



ON LOW-COST PRIVACY EXPOSURE ATTACKS IN LTE MOBILE COMMUNICATION

Ruxandra F. OLIMID^{*,**}, Stig F. MJØLSNES^{*}

^{*} Department of Information Security and Communication Technology,
NTNU, Norwegian University of Science and Technology,
Trondheim, Norway

^{**} Department of Computer Science University of Bucharest, Romania
E-mail: ruxandra.olimid@ntnu.no, sfm@ntnu.no

Abstract. The security of mobile communication is of great interest nowadays because of the wide spread and extensive use of mobile communication worldwide. Although LTE has been designed to provide better security than previous generations mobile networks, it is still vulnerable to attacks. In particular, it fails to protect the privacy of the subscribers. This paper focuses on the sensitive identities and parameters whose disclosure can directly damage the privacy of the subscribers or can be used as a basis to mount more advanced attacks. The sensitive data can be collected either by physical access to the user equipment or by attacking the radio link between the subscriber and the mobile station. We describe some low-cost possibilities to collect the data and refer to both passive and active attacks in LTE networks.

Key words: LTE, Mobile Communication, Privacy, IMSI Catchers, Software Defined Radio, Mobile Applications.

1. INTRODUCTION

1.1. Motivation and Contribution

The percent of the worldwide population that owns a mobile phone was estimated to be 62.9% in 2016, and it is forecasted to grow up to 67% in 2019 [1]. In March 2017, LTE market reached 28% of all mobile wireless technologies connections [2], and it is expected to continuously grow in the next years due to the increase in the usage of smartphones. Under these circumstances, the security of mobile communication in general, and LTE in particular, is of great interest. Although LTE has been designed to provide better security than previous generations networks, it is still prone to attacks. An important aspect in mobile security is the privacy of subscribers, for which LTE has been proved to remain vulnerable. For example, in LTE is still possible to test the presence or absence of subscribers in a given area, and even track their movement in time.

This paper focuses on the sensitive information that can be revealed at the user side or by attacking the radio link in the LTE access network. We first assume physical access to the user equipment and test by experiment how to access sensitive data.

We exemplify this by using some built-in codes and mobile applications on Android. Then, we point out to some ways to attack the radio interface between the user equipment and the base station. We refer to both passive and active attacks, and we mostly base the description of these attacks on personal previous results [3, 4]. Unlike the previous work, we do not only look at the network side (base stations), but also at the client side (user equipment). Moreover, we do not focus on how to implement particular types of attacks, but give an overview of means in which the sensitive information can be leaked at both ends.

1.2. Related work

LTE has been proved vulnerable to attacks that makes it susceptible to sensitive information leakage. Much work has been done both on eavesdropping and collecting the data that is sent in clear in regular

communication settings (*passive attacks*), and on building rogue base stations that impersonate commercial networks (*active attacks*). Examples include IMSI catching, downgrade to previous generations mobile networks (2G/3G), DoS (Denial-of-Service) and location tracking [3, 4, 5, 6, 7, 8, 9, 10].

Compliance with the LTE standards has been tested for several settings. Rupprecht et al. tested compliance of some equipment (phones and modems) with respect to encryption and authentication mechanisms [9]. We have tested compliance of modern smartphones with respect to IMEI disclosure [4].

Commercial LTE IMSI Catchers have been available to police and governmental institutions for many years now. Examples include the Stingray device, for which the manuals had been made public very recently [11] and the Cobham spy equipment [12].

Work has been done to mitigate and counter attacks in LTE [13, 14]. Much effort has been spent lately to eliminate the possibility to send IMSIs in clear, for example by using public key cryptography or new types of identifiers [15, 16, 17, 18, 19]. However, the existing solutions are not feasible in practice because lack of efficiency, necessity to change the existing architecture of the network and availability issues (limited number of usage). Cryptographic solutions to improve the AKA (Authentication and Key Agreement) mechanism so that it provides subscriber privacy has been considered. Fouque et al. proposed a variant of AKA that is resilient against Man-in-the-Middle attacks and disallow linkage of subscribers' sessions in the absence of corruption [20]. Previous similar solutions existed, but there were proved to fail some of the security requirements or fail to resist attacks [21, 22].

