Advance Security aspects of Universal Mobile Telecommunication System (UMTS)

Faisal Imran[1], Mureed Hussain[2]

Department of Computer Science & IT
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology Islamabad, Pakistan
faisalimran_84@yahoo.com, hmureed@yahoo.com

Abstract

Wireless communication is known as key to global development and has become main stream of our daily business. Protecting information and communication speed is an issue which we need to focus on the wireless networks. Universal mobile telecommunication system (UMTS) is evolution of third generation mobile communication system. It was built on the success of global system for mobile communication (GSM), UMTS security is also built upon GSM, so there is lot of security challenges such as the user identity, confidentiality. The international mobile subscriber identity travels through radio interface in free text format without any encryption. Due to this, the user identity and location can be theft which is serious problem. In this paper, we have proposed and emulated a model which protects user identity through IMSI hashing, which will provide anonymity to user. We have compared different hashing techniques and the results are given at the end.

Keywords- *UMTS; Security; Hashing; MD5; SHA; IMSI*

1. Introduction

Wireless communication is gaining more importance in our daily life. A lot of users are using the services so there is requirement for high bandwidth and security and every body wants fast and secure communication. Security and speed are major required parameters. People want to use it in online banking, shopping, video conferencing etc. Further more, universal mobile telecommunication system (UMTS) is also being developed in 4G [1]. It is part of ITU-IMT200 standard. The objective of which is to deliver pictures, graphics, video and other multimedia information on wireless networks.

Its network topology basically depends upon GSM and general Packet Radio Service (GPRS). UMTS uses GSM at back end. UMTS uses Wideband code division multiple access (WCDMA 200) and provides data rate up to 2Mb/s. it can also provide data rate up to 21 Mb/s through high speed downlink packet access (HSDPA) [10]. There has been great evolution in the field of wireless network security. Network security is one of the primary features in the performance of network. Now the security has more importance than anything else because when a network is implemented poorly, security threats and attacks exist. If we implement all the security features to make that network secure there threats can be reduced. No doubt that cost and the bandwidth consumption are also two main issues for securing network. So, secure network have both advantages and disadvantages. It is also main issue in UMTS.

The paper discusses the problems related to user and provides solutions to resolve these problems. User anonymity is too much compromised in this network. International mobile

subscriber identity (IMSI) is the user identity in UMTS network. It travels in open text in UMTS networks. Basically UMTS IMSI is used to create reliable connection between user and UMTS network. The current study is very much concentrated around how to provide anonymity with provisioning of hashing in UMTS. Different hashing algorithms are studied in depth and results are given to show which one is best in a particular situation.

The paper is further divided into different sections; second section describes UMTS Architecture, in third section IMSI Structure is discussed, fourth is Problem statement, then the next section is related to proposed solution and results, and in the last section we conclude with future work.

2. UMTS Architecture

UMTS architecture consists of three main parts. Core network (CN), UMTS terrestrial radio access network (UTRAN) and user equipment (UE).

a. Core Network

The core network architecture of UMTS is based on UMTS network with GPRS. It is modified for UMTS operation and services. It consists of two domain circuit switching (CS domain) and packet switching (PS domain). Circuit switching have mobile services switching centre (MSC), visitor locator register (VLR) and gateway MSC. But packet switching has serving GPRS support node SGSN and gateway GPRS node GGSN. Some network elements like EIR, HLR, VLR and AUC are also present which are shared by both domains.

b. UMTS Terrestrial Radio Access Network (Utran)

It consists of radio network controller and node B. UTRAN provides access to radio mobility and resource utilization. The serving radio network controller (SRNC) built the logical connection between the UE and CN. The drift radio network controller (DRNC) provides additional radio resources for UE. The node B which is attached to DRNC provides physical resource to UE and information on the uplink and downlink which are routed towards the SRNC. There are four interfaces which have connection between UMTS terrestrial radio access network (UTRAN) internally or externally Lu, Uu, Iub and Iur. The Lu and Uu are the external interfaces which connect the radio network controller (RNC) to CN and node B with user equipment. The Iub is an internal interface which connects the RNC with node B and at last there is the Iur interface which is an internal interface most of the time and can exceptionally be an external interface to for some network architecture. The Iur connects to R NCs with each other. RNC in UMTS provides the same functionality as Base Station Controller (BSC) works in the GSM.

