Computer Communications 000 (2016) 1–11

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

# A privacy-enhanced computationally-efficient and comprehensive LTE-AKA

Khodor Hamandi, Jacques Bou Abdo, Imad H. Elhajj, Ayman Kayssi*, Ali Chehab

*Department of Electrical and Computer Engineering, American University of Beirut, Lebanon*

ARTICLE INFO

*Article history:*
Received 23 January 2013
Revised 13 September 2016
Accepted 17 September 2016
Available online xxx

*Keyword:*
LTE
AKA
Privacy
Attacks
Passive attacks
Active attacks
Replay attacks

ABSTRACT

Evolved Packet System (EPS) was designed to be an umbrella technology for next generation LTE wireless networks. The enhanced data rates, innovative core architecture, and improved security mechanisms motivate operators and vendors to invest in the LTE technology that is intended to stay for the long term. The Authentication and Key Agreement protocol in EPS has a privacy-breaching vulnerability that is considered too expensive to solve. Previously, attackers were not able to locate precisely the users who are trying to connect to a network because the area covered by the monitored cell is in terms of kilometers squared. Currently, with the increase in the use of femtocells and the decreasing cost of attack equipment, the above hypothesis fails, and the expected rate of attacks exploiting this vulnerability increases. In this paper, we propose a new protocol to solve these privacy concerns, compare it to other solutions, and verify its security using the AVISPA tool.

## 1. Introduction

Evolved Packet System (EPS) is the first entirely packet-switched [1] version of 3GPP mobile networks, a successor of seven previous releases that progressively prepared for this architecture. Although EPS has implemented radical modifications (flatter architecture, less network elements and all-IP) [1], it has maintained its compatibility with its predecessors, thus many underlying vulnerabilities that were applicable on third generation (3 G) or even second-generation (GSM) networks are still applicable on EPS.

The enhanced security architecture implemented in EPS is the result of previous experience with designing 3 G networks and evaluating their security performance. Even though the security models implemented by EPS are stricter than those of 3 G, they are still exploitable under the same environment of network configuration (usage of femtocells, heterogeneous networks, inter-operator handover enabled, etc.) and mobile traffic schemes (used mobile applications and average call rates). EPS's compatibility with 3 G and GSM forces the need for implementing legacy algorithms. New threats become available with the introduction of femtocells and hotspot access points which ease the exploitation of EPS's vulnerabilities, as discussed in this paper.

EPS implemented minor modifications on the Authentication and Key Agreement (AKA) procedure, but many weaknesses are still present. One of the privacy breaching attacks on the 3 G UMTS AKA is IMSI catching, and this attack is still possible with LTE-AKA; but it was neglected by the standardization body since its occurrence was considered very rare. Since the reliance on femtocells is becoming widespread, it will become very frequent for users to connect to one of these Home eNBs (HeNB), and hence allowing an attacker to precisely locate a victim. This attack is due to the implementation of a vulnerable protocol that was adopted from previous releases. Further analysis of this and other privacy breaching attacks will be discussed in this paper and an effective solution will be proposed and verified.

Location-based services are applications that take advantage of the positioning systems available in many recent mobiles [2] to offer automatic detection of other users as well as other types of services that are used in social networking. These services can be exploited by passive attackers to breach the users' location privacy. Moreover, new attack scenarios become possible in this environment.

Since we are interested in protecting the network against physical, Access Stratum (AS), and Non-Access Stratum (NAS) layer attacks, we will only address network attacks and vulnerabilities while location-based services are considered outside the scope of this paper. The AS involves the protocols to maintain connectivity at the air interface between the device and the base station. On

* Corresponding author. Fax: +961 1 744 462.
*E-mail address:* ayman@aub.edu.lb (A. Kayssi).

http://dx.doi.org/10.1016/j.comcom.2016.09.009
0140-3664/

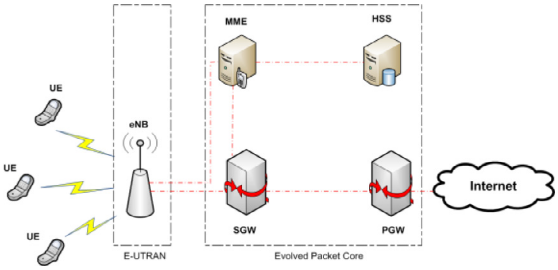

**Fig. 1.** LTE Architecture.

the other hand, the NAS involves the protocols to maintain mobility management of the device.

Privacy ensuring mechanisms differ based on the characteristics of the underlying network. In public switched telephone network (PSTN), the Call-initiating terminal does not have to transmit its identity because the underlying physical connection is point-to-point with the core network. Broadband wired networks utilize shared channels among users, but the communicating peers (PCs, laptops, servers, etc.) have sufficient computation and power resources to send their identities confidentially. Vehicular networks (MANETs and VANETs) utilize wireless shared channels, and their communicating peers have enough resources to run complex operations to ensure privacy.

On the other hand, in mobile networks, the communicating devices usually have very limited power resources and a wide variation in computation resources in addition to a very expensive shared medium. The designers of privacy ensuring mechanisms in mobile networks have to compromise between the privacy level on one hand and the added overhead in computation, signaling, and delay on the other hand. Several recommendations have been published from 3GPP on how to secure AKA [3], but no secure standard protocol was announced.

