A Review of Security Attacks on the GSM Standard

Giuseppe Cattaneo, Giancarlo Maio, Pompeo Faruolo, Umberto Petrillo

A Review of Security Attacks on the GSM Standard

Giuseppe Cattaneo[1], Giancarlo De Maio[1],
Pompeo Faruolo[1], and Umberto Ferraro Petrillo[2⋆]

[1] Dipartimento di Informatica *"R. M. Capocelli"*
Università di Salerno, I-84084, Fisciano (SA), Italy
cattaneo@dia.unisa.it, demaio@dia.unisa.it, pomfar@dia.unisa.it
[2] Dipartimento di Scienze Statistiche
Università di Roma *"La Sapienza"*, I-00185, Roma, Italy
umberto.ferraro@uniroma1.it

Abstract. The Global Systems for Mobile communications (GSM) is the most widespread mobile communication technology existing nowadays. Despite being a mature technology, its introduction dates back to the late eighties, it suffers from several security vulnerabilities, which have been targeted by many attacks aimed to break the underlying communication protocol. Most of these attacks focuses on the A5/1 algorithm used to protect over-the-air communication between the two parties of a phone call. This algorithm has been superseded by new and more secure algorithms. However, it is still in use in the GSM networks as a fallback option, thus still putting at risk the security of the GSM based conversations. The objective of this work is to review some of the most relevant results in this field and discuss their practical feasibility. To this end, we consider not only the contributions coming from the canonical scientific literature but also those that have been proposed in a more informal context, such as during hacker conferences.

Keywords: GSM, mobile security, security attacks, encryption

1 Introduction

The GSM is the most widespread mobile communication technology, accounting for more than five billion subscriptions. Far from being just a personal communication technology, it has become the medium of choice for implementing and delivering a vast array of services ranging from mobile banking applications to electronic ticketing. This widespread use is also motivating the interest of researchers in evaluating the security mechanisms provided by GSM to protect user communication. In particular, the GSM protocols suffer from many weakness which allowed for the development of several attacks able to break confidentiality and privacy of subscribers. GSM carriers seem to have underestimated these

⋆ Corresponding author: Umberto Ferraro Petrillo, umberto.ferraro@uniroma1.it, Phone: +390649910513

threats, as witnessed by the several solutions for providing security to GSM-based communications (see [4, 5, 7, 10]) proposed so far.
The objective of this paper is to review some of the most relevant security attacks to the GSM related technologies, including also those techniques that, although not being presented in a formal scientific context, have proved to be very effective in practice.

2 The GSM Standard

The GSM has been developed by the ETSI as a standard [1] to describe protocols for second generation digital cellular networks used by mobile phones. It offers several services based on voice transmission and data transmission. Three are the main elements of a GSM network. The first is the *Mobile Station*. It is made up of the Mobile Equipment (ME), the physical phone itself, and the Subscriber Identity Module (SIM). The SIM is a smart card that carries information specific to the subscriber together with the encryption keys (Ki and Kc). The second element is the *Core Network*. It carries out call switching and mobility management functions for mobile phones roaming on the network of base stations. It is made of several components. The third element is the *Base Station Subsystem*. It is responsible for handling traffic and signaling between a mobile station and the core network.

2.1 Security Features

The GSM standard defines several security mechanisms for protecting both the integrity of the network and the privacy of the subscribers. Whenever a ME tries to join a GSM network, it has to pass through an authentication procedure required to verify the identity of the subscriber using it. This denies the possibility for a subscriber to impersonate another one and guarantees that only authorized subscribers may access the network. When connected, the signaling and data channels over the radio path between a base station and the ME are protected by means of an encryption scheme. This ensures the confidentiality of the conversations. In the following we provide more details about these schemes and about the cryptographic machinery they use.

Authentication. The GSM network authenticates the identity of a subscriber using a challenge-response mechanism. Firstly, the Authentication Center (AuC), located within the core network, generates a 128-bit random number ($RAND$) and sends it to the ME. Then, the ME computes the 32-bit signed response ($SRES$) based on the encryption of $RAND$ with the authentication algorithm ($A3$) using the individual subscriber authentication key (Ki). The computation is entirely done within the SIM. This provides enhanced security, because the confidential subscriber information such as the individual subscriber authentication key (Ki) is never released from the SIM during the process. On the network, upon receiving the signed response ($SRES$) from the subscriber, the AuC compares its value of $SRES$ with the value received from the ME.

If the two values match, the authentication is successful and the subscriber joins the network. Notice that GSM authenticates the user to the network and not vice-versa. So, the security model offers confidentiality and authentication, but not the non-repudiation.

Data Confidentiality. The SIM contains the implementation of the key generation algorithm (A8) which is used to produce the 64-bit ciphering key (Kc) to be used to encrypt and decrypt the data between the ME and the base station. It 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). Additional security is provided by the periodic change of the ciphering key. Similarly to the authentication process, the computation of the ciphering key (Kc) is done within the SIM.
Encrypted communications between the MS and the network is done using one of the A5 ciphering algorithms. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the selected ciphering algorithm and the ciphering key (Kc). The A5 algorithms are implemented in the hardware of the ME, as they have to encrypt and decrypt data on the fly.

