Robust Crypto Authentication and Key Agreement Protocol

Poonam Saini
Department of Computer Applications, National Institute of Technology Kurukshetra, Haryana, India

Ritu Rani
Department of Computer Applications, National Institute of Technology Kurukshetra, Haryana, India

Hitesh Sharma
Department of Computer Applications, National Institute of Technology Kurukshetra, Haryana, India

Sandeep Kumar
Department of Computer Applications, National Institute of Technology Kurukshetra, Haryana, India

Abstract – This paper presents a advanced security in next generation network (4G or 5G) all are based on IP and supports very high data rates which make them more susceptible to various attacks such as revelation of user personal information, man-in-middle attack(MITM), stingray phone tracking etc. Due to several flaws in the existing mutual authentication protocol, which lets user equipment (mobile, laptop etc) communicate securely with the subscriber's cell network (evolved -Base station (eNB)). For remediation from such security and privacy violation, this paper presents a robust and efficient protocol named, Robust Crypto Key Authentication and Key Agreement (RC-AKA) protocol, which uses RSA algorithm to secure IMSI number and asymmetric key Cryptosystem to secure user personal data, intermediate control plane data and for Sequence Number (SQN) synchronization. This is a preventative protocol which LTE can adept to enhance its security architecture. This paper provides a formal verification of results, which proves that this protocol is more secure, and resistance to prevailing attacks in fourth generation networks.

Index Terms – Access stratum (AS), EPS-AKA, IMSI number, LTE, MITM, Non-Access stratum (NAS), RC-AKA , RSA, Stingray phone tracking.

1. INTRODUCTION

Due to high pace of growth in wireless network technologies and increase demand for high data rates, more reliability and security for internet and multimedia services like video streaming, games, online TV and music etc., a large set of world population is moving towards Long Term Evolution (LTE) technology which is supported by 4G or Next Generation Networks(NGN). 4G network has many key difference from previous generation networks like 2G, 3G, UTMS etc because it all-IP and some other technology like MIMO etc. made it eligible to provide several feature like high data rate, better spectral efficiency, higher security, mutual authentication, lower latencies etc. Due to all-IP nature, it is vulnerable to a number of privacy attacks. Unlike architecture of previous generation network, it is made up of two-part core network named EPC (Evolved packet core) and E-UTRAN (Evolved Universal Terrestrial Radio Access Networks). Furthermore, E-UTRAN consists of evolved base station eNB which communicate with user equipment (UEs**)** [1] in every cell. To establish a network connection UE and eNB must mutual authentication with each other, this feature is note present in UTMS which makes UTMS more easy to be exploited by various attackers, and attack such as impersonation attack, MitM attacks [2], stingray attack, rogue base station attacks [3] and Deny of Services (DoS) attacks [4], IMSI thefts etc. so that these shortcoming of note to be inherited in NGNs, Mutual authentication feature is added to LTE technology. For authentication, any key agreement UTMS uses UTMS-AKA protocol and to provide mutual authentication where LTE uses magnifical UTMS-AKA, which is, known by the name EPS-AKA protocol [5]. Now as well LTE is not completely secured it also contains many loopholes, which hackers try to exploit very often to remove this loopholes various studies are taking place. There are several paper, which published various security threats of LTE [6]-[9]. In paper [6] an overview of these loop holes of 4G network is given. In this paper, security architecture of LTE is studied and a simulation tool is suggested for such type of network to further analyze the problem of LTE technology and it is also gives a brief overview of the weaknesses of prevailing and widely used LTE technology. This paper also pointed out the problems when UE try to access network due to heterogeneous and ALL-IP network of LTE technology. In one other paper, the complete architecture of LTE is explained [7], along with EPS-AKA procedure which LTE used for secure connection established and data transfer between UEs and eNB network. After discussing them, loopholes of EPS are explained along with experimental results, which prove their authentication. This studies proves that 4G is also not completely secure it also have several weak point which need to be addressed for more security such as Key Derivation Function (KDF), secure keys generated in between UE and core network, cipher key , SQN number, RAND,IMSI number and so on. An analysis of Challenges in the advance networks and advance security of 4G networks has been offered in [8]. After analyzing, the security threat of LTE networks specified possible vulnerabilities connected with the LTE systems. The survey of security points of 4G systems at application layer has been discussed in [9]. In addition, some secure strategies for 4G mobile networks system with IPv6 networks has been suggested in [9].