c. User Equipment (UE)

The radio terminal which is used by the subscriber to access services from UTRAN is known as UE. This can be PDA or any other hand set. With the change of cost capability of UE changes. It is connected to base station (Node B). It has different identities such as international mobile equipment identity (IMEI), MSISDN, international mobile subscriber identity (IMSI) and temporary mobile subscriber identity (TMSI).

d. Node B

It is the radio transmission and reception unit. It provides communication between radio cells. Only one node B can provide services to several users. It basically connects UE through Wide-band code division multiple access (WCDMA). It provides both facilities of frequency division duplex (FDD) and Time division duplex (TDD). UE and node B are connected through Uu interface. While through Iub interface provides connection between node B and RNC by using Asynchronous Transfer Mod (ATM). Node B also provides transmission power control facility.

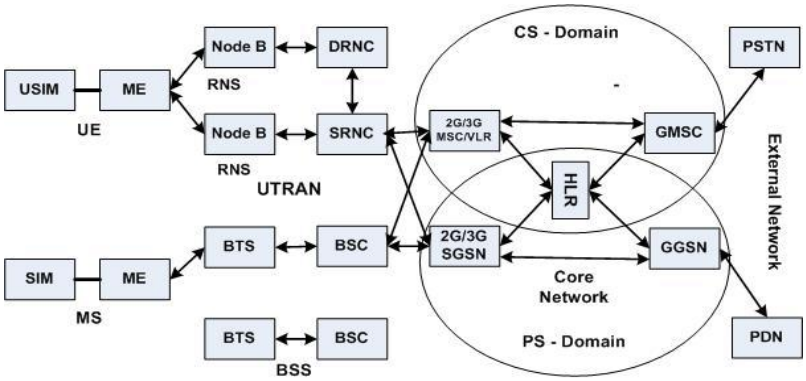

Figure 1. UMTS Architecture

3. UMTS Security Features

There are five basic security features which are given in UMTS network. The first one is the network access security. Through this feature there is secure user access towards the UMTS services. There are further steps in the UMTS access security like entity authentication which provides subscriber authentication and network authentication [8]. Next one is data integrity and origin authentication. This provides integrity algorithm agreement, integrity key agreement and data integrity origin authentication. User traffic confidentiality is provided through ciphering algorithm agreement. User identity and location confidentiality is provided through the temporary mobile subscriber identity (TMSI). User untraceability is also provided through this one. User_to-USIM authentication is also provided in network access security.

Mutual authentication is also a security procedure which occurs through the Authentication and Key Agreement (AKA) protocol. Which is a secure protocol used in UMTS. Through which the keys exchange occurs and then secure mod is setup.

The next one is the network domain security to set security features which provide secure exchange of signaling data and provide security against the attacks on wireless networks [7]. Another one is user domain security which provides secure access to mobile station. Application domain security provides both user and provider domain security by enabling applications. Visibility and configurability is the next UMTS security features. There are different algorithms which are used to provide security through ciphering. The f9 algorithm in UMTS is used to provide the data integrity and f8 algorithm is used to provide the data confidentiality. The basic algorithm used for integrity and confidentiality is called KASUMI. It's a secure algorithm [9].

4. Problem Statement

There are three main parties which communicate with each other in UMTS. The Home environment (HE), the serving network (SN) and the Mobile station (MS). Here network access security is one of the key procedures. UMTS authentication key agreement procedure (UMTA-AKA) is one of them. It basically performs mutual authentication and key agreement between MS and network.

Basically authentication key agreement protocol (AKA) consists of two phases. In first phase it distributes some authentication vector from HE to SN for the sake of security. When trust is established between HE and SN the second phase starts. When mutual authentication occurs between SN and MS, cipher and integrity key exchange also occurs between them. These keys are used to provide confidentiality and integrity of that data which is transmitted on radio link.

