AUTHENTICATION AND CIPHERING IN GPRS NETWORK

Ali DİNÇKAN
e-mail: dinckan@uekae.tubitak.gov.tr

Aktül KAVAS
e-mail: kavas@yildiz..edu.tr

Yıldız Technical University, Faculty of Electrical and Electronic Engineering,
Department of Electronics & Communication Engineering
34349 Beşiktaş, Istanbul, Turkey

Key words: GSM, GPRS, Security, Algorithms, Authentication, Ciphering

ABSTRACT

GPRS, General Packet Radio Service is one way of connecting internet or corporate intranet with maximum 172kbps transmission rate by using GSM infrastructure. GPRS provides subscribers the ability of being mobile at any time from anywhere using a mobile communication channel. GPRS subscribers are always on internet as long as they catch a signal from GSM network. Today's companies provide their employees Virtual Private Network (VPN) over GPRS to access their Local Area Network (LAN) directly. Therefore, GPRS technology brings a solution for the requirement of remote working with high speed. Since GPRS is a connection method of Internet, all the threats related with the internet are valid for the GPRS subscribers. GPRS network has some security mechanisms such as authentication and ciphering to protect subscriber's data. In this study, authentication and ciphering security mechanisms used for confidentiality of subscriber data are presented and weaknesses of the algorithms are established.

I. INTRODUCTION

GPRS system has user authentication and ciphering methods to protect unauthorised access and data confidentiality that is similar to GSM system use. GPRS service provider wants to ensure that the subscriber requesting the service is the real GPRS subscriber. The subscriber wants to access to the services without compromising privacy. During GPRS attach, each subscriber is identified using a cryptographic security mechanism. Both of GSM and GPRS systems use the same security algorithms A3, A5 and A8. Only A5 algorithm used in GPRS system is developed from GSM A5 algorithm and called as GPRS-A5[1][2][3].

In GSM system, ciphering is performed between Mobile Station (MS) and Base Station Subsystem (BSS). On the other hand, ciphering in GPRS system is performed between MS and Serving GPRS Support Node (SGSN) and it doesn't deciphered in BSS. Required algorithms and keys for authentication and ciphering are stored in subscriber identity module (SIM) of MS and Authentication Center (AuC) of GSM/GPRS network.

In this study, authentication and ciphering GPRS security mechanisms including security algorithms and required keys are examined. Detailed explanations of GSM/GPRS system components are given. Lastly, GPRS security issue related with security algorithms and keys are discussed.

II. GPRS ARCHITECTURE

GPRS network architecture and interfaces including GSM infrastructure is given in Figure 1.

SGSN and GGSN nodes are added in GSM infrastructure to provide IP based services. SGSN is the first node used for serving MS to connect GPRS network. It is responsible for GPRS Mobility Management (GMM) service and it delivers packets to MS and communicates with Home Location Register (HLR) to obtain GPRS subscriber identity. SGSN manages registration of the new mobile subscribers in order to keep a record of their Location Area (LA) for packet data routing purposes [4].

Second node is the Gateway GPRS Support Node (GGSN) that provides interworking with external Packet Data Networks (PDNs) by using Gi interface such as Internet. It is connected to SGSN via IP-based network by using Gn interface. GGSN acts like a router, forwards incoming packets from Internet to SGSN. It also forwards outgoing packets from SGSN to Internet.

Generally, SGSN and GGSN are computers that have UNIX operating system and related application program developed for this special service. There is a new open working group developing application program for SGSN and GGSN[8]. This application program will work on Linux operation system. The group is working on implementing GGSN and SGSN nodes fully compliant to the 3GPP standards.

