Security analysis of LTE/SAE networks over E-UTRAN

Mourad Abdeljebbar
Dept. of Multimedia, Signal and Communications System
National Institute of Posts and Telecommunications
Rabat, Morocco
abj.mourad@gmail.com

Rachid ELKOUCH
Dept. of Multimedia, Signal and Communications System
National Institute of Posts and Telecommunications
Rabat, Morocco
elkouch@inpt.ac.ma

***Abstract*—The security is an important issue in the mobile communications such as LTE/SAE systems, especially the mobile users' authentication and key production process which includes the most important risks. In this paper, we survey and compare authentication and key production solutions, namely the traditional solution EPS-AKA (Evolved Packet Switching – Authentication and key Agreement) which we consider as a benchmark solution and the J-PAKE (Password authenticated Key Exchange by Juggling) mechanism, included in the 4G networks by Cristina-Elena Vintilă et al., which have many advantages such as off-line and on-line dictionary attacks resistance, forward secrecy and Known-key security, so that we can show the strengths and weakness of these solutions.**

Keywords—LTE/SAE; EPS-AKA; J-PAKE; Security threats

I. INTRODUCTION

The LTE/SAE system as a 4G network offers many advantages compared to the previous networks like the number of network nodes which is fewer compared to the others networks, which can minimize the protocol processing, latency and increase the security and reliability of communications. In fact, the LTE/SAE architecture contains two main evolved subsystems: Evolved UTRAN (E-UTRAN) and Evolved Packet Core (EPC) (Fig. 1) [1].

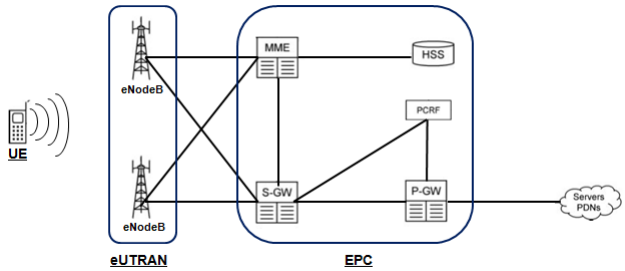

Fig. 1. LTE/SAE architecture.

The E-UTRAN is a set of base stations, called eNodeB, connected directly to mobile users via radio interfaces. The main functionality of these base stations is to forward the users' traffic to EPC with a good management of radio resources. While the EPC is an IP-based network that contains the following five network elements [1]:

1) Home Subscriber Server (HSS): The subscribers' database that contains information about subscription and location of the home operator's mobile users. As well, it contains the necessary parameters to authenticate and communicate with the mobile users.

2) Mobility Management Entity (MME): The main control node in the LTE/SAE system which handles a number of control functionalities, especially the security functionalities. Actually, the MME interacts with the HSS to authenticate the mobile users and then start the security concepts of each one.

3) Packet Data Network Gateway (PGW): It is the contact point of the EPC subsystem with the outside packet networks in order to exchange the mobile users' traffic.

4) Serving Gateway (SGW): The main feature of SGW is to manage the user plan mobility by acting as a router of user data between the eNodeB and PGW.

5) Policy and Charging Rules Function (PCRF): The PCRF is designed to determine policy and charging rules for each service data flow.

Actually, the security has become the most important issue of any communication systems such as LTE/SAE system. Therefore, it should be away from any threats and malicious attacks without influencing its availability, quickness, reliability, integrity, scalability and sincerity. To avoid such situation, the 3GPP has defined a technical specification of SAE security architecture by specifying five security feature groups, as follow [2]:

1) Network Access Security (I): The set of security features in which the mobile user is protected against attacks when it access to the serving network, especially in the radio access link.

2) Network Domain Security (II): The set of security features in which the wired network nodes exchange between each other securely signaling data and user data.

3) User Domain Security (III): The set of security features in which the access to mobile user is secured.

4) Application Domain Security (IV): The set of security features in which the mobile user applications and serving network applications exchange messages securely.

5) Visibility and configurability of security (V): The set of features in which the mobile user informs himself that a

978-1-4673-7689-1/16/$31.00 ©2016 IEEE

security feature is in operation or not and whether the use and provision of services should depend on the security feature.

However, the appearance of new threats and attacks lead us to seek for new solutions or improving the existing ones. Thus, the protection of the authentication process and user's keys are very important in any security process because the weakness of kind of process can affect the whole security of the system. Therefore, our paper is focused to present and compare only two proposed solutions: EPS-AKA protocol and J-PAKE mechanism. For this purpose, we present these solutions in the second and third paragraph while in the fourth paragraph; we will analyze the security of LTE/SAE system according to some security threats when these solutions are used.

