Enhancing Security in GSM

Chenthurvasan Duraiappan Yuliang Zheng *
University of Wollongong

E-mail: [g9215360, yuliang]@cs.uow.edu.au

Abstract

This paper points out certain weaknesses in the existing security system of Global System of Mobile Communications (GSM) and proposes a better security system for GSM. The proposed security system provides an authenticated session key distribution protocol between the authentication center (AUC) and the mobile station (MS) for every call attempt made by a MS. At the end of an authenticated session key distribution protocol, the identities are mutually verified between the AUC of a Public Land Mobile Network (PLMN) and the Subscriber Identity Module (SIM) of a MS as well as the session key for call encryption is distributed to the MS.

Keywords:
GSM, Secure protocols, Key Distribution, Authentication, Encryption, Roaming.

1 Introduction

Mobile communications have been known to be vulnerable to interception and unauthorized access. In recent years, both public and private sectors extensively rely upon mobile communication networks for communicating sensitive technical, financial, political and personal information. Securing this information and its transmission as well as the access to the mobile network is necessary for the secure and smooth operation of the system. The Global System of Mobile Communications (GSM) is the first digital cellular mobile communication system, with mobility between 17 different European countries and have integrated security features like digital encryption and authentication with the special active role played by smart cards. This paper explains the existing security system for GSM then points out certain weaknesses in the current security systems and proposes a new security system for GSM. For a more elaborate description of cellular mobile communication principles, existing security systems and terminologies, the reader is referred to [2].

*Support for this work was provided in part by Australian Research Council under the reference number A49232172 .

2 The Existing Security System in GSM

In the GSM, the security system provides three different security functions from the user's point of view. They are explained below.

2.1 Temporary Identities

Each subscriber of the GSM network has a unique international mobile subscriber identity (IMSI) that is nothing but the mobile station's service number in the GSM PLMN. Using this unique number one can easily find, which mobile network a mobile station belongs to. So within the network and the radio link between a mobile station and the base station (BSS), instead of using IMSI, a temporary mobile subscriber identity (TMSI) is given to each and every subscriber by the PLMN which is used within the network. But the TMSI is stored and accessed in conjunction with the Location Area Identity (LAI). The LAI is also provided by the PLMN along with TMSI to the mobile station in the smart card. The LAI that is generally broadcasts from the local BSS providing local information like area identity. The TMSI will be different for each different VLR area. The system of using TMSI instead of IMSI in the current GSM provides the confidentiality for the user identity.

2.2 Authentication

The main purpose of the authentication process is to prevent unauthorized access of the network by a masquerading attacker and to ensure correct billing.

The authentication process takes place between the VLR and the SIM. The AUC/HLR and the SIM have special "A3" authentication algorithm, "A8" ciphering

Figure 1: Authentication Process (Symmetric technique).

key (K_c) generating algorithm and the unique secret key K_i for A3 and A8are stored in a physically safe place. However, the parameters such as ciphering key K_c, RAND and response (SRES) for authenticating a subscriber can only be supplied by the AUC/HLR in the Home PLMN to the VLR. The SRES is the output of A3 for the input RAND and K_i. The VLR initiates the authentication process by sending the RAND to the MS. Upon receiving the RAND, the MS puts the RAND into the A3 algorithm stored in it and gets the response SRES which it then sends to the VLR. The VLR checks the authenticity of a MS by comparing the SRES with the one it already has. If these two are matching then the VLR obtains assurance that the claimee is a valid subscriber. This process is illustrated in Figure 1.

2.3 Enciphering

The actual enciphering process is carried out between the BSS and the MS. The enciphering algorithm is called A5 algorithm and is stored in both the mobile equipment (ME) i.e., the MS without the SIM, and the BSS in the PLMN. The purpose of the enciphering process is to provide confidentiality of user data.