1.3. Outline

This paper analyses the sensitive information disclosure in LTE from two different perspectives: when the adversary has physical access to the user equipment, and when the adversary attacks the radio link between the user equipment and the base station. The next section introduces a short description of the LTE architecture and lists sensitive identities and parameters defining the subscriber or the network. Section 3 describes the hardware and software used for emulating an LTE network and the mobile applications used for testing purposes. Section 4 introduces a short analysis of data retrieval by physical access to the device. Sections 5 and 6 summarise passive and active attacks against the radio link, and Section 6 concludes.

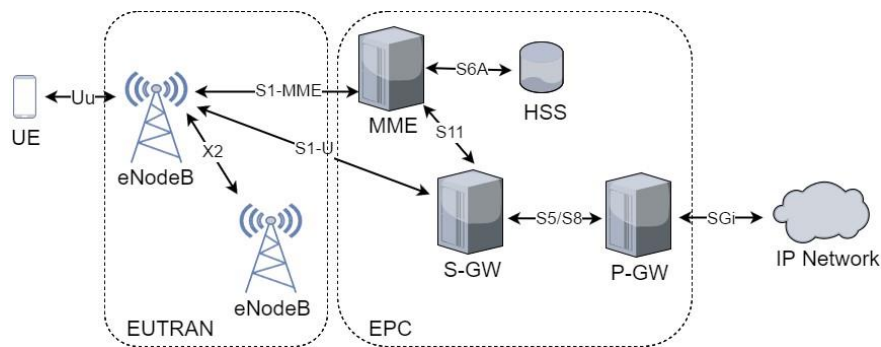


Fig. 1 – LTE architecture [3].

2. PRELIMINARIES

2.1. LTE Architecture

The LTE architecture is illustrated in Figure 1. The UE (User Equipment) is the user device (e.g.: mobile phone, modem) equipped with a USIM (Universal Subscriber Identity Module) card that stores the permanent identity of the subscriber (IMSI) and the root cryptographic key (K). The UE gets access to the operator network by connecting via radio link to a base station, called *eNodeB*. When the UE successfully attaches to the radio access network, it is said that the UE *camp on a cell*, where each *cell* operates on a specific frequency (EARFCN) and is identified by a *cell ID*. The access network in LTE is called EUTRAN (Evolved Universal Terrestrial Radio Access Network). The core network in LTE is called EPC (Evolved Packet Core) and is

responsible of identification and authentication of subscribers, resource allocation, mobility management and interconnection to other networks. A complete description of the LTE architecture is beyond the scope of this paper. The reader can find the detailed description of LTE architecture in 3GPP standards [23] or white papers [24, 25]. More about the security architecture can be found in [26].

2.2. Identities and Parameters

Sensitive data reside both at the subscriber's and the mobile operator's side. Parameters that uniquely identify a subscriber can expose the physical identity of the person using the subscription and facilitate location tracking. Similar, mobile network configuration provides valuable input that may be sufficient for an adversary to set up a rogue base station. We now describe some of the most important identities and parameters, at both sides.

Sensitive parameters at the user side include:

- IMSI (International Mobile Subscriber Identity): The permanent identifier of the USIM that uniquely identifies the subscriber, and it is used to grant access to services and payment management;
- IMEI (International Mobile Equipment Identifier): The unique identifier of the user equipment (e.g.: mobile phone, modem), which can be used by the operator in case of device thefts to deny connectivity to the mobile network;
- IMEISV (IMEI Software Version): A unique identifier of the user equipment that adds a 2-digit Software Version Number (SVN), which indicates the software version installed on the device;
 - TMSI (Temporary Mobile Subscriber Identity), GUTI (Globally Unique Temporary ID), GUMMEI (Globally Unique Mobility Management Entity Identifier): Temporary identifiers of subscribers that are used instead of the IMSI with the main goal to avoid privacy breaches (e.g.: identification, location tracking, etc.) and are periodically changed at intervals established by the network operator;
- The private key K : The root key used to derive the hierarchy of cryptographic keys that are subsequently used to provide authentication, confidentiality and integrity.

The parameters are available in the core network too, being necessary for the identification and authentication of the subscribers. More precise, a challenge-response mechanism takes place, during which the core network verifies by a random challenge that the subscriber knows the private key K that corresponds to the given IMSI.

Parameters at the network side, which define the operator and the actual implementation of the network, include:

- MCC (Mobile Country Code): The identifier of the country where the network is deployed;
- MNC (Mobile Network Code): The identifier of the network operator in a country;
- TAC (Tracking Area Code): A code that identifies a geographical region of a network operator that is served by the same MME (Mobile Management Entity) in the EPS;
- EARFCN (EUTRA Absolute Radio-Frequency Channel Number): The uniquely identifier for the LTE band and carrier frequency in a cell, with a 1-to-1 correspondence between the EARFCN and the uplink and downlink frequencies used for mobile communication.

