RESEARCH ARTICLE OPEN ACCESS

GSM Mobile Authentication Based On User SIM

Sandip Mishra[1], Dr. Nilesh Modi[2]
Research Scholar[1], Research Guide[2]
Department of Computer Science
Karpagam University, Coimbatore
Tamil Nadu - Chennai

ABSTRACT

This paper will introduce about authentication mechanism of mobile communication Network in GSM which how user will make mobile authentication is done in network. This mechanism will use how encryption is done in mobile and base station. The purpose of this paper is to analyze the effectiveness of current authentication mechanism in mobile communication. This paper also declare about how different types of algorithm used in mobile to authenticate with base station and mobile switching center. This paper also introduce about how all the mobile handset uses unique identification for getting connected with mobile network. Using Mobile SIM authentication subscriber will performs several encryption methodologies to getting connected with other mobile user.

Keywords:- GSM (Global System for Mobile Communication), AAA (Authentication, Authorization, and Accounting), NSS(Network Subsystem), EAP (Extensible Authentication Protocol), HLR (Home Location Register)

I. INTRODUCTION

In this paper we have discuss about GSM authentication mechanism. In GSM (Global System for Mobile Communication) uses symmetric cryptography for encryption and authentication which uses standardization cryptosystem for whole world telecommunication network. Main objective of GSM mobile communication is to make mobile phone system secure. [1] This is very much secure for public switched telephone network. GSM uses symmetric cryptography to make authentication of mobile station and base station and to protect confidentiality of user data and information during transmission from mobile device to base station. In GSM mobile communication mobile station and network share common secret key for entire communication.

In GSM secret key distribution is done between mobile handset and a smart card SIM (Subscriber identity module). When subscriber receives its SIM (Subscriber identity module) at that time it will sign up for service. After that subscriber receive a PIN (Personal Identification Number) which unlocks that card. After unlocking a SIM card IMSI (International mobile subscriber identity) which uniquely identifies mobile phone number for after communication with mobile network. A subscriber authentication key Ki, Which is 128-bit key has been used for authentication centre (AC) in its home network environment.

II. SIM BASED AUTHENTICATION MECHANISM

Currently cellular operators are work on how to incorporate WLANs (Wireless Local Area Network) in their service substance and business framework. Currently GSM (Global System for Mobile Communications) operators furnish Subscriber Identity Module (SIM) for each subscriber on their system. World-wide, GSM systems are the most widely distribute digital cellular mobile network regulation. The role of SIM is to certify the user on the GSM network and to alleviate impressive billing. Operators are now seeking to pass this SIM-authentication functionality to WLAN services, instead of the present username id/password or prepaid service WLAN authentication methods. [2] This paper will provide a little summary of the validation process in a GSM network, and will then describe a method of WLAN authentication using SIM cards.

A) SIM - Subscriber Identity Module

SIM (Subscriber identity module) in GSM networks is to secure that only licensed users can approach the network. In order to authenticate a user, it must be able to store data, protector against unauthorised right to the stored data, and execute a cryptographically algorithmic program under secured conditions.[5] The mobile device and SIM (Subscriber identity module) is authenticated with a background system. The data transferred between the base station and mobile station across the air surface is encrypted.

B) Authentication on GSM Networks

GSM Network contains three main Components.

1) Mobile station or mobile phone has SIM (Subscriber identity module) which provides the identity to unique user while communication with other user.
2) Base station subsystem, who communicates to user on mobile station to other mobile/landline user in mobile network.
3) Network Subsystem (NSS), which is resourceful of routing calls and from the non-moving network via the BSC (Base Station Controller) and BTS (Base Transceiver Station) to different mobile stations or other communicating medium.