In network access security, user identity confidentiality against sniffer is also required. For the sake of this one IMSI cannot be eavesdropped (identity confidentiality). The arrival or presence of a user in a certain area cannot be determined and delivery of any service to user cannot be deduced. These three prosperities are known as the user anonymity.

To achieve all these objectives UMTS uses only Temporary Mobile Subscriber Identity (TMSI). This TMSI is issued by SN for any visiting MS. SN also keeps the relation between TMSI and IMSI. SN also saves it in its database. It is used for identification between SN and MS. It is reallocated by SN when it is not being used for a long period of time and transmitted in protected mode on radio network.

When, a new MS comes into area of SN. It sends its TMSI for identification. The new SN which has no knowledge about its IMSI it will send a request to old SN by using that TMSI. The old SN searches it in its database of that MS. If it found then it will send response including IMSI of that MS. But there are some ways in which IMSI is visible in network.

1) When MS newly registers in SN and there is no valid TMSI for that MS.
2) When the database of SN fails to retrieve IMSI against a TMSI which it received.

In all these situations when SN will not receive IMSI, it will request for IMSI from MS. The MS will send IMSI to SN which will be in form of clear text. When the identity confidentiality of user is compromised IMSI is also visible to HE.

5. Authentication Process

The user authentication process starts between the MS, BSS and HOLMN. It starts when the user sends its TMSI with LAI and VLR cannot verify it from its existing VLR. There are both ways that may VLR database crashed or that user is going to be newly registered in that SN. Then VLR sends request for IMSI. UE will send IMSI in clear text format. It consists of six steps. The authentication process starts like this one.

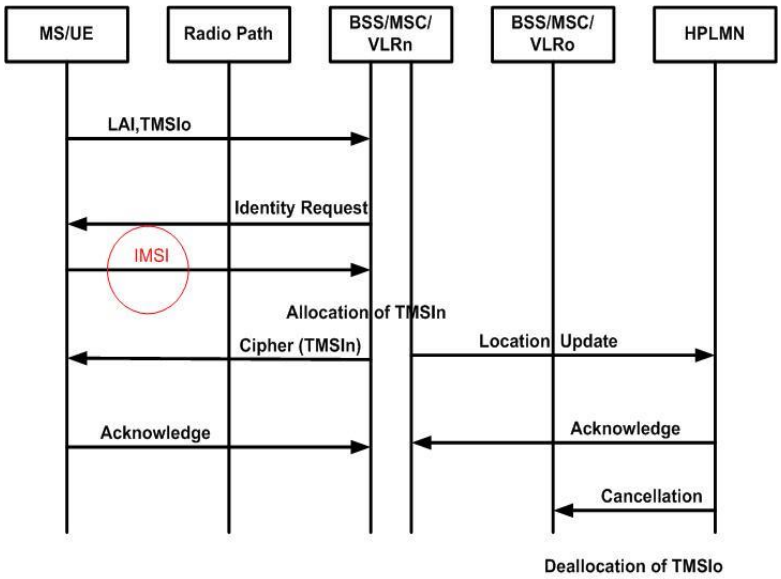

Figure 2. UMTS Authentication

1) A UE sends a request for location update with old TMSI (TMSIo) and old Location Area Identity (LAI).
2) The new MSC/VLRn can not reached old MSC/VLRo.
3) The new request for identity from MSC/VLRn.
4) UE sends IMSI in clear text.
5) Then the TMSIn is calculated.
6) The ciphered TMSIn is transferred to UE and inform to HPLN of UE.
7) Both send the acknowledgement.
8) The old TMSIo is reallocated from database.

Here in step 4 there is a problem where IMSI comes in radio path in clear text form. So the IMSI catcher which is used as fake base station can be used to catch user permanent identity.

6. International Mobile Subscriber Identity (Imsi) Structure

Basically IMSI consists of total fifteen digits and three parts. The first portion is Mobile country code (MCC), Consisting three digits. Next one is the Mobile Network Code (MNC). This consists of two or three digits. Third part is Mobile subscriber Identity number (MSIN) having the remaining digits. The MSIN and MNC are collectively known as National Mobile Subscriber Identity code (NMSI) having approximately thirteen digits.