3. EQUIPMENT AND TOOLS

3.1. Emulation of the LTE Network

A LTE network can be setup with low cost COTS (Commercial Off The Shelf) hardware and open source software. All the functionality is emulated on a computer, while the radio connectivity is supplied by a SDR (Software Device Radio). The software allows the emulation of the core network on a personal computer. It also provides connectivity to the SDR, which is configured to run as an eNodeB. Hence, the EPC runs completely on one computer, and the access network (E-UTRAN) consists in the SDR that is connected to the computer (Figure 2).

There exist several manufacturers of SDR devices. Examples of popular SDR devices include the USRP (Universal Software Radio Peripheral) series from Ettus [27], HackRF One [28], bladeRF [29], Eureka

ExpressMIMO II [30], limeSDR [31]. For our experiments, we have successfully used B200mini from Ettus (Figure 3(a)), and HackRF One (Figure 3(b)) [3, 4].

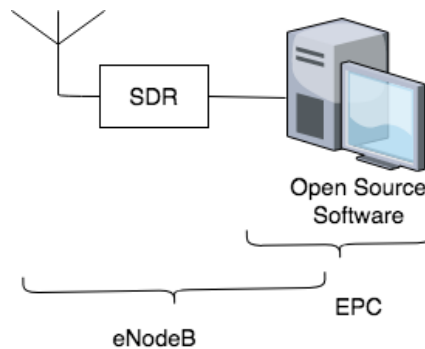
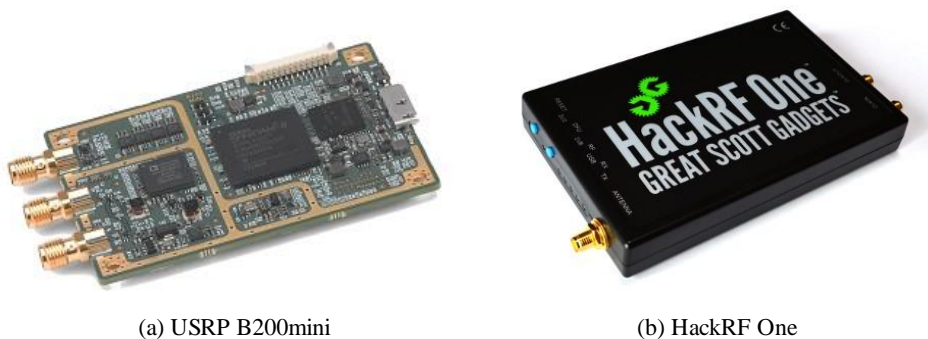


Fig. 2 – Implementation of a LTE network using SDR and open source software [4].



(a) USRP B200mini

(b) HackRF One

Fig. 3 – SDR Equipment.

Specialized software that emulates the functionality of the mobile network is freely available online. Examples for 4G mobile networks include OpenLTE [32], srsLTE [33, 34], gr-LTE [35] and Open Air Interface (OAI) [36], but implementations for previous generations also exist (e.g.: OpenBTS for GSM networks [37]). Different software systems must be used for different purposes. This is because even though all aim to be compliant with the LTE standard, not all functionalities are currently implemented. For example, paging is not implemented in OAI at the moment, so it cannot be used to set up paging attacks. We refer to paging attacks in Section 5.

Setting up a LTE network with the correct parameters can impersonate a commercial mobile network and can force the UE to connect to the false network, where it will reveal private information. This results in an active attack against the privacy of the subscriber. We refer to active attacks in Section 6.

3.2. Mobile Applications

For testing purposes on the user side we have used five free applications available on Google Play Store [38] that display information about the USIM or the LTE network. There is a multitude of such applications online, and we did not aim to exhaustively test all of them, but to show that it is possible to get access to data by using mobile applications. Table 1 lists the applications we tested. We have installed and run these applications on Nexus5 and Nexus5X smartphones. Section 4 contains the results.

4. PHYSICAL ACCESS TO THE UE

Some mobile network parameters can be found by physical access to the user equipment. This can be done either by running specific built-in codes, or by running applications that are available at no costs on the

application repositories. Side channel attacks or low-level programming on the baseband processor proved to reveal private information that is supposed to be unreachable to attackers [39, 40].

