BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi” din Iaşi
Tomul LX (LXIV), Fasc. 1, 2014
Secția
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

GSM SECURITY-ATTACKS AND PROTECTION METHODS (I)

BY

SEBASTIAN CIORNEI[*] and ION BOGDAN

“Gheorghe Asachi” Technical University of Iași
Faculty of Electronics, Telecommunications and Information Technology

Received: March 3, 2014
Accepted for publication: March 30, 2014

Abstract. Global System for Mobile Communications (GSM) was the first communication system that took call security into consideration from the design phase. One of the key points of the GSM standard is that it is a digital communication system, allowing for using modern security methods. GSM system uses a flexible implementation of the security layer, allowing more algorithms to be used for the same task. This way, new algorithms can be introduced and old ones disabled, making the security upgrade easy and transparent to the user. This work is a two part discussion paper on the security of GSM systems. The main goal of the first part is a critical discussion on the strengths and drawbacks of the most used authentication and encryption algorithms in GSM systems. The second part is a mapping between the theoretically feasible and the practical methods of cracking and protecting GSM systems. Solutions for both the network operators and the end users are also presented.

Key words: authentication; encryption; GSM security.

1. Introduction

On top of the machine to machine systems (Lawton, 2004; Chen & Lien, 2013) that use the telecommunication networks continuously, it is also expected that in 2014, the number of handset to exceed the population of the planet. Provided that more than 80% of the global mobile market still uses the

[*]Corresponding author : *e-mail*: sciornei@ieee.org

GSM standard (Benikovsky, Brida *et al*., 2010), it is expected that more than six billions of devices are currently active and using this standard. This is the second generation of radio telephony, but the most successful of them all until now. One of the key points of the GSM standard is that it uses a digital communication system, making the data communication easily included in the system. Another fact that helped GSM being adopted by many subscribers is the compatibility between the devices along with the roaming services offered by carriers. Being according to only one and clearly defined standard, many hardware producers are able to make compatible equipment. This way, network operators have more options and better prices than those for other systems.

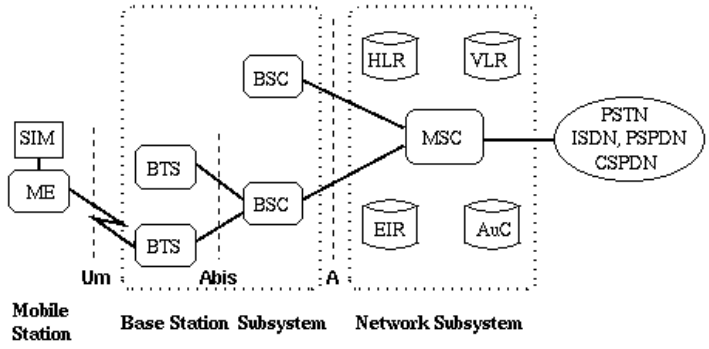
GSM is a cellular network, and while moving, the mobile station roams from cell to cell. Each cell has a different coverage area, different frequency than their neighbors and other specific differences. Still, all the cells owned by a network operator are being interconnected and are being managed in a hierarchical manner. In the same area there could be more GSM network operators. There are up to fourteen different frequency ranges, usually each allocated to a different operator. Most of the networks operate in the 900 MHz or 1800 MHz bands, but in some areas (notably Americas) the bands were already allocated for other networks, and therefore, other two bands are used: 950 MHz and 1900 MHz. Most of the newly developed mobile phones are capable of using most of the bands. Each band is formed by two parts: the uplink frequencies - mobile station (MS) to base station (BS), and downlink frequencies (from BS to the MS). Each band is split in channels. For example the 900 MHz band is split in 124 physical channels for uplink and 124 for downlink. The multiplexing is done in time with a technique named Time Division Multiple Access (TDMA). Each TDMA frame is 4.615 ms and is split in eight Time Slots (TS). A TS on a TDMA frame is called *a physical channel*. The information is grouped into different logical channels. Each of these logical channels is used for a specific purpose (*e.g*. paging, call set-up or speech).