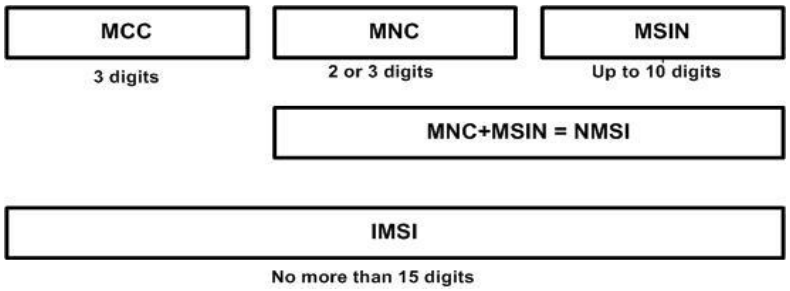

Figure 3. IMSI Size

7. Hashing Techniques

Basically hashing is a technique in which a fixed size digests or finger print is calculated by application of some one-way mathematical function. There are three main hashing techniques which are implemented and compare in this paper. The first one is the MD5 hashing function [8]. In MD5 it takes variable length message and produce fixed length digest which has size of 128bits [8]. MD5 have up to four rounds. The MD5 works on 512 bits chunk of data to create a hash of 128 bits. The next one is the SHA1 [7] which is also a hashing technique. This technique produces an output digest as 160bits with a maximum length 264 − 1bits [7]. It has eighty rounds. It uses the same principle as MD5 but it has more complex design as compare to MD5. Its official version was released in 2002.

TABLE I. HASHING FUNCTIONS AND THEIR SIZE IN BITS

Algorithm		Output size (bits)	Internal state size (bits)	Block size (bits)	Length Size	Word size (bits)	Rounds
MD-5		128	128	512	264 − 1	32	4
SHA-1		160	160	512	264 − 1	32	80
SHA-2	SHA-256/224	256/224	256	512	264 − 1	32	64
	SHA-512/384	512/384	512	1024	2128 − 1	64	80

The next one is the SHA2 family which has further more hashing functions like SHA224, SHA256, SHA384 and SHA512. It was released by Federal Information Processing Standard (FIPS) in 2004[6].

SHA224 and SHA256 are known as novel hashed functions which compute 32 bits and 64bits words. Those have output digest size 224bits and 256bits respectively. These both also have sixty four rounds. Where as SHA384 and SHA512 have word size of 64bits. It produces digest of 384 and 512bits respectively. These also have 80 rounds [6]. There is no collision found in SHA1 and SHA2 but In MD5 the collision is found. SHA2 family also has more complex structure than SHA. The comparative table is also shown for all these algorithms.

8. Solution

This problem is already discussed in [2]. They basically provide the vulnerabilities of UMTS access domain security. They have discussed different Denial of Service (DoS) attacks. This basically works on the IMSI. But there is also a solution which is given by [3]

one year before the publication of this paper but there is no discussion about the solution. [4] Discusses two models one uses the hashing to make the digest of the IMSI and also describes an algorithm for this purpose. The second model uses simple PKI for encryption of IMSI. As we know PKI creates too much over head and takes to much time for encryption. This will reduce the data flow speed.

These two models are discussed in [4] but with no simulation or implementation results. In [3] there is a proposed model for improving user identity confidentiality and had introduced an anonymous ticket manger module, which calculate anonymous ticket and send it on the air interface. This module manages the whole exchange of this ticket on the network. An algorithm for all this Procedure is also described. But from our point of view it will create an over head on network and use more resources to calculate and transmit that ticket. In that sequence number generation asymmetric cryptography can cause more delay and bandwidth consumption

9. Proposed Authentication Process

In our model when the authentication starts and the visiting location register (VLR) sends an identity request to user equipment (UE). Then UE sends the identity which is international mobile subscriber identity (IMSI) in the form of hash digest.

The authentication process starts from user equipment.

