Enhancement Mobile Security and User Confidentiality for UMTS

Ja'afer AL-Saraireh, Sufian Yousef & Mohammed AL Nabhan

Anglia Ruskin University
Bishop Hall Lane, Chelmsford, Essex, CM1 1SQ, UK
e-mail: j.al-saraireh@anglia.ac.uk, s.yousef@anglia.ac.uk, m.alnabhan@anglia.ac.uk

Abstract : *The permanent user international mobile subscriber identity (IMSI) is used in authentication process and in the first step for authentication process in initial registration; the mobile station sends the IMSI in clear text without encryption between the communication parties over the radio interface. This represents a violation of user identity confidentiality. Sending IMSI in clear text causes serious security problems for universal mobile telecommunication system (UMTS). This paper suggests a new technique to protected user identity by encrypted IMSI to provide user confidentiality and consequently the IMSI cannot be eavesdropped, and to ensure the confidentiality of user data and signaling traffic by preventing localizing and tracking of a mobile station.*
Keywords: UMTS, Home Network, Visited Network, Authentication, Security.

1. Introduction

In order to provide security services in wireless networks, authentication is used as an initial process to authorize a mobile terminal; for communication through secret credentials [L. Salgarelli 2003]. In authentication process, a mobile is required to submit secret materials such as certificate or challenge and response values for verification.

Third generation (3G) mobile systems such as Universal Mobile Telecommunication System (UMTS) specified by Third Generation Partnership Project (3GPP) [IETF 2003] was built on the success of GSM and other second generation system by introducing new and enhanced security features that are designed to stop threats [J. Al_muhtadi 2002, Mark 2002]. These include: Mutual Authentication which allows the mobile user and serving network to authenticate each other and, Network to Network security that secure communication between serving networks.

2. Security Service in UMTS

The objective of UMTS security is to provide entity authentication, data confidentiality, user confidentiality and data integrity.

Authentication is a process of verifying the identity of an entity and makes sure that the communication is authentic between parties. Authentication is needed for insuring all parties of the communication are the ones they are claiming to be. One important tool to achieve this goal is the digital signature.
Confidentiality can be defined as the prevention of unauthorized disclosure of information [Gollmann 1999], and it is about not letting unauthorized users read, or learn, sensitive information. In using encryption, a process of taking readable and meaningful data, and scrambling or transforming it so that someone who happens to intercept the data can no longer understands it.

Integrity means keeping the data in unaltered form, Integrity ensures that information is not changed or altered in transit and includes the detection modification, insertion, deletion, or replay of transmitted data [Gollmann 1999].

User confidentiality is that the permanent user identity (IMSI) cannot be eavesdropped. This service is implemented by using a temporary user identity (TMSI), which is known by the visited serving network. Confidentiality is used to keep information secured from eavesdropper and hacker. This is achieved by ciphering of the user and signaling data between the subscriber and the network and by referring to the subscriber by temporary identities TMSI instead of using IMSI. Mobile networks must provide subscriber identity confidentiality, subscriber location confidentiality, user data (i.e. voice and data) and signaling data confidentiality.

3. UMTS Architecture.

The figure 1 illustrate the entities that evolved in UMTS network security are the mobile station which consists of user equipment (UE) and the UMTS mobile subscriber identity (USIM), the radio network controller (RNC), the visited location register in the serving network (VLR/SN) and the user home environment and authentication center (HE/AuC).