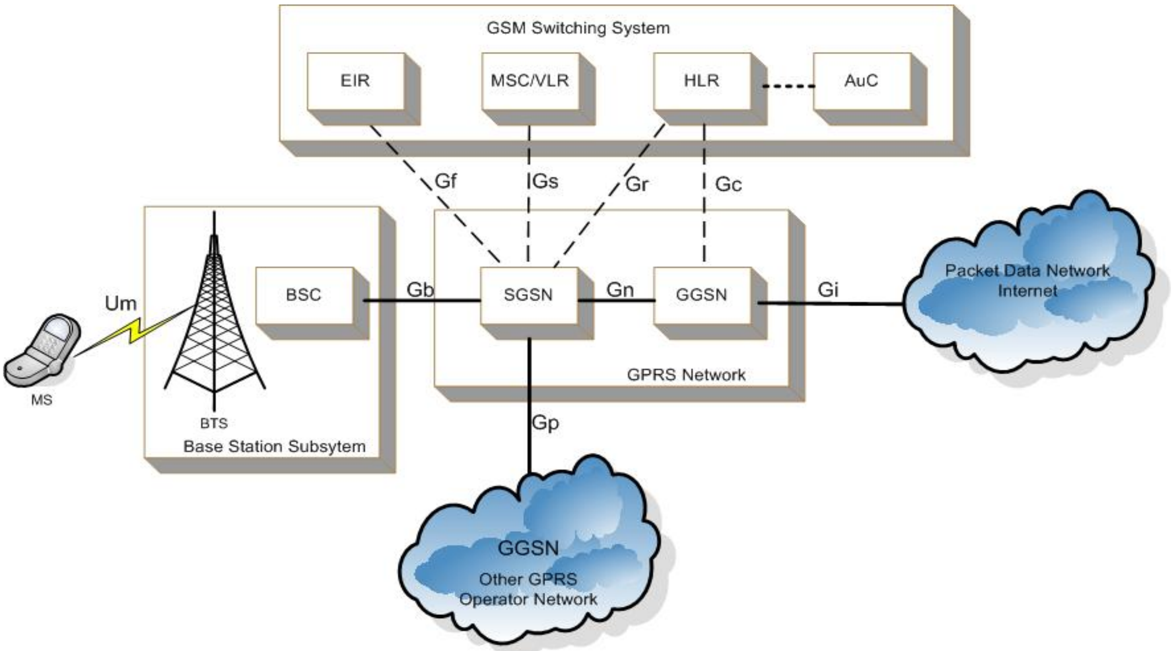

Figure 1 GPRS Architecture and Interfaces

The HLR is a database that contains packet domain subscription data and routing information. It uses Gr interface for SGSN and Gc interface for GGSN communication to exchange of user subscription, service and location data.

Mobile Switching Center/Visitor Location Register (MSC/VLR) coordinates call setups to and from GSM users and manages GSM mobility. Gs signalling interface is used for communication between SGSN and MSC. It forwards circuit-switched paging for the GPRS-attached MSs to SGSN; therefore, MSC is not directly involved in the GPRS network.

The BSS ensures the radio connection between mobile station and network using Um and Gb interfaces. Interface between MS and BTS is called Um and interface between BSC and SGSN is called Gb.

The Base Station Controller (BSC) has switching capabilities used for circuit-switched calls and also carrying GPRS traffic.

The Equipment Identity Register (EIR) is a database that contains MS identities. SGSN uses Gf signalling interface to communicate with EIR for an extra equipment check in GPRS.

III. GPRS SECURITY MODEL

The security mechanisms of GPRS are implemented in SIM card of MS and the authentication centre (AuC) of network. Stored information in these systems, algorithms and keys are given below;

- **Ki:** This is an 128-bit long individual identification key like a password for the subscriber.
- **GPRS-Kc:** This is a 64-bit ciphering key which is generated for every single connection to avoid eavesdropping.
- **A3/A8 Algorithms:** SIM and AuC contain both A3/A8 algorithms to generate the related keys for authentication and ciphering respectively.

Two another identifiers defined as IMSI and P-TMSI are stored in SIM card and SGSN separately:

- **IMSI (**The International Mobile Subscriber Identity number) serves as a fixed subscriber number to identify the subscriber towards the network. IMSI is also stored in HLR and AuC.
- **P-TMSI** (The Packet Temporary Mobile Subscriber Identity) serves as a temporary subscriber number to identify the subscriber in air interface towards the network to protect IMSI number. P-TMSI prevents recognition of GPRS subscriber by a potential dropper. The subscriber uses P-TMSI during location update, GPRS attach or detach GPRS packet transfer. P-TMSI is allocated by SGSN, which may also regularly reallocate a new P-TMSI to MS.