SIM(Subscriber identity module) authentication procedure on GSM mobile networks checks valid ness of the subscriber's SIM(Subscriber identity module) card and then resolve whether the mobile station is allowed for particular network communication or not. The both communicating parties are involved in the authentication process are end user or holder of the SIM (Subscriber identity module) card and a non-grey listed and certified handset and other the network operator (GSM service provider).[6] Authentication process is one-way since the user is being authenticated firstly to the phone through the PIN number and then the operator though their SIM (Subscriber identity module) based AAA (Authentication, Authorization, and Accounting) mechanism. The network authenticates the subscriber which is shown in figure through the use of a challenge-response method: [7, 8, 9, and 10]

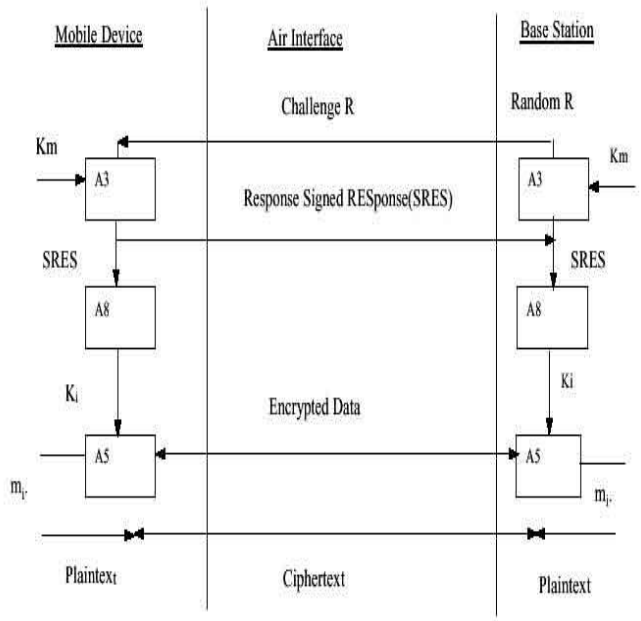

Fig.1 Authentication between mobile and base station

1) A subscriber wants to conduct phone conversation, the mobile station sets up a radio link to the base station, and relays the IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity) from the SIM(Subscriber identity module) to the base station.

2) The subscriber's IMSI registers at the base station, the mobile station receives the 128 bit random number (RAND) transmitted through air interface, which is passed to SIM (Subscriber identity module).

3) The RAND is passing to the SIM (Subscriber identity module) card, which is sent through with A3 algorithm jointly with card specific key (Ki). The result of A3 algorithm is the signed response (SRES).

4) The output of a cipher text block, SRES, which is transferred from to the mobile station to base station via the air interface medium.

5) When network subsystem, which is connected to the base station, derives the card specific key from IMSI and performs computational part to the SIM (Subscriber identity module) and generates SRES' for communication.

6) The Signed Response (SRES) sent to the network subsystem and then compared with the SRES' to authenticate the subscriber and thus authorize him/her to place a call between caller and collie.

7) In background process, system and SIM (Subscriber identity module) uses A8 algorithm with RAND number and card specific key (Ki) to generate the temporary ciphering key (Kc), which is used to encrypt data for transmission through the air interface medium.

8) The newly computed ciphering key (Kc) is then passed from SIM to mobile station, which performs data encryption method and decryption method using A5 algorithm.

C) SIM Based Authentication

Authentication mechanism allows an operator insure that only authorized subscribers in the ownership of an operator supplied SIM(Subscriber identity module) card (i.e., using a phone that is not purloined) are the only ones allowed to make calls on the network. Validation ensures that network is being used by paying customer and the call ends up making actual income for the operator.

There are few drawbacks in the GSM security architecture and algorithms that makes it vulnerable to fraud detection in network. There must be two types of fraud are possible – one is, making "free" calls using a stolen SIM(Subscriber identity module) and/or equipment and other one is, making "free" calls using a cloned SIM(Subscriber identity module). ETSI (European Telecommunications Standards Institute), the Global System for Mobile Communications standards body, has been making several improvements in the Global System for Mobile Communications security (improved cryptographic algorithm, etc) while Global System for Mobile Communications operators have setup sophisticated fraud detection and management system. For example, Global System for Mobile Communications networks prohibit duplicate SIMs to be active simultaneously, Global System for Mobile Communications handsets will not work without a SIM(Subscriber identity module), and handsets are verified against a database to determine if they are stolen and are then restricted to emergency calls only.

III. SIM BASED AUTHENTICATION IN WIRELESS NETWORKS

A) Wireless Authentication Process

SIM based WLAN authentication requires to use of a SIM reader connected to the computing device, so that the authentication software can perform several SIM credentials. The EAP-SIM protocol, resident on the client, specifies the Extensible Authentication Protocol (EAP) mechanism for authentication and session key distribution using GSM SIM.