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

4.1. Built-in Dial Codes

Mobile operating systems permit to dial codes that display information that is normally hidden to ordinary users. The codes are handy to programmers for troubleshooting, but might also be useful to users with a deeper understanding level.

The codes and the data they display are dependent on the operating system and the hardware. They are mostly accessible online [41, 42, 43]. Tables 2 and 3 contain examples of built-in codes that display sensitive parameters.

Table 2

Information Disclosure - User Equipment

Handset	Operation System	IMSI	IMEI	IMEIS V
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	-

4.2. Applications

We investigate which pieces of information can be exposed by using freely available software, both at the user and at the network side.

We are interested in the identities and parameters whose disclosure affect the privacy of the user or the security of the communication in general. The list does not aim to be comprehensive, but our goal is to emphasize by a few examples that this is possible. The large number of such applications that exists on repositories show the high interest in the area.

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

Tables 2 and 3 show the displayed identities and parameters. The built-in codes and applications give also additional information on the network operator implementation (e.g.: eNodeB ID, Cell ID, etc.) and radio channel parameters (e.g.: noise ratio, signal strength, etc.).

Mobile malware is a significant threat to mobile security. Installing malware does not necessarily require physical access to the device. Malware can disclose sensitive information such as permanent and temporary identities (which lead to localization of the subscribers and movement tracking) or cryptographic keys. As an example, Xenakis and Ntantogian showed how to attack the baseband modem of mobile phones and steal security credentials, identities and cryptographic keys [40]. Their attacks work for both Android and iPhone devices. Unlike malware, there are applications that leak private information without intention, but because of insecure implementation or other factors. Graa et al. exploited side channels attacks and found that 35% of the analyzed mobile applications leaked sensitive information [39]. Their study was conducted for Android applications only.



Fig. 4 – SIB messages [4].

5. PASSIVE ATTACKS

An adversary can easily intercept the messages sent on the radio link. If the messages are sent in clear (unencrypted), the attacker can simply eavesdrop the radio link and find values that might be of interest by themselves or might help to setup more advanced attacks. Because the adversary does not actively interfere in the message flow, but only eavesdrops on the communication channel, these types of attacks are called *passive*.

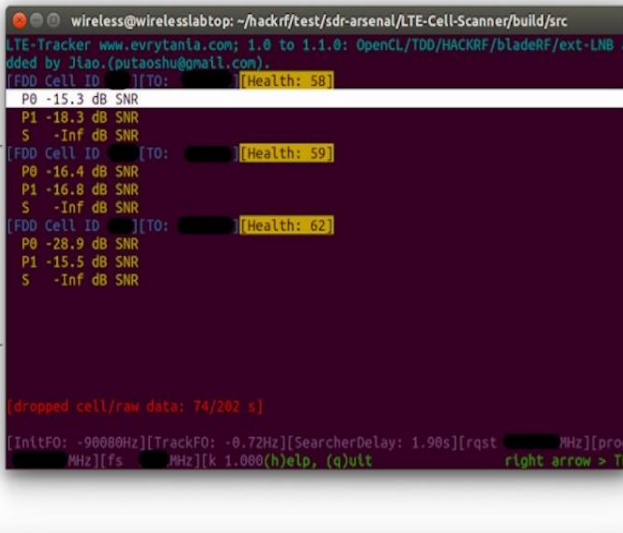
Passive attacks with direct or indirect consequences against the privacy of a LTE subscriber include: interception and decoding of MIB (Master Information Block) and SIB (System Information Block) messages, paging messages and measurements reports.

Interception and decoding of MIB and SIB messages. Information block messages are broadcasted by the eNodeB in the coverage area to notify its presence to the subscribers. MIB messages contain the configuration details such as the bandwidth and SIB scheduling information. SIB messages contain more specific information, depending on their type [44]. For example, SIB1 contains cell access related data (MCC, MNC, TAC) and SIB5 contains inter-frequency reselection related data (the frequencies in use for the existing cells in the area and their associated priorities). Although MIB and SIB messages do not contain data that disclose subscribers' privacy directly, the

```

322967 Cell 1 information:-----
322968     Cell mode: FDD
322969     Cell ID: ██████████
322970     Num. eNB Ant ports: 2
322971     Carrier frequency: ██████████
322972 Residual freq. offset: ██████████
322973     RX power level: 4.766
322974     CP type: normal
322975     Num. RB: 100
322976     PHICH duration: normal
322977     PHICH resource type: 1
322978 Cell 2 information:-----
322979     Cell mode: FDD
322980     Cell ID: ██████████
322981     Num. eNB Ant ports: 2
322982     Carrier frequency: ██████████
322983 Residual freq. offset: ██████████
322984     RX power level: -1.8114
322985     CP type: normal
322986     Num. RB: 100
322987     PHICH duration: normal
322988     PHICH resource type: 1
322989 Cell 3 information:-----
322990     Cell mode: FDD
322991     Cell ID: ██████████
322992     Num. eNB Ant ports: 2
322993     Carrier frequency: ██████████
322994 Residual freq. offset: ██████████
322995     RX power level: 4.3475
322996     CP type: normal
322997     Num. RB: 100
322998     PHICH duration: normal
322999     PHICH resource type: 1