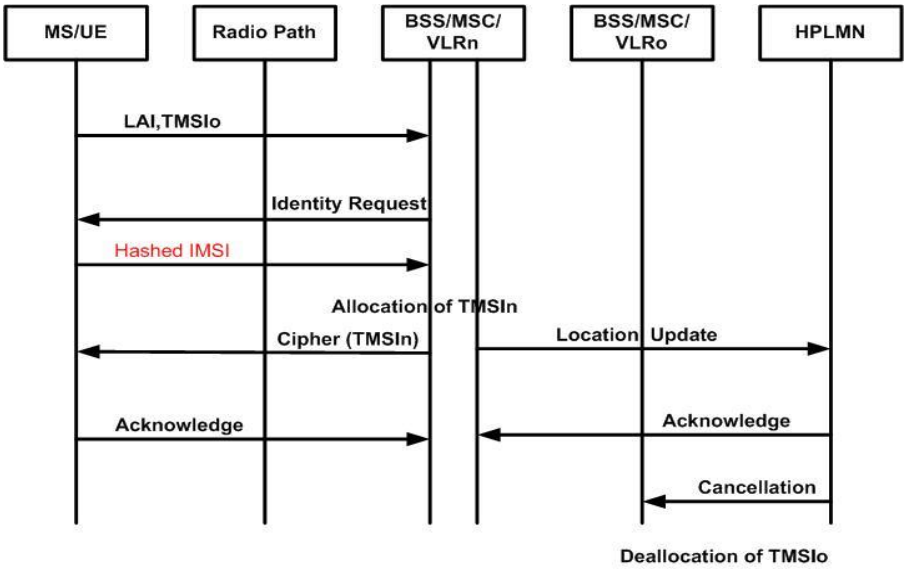

Figure 4. Proposed UMTS Authentication

1) A UE sends a request for location update with old TMSI (TMSIo) and old Location Area Identity (LAI).
2) The new MSC/VLRn can not reached old MSC/VLRo.
3) The new request for identity from MSC/VLRn.
4) UE sends Hashed IMSI.
5) Then the TMSIn is calculated.

6) The ciphered TMSIn is transferred to UE and inform to HPLN of UE.

7) Both send the acknowledgement.

8) The old TMSIo is reallocated from database.

Hashed IMSI = Hashing Algorithm (IMSI).

So, we are using different hashing techniques to secure IMSI. We send hashed IMSI from UE to VLR. We have implemented MD5 algorithm to calculate hash. Through emulation we saw that its size increases from136 to 256 bits and in SHA1 and SHA2 to 320bits and 512bits respectively. The comparison of the three algorithms is given in Figure 5. That shows that comparatively data increase when we move from MD5 towards SHA2. The delay will also increase as we move from MD5 to SHA2 as shown in Figure 6. We have performed emulation on 15digits IMSI and results are shown in Figure 5.

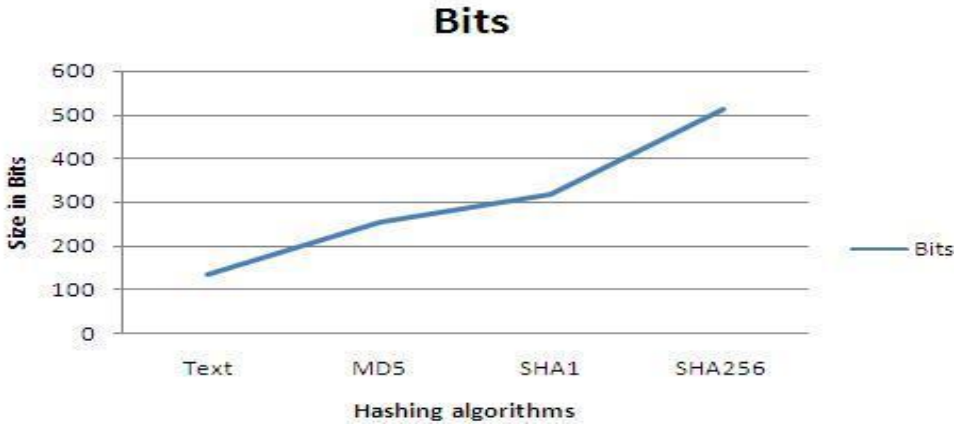

Figure 5. Hashing Comparision

We hashed that IMSI with MD5 for first time and then we hashed it with SHA1 and at the end we hashed it with SHA2. We have compared all these algorithms with each other. We calculated the delay and traffic analysis from UE to VLR. After applying fixed size hash. We know SHA2 is more secure than SHA1 and MD5 but SHA1 is more secure than MD5. Which means that with hash calculating delay will also produce more bits than original data. But this hash is to much secure then the clear text format. As we will move towards the most secure hashing technique the bit rate will increase. There will be some overhead in data size and delay also.