The last algorithm GPRS-A5 implemented in MS and SGSN ciphers the data. The ciphering is a task performed by the Logical Link Control (LLC) protocol which is transported transparently between MS and SGSN. LLC information is not deciphered in the base station. That means ciphered data is carried to the SGSN node of the GPRS network [5].

IV. GPRS AUTHENTICATION

When MS initiates a connection to GPRS network, it has to be authenticated before it is allowed to have access. GPRS authentication is conducted at the start of:

- a routing area update
- a GPRS attach or detach
- a GPRS packet transfer

Authentication refers to the necessity for checking the identity of the MS before it is allowed to make use of network resources. Initially this procedure was intended to protect the subscriber from attackers who would make illegal use of the network by stealing and using their identities [5].

The GPRS operator wants to know who is trying to initiate a connection with the network. The aim of the authentication process is to identify that the user has a correct SIM card with a valid Ki key. This process must be verified without sending Ki over the radio interface.

The authentication process is initiated and controlled by SGSN, supported by AuC and MS. During GPRS attach process, SGSN sends a message containing the IMSI of the subscriber to the AuC and requests triplets, shown in Figure 1. A triplet is composed of three keys called RAND, SRES and Kc, which are explained below:

- **RAND** is randomly generated 128 bit number used for providing triples always different.
- **SRES** (signed response) is 32 bit long number generated by A3 algorithm and used as digital signature of MS.
- **GPRS-Kc** is 64 bit ciphering key generated by A8 algorithm and used for encrypting data between MS and SGSN.

A3 and A8 security algorithms both use Ki and RAND as input parameters. A3 and A8 algorithms are demonstrated in Figure 2.

After getting triplets from AuC, SGSN sends RAND number to MS for authentication. SIM generates SRES based on RAND and Ki by using A3 algorithm. The MS transmits its SRES value to the SGSN that compares it with SRES from AuC. If both values agree, the authentication is successful .Figure2, 3.

Each execution of the algorithm A3 is performed with a new value of the RAND which cannot be predetermined; in this way recording the channel transmission and playing it back cannot be used to fake an identity. A common cause for concern is that all these messages over the radio interface are sent unencrypted because the ciphering starts after the authentication. Security conscious users worry that if someone manages to intercept RAND and SRES as they are transmitted over the radio interface, and if this person knows the algorithm A3, it may be possible to reverse the calculation to derive Ki.[6]

In fact the algorithms used in GSM/GPRS are designed to make extremely difficult to calculate the input Ki (128 bits) from the output SRES (32 bits). Such inverse problems require a lot of processing time on a computer to find the solution [2]. Today's faster computer technology brings a solution that inverse problem. In this study, Ki is obtained from SRES and RAND by using a PII 450MHz, 256MB RAM computer and SimScan V2 [11] program in one hour. By using Ki, it is possible to generate ciphering key GPRS-Kc which influences data confidentiality of the subscriber.