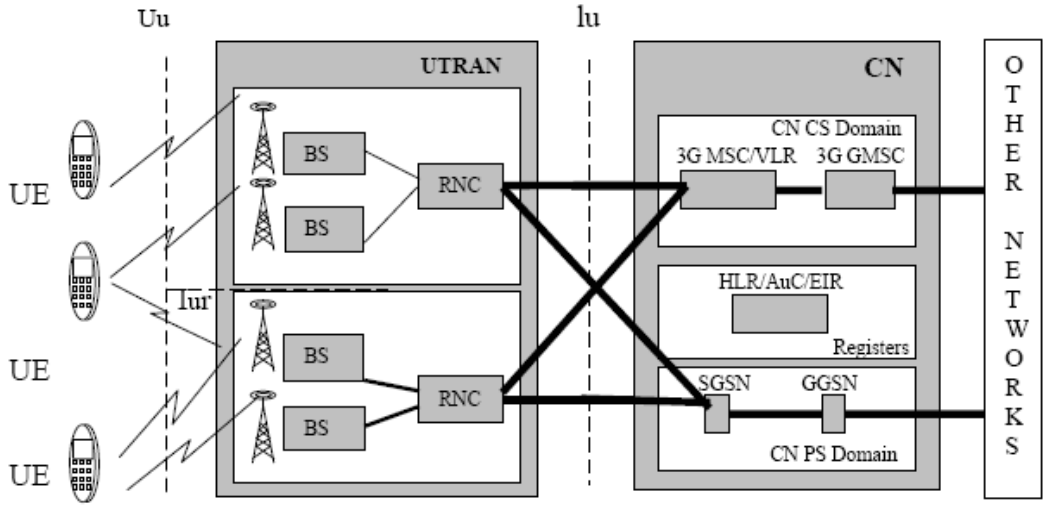

Figure 1 UMTS Architecture

4. International Mobile Subscriber Identity and Temporary International Mobile Subscriber Identity

The International Mobile Subscriber Identity (IMSI) is a unique identifier allocated to each mobile subscriber in a GSM and UMTS network. It consists of a mobile country code (MCC), a mobile network code (MNC) and mobile station identification number (MSIN). The MCC is a three digit number that uniquely identifying country but the MNC is either a two or three digit number used to uniquely identify a network from within a specified country. Figure 2 illustrates the contents of IMSI.

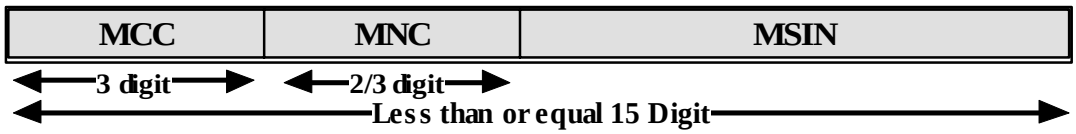

Figure 2 International Mobile Subscriber Identity

The mobile networks use temporary mobile subscriber identity (TMSI) to ensure subscriber identity confidentiality. The visitor location register (VLR) and serving GPRS support node (SGSN) allocate TMSI to visiting mobile subscribers. The VLR and SGSN must be capable of correlating an allocated TMSI with

the IMSI of the mobile station (MS) to which it is allocated. A MS may be allocated two TMSI, one for services provided through the VLR, and the other known as the Packet TMSI (P-TMSI) for services provided through the SGSN [Mpirica]. A TMSI is used to prevent traffic analysis and to provide user confidentiality on the mobile networks.

To generate the ciphering code K_c it is needed to know the identity of the subscriber, but to minimise the plain text transmissions of the IMSI (International Mobile Subscriber Identity, a TMSI is used instead of IMSI. The TMSI is allocated from the VLR to the MS.

There is no possibility to make the connection establishment with a TMSI at the first registration in a new Public Land Mobile Network (PLMN) or if there is no TMSI on the SIM card stored (turn on of the MS, for example) and therefore the users IMSI has to be transmitted to the VLR in plain text. The TMSI is not stationary and can be changed from the VLR at any time, at the start of every authentication check and ciphering, for example, but in this case the IMSI has not to be transmitted.

Transmission of the IMSI in the mobile networks as a clear text occurs in some cases such as, when the subscriber registers for the first time, or when the serving network cannot retrieve the IMSI from the TMSI by which the user identifies itself. This case occurs when the old VLR is not contactable or when software error occurs or database failure, if the VLR database is partially lost or no correct subscriber data is available (Loss of TMSI, TMS unknown at VLR, etc.). Figure 3 illustrates the transmission of the IMSI in mobile networks.