II. EPS-AKA PROTOCOL

A. EPS-AKA procedure

As mentioned above, the 3GPP group has defined the security architecture of LTE/SAE network and also the authentication and key agreement procedure, called EPS-AKA, which is similar to procedure used in 3G network but with a few changes such as the use of a master key (KASME) instead of cipher key CK and integrity key IK. In fact, the challenge-response procedure is achieved between the mobile users and MME while authentication parameters are generated in HSS database. This procedure is illustrated and explained bellow [3]:

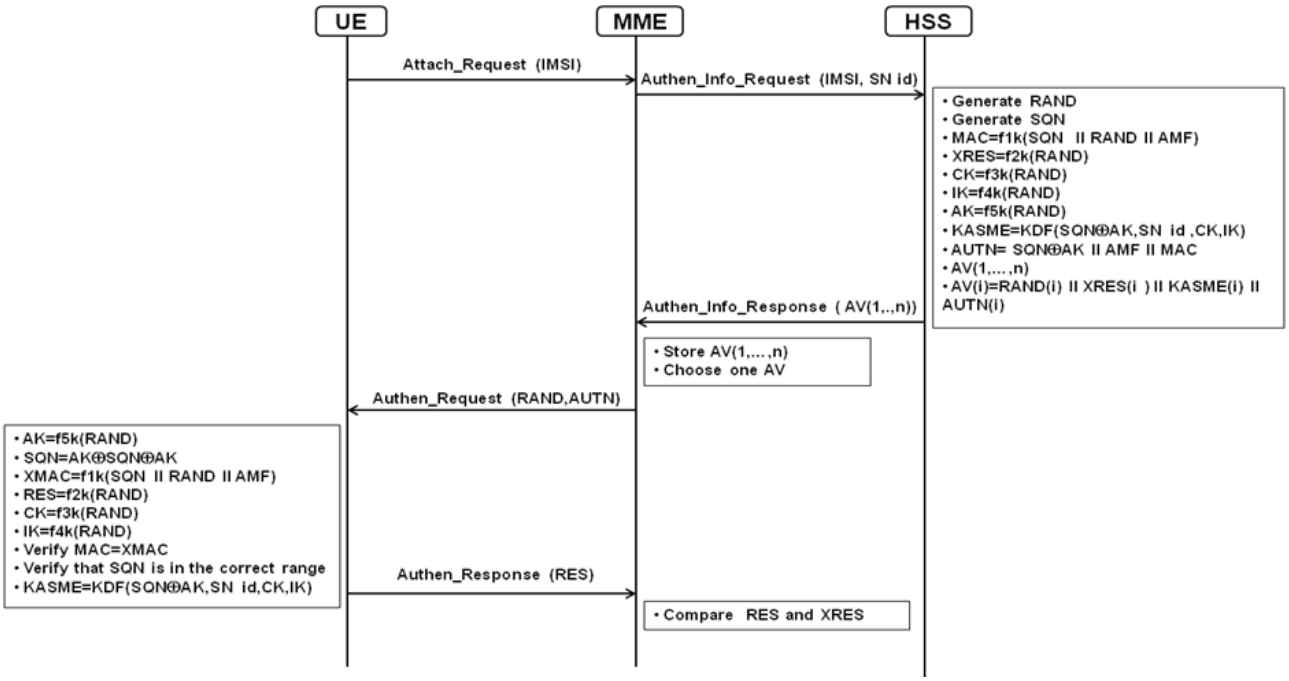

Fig. 2. EPS-AKA procedure.

1) UE ➔ MME: During the initial network access, the UE initiates an authentication request by sending in clear text its permanent identity IMSI to the serving MME. Occasionally, the UE will sends its temporary identity GUTI and tracking area identity (TAI) to MME if a EPS-AKA procedure was did previously.

2) MME ➔ HSS: When the MME receives this request, it forwards this IMSI and its network identity (SNID) to HSS.

3) HSS ➔ MME: Then, the HSS verifies these identities and generates an authentication vectors array if the previous verification was done successfully. Therefore, it shares this authentication array with the MME by the authentication data response message. In fact, each authentication vector contains the following items: one random number RAND, a local master key K_{ASME}, an expected response XRES and an authentication token AUTN.

4) MME ➔ UE: After that, the MME stores these authentication vectors and choose one to answer to UE request in which the value of RAND and AUTN are sent to UE in the response request message. For future authentication, the MME will choose an unused authentication vector from its database or from previous serving MME in case of handover process.

