ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/282023158

Improving LTE EPS-AKA using the security request vector

Conference Paper · June 2015

DOI: 10.1109/ECAI.2015.7301207

CITATIONS
4

READS
438

2 authors:



Cristian-Gabriel Apostol
Technical Military Academy of Bucharest
10 PUBLICATIONS **20** CITATIONS
SEE PROFILE



Ciprian Racuciu
Titu Maiorescu University
34 PUBLICATIONS **92** CITATIONS
SEE PROFILE

All content following this page was uploaded by Cristian-Gabriel Apostol on 27 September 2015.

The user has requested enhancement of the downloaded file.

ECAI 2015 - International Conference – 7th Edition
Electronics, Computers and Artificial Intelligence
25 June -27 June, 2015, Bucharest, ROMÂNIA

Improving LTE EPS-AKA using the Security Request Vector

Cristian-Gabriel Apostol
Electronics and Telecommunications Department
Military Technical Academy
Bucharest, Romania
Crs.Apostol@gmail.com

Ciprian Răcuciu
Informatics Department
Titu Maiorescu University
Bucharest, Romania
Ciprian.Racuciu@gmail.com

***Abstract* – Nowadays the telecommunications industry focuses on two user requirements: increased data-rates at high speed mobility and robust network security. The emerging technology for these milestones is the 3GPP Long Term Evolution standard and the LTE-Advanced improvement of this standard. The paper describes the main features of these modern networks and conducts an analysis on the LTE EPS-AKA proposing an improvement to address the Denial of Service attacks pointed out by researchers in the last years.**

Keywords-EPS-AKA, LTE, Denial of Service, 4G security, Security Request Vector, Authentication, HSS protection.

I. INTRODUCTION

The request for high speed data rates of mobile applications has been the background for developing the new 4G technologies. Providing increased data rates at high speed movement of the UEs, with a reduced cost of implementation has pushed the 3GPP community to develop new radio interfaces like OFDMA and SC-FDMA, used in today's mobile networks. Also we can see a high necessity for data and network security because sensitive medical, financial, governmental and personal information is sent through these new networks.

In order to provide efficient and sufficient network security, security policies and mechanisms should regard the best practices in the telecommunications industry. The network security architecture should regard two principles. First of all hierarchical defense should be considered and then further developments should apply deep defense principles. The first concept aims to execute security policies in multiple areas of the network by using various methods to ensure that no single point failure can occur in the network. Deep defense provides further protection, thus improving network security. Deep defense uses the multiline defense policy to manage risks. When one line of defense is broken, another line of defense prevents the system from being damaged. The security system needs to be planned hierarchically and from outside to inside – from the network border to the internal network and to the core servers. In this paper we will focus on a deep defense improvement of LTE/LTE-Advanced networks.

When implementing security in a communication network, it is useful to divide signals into different data flows like management, control and user plane as specified in the ITU-T X805 general security model. Each plane consists of network devices, connections and network applications. Furthermore each plane can be divided into device layer, network layer and application layer. With the plane based, hierarchical security architecture model, we have the possibility to analyze the security threats of 4G networks and provide corresponding security policies and solutions.

As the control center of all security mechanisms, security management provides the mechanisms such as security policy management and event collection, analysis, and response.

II. 4G NETWORK ARCHITECTURE

Long Term Evolution or LTE is a new cellular standard which evolves from the 3GPP family, defining a simplified all IP based network model composed of the System Architecture Evolution (SAE) and the Evolved Packet Core (EPC).

The Radio Access Network introduces a new entity, the evolved Node-B (eNB), the major component of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN). This entity handles the radio requirements independently, in comparison to the BTS/NodeB elements of 2G/3G which need the specific standard controllers BSC/RNC. Also new direct communication interfaces between these base stations are defined, the X2 interfaces which allows direct communication and IP based handover between two or more eNodeBs. The X2 interface supports the exchange of signaling information between eNodeBs and it also supports forwarding of PDUs to the peers of the tunnel. Even if two eNodeBs are not directly connected physically, the X2 interface is established using the backhaul network between the Base Stations. It also offers the possibility of handover and direct communication between the network entities which are produced by two different vendors, thus achieving one of the main objectives of this standard which required the definition of open interfaces for all vendors.