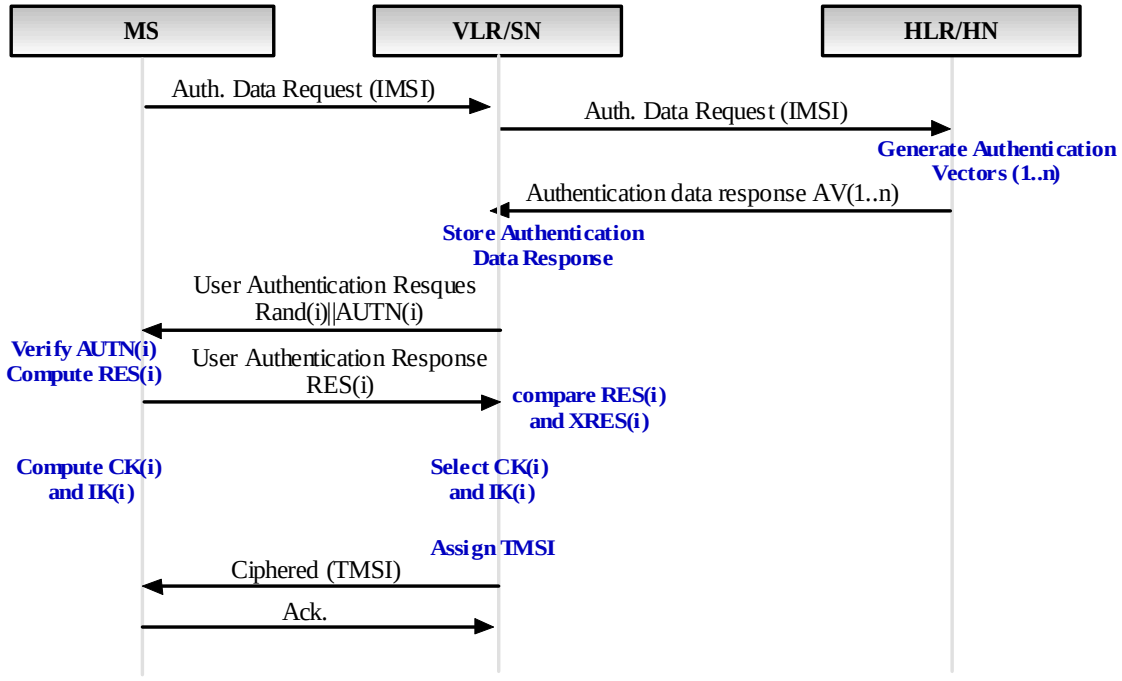

Figure 3 Clear Text transmission of the IMSI when the TMSI is unknown

5. Encryption of International Mobile Subscriber Identity (IMSI)

When the IMSI is transferred in clear text, it is possible to follow the movements of the mobile station by monitoring the radio connections established between mobile station and the network. But if the IMSI is protected by encryption then hacker and eavesdropper cannot decipher of data communications. In mobile networks system, the IMSI is transferred in each data packet that sent by MS, and so the IMSI can be

encrypted by using encryption method. This proposed method solved the problem of disclosure of IMSI by transmission IMSI to the user home network or to other network by encrypted IMSI.

There are secrete key (K_{mh}) for home network, one way hash function (f_9) used to generate cipher key K_c, this cipher key is used for encryptions the IMSI, and one way hash function (f_{10}) used to encryption IMSI. This one way function f_9, f_{10} and K_{mh} are shared between mobile station and home network. This key and one way functions are stored in the SIM card for mobile user and in the home network for the user. The secrete key (K_{mh}) for the home network is stored in all mobiles belongs to the same home network. For the first registration, the mobile station needed to make authentication. The MS generate random number (Rand) and compute cipher key K_c to encrypt IMSI. $K_c = f_9(K_{mh}, Rand)$, and then MS send authentication request with encrypted IMSI, $Enc(IMSI) = f_{10}(K_c, IMSI)$, and then send identification of home network ID_{HN}, Enc(IMSI) and Rand to VLR/SN and then passes this request to HLR/AuC. The ID_{HN} is used to routing the message to correct home network. The HLR compute the $K_c = f_9(K_{mh}, Rand)$, and then decryption the received message to get $IMSI = Decrypt(K_c, Enc(IMSI))$. Figure 4 illustrates how the proposed method for initial registration is working.

The second technique is using public key cryptography; each home network has a public key and private key. The public key of home network is stored in SIM card for each subscriber belongs to this home network. The mobile station using public key of home network to encrypt the IMSI as illustrates in the figure 5.