5) UE ➔ MME: Consequently, the UE calculates its AUTN and the value of RES that will be sent to MME.

6) MME/UE: Finally, the UE compares its ATN with the MME's ATN to authenticate the serving network and at the same time MME compares the values of RES and XRES to authenticate the UE. Therefore, if the both comparaison are matched, the authentication procedure is done successfully.

B. EPS-AKA Improvements

In order to prevent EPS-AKA weaknesses several researches were done by improving the initial procedure. Unfortunately, these researches don't cover all malicious attacks, so a strong solution is deeply needed. In fact, bellow seven solutions that have been studied:

1) Enhanced AKA (EAKA): It was proposed by Geir Myrdahl Køien to make the EPS-AKA procedure as a full mutual entity authentication protocol. Therefore, he proposed to replace the current subscriber module USIM by an enhanced one, called Enhanced SIM, add new message elements and redefine the authentication token AUTN [4].

2) HSK AKA: It was proposed by Khodor Hamandi et al. to solve privacy problem and prevent MME masquerading by taking into account the limited energy of the UE's device. In fact, this solution protects the UE's identities (IMSI and GUTI), even at the initial access to network. As well, they proposed to change frequently the UE's temporary identity, even if the user is geographically fixed. Additionally, authenticating the MME can solve the problem of MME masquerading [5].

3) Security Enhanced AKA (SE-AKA): It was proposed by Li Xiehua et al. to enhance the security of the current EPS-AKA by using the Wireless Public Key Infrastructure (WPKI). This solution was made to solve some EPS-AKA weakness such as the disclosure of the user identity and the non-secure link between the MME and HSS with limited energy consumption [6].

4) Improved 3GPP SAE AKA: It was proposed by Yaping Deng et al. to satisfy the basic security requirements and solve some weaknesses of 3GPP SAE AKA. Indeed, they proposed to use a certification mechanism and make some change on the current protocol such as the introduction of the public and secret keys of the involved elements. Therefore, this solution protects the user's identity and authentication vectors in the network domain [7].

5) New EPS AKA: It was proposed by Masoumeh Purkhiabani et al. to remove bandwidth consumption and authentication signaling overhead between serving and home networks, storage space in the serving network, number of complicated hash function computed during the authentication procedure and the incomplete mutual authentication. In fact, the purpose of this solution is to increase a little the computation in the MME and introduce it in the authentication vectors calculation [8].

6) Ensured Confidentiality AKA (EC-AKA): The EC-AKA was proposed by Jacques Bou Abdo et al. to enhance the mobile users' confidentiality and cover some vulnerabilities of SE-AKA by adding two random keys and new random number. As well, they proposed to use the 10 last digits of IMSI instead of the whole number [9].

7) EC-AKA2: It was proposed by Jacques Bou Abdou et al. to solve the problem of IMSI catching and mobile user tracking in which its purpose is to make this solution capable of fortifying vulnerabilities outside EC-AKA's scope of interest. In fact, the new solution differs from EC-AKA in parameters and restrictions [10].

III. J-PAKE PROTOCOL

The J-PAKE, or Password Authenticated Key Exchange by Juggling, is one of the balanced PAKE protocols which use a symmetric key to provide a private and authenticated communication between two participants. Using J-PAKE on the LTE/SAE networks was proposed by Cristina-Elena Vintilă et al. in which the goal is to accomplish two computational rounds between mobile user and MME after validating the mobile user's identity by the HSS. J-PAKE like any PAKE protocols fulfills the following security properties:

1) Off-line dictionary attacks resistance: No information that can be used by an attacker to search for the password off-line is leaked.

2) On-line dictionary attacks resistance: An attacker can only test one password per execution on-line.

3) Forward secrecy: The information still protected even if an attacker discloses the original shared secret.

4) Known-key security: The information is protected with other session keys even if one session key is disclosed.

