Experimental Security Analysis for Fake eNodeB Attack on LTE Network

Fardan
School of Electrical Engineering, Telkom University
Bandung, Indonesia
fardanfnn@telkomuniversity.ac.id

Istikmal
School of Electrical Engineering, Telkom University
Bandung, Indonesia
istikmal@telkomuniversity.ac.id

Ikbal Mawaldi
Telco Researcher idNSA
Bandung, Indonesia
ikbal.mawaldi@idnsa.id

Tides Anugraha
Telco Researcher idNSA
Bandung, Indonesia
Tides.anugraha@idnsa.id

Ishak Ginting
School of Electrical Engineering, Telkom University
Bandung, Indonesia
ishakg@telkomuniversity.ac.id

Nyoman Karna
School of Electrical Engineering, Telkom University
Bandung, Indonesia
aditya@telkomuniversity.ac.id

***Abstract*— The Long Term Evolution (LTE) user network is the largest population used nowadays compared to 2G and 3G in mobile telecom landscape. It is declared that LTE has provided a strong security standard in term of protecting its user for security attack on mobile communication. Fake Base Station is one of attack scheme in mobile communication infrastructure. The paper showcases the experimental analysis of the vulnerability of the LTE network which is impact to the user if we perform Fake eNodeB attack. In this experiment, we use OpenAirInterface5G, an opensource cellular platform that supports the full stack of LTE including 5G standard as the Fake eNodeB. The attack is performed by impersonating a real 4G network Operator. The result of this attack is IMSI number of users is obtained which lead the users is traceable as well as it is possible to force the target unable to be served back by the legitimate base station which leads to Denial of Service (DOS) attack. We also point out on describing the flaws of the LTE protocol that lead into this possibility of attacking and its implication especially on user identity and user connection with the operator that possibly harmed. We describe also several options to overcome the issue in the future.**

Keywords— LTE, mobile network, OpenAirInterface5G, IMSI, LTE security

I. INTRODUCTION

Long-Term Evolution (LTE) is the technology in mobile communication generation with the largest user around the world [1]. High data rates of transfer offered by LTE is achieved by providing radio resource management as well as data transmissions from the network to its mobile users by delivering physical layer control messages in high time precision [2]. in term of security, a study of a comparative survey of legacy and the LTE platform in term of the network security was explored in [3][4] for the land mobile radio system-LTE convergence and mission-critical push-to-talk over LTE. in addition, Survey on wireless technologies and security procedures is an important matter in High-Speed Packet Access (HSPA) and LTE networks to provide real progress of communication [5]. An overview of the security functionality and vulnerabilities of the LTE and LTE-A networks are explored with a review of existing solutions [6]. Several vulnerabilities in LTE/SAE (System Architecture Evolution) security architecture has been analyzed in the deployment of the emerging insecure AKA (Authentication and Key Agreement) key derivation procedures and the lack of fast re-authentication during handovers and Denial of Service attacks [7][8]. Because of the high user population around the world, protection for this platform is important. Thus, examining an impact from an attack model to the LTE network in order to find the vulnerability is needed.

The paper shows the analysis of Fake eNodeB attack which performs against LTE Network, examining its impact on LTE users. Using OAI as the LTE software platform to build the network, it has been discovered that it shows us the possibility to perform such attack both passive and active on the network. The OpenAirInterface5G (OAI) itself is a project focuses on open source software/hardware development for both the radio access networks (EUTRAN) and core networks (EPC) of 3GPP mobile communication networks [9]. In addition, we choose OAI due to its support the complete protocol stack of LTE. For hardware, the attack implemented with Universal Software Radio Peripheral (USRP) hardware. There is to be noted it is becoming more critical that OAI without change on its source code has already enough to perform the attack.

The paper is organized into three sections as follows: Section 2 will provide the background, explain briefly the LTE architecture, LTE security and the OpenAirInterface5G open-source software. Section 3 describes the attack concept scenario that has been done in the experiment. There are two scenarios: first, impersonating with different parameter setting from existing LTE base station existed around and the second is by imitating the real LTE base station. Section 4 explains the setup configuration and followed by highlight the vulnerabilities discovered in the experiment such as IMSI Cather attack and DoS Attack. Finally, the paper ends with a conclusion.