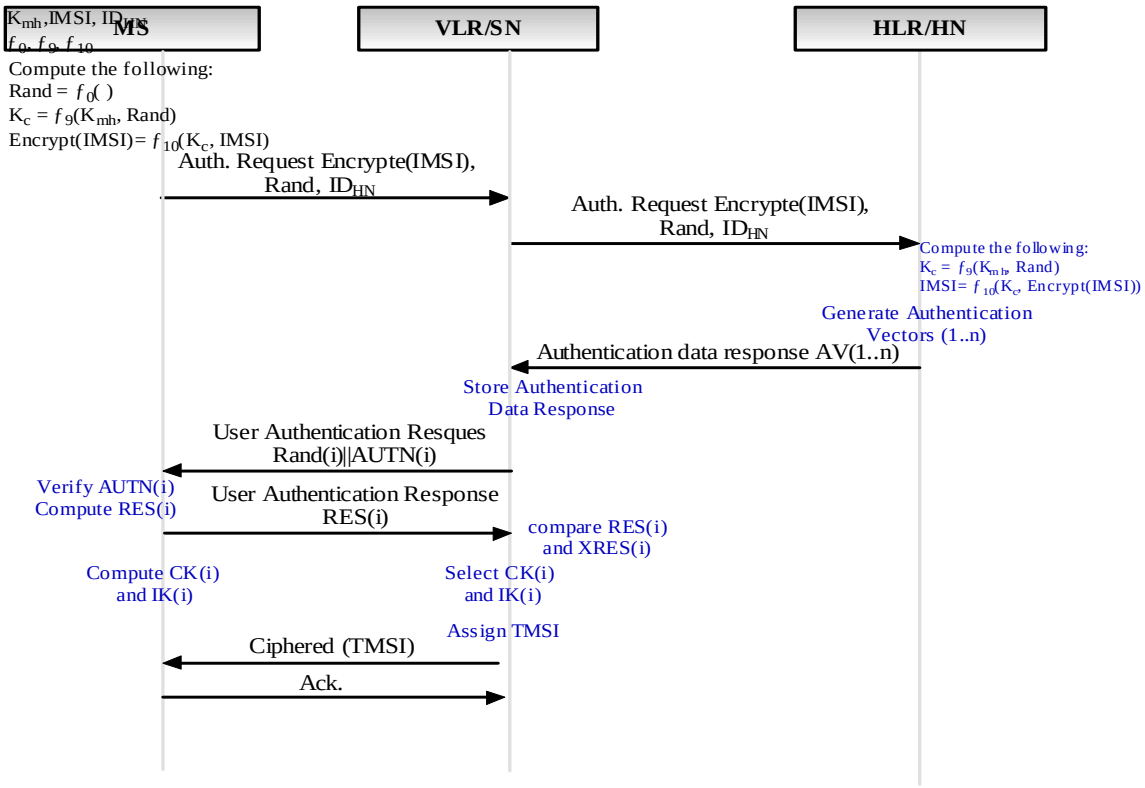

Figure 4 Encrypted Text transmission of the IMSI when the TMSI is unknown

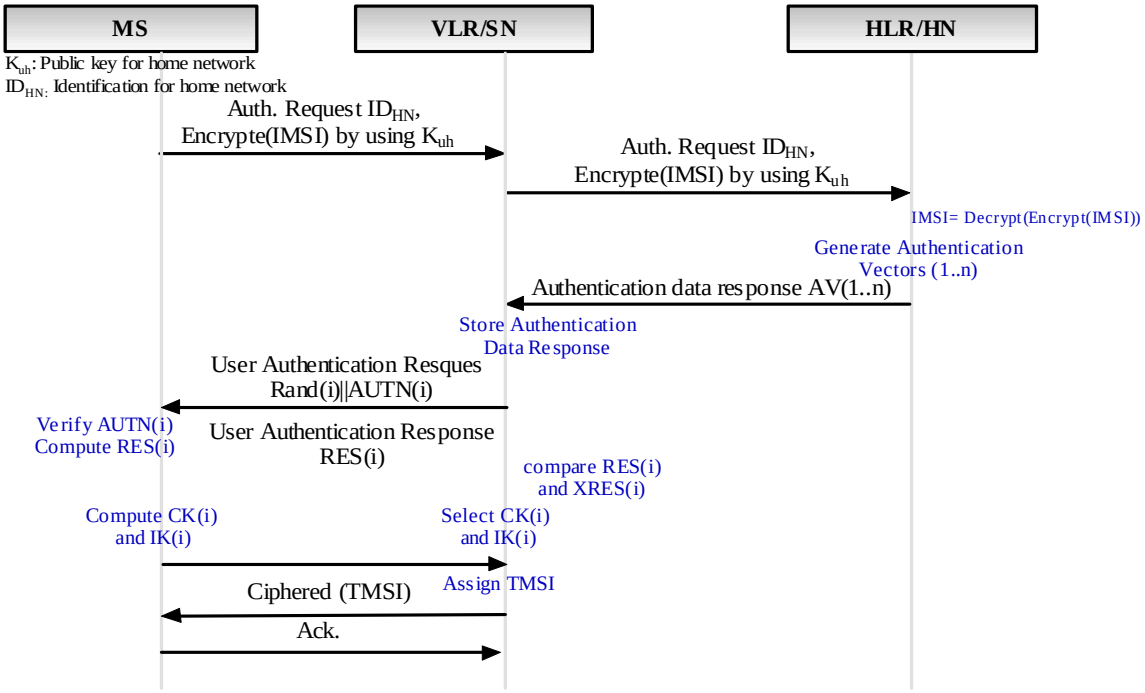

Figure 5 Encrypted Text transmission of the IMSI Using Public key

6. Conclusions

The new method provides confidentiality of the user identity over the air interface, to prevent an interceptor of air interface communications from learning the mobile user's identity and being able to track particular mobile users. Also the new method protects the user's traffic, both voice, data, and sensitive signalling data, such as dialled telephone numbers, against eavesdropping on the radio path. The user should not use the same TMSI for a long period. The following security features related to user identity confidentiality are provided by the proposed method:

i. **User identity confidentiality**: the permanent user identity (IMSI) of a user to whom services are delivered cannot be eavesdropped on the radio access link.
ii. **User location confidentiality**: the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link.
iii. **User untraceability**: an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

References

G. Horn, K. Martin, and C. Mitchell, (2002). Authentication protocols for mobile network environment value-added services. IEEE Trans. Vehicular Technology, vol. 51, no. 2, pp. 383-392.

Gollmann Dieter, (199), Computer Security , John Wiley & Sons.

Hongyuan Chen, and T.V.L.N Sivakumar, (2005). New Authentication Method for Mobile Centric Communication. IEEE Trans. Communications.