The EPC can contain one or more Mobile Management Entities (MMEs), Serving Gateways (S-

GW) and also Packet Data Network Gateways (P-GW), depending on the size of the network and one Home Subscriber Server (HSS) which can be doubled for redundancy.

The MME is responsible for NAS signaling, NAS signaling security, inter core network node signaling between 3GPP access networks terminating the S3 interface. Also the MME holds the Tracking Area List for the UEs and it also selects the S-GW and P-GW for the UE user plane.

Besides all these important features and others defined in the 3GPP LTE standard, for our paper the significant features are represented by user authentication and authorization. The S-GW and P-GW are used to transfer traffic from and to the user, after being allocated by the MME. An important aspect is that user traffic after authentication does not cross the MME, being routed directly by the eNodeB to the SGW and furthermore to the PGW. If lawful interception will be implemented, these are the points in which the user traffic can be monitored. The Serving GW is the termination point of the packet data interface towards E-UTRAN. When the UEs move between eNodeBs, the Serving GW takes the role of the local mobility anchor. This means that packets are routed by this entity for intra and inter E-UTRAN mobility.

The P-GW is similar to the S-GW, the difference is that it represents the termination of the user plane in the LTE network, and the gateway to exterior fixed/mobile data networks. It's also responsible with applying the operator's defined rules for allocating resources.

The HSS server can be seen as a merging server between the Home Location Register (HLR) and the Authentication Center (AuC), two functions present in 2G and 3G networks. The HLR part consists of a database which stores user subscription information, user profile information (service subscriptions, the QoS defining the Committed Information Rate (CIR) and Maximum Information Rate (MIR) for the services) and the mobile telephone number (MSISDN). The AuC part of the HSS is the other entity followed up by our paper, because it regards the generation of the Authentication Vector (AV) used for mutual authentication between the user and the network, ciphering and integrity protection on the radio link.

In recent years a Security Gateway (Se-GW) has been introduced in the network to provide core network protection and IPSEC encrypted traffic between the eNodeB and the Core Network.

The PCRF (Policy and Charging Rules Function) Server is in charge of managing each user session and accounting rule. Compared to UMTS the PCRF is a combination of the Policy Decision Function (PDF) and the Charging Rules Function (CRF).

In the PDF network entity, policy decisions are made. During an IMS session setup, media requirements of SIP signaling are exchanged between the UE and the Proxy-Call Session Control Function P-CSCF. During session establishment, the PDF receives the connection requirements from the P-CSCF and decides the connection feature based on: Approval or denial of media requests, creating a new or using an existing PDP context for an incoming request and verifying the new resources capabilities compared to the maximum authorized MIR. The main role of the CRFs is to provide operator specific charging rules for each user service flow. The CRF selects the application identifier, service type (audio, video) and sustained data rate which are provided by the P-CSCF.

The main components of the LTE Network and the interfaces used for interconnections are described in "Figure 1".

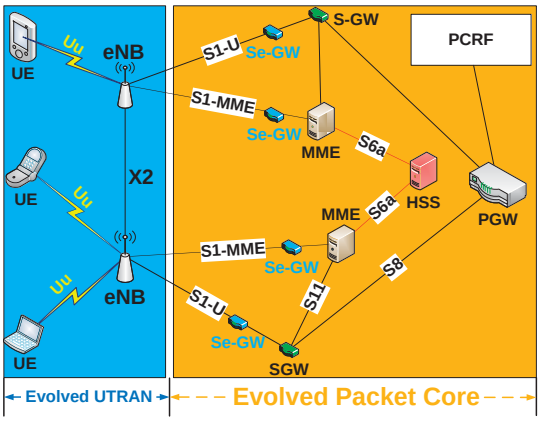


Figure 1: LTE network architecture model

III. Existing Network Security

The 3GPP2 Long Term Evolution communications standard, describes two types of security, depending on its place in the network, as described in "Figure 2". The Access Stratum (AS) Security focuses on the radio access link while the Non Access Stratum Security acts between the UE and the core network.