```



```

wireless@wirelesslabtop: ~/hackrf/test/sdr-arsenal/LTE-Cell-Scanner/build/src
LTE-Tracker www.evrytanla.com; 1.0 to 1.1.0: OpenCL/TDD/HACKRF/bladeRF/ext-LNB a
dded by Jtao.(putaoshu@gmail.com).
[FDD Cell ID: ██████████][TO: ██████████][Health: 58]
P0 -15.3 dB SNR
P1 -18.3 dB SNR
S -Inf dB SNR
[FDD Cell ID: ██████████][TO: ██████████][Health: 59]
P0 -16.4 dB SNR
P1 -16.8 dB SNR
S -Inf dB SNR
[FDD Cell ID: ██████████][TO: ██████████][Health: 62]
P0 -28.9 dB SNR
P1 -15.5 dB SNR
S -Inf dB SNR

```

Fig. 5 – Cell scanning.

values they broadcast are required for more advanced attacks (e.g.: the inter-frequency reselection priority list gives the correct configuration for a false base station such that user equipment trigger cell reselection). Figure 4 illustrates SIB1 and SIB5 messages sent by a commercial network operator [4].

The messages were intercepted and decoded by using LTE Cell Scanner and Tracker, an open source software that can be used to sniff the radio interface and decode messages in the 20MHz downlink bandwidth [45]. Figure 5 shows cell scanning in the area of NTNU and the information obtained from the MIB messages.

Interception and decoding of paging messages. Paging messages are used to discover the presence of a subscriber in an area and contain identifiers of subscribers [44]. A paging is usually a wake-up message for a UE that is in *idle* mode, indicating that the network needs to communicate something to the subscriber. For efficiency reasons, the paging messages are only sent in a limited area, where the UE is most likely located, and not over the entire radio coverage.

It follows that once a paging message was sent for a given identity in a specific area, the probability to locate the subscriber in the area is high. Although a safe implementation of the mobile network imposes that the identity present in the paging messages is a temporary one, it was proved that linkability between the temporary and the permanent identity of the subscriber is possible (by more advanced attacks), both in previous generations mobile networks and in LTE [6, 46].

Interception and decoding of measurements reports. Upon request, the UE performs radio measurements and send reports to the eNodeB. The communication is unencrypted, which makes them vulnerable to eavesdropping. Because the measurement reports contain information about the nearby base stations and their corresponding transmitting power, the adversary can use the data to determine the subscriber's location [6, 7].

6. ACTIVE ATTACKS

An *active* attack is more advanced than a passive attack in the sense that the adversary does not only eavesdrop on the radio link, but can also actively interfere in the message flow. Active attacks that damage the privacy of a LTE subscriber include: IMSI Catchers and triggering passive attacks.

IMSI Catchers. They are active devices that make the UE disconnect from the commercial LTE network and attach to the rogue eNodeB, disclosing information about the subscriber's identity. Building a simple IMSI Catcher whose only purpose is to collect IMSIs is easy and can be done at affordable price for individuals [3]. Figure 6 shows the capture of an IMSI, as a result of an *Identity Request* message initiated by the rogue eNodeB. This is possible because of a security policy breach that allows the UE to send the IMSI in clear as a response to a eNodeB request. The risk of exposure was well known at the moment of standardization and assumed by the 3GPP: "*The user's response contains the IMSI in cleartext. This represents a breach in the provision of user identity confidentiality*" [26]. This allows an adversary to setup a rogue eNodeB that impersonates the commercial network, force the UE to try attachment and then request the IMSI. Forcing this behavior is possible if the IMSI Catcher is configured with the correct parameters, based on the network identity (MNC, MCC, TAC) and the priority of frequencies that are broadcasted in the SIB messages. IMEI can also be queried by a similar request, but the devices do not respond with the IMEI unless there is no USIM card available or emergency procedure is in place, which makes them compliant to standard [26]. Some old devices have been shown to be vulnerable to this kind of attacks and exposed their IMEI [47].

