Exploration of GSM and UMTS Security Architecture with Aka Protocol

Jyoti Kataria*, Dr. Abhay Bansal**

* Amity University, Noida, Uttar Pradesh
** Amity University, Noida, Uttar Pradesh

Abstract- With the expansion of mobile communication network, incredible changes are taking place in the field of mobile technologies, as requirements are increasing day by day for mobile data services along with them security concerns are also expanding. This paper focuses on the architecture of GSM and UMTS along with Authentication and Key Agreement protocol description, which shows the encryption process used in the authentication of the network and the client over the air interface. In addition, this paper also gives an introduction to some concepts of UMTS security architecture.

Index Terms- GSM, UMTS, Authentication and key agreement, 3GPP and Authentication Vector

I. INTRODUCTION

In the past decade, communications which are wireless in nature experienced an impulsive growth and also became a vital part of the society. Authentication, Encryption, Security and access control are some essential features that should be present in communication network. One of the main reason because of which security is so much important is rely of communication process on radio waves. As they are not protected by any physical boundaries or walls rather than they are created to cover as much area as they can. And due to this they are more exposed for any kind of interception. After considering so many issues in security area, Second Generation (2G) system was developed. In 2G Global System for Mobile Communications (GSM) was most successful one. It was the first one which introduces encryption and cryptographic mechanisms for confidentiality and authentication of telephone system. But GSM also suffers from some security problems similar to weak encryption and authentication algorithms, along with short length of secret key and no authentication process for the network.

The Universal Mobile Telecommunications System (UMTS) is a Third Generation (3G) mobile system which was based on the Global System for Mobile Communications and specified by Third Generation Partnership Project (3GPP) [1]. It was developed on the success of GSM [2, 3, 4, 5]. UMTS offers more bandwidth and spectral efficiency to the network operators by using Wideband Code Division Multiple Access (WCDMA) technology.

This paper is organized as follows: Section II discuss about the security system in GSM. Section III explains about the security architecture of UMTS and 3GPP. Finally, conclusion is present in section IV.

II. GSM SECURITY

Global System for Mobile Communications (GSM) is a standard set which was used to illustrate protocols for 2G cellular network. GSM has been one of the most successful part of the 2G (Second Generation) mobile systems. TDMA was also one of the leading 2G technologies in the United States. One of the main features of 2G was the launch of information transmission in digital form through the air interface. Some advantages of 2G over the earlier ones were improved speech quality, better network capacity, easy data communication process and also enhanced security. The main goal of GSM security is to provide exact billings of phone calls. For the subscriber's authentication a secret key is stored in SIM cards and to protect the authentication, different types of cryptographic algorithms are used. The one of the excellent feature in GSM is its invisibility to the user.

Some essential security features of GSM are:

- User's authentication
- Use of temporary identities for the protection of user privacy
- Encrypted form for communication

But along with these advantages there are some disadvantages also, which are as following:

- Authentication triplets which contain ciphering keys are sent over network without any kind of protection
- Possibility of active attacks over the network

Subscriber's authentication process in GSM needs a secret key K, which is stored in following locations:

- In the users SIM card i.e. Subscriber Identity Module
- In the AuC i.e. Authentication center

The complete process of authentication is based on one key which is stored in user's mobile device. The authentication process is a challenge responsive mechanism which is based on one-way function [6]. The network releases a challenge to the mobile, which contains a random value, but the main attribute is that the challenge should be non-repeatable and also unpredictable. After receiving the challenge mobile device passes it to the subscriber identity module, which further computes an output from the help of one-way function. This output is then sent to the network. There also exists a expected output which is computed by network itself. When both the output gathers at network then it compares them with each other. If both values are

same then it ensures the authentication of mobile. But still there is one flaw in this communication. Suppose there is an active attacker which access a node from the middle of the communication process and showed that this is the end part of the communication line. To handle this kind of problem a cryptographic key can be used to protect the communication.

III. GSM CIPHERING

During the process of authentication a session key (Kc) is generated which is of secret in nature. With the help of this key and encryption algorithm A5, all calls are changed into encrypted form. There are three different standard A5 algorithms present, which are A5/1, A5/2 and A5/3. From these three algorithms A5/1 and A5/2 are confidentially managed by the association of GSM which provides them under some specific license only to its vendors [7]. The A5/3 is a new approach and it is based on f8 ciphering algorithm of UMTS and is easily available on websites also.