II. BACKGROUND

A. LTE Network Architecture

The latest standard in mobile communication network technology used by most of the user around the world is LTE. It is developed to have such technology with high data rates both uplink and downlink and also efficient at using bandwidth. Its security feature of this technology has been also improved compared to the previous technology (3G).

Both general architecture and principles of LTE Network are described in the several standards specifically on 3GPP specifications TS 36.300 [11] and TS 36.401 [12].

The LTE infrastructure consists of several components. It is divided into two parts (see Figure 1); all components involved in access link which is eNodeB and UE is categorized as the Evolved Universal Terrestrial Radio

Access Network (E-UTRAN). The other part which is categorized as Evolved Packet Core (EPC) is basically the core network. Furthermore, the EPC itself consists of MME and HSS.

User Equipment (UE) is part of the network that has the applications and services in user hand. It receives and transmits data to and from the network. Universal Subscriber Identity Module (USIM) is placed on UE which stores the International Mobile Subscriber Identity (IMSI) used as identity of user over the network. another main function for IMSI is to work as the pre-shared key K in order to generate further key for authentication procedure.

Evolved NodeB (eNodeB) is the base station or access point for LTE. Radio management data and encrypted data of communication between user and network are managed by eNodeB.

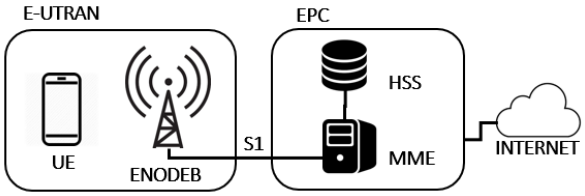

Figure 1: LTE network architecture [10].

Mobility Management Entity (MME). The MME manages the establishment of new connections and the authentication process. Connected UEs mobility data is controlled by this part. During the communication to and from MME, encryption and integrity protection are applied.

Home Subscriber Server (HSS). The information of LTE mobile subscribers is stored in the HSS as well as its authentication information. HSS plays the important role when establish the authentication procedure, especially while establish connection between unconnected UE to the network by providing user security information. Other than that, the EPC and E-UTRAN are connected via S1 interface. However, the logical connection between the components is specify into two type as follow.

Access Stratum (AS). The AS is used as a connection between UEs and eNodeBs. All messages exchanged on the radio layer to physically access of LTE will be covered by AS connection.

Non-Access Stratum (NAS). The NAS represents the logical connection between the UE and the MME. The communication between these two components will be covered by NAS such as identity management while authentication process and mobility.

B. LTE Security

On LTE, there are several standard security procedures. It is involved all components in the system such as UE, EnodeB, MME and HSS.

In the following, we describe the procedure implemented to handle a detached UE establish connection to the network. The full diagram can be seen in Figure 2. Firstly, the detached UE initiates the connection over the radio or physical connection to eNodeB. But from logical connection, the initialization started by sending an Attach Request message to the MME. When the UE could only provide the temporary identity for example from the previous connection then UE can be forced to send its IMSI as well by MME sending Identity request message.

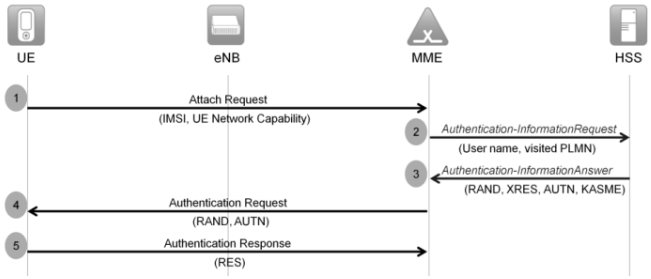

Figure 2: Attach process [13].