Triggering passive attacks. Active attacks can be used to trigger a passive attack, at a time that is convenient for the adversary and under specific circumstances. For example, the adversary does not have to wait for a paging request to take place, but can trigger paging by himself and then use the same approach as in the passive paging attack. Social applications (e.g.: Facebook, WhatsUp) can be used to trigger paging messages [6]. This is because a paging message is triggered whenever, for example, someone starts to write a message. The recipient is notified that a message is being typed, and this is performed by a paging message. Hence, an adversary can trigger a paging attack against a subscriber if it knows his identity and starts (or at least pretends to start) a communication with him on a social network. Similar attacks are possible for the measurement reports, an attacker being capable to request to the user specific report information that include for example even its GPS coordinates [6]. This is of course a clear example of privacy disclosure, because the adversary finds where the subscriber is.

Advanced functionalities of IMSI Catchers. Advanced IMSI Catchers can create a different behavior for the UE. For example, the rogue eNodeB can deny access to the UE and send it back to the commercial network. This decreases the chances to notice the attack is taking place, because the reconnection to the commercial network is performed fast. However, in addition to capturing the IMSI, the IMSI Catcher can make the UE downgrade to 2G/3G or even deny access of the subscriber to any mobile service, until restart [3, 4, 6, 7]. Downgrading to previous generations network makes the UE susceptible to the existing attacks in less secure networks, while access deniability concludes in a DoS (Denial of Service). Both attacks are easy to mount and only require basic changes to the open source software code [3, 4].

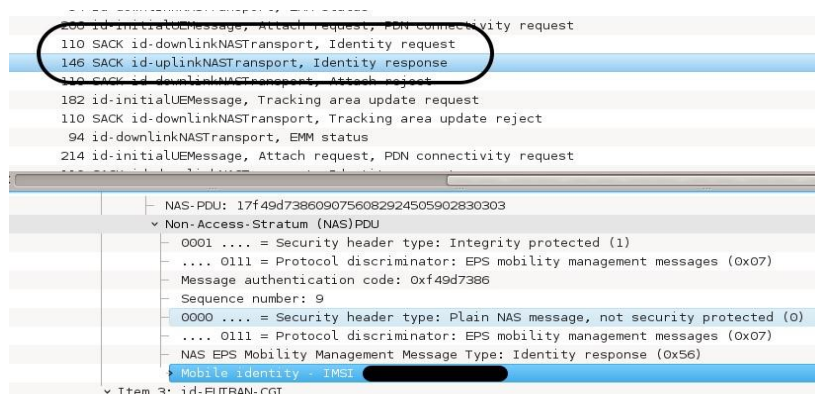


Fig. 6 – IMSI Catcher [4].

7. CONCLUSIONS

LTE security analysis is a hot topic nowadays, being of great interest to both academia and industry. Although designed to provide better security than previous generation networks, LTE cannot fully protect the privacy of the subscribers. This is because security policy breaches were allowed in the standard (e.g.: IMSI transmission over the radio link in clear), but also because of improper design and implementation performed by the operators and manufacturers, as many configurations are left to their choice (e.g.: the time interval to change the temporary identifiers, a clear indication on the mobile phone if the communication is encrypted or not).

We have presented some possibilities to collect sensitive information either by physical access to the user equipment or by listening to the radio communication link, which can be further used to mount more advanced active attacks. We give a brief classification of different types of passive and active attacks against LTE. To conclude, we highlight the existence of breaches in the security of mobile communications, and we emphasize the need for more secure mobile systems, especially in the context of the Internet of Things (IoT).