EAP-SIM performs several RAND challenges are used for creating several 64-bit key (ciphering keys) is (Kc), which are combined to create a longer session key. EAP/SIM also enhances the basic GSM authentication mechanism by associated the RAND challenges with message authentication code in order to provide mutual authentication. The EAP-SIM client starts the authentication process by connecting to the AAA (Authentication, Authorization, and Accounting) server. The AAA (Authentication, Authorization, and Accounting) server issues a challenge over the 802.11b radio interface, which is then forwarded to the SIM reader by the EAP-SIM client. The EAP-SIM client communicates to the SIM through the SIM reader, the SIM calculates the response that contains the SRES and Kc, which is sent to the EAP-SIM client. The EAP- SIM client then forwards the response to the AAA (Authentication, Authorization, and Accounting) server, which then checks the response and provides access appropriately. In this scenario it is assumed that the AAA (Authentication, Authorization, and Accounting) server has a secure connection to GSM backbone network mechanism like HLR.

B) GSM Authentication

UMTS addresses these weaknesses in a number of ways. Like GSM, a one pass authentication and key agreement (AKA) procedure is used with immediate activation of ciphering after successful authentication. When a mobile station first connects to the network it sends its identity (IMSI or T-IMSI) which is stored on the SIM card. In case the subscriber is not known by the MSC/VLR, which is responsible circuit switched connections, or the SGSN, responsible for a packet sessions, authentication information has to be requested from the authentication centre which is part of HLR (cp. figure 1.14). In addition to the random number (RAND), the expected response (SRES, referred to as XRES in UMTS) and the ciphering key (Kc, referred to as CK in UMTS) which are already known from GSM, two additional values are returned. These are the integrity key (IK) and the authentication token (AUTN). Together, these five values form an authentication vector.

C) The Authentication Token

Authentication Token (AUTN), which is new in UMTS, serves two purposes. The AuC creates the AUTN using a random and the secret-key of the subscriber mobile. Then it is forwarded combine with the random number to the mobile in a MM (mobility management) authentication request message. All other values are retained at the MSC (Mobile Switching Centre)/VLR (Visitor Location Register) or Serving GSN for the moment. The mobile station then uses the AUTN to verify that the authentication procedure was initiated by validate authorized network. The authentication token in addition includes a sequence number which is enlarged in both the network and the mobile after every victorious authentication. This prevents third parties involvement using intercepted authentication vectors for fake authentications later on.

D) Security Standards in Wireless (MAN)

WMAN (WiMAX) security standards largely include 802.16 D3, 802.16E and WiBro. 802.16 D3 defines a safe and sound sub-layer on MAC layer to assurance security. Safe and sound sub-layer consists of main two protocols: Data Encryption Encapsulation Protocol and Key Management Protocol (PKM). Data Encryption Encapsulation Protocol defines encryption collection supported by IEEE 802.16 protocol, which includes data encryption and integrity confirmation algorithm, rules of implementing these algorithms to MAC PDU load. This Key management protocol defines secure distribution way of key management principle of data from base station to user workstation and key data management and limitations to access network services.802.16e is improved based on the 802.16d to support vehicular and mobile services between 2.11GHz band, and support handoff between station and sector. It is mainly to solve few running problem solving deficiencies of original 802.16 security mechanism. IEEE 802.16e protected sub-layer supports PKMv1 and PKMv2 two versions. PKMv2 can supports broadcasting and multicasting service between MSS and BS for mutual authentication, etc. Standards of WiBro (Wireless Broadband) is beginning in January 2004, is to be developed from the Electronics and Telecommunications Association (ETRI), Samsung Electronics and HPI (High Speed Portable Internet) project launched by South Korea's major operator. South Korea's Ministry of Information and Communication declared definitely that WiBro should fully comply with 802.16e and began to coordinate with 802.16e to integrate WiBro and 802.16e.

