Averting Paging Related Attacks in 4G LTE Communication System

Vignesh Kumar V, Lakshmy K V

Abstract*: *Long Term Evolution (LTE) objective is to provide secured communication at higher data rate for the users. It's been long time that the technology is being consumed by the users. However, there are still security vulnerabilities that provides scope for various attacks on the network. One such scenario is that attacks related paging procedure itself. This paper discusses about the possible attacks related to paging and how these attacks affect the security of the network and also propose a scheme to avert these attacks by leveraging the existing LTE communication system and also the simulation of the proposed scheme with the security analysis of the same.

Index Terms*: *Authentication, Confidentiality, International Mobile subscriber Identity, Long Term Evolution

I. INTRODUCTION

LTE (Long Term Evolution) is the project name given to development of a high-performance air interface for cellular mobile communication systems. It is the last step toward the 4th generation (4G) of radio technologies designed to increase the capacity and speed of mobile telephone networks. LTE is designed in an effort to combine various security features and performance goals such as low latency and high transmission rates. The 4G LTE has been adopted in most of the countries which is not only is limited to the cellular communication but also support the critical infrastructure needs such as business, navigation, public safety message dissemination. Due to these critical applications of 4G LTE it has been attractive target for attacks by malicious parties. Thus, it is important to secure the network from end to end by eliminating the potential vulnerabilities without affecting its usability.

The LTE architecture is also known as Evolved Packet System (EPS) which majorly comprises of three components namely the user Equipment (UE), Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) and Evolved Packet Core (EPC) as shown in Fig. 1, The user Equipment consists of International Subscriber Identity (IMSI), Universal Subscriber Identity Module (USIM) and the master key, which helps in authenticating the user with the home server to access the network.

The E-UTRAN consists of an evolved base station (eNodeB) which acts intermediary providing communication between the Evolved Packet Core (EPC) and the User Equipment (UE). The EPC consists a Mobility Management Entity (MME), Packet Data Network (PDN) Gateway, Home Subscriber Server (HSS), Serving Gateway (S-GW). The MME is responsible for attach, paging and detach procedures of the UE under an eNodeB. The Home Subscriber Server stores UE's identities such as IMSI, IMEI and also the QOS profiles along with the cryptographic master keys for each user.

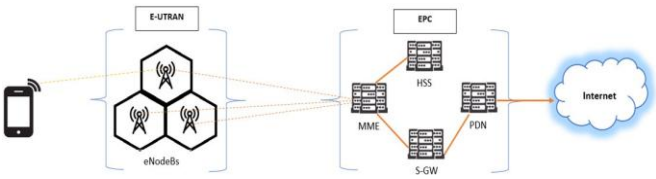

Fig. 1. LTE Network Architecture

Although the LTE architecture is designed to avert various security risks. It still has vulnerabilities which can easily be exploited and would cost drastically to the user and the network. Here, we discuss the various attacks related to paging and propose a new scheme to mitigate these vulnerabilities.

In this paper we discuss about the paging procedure, various attacks possible, related works and proposed scheme and its security analysis.

II. PAGING PROCEDURE AND POSSIBLE ATTACKS

In LTE, IMSI is used to identify a subscriber. The LTE specifications try to reduce the transmission of the IMSI over the air for various security reasons. Instead Temporary Mobile Subscriber Identity is used to communicate with the network which is assigned periodically during the attach procedures. During the attach procedure the UE sends an attach request message to eNodeB which is forwarded to the MME. It included the IMSI and security capabilities in plain text, on receiving the attach-request the MME challenges the UE with an authentication challenge that is sent by HSS. Using the UE master key solves the challenge and sends the response to the MME. Then the MME sends back the integrity protected security mode command message which includes the security capabilities sent by the UE. Then the UE verifies then UE send the security mode complete message. By which the UE is authenticated with the network.

A. Paging in LTE

Paging is a process used when the MME need to know the location of a UE to deliver the network service such as

Revised Manuscript Received on July 05, 2019.

Vignesh Kumar V, TIFAC-CORE in Cyber Security, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India.
Lakshmy K V, TIFAC-CORE in Cyber Security, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India.

SMS, Incoming Calls. The UE updates the MME about its change in location through tracking area update request which is similar to that of attach request. When a UE has no data to send, it enters an idle mode and wakes up periodically which is called the paging occasion and this period is known as paging cycle. Paging can be either initiated by the MME or eNodeB. In MME Initiated Paging, the MME has to locate the UE in a particular tracking Area to deliver the network service such as incoming message, SMS. The MME instructs all the eNodeBs to generate the paging message. When the UE receives the Paging message it detaches itself from the existing connection and re-initiates the attach procedure. In eNodeB initiated paging, the eNodeB will generate a paging message without the MME especially when it needs to notify a system change, emergency such as amber alert or an earthquake, tsunami warning.