In 4G LTE system architecture evolution (LTE/SAE) [10], also known as EPS is all IP System. The EPC contains the mobility management entity (MME), Home Subscriber Server (HSS), policy and charging rules function (PCRF), the serving gateway (SGW) forwards and route packets and handle inter and intra-handover connectivity across eNBs, and the packet data network (PDN). Another part of LTE Network is Access Network, which is the network of eNBs also named as E-UTRAN.

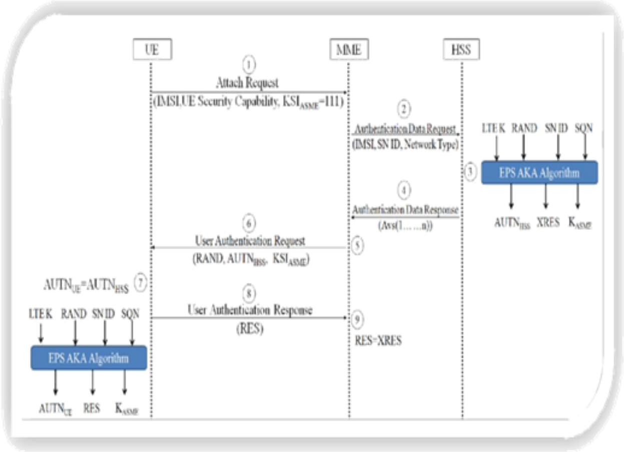
UE
MME
HSS
1
Attach Request
(IMSI,UE Security Capability, KSI_ASME=111)
2
Authentication Data Request
(IMSI, SN ID, Network Type)
LTE K RAND SN ID SQN
3
EPS AKA Algorithm
AUTN_HSS XRES K_ASME
4
Authentication Data Response
(Avs(1……n))
5
6
User Authentication Request
(RAND, AUTN_HSS, KSI_ASME)
AUTN_UE=AUTN_HSS
7
8
User Authentication Response
(RES)
9
RES=XRES
LTE K RAND SN ID SQN
EPS AKA Algorithm
AUTN_UE RES K_ASME

Fig. 1 LTE for EPS-AKA

For providing mutual authentication between user and the core network LTE uses EPS-AKA protocol, which is the latest version of the UMTS-AK. This protocol generates all cipher and integrity key needs for encrypting the data sent over the network, using a key derivation function. The main components of this protocol are Subscriber Identity Number, eNBs, MME and HSS as shown in fig.1 [1]. This protocol comes into play when MME sends a user identification request to the User Equipment or subscriber for establishing a connection.

2. RELATED WORK

Many research works are going on to improve the performance of EPS-AKA protocol some of them includes protection from certain type of attacks such as subscriber identity disclosure, MitM, DoS etc. some of the solution has been presented in the following paper:

Efficient EPS-AKA protocol is proposed in [1]. This protocol is based upon one of the strong EAP protocol named simple password exponential key Exchange (SPEKE) protocol. The proposed protocol improves the SPEKE protocol to protect IMSI and generate strong key which is shared among UE, MME and HSS. This method uses symmetric cryptographic method so authentication delay and storage overhead is reduced.

Analyze of EPS-AKA protocol and its security threat is describe in [11]. It proposed new authentication model to deal with the security threat of EPS-AKA. It proposed a improve approached based on Diffe-Hellmen Algorithm to secure the RAND which is used for generating a number of key to secure data and user information. Author also present a pair key mechanism to generate all parameters i.e. two input are required to generate parameters and two dimensional operation which make this protocol secure from brute force and other attacks.

3. PROPOSED MODELLING

The proposed protocol uses the essentials of RSA asymmetric Cryptography Algorithm with some modifications to secure IMSI number from being stolen by the false base stations and IMSI catchers by generating several powerful encrypted key between UE, MME and HSS. This protocol comes into play when MME sends the attach request to the UE in response to this user identity request UE sends its user identity in encrypted form Temporary subscriber mobile identity (TMSI).