The procedure of this solution is illustrated and explained bellow [11]:

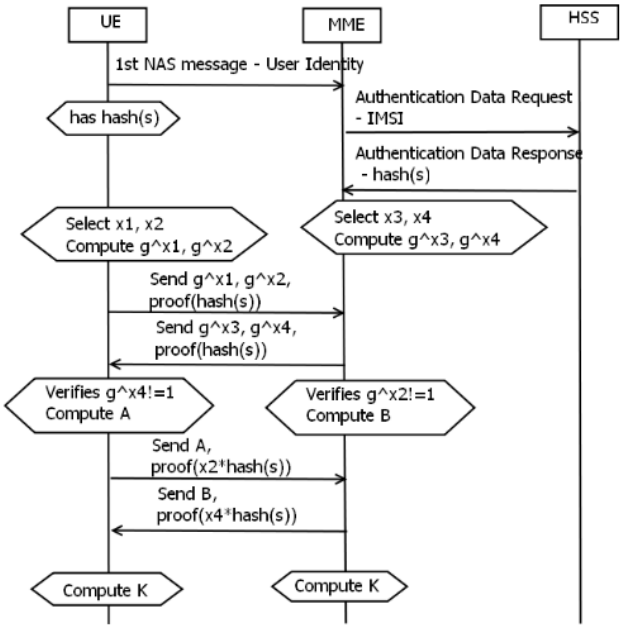

Fig. 3. J-PAKE mechanism in LTE/SAE networks.

1) UE ➔ MME: The UE sends its permanent identity IMSI in the first NAS message to the serving MME.

2) MME ➔ HSS: Thereafter, the MME forwards this identity to HSS in the authentication data request.

3) HSS ➔ MME: Then, the HSS gets the IMSI from the receiving request in order to check that subscriber is located in its databases. If the verification was done successfully, the HSS replays to MME request by sending a secure mobile user secret in the authentication data response.

4) UE ←→ MME: Independently, UE selects two random numbers (x1 and x2) and MME selects also two others random numbers (x3 and x4) provided that x2 and x4 must not be null and all of the four numbers are elements in a group G.

5) UE → MME: Then, the UE calculates g^x1 and g^x2 in which g is the generator of the group G and then sends its values to MME with the secured UE's secret.

6) MME → UE: At the same time, the MME calculates g^x3 and g^x4 and then sends its values to UE with the secured UE's secret which was received from HSS.

7) UE → MME: After that, the UE verifies that the receiving value of x4 is not null and then calculates A=g^(x1+x3+x4)*x2*hash(s) which is sent to MME with the value of x2*hash(s).

8) MME → UE: At the same time, the MME verifies that the receiving value of x2 is not null and then calculates B=g^(x1+x2+x3)*x4*hash(s) which is sent to UE with the value of x4*hash(s).

9) UE ←→ MME: Finally, both of them calculates the value of K in which K=(B/(g^(x2*x4*hash(s))))^x2 for UE and K=(A/(g^(x2*x4*hash(s))))^x4 for MME. If this values are equal to g^(x1+x3)*x2*x4*hash(s), the UE and MME derive the same session key k from the previous K. This session key k is used to derive CK and IK as the 3GPP specification.

IV. LTE/SAE SECURITY ANALYSIS

In general, the LTE/SAE networks like any communication networks present many threats and vulnerabilities. Moreover, there are four specific groups of these issues which concern system architecture, access procedure, handover procedure and interworking procedure. In this paper, we will not go through all of these four groups but only the access procedure threats that will be studied. Furthermore, the analysis bellow has been done by explaining each threat and its effect on EPS-AKA protocol and J-PAKE mechanism:

1) IMSI leakage: The UE sends its permanent identity (IMSI) in plaintext during the first access to network and when the MME ask them to send it. Thus, this is the case for both EPS-AKA procedure and J-PAKE mechanism which may affect the authentication process of the UE when this identity is caught by an attacker. For that, the user identity must be confidential to the third parties [6] [11].

2) SNID leakage: In case of EPS-AKA procedure, the transmission of SNID over both air link and wired link is in plaintext. In fact, an attacker can easily get this identity and then starts the attacks by impersonating this serving network. Therefore, the SNID should be protected in the air interface and even in the wired link. However, the J-PAKE mechanism does not use any information to specify the serving network, so it is not protected against attacks from malicious networks [6] [11].

3) GUTI Tracking: The radio channel is susceptible to be eavesdropped, so an attacker who can catch the mobile user identities such as the temporary identity (GUTI) can be easily tracked. Therefore, a fake eNodeB can use this identity to force the UE to send its permanent identity (IMSI) and then influence the confidentiality of this mobile user [10].

4) Key leaked: Generally, the cipher and integrity keys are used to derive the mobile user's session key. In EPS-AKA, this key is calculated during the authentication process while in J-PAKE procedure it is calculated after the successful authentication process. Thus, the attacker who gets this session key can communicate easily with the mobile user and the serving network, and then influence the communications' process security. Therefore, this common key must be away from the third parties [6] [11].