The next step is, there will be an authentication procedure between UE and LTE network which is called as Authentication and Key Agreement (AKA) explained in the following. It is mentioned previously that HSS and UE share the same key K. First, the MME sends an Authentication Information Request to the HSS, which stores the pre-shared key K of the specific user including its IMSI, in this case the user is who is applying attach process. Second, The HSS starts a challenge-response communication between the network and the UE by generate an Authentication Vector (AV) and sending it back to the MME via an Authentication information Answer. The AV has the following parameters:

- Random Number (RAND)
- Expected Response (XRES)
- Authentication Token (AUTN)
- Intermediate Key (KASME),

with KASME—Access Security Management Entity being derived from the long-term key K (LTE K) and AUTN containing, e. g., a Sequence Number (SQN), which is synchronized to the current state of the UE. It can be seen from Figure 3.

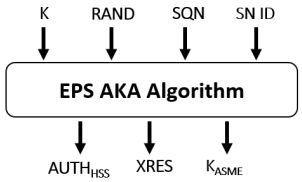

Figure 3. in MME

The UE then verifies AUTN by checking the range of the SQN, computes Response (RES), and its own intermediate key KASME. While computed RES is sent back to the MME, UE compare whether the received XRES are equal with RES. If the UE proved that it has the same key K, then UE has authenticated itself against the LTE network. Otherwise, the AKA procedure is aborted

C. OpenAirInterface5G

The OpenAirInterface5G (OAI) is an opensource project focus for mobile communication infrastructure which follows both the radio access networks and core networks set by 3GPP mobile communication networks. OAI was maintenance and controlled by Eurocom Project. All protocol stack as well as LTE component has already fully

supported by OAI both core network and access network [13].

There is several hardware has been tested work with OAI such as USRP B210, USRP X310, BladeRF, LimeSDR and EURECOM EXPRESSMIMO2 RF. Currently the main goal to develop a 5GNR Cellular Stack on COTS Hardware. the last version of LTE supported is Release 10. In short, all LTE software platform in emulated on Computer devices both for eNodeB and all EPC components, then USRP hardware to transmit and receive radio signals.

III. Attack Concept Overview

In this chapter we provide an operational informations of the steps in order to perform Fake eNodeB attack on LTE Network.

In our experiment, we setup USRP B200 OAI eNodeB and OAI EPC on the same host. We use Xiao MI A1, and iPhone 5S to connect to the network. Our LTE Fake eNodeB setup is shown in Figure 4.

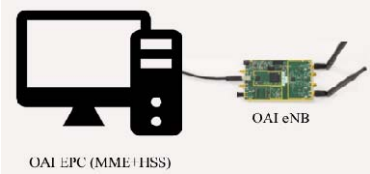

Figure 4. OAI Setup

There are two configurations implemented, using different MCC MNC parameter and another one impersonating the MCC MNC of the existing operator network around the lab.

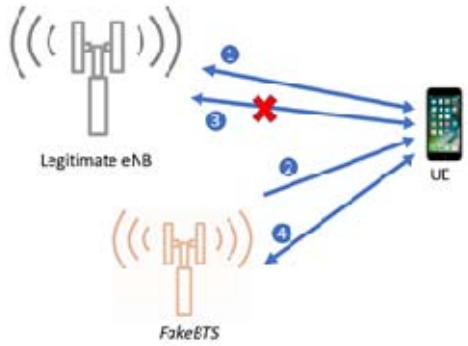

Figure 5. The experimental scenario

For the experimental scenarios, there are four steps expected

1. UE is still in connection to legitimate eNodeB which is a real operator network
2. Swich on the Fake eNodeB with modified parameter in order to impersonate the real network operator
3. The connection between UE and legitimate eNodeB is lost
4. The UE connect to a Fake eNodeB Network

Our experiments were run in our wireless security lab for educational and research purposes. We observe and analyze the LTE security mechanism during the authentication process between OAI and UE.

IV. Experiment and Discussion

The International Mobile Subscriber Identity (IMSI) uniquely identifies a mobile network user subscription. A Subscriber Identity Module (SIM) contains and protects the IMSI and it is used for authentication and identification of users. LTE specifications has been set to reduce its data information transmitted over-the-air radio communication for security and privacy purposes. As described before in Attach Procedure section, there are several things about the user's privacy data. In this section will be discussed and described the findings about LTE security mechanism with USRP B200 and OpenAirInterface5G.