The minutiae of the proposed protocol is shown below

1. MME computes its shared key K_{um} by steps
   - Generate two random prime numbers R_p and R_q
   - Then calculate $N = R_p * R_q$
   - Calculate λ =LCM $(R_p - 1)(R_q - 1)$
   - Choose a random prime number K_{UM} $(1< K_{UM} < \lambda)$
   - And the user identity attach request to UE along with this K_{UM}
2. Now at UE ,UE compute its private key K_{UE} and use it to encrypt IMSI by
   - Generate two random prime numbers R_p and R_q
   - Calculate $N = R_p * R_q$
   - Calculate λ =LCM $(R_p - 1)(R_q - 1)$
   - Then compute $K_{UE} = e^{-1}(\mathrm{mod}\ \lambda)$

- TMSI = (IMSI) ^ K_{UM} (Mod N) and forward it to MME

3. Upon receiving subscriber unique identity response message, MME forwards (K_{UM}, TMSI, R_p and R_q) to HSS.
4. Then HSS retrieve IMSI number from TMSI using (K_{UM} ,TMSI ,R_p and R_q)
    - Generate RANDOM
    - Calculate MAC=f1 (K, SQN_H, RANDOM)
    - Calculate expected response (XRES) =f2 (K, RANDOM)
    - After that several keys are calculated
    - Cipher Key (CK) = f3 (K, RANDOM)
    - Integrity Key (IK) = f3 (K, RANDOM)
    - Authentication Key (AUTN) = SQN_H || MAC
    - Session Key (K_{asme}) = KDF (CK, IK, SNID), where KDF is a key derivation function.
    - Then AV is computed using (RANDOM, AUTN, XRES and Kasme)
    - Forward AVs to MME
5. HSS response to MME by sending AVs which are computed in above step.
6. Now MME sends a User Authentication Request which contains ERAND, AUTN and KSIasme and it is used to identify Kasme. Here MME encrypt RANDOM with the help of KUE and form ERAND.
7. On receiving the message UE obtain SQN_H and generates the XMAC and for freshness reasons match it with the MAC received in AUTN, then it checks the SQN_H received from HSS with its SQN if any of the two checks fails it sends errors otherwise it computes the response RES and sends it to MME and computes the Kasme .

4. SIMULATION

For simulation of network related protocol we use Omnet++ 5.0. OMNeT++ is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators**.** OMNeT++ provides component architecture for models. Components *(modules)* are programmed in C++, and then assembled into larger components and models using a high-level language *(NED)*. Reusability of models comes for free. OMNeT++ has extensive GUI support, and due to its modular architecture, the simulation kernel (and models) can be embedded easily into your applications. As it's all components are built in c++ so we build our protocol in c++. For this we use a laptop of 8GB RAM with Windows 10 and Quad Core processor, and Dev-C++ 4.11 installed.

Module 1:- Implements RSA algorithm with modification to secure IMSI number

Module 2:- Generate LTE Network in Omnet++ where one node send packet to another

Module 3:- Generate various keys and Authentication vectors for implementing proposed algorithm

5. RESULTS AND DISCUSSIONS

When we create an LTE network we need some User Equipment and a core network named as EPC. After creating the LTE we secure IMSI and RAND by asymmetric key cryptosystem which protect it from various user identity attacks and stingray attack. AVs are successfully created and transmitted over network which carry encrypted keys required for successful connection establishment.

Using the time taken by RSA to secure data we plot a graph between our algorithm and Diffe Hellmen algorithm which proves that our algorithm is more secure than later one as shown in Figure 2.

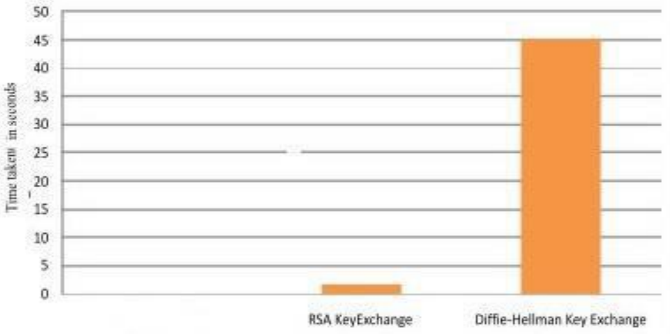

Fig. 2 Comparison b/w RSA and DH algorithm

Also by increasing key length for RSA we can increase its decryption time as shown in graph of Figure 3 which makes it a lot tougher for hackers to crack.