REFERENCES

1. S. T. S. PORTAL, *Number of mobile phone users worldwide from 2013 to 2019 (in billions)*, <https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/>, 2017.
2. 5G AMERICAS, *Global LTE market share nearly 28% – 2.16 billion LTE connections*, <http://www.5gamericas.org/en/newsroom/press-releases/global-lte-market-share-nearly-28-216-billion-lte-connections/>, 2017.
3. S. F. MJØLSNES, R. F. OLIMID, *Easy 4G/LTE IMSI Catchers for Non-Programmers*, ArXiv e-prints, Feb. 2017, Accepted for publication at MMM-ACNS 2017.
4. S. MJØLSNES, R. OLIMID, *Experimental Assessment of Private Information Disclosure in LTE Mobile Networks*, 2017. Accepted for publication at Secrypt 2017.
5. R. P. JOVER, *Security attacks against the availability of LTE mobility networks: Overview and research directions*, in Wireless Personal Multimedia Communications (WPMC), 16th International Symposium on IEEE, pp. 1–9, 2013.
6. A. SHAIK, J. SEIFERT, R. BORGAONKAR, N. ASOKAN, V. NIEMI, *Practical attacks against privacy and availability in 4G/LTE mobile communication systems*, in 23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016. [Online]. Available: <http://www.internetsociety.org/sites/default/files/blogs-media/practical-attacks-against-privacy-availability-4g-lte-mobile-communication-systems.pdf>.
7. R. P. JOVER, *LTE security, protocol exploits and location tracking experimentation with low-cost software radio*, CoRR, **abs/1607.05171**, 2016. [Online]. Available: <http://arxiv.org/abs/1607.05171>.
8. M. LICHTMAN, R. P. JOVER, M. LABIB, R. RAO, V. MAROJEVIC, J. H. REED, *LTE/LTE-a jamming, spoofing, and sniffing: threat assessment and mitigation*, IEEE Communications Magazine, **54**, 4, pp. 54–61, 2016.
9. D. RUPPRECHT, K. JANSEN, C. POPPER, *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. [Online]. Available: <https://www.usenix.org/conference/woot16/workshop-program/presentation/rupprecht>.
10. R. BORGAONKAR, A. MARTIN, L. HIRSCHI, S. PARK, A. SHAIK, J.-P. SEIFERT, *New adventures in spying 3G and 4G users: Locate, track & monitor*, 2017, Blackhat, Las Vegas Conference (to be presented).
11. THE INTERCEPT, *Long-secret Stingray manuals detail how police can spy on phones*, <https://theintercept.com/2016/09/12/long-secret-stingray-manuals-detail-how-police-can-spy-on-phones/>.
12. ***, *Leaked catalogue reveals a vast array of military spy gear offered to U.S. police*, <https://theintercept.com/2016/09/01/leaked-catalogue-reveals-a-vast-array-of-military-spy-gear-offered-to-u-s-police/>.
13. A. DABROWSKI, N. PIANTA, T. KLEPP, M. MULAZZANI, E. WEIPPL, *IMSI-catch me if you can: IMSI-catcher catchers*, in Proceedings of the 30th annual computer security applications Conference. ACM, 2014, pp. 246–255.
14. A. DABROWSKI, G. PETZL, E. R. WEIPPL, *The messenger shoots back: Network operator based IMSI catcher detection*, in Proceedings of Research in Attacks, Intrusions, and Defenses - 19th International Symposium (RAID 2016), Paris, France, September 19-21, 2016, pp. 279–302.
15. M. S. A. KHAN, C. J. MITCHELL, *Improving air interface user privacy in mobile telephony*, in Proceedings of Security Standardisation Research - Second International Conference (SSR 2015), Tokyo, Japan, December 15-16, 2015, pp. 165–184.
16. H. CHOUDHURY, B. ROYCHOUDHURY, D. K. SAIKIA, *Enhancing user identity privacy in LTE*, in 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2012), Liverpool, United Kingdom, June 25-27, 2012, pp. 949–957.
17. A. A. MUTHANA, M. M. SAEED, *Analysis of user identity privacy in LTE and proposed solution*, International Journal of Computer Network and Information Security, **9**, 1, p. 54, 2017.
18. V. CHANDRASEKARAN, F. AMJAD, A. SHARMA, L. SUBRAMANIAN, *Secure mobile identities*, CoRR, **abs/1604.04667**, 2016. [Online]. Available: <http://arxiv.org/abs/1604.04667>.