A. Experimental Setup

In the experiment, we use OpenAirInterface5G (OAI) as our LTE network that implements the core network (EPC), and access network (eNodeB). The OAI software is installed in single PC with 8 GB of RAM memory and Intel Core i5-6500 CPU @ 3.20GHz x 4, which has good cost performance and high-speed processing. The PC is connected with Universal Software Radio Peripheral (USRP) B200 device over USB3 port, acting as an eNodeB. We install and configure (OAI) with minimal modification from OAI sample config files and source codes. For the commercial off the self (COTS) UE, we have Xiao MI A1, and iPhone 5S.

The operating system (OS) is 64-bit Ubuntu 14.04 LTS with low-latency kernel 3.19. It will work for master branch of OpenAirInterface5G5G and develop branch of openair-cn.

The OAI software was running in real-time with Frequency Division Duplexing (FDD) single input single output (SISO) mode. We use the netmonitor application to read the available EARFCN around the user equipment, which we will apply to our eNodeB.

B. Experimenal Result and Discussion

The first experiment, we setup the OAI with this parameter:

- MCC: 208
- MNC: 92
- EARFCN: 3350
- Band : 7

We set band 7 because this is the band used in Indonesia as well as set up the EARFCN in 3350 because this is not occupied by the available network. Once the eNodeB is powered up, we use manual search mode in the UE app to see the available network. From Figure 6 it can be seen that 20892 is now available which means that our OAI eNobeB has already active.

We try then to register manually but then it is rejected, and network switched to No services status. After that we look at the log of OAI and found that there is a transaction between the eNobeB and the UE. Attach request procedure is implemented.

Figure 6. Connected LTE NEtwork

Next trial is by using impersonation attack. The OAI is setup to be configured as following parameters;

- MCC: 510
- MNC: 10
- EARFCN: 1850
- Band : 3
- TAC: 2097

The result is impressive. The UE still connected with the valid eNodeB from the operator, but now the fake eNobe appears on the network list. Net Monitoring app is used to show the list. It can be seen from Figure 7 that detected as 'valid' neighbor network. The OAI eNode is detected as TAC 2097. We wait for couple second while moving the UE distance closer to the eNodeB and suddenly the UE lost the connection, and network switched to No services. Rejected status appear on OAI log file.

Based on that experiment there are two security issues we found will be explained in the next following section.

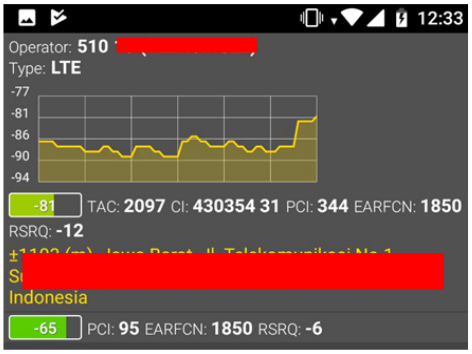

Figure 7. LTE Network

C. *User IMSI Data*

First trial is by running OAI eNodeB with unique MCC MNC then pushed UE to register manually. The communication messages between OAI component and UE can be seen by dump the data packet communication between E-UTRAN and EPC through wireshark. All communication is monitored in wireshark both before the registration process as well as when UE is trying to register manually. The picture in Figure 8 shows one of messages specifically on Identity response sent by UE.

When we look the procedure how the connection is established in LTE as shown in Figure 4, The UE begin with sending an attack request. By default, UE started the attach request procedure by sending a Tracking Area Update procedure since UE think that it moves to new serving base station (another LTE eNodeB). The network which is the OAI, because it is not belong to the legitimate base station of the UE, then TAU update request is then rejected due to the UE is not recognized in the OAI network.