The A5 Ciphering Algorithms. In the GSM protocol, the data is sent as sequence of frames, where each frame contains 228 bit. Each plaindata frame is XORed with a pseudorandom sequence generated by one of A5 stream cipher algorithms for ensuring over-the-air voice privacy.
The A5/1 algorithm was developed in late 1987 and is based on three *linear feedback shift registers* (LFSR). The keystream is built by running an algorithm, called *clock*, that produces 1 bit at each step. The output of the algorithm is the XOR of the leftmost bit of the three LFSR registers. Each register has a *clocking bit*. At each cycle, the clocking bits of the registers are given as input to a *function* that computes the *majority bit*. A register is *clocked* if the clocking bit agrees with the majority bit. The A5/2 algorithm was introduced in 1989, it is a deliberate weakened version of the A5/1 that is almost identical to its counterpart except for an additional LFSR used to produce the three clocking bits. Since 2007, A5/2 is not implemented anymore in mobile phones for security reasons. Finally, the A5/3 algorithm was developed in 1997 and is based on the MISTY cipher [12]. In the 2002 it was modified in order to obtain a faster and more hardware-friendly version, called KASUMI [1].

3 Attacks

There is a wide category of attacks against mobile communications that do not depend on network weaknesses. It includes mobile phones malware, identity theft by SIM cloning and so on. Some other attacks, such as phishing with SMS, may exploit human factors as well. A good review of such security issues can be found in [6]. On the contrary, this work focuses on attacks that exploit vulnerabilities of GSM protocols.

Most of these attacks target the A5 family of ciphering algorithms. The exact formulation of these algorithms is still officially secret. However, the research community has been able to recover it through a mix of reverse engineering and cryptoanalysis. Namely, the general design of A5/1 was leaked in 1994 and the first cryptanalysis of A5/1 has been performed by Golic [9].
In this section we review some of the most interesting attacks proposed so far, distinguishing by passive and active attacks.

3.1 Passive Attacks

The first attack targeting the A5/1 algorithm has been proposed by Golic [9], which introduced an effective Time-Memory Trade-Off (TMTO) attack based on the birthday paradox. The basic idea of the TMTO is to pre-compute a large set of states A, and to consider the set of states B through which the algorithm progresses during the generation of output bits. Any intersection between A and B allows to identify an actual state of the algorithm. The proposed attack would be practicable only having 15 TB of pre-calculated data or 3 hours of known conversation [3].
Biryukov *et al.* presented two attacks based on a TMTO [3]. The first attack requires 2 minutes of known-conversation data and one second of processing time, while the second requires 2 seconds of plaintext data and several minutes of processing time. The amount of required storage is up to 290 GB. Unfortunately, its execution time grows exponentially with the decreasing of the input sequence. The attack exploits many weaknesses of A5/1, like the possibility of identifying states by prefixes of their output sequences, the ability to quickly retrieve the initial state of an intermediate frame and the possibility to extract the key from the initial state of any frame. The major drawback of this attack is the considerable amount of known-conversation data required.
A different strategy, based on a correlation attack, was introduced by Ekdahl *et al.* [8]. The main advantage is that whereas TMTO attacks have a complexity which is exponential with the shift register length, here the complexity is almost independent from it. This attack exploits the weakness that the key and the frame counter are initialized in a linear fashion, which enables to separate the session key from the frame number in binary linear expressions. This allows to decrypt a conversation in less than 5 minutes, provided that few minutes of plaintext conversation are available. Moreover, the time and space requirements for the tables precomputation are much smaller than in previous attacks.
All the attacks presented so far had very high computational cost and/or were based on unrealistic assumptions. Instead, the first practicable attack, implementable by means of open-source software and commodity hardware, has been made public by Nohl in 2009 [13]. This work showed that A5/1 is vulnerable to generic pre-computation attacks. In fact, for a cipher with small key (64 bit in the case of A5/1), it is possible to construct a *code book*. It can be exploited to perform a known-plaintext attack. For the case of A5/1, if an adequate number of plaintext/ciphertext couples are known, it is possible to recover the encryption key. In the case of GSM, a number of predetermined control messages can be leveraged

as known plaintexts [14]. Considering all the possible combinations, Nohl estimated that a code book for A5/1 would have been sized 128 PB and would have taken more than 100,000 years to be computed on a standard PC. In their talk, Nohl and Paget revisited techniques for computing the code book faster and for storing it compressed. They proposed a tweaked A5/1 engine optimized for parallelization. By using this technique a full code book for A5/1 can be computed in 3 months using commodity hardware. Some tweaks presented in subsequent talks [14, 17] allowed to lower this boundary to 1 month on 4 ATI GPUs. Moreover, he proposed the use of a combined approach for data storage which makes use of distinguished point and rainbow tables [11], by means of which it is possible to reduce the size of the code book to just 2 TB.
Nohl estimates that the attack has a 99% success rate when data from a phone registered to the network can be collected, which maximizes the amount of known control frames. Otherwise, the success rate drops to 50%, since only a small number of frames with known plaintext is available. In a subsequent talk, Nohl and Munaut performed a demonstration on how it is possible to find phones and decrypt their calls [15].