Once the authenticity is verified, the ciphering K_c is given to the BSS by the VLR and in the mobile station, the K_c can be derived by putting the RAND and the K_i into the A8 algorithm. The same A5 algorithm is used in all ME throughout the GSM service area. The A5 algorithm is like modulo 2 addition of plaintext and the ciphertext. After BSS gets the K_c, it sends the start ciphering message to the mobile station and then starts enciphering/deciphering at its end. It does not expect any reply from the mobile station except in requiring the mobile station to start enciphering/deciphering immediately.

3 Weaknesses in Existing GSM Security

This section lists certain weakness in the existing security system.

- The challenge response entity authentication used in the existing security system to verify the authenticity of the mobile station by the network could be vulnerable to reflection attacks. Such an attack is characterized by the fact that an intruder "reflects" the challenge RAND sent by the PLMN and intended for mobile station to PLMN. He then uses PLMN's response to this challenge to impersonate a mobile station. The reason why such an attack would succeed is because the SRES does not contain enough information about either he originator or the receiver.

- IMSI is used within the fixed infrastructure of GSM PLMN unprotected and often transmitted across VLRs during the location update of a mobile station which moves from one VLR area to the another. The attackers have higher chances of copying subscriber data like IMSI and later on sending a request for the triplet [RAND, SRES, K_c] using the copied IMSI and also trace the location of mobile station by keep track of watching the TMSI assigned to the mobile station.

- During the inter PLMN location update of a mobile station, the triplet is sent unprotected to the foreign PLMN. However the triplet has to be sent, because only the Home PLMN can authenticate its subscriber in the foreign PLMN. Here the triplet contains important subscription authentication parameters like RAND, SRES, K_c. An attacker can copy the encryption key K_c from the unprotected triplet which passes across the border between two countries and decipher the encrypted voice data of that particular subscription.

- The user's voice data is protected only in the radio link between the mobile station and the BSS of the PLMN. No protection of voice data is provided in the fixed infrastructure of the GSM PLMN. This leads to the possibility of eavesdropping of voice data at the fixed infrastructure of the GSM PLMN.

4 Proposed Security System For GSM

This section gives suggestions to solve the above mentioned problems. Before we discuss our solutions to these problems, we propose a new key distribution protocol, a protocol to issue a ticket, a key management in the PLMN, and implementation of encryption algorithm in the mobile network components as well as in

the mobile station. The following subsections describe the assumptions on the encryption algorithm and key management techniques adopted in the proposed security system. Using these assumptions and key management, we propose solutions to the weaknesses in the existing system.

4.1 Special Changes in the Existing Security System

The proposed security system introduces some special changes in the existing security system. The Triple key DES in OFB mode is implemented instead of A3, A5, and A8 algorithms and used in all AUCs, GMSCs, VLRs and all Mobile Stations (MS) of all PLMNs within the GSM PLMN for the purpose of user voice data protection and also for subscriber data protection across the GSM PLMN. The Triple key DES is the "block mixing transformation" construction on DES. The 256-bit-block implementation of Triple key DES provides the strength of three DES keys. The exhaustive search on Triple key DES's 224-bit keyspace is 2**168 times the conventional DES keyspace. The Triple key DES avoids Differential Cryptanalysis by using only balanced full-substitution tables and by using fully block mixing transform to avoid "divide and conquer".

The replacement of A5 with the Triple key DES in the proposed security system provides the greater strength to the voice encryption. Because, according to [7], the A5 is not very good. Its effective key length is at most five bytes and the key stream of A5 is the XOR of three clock controlled registers. The clock control of each register is that register's own middle bit, XOR'ed with a threshold function of the middle bits of all three registers (ie if two or more of the middle bits are 1, then invert each of these bits; otherwise just use them as they are). The register lengths are 19, 22 and 23, and all the feedback polynomials are sparse. There is a trivial 2^{40} attack (guess the contents of registers 1 and 2, work out register 3 from the keystream, and then step on to check whether the guess was right). 2^{40} trial encryptions could take weeks on a workstation, but the low gate count of the algorithm means that a Xilinx chip can easily be programmed to do keysearch, and an A5 cracker might have a few dozen of these running at maybe 2 keys per microsecond each. For more details, the reader is referred to [7].