We will discuss in this paper 3GPP's standard approach to privacy-ensuring mechanisms, proposed modifications from the literature, and the latest attacks which succeeded in exploiting the above procedures. We will propose then our enhanced procedure and prove its immunity against all the previously-mentioned attacks.

The rest of this paper is organized as follows. Section 2 describes the standard LTE-AKA architecture, notations, and mechanisms. Threats leading to privacy-breaching attacks are discussed in Section 3, where AKA's vulnerabilities are described in addition to possible exploiting scenarios. Section 4 describes previous work; previously proposed protocols and their vulnerabilities. In Section 5, we present our proposed enhanced AKA model, which is then analyzed, verified, and evaluated in Section 6. Section 7 concludes the paper.

## 2. LTE-AKA

EPS identifies subscribers permanently using a unique identifier called International Mobile Subscriber Identity (IMSI) [1]. IMSI is a 15-digit identifier formed by the concatenation of Mobile Country Code (MCC), Mobile Network Code (MNC), and Mobile Subscriber Identification Number (MSIN) which explicitly shows the country of origin and operator of origin to facilitate roaming.

Capturing a user's permanent identifier while being transmitted over the air channel will allow the detection of the user's current position, tracking the user, in addition to other privacy-breaching attacks. 3GPP has tried to overcome these attacks by introducing a new temporary identifier, the Globally Unique Temporary UE Identity (GUTI), to provide an unambiguous identification of the UE [1]. GUTI is only relevant in the serving MME's area (see Fig. 1), thus it is sent by the network over Non-Access Stratum layer connection where confidentiality and integrity are protected.

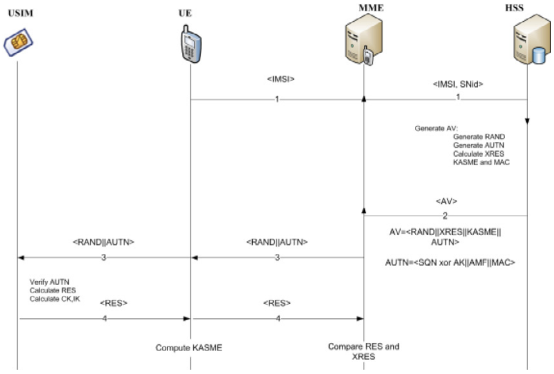

**Fig. 2.** Original LTE-AKA.

GUTI is defined as following:

$$GUTI = \langle GUMMEI||M - TMSI\rangle$$

The GUMMEI entity incorporates MCC, MNC, and MMEI. On the other hand, the M-TMSI identifies the UE within a serving MME.

A user's GUTI is not expected to be constant over a long period of time in order to prevent the user from being tracked. GUTI might be updated in an Attach Accept message, Tracking Area Update (TAU) Accept message [1], or GUTI Reallocation command [4]. This modification is presented in using GUTI instead of previously used Temporary Mobile Subscriber Identity (TMSI).

Accordingly, GUTI is only transmitted during the NAS layer connection where confidentiality and integrity are protected. However, confidentiality and integrity protection are enabled only after key sharing which is a late step in the access control mechanism. Conceptual steps in access control are: Identification, authentication, authorization, key sharing, and finally enabling secure access. It can be seen from these steps that Identification occurs before establishing a secure connection, thus user identities are transmitted in plaintext. Confidential identification is a very expensive task when compared to confidential data exchange in a security established connection, thus a compromise has to be made between additional costs resulting from ID hiding and a high level of privacy. This dilemma faced the designers of GSM, UMTS, and finally LTE.

AKA is responsible for user identification, user authentication, network authentication, and generation of master keys which will be used to derive the confidentiality and integrity keys. The AKA procedure involves the UE (User equipment), eNB (evolved Node B), S-MME (Serving network's MME) and H–HSS (Home network HSS) as shown in Fig. 1.

The LTE-AKA Procedure shown in Fig. 2 is described next.

1. **UE → S-MME: NAS Attach Request (IMSI)**
   When a user tries to connect to a network, but has no previous temporary identifier, she has to identify herself by transmitting her permanent identifier (IMSI) in a NAS attach request. If the user has a temporary identifier from a previous connection, she can send her GUTI||LAI/RAI. The S-MME will contact the MME serving the LAI sent by the user and if it succeeds in retrieving the GUTI/IMSI pair it proceeds to step 2, otherwise, it requests the user to send her permanent identifier.
2. **S-MME → H–HSS: Authentication Info Request (IMSI, SNID)**
   S-MME retrieves MCC||MNC from IMSI and routes the request to H–HSS concatenated with the serving network ID (IMSI||SNID). It then concatenates its ID to the request sent by the user and forwards it to the corresponding HSS.
3. **H–HSS → S-MME: Authentication Info Answer (RAND || XRES || KASME || AUTN)**

Please cite this article as: K. Hamandi et al., A privacy-enhanced computationally-efficient and comprehensive LTE-AKA, Computer Communications (2016), http://dx.doi.org/10.1016/j.comcom.2016.09.009