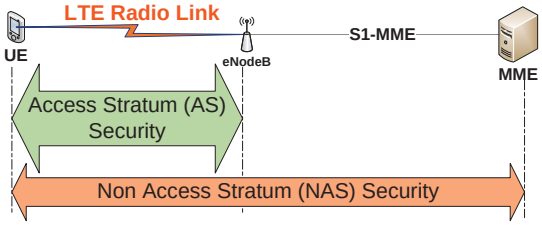


Figure 2: AS and NAS Distribution in LTE Networks

In LTE the authentication method, named EPS-AKA (Evolved Packet System – Authorization and Key Agreement), is a development of 3G AKA (UMTS AKA), not being a totally new authentication method. The main reason for this is good interoperability with the existing technologies and low cost of implementation for the 4G networks.

EPS-AKA is very similar to the more than 20 years old GSM AKA protocol, with slight improvements. One of the main problems with this family of protocols is that they are delegated protocols. This means that the authentication is delegated from the home network to the visited network. [2] Also the

protocol is vulnerable to DoS attacks, as specified in [1], the point in which this improvement is based on.

The AKA security mechanism is based on a secret key shared between the subscriber USIM card (Universal Subscriber Identity Module) and the AuC (Authentication Center). The keys are different for each and every subscriber, in order to provide data confidentiality and authentication. During the protocol's development, in order to meet the new 4G security requirements, the following targets were considered [3]:

- *Full mutual authentication between the MS and the LTE network.*
- *Ciphering (CK) and Integrity keys (IK) generated by the USIM in the user part, not transmited on the air interface.*
- *Strong key separation.*
- *MME receives from HSS only KASME, and not the specific keys (IK and CK).*
- *Ciphering at AS (signalling and data) and NAS (Non Access Stratum) level.*
- *Integrity protection for both AS and NAS*

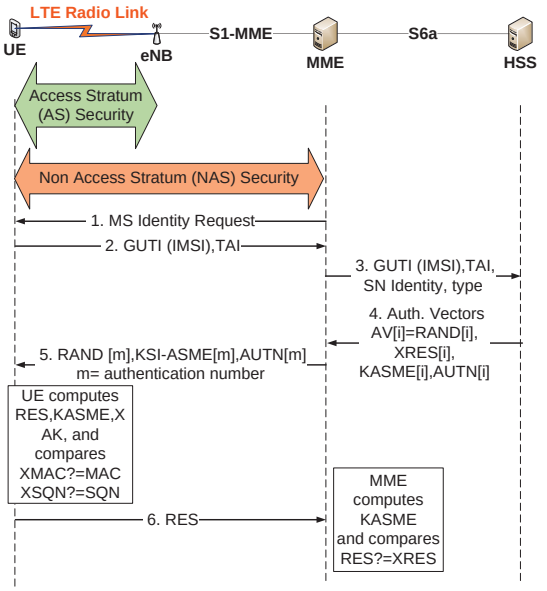


Figure 3: EPS-AKA Authentication Process

The LTE authentication is described as the following [4]:

a) The UE sends to the MME the Attach Request (IMSI, Security capability, key set identifier KSI-ASME).

b) MME forwards the authentication data request to the HSS, and also the server network identity (SNID) and the type of network (wired or radio).

c) The Home Subscriber Server (HSS) authenticates the Service Network Identificator (SNID), gets the UE coresponding security key from its database and computes this parameter with a chosen sequence number (SQN) and a random number (RAND) generating the authentication vector AV. The AV is composed by four parameters: XRES (expected response from the UE), authentication token (AUTN), RAND and KASME. The functions and parameters involved in the AV generation are described in "Figure 4".