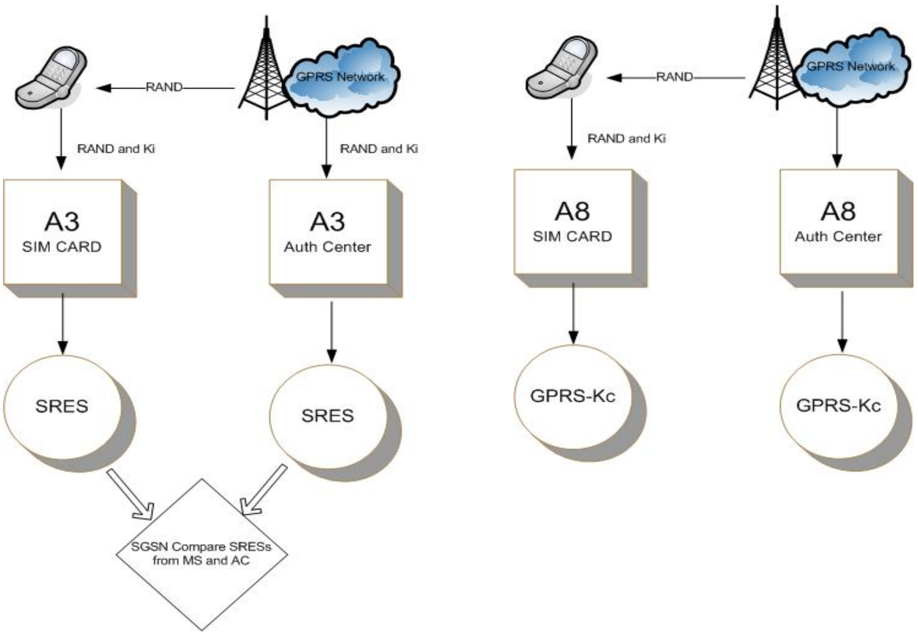

Figure 2 A3 and A8 Algorithm

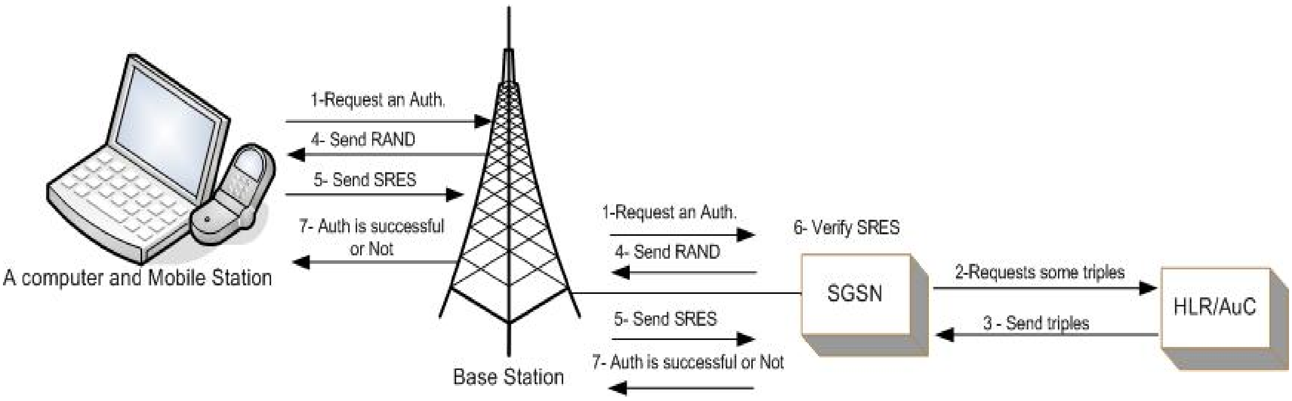

Figure 3 GPRS Authentication and ciphering

V. GPRS CIPHERING

When authentication process successfully completed, SGSN sends a message *"Authentication is successful"*. At the time of receiving that message from MS, it sends a response message to SGSN and starts ciphering shown in Figure 3.

Ciphering process in GPRS needs a ciphering key and a ciphering algorithm. On the fixed network side, SGSN has GPRS-Kc key as ciphering key and GPRS-A5 as ciphering algorithm. The SGSN receives GPRS-Kc key as part of the triplet from AuC, while the MS generates GPRS-Kc in SIM after receiving RAND from network.[5]

Although GSM and GPRS systems use the same ciphering key and similar algorithms, there are some differences between ciphering in GSM and GPRS. In GSM, ciphering is performed between MS and BTS and uses one of three versions of A5 (A5-0, A5-1 or A5-2), depending on the level of ciphering permitted. In GPRS, ciphering is performed between MS and SGSN and use a new version of A5 developed especially for packet transmission (A5-3). That version of A5 is called GPRS-A5.

GPRS ciphering algorithm GPRS-A5 does not use only GPRS-Kc key during ciphering, it also uses two additional parameters defined as *input* and *direction* to protect subscriber data confidentiality. If GPRS Kc was the only one input parameter, the ciphering bit sequence (Ciph-S) would be the same for every GPRS session. One of input parameters named *input* depends on the LLC frame number; the other parameter *direction* depends on data transmission direction. As a result, each LLC frame is ciphered with a different Ciph-S. It has the same length as the LLC frame being ciphered. The length of the LLC frames is variable and may be up to 1523 octets long. It is very clear that the SGSN must regularly send the LLC frame number to MS for staying synchronous.