A secret key Key_A is implemented in the SIM, instead of the authentication key K_i and cipher key sequence number generating algorithm. A special cryptographic algorithm is implemented only in the AUC of a Home PLMN and all MSs belonging to that particular Home PLMN. The special algorithm is unique

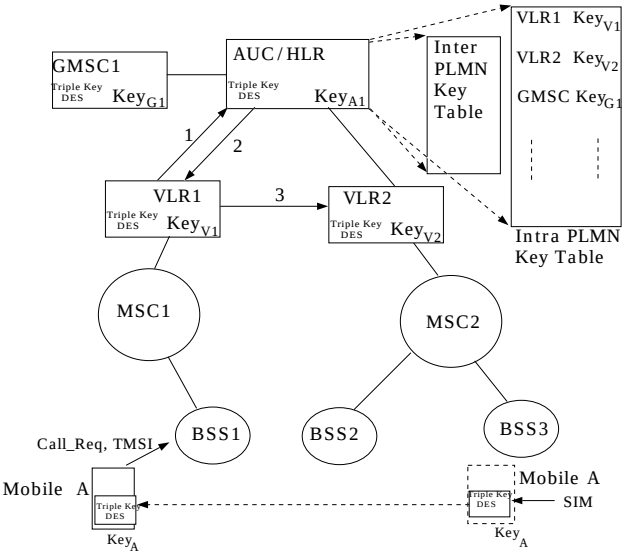

Figure 2: Key Allocations and Secure Location Update Within PLMN.

for each PLMN and its subscribers. The special cryptographic algorithm takes the secret key Key_A from the SIM and derives a new secret session key $SKey_A$, when a mobile station roams into the foreign PLMN. Before a mobile station executes the special cryptographic algorithm it should determine whether it has entered into a foreign PLMN or not. The transmitting Location Area Identity (LAI) through the Broadcast Control Channels (BCCH) of a new cell denotes that the mobile station is in foreign PLMN. It then executes a special cryptographic algorithm to derive a secret session key $SKey_A$. In the foreign PLMN, the mobile station uses only $SKey_A$ as a secret key. When the mobile station returns to the Home PLMN, it uses Key_A as the secret key.

During inter PLMN roaming two extra digits are added to the original TMSI and sent to the foreign PLMN along with the normal LAI as the inter PLMN location update request. Otherwise the IMSI is sent as a request for inter PLMN location update. The proposed security system assumes that the two added digits of TMSI show the significants of the Home PLMN of the newly entered mobile station to the foreign PLMN. In all other cases the ordinary TMSI is sent to identify the mobile station across the PLMN. For example, in all other cases ordinary TMSI is sent as a request for location update, call request, and paging response of a mobile station within a PLMN. The purpose of adding two digits to the normal TMSI is to protect the IMSI from exposure during inter PLMN roaming. The VLR or HLR in the foreign PLMN can identify the Home PLMN of a newly entered mobile station from

the added two digits for obtaining the subscriber's details from its Home PLMN.

The key management and the implementation of the encryption algorithm in the proposed security system are illustrated in Figure 2. The AUC maintains a subscribers private key table with the private keys of all the subscribers in a particular Home PLMN as well as the private session keys of all foreign subscribers currently registered to that particular PLMN.

The mobile network components like HLR, VLRs and the GMSCs have a private key which is only known to the AUC and the components. Based on this, AUC maintains a table called the Intra PLMN key table which contains the private key of all components, mainly HLR, VLRs and GMSCs of a Home PLMN. These Intra PLMN keys are used to establish a secure location update of subscriber data in the fixed infrastructure of a mobile network, when the mobile station moves from one VLR area to the other VLR area of a PLMN. The use of these keys is explained in section 5 and 7. The AUC maintains another table called Inter PLMN key table which contains one to one private keys to communicate with the other AUCs in the GSM PLMN. These one to one private keys in the Inter PLMN key table are used during the session key distribution from Home PLMN to the other PLMN for inter PLMN call set up. These keys are also used during the inter PLMN location update for transferring subscriber data from one PLMN to another. The utilization of these keys is explained in the section 6.