d) HSS sends the AV to the MME.

e) MME sends the authentication request to the UE, including RAND, AUTN and KSI-ASME. The last parameter is used by the UE to generate an identical K-ASME as the one used by the HSS.

f) UE authenticates the MME (network). It uses f1 to generate XMAC and compares it with the MAC in the received AUTN.

g) UE uses f2 to compute RES, and also generates CK using f3(RAND) and IK using f4(RAND).

h) The UE sends the RES authentication response to the MME.

i) MME compares UE RES with HSS XRES, and if they coincide the UE becomes succesfully authenticated. If they are different, MME discards the connection to the UE.

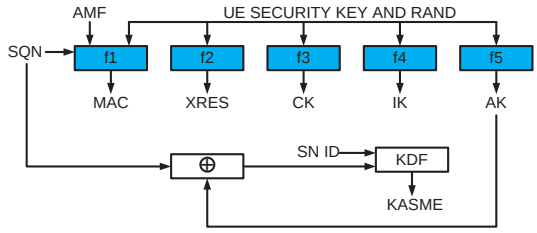


Figure 4: The generation of AV [4, 8, 9]

Based on these specified targets, we can point out two phases of the EPS-AKA protocol. First we have the generation and distribution of the authentication information from the HSS to the MMEs and secondly the mutual authentication process between the UE and MME.

IV. Proposed Improvements EPS-AKA With Security Vector (EPS-AKASV)

As we can see in step *c)* of EPS-AKA, illustrated in "Figure 3" before sending the AV, the HSS computes directly the authentication vector. It does not have a measure to protect itself against malicious attacks from the UEs. Also this vulnerability was specified in [5-6], stating that the access protocol used in LTE, known as the EPS-AKA scheme cannot prevent Denial of Service (DoS) attacks. The MME must forward the UEs requests to the HSS before the UE receives the authentication acknowledgement from the network. In addition the MME can only authenticate the UE after the calculated RES has been received from the UE, which obtains the value by computing the authentication vector received from the HSS.

Based on these specifications of EPS-AKA, an attacker can use a legitimate UE to constantly send fake IMSIs in order to overload the HSS/AuC. This will consume processing power and overwhelm the memory buffer. Furthermore it can lead to a service shut-down of the HSS after a certain period of time, depending on the number of attacks and the hardware and software specifications of the HSS.

This means that this vulnerability of EPS-AKA can be sustainable to DoS attacks in real life, with no protection for the HSS.

We propose EPS-AKA with Security Vector in which the HSS first compares if it has already received an authentication requests from the same hardware address of the UE, before computing the Authentication Vector. The physical address of the UE will be stored in the *Security Vector* and if a new request will be found in the security vector, then the HSS/AuC will discard the request from the UE for a predefined period of time. This concept will ensure that a device which is trying to sustain DoS attacks will not overload the HSS/MME.

The security vector will have a length of 300 values for the Physical UE addresses, in order to keep safe the HSS buffer and not to request processing power when verifying if a new IMEI value already exists in the computed requests. The IMEI check is computationally very simple, using two functions "for" and "if" to check whether the new IMEI is in the Security Vector (SV).

The improvement based on Security Request Vector, and its place in the whole authentication process is represented in figure 5.

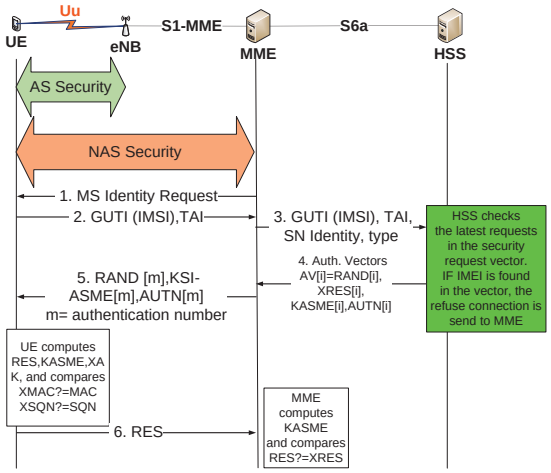


Figure 5: Proposed EPS-AKA with hardware verification method, introducing the Security Request Vector

V. Conclusions And Perspectives

Nowadays security and high data rates rank in the top priorities of customers, telecom operators and vendors.

