GSM SECURITY AND ENCRYPTION

NIDHI GOEL[1], Dr. DEEPTI MEHROTRA[2]
[1]*Department of CS,* [2]*Department of MCA*
AMITY UNIVERSITY, NOIDA
nidhi_csit24@rediffmail.com, mehdeepti@gmail.com

***Abstract*— the security mechanisms of GSM are implemented in three different system elements; the Subscriber Identity Module (SIM), the GSM handset or MS, and the GSM network. The SIM contains the IMSI, the individual subscriber authentication key (Ki), the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN). The GSM handset contains the ciphering algorithm (A5). The encryption algorithms (A3, A5, and A8) are present in the GSM network as well. The Authentication Center (AUC), part of the Operation and Maintenance Subsystem (OMS) of the GSM network, consists of a database of identification and authentication information for subscribers. This information consists of the IMSI, the TMSI, the Location Area Identity (LAI), and the individual subscriber authentication key (Ki) for each user. In order for the authentication and security mechanisms to function, all three elements (SIM, handset, and GSM network) are required. This distribution of security credentials and encryption algorithms provides an additional measure of security both in ensuring the privacy of cellular telephone conversations and in the prevention of cellular telephone fraud [4].**

*****

I. INTRODUCTION

The motivations for security in cellular telecommunications systems are to secure conversations and signaling data from interception as well as to prevent cellular telephone fraud. With the older analog-based cellular telephone systems such as the Advanced Mobile Phone System (AMPS) and the Total Access Communication System (TACS), it is a relatively simple matter for the radio hobbyist to intercept cellular telephone conversations with a police scanner. A well-publicized case involved a potentially embarrassing cellular telephone conversation with a member of the British royal family being recorded and released to the media. Another security consideration with cellular telecommunications systems involves identification credentials such as the Electronic Serial Number (ESN), which are transmitted "in the clear", in analog systems. With more complicated equipment, it is possible to receive the ESN and use it to commit cellular telephone fraud by "cloning" another cellular phone and placing calls with it. Estimates for cellular
Frauds in the U.S. in 1993 are as high as $500 million [1].

II. DESCRIPTION OF GSM SECURITY FEATURES

Security in GSM consists of the following aspects: subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. The subscriber is uniquely identified by the International Mobile Subscriber Identity (IMSI). This information, along with the individual subscriber authentication key (Ki), constitutes sensitive identification credentials analogous to the Electronic Serial Number (ESN) in analog systems such as AMPS and TACS. The design of the GSM authentication and encryption schemes is such that this sensitive information is never transmitted over the radio channel. Rather, a challenge-response mechanism is used to perform authentication. The actual conversations are encrypted using a temporary, randomly generated ciphering key (Kc). The MS identifies itself by means of the Temporary Mobile Subscriber Identity (TMSI), which is issued by the network and may be changed periodically (i.e. during hand-offs) for additional security [2].

III. AUTHENTICATION

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit random number (RAND) is sent to the MS. The MS computes the 32-bit signed response (SRES) based on the encryption of the random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key
(Ki). Upon receiving the signed response (SRES) from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber [3]. Note that the individual subscriber authentication key (Ki) is never

transmitted over the radio channel. It is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases as previously described. If the received SRES
Agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure indicated to the MS [2].

IV. Signaling and Data Confidentiality

The SIM contains the ciphering key generating algorithm (A8) which is used to produce the 64-bit ciphering key (Kc). The ciphering key is computed by applying the same random number (RAND) used in the authentication process to the ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki). As will be shown in later sections, the
Ciphering key (Kc) is used to encrypt and decrypt the data between the MS and BS. An additional level of security is provided by having the means to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required by network design and security considerations. Figure 6 below shows the calculation of the ciphering key (Kc)[5].

V. Subscriber Identity Confidentiality

To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity
(TMSI) is used. The TMSI is sent to the mobile station after the authentication and encryption procedures have taken place. The mobile station responds by confirming reception of the TMSI. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI [1].

VI. GSM Encryption Algorithms

A partial source code implementation of the GSM A5 algorithm was leaked to the Internet in June, 1994. The details of this implementation, as well as some documented facts about A5, are summarized below:

- A5 is a stream cipher consisting of three clock-controlled LFSRs of degree 19, 22, and 23.
- The clock control is a threshold function of the middle bits of each of the three shift registers.
- The sum of the degrees of the three shift registers is 64. The 64-bit session key is used to initialize the contents of the shift registers.
- The 22-bit TDMA frame number is fed into the shift registers [2].

VII. References

[1] Biala, J., "Mobilfunk und Intelligente Netze," Friedr., Vieweg & Sohn Verlagsgesellschaft,1994.

[2] Cooke, J.C.; Brewster, R.L., "Cyptographic Security Techniques for Digital Mobile Telephones," Proceedings of the IEEE International Conference on Selected Topics in Wireless communications, Vancouver, B.C., Canada, 1992.

[3] Williamson, J., "GSM Bids for Global Recognition in a Crowded Cellular World,"
Telephony, vol. 333, no. 14, April 1992, pp. 36-40

[4] Siegmund H. Redl, Matthias Weber, Malcolm W. Oliphant. “An Introduction to GSM (Mobile Communications Library)”, Artech house publisher.

[5] Jukka Lempiäinen, Matti Manninen. ”Radio Interface System Planning for GSM/GPRS/UMTS” Kluwer Academic Publisher (2001)