During the Paging procedure, the UE is in idle state decodes the RRC paging message, if the paging message contains the IMSI of the UE then the UE understands that the MME or eNodeB is probing for it and it detaches itself from the present connection and proceeds with the new connection request and connection setup with the new eNodeB and establishes the connection as shown in Fig. 2.

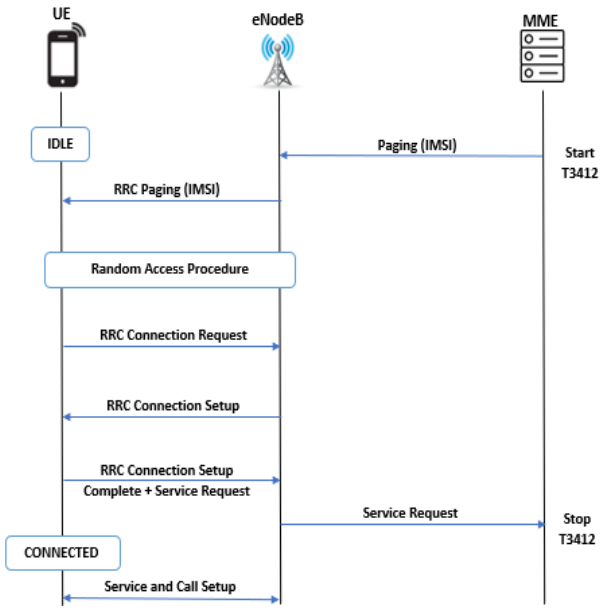

Fig. 2. Paging in LTE

B. Attacks Possible

As observed, During the paging procedure the data exchange between the UE and eNodeB is not encrypted, the IMSI and security mode commands are sent in plain text over the air, which can be easily captured by the adversary, the adversary can either snoop these details and impersonate as the original UE or the adversary can further simply setup the rouge eNodeBs and capture these information which is related to privacy of the user. Thus, the following attacks are possible as demonstrated by Syed et al [2], which leads to compromising the privacy of the user and leads to deterioration of the service provided by the network to the user.

Traceability Attack: This attack exploits the fact that the security mode command messages are exchanged in plain text and it uses these messages to track a particular UE. In this attack we assume that the adversary already has the security mode command messages and the adversary has also setup a fake/rouge eNodeB. The fake eNodeB setup by the adversary simply broadcasts the security mode command message in a particular tracking area, on receiving this message the UE under this tracking area verifies that the message. Thus, all the UE except the victim UE responds with the security mode reject message whereas the victim UE responds with security mode complete message as shown in Fig. 3, By which the adversary can easily locate the location of the victim UE. This affects the privacy of the user.

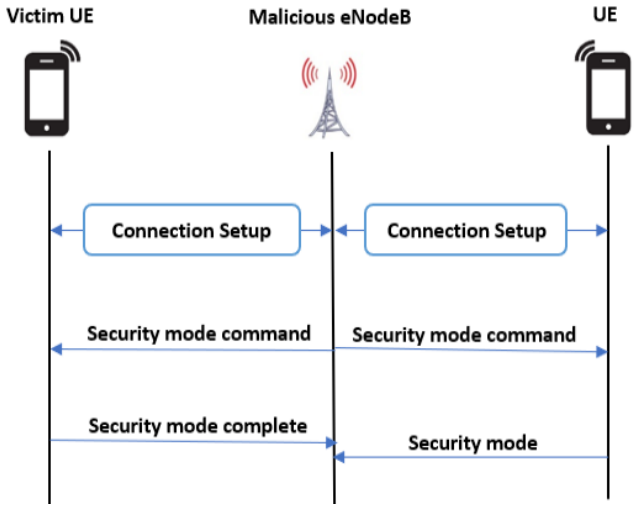

Fig. 3. Traceability Attack

Paging Channel Hijacking Attack: To hijack the paging channel the adversary deploys a malicious eNodeB which is operated as the same frequency as the authentic eNodeB so the victim UE does not perceive any network changes. Then the malicious eNodeB broadcasts the signal with higher power as compared to the authentic eNodeB. Thus, the Victim UE connects to malicious UE when the adversary create a paging message with already captured IMSI of the UE, on receiving the Paging request from the victim UE detaches itself and connects to the malicious eNodeB as shown in Fig. 4. This can lead to various attacks further such as Authentication Relay attack which would cost huge loss to the network and also the user.