E) Security Analysis of EAP

Extensible Authentication Protocol (EAP) is a general protocol for PPP authentication which can support multiple authentication methods. EAP didn't specify authentication method during the link establishment period, but defer the process to certification stage. So certification side can get more information in order to decide which authentication method to use. This mechanism also allows the parties of PPP authentication passing through the received certification packet to the authentication server at the rear, so that authentication server from the rear can realize a variety of authentication methods. WPA and WPA2 both can support to provide stronger authentication with EAP. The advantages of EAP can support multiple authentication mechanisms without having to specify in the pre-consultation process of LCP stage. Currently, EAP security issues are:

1) ***Identity Protection:*** Identity exchange is optional in the EAP, so it may be completely ignored.
2) ***Man in Middle Attack:*** When EAP run in other protocol, if the other side authentication is neglected, it will lead to a middleman attack.
3) ***Modify the packet:*** EAP is to be ensuring the data packet's source authentication, integrity and anti-replay

mechanism, but this protection is not sort enough in the EAP layer, so a challenger can fruitfully insert or replay EAP packets by guessing identifier.

4) ***Dictionary attacks:*** Password-based authentication method (such as EAP-MD5, MS-CHAPv1) cannot resist a dictionary attack, so intends to adopt some against-dictionary attacks.

5) ***Links to the untrusting network:*** EAP support one-way authentication (such as EAP-MD5), as the user don't authenticate the authentication device, resulting in the user easy to be deceived by fake authentication device.

IV. AUTHENTICATION ALGORITHM FOR GSM

The main limitation of security in cellular communication network is result of all cellular communication is sent over the air interface, which then gives rise to terrorization from eavesdroppers with suitable receivers. This thing keeping this in account, security pedals were incorporated into GSM to make the system as secure as PSTN (public switched telephone networks). The security functions are given below:

A) Anonymity: It implies that it is not too simple and too easy to track the user of the system. According to Srinivas (2001), when a new GSM subscriber switches on his/her mobile phone for the first time, its International Mobile Subscriber Identity (IMSI), i.e. real identification is used and a Temporary Mobile Subscriber Identity (TMSI) is issued for the subscriber, which from that time forward is always used. Use of this TMSI, prevents the gratitude of a GSM user by the potential eavesdropper.

B) Authentication: This will checks the uniqueness of the holder of the smart card and then decides whether the mobile station is allowed on a particular network. The authentication by the network is done by a answer and challenge method. A random 128-bit number (RAND) is created by the network and sent to the mobile. The mobile uses this RAND as an input and through A3 algorithm using a secret key Ki (128 bits) assigned to that mobile, encrypts the RAND and sends the signed response (SRES-32 bits) back. Network.

A3

SRES (made of 32-bit)

RAND Challenge (made of 128-bit)

Ki (made of 128- bit)

Performs the same SRES process and matches its value with the response it has received from the mobile handset so as to check whether the mobile contains secret key. This authentication becomes victorious when the two values of SRES match which enables the subscriber to join the network. Since every time a new random number is generated, eavesdroppers don't get any relevant information by listening to the channel.

C) User Data & Signaling Protection:

A8

Kc (made of 64-bit)

RAND Challenge (made of 128-bit)

Ki (made of 128- bit)

Mr. Srinivas stated that to protect both user data & signaling, GSM uses cipher key. After the authenticating the user, the A8 ciphering key generating algorithm (stored in the SIM card) is used. Taking the RAND and Ki as inputs, it results the ciphering key Kc which is to be sent through. To encipher or decipher generated the data, this Kc (54 bits) is used with the A5 ciphering algorithm. This algorithm is enclosed within the hardware of mobile phone so as to encrypt and decrypt data while roaming.

Algorithms used to make mobile traffic secure.

D) Authentication Algorithm A3: One way function, A3 is an operator-dependent stream cipher. It computes the output of SRES by using A3 is easy but it is difficult to discover given input (RAND and Ki) from the output. To face the issue of international wandering, it was compulsory that each operator may choose to use A3 autonomously. The basis of GSM's security is to keep Ki secret (Srinivas, 2001)

E) Ciphering Algorithm A5: In recent times, many series of A5 exists but the most common ones are A5/0(unencrypted), A5/1 and A5/2. Because of the export regulations of encryption technologies there is the existence of a series of A5 algorithms (Brookson, 1994).