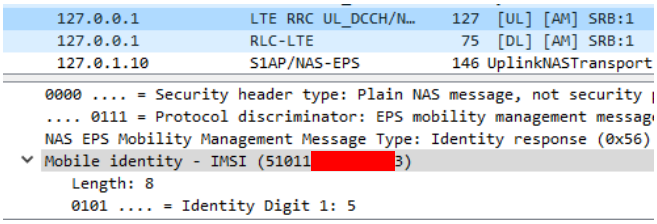

Figure 8. IMSI Catcher

The next procedure is OAI network sends Identity request to UE in order to verify the UE identity. Without checking whether the base station who ask for Identity request is legitimate or not, the UE reply by sending attack request included with IMSI number. This message can be seen in Figure 8 explicitly without any cover or encrypted message. This experiment proves that using the OAI, the IMSI is obtained.

The fact of IMSI is exposed easily literally the fact of the flaws of LTE protocol. Firstly because the protocol does not protect the communication message between the UE and the network that just before the authentication procedure or called pre-authentication phase. Before authentication handshake is deal, all messages are revealed. This protocol flaws allow us to see the UE identity once the network send Identity request. Secondly, the critical point in this LTE protocol flaw is that there is no checking procedure for the UE to be able to distinguish whether the UE communicate with the legitimate network or not. If there is a protection procedure, then the communication can be cut off just before UE send its any identity information.

We created a simple script to capture only the IMSI and match the operator name based on MCC MNC. The result is captured in Figure 9.

Figure 9. IMSI CAther

The important lesson, this simple attack can be applied with low cost hardware and readily available software OAI that even does not need to change any base line of its source code.

D. *DoS Attack*

The second trial of experiment, OAI eNobeB is running with the same radio parameter of existing LTE eNodeB in that area. Simply, we build a fake LTE Base station by imitating one of the base station configurations (see Figure 10) that available around the experiment area. The chosen eNodeB is from the same operator of the targeted UE.

While UEs are still connecting with the legitimate base station, from the same operator, the fake eNodeB is powered up. In order not to harm other UE, the fake eNodeB is setup with lower power level. Because the power level is low, to get maximum experience, the UE is placed closer to the fake eNodeB. No need to take any further action, suddenly we found the UEs are lost the connection and the status changed into no services. Meanwhile, from the OAI log record, there is an Attach request as well as the Authentication reject message is received. It has the similar process as described in IMSI Cather section previously.

As shown in Figure 10, after attach request message from the UE then network responds to the UE attach reject then cause MAC Failure, which lead into the UE unavailable until reboot. There are other several causes set into this condition such as cause 3 (Illegal UE) and cause 7 (EPS services not allowed).

When authentication failure occurs, there are at least three different status such as (1) MAC Failure, (2) Non-EPS authentication unacceptable and (3) Synch Failure. Those failure mostly related to invalid AUTN value in Authentication Request message.

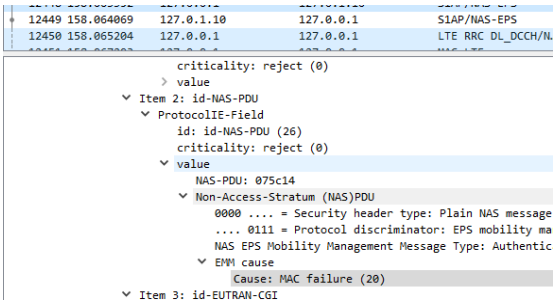

Figure 10. MAC Failure

Invalid AUNT parameter cause MAC failure as shown by Figure 9, can be explained refer to Figure 3. The UEs identity is not stored in the OAI HSS which means generating the same value of AUNT become impossible in both side, UE and network because the K parameter of UE does not exist in HSS therefor MME generates invalid parameter of AUNT. Resulting the challenge-response for authentication become invalid.

The important notes, this MAC failure not only move UE terminated any EMM signaling procedure and jump into EMM-deregistered state but also, the UE then change set into update status to EU3 Roaming. Consequently, this led UE to delete all saved GUTI parameter, TAI list, as well as last visited registered TAI and KSIasme on the USIM.

The impact of last procedure occurred is the USIM on UE then would be treated as invalid unless the UE is switched off or rebooted and USIM is removed then reinsert. This situation happens actually where we found before once the UE connect to OAI then it became no service. The UE unable to connect back to legitimate base station unless the UE is restarted.

