ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

Designing Authentication for Wireless Communication Security Protocol

Ms. Roshni Chandrawanshi, Prof. Ravi Mohan, Mr. Shiv Prakash Chandrawanshi

***Abstract*— Security is considered an important issue for mobile communication systems. In particular, the design of authentication mechanisms has received considerable research interest recently. However, most of the current authentication schemes for mobile systems only have simple security functions and usually have some weaknesses, such as leakage of user identities and high update overhead of temporary identities. Moreover, these schemes cannot fulfill the security requirements specified in third generation mobile systems (IMT-2000, UMTS). In this paper, we propose a secure and flexible authentication framework for mobile communication systems. In the proposed framework, service providers can dynamically choose authentication mechanisms without the cooperation of network operators in visited domains. Based on the new framework, a secure authentication protocol is proposed. The proposed protocol can satisfy the security requirements of third generation mobile communication systems.**

***Index Terms*— network security, flexible authentication framework, authentication protocol, mobile networks, 3G communication systems.**

1.. INTRODUCTION

An analysis model is a description specifically created to examine and evaluate an object. Such description is realized using a formal language and it reflects properties or behaviors of the original object, while it abstracts from other aspects. In general, the objects of interest may be anything, like complex physical phenomena or computer systems composed of parallel processes executing together.

The objects we consider are security protocols, also known as cryptographic protocols. Security protocol principals, such as human beings or computers, execute a security protocol by exchanging messages over a medium to achieve some particular goal. We assume that such a medium (the network) is not private to the principals, but shared between all other participants. This implies that other participants not taking part in the execution may still see messages passing by, and potentially play an active role in the communication. Moreover, participants do not necessarily trust each other, and thus principals executing the security protocol cannot rely on other participants to simply avert their eyes and behave honestly. A prominent example of such a medium is the Internet. On the other hand, a good identity authentication system means that no unauthorized user gets the required services from the home system. In the original design, mobile users are authenticated by using a shared secret cryptographic system. To equip the GSM system with better power of security, in this paper, we shall focus on developing the solutions to possible user authentication.

2. GSM Network:

In the GSM Network, three subsystems involved are the mobile station (MS) subsystem, the base station subsystem, the home subsystem. The MS subsystem consists of the mobile equipment (ME) and the smart card called equipment is uniquely identified by the international mobile equipment identity. The SIM card contains the International subscriber to the system, a secret key for authentication, and subsystem consists of the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These are the connections between the mobile stations and the Mobile Switching Centre (MSC). The home subsystem is composed of five parts, the Mobile Switching Center (MSC), the

Manuscript received Sep 15, 2012.

Ms. Roshni Chandrawanshi , Electronics & communication shri ram institute of science & technology, jabalpur, m.p. India. Jabalpur M.P., India

Prof. Ravi Mohan, Electronics & communication shri ram institute of science & technology, jabalpur, m.p. India.

Mr. shiv prakash Computer science, HCET Jbp. M.P. India.

Home Location Register (HLR), the Visitor Location Register (VLR), the Center (AuC), and the Equipment Identity Register (EIR). We explain the diff HLR and VLR as follows. The HLR is a database that contains complete information of the local customer. It is the main database. The VLR contains the roamer information. The VLR make sure that you are a valid subscriber and then retrieves distant HLR to manage your call.

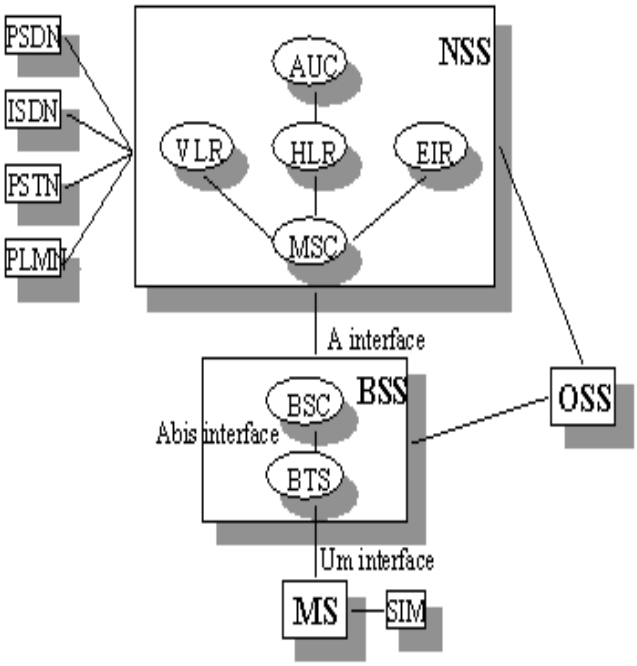

Figure 1: GSM architecture.

