IMPROVING SPEECH SECURITY AND AUTHENTICATION IN MOBILE COMMUNICATIONS

Chenthurvasan Duraiappan and Yuliang Zheng *
Department of Computer Science
University of Wollongong

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, Scrambling, Digitization, 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 (Clayton, 1991).

2 Speech Encryption

There have been two methods of performing the speech signal processing, enciphering and transmission functions in the mobile communications as well as the fixed telecommunications: the analogue and the digital way. These two methods are explained below.

2.1 Analog Scrambling

In analog scrambling, the original speech signal $x(t)$ is directly scrambled into a different analog wave form $y(t)$ by some scrambling algorithm K_s:

$$y(t) = K_s(x(t))$$

$y(t)$ is the scrambled output of speech, which is to be transmitted through an analog transmission system (Lee, 1985). This is illustrated in Fig 1. Unfortunately, scrambling cannot offer a high degree of security. The protection it offers is just to avoid non professional eavesdroppers from eavesdropping it.

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

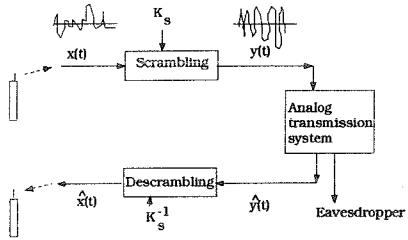

Figure 1: The Analog Scrambling Concept.

2.2 Digital Encryption

The microphone in the mobile transmitter/receiver unit converts speech data into analog signal. The analog signal is sampled, quantized and encoded into digital signals by using pulse code modulation (PCM). The quantization and the encoding combined together are called as analog to digital conversion. The digital signal is enciphered by using an encryption algorithm which is stored in the SIM of a mobile station. The digital speech encryption can offer high degree of security because each digital bit stream resulting from speech signal is cryptographically converted by the encryption algorithm into different form of cipher bit stream. This enciphered digital speech data is converted into transmittable digital data with the help of frequency shift keying (FSK) method, and transmitted into the air interface to reach the local transceiver (local transmitter/receiver).

2.2.1 Transmission of Digital Signal

The generated digital signal from analog speech is organized in a special way before enciphering, modulating and transmitting across the air interface. A special operating system called Time Division Multiple Access (TDMA) is employed for organizing and allocating a timeslot for digital data in a particular radio frequency channel. In TDMA, each Radio frequency channel is divided into timeslot of approximately 577micro sec duration. These timeslots are grouped together in sets of eight consecutive timeslots as one TDMA frame. These frames are then grouped together in one of two ways as multiframes.

1: A 26 frame multiframes comprising of 26 TDMA frames. This multiframe is used to carry traffic channels and their associated control channels.

2: A 51 frame multiframe comprising of 51 TDMA frames. This multiframe is used exclusively for control channels.

Each radio frequency channel is logically divided into eight physical channels in GSM type of TDMA. Out of these eight physical channels, one channel is called traffic channel and rest of the channels are called control channels. The traffic channel is used to carry speech data and its associated control signals. So this 26 frame multiframe undergoes speech coding, channel coding, and interleaving finally made into blocks of 114 bits. This bits can be encrypted, modulated and sent it to the allocated radio frequency by the mobile station. The speech coding, channel coding and interleaving are explained in (Hodges, January 1990).

3 The Existing Security System in GSM

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

3.1 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 key (K_c) generating algorithm and the

unique secret key K_i for A3 and A8 are 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.

3.2 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. The ciphering process is illustrated in Figure 2.

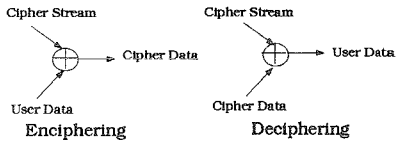

Figure 2: Enciphering Process.

4 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.
- 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.

5 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 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.

5.1 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".

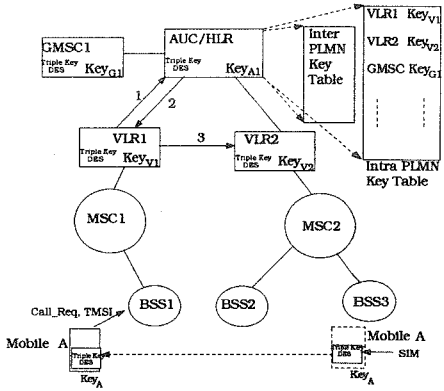

Figure 3: Key Allocations Within PLMN.

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 (Anderson, 17th Jun 1994), 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 (Anderson, 17th Jun 1994).

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 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 3. 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 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.

6 Authenticated Session Key Distribution Protocol

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.

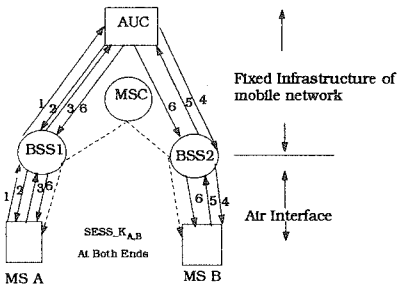

Figure 4: Authenticated Session Key Distribution

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.

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 infra-structure of the GSM PLMN from mobile A to Mobile B.

7 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

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

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

Hodges, M.R.L (January 1990) *The GSM radio interface* , British Telecom Technology Journal Vol 8, NO 1.

Lee, L.S, (July 1985) *A Speech Security System Not Requiring Synchronisation.* pp 42 - 43, 0163-6804/85/0700-0042 01.00, 1985 IEEE, vol.23, No.7, IEEE Communications Magazine.

Mitchel, C. (17th Aug. 1989) *Limitations of Challenge-Response Entity Authentication* , Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, United Kingdom, 19th May 1989. Electronic Letters, Vol.25, No.17.

Vedder, K. (1992) *Security Aspects of Mobile Communications.* GAO Gesellschaft fur Automation und Organization mbH, Euckenstr, 12, 8000, Munchen 70, Germany.