The Figure 5 shows the data size which increases by applying the different hashes on the plain text international mobile subscriber identity and figure 6 shows the delay produced when we hashed international mobile subscriber identity with MD5, SHA1 and SHA2 algorithms.

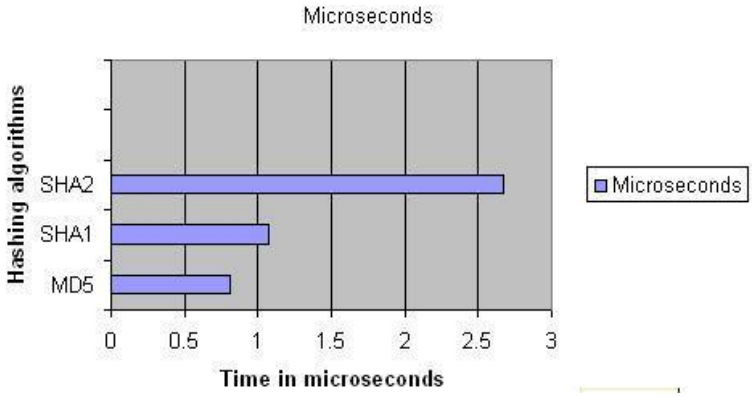

Figure 6. Delay Graph

10. Conclusion

With the use of hashing the data will be secure. So, from our point of view SHA2 is best for security point of view but from over head point of view MD5 is the best. By applying hashing the digest will be secure and can travel on air interface securely. User Anonymity, Location confidentiality and untraceability are the security features related to user are provided by the proposed method. The permanent user identity (IMSI) of a user to whom services are delivered cannot be eavesdropped on the radio access link. And the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link and at last an intruder cannot assume whether different services are delivered to the same user by eavesdropping on the radio access link. So our conclusion is to use SHA1 for hashing which provides security and have less overhead.

References

[1] www.umtsworld.com

[2] Muzammil Khan, Attiq Ahmad, Ahmad Raza Cheema "Vulnerabilities of UMTS Access Domain Security Architecture" IEEE in Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 2008

[3] Behman Sattarzadeh, Mahdi Asadpour and Rasool Jalilil, "Improved User Identity Confidentiality for UMTS Mobile Networks" in Proceeding of IEEE Fourth European Conference on Universal Multiservice Networks 2007.

[4] Ja'afer AL-Saraireh, Sufian Yousef & Mohammed AL Nabhan "Enhancement Mobile Security and User Confidentiality for UMTS" In proceeding of Second European Conference on Mobile Government 2006.

[5] 3GPP TS 33.102. "3GPP: Technical Specification Group services and System Aspects, 3G Security, Security Architecture".

[6] Ryan Glabb a, Laurent Imbert b,a,c, Graham Jullien a, Arnaud Tisserand b, Nicolas Veyrat-Charvillon "Multi-mode operator for SHA-2 hash functions" In proceeding of Science Direct Journal of Systems Architecture 2007.

[7] Mine Lei, Hai Bi, Zhengjin Feng "Security Architecture and Mechanism of Third Generation Mobile Communication" IEEE 2002.

[8] K. Boman, G. Horn, P. Howard and V. Niemi "UMTS Security" Electronics and Communication Engineering Journal, 2002

[9] K. Nyberg "Cryptographic Algorithms for UMTS" European Congress on Computational Methods in Applied Sciences and Engineering, 2004

[10] www.cellular.co.za

Author

Faisal Imran I have done BS(CS) from Allama Iqball Open University. Now doing his MS in information Technology from Shaheed Zulfikar Ali Bhutto Institute of Science and Technology Islamabad, Pakistan. Also, doing research in network access control field.