3. The Operation Modes:

In our framework, the authentication server maintains the profiles and privileges of registered clients. Thus, only the client's home authentication server has the ability to initially authenticate the client. Another entity, the authentication proxy, is mainly responsible for forwarding the client's authentication request to the authentication server. In the proposed framework, after initial authentication has been performed, the authentication proxy is then capable of authenticating the client when subsequent authentication is required. That is, the proposed authentication framework contains two operation modes for initial and subsequent authentication

3.1 Initial Authentication:

When the client *c* leaves his home domain and roams to a visited domain, the initial authentication shown in Fig. 2 is performed among the three parties. First, the request message $Request_c$ is generated by the client *c* and sent to the authentication proxy *p* in the visited domain. Since the authentication proxy is unable to authenticate the client *c* by Itself, it generates a Forwarded $Request_c$ containing the $Request_c$ and forwards it to the designated authentication server *s* in c's home domain. The verification procedure is performed by the authentication server *s*, and a response message $Response_s$ is generated Corresponding to the authentication result. The authentication proxy forwards the Forwarded $Response_s$ containing the $Response_s$ to the client and decides whether or not to provide the service to the client according to the authentication result.

Here, the authentication Proxy caches some authentication information, which can be used in subsequent Authentication. The response message $Response_c$ lets the client *c* know whether the authentication was successful or not. After the initial authentication, both the proxy *p* and client *c* obtain the authentication result from the authentication server and share some secret information.

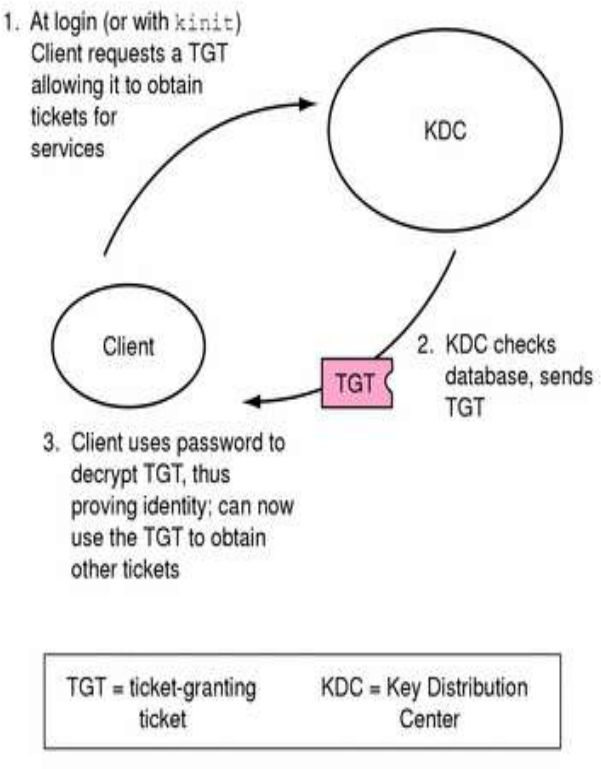

Figure 2: Initial Authentication

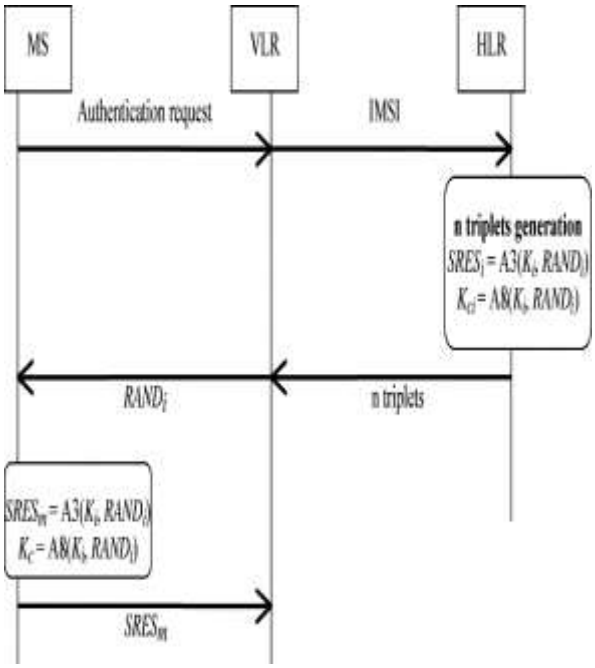

Figure 3 GSM authentication protocols

4. Analysis of current GSM Authentication protocol-

4.1 Working of Protocol

Let's first see the working of the existing GSM authentication protocol as shown in the figure 3. The details are described as follows:

(1) When MS enters a new visiting area and requires new communication services, he/she sends an authentication request to the visited VLR. The request contains the TMSI and the LAI.