There are two main goals of GSM ciphering which are as following:

- Protection of call from eavesdropping scenario between the base station and the mobile device
- Protection of call from those who are non-paying users

The process of ciphering is managed by the base station, it also chooses the type of algorithm which has to be used for the process. But using only ciphering algorithm cannot provide complete protection, since some of them are also weak in nature [8]. This type of flaw in the security architecture of GSM has been improved in the 3G by using different algorithm for confidentiality and integrity over the air interface and by using mutual authentication.

IV. UMTS SECURITY

Design of third generation (3G) was initiated by some organizations like UMTS Forum, European Telecommunications Institute (ETSI), Telecommunications Conference (CEPT) and European Posts. The main idea behind this was to achieve global roaming, so that it will become easy for users to access their mobile systems throughout the world. In starting UMTS was only done on theoretical concepts. Later in 1998, organizations of five standards decide to combine efforts and generate global interoperability. 3rd Generation Partnership Project (3GPP) was formed by combination of some organizations such as Telecommunications Technology Association (TTA), Committee on Telecommunications of American National Institute of Standards (ATSI), ETSI, ARIB and TTC. Introduction of 3G changed the technology to WCDMA from TDMA but still requirements for security remain same.

V. MUTUAL AUTHENTICATION

UMTS provides some security mechanisms and one of them is Authentication and Key Agreement (AKA) protocol, which is designed to help an outside or foreign network in the authentication process of a roaming mobile device through the vectors which are generated by AuC in the home network. For the execution process of authentication and key agreement amount of time consumption is near about few hundred milliseconds only.

Mutual authentication means that both the network and the device engage in a response and challenge exchange. The main objective of authentication and key agreement is to verify that the network contains the secret key for the client and the client contains the secret key for the network, without any actual exchange of the key [9]. There are three entities which are involved in the process of authentication of UMTS system, these are [10]:

- Authentication Center (AuC) and Home Environment,
- Visitors Location Register (VLR),
- Terminal or USIM.

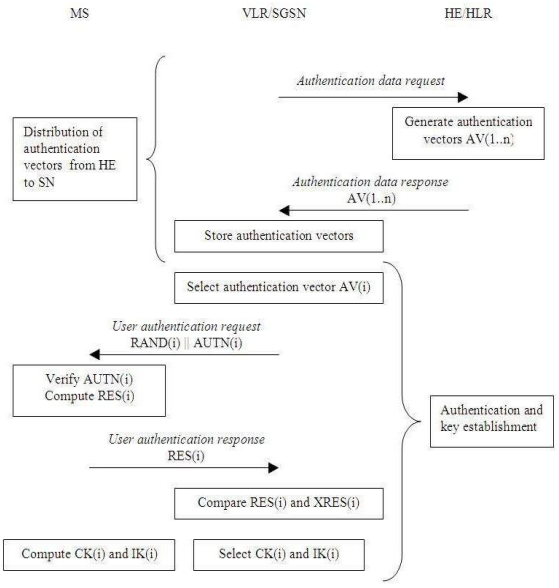

Fig 1: Working of AKA process in UMTS from [11]

When Home Environment receives an authentication request then it generates authentication vectors of five components Expected Result (XRES), Integrity Check (IK), Session Key (CK), Random Challenge (RAND) and Authentication Token (AUTN). Each of Authentication Vectors can be used only one time for the authentication of USIM [11]. Each of AV is generated using sequence number (SQN) and Key. After receiving these authentication vectors are stored in visitor location register. In the next step only one of the AV is selected and a user authentication request which contains RAND and AUTN is sent to the MS or Mobile Station. The MS then examines the network authentication token (AUTN) by verifying the SQN is not in sync then it discards the authentication process but also allows for retry. If SQN and AUTN are correctly verified by the Mobile Station, then it shows that the network has been successfully authenticated by the client.

After this MS generates its own RES or authentication response by using both RAND and Key then send it to the network. Network then also compares the RES and XRES similarly like GSM. If both the values are equal then it shows the successful authentication to the network and the client.

VI. AUTHENTICATION VECTORS OF AKA

The main core of the authentication mechanism in AKA is combination of authentication vectors. Each AV is used for one session of authentication and key agreement between the AuC or the HE and the Mobile Station.

