the experiment ends up in a DoS attack, which makes the attack easily detectable. We now make the UE reconnect to the commercial network immediately after disclosing the IMSI, which mitigates the detection of the attack at the user side. The user might still recognise an improper behaviour if it is in the middle of a conversation, but the probability of detection in practice is significantly lower. Moreover, in a second experiment we add an additional behaviour: the UE returns to the commercial network, but it denies LTE services. This results in a downgrade attack to 2G/3G, making the UE susceptible to the attacks in previous generation mobile networks.

The change in the OAI source code is minimal, and consists in changing the EMM Cause returned in the Attach Reject message from Cause #3 - Illegal UE to Cause #15 - No suitable cells in tracking area, respectively to Cause #7 - EPS services not allowed (ETSI TS 124 301 V12.6.0 (2014-10), 2014). We have tested both scenarios with successful results: UE disclosed the IMSI and returned to the commercial LTE network, respectively UE disclosed the IMSI and downgraded to a non-LTE service of the commercial network in a few seconds of operation. Figure 5 exemplifies an Identity Response message displayed in Wireshark (Wireshark, 2017) containing the IMSI, while Figures 6 and 7 illustrate the EMM causes in the two scenarios. In our experiments, Cause #7 - EPS services not allowed triggered downgrade to the commercial network to WCDMA.

3.2.2 IMEI Catcher

By default, in the Identification Request message, the rogue mobile network asks the UE device to identify

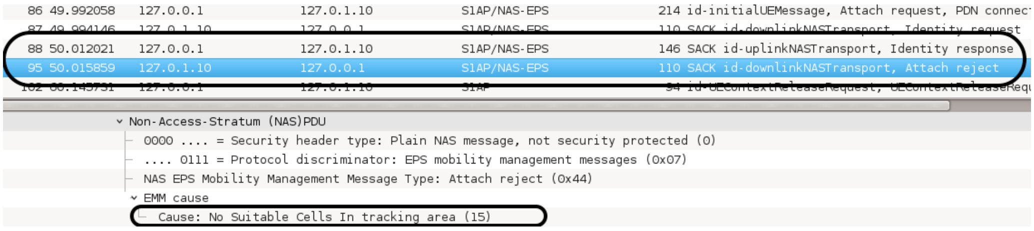
[1] The errors were easy to fix and might have been dependent on the version of the software. For example, we encountered a *Matrix dimensions must agree* error, which we solved by simply changing the starting index of a matrix from 2 to 1.



```
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]
```

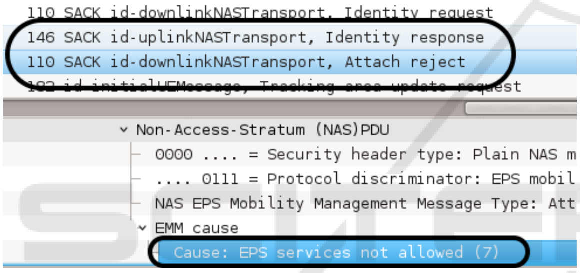
Figure 5: IMSI capture.



```
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

  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)
    EMM cause
      Cause: No Suitable Cells In tracking area (15)
```

Figure 6: Trigger reconnection to commercial network.



```
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

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

Figure 7: Trigger downgrade to non-LTE services in commercial network.

itself using the IMSI. We change the request to ask for IMEI instead. By this, we test compliance of UE to standard: IMEI should never be sent over the network in clear, except during the emergency calls, or when the UE has no IMSI, or no valid temporary identifier (ETSI TS 133 401 V10.3.0 (2012-07), 2012).

The change in the OAI source code needed is again minimal and consists in changing the EMM_IDENT_TYPE_IMSI to EMM_IDENT_TYPE_IMEI in the identification request function. Both devices that we tested proved to be standard compliant: they do not reply with an Identity Response message, and hence they do not disclose the IMEI. Figure 8 illustrates an example of IMEI request, followed by the Attach Reject message. Notice that there is no Identity Response message.

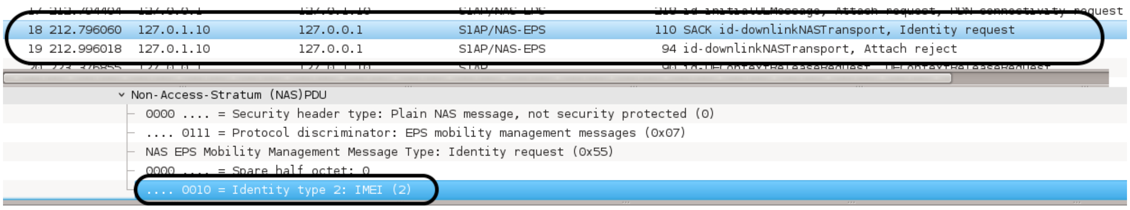
To make the IMEI request experiment less time consuming, we kept the EMM cause changed to Cause #15 - No suitable cells in tracking area, which allows the IMEI experiment to run several times without the necessity to reboot the UE, but only change the value of the TAC in the rogue network.

4 CONCLUSIONS

We argue the simplicity of breaking privacy in LTE networks. We show by experiment how to collect sensitive identifiers and parameters both at the subscriber level and the network level. Examples include the IMSI (permanent identifier of the subscriber) and the the list of high priority frequencies (parametrised at the network side). First, we show the possibility of eavesdropping on the LTE downlink using publicly available open source software and low cost hardware. Second, we improve existing work by mitigating the detection of rogue eNodeBs by subscribers and show that the downgrade attack can be implemented in LTE using OAI software too. Finally, we give a method to test compliancy to the standard with respect to IMEI disclosure. Our work shows that LTE security is still an open problem and that new vulnerabilities arise. Future research should focus on mitigating methods and countermeasures, with the goal to make mobile communication more secure.

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.