The paper offers a security analysis of the existing 4G networks and the DoS vulnerabilities they are encountering. A weakness has been pointed out regarding the authentication process, due to the fact that the HSS directly computes the authentication vector, even if the UEs are malicious and send successive request using fake IMSIs. This can overwhelmed the important HSS core server because of possible fake request, resulting in a possible service shut-down. Furthermore an improvement of the existing EPS-AKA is proposed based on correlating the authentication requests of the UEs to the hardware serial number of the equipment (IMEI), stored in the Security Request Vector for the last authentication requests received and stored in the HSS. In this manner the HSS will be protected against DoS attacks, a security vulnerability which is not addressed by the protection methods included in the 3GPP LTE standard.

A possible study of this method in the future can take into account the possibility of using in the Security Request Vector the following parameters: Tracking Area Code and Cell Information corresponding to a malicious user location in idle/active mode.

Acknowledgment

This paper has been supported by the HORIZON 2020 project of the International Economy Institute, represented by the Electronics Doctoral School of the Military Technical Academy in Bucharest, Romania.
I would also like to thank professor Cristian-Iulian Rincu from the Military Technical Academy, for his opinions and advice on the research matters.

References

[1] Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, Zhenxing Luo, "A Survey on Security Aspects for LTE and LTE-A Networks", IEEE Communications Surveys & Tutorials, Vol. 16, No. 1, First Quarter, 2014.

[2] Koien, G.M., "Mutual entity authentication for LTE", Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, 4-8 July 2011, pp. 689-694, Istambul, Turkey.

[3] Chan-Kyu Han, Hyoung-Kee Choi, Jung Woo Baek, Ho Woo Lee, "Evaluation of Authentication Signaling Loads in 3GPP LTE/SAE Networks" 2009 IEEE 34th conference on Local Computer Networks (LCN 2009), 20-23 October 2009, Zurich, Switzerland.

[4] Fang-Yie Leu, Yi-Li Huang, Kangbin Yim, Cheng-Ru Dai, "Improving security level of LTE Authentication and Key Agreement Procedure", GC'12 Workshop: The 4th IEEE International Workshop on Mobility Management in the Networks of the Future World.

[5] D.Forsberg, L. Huang, K. Tsuyoshi, S.Alanara, "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface", Proc. Personal, Indoor and Mobile Radio Communications (PIMRC), September 2007, pp. 1-5.

[6] T.Ahmed, D.Barankanira, S. Antoine, X. Huang, H. Duvocelle, "Inter System Mobility in Evolved Packet System (EPS): Connecting Non-3GPP Accesses", Proc. Intelligence in Next Generation Networks (ICIN), October 2010, pp.1-6.

[7] D.Yu, W.Wen, "Non-Access-stratum Request Attack in E-UTRAN", Proc. Computing, Communications and Applications Conference (Com-ComAp), January 2012, pp. 48-53.

[8] M. Purkhiabani, A. Salahi, "Enhanced Authentication and Key Agreement procedure of next Generation 3GPP Mobile Networks", International Journal of Information and Electronics Engineering, vol. 2, no. 1, January 2012, pp.69-77

[9] Prashant Panigrahi, 3G LTE Info blog on wireless tutorials and training, LTE Security Architecture, , accessed on 25 April 2015
http://www.3glteinfo.com/lte-security-architecture-20110325

[9] Cristian-Gabriel Apostol, Ciprian Racuciu, "Communications standards based on radio carriers" PhD report one, July 2013, Military Technical Academy.

View publication stats