IETS, 2002. Internet Engineering Task Force (IETF). Working Group. IP Security Protocol (IPsec), *http://www.itef.org/html.charters/upsec-cgarter.html*, [Internet Accessed 12 April 2003].

J. Al-Muhtadi, D. Mickunas, & R. Campbell, (2002). A Lightweight Reconfigurable Security Mechanism for 3G/4G Mobile. IEEE Wireless Communications, Vol. 9, pp. 60-65, April 2002.

Jorg E., Hans J. and Christian B, (2001), GSM Switching, Services and Protocols, 2nd edition, John Wiley and Sons Ltd., ISBN 01-471-49903-X.

L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, (2003). The Evaluation of wireless LANs and PANs – Efficient Authentication and Key Distribution in Wireless IP Networks. IEEE Personal Comm. on Wireless Communication 10(6):52-61.

Mpirical *htpp://mpirical.com/companion/Multi_Tech/TMSIdentity.html*

M. Johnson, (2002). Revenue Assurance, Fraud and Security in 3G Telecom Service. Journal of Economic Management, Volume 1, Issue 2.

M. Walker, (2003). On the Security of 3GPP Networks, *http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000/mike_walker.pdf* , [Internet Accessed 20 April 2003].

R.R. Joos and A.R. Tripathi, (1997). Mutual Authentication in Wireless Networks. Technical Report, Computer Science Department University of Minnesota, 1997.

S. Suzuki and K. Nakada, (1997). An authentication technique based on distributed security management for the global mobility network. IEEE Journal Selected Areas Communication Vol. 15, pp. 1608- 1617.