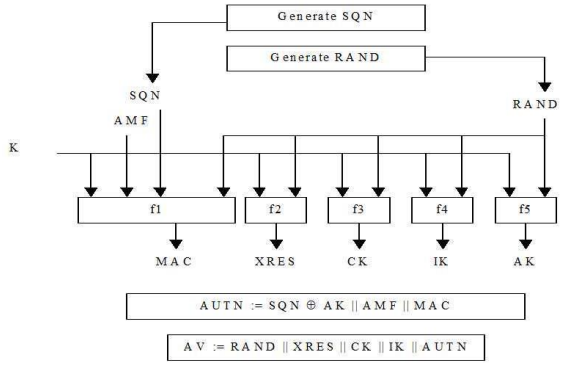

Fig 2 : Authentication vectors generation process from [11]

The authentication vector AUTN is of size 16 bytes, IK is of size 16 bytes, CK is of size 16 bytes, XRES is of size range between 4-16 bytes and RAND is of size 16 bytes. There are seven algorithms which are used for cryptography process of AKA in UMTS [12, 13, 14, 15]:

f1 : Calculation of Message Authentication Code (MAC)
f1* : Calculation of MAC-S
f2 : Calculation of RES and XRES
f3 : For the computation of CK
f4 : For the computation of IK
f5 : For the computation of AK
f5* : For the computation of AK but in the re-synchronization process

There are some flaws in 3GPP – AKA protocol, which are as follows:

- Transmission process of Authentication vectors is unsecure
- Difficulty in operating sequence number
- Incomplete bidirectional authentication process
- Only same key is shared between mobile equipment and home environment

VII. CONCLUSION

Since the cellular communication systems are the base line for the future communication services, the security part is essential. In this paper we explore some features and beneficial points of GSM and UMTS. In this we also elaborate the use and implementation of AKA mechanism along with its mutual authentication which helps to eliminate the chances of man-in-the-middle attacks which were quiet possible with GSM. But still there are some flaws in AKA protocol which have an area for future work.

REFERENCES

[1] IP Security Protocol, Internet Engineering Task Force (IETF). Working Group, http://www.itef.org/html.charters/upsec-cgarter.html, 2002.

[2] Johnson, M., Revenue Assurance, Fraud and Security in 3G Telecom Services, VP Business Development Visual Wireless AB, Journal of Economic Management, Volume 1, Issue 2, 2002.

[3] Stalling, W., Cryptography and Network Security, Principles and Practice, 3rd edition, USA, Prentice Hall, 2003.

[4] Stefan, P, and Fridrich R., Authentication Schemes for 3G mobile radio, Systems, The Ninth IEEE International Symposium on, 1998.

[5] Zhang, M. and Fang, Y., Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol. IEEE Transactions on wireless communications, Vol. 4, No. 2, 2005.

[6] ISO/IEC 9798-4: 1999, Information technology – Security Techniques – Entity authentication – part 4: Mechanisms using a cryptographic check function.

[7] GSM Association, http:// www.gsmworld.com/using/algorithms/index.shtml

[8] E. Babbage and E. Biham and N. Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communicatio, Proceedings of Crypto 2003, Springer- Verlag, 2003.

[9] 3GPP TS 21.133. 3GPP Security; Security Architecture.

[10] Lin, H., Security and Authentication in PCS. Computers & Electrical Engineering, Vol. 25, No. 4, 1999.

[11] 3GPP TS 33.102 version 8.4.0 Universal Mobile Telecommunications System (UMTS); LTE; 3G security;
Security architecture, http://www.3gpp.org/ftp/specs/html-info/33102.html.

[12] A. Canteaut and M. Videau. Degree of Composition of Highly Nonlinear Functions and Applications to Higher Order Different Cryptanalysis. In Lars Knudsen (Ed.) Advances in Cryptology – Eurocrypt 2002, Lecture Notes in Computer Science 2501, Springer – Verlag, 2002.

[13] 3GPP TS 35.205. 3GPP Security; Specification of the MILENAGE Algorithm Set; Document 1: General.

[14] 3GPP TS 35.206. 3GPP Security; Specification of the MILENAGE Algorithm Set; Document 2: Algorithm specification.

[15] 3GPP TS 35.207. 3GPP Security; Specification of the MILENAGE Algorithm Set; Document 3: Implement test data.

[16] Walker, M., On the Security of 3GPP Networks, http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000/mike_walker.pdf, 2003

AUTHORS

First Author – Jyoti Kataria, Amity University, Noida, Uttar Pradesh, Kataria.jyoti87@gmail.com
Second Author – Dr. Abhay Bansal, Amity University, Noida, Uttar Pradesh, abansal1@amity.edu