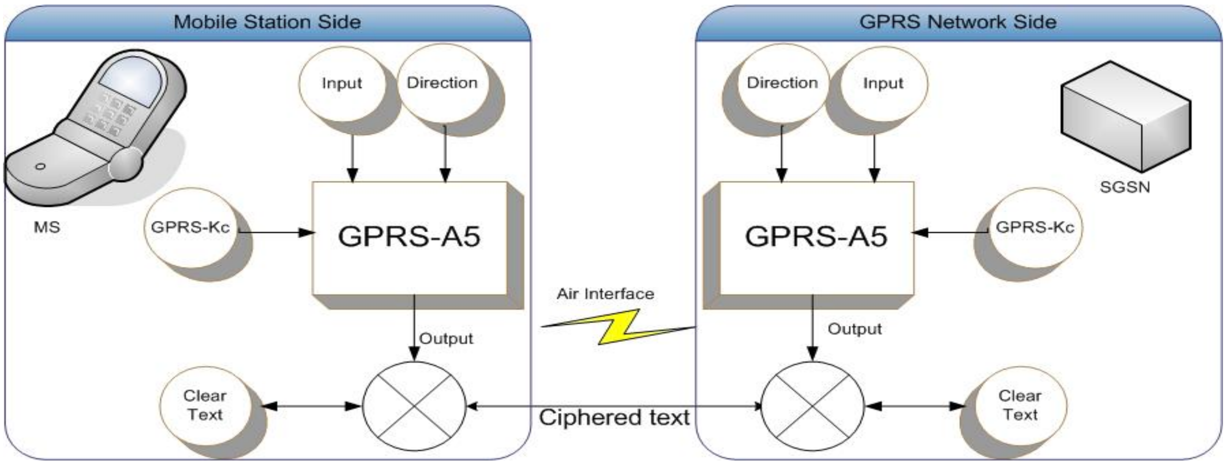

Figure 4 GPRS A5 Algorithm

VI. CONCLUSION

In this study, security over the whole General Packet Radio Service is analysed. In the air interface, security remains in encryption and authentication. SGSN is responsible for the authentication of the subscriber. A signed response (SRES) and a ciphering key (Kc) are derived from security algorithms (A3, A5), individual identification key (Ki) and a Random Number (RAND). These keys are used for authentication and encryption. If the authentication is successful, then the encryption of data and signalling is targeted. Unfortunately, the distribution of the keys is less reliable. The keys are sent through the fixed network in clear text format. On this point of view, GPRS network is quite insecure. The keys should be regularly changed over a session and short key life time should be used in order to get a secure data communication.

The strength of A3 algorithm is tested and individual identification key (Ki) is obtained from SRES and RAND in one hour. it is possible to generate ciphering key GPRS-Kc by using obtained individual identification key (Ki) which influences directly data confidentiality of subscriber. As a solution, GPRS operator or the standardization organisation can develop new algorithm to improve the security. Since the algorithm is stored in the SIM card of MS, GPRS operators can make the changes themselves without involving the hardware or software manufacturers.

REFERENCES

1. ETSI EN 300 920: Digital cellular telecommunications system (Phase 2+); Security aspects (GSM 02.09 V7.1.1 Release 1998)
2. ETSI TS 121 133: Universal Mobile Telecommunication System (UMTS); 3G Security; Security Threads and Requirements (V3.1.0 Release 1999)
3. ETSI TS 133 120: Universal Mobile Telecommunication System (UMTS); 3G Security; Security Principles and Objectives (V3.0.0 Release 1999)
4. Emmanuel Seurre, Patrick Savelli and Jean-Pierre Pietri, GPRS for Mobile Internet, Artech House,2003
5. Geoff Sanders, Lionel Thorens, GPRS Networks, John Wiley & Sons Ltd,2003
6. GSM and GPRS Security, Chengyuan Peng, Helsinki University of Technology
7. C. Bettstetter, GSM 2+ General Packet Radio Service GPRS: Architecture, Protocols, and Air interface. IEEE Communications Surveys, 1999
8. An open source implementation of GGSN, http://www.openggsn.org/index.html
9. *The 3rd Generation Partnership Project , http://www.3gpp.org/*
10. GPRS Security. Charles Brookson. December 2001, *http://www.brookson.com/gsm/gprs.pdf*
11. *SIM SCAN v2.00 (Mar 17 2003),* GSM SmartCard analyzer, written by Dejan Kaljevic*, http://users.net.yu/~dejan*