```
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

    ˅ 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 8: Identity Request (IMEI) followed by Attach Reject (no Identity Response).

REFERENCES

Bhattarai, S., Rook, S., Ge, L., Wei, S., Yu, W., and Fu, X. (2014). On simulation studies of cyber attacks against LTE networks. In *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, pages 1–8. IEEE.

Borgaonkar, R., Martin, A., Hirschi, L., Park, S., Shaik, A., and Seifert, J.-P. (2017). New adventures in spying 3G and 4G users: Locate, track & monitor. Blackhat Las Vegas Conference (to be presented).

Dabrowski, A., Petzl, G., and Weippl, E. R. (2016). The messenger shoots back: Network operator based IMSI catcher detection. In *International Symposium on Research in Attacks, Intrusions, and Defenses*, pages 279–302. Springer.

Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M., and Weippl, E. (2014). IMSI-catch me if you can: IMSI-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference*, pages 246–255. ACM.

ETSI TS 124 301 V12.6.0 (2014-10) (2014). Universal Mobile Telecommunications System (UMTS); LTE; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (3GPP TS 24.301 version 12.6.0 Release 12).

ETSI TS 133 401 V10.3.0 (2012-07) (2012). Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 10.3.0 Release 10).

Ettus Research (2017a). A National Instruments Company. https://www.ettus.com/ Last accessed: April 2017.

Ettus Research (2017b). USRP B200mini (Board only). https://www.ettus.com/product/details/USRP-B200mini Last accessed: April 2017.

Gomez-Miguelez, I., Garcia-Saavedra, A., Sutton, P. D., Serrano, P., Cano, C., and Leith, D. J. (2016). srsLTE: an open-source platform for LTE evolution and experimentation. *arXiv preprint arXiv:1602.04629*.

gr-LTE (2017). GNU Radio LTE receiver. https://github.com/kit-cel/gr-lte Last accessed: April 2017.

Great Scott Gadgets (2017). HackRF One. https://greatscottgadgets.com/hackrf/ Last accessed: April 2017.

Jiao Xianjun (2017). Cell Scanner and Tracker. https://github.com/JiaoXianjun/LTE-Cell-Scanner Last accessed: April 2017.

Jover, R. P. (2013). Security attacks against the availability of LTE mobility networks: Overview and research directions. In *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, pages 1–9. IEEE.

Jover, R. P. (2016). LTE security, protocol exploits and location tracking experimentation with low-cost software radio. *CoRR*, abs/1607.05171.

Lichtman, M., Jover, R. P., Labib, M., Rao, R., Marojevic, V., and Reed, J. H. (2016). LTE/LTE-a jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Communications Magazine*, 54(4):54–61.

Mjølsnes, S. F. and Olimid, R. F. (2017). Easy 4G/LTE IMSI Catchers for Non-Programmers. *arXiv preprint arXiv:1702.04434*.

Open Air Interface (2017). 5G software alliance for democratising wireless innovation. http://www.openairinterface.org Last accessed: April 2017.

OpenLTE (2017). An open source 3GPP LTE implementation. https://sourceforge.net/projects/openlte/ Last accessed: April 2017.

Rupprecht, D., Jansen, K., and Pöpper, C. (2016). Putting LTE security functions to the test: A framework to evaluate implementation correctness. In *10th USENIX Workshop on Offensive Technologies, WOOT 16, Austin, TX, August 8-9, 2016.*

Shaik, A., Seifert, J., Borgaonkar, R., Asokan, N., and Niemi, V. (2016). Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In *23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016.*

srsLTE (2017). Open source 3GPP LTE library. https://github.com/srsLTE/srsLTE Last accessed: April 2017.

The Register (2016). Every LTE call, text, can be intercepted, blacked out, hacker finds. http://www.theregister.co.uk/2016/10/23/ Last accessed: April 2017.

Wireshark (2017). https://www.wireshark.org/ Last accessed: April 2017.