Targeted Detach Attack: In this Attack the adversary first collects the list of IMSI which is transferred without any kind of encryption then the adversary deploys a malicious eNodeB and sends an identity request in the tracking area. On receiving the identity request all the UE in the tracking area responds with the identity response which contains the IMSI then looks up in the list of IMSI it had collected, and the adversary sends out a detach request to those IMSI. Once the victim UE receives the detach request the UE detaches itself from the network as showed in Fig. 4. This attack leads to the disruption of network and also leads to loss of credibility of the network.

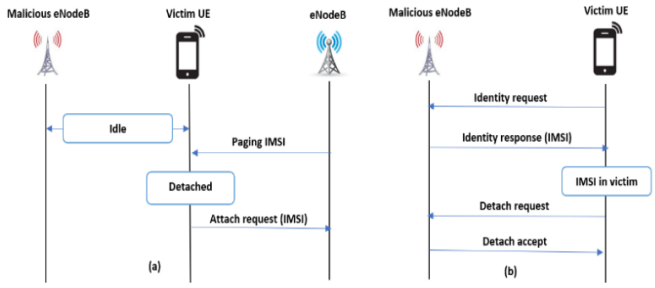

Fig. 4. (a) Paging Channel Hijacking Attack (b) Targeted Detach Attack

Apart from these various other attacks are possible such as Downgrade attack which downgrades the network from 4G to lower standards such as 3G or 2G or even deny the service to a particular UE. Energy depletion attack in which a victim UE is constantly paged by a malicious eNodeB, which leads to depletion of the limited power resources available in the UE. Further these attacks can be chained together to perform complex attack such as authentication relay attack, which would cause a disruption in the network and also tarnishes the best efforts of the network to provide a quality network service to the users.

III. PROPOSED SOLUTION

As observed in the previous sections all the attacks are possible due to lack of any form of encryption or masquerading of the IMSI and other security mode commands exchanged between eNodeB and the UE. Thus, providing encryption between the UE and eNodeB should mitigate the attack.

The proposed solution encrypts the messages between the UE and eNodeB and adds a challenge response mechanism between the former and later. In 4G LTE communication, during the authentication phase the HSS generates the *Authentication vector* and sends it to the UE through MME, then the MME sends *the RAND, AUTN, XRES, K-ASME* to UE to create response message. In the proposed Scheme, the UE is embedded with the temporary key which will be used to access the network through eNodeB for the first time and during the Authentication Phase the MME shares an eK* along with the other information required for creating the *Authentication response*. This *eK** is used as the key for future communication between the eNodeB and the UE.

In the proposed scheme, During the paging procedure when the MME send a paging request for a particular IMSI to the eNodeB. The eNodeB before broadcasting the paging message it encrypts the IMSI and a *random number with eK** and broadcasts the message. The UE in that particular tracking area receives the paging message and then decodes the received message with the shared *eK** during the Authentication Phase.

After decrypting the message, the UE verifies that if the paging message is corresponding to it by looking at the IMSI, if the request is corresponding to that particular UE. Then the UE Encrypts the IMSI and *random number + 1* with *eK** and sends it to eNodeB. Once the eNodeB receives the connection request and encrypted message it decrypts the message and verifies the *random number + 1*. If the random number and IMSI are valid then the eNodeB proceeds further performs *Connection Setup*, if not it drops the connection as shown in Fig. 5.

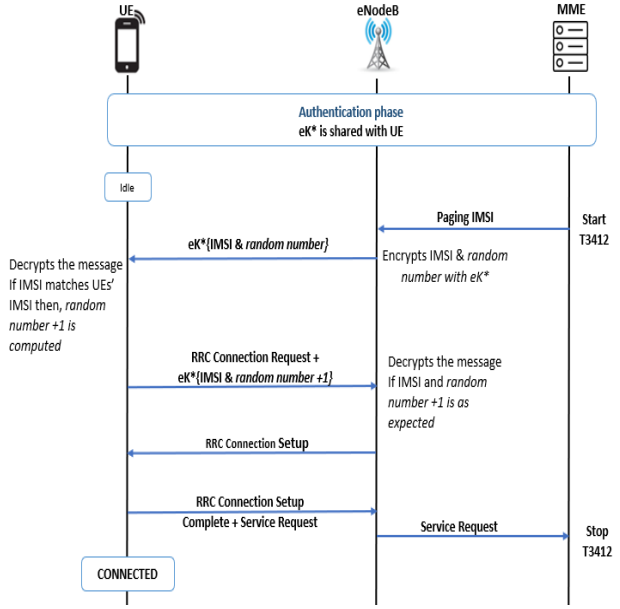

Fig. 5. Proposed Scheme

IV. SIMULATION AND SECURITY ANALYSIS

This Section includes the informal discussion of the security issues comparing the existing and proposed scheme and also simulation of the proposed scheme using NS-3 simulator.