5 Ticket Issuing Protocol

This protocol is employed to secure subscribers data passing between two VLRs, when the mobile station moves from one VLR region to another VLR region. As can be seen in Fig 2, Mobile station A moves from VLR2 region to the VLR1 region and sends a call request to the VLR1 by sending the old TMSI assigned by VLR2. At this point, VLR1 does not have any information about A. From the TMSI sent, the VLR1 knows that communicating with VLR2 would help in updating subscription details of mobile station A at VLR1 from VLR2. It does not know the private key of VLR2. Hence it sends a request to the AUC/HLR to update A's details from VLR2. The protocol is as follows.

1. $VLR1 \rightarrow AUC$: $VLR1, VLR2$
2. $AUC \rightarrow VLR1$: $Key_{V1}[VLR2, TS, SESS\_K_{V1,V2}, Ticket_{Life}, Y]$
3. $VLR1 \rightarrow VLR2$: $Y = Key_{V2}[VLR1, TS, SESS\_K_{V1,V2}, Ticket_{Life}]$

In step 1, VLR1 sends a request to the AUC to issue a session key between VLR1 and VLR2. In step two, AUC sends a session key $SESS\_K_{V1,V2}$ which is valid for the time mentioned in the parameter $Ticket_{Life}$. Y is sent to VLR1 in encrypted form to re-direct it to VLR2, that is why $VLR2$ is included in the encrypted message to VLR1. The timestamp TS is used to prove that the message in step 2 is fresh.

In step 3, VLR1 decrypts the message from AUC and sends Y to the VLR2. Y contains a timestamp and a session key $SESS\_K_{V1,V2}$ which is valid up to time $Ticket_{Life}$. At the end of the protocol VLR1 and VLR2 have the session key $SESS\_K_{V1,V2}$. Using the session key $SESS\_K_{V1,V2}$, important parameters like encryption key K_A and the IMSI of mobile station A can be securely transferred between VLR1 and VLR2. The parameter $VLR1$ in Y tells VLR2 that the key $SESS\_K_{V1,V2}$ is for communicating with VLR1. The Keys Key_{V2} and Key_{V1} are the private keys of VLR2 and VLR1 respectively, which are taken from Intra PLMN key table at the AUC/HLR.

6 Secure Inter PLMN Roaming

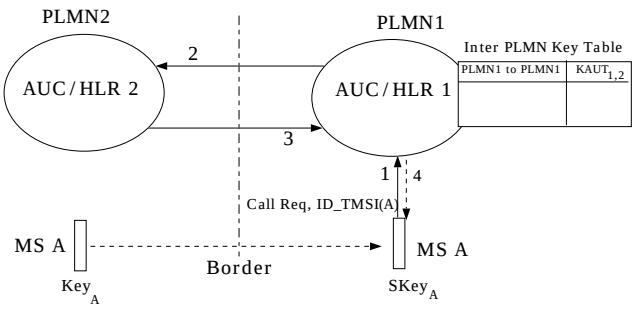

Figure 3: Secure Inter PLMN Location Update

This protocol is employed to secure subscribers data passing between two PLMNs, when the mobile station moves from one PLMN to another PLMN. As can be seen in Fig 3, Mobile station A moves from PLMN2 to PLMN1 and sends a call request to the PLMN1 by sending the parameter ID_TMSI, which is nothing but concatenation of TMSI assigned by the old VLR in PLMN2 and the two digit Home PLMN identifier. Upon getting ID_TMSI from mobile A, PLMN1 identifies which PLMN to contact to obtain the subscription details for A. The subscription details include IMSI of A and secret session key of A to authenticate the newly entered mobile station A. To obtain the subscription details, PLMN1 initiates the

following protocol.