5) Link leakage: Usually, the wired links between network entities are not protected like the links between HSS and MME. Accordingly, an attacker can affect the mobile user's security, mainly in case of MME and HSS are belongs to different networks. In EPS-AKA procedure, the authentication vectors are sent from HSS to MME in plaintext, so it is easy for an attacker who can affect these links to intercept these vectors. Therefore, a fake MME can affect the mobile users privacy. In J-PAKE procedure, the shared mobile user secret between MME and HSS is secured by a hash fonction, thus it is protected [6] [11].

6) Traffic redirection: In EPS-AKA protocol, the UE authenticates the HSS and MME authenticates the UE but the UE doesn't authenticate MME and also MME doesn't authenticate HSS. On the other side in J-PAKE mechanism, the authentication is done between UE and MME without authenticating the HSS. Therefore, an attacker can redirect easily user traffic from one network to another. To avoid such situation, each entity should be authenticated by the others [7] [11].

7) Denial of Service (DoS): The DoS attack is an attempt to make the network resources unavailable to its intended users, thus the transmission of traffic between users and the network will be prevented. In fact, the first round in both EPS-AKA and J-PAKE can be easily completed by an attacker because the MME forwards the receiving request from UE to HSS without any verification although it may have a wrong information. This weakness can prevent the access to network as in case of a brutal attack. Therefore, the session connection between mbile users and network must be away from attackers [11] [12].

V. CONCLUSION

In this paper, we have described the EPS-AKA procedure and J-PAKE protocol as a solution for the authentication process in the LTE/SAE networks, although these are not the only solutions that exist but other propositions may exist. Yu Zheng et al. in their article titled "AKA and Authorization Scheme For 4G Mobile Networks Based on Trusted Mobile Platform" published on the 5th International Conference on Information Communications and Signal Processing held in Bangkok between 6 and 9 December 2005, have proposed a hybrid AKA in which the Trusted Mobile Platform is used to authenticate mobile users. The purpose of this solution is to

combine between user's fingerprint and USIM's public key as a mobile user's secret. However, in our case we have analyzed the safety of EPS-AKA and J-PAKE according to access procedure threats in which we concluded that both of them are sensible to attacks. This will be the object of the next article in which we will propose a new solution that will minimize the malicious attacks.

REFERENCES

[1] C. Cox, An introduction to LTE LTE-advanced SAE and 4G mobile communications, 1st ed., A John Wiley & Sons Ltd., 2012.

[2] 3rd Generation Partnership Project, 3GPP TS 33.401 V12.14.0 (2015-03), 3GPP System Architecture Evolution (SAE) / Security architecture (Release 12).

[3] D. Forsberg, G. Horn, W.D. Moeller, and V. Niemi, LTE Security, 2sd ed., A John Wiley & Sons Ltd., 2013.

[4] G.M. Koien, "Mutual entity authentication for LTE," 7th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 689-694, July 2011.

[5] K. Hamandi, I. Sarji, A. Chehab, I.H. Elhajj, and A. Kayssi, "Privacy Enhanced and Computationally Efficient HSK-AKA LTE Scheme," 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 929-934, March 2013.

[6] L. Xiehua, and W. Yongjun, "Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network," 17th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), pp. 1-4, Septmber 2011.

[7] Y. Deng, H. Fu, X. Xie, J. Zhou, Y. Zhang, and J. Shi, "A novel 3GPP SAE Authentication and key agreement protocol," IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC), pp. 557-561, November 2009.

[8] M. Purkhiabani and A. Salahi, "Enhanced Authentication and Key Agreement Procedure of Next Generation Evolved Mobile Networks," 3rd International Conference on Communication Software and Networks (ICCSN), pp. 557-563, May 2011.

[9] J.B. Abdo, H. Chaouchi, and M. Aoude, "Ensured Confidentiality Authentication and Key Agreement Protocol for EPS," Symposium on Broadband Networks and Fast Internet (RELABIRA), pp. 73-77, May 2012.

[10] J.B. Abdo, J. Demerjian, H. Chaouchi, and G. Pujolle, "EC-AKA2 a revolutionary AKA protocol," International Conference on Computer Applications Technology (ICCAT), pp. 1-6, January 2013.

[11] C.E. Vintilă, V.V. Patriciu, and I. Bica, "A J-PAKE based Solution for Secure Authentication in a 4G Network," World Scientific and Engineering Academy and Society (WSEAS), pp. 42-47, 2011.

[12] L. Gu, M.A Gregory, "A Green and Secure Authentication for the 4Th Generation Mobile Network," Australasian Telecommunication Networks and Applications Conference (ATNAC), pp. 1-7, November 2011.