(2) After receiving the TMSI, the new VLR can use the TMSI to get the IMSI from the old VLR. Then the new VLR sends the IMSI to HLR.

(3) The HLR/AuC then generates *n* copies of the triplet authentication parameters {*RAND*, *SRES*, *Kc*} at a time for the mobile station to use later for each call, and then the HLR sends them to the VLR through a secure channel.

(4) After receiving these authentication parameters, the VLR keeps them in its own database and then he/she selects a triplet {*RAND*, *SRES*, *Kc*} to authenticate the mobile station for each call. Then the VLR forwards the selected *RAND* to the MS.

(5) When the MS receives *RAND*, he/she can compute *SRES* and *Kc* and send the computed *SRES*' back to the VLR. Then the MS keeps *Kc* for secret communication.

(6) Once the VLR receives *SRES*' from the MS, it compares it with the selected *SRES*. If they are the same, the MS is authenticated; otherwise, the MS is not a legal user.

5. Drawbacks of Existing Protocols -

(a) Not supporting Bilateral Authentication: This is the major setback of the existing protocol, in which the MS can be authenticated by the VLR but VLR cannot be authenticated by the MS thus supporting unilateral authentication.

(b) Huge Bandwidth consumption between VLR and HLR: As per the existing protocol each time when MS wants to establish a session, VLR has to request for the authenticity of that MS from the HLR thus consuming huge bandwidth.

(c) Storage space overhead in VLR: Since each time HLR sends the n copies of RAND number to the VLR, thus VLR have to save all these n copies in its database thus making the database of VLR overloaded.

(d) Overload in HLR with authentication of MS: Since every time VLR request to the HLR for the authenticity of MS thus making the database of the HLR overloaded.

(e) Man- In- Middle attack: Since in the existing protocol there is unilateral authentication, so any unauthorized user can be able to know the contents of the session that is going on between MS and VLR because VLR is not authenticated by the MS

.

(f) Impersonating attacks: Any attacker can impersonate himself as VLR and try to get the required data for him because this existing protocol supports unilateral authentication and MS can easily be fooled by the attacker.

6. Distribution of IDv to each VLR-

In this phase HLR will distribute a unique identification value to each VLR which comes under its region. This IDv help the VLR to be authenticated by the mobile station when the certificate is generated with the help of Ki and A3 security algorithm.

6.1 Mutual Authentication Phase-

This is the last phase of our proposed protocol, in this phase mobile station and the VLR will be authenticated by each other during the calls made and attended by the mobile station with the help of HLR. So this proposed protocol will provide the mutual authentication between MS and VLR.