1. $A \rightarrow AUC1$:
   $Call\_Req, ID\_TMSI(A)$
2. $AUC1 \rightarrow AUC2$:
   $KAUT_{1,2}[AUC1, Loc\_Up\_Req, ID\_TMSI(A), TS]$
3. $AUC2 \rightarrow AUC1$:
   $KAUT_{1,2}[AUC2, TS+1, SKey_A, IMSI(A)]$
4. $AUC1 \rightarrow A$:
   $Authentication\_For\_Mobile(A)\_Using\_SKey_A$

In step 2, PLMN1 gets one to one private key of PLMN2 to PLMN1 from its inter PLMN key table, $KAUT_{1,2}$, and encrypts a location update request for mobile station A along with $ID\_TMSI(A)$, TS and sends it to PLMN2. The key $KAUT_{1,2}$ proves the identity of PLMN1 and the timestamp TS is used to prove that themessage is fresh. The $AUC1$ shows the originator of message in step 2. Upon getting the message in step 2 at AUC2, PLMN2 gets the IMSI of A that corresponds to TMSI(A). It also calculates a secret session key for A, which can be derived from a special cryptographic algorithm using the actual secret key of A. Then PLMN2 sends the response to PLMN1, which is illustrated in step 3 of the above protocol.

In step 3, $KAUT_{1,2}$ is a one to one private key of PLMN2 to PLMN1 which is taken from inter PLMN Key table of PLMN2. The $Timestamp+1$ is the proof for correct reply from PLMN2. A's subscribers data $SKey_A$ and $IMSI(A)$ are used to identify and authenticate the newly entered mobile station A in the PLMN1. The $AUC2$ shows the originator of the message in step 3. During this time, the mobile station A derives the secret session $SKey_A$ at its end to prepare for the authentication check. Once the A's subscriber data has safely reached, PLMN1 initiates the authentication and session key distribution for A.

This protocol prevents A's IMSI being exposed in step 1 likewise, in existing security system for GSM and securely transfer A's subscriber data across the border between two PLMNs.

7 Authenticated Session Key Distribution Protocol

The protocols we have seen so far are used to secure the subscriber data (non-voice data) across the fixed infrastructure of a GSM PLMN. However this key distribution protocol is for encrypting a user's voice data at both the air interface and the fixed infrastructure of a GSM PLMN.

The authenticated key distribution protocol for voice encryption is illustrated in Figure 4. In the proposed security system, one protocol establishes a mutual authentication between the network and the mobile station as well as the distribution of session key to the mobile stations for call encryption. In Figure 4 mobile station A initialize a call to mobile station B in the same PLMN. The protocol for authentication, session key distribution and point to point encryption between A and B is as follows.

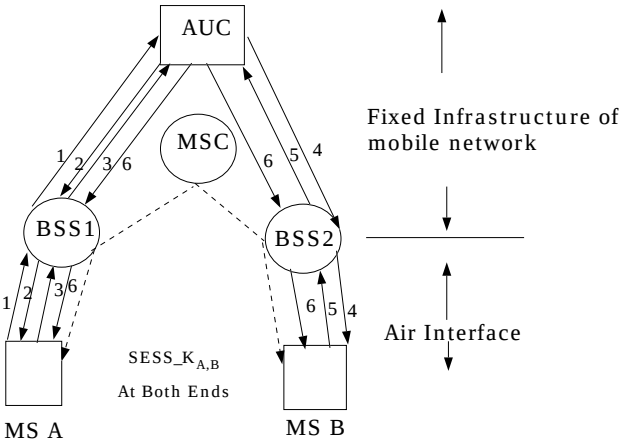

Figure 4: Authenticated Session Key Distribution

.

1. $A \rightarrow AUC$:
   $Call\_Req, TMSI(A), R_A$
2. $AUC \rightarrow A$:
   $Key_A[HPLMN, R_A, SESS\_Key, R_{HPLMN}]$
3. $A \rightarrow AUC$:
   $Key_A[TMSI(A), R_{HPLMN}, ISDN(B)]$
4. $AUC \rightarrow B$:
   $Page\_Req, R1_{HPLM}$
5. $B \rightarrow AUC$:
   $Key_B[Page_Res, TMSI(B), R1_{HPLMN}, R_B]$
6. $AUC \rightarrow B$:
   $Key_B[HPLMN, R_B, SESS\_Key], StartCiphering$
6. $AUC \rightarrow A$:
   $StartCiphering$