19. M. S. A. KHAN, C. J. MITCHELL, *Trashing IMSI catchers in mobile networks*, in Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2017), Boston, MA, USA, July 18-20, 2017, pp. 207–218. [Online]. Available: <http://doi.acm.org/10.1145/3098243.3098248>.
20. P. FOUQUE, C. ONETE, B. RICHARD, *Achieving better privacy for the 3gpp AKA protocol*, PoPETs, **2016**, 4, pp. 255–275, 2016. [Online]. Available: <https://doi.org/10.1515/popets-2016-0039>.
21. F. VAN DEN BROEK, R. VERDULT, J. DE RUITER, *Defeating IMSI catchers*, in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015, pp. 340–351.
22. M. ARAPINIS, L. I. MANCINI, E. RITTER, M. RYAN, N. GOLDE, K. REDON, R. BORGAONKAR, *New privacy issues in mobile telephony: fix and verification*, in the ACM Conference on Computer and Communications Security (CCS'12), Raleigh, NC, USA, October 16-18, 2012, pp. 205–216.
23. ETSI TS 123 002 V14.1.0 (2017-05), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Network architecture (3GPP TS 23.002 version 14.1.0 Release 14)*, 2017.
24. ALCATEL-LUCENT, *The LTE network architecture – a comprehensive tutorial*, [http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE Alcatel White Paper.pdf](http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE%20Alcatel%20White%20Paper.pdf), 2013.
25. J. CICHONSKI, J. M. FRANKLIN, M. BARCOCK, *LTE architecture overview and security analysis*, NIST Draft NISTIR, **8071**, 2016.
26. ETSI TS 133 401 V10.3.0 (2012-07), *Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 10.3.0 Release 10)*, 2012.
27. ETTUS RESEARCH, *A National Instruments Company*, <https://www.ettus.com/>.
28. GREAT SCOTT GADGETS, *HackRF One*, <https://greatscottgadgets.com/hackrf/>.
29. NUAND, *BladeRF*, <https://www.nuand.com/>.
30. EUROCOM, *ExpressMIMO*, <http://openairinterface.eurecom.fr/expressmimo2>.
31. LIME MICROSYSTEMS, *LimeSDR*, <http://www.limemicro.com/>.
32. OPENLTE, *An open source 3GPP LTE implementation*, <https://sourceforge.net/projects/openlte/>.
33. SRSLTE, *Open source 3GPP LTE library*, <https://github.com/srsLTE/srsLTE>.
34. I. GOMEZ-MIGUELEZ, A. GARCIA-SAAVEDRA, P. D. SUTTON, P. SERRANO, C. CANO, AND D. J. LEITH, *srsLTE: an open-source platform for LTE evolution and experimentation*, arXiv preprint arXiv:1602.04629, 2016.
35. gr-LTE, *GNU Radio LTE receiver*, <https://github.com/kit-cel/gr-lte>.
36. OPEN AIR INTERFACE, *5G software alliance for democratising wireless innovation*, <http://www.openairinterface.org>.
37. OPENBTS, *Open source cellular infrastructure*, <http://openbts.org/>.
38. GOOGLE, *Play Store - Apps*, <https://play.google.com/store/apps?hl=en>.
39. M. GRAA, N. CUPPENS-BOULAHIA, F. CUPPENS, J.-L. LANET, R. MOUSSAILEB, *Detection of Side Channel Attacks Based on Data Tainting in Android Systems*, Cham: Springer International Publishing, 2017, pp. 205–218. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-58469-0_14
40. C. XENAKIS, C. NTANTOGIAN, *Attacking the baseband modem of mobile phones to breach the users' privacy and network security*, in Cyber Conflict: Architectures in Cyberspace (CyCon), 7th International Conference on. IEEE, 2015, pp. 231–244.
41. ANDROID PIT, *Access hidden info on your android device with these secret codes*, <http://www.ni.com/en-no.html>.
42. IPHONE TRICKS, *17 secret iphone interrogation codes*, <http://www.iphone-tricks.org/17-secret-iphone-interrogation-codes/>.
43. TECHVIRAL, *20+ best hidden iphone secret codes 2017*, <https://techviral.net/best-iphone-secret-codes/>.
44. ETSI TS 125 331 V14.2.0 (2017-04), *Universal Mobile Telecommunications System (UMTS); Radio Resource Control (RRC); Protocol specification (3GPP TS 25.331 version 14.2.0 Release 14)*, 2017.
45. JIAO XIANJUN, *Cell Scanner and Tracker*, <https://github.com/0x90/sdr-arsenal/tree/master/LTE-Cell-Scanner>.
46. D. F. KUNE, J. KOŁNDORFER, N. HOPPER, Y. KIM, *Location leaks over the GSM air interface*, in 19th Annual Network and Distributed System Security Symposium (NDSS 2012), San Diego, California, USA, February 5-8, 2012. [Online]. Available: <http://www.internetsociety.org/location-leaks-over-gsm-air-interface>.
47. B. MICHAU, C. DEVINE, *How to not break LTE crypto*, Symposium sur la sécurité des technologies de l'information et des communications, 2016.