An example of logical channel is the Traffic CHannel (TCH) which carries the speech during a call. The logical channels are split in two categories: traffic and signaling. TCHs are of two types: full rate (TCH/F) with a speed of 22.8 kbit/s, and half rate channel (TCH/H) with a speed of 11.4 kbit/s. Signaling channels are subdivided into three categories: Broadcast CHannels (BCH), Common Control CHannels (CCCH) and Dedicated Control CHannels (DCCH), each with another three subcategories.

For a better understanding some of these logical channels are briefly overviewed below. Paging CHannel is part of the Common Control Channels and is used by the network to contact the mobile when there is a need to exchange information (*e.g*. an incoming call or short message (SMS)). In a paging message, one can find the MS's identity number (IMSI) or its temporary number (TMSI), if one has been set. Note that the PCH is transmitted downlink only. When the connection is the other way (uplink), the MS uses the Random Access CHannel (RACH) to contact the network. When the network assigns a

channel to an MS, it uses the Access Grant CHannel (AGCH). Under the group of Dedicate Control Channels (DCCH) there are two types of logical channels. Stand-alone Dedicated Control CHannel (SDCCH) is being used for the call setup (decisions on the TCH to be used, etc) or SMS transmission. Note that this channel is between the BS and only one MS. The channel is being freed after the SMS has been transmitted or after the TCH has been decided and MS told to switch to it. The Slow Associated Control CHannel (SACCH) is part of the same physical channel with an SDCCH or TCH. On this channel the MS and BS exchange information related to the signal strength, transmitting power (Rahnema, 1993).

Fig. 1 graphically explains how the calls are made from and towards an MS and it also depicts the main devices that form the GSM networks. It is important to note that the subscriber identity module (SIM) is not part of the Mobile Equipment (ME), but it only works along with it and forms the Mobile Station (MS). This way the subscriber can easily select the ME of choice, upgrade or change it any time. This fact also had a major impact on the ME market, allowing companies to produce these devices without a previous contract with specific network operators.



SIM Subscriber Identity Module BSC Base Station Controller MSC Mobile services Switching Center
ME Mobile Equipment HLR Home Location Register EIR Equipment Identity Register
BTS Base Transceiver Station VLR Visitor Location Register AuC Authentication Center

Fig. 1 – GSM System Architecture (Isomäki, 1999).

1.1. Call from MS

1. MS uses RACH (Random Access CHannel) to ask for a signaling channel, SDCCH (Stand alone Dedicated Control channel).

2. Base Station Controller (BSC) allocates a signaling channel, using AGCH (Access Grant CHannel).

3. MS sends a call set up request *via* SDCCH to the Mobile services Switching Center (MSC) or Visitor Location Register (VLR). Over SDCCH all signaling preceding a call takes place. This includes marking the MS ”busy” in

MSC/VLR, authentication procedure, start ciphering equipment identification, sending the number to the called subscriber.

4. MSC/VLR asks the BSC to allocate a free TCH (Traffic CHannel) and both BTS and MS activate the TCH.

5. When the destination subscriber answers, the connection is established.

1.2. Call to MS

When one initiates a call to a mobile subscriber the location of the mobile subscriber is not known. Therefore, we must locate and page the MS before we can set up a connection (Fig. 2). A step by step procedure is described below:

1. A subscriber dials the destination Mobile Subscriber Integrated Services Digital Network Number (MSISDN). The MSISDN is analysed and if it is not from the same network, it connects to the Gateway MSC (GMSC).

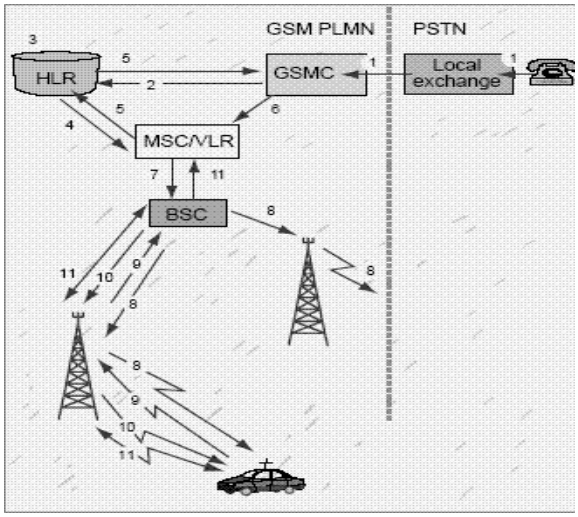


Fig. 2 – Call routing (Hibberd, 2008).

2. GMSC analyses MSISDN to find out in which Home Location Register (HLR) the MS is registered and then interrogates it for information about how to route the call to the serving MSC/VLR.

3. HLR translates MSISDN into IMSI, and finds out which MSC/VLR is currently serving the MS.

4. HLR requests a roaming number, Mobile Station Roaming Number (MSRN), from the serving MSC/VLR. MSRN identifies the MSC/VLR.

5. MSC/VLR returns the MSRN *via* HLR to the GMSC.

6. GMSC reroutes the call to the MSC/VLR, directly or *via* the PSTN.

7. The MSC/VLR knows in which Location Area (LA) the MS is. A Paging message is sent to the BSCs controlling the LA.

8. The BSCs distribute the Paging message to the BTSs in the wanted LA. The BTSs transmit the message over the air interface using PCH (Paging channel). To page the MS, IMSI (International Mobile Subscriber Identity) or TMSI (Temporary Mobile Subscriber Identity, valid only in the current MSC/VLR service area) is used.

9. When the MS detects the paging message it sends a request for a signaling channel, SDCCH.

10. BSC provides an SDCCH, using AGCH (Access Grant channel)

11. SDCCH is used for the call set up procedures, as in the case for ”Call from MS”, and then a TCH is allocated. SDCCH is released.

2. GSM Security

The GSM network is the first widely deployed telephony standard that took the security of the call into account. At that point, it was supposed that it worth to encrypt only the air interface since this one is the most vulnerable part of the system (Scripcariu *et al*., 2008). In this section GSM equipment is be presented, together with authentication and encryption methods and a detailed description of the encryption algorithms in use.

2.1. Authentication and Key Derivation Algorithms A3 and A8

The authentication process starts (or should start) whenever the MS makes a call, sends an SMS or updates his/her location. The subscriber's home AuC receives his TMSI (or IMSI), and computes a set of three values which are sent back to the VLR. This triplet is formed by: a 128 bit random number (challenge) generated by AuC itself (RAND), a 64 bit authentication number named *signed response* (SRES) and a 64 bit cipher key named Kc.

The AuC searches for user's secret 256 bit key (Ki) in its DB (according to TMSI/IMSI), and, along with the RAND value and A3/A8 algorithms, it derives the SRES and Kc as presented in Fig. 3.

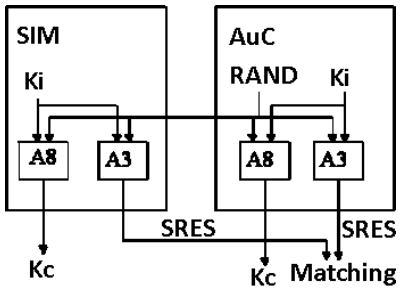


Fig. 3 – A3/A8 HOWTO (Isomäki, 1999).

Once all three values reach user's current network, the VLR sends the RAND value to the MS. User's SIM contains the same information as AuC does: Ki, A3&A8. Having the RAND, it also computes an SRES value and

sends it across network to the VLR. Here the matching is done: if the two SRES values are identical, the subscriber is authorized to use the network and his current BTS receives the Kc which will be used to encrypt the downlink data and decrypt the uplink one.

Both A3 and A8 algorithms are operator specific, but sometimes the example presented in the standard is implemented (COMP128-1) and this one computes both SRES and Kc in the same time. Algorithm's output is a string of 96 bits, out of which the first 32 are used for authentication (SRES) and the remaining 64 for encryption/decryption (Kc).

It should be noted that the Key (Kc) and Signed Response (SRES) don't depend on the encryption algorithm to be used with.

2.2 Encryption Algorithms A5/0 1 2 3

The general requirements for all the algorithms in the A5 group (besides A5/0), are to have as inputs a 64 bit cipher key and a time variable (COUNT). COUNT is a 22 bit value split in 3 groups T1, T2, T3. All three are computed from the TDMA frame number (denoted by F) as indicated in Fig. 4.

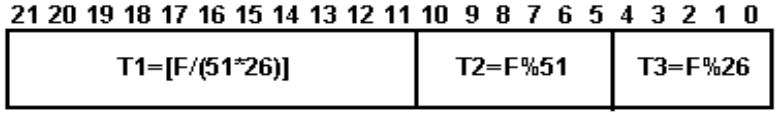


Fig. 4 – COUNT register.

The output is to 228 bits long, split in two 114 bit groups (Block 1 and Block 2, one for downlink and the second one for the uplink) and are used to crypt and decrypt the data transmitted in each time slot (ETSI 1996).

a) **A5/1**

A5/1 is the first adopted and the most used encryption algorithm. Statistically, now it is used by more than two billions GSM customers to protect their voice and data connections. As presented above, the algorithm has as inputs the 64 bit cipher Key (Kc) and the frame number in the format presented in Fig. 5.

During the initialization phase, the following steps are done: all 3 registers, *R*1, *R*2, *R*3, are reset. Afterwards, the Kc is inserted in the registers, bit by bit. In the next step the frame number is introduced as a "salt" and keyed in the stream. In the last step of the algorithm, the combination of the three linear feedback shift registers (LFSR) is run for 100 times and output ignored (dropped).

It is to be noted that only one function introduces non-linearities in this algorithm (it is a quadratic function called *majority* (*a*,*b*,*c*) = *a***b* + *a***c* + *b**c.

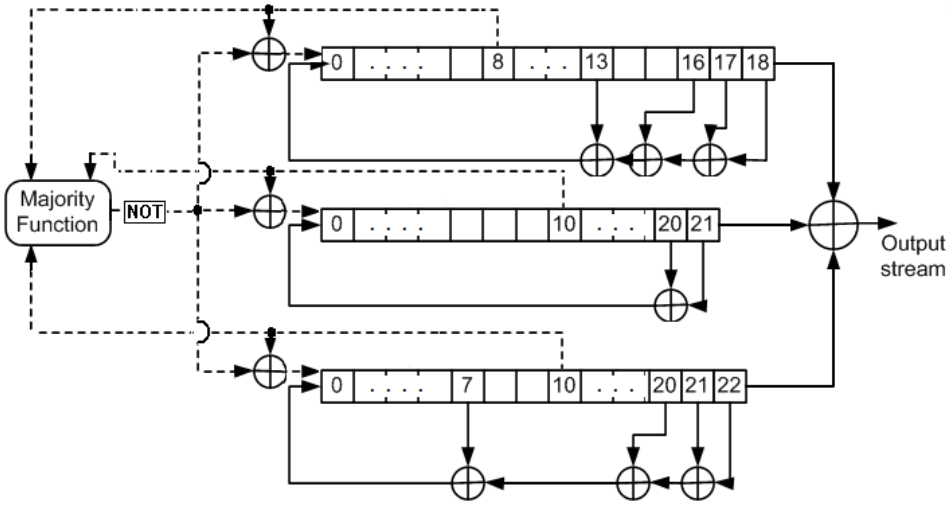


Fig. 5 – A5/1 internal structure.

b) **A5/0**

Security researcher Ross Anderson reported that "there was a terrific row between the NATO signals agencies in the mid 1980s over whether GSM encryption should be strong or not." (Anderson & Roe, 1994). As a final result, two years later after the A5/1, two more methods added to the A5 group. One of them is the A5/0 which basically means that there is no encryption at all.

c) **A5/2**

After debates, it was decided that a second algorithm should be created for certain export regions. This was named A5/2. The instructions for the algorithm were to be distinct from the existing A5/1, to reuse the components of A5/1 and to have a minimal increase in the number of transistors when used along with the already implemented A5/1 (ETSI 1996).

The cipher is based on four linear feedback shift registers with irregular clocking and a non-linear combiner. This way, the algorithm is quite similar with the A5/1: in the beginning all 4 registers, *R*1, *R*2, *R*3, *R*4 are reset. Afterwards the Kc (64 bits) is inserted in the registers, bit by bit, as presented in the code below. In the next step the frame number (22 bits) is introduced as a "salt" and keyed in the stream. Afterwards, four of the bits (*R*1[15], *R*2[16], *R*3[18], *R*4[10]) are set to 1. In the last step of the algorithm, the combination of four linear feedback shift registers (LFSR) is run for 99 times (not 100 times as

in A5/1) and output ignored. From this step onwards (228 cycles) the output is used for encryption/decryption.

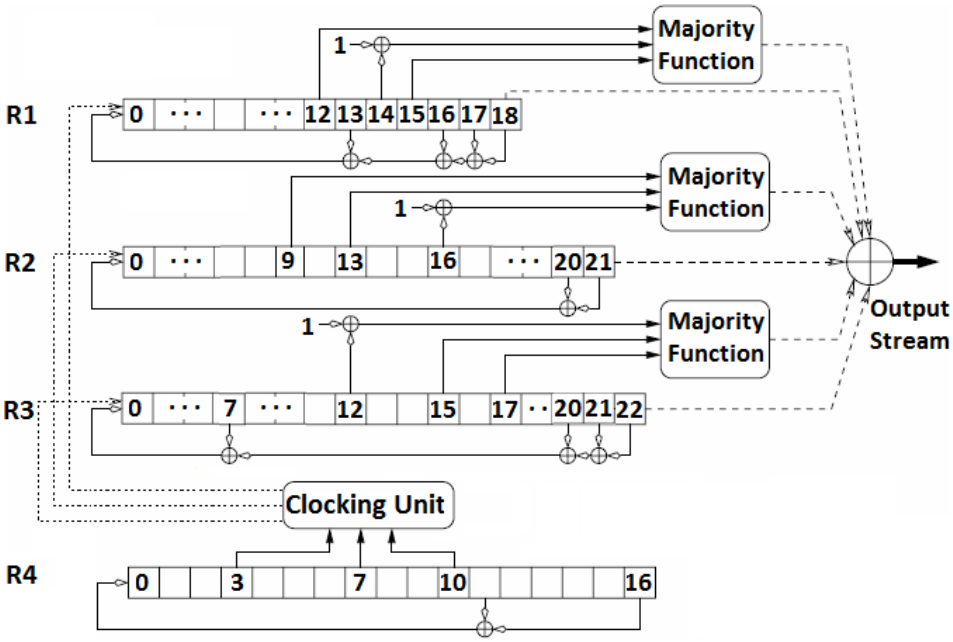


Fig. 6 – A5/2 internal structure (Barkan *et al*., 2003).

Along with A5/1, the algorithms are being kept secret. However, the general design was leaked in 1994, and the algorithms were reverse engineered by Marc Briceno from a GSM telephone in 1999 (Briceno, Goldberg *et al*., 1999).

d) **A5/3**

This is a new algorithm based on the UMTS/WCDMA algorithm Kasumi. In its turn, Kasumi was designed by the ETSI based on an existing algorithm, MISTY1, which has been optimized for implementation in hardware. Katsumi uses a Feistel scheme which makes the encryption and decryption phase very similar (if not identical) and allows the designers to use the same circuits for both activities.

GPRS encryption uses a different set of algorithms: GEA0 (none), GEA1 (export), GEA2 (normal strength) and GEA3 (the same as A5/3). Out of these, only A5/3 is publicly known (ETSI/SAGE 2002). Practical A5/3 attacks have been discovered and according to Dunkelman, Keller *et al*., (2010), it can be implemented with the computing power of a PC.

2.3 IMSI/TMSI

At the beginning of a data connection (when a call is being made, SMS sent or location updated), the subscriber sends its IMSI or Temporal Mobile Subscriber Identity (TMSI) to the network. This identifies him in HLR/AuC. While IMSI is permanent, TMSI can and should be changed at the end of every transaction (while the connection is still encrypted). This way, the new TMSI is renegotiated in a secure way and it is known only by the network and the subscriber.

3. Conclusions

The GSM network is the first widely deployed telephony standard that took the security of the call into account. Being a digital communication system, the newer digital security methods are used. New generation systems (GPRS, UMTS) bring newer and more secure encryption algorithms (A5/3) with even higher level of protection against eaves dropping. The layered security system allows flexible and hassle free upgrades of the network. Our future work will be to search for practical methods of breaking these algorithms and testing the communications systems' security. In the GSM network, user's identity is protected by means of temporary identification.

Even though A5/3 improves on security, GSM still remains a strong part of the world's phone network for years to come to provide a smooth transition to both 3G and 4G, especially for the voice channels.

REFERENCES

Barkan E. *et al*., *Instant ciphertext-only cryptanalysis of GSM encrypted communication*. Advances in Cryptology-CRYPTO 2003, Springer**:** 600-616.

Benikovsky J. *et al*., *Localization in Real GSM Network with Fingerprinting Utilization*. Mobile Lightweight Wireless Systems, Springer**:** 699-709, 2010.

Briceno M. *et al*., *A Pedagogical Implementation of the GSM A5/1 and A5/2 "Voice Privacy" Encryption Algorithms*. Originally published at http://www. scard. org, mirror at http://cryptome. org/gsm-a512. Htm, 1999.

Chen K.-C., Lien S.-Y., *Machine-to-Machine Communications: Technologies and Challenges*. Ad Hoc Networks, 2013.

Dunkelman O. *et al*., *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony*. IACR Cryptology ePrint Archive, 13, 2010.

Isomäki M., (1999), *Security in the Traditional Telecommunications Networks and in the Internet*.

Lawton G., *Machine-to-Machine Technology Gears up for Growth*. Computer, **37**, *9*, 12-15 (2004).

Rahnema M., *Overview of the GSM System and Protocol Architecture*. Commun. Mag., IEEE **31**, *4*, 92-100 (1993).

Scripcariu L. *et al*., *Securitatea reţelelor de comunicaţii*. Edit. Venus, Iaşi, 2008.

* * * *Security Algorithms Group of Experts (SAGE); Report on the Specification and Evaluation of the GSM Cipher Algorithm A5/2*. Europ. Telecomm. Standards Inst. (ETSI), 1996.

* * * *Specification of the A5/3 Encryption. Algorithms for GSM and EDGE, and GEA3 Encryption. Algorithm for GPRS*. ETSI/SAGE, Document 1: A5/3 and GEA3 Specifications, 2002.

SECURITATEA ÎN REȚELELE GSM – ATACURI ŞI METODE DE PROTECȚIE (I)

(Rezumat)

Global System for Mobile Communications (GSM) este primul sistem care a luat în calcul, încă din faza de proiect, securitatea transmisiei. Acest sistem fiind unul digital, a avut un avantaj major deoarece s-au putut folosi metode moderne de securizare. Sistemul GSM este stucturat pe nivele, dand posibilitatea modificării algoritmilor de securitate fără a întrerupe serviciile către utilizatori. Astfel, noi algoritmi pot fi introduşi, respectiv algoritmii vechi pot fi scoşi din funcție. Lucrarea se doreşte a fi o introspectivă critică a securității în rețelele GSM fiind împărțită în două părți. Scopul principal al primei părți este de a prezenta avantajele şi dezavantajele unora din cei mai utilizați algoritmi de autentificare şi de criptare. Partea a doua pune accentul pe metode atât teoretice cât şi practice de spargere a acestor algoritmi, precum şi soluții viabile atât pentru operatorii de telefonie mobilă cât şi pentru utilizatori.