Mobile station A initiates a call, which is shown in step 1. In this step TMSI(A) is the identity of A in PLMN and R_A is a random number to authenticate the network. Upon getting this at the AUC, step 2 of the protocol is initiated. In step 2, Key_A and R_A are used to verify the identity of the network and the R_A is also used to prove that the message is a fresh reply from the network. The R_{HPLMN} in step two is used to authenticate the mobile station A by the network. The $HPLMN$ shows the originator of the message. At this point network believes that the request is genuine and then sends a session key $SESS\_Key$ to A. If the

request is from an attacker, then at this point it is impossible for an attacker to decrypt the session key.

Once A gets the message in step 2, it initiates step 3. In step 3 of the protocol, Key_A and the R_{HPLMN} are used to verify the authenticity of the mobile station by the network. The TMSI(A) shows the originator of the message. Only in step 3 the mobile station A sends the ISDN of B (telephone number of B), because this should not be exposed for security reasons. Basically step 3 is the call set-up from mobile A.

Once AUC gets the message in step 3, it sends a page request to the mobile station B for setting up an incoming call for B. This is shown in step 4, $R1_{HPLM}$ is for B authenticating the network. Upon getting this B initiates step 5, which is a page response from B. In step 5, Key_B and the R_{HPLMN} are used to prove the authenticity of B. $TMSI(B)$ shows the originator of the message and the parameter R_B is to verify the authenticity of the network by B. At the end of the step 5, the AUC verifies the authenticity of B, then initiates step 6 for both A and B. Step 6 for B contains the session key $SESS\_Key$ for voice encryption , and R_B and Key_B which are used to verify the identity of the AUC by B and $HPLMN$ which shows the originator of the message. After B decrypts the message in step 6, it takes the $SESS\_Key$ and inputs to the Triple key DES encryption algorithm to start enciphering. A also does the same thing after it gets the start ciphering message from the AUC. This makes sure that the whole call is encrypted both at the air interface and the fixed infrastructure of the GSM PLMN from mobile A to Mobile B.

8 Conclusion

We proposed a single protocol to mutually verify the authenticity of the network and the mobile station as well as to distribute the session key for voice encryption. As a result of this user voice data is protected across GSM PLMN. The proposed security system for GSM completely stopped the exposure of IMSI across the GSM PLMN. The encryption algorithm proposed in the new security system is much stronger than the A5 encryption algorithm used in the existing security system.

References

[1] Dorothy E. Denning, Giovanni Maria Sacco. *Timestamps in Key Distribution Protocols.* Communications of ACM, August, Volume 24, Number 8.

[2] Michael Clayton. *GSM Global System for Mobile Communications.* Security Domain Pty Ltd (ACN Number : 003823461), 1991.

[3] Klaus Vedder *Security Aspects of Mobile Communications.* GAO Gesellschaft fur Automation und Organization mbH, Euckenstr, 12, 8000, Munchen 70, Germany.

[4] C.MITCHELL. *Limitations of Challenge-Response Entity Authentication* , Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, United Kingdom, 19th May 1989. Electronic Letters 17th August 1989, Vol.25 No.17.

[5] Jennifer G.Steiner, Clifford Neuman, Jeffrey I. Schiller. *Kerberos: An Authentication Service for Open Network Systems* , Project Athena, MIT Cambridge, MA 02139, University of Washington, Seattle, WA 98195, [steiner,jis]@ATHENA.MIT.EDU, ben@CS.WASHINGTON.EDU.

[6] Ross Anderson. *Hacking Digital Phones* , Organization: U of Cambridge Computer Lab, UK, Newsgroups: sci.crypt,alt.security,uk.telecom, Date: 17 Jun 1994 13:43:28 GMT, From: rja14@cl.cam.ac.uk (Ross Anderson), Message-ID: ⟨ 2ts9a095r@lyra.csx.cam.ac.uk ⟩, NNTP-Posting-Host: nene.cl .cam.ac.uk.