This type of attack where we set up fake LTE eNodeB is not only the IMSI of the subscriber will be obtained by the attacker but also set the subscriber unable to connect back to the legitimate base station. In this situation, no services status literally the UE is never be served or got DoS (Denial of Service).

The flaws in the protocol which allow to perform the DoS attack as implemented in this paper basically can be figure out in two aspect. The first is that similar with we have discussed in IMSI Catcher part previously, it is needed there is ability or procedure applied into the network standard to allow the UE validated the base station where it camps to before continuing to any further procedure. The second issue, that the legacy from the previous mobile network generation where all the radio network configuration is broadcasted should be leaved. Because it allows the attacker collecting the information of legitimate base station and imitate the setting to its fake eNobeB.

V. Conclusion

We have shown the impact of Fake eNodeB attack on LTE network. There are two security issues found in LTE network protocol specifically related to Authentication request procedure, (1) IMSI catcher and (2) DoS attack. The IMSI number which is an identity of user in the network can be obtained. Attacker could use this information to detect mobility of the target user. In the operator side, Fake eNodeB attack can disturb services given to the user by not only being disconnected but also failed to reconnecting back and getting service from the legitimate operator. The UE will remain failure to connect on any cell (Denial-of-Service attack) as long as our fake eNodeB or Fake eNodeB is still up, and the UE is not restarted. We also verify that those type of attack can be done simply by using USRP B200 and open source cellular platform such as OpenAIrInterface. We have shown that these attacks can be performed easily with the low cost of hardware and open source software like OAI. We should consider these issues for next-generation (5G) and beyond generation such as considering architectural or change the procedure at the protocols in order to protect user privacy like IMSI or its base station parameter. Adding a new procedure of attaching request where UE would be able to verify the legitimate base station first would be very useful. The last one, approach a new paradigm of network protocol as not to follow the older generation is something necessary, all these options are still under study.

Acknowledgment

This work cannot be done without support from Chaosmatic and Indonesian Digital Network Association (idNSA) for the USRP. As well as for Telkom University for internal funding to support this publication.

References

[1] J. Abichandani et al., "A Comparative Study of Voice Quality and Coverage for Voice over Long Term Evolution Calls Using Different Codec Mode-sets," in IEEE Access, vol. 5, pp. 10315-10322, 2017.

[2] M. Wang et al., "The Evolution of LTE Physical Layer Control Channels," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1336-1354, Secondquarter 2016

[3] A. Kumbhar, F. Koohifar, İ. Güvenç and B. Mueller, "A Survey on Legacy and Emerging Technologies for Public Safety Communications," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 97-124, Firstquarter 2017.

[4] A. Jarwan, A. Sabbah, M. Ibnkahla and O. Issa, "LTE-Based Public Safety Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1165-1187, Secondquarter 2019.

[5] S. Vajjiravelu and A. Punitha, "Survey on wireless technologies and security procedures," 2013 International Conference on Information

Communication and Embedded Systems (ICICES), Chennai, 2013, pp. 352-355.

[6] J. Cao, M. Ma, H. Li, Y. Zhang and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 283-302, First Quarter 2014.

[7] A. N. Bikos and N. Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks," in IEEE Security & Privacy, vol. 11, no. 2, pp. 55-62, March-April 2013.

[8] C. Apostol and C. Racuciu, "Improving LTE EPS-AKA using the security request vector," 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, 2015, pp. WSD-5-WSD-8, doi: 10.1109/ECAI.2015.7301207.

[9] OpenAirInterface5G - 5G Software Alliance for Democratising Wireless Innovation. http://www.OpenAirInterface5G.org. Accessed: 14-10-2018

[10] Rupprecht, David, Kai Jansen, and Christina Pöpper. "Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness." WOOT. 2016.

[11] 3GPP TS 36.300. http://www.3gpp.org/DynaReport/36300.htm.

[12] 3GPP TS 36.401. http://www.3gpp.org/DynaReport/36401.htm

Open Air Interface: 5G software alliance for democratising wireless innovation. http://www.OpenAirInterface5G.org

[13] “UE States and LTE/SAE Signalling”. NOKIA Solutions. 2018