A. Simulation

The proposed Scheme is simulated using the NS-3 simulator which is built using C++ and python. The code for the simulation is written in C++ and makes use of LTE model by the LENA project. The handover of UE from one eNodeB to another authentic eNodeB which consists the paging procedure is simulated in the simulator. A simple substitution cipher encryption algorithm has been employed to encrypt the IMSI using the eK* provided during the authentication phase. Through the outputs of the simulation as shown in Fig. 6.

Fig. 6. Simulation of the proposed scheme

It is observed that it increases a very small computational overhead on the UE and eNodeB. However, the overhead has very small scale impact on the network, which is a trade off for achieving the end to end security in the network.

B. Authentication

The process of proving that the UE and the eNodeB is genuine and valid is known as

Authentication. In the existing scheme there is no way to validate that the UE and the eNodeB is genuine during the paging process. In the proposed Scheme by encrypting the IMSI and the random number it proves that the authentic eNodeB is trying to communicate with the UE.

C. Confidentiality

The Attacks that were mentioned in the previous sections are possible because there is no confidentiality between the eNodeB and the UE, the messages are transferred in the plain text. By adding an encryption scheme to the messages no third person will be able to read the message, which provides the confidentiality.

D. Replay Attack Prevention

As in the proposed scheme the IMSI is encrypted along with the random number the adversary will not be able to replay the messages to the UE or eNodeB. If the messages are replayed the UE and eNodeB will know that the message has been replayed and will stop further communication.

V. CONCLUSION

In this paper, a scheme is proposed to eliminate the malicious eNodeB in the network which encrypts the data communication between the UE and eNodeB during the paging procedure which avoids the transmission of IMSI in plain text which was basis of various attacks on the network in the previous scheme. It is also observed the proposed Scheme does not add much cost over head to the network and also has very minimal impact on the performance of the network by providing confidentiality and also authenticating the UE and the eNodeB. The future work of this scheme can be incorporating methods to provide an efficient key the authentication phase and encryption algorithm during which will further decrease the communication cost during paging procedure due to the addition of encryption to the network.

REFERENCES

1. L. Dhariruman and Dr. Senthil Kumar M, “A time-invariant scheme for handover key management using identity based encryption in 4G long term evolution networks”, International Journal of Control Theory and Applications, vol. 8, no. 5, 2015.
2. H. Syed, C. Omar, M. Shagufta and B. Elisa, “LTEInspector: A systematic approach for adversarial testing of 4G LTE”, Network and Distributed System Security Symposium, 2018.
3. M. Senthilkumar and D. Lavanya, “Prevention of desynchronization attack in 4G LTE networks using double authentication scheme”, Procedia Computer Science, vol. 89, pp. 170-179, 2016.
4. S. Mohapatra, B. Swain and P. Das, “Comprehensive survey of possible security issues on 4G networks”, International Journal of Network Security Its Applications, vol. 7, no. 2, pp. 61-69, 2015.
5. B. Sridevi and M. Divya,“Security analysis of Handover Key Management among 4G LTE entities Using Device Certification”,2015.
6. 3GPP, “3gpp.org”, 2019. [Online]. Available: http://www.3gpp.org/. [Accessed: 07- Mar- 2019].
7. C. Popper and D. Rupprecht, ”Breaking LTE on Layer Two”, 2018

AUTHORS PROFILE

Vignesh Kumar V, He did his Bachelor’s in Computer Science and Engineering . Currently, He is pursuing his final year of M.Tech., in Cyber Security in TIFAC-CORE in Cyber Security, Amrita Vishwa Vidyapeetham University, Coimbatore.

Dr. Lakshmy K. V. Obtained her PhD (Cryptography) from Amrita Vishwa Vidyapeetham. Currently, She is working as an Assistant professor in the TIFAC-CORE in Cyber Security, Amrita Vishwa Vidyapeetham University, Coimbatore.