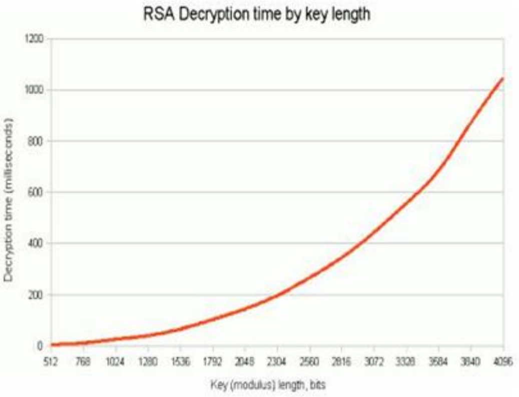

Fig. 3 RSA description time by key length

6. CONCLUSION AND FUTURE SCOPE

Despite its security and effectiveness EPS-AKA does not provide full security from various threats like user identity threats, DoS, DDoS, signalling overhead, stingray phone tracking etc. User identity can be revealed by decrypting the IMSI which is sent in clear text in the connection establishment phase. Additionally forward confidentiality is not fully provided as the primary key can be accessed by getting RAND number sent between UE and HSS.

The Proposed algorithm removes prevailing security threats by securing IMSI by using RSA which prevents the user identity attacks, Several other attacks like MITM, Replay, DoS and DDoS. Stingray phone tracking etc. It is prevented by securing RAND number sent between UE and HSS using RSA algorithm or by using pair key method. Modified version of this protocol can be used in Next Generation Networks (NGNs) like 5G for securing connection establishment phase.

REFERENCES

[1] K.A. Alezabi,, F. Hashim,, S.J. Hashim,, B.M. Ali, " An efficient authentication and key agreement protocol for 4G (LTE) networks", Region 10 Symposium, 2014 IEEE,2014.

[2] U. Meyer and S. Wetzel, "A Man-in-the-Middle Attack on UMTS," Proc. 3rd ACM Workshop on Wireless Security, Octomber 2004, pp. 90-97

[3] M. Zhang and Y. Fang, "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans. Wireless Commun., Vol.4, No.2, Mar. 2005, pp. 734- 742.

[4] C. Tang and D.O. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks," IEEE Trans. Wireless Commun., Vol.7, No.4, April 2008, pp.1408-1416

[5] K.A. Alezabi,, F. Hashim,, S.J. Hashim,, B.M. Ali, "T. G. P. P. (3GPP): 3g system architecture evolution (sae); security architecture (release 8), in 3GPP TS 33.401 v8.2.1" 2009.

[6] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks," Proc. IEEE Globecom Workshops, November 2007, pp.1-6..

[7] C.B. Sankaran, "Network Access Security in Next-generation 3GPP Systems: A Tutorial," IEEE Commun. Mag., Vol.47, No.2, February 2009, pp.84-91.

[8] N. Seddigh, B. Nandy, R. Makkar, and J.F. Beaumont, "Security Advances and Challenges in 4G Wireless Networks," Proc. Eighth Annual International Conference on Privacy Security and Trust (PST), August 2010, pp.62-71.

[9] J. Zheng, "Research on the Security of 4G Mobile System in the IPv6 Network," Recent Advances in Computer Science and Information Engineering, Vol. 126, 2012, pp. 829-834.

[10] M. Aoude,, H. Chaouchi,, J.B. Abdo, "3rd Generation Partnership Project, 3GPP TS 33.401 V11.2.0 (2011-12), 3GPP System Architecture Evolution (SAE); Security architecture (Release 11)", 2012.

[11] F.Y. Leu,, I. You, Y.L., Yim, K. Huang,, C.R. Dai, " Improve the security level of LTE authentication and key agreement procedure", 4th IEEE International Workshop on mobility Management in the Network of the future World, 978-1-4673-4941, IEEE,2012.