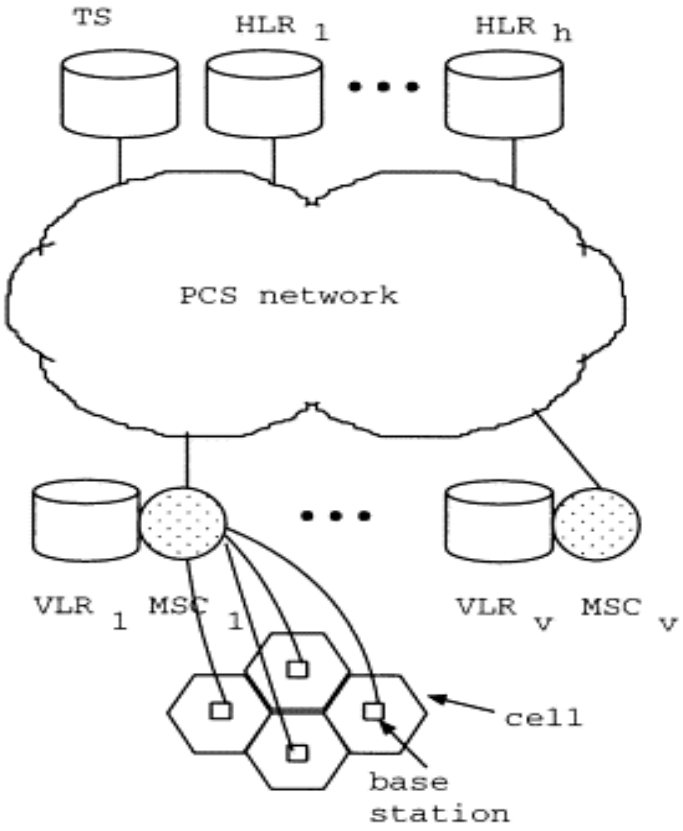

Figure 4: Mutual authentication phase

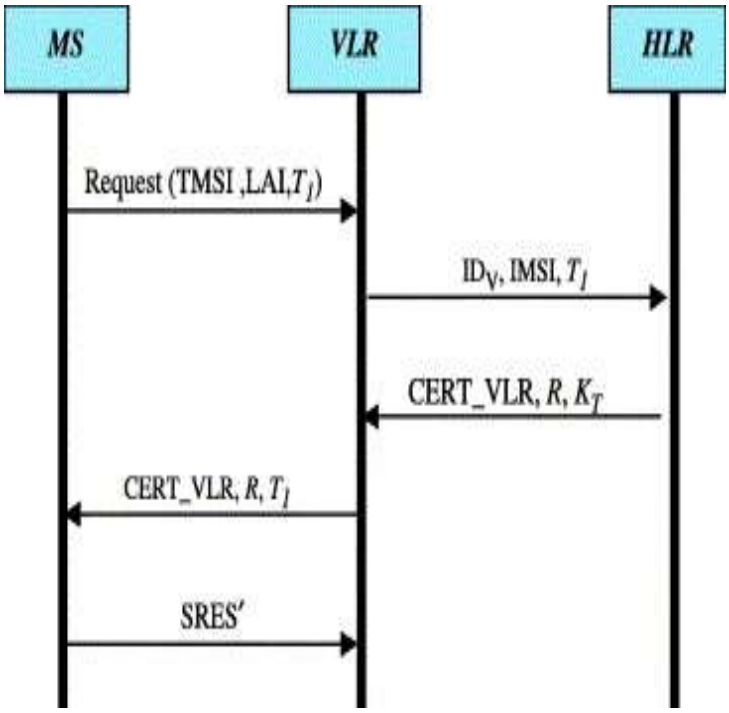

Figure 5: Mutual Authentication Phase

7. Conclusion-

Nowadays, 3G mobile systems are becoming more and more popular in the market. However, the cost for base station construction is still very high. Many telecommunication companies still use the old standard of GSM or integrate the GSM system with their 3G systems. Therefore, the GSM system is still popular and widespread because of its simplicity and efficiency. Many authentication protocols have been developed to improve the original authentication protocol of GSM, but mostly cannot solve the problems without modifying the architecture of GSM. In the authentication framework, the authentication server can dynamically choose which authentication mechanism to use for each authentication request. Moreover, this property provides service providers with the ability to develop proprietary authentication mechanisms and adjust the security policy in run time. In this paper, we have pointed out the drawbacks of the GSM authentication protocol and presented a new authentication protocol that can fix all the drawbacks. Also, the concept of this protocol can also be applied to 3G mobile systems.

References-

1. G. Horn, K. M. Martin, and C. J. Mitchell, "Authentication protocols for mobile network environment value-added services," *IEEE Transactions on Vehicular Technology*, Vol. 51, 2002, pp. 383-392.

2. M. Looi, "Enhanced authentication services for internet systems using mobile networks,"*IEEE Global Telecommunications Conference*, Vol. 6, 2001, pp. 3468-3472.

3. G. Vanneste *et al.*, "Authentication for UMTS: introduction and demonstration," *The 2nd International Distributed Conference on Network Interoperability*, 1997, pp. 715-721.

4. WAP Forum, "Wireless application protocol 2," WAP 2.0 Technical White Paper, http://www.wapforum.org/, 2002.

5. J. Kim, M. Oh, and T. Kim "Security requirements of next generation wireless communications," in *Proceeding of International Conference on Communication Technology*, Vol. 1, 1998, pp. S2802-1-6.

6. ITU-R Rec. M.1078, "Security principles for international mobile telecommunications- 2000 (IMT-2000)," 1997.

7. A. Barba, F. Recacha, and J. L. Melus "Security architecture in the third generation networks," in *Proceedings of IEEE Singapore International Conference on Networks/ International Conference on Information Engineering* '*93*, Vol. 1, 1993, pp. 421-425.

8. S. Putz, S. Putz and R. Schmitz, "Secure interoperation between 2G and 3G mobile radio networks," *The 1rst International Conference on 3G Mobile Communication Technologies*, 2000, pp. 28-32.

9. S. Miller, C. Neuman, J. Schiller, and J. Saltzer, "Section E.2.1: Kerberos authentication and authorization system," M.I.T. Project Athena, Cambridge, Massachusetts, 1987.

10. Chin-Chen Chang*, Jung-San Lee, Ya-Fen Chang(2005).") *Efficient authentication protocols for GSM*".Computer Communications,28,921-928.