F) A8 (Ciphering Key Generating Algorithm): As given in A3 algorithm, it is also operator-dependent. Most providers join A3 and A8 algorithms into a single hash function known as COMP128. The COMP128 creates KC and SRES, in a single instance (Huynh & Nguyen, 2003).

V. CONCLUSIONS

This paper will elaborate about how false base station performs with different subscriber and mobile switching center. How data are lost during transmitting from one location to another location and then it will regenerated from impersonate user using same SIM based authentication. Also this cases a vulnerability of algorithm that is to be cracked by any particular attacker. Using this attacker can access call, use call forwarding, and conference call. The real issue with GSM security is to designing goals is too much limit. The major

loop holes in security in GSM include the weak cryptography mechanism. Secondly SIM issues, like fake profile of base station, and totally lack of replay attack. GSM was commercially successful. It is interesting to consider GSM achieved GSM Security designing goal.

This paper also declares about authentication algorithm will uses mutual encryption and decryption algorithm to get key from subscriber and mobile handset.

ACKNOWLEDGMENT

A special thanks to Prof. Dr. Nilesh K. Modi. (Professor and Head of the Department, S V Institute of Computer Studies, Gujarat, India) who provide me guidance in Mobile communication network to understand with better hands.

REFERENCES

[1] Start 3GPP Technical Specification, "3GPP TS 33.102, V5.3.0, Third Generation Partnership Project; Technical Specifications Group Services and System Aspects; 3G Security; Security Architecture," September 2003

[2] E. Barkan, E. Biham, and N. Keller, "Instant cipher text-only cryptanalysis of GSM encrypted communication," in Advances in Cryptology – CRYPTO 2003 , vol. 2729 of LNCS , pp. 600–616, August 2003.

[3] D. Fox, "Der IMSI-catcher," DuD, Datenschutz und Datensicherheit, 2002.

[4] ETSI Technical Specification, "ETSI TS 100.929, V8.0.0, Digital Cellular Telecommunications System (phase 2+)(GSM); Security related network functions," 2000.

[5] U. Meyer and S.Wetzel, "A man-in-the-middle attack on UMTS." In submission.

[6] 3GPP Technical Specification, "3GPP TS 35.202 V5.0.0, Third Generation Partnership Project; Technical Specification Group; 3G Security; specification of the 3GPP confidentiality and integrity algorithms; document 2: Kasumi algorithm specification," Jun 2002.

[7] M. G. I. Briceno and D. Wagner, "A pedagogical implementation of the gsm A5/1 and A5/2 "voice privacy" encryption algorithms." http://cryptome.org/gsm-a512.htm, 1999.

[8] J. Golic, "Cryptanalysis of alleged A5 stream ci-pher," in Advances in Cryptology ,vol. 1233 of LNCS , pp. 239–255, Springer Verlag.

[9] A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of A5/1 on a pc," in Advances in Cryptology, proceedings of Fast Software Encryption'00 , vol. 1978, pp. 1–18, Springer-Verlag, 2001.

[10] E. Biham and O. Dunkelman, "Cryptanalysis of the A5/1 gsm stream cipher," in Progress in Cryptology, proceeding s of Indocrypt"00, LNCS, pp. 43–51, Springer- Verlag , 2000.

[11] P. Ekdahl and T. Johansson, "Another attack on A5/1," Transactions on Information Theory , vol. 49, pp. 284– 289, 2003.

[12] I. Goldberg, D. Wagner, and L. Green, "The (real-time) cryptanalysis of A5/2." Presented at the Rump Session of Crypto'99, 1999.

[13] S. Petrovic and A. Fuster-Sabater, "Cryptanalysis of the A5/2 algorithm." Cryptology ePrint Archive, Report 200/052, http://eprint.iacr.org, 2000.

[14] U. Meyer, K. Kastell, and R. Jakoby, "Secure handover procedures," in Proceedings of the 8th Conference on Cellular and Intelligent Communications , October 2003.

[15] Boman, K., Horn, G., Howard, P. and Niemi, V.: UMTS security. Electronics & Communication Engineering Journal, Oct 2002, pp. 191-204.

[16] TS 33.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture.

[17] TS 33.402, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security aspects of non-3GPP accesses.

[18] IETF RFC 5448: Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA').