BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi” din Iaşi
Tomul LX (LXIV), Fasc. 2, 2014
Secția
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ

GSM SECURITY-ATTACKS AND PROTECTION METHODS (II)

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: May 14, 2014

Abstract. This paper presents a mapping between the theoretically feasible and practical methods of cracking and protecting GSM (Global System for Mobile) communications. In order to prove the practical methods, various implementations are explained. Two topics are detailed: core/distribution layers security and over the air security. The wireless part security is devided among types of algorithms and feasible attacks. A set of solutions for network operators and end users are presented: some of them easily applied with few resources, but with a big impact on the security level, while others being more expensive and harder to implement, but removing the root cause of current and future attacks.

Key words: A5/x algorithms; GSM security; protection; rainbow tables.

1. Introduction

Wireless connectivity is very convenient, but can be a very unsafe solution for communication. Possible attacks target all possible areas, from standards to implementations and from networks to mobile equipment. The GSM standard does not specify security guidelines for all sections of the network, leaving it to the network operations’ choice. For example, one of the main issues related to the core of GSM system is that only the air interface is secured, while the traffic through current and interconnected operators' networks is unencrypted.

*Corresponding author : *e-mail*: bogdani@etti.tuiasi.ro

Where the standard does provide guidelines, either they allow for unsecure methods, or the suggested algorithms are cryptographically weak. After the A5/1, A5/2 have been reverse engineered, a set of “known plain text” attacks appeared. As COMP128 (A3/A8) has been reverse engineered as well, SIM cloning attacks were created. As of 2008, Elad Barkan demonstrated passive known plain-text or cipher text only attacks against A5/2. By means of active attacks A5/2, A5/1 (Barkan *et al*., 2008) and even A5/3, A5/3, A5/4 can be cracked (Dunkelman *et al*., 2010).

These points of attacks are targeted by both commercial and open source systems and such techniques are now easily available and at low prices. A series of guidelines are presented for the security conscious subscribers (Scripcariu *et al*., 2008).

This paper is structured as follows: section **2** presents security issues related to core network, over the air security, and SIM related attacks and emphasizes that tools are already available to anyone, including low budget groups. Section **3** presents the solutions which can be used by all three parties: network operators, device and SIM cards manufacturers, and subscribers. The paper concludes with the **4**th section where the information is wrapped up.

2. Forms of Attacks

2.1. Attacks at Core Network Level

Because landlines are expensive, the distribution layer is also wireless (Pagliusi, 2002). As the GSM standard does not impose any measure on this part, some of these radio links that carry the calls from a whole cell might not use a secured (or secure enough) connection. An attacker can align with the beam and eavesdrops into many calls simultaneously. The only required equipment is a directional antenna, a wideband receiver and a channel demultiplexing device.

Other types of core level attacks are related to the GPRS Tunneling Protocol (GTP). Out of the protocol anomalies group of attacks the easiest to conduct is packet spoofing. In this attack a malicious Mobile Station (MS) creates "forged" GTP packets which are forwarded by the network to the SGSN. Here the data is packed in GTP (once again) and forwarded to GGSN. The outer layer is being removed and packets forwarded into the GPRS infrastructure. If the system is not well protected (Jokinen & Uskela, 2008), it could unpack the data once more and the forged packets could reach the "inside" network, skipping all the firewalls up to that point (Whitehouse, 2004).

2.2. Attacks on Authentication Algorithms (A3/A8)

Initially it was determined that Ki from a SIM can be found through traditional cryptanalysis from the outputs generated on 150,000 chosen plaintext values, but further improvements have shown that this is possible with an

average of only 18,000 values (Quirke, 2004). Given the fact that a SIM card reader can make up to 6 queries per second, this attack lasts about 7 hours. One may note that this attack does not require physical access to the card and it can be conducted remotely by using a fake BS.

GSM is the living proof that security by obscurity is not a good solution. There are many examples, but the one that mostly threatens the privacy is in A3/A8 algorithms. Even though the COMP128 was never made public, the algorithm was reverse engineered and crypt analysed in 1998. Eventually, one document presenting the original algorithm leaked and now can be found on the internet in a few locations (RACAL 1998; Briceno *et al*., 1998).

Authentication is done (mainly) one way only: the MS authenticates to the network (Quirke, 2004). One may say that the network authenticates to the MS by being able to encrypt the data to be sent (with Kc which was derived from the Ki), but still, one can conduct Man In the Middle (MIM) attacks, so this method cannot be considered a viable authentication. This type of attack, along with the fact that GPRS uses the same key agreement and the same type of RAND/SRES/Kc values, endangers the security of the GPRS also. Here is an example of a MIM attack on GPRS: the attacker starts a GPRS session with the real network. After the GPRS-RAND is received, the attacker, using a fake BS, initiates a non-GPRS session with the victim (forcing him to use the A5/2 algorithm) and passes to the victim the received GPRS-RAND in the form of the initial RAND. Victim computes the SRES and sends it to the fake BS. Out of this traffic, the Kc can be retrieved. The attacker sends the SRES to the real network, gets authenticated and, by the use of Kc, it successfully impersonates the victim and make calls.

2.3. Attacks on Encryption Algorithms (A5/x)

The simplest attacks are the MIM attacks using the non-encrypted mode (A5/0). An attacker with a fake BS can "lure" a victim to use this A5 variant, eavesdropping in the victims' connection even though the network allows only secure connection (A5/3, A5/1, and A5/2).

a) *A5/2 known plain text attacks*

The attack (Briceno *et al*., 1999; Goldberg *et al*., 1999) needs only two known plain-text data frames which are separated by $26 \times 51 = 1{,}326$ frames. This means that 6 (or 12 s) have to be spent before the data can be recovered. Nothing from the conversation is lost, as the first 6/12 s are recorded and deciphered after the Kc is recovered.

A faster attack (Petrovic & Fuster-Sabater, 2000) is created with a system of quadratic eqs. out of the four known plain-text frames. Based on the solution of the quadratic eqs. one can decrypt the remaining part of the conversation. It should be noted that Kc is not recovered, so the first part of the conversation could be lost (Barkan *et al*., 2008).

The plain text data comes from the first 4 packets that are sent at the

beginning at each call (in case the International Mobile Equipment Identity and Software Version (IMEISV) is not requested by the network). This gives us 456 bits for each call. In case the network asks for the IMEISV also, a MIM attack can be done in advance and IMEISV found. Note, this is an one-time task, as this value changes on firmware upgrades only.

b) *A5/2 cipher-text only attacks*

One major flaw that makes the cipher text only attack viable is the fact that the error correction is done before the encryption and this introduces known linear relations between the bits to be encrypted (Quirke, 2004).

c) *A5/1*

Initially presented by Golić, (1997), the A5/1 known plain text attack has become practical (Biryukov *et al*., 2001).

For cipher-text only attacks there are more methods, presented in the increased order of computation needed, but it should be noted that the two main factors that make the A5/1 and even A5/3 and above easy to break: the backwards compatibility of the mobile stations with the weaker encryption algorithms and the fact that all encryption algorithms use the same key. This way, if one can break the A5/2 or use a fake BS, the recovered key can be reused also for A5/1 or even A5/3 and newer.

The latter is done by creating a fake base station (BS). It is not a necessity to have a real base station, but another mobile station with the appropriate software. To make a phone to connect to the fake BS instead of the real one, the power signal from the fake BS has to be greater than the real BS. Having the victim connected to the fake BS, when a new call is initiated, the fake BS will "force" the client to fall back to A5/2 (or even A5/0). In the same time the fake BS acts as a normal client to the real BS and initiates a call. For the next few milliseconds the fake BS acts as a tunnel, passing the values from one connection to another. In other words, the network sends the RAND value and the value is being forwarded to the victim. The victim answers and starts to send data. Having the first few packets sent by the victim with the A5/2 (a few milliseconds are enough), one can use the previous attack to find the encryption key (Kc). After this, the attacker uses the SRES to confirm the authentication to the network, uses it for the A5/1 along with the key derived from the other connection (Kc) and forward the call to the network.

Another active attacking technique is to record the call, and later, by pretending to be a BS that has a call, initiate a call with A5/2, send the RAND which has been sent by the network in the previous call, find the Kc and decrypt the previous call. Overall this would be a much easier solution compared to the direct A5/1 cracking, but it requires fake BS and co-localization with the victim. As the keys are reused from one call to another, if there is not enough data for the A5/1 attack, more data can be created by simply initiating another call to the victim (through the real BS).

Another cipher-text only method has been suggested by David Hulton

and Steve Miller who proposed to see the whole A5/1 system as an one way function on which the rainbow tables solution was tried (Nohl, 2010; Kalenderi *et al*., 2012). Further improvements and balancing between time/memory have been done by Oechslin, (2003), Avoine *et al*., (2008). An explanation and comparison on rainbow tables methods can be found in the paper published by Stoffelen *et al*., (2013). The algorithm was implemented in a multi-threading manner, so adding more GPUs/FPGAs increases the speed accordingly. In the proposed method, the pre-computation phase would need a 5Tb storage with a set of 100 FPGAs and could be done in about two months. In the real-time phase (attack phase) the key can be cracked in a range from few seconds to few 5 min. depending on the number of FPGAs used. To make it a practical method, the group added also the information which can be found easily by means of known first four frames which are being exchanged at the beginning of each connection.

It is supposed that one has the plain-text, so if the values in two of the registers are known, the third can be computed. Once R3 is found, the system has to be reverted back to its first state to find the Kc. It is worth noting that even though the Kc is 64 bits, the last 10 bits are set to zero before the key is being used as well, as not all operators change Kc for each call.

d) *A5/3&4*

These are stronger algorithms, based on the KASUMI 64-bit block cipher, (Biham *et al*., 2005), but practical solutions targeting directly the algorithms are already available (Dunkelman *et al*., 2010). Even easier are the "walk around" A5/3 by using active attacks with fake BS.

e) *IMSI/TMSI*

According to the GSM standards, the change of TMSI is optional, and its use depends on the operator's decision, so once the target is identified, it can be easily traced (Isomäki 1999). For the first identification one can simply listen to the cell under which the victim is, and, in the same time, call or send a SMS: TMSI will show up in the traffic. This can be done transparent to the victim by sending a bad formatted SMS, which the phone will ignore.

2.4. SIM Attacks

SIM cloning can be done either *via* cryptanalysis (2.1) or side channels attacks (electromagnetic emissions, time taken for processing or power consumption). With these methods Ki can be derived in 1,000 queries with random known plaintext queries or 255 queries with chosen known plaintext values or with 8 known plaintext values selected at runtime, according to the results received till that point (Rao *et al*., 2002). This last attack is based on the fact that A3/A8 requires queries in five tables of different sizes (512, 256, 128, 64, 32 bytes).

The new SIM cards have some more restrictions like limited number of

key generation requests. This way a brute force attack on finding the Ki will render the SIM unusable. An alternative solution is the use of powerful microscopes, acid and lasers to take the silicon layer by layer and read the information directly from the SIM (Helfmeier *et al*., 2013), from a stolen/older SIM card.

One more issue is that the session key (Kc) is reused for more calls (until the MSC decides to authenticate the MS again). It should be noted also that the authentication session cannot be initiated by the MS.

Yet another technique that should be studied in more depth is related to the new SIM cards in the market. They contain a full API ready to execute a code received from the network. An attacker that has access to the network would be able to upload and execute various codes on the phone, including recording/forwarding voice calls.

2.5. Another Security Issue are the Tools Already Available

Nowadays there are plenty of commercially available devices that can monitor, hijack or alter the call with prices so low that even individuals can afford to conduct GSM attacks: SingInt group, Comstrac, Shoghi Communications Ltd, and Stratign.

The open international communities proved to be some of the best sources for research. Projects like OpenBTS, GNURadio, USRP, OpenMoko as well as commercially available mini networks backpacks Vodafone Instant Network Mini picocells provide an excellent start for independent researchers and hackers alike (Lackey & Hulton, 2007). With budgets of 1,000 $ (2TB HDD and 1+ LX50 FPGAs) one can crack A5/1 in about 30…60 min. ASICs can increase the speed by a factor of 200 or more (Keller & Seitz, 2001; Gendrullis *et al*., 2008). The current studies are focused on "GSM analyser" which can track MS, listen for associations and find the approximate distance of the MS from the BS which uses USRP acting as a receiver for the GSM network. If it will go to the next stage where it will be able to also transmit frames into the network and more powerful attacks can be done: MIM attacks, DOS (Denial Of Services) attacks on the cell, try to break in the network itself by means of buffer overflows or other known software bugs.

The “Nokia DCT3 Debug Trace” project uses a flow found in a commercial MS, Nokia 3310, sold with the debug symbols enabled. One can connect the phone to a computer and use specialized software: gammu, Nokia Netmonitor to get access to all the traffic information in the local beacon channel.

3. Solutions

GSM system is a success story. It was deployed very fast and in all corners of the world. But the fact that is so widespread makes it much more tested and verified. Also, this makes a security issue in the standard become a

worldwide problem within minutes it is discovered. The weaknesses are not only transformed in commercial products by many vendors, but also officially patented (Barkan & Biham, 2012). For this reason more and more operators and people question the confidentiality in their networks/calls. We present some solutions to prevent such situations. Some can be applied easily, while others require higher budget and longer time to deploy.

3.1. Solutions for Network Operators

One of the easiest solutions to quickly solve some of the most attacks (ETSI, 1996) would be to remove A5/0,2,1 from the list of accepted algorithms for encryption and use A5/3 and above only. The second step is to have the mobile authenticated, authorized and new key derived for every new service: call, SMS exchange, location update. A third step would be to always use and update TMSI after each encrypted session. The new value can be decided between the station and network in a secure way: at the end of each encrypted connection. A forth step would be replacing the old SIM cards with new ones, capable of COMP128-2 and COMP128-3.

3.2. Solutions for the Phone/SIM Cards Manufacturers

The A5/2 needs to be removed/disabled from the handsets. SIM cards should be better protected against side channel attacks like timing operations, power consumption or electromagnetic emissions (EME) with solutions suggested in the literature (Rao *et al*., 2002).

By definition relevant bits are those bits which determine what events will occur or are affected by the events in the current cycle. Because the events are usually associated with a different power consumption or EME, (Chari *et al*., 1999) presented a general Cardinal Principle "Relevant bits of all intermediate cycles and their values should be statistically independent of the inputs, outputs and sensitive information."

3.3 Solutions for Subscribers

Use secure phones which are already commercially available, ranging from user friendly ones like Blackphone with SilentCircle (Zimmerman, 2014) to security focused only ones, like CryptoPhones, (2014), Cellcrypt, (2013).

An even simpler guideline is to safely dispose old SIM cards, to keep previous conversations safe from SIM Cloning attacks.

4. Conclusions

Whenever wireless communications are involved, not long after their launch, some security issues appear (*e.g.* WiFi security issues). Worst comes when the state of security in vital systems like GSM is being questioned.

Despite the solutions that come with the new generation systems GPRS, UMTS, the insecurity will remain until the authentication and encryption between them and the second generation systems will be set apart completely. This issue appears because most of the phones allow using GSM as a fall-back solution when 3G is not available, and a GSM based attack works even when using a new phone on a 3G network. Having these major examples, GSM existing issues, GPRS/UMTS side attacks and WiFi flaws, we aim our future work in finding a solution for encrypting both current and future digital radio communications, focusing on voice communication.

REFERENCES

Avoine G., Junod P., Oechslin P., *Characterization and Improvement of Time-Memory Trade-Off Based on Perfect Tables*. ACM Trans. on Inf. and Sys. Security (TISSEC), **11**, *4*, 17.1-17.22 (2008).

Barkan E., Biham E., *Cryptanalysis method and system*. Google Patents., Patent no. US8295477 B2, 2012.

Barkan E., Biham E., Keller N., *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication.* J. of Crypt., **21**, *3*, 392-429 (2008).

Biham E., Dunkelman O., Keller N., *A Related-Key Rectangle Attack on the Full KASUMI*. Adv. in Crypt. Proc of Internat. Conf. on Th. a. Appl. of Crypt. ASIACRYPT 2005, Chennai, India, 2005, 443-461.

Biryukov A., Shamir A., Wagner D., *Real Time Cryptanalysis of A5/1 on a PC*. Proc. of 7th Internat. Workshop on Fast Soft. Ener., New York, USA, 2001, 1-18.

Briceno M., Goldberg I., Wagner D., *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.

Briceno M., Goldberg I., Wagner D., *An Implementation of the GSM A3A8 Algorithm*. Specifically, COMP128, from http://www.scard.org/gsm/a3a8.txt, 1998.

Chari S., Jutla C.S., Rao J.R., Rohatgi P., *Towards Sound Approaches to Counteract Power-Analysis Attacks.* Proc. of 19th Ann. Iniernat. Conf., Santa Barbara, USA, August 15-19, 1999 – CRYPTO'99, 398-412.

Dunkelman O., Keller N., Shamir A.,*A Practical-Time Attack on the A5/3 Crypto-system Used in 3rd Generation GSM Telephony*. IACR Cryptology ePrint Archive 2010, 2010/013, https://eprint.iacr.org/2010.

Gendrullis T., Novotný M., Rupp A., *A Real-World Attack Breaking A5/1 within Hours*. Proc. of Worksh. on Cryptographic Hardware and Embedded Systems, CHES, Washington, USA, Aug. 10-13, 2008, 266-282.

Goldberg I., Briceno M., *GSM Cloning.* Internet Sec. Appl. Anth. a. Crypt. (ISAAC) Research. Group, Univ. of Calif., www.isaac.cs.berkeley.edu/issac/gsm.html, 1998.

Goldberg I., Wagner D., Green L. *The Real-Time Cryptanalysis of A5/2*. Rump session of Crypto, **99**, 239-255 (1999).

Golić J.D., *Cryptanalysis of Alleged A5 Stream Cipher*. Adv. in Crypt., Proc. of 15th Internat. Conf. on Th. a. Appl. of Crypt. Tech. EUROCRYPT'97, May 11-15, 1997, Konstanz, Germany, 239-255.

Helfmeier C., Nedospasov D., Tarnovsky C., Krissler J.S., Boit C., Seifert J.-P., *Breaking and Entering through the Silicon*. Proc. of the 2013 ACM SIGSAC Conf. on Comp. & Commun. Security, Nov. 4-8, 2013, Berlin, Germany, 733-744.

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

Jokinen H., Uskela S., *Prevention of Spoofing In Telecommunications Systems*. Google Patents, US Patent no. 7,342,926 (2008), http://patents.com/us-7342926.html.

Kalenderi M., Pnevmatikatos D., Papaefstathiou I., Manifavas C. *Breaking the GSM A5/1 Cryptography Algorithm with Rainbow Tables and High-End FPGAS*. Proc. of 22nd Internat. Conf. on Field Progr. Logic a. Appl – FPL2012, Aug. 29-31, 2012, Oslo, Normay, 747-753.

Keller J., Seitz B. *A Hardware-Based Attack on the A5/1 Stream Cipher*. VDE ITG Fachbericht, Oct. 10-12, 2001, Munchen, Germany, 155-158.

Lackey J., Hulton D. *The A5 Cracking Project: Practical Attacks on GSM Using GNU Radio and FPGAs*. Proc. of Internat. Hacker Meet. on Chaos Comm. Camp, Aug. 8-12, 2007, Finowfurt, Berlin, Germany, Lecture ID: 2015.

Nohl K., *Attacking Phone Privacy*. Black Hat USA, srlabs.de/blog/wp-content/ uploads/2010/07/Attacking.Phone_.Privacy_Karsten_1.pdf, 2010.

Oechslin P., *Making a Faster Cryptanalytic Time-Memory Trade-Off*. Advances in Cryptology Proc. of 23rd Ann. Internet. Crypt. Conf., Santa Barbara, USA, Aug. 18-21, 2003, CRYPTO 2003, 617-630.

Pagliusi P.S., *A Contemporary Foreword on GSM Security*. *Infrastructure Security*. Proc. of Internat. Conf. on Infr. Sec., Oct. 1-3, 2002, Bristol, UK, 129-144.

Petrovic S., Fuster-Sabater A., *Cryptanalysis of the A5/2 Algorithm*. IACR Cryptology ePrint Archive 2000, 2000/052, https://eprint.iacr.org/2000.

Quirke J., *Security in the GSM System*. http://www.ausmobile.com, 2004.

Rao J.R., Rohatgi P., Scherzer H., Tinguely S., *Partitioning Attacks: or How to Rapidly Clone Some GSM Cards*. Proc. 2002 IEEE Symp. on Sec. a. Priv., May 12-15, 2002, Berkeley, USA, 31-41.

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

Stoffelen K., Poll E., van den Broek F., Schwabe P., *Comparison of Chain Merge Behaviour of TMTO Methods*. BSc Ihesis, Radboud Univ., http://www.cs.ru.nl/ 2012/Ko_Stoffelen_3030547_Comparison_of_chain_merge_behaviour_of_TMTO_methods.pdf, 2012.

Whitehouse O., *Attacks and Counter Measures in 2.5G and 3G -Cellular IP Networks*. www.csisoft.com/security/checkpoint/atstake_cellular_cg3.pdf,2004.

Zimmerman P., Javier Agüera J.C., *BlackPhone*. from http://www.blackphone.ch/, 2014.

* * * *Cellcrypt*. from www.cellcrypt.com; http://www.cellcrypt. com/gsm-cracking, 2013.

* * * *GSM System Security Study*. RACAL, from https://web.archive.org/web/ 20060714110045/http://jya.com/gsm-cloned.htm.

* * * *GSMK CryptoPhones*. from www.cryptophone.de; http://www.cryptophone.de/en/ background/gsm-insecurity/references/, 2014.

* * * *Security Algorithms Group of Experts* (*SAGE*). ETSI, Report on the specification and evaluation of the GSM cipher algorithm A5/2, Europ. Telecommun. Standards Inst., 1996.

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

(Rezumat)

În lucrare se prezintă o paralelă între atacurile teoretice asupra sistemului GSM şi cele ce pot fi implementate practic. Sunt detaliate diferite implementări pentru a demonstra aplicabilitatea lor. Două subiecte importante sunt abordate şi anume: securitatea la nivelul de distribuție şi securitatea pe interfața radio. Aceasta din urmă este analizată atât pe tipuri de algoritmi cât şi pe tipurile de atacuri. Sunt detaliate, de asemenea, o serie de soluții ce pot fi aplicate atât de operatori cât şi de utilizatori în vederea îmbunătățirii securității. Unele metode de protecție pot fi implementate cu un buget mai redus (spre exemplu întreruperea utilizării algoritmilor mai slabi gen A5/2), în timp ce alte metode sunt mai costisitoare, dar rezolvă unele probleme de bază gen autentificarea rețelei de către utilizator. În ultima parte se prezintă concluzii asupra nivelului curent de securitate în rețelele heterogene cu tehnologii 2G, 2.G şi, respectiv, 3G. 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.