3.2 Active Attacks

Differently from passive attacks, active attacks exploit some design weaknesses of the telecommunication infrastructure which make possible to introduce a false mobile tower controlled by the attacker. The major security hole exploited by the fake tower, also called IMSI Catcher, is that the GSM specification does not require authentication of the network to the mobile phone. The IMSI Catcher acts between the victim mobile phone(s) and the real towers provided by the service provider, and it is able to both control communication parameters, like encryption algorithms, and eavesdrop traffic. Such an attack falls into the category of Man-In-The-Middle (MITM) attacks.
Some MITM attacks against GSM have been introduced in [2]. They suppose that the victim is connected to a fake base station, which is able to intercept and forward the data sent by the phone to the network and vice versa. At this point, independently from the encryption algorithm chosen by the network, the attacker can request the victim to use a weak cipher like A5/2 (or even no encryption). Then, the attacker can employ cryptanalysis of A5/2 to retrieve the encryption key. It is worth noting that the key generation algorithm only depends on the RAND parameter specified by the network. As consequence, the encryption key used between the victim and the attacker is the same used between the attacker and the network, so that the attacker can decrypt all the traffic even if a secure encryption algorithm like A5/3 is requested by the network.
Paget and Nohl showed how it is possible to catch IMSI of a subscriber by means of an active attack [17]. Their attack makes use of a fake base station that could even be built from open source components.
In 2010 a practical attack to GSM has been presented by Paget [16] using open source components. It exploits the vulnerability that the mobile phone connects to the strongest base station signal. Since the base station has full control over communication protocols, the handset can be

instructed in order to use no traffic encryption (A5/0). In this way, the attacker can intercept all the traffic in plaintext.

References

1. 3rd Generation Partnership Project (3GPP): Technical Specifications for GSM systems. http://www.3gpp.org/
2. Barkan, E., Biham, E., Keller, N.: Instant ciphertext-only cryptanalysis of GSM encrypted communication. Advances in Cryptology-CRYPTO 2003 (2003)
3. Biryukov, A., Shamir, A., Wagner, D.: Real time cryptanalysis of A5/1 on a PC. Fast Software Encryption (2001)
4. Castiglione, A., Cattaneo, G., Maio, G., Petagna, F.: SECR3T: Secure End-to-End Communication over 3G Telecommunication Networks. In: IMIS 2011. pp. 520 –526 (2011)
5. Castiglione, A., Cattaneo, G., Cembalo, M., De Santis, A., Faruolo, P., Petagna, F., Ferraro Petrillo, U.: Engineering a secure mobile messaging framework. Computers & Security 31(6), 771 – 781 (2012)
6. Castiglione, A., Prisco, R.D., Santis, A.D.: Do you trust your phone? In: Noia, T.D., Buccafurri, F. (eds.) EC-Web. Lecture Notes in Computer Science, vol. 5692, pp. 50–61. Springer (2009)
7. De Santis, A., Castiglione, A., Cattaneo, G., Cembalo, M., Petagna, F., Ferraro Petrillo, U.: An Extensible Framework for Efficient Secure SMS. IMIS 2010 pp. 843 – 850 (2010)
8. Ekdahl, P., Johansson, T.: Another attack on A5/1. Information Theory (2003)
9. Golic, J.D.: Cryptanalysis of Alleged A5 Stream Cipher. In: Fumy, W. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 1233, pp. 239–255. Springer (1997)
10. GSMK: Cryptophone. http://www.cryptophone.de/ (2012)
11. Lee, G.W., Hong, J.: A comparison of perfect table cryptanalytic tradeoff algorithms. Cryptology ePrint Archive, Report 2012/540 (2012), http://eprint.iacr.org/
12. Matsui, M.: New Block Encryption Algorithm MISTY. In: Biham, E. (ed.) FSE. Lecture Notes in Computer Science, vol. 1267, pp. 54–68. Springer (1997)
13. Nohl, K.: Subverting the security base of GSM. In: Hacking at Random (2009), https://har2009.org/program/events/187.en.html
14. Nohl, K.: Attacking phone privacy. In: BLACK HAT USA (2010), http://www.blackhat.com/html/bh-us-10/bh-us-10-archives.html
15. Nohl, K.: Wideband GSM sniffing. In: 27th Chaos Communication Congress (2010), http://events.ccc.de/congress/2010/Fahrplan/events/4208.en.html
16. Paget, C.: Practical Cellphone Spying. In: DEF CON 18 (2010), http://defcon.org/html/links/dc-archives/dc-18-archive.html
17. Paget, C., Nohl, K.: GSM: SRSLY? In: 26th Chaos Communication Congress (2009), http://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html