University of Ljubljana
Faculty of Computer and Information Science

Analysis of SIM card

Aleksandra Turanjanin

Mentor: Prof. Dr. Aleksandar Jurišić

January, 2018

Introduction

By the 2018 SIM cards have become one of the most used smart cards in the world. Mobile phones without SIM cards, for now, are barely usable and these cards are also used in other gadgets as well, mostly for notifying of security alarms or for collecting data from some device that is on far distance from us.

But have we ever wondered does anyone can track us and our phones? Or could our phone numbers be used without us knowing it? What mechanisms are supposed to protect our privacy?

In this project I will try to answer these questions and explain usage of SIM card, security mechanism and its flaws.

1 SIM card

1.1 The evolution of the SIM card

A SIM card or Subscriber Identity Module is an element of a mobile phone which is used to authenticate and identify subscribers on mobile telephone devices. The SIM was initially specified by the European Telecommunications Standards Institute. The first SIM card was developed in 1991 by Munich smart card maker Giesecke & Devrient, who sold the first 300 SIM cards to the Finnish wireless network operator. Today, SIM cards are ubiquitous, allowing over 7 billion devices to connect to cellular networks around the world. According to the International Card Manufacturers Association, there were 5.4 billion SIM cards manufactured globally in 2016. The rise of cellular IoT (Internet of Things) and 5G networks is predicted to drive growth of the addressable market for SIM card manufacturers to over 20 billion wireless devices by 2020.

The SIM card was not born at the same time as the cellular phone. (1) The first mobile phones supported only embedded communication standards: the subscription parameters were hard-coded into the mobile terminal's memory. The oldest analogue standards used in mobile phones did not have any means of security. The subscription data could be copied into another device and cloned, making it possible to call and accept calls on the owner's behalf, free of charge. The first means of security was the so called Subscriber Identity Security or SIS code. SIS code was 18-digit number which was unique to a device and hard-coded into an application processor. These codes used to be evenly distributed among the vendors so two devices could not share the same SIS code. The processor also stored a 7-digit reseller identification (RID) code which was transmitted to a base station when a subscriber registered to a network. The base station would generate a random number, which packed with unique SIS response, SIS processor would use to produce the authorization key. Both keys and numbers were relatively short but adequate for that time.

The system was later cracked, just three years before the Global System for Mobile Communications (GSM) standard emerged. GSM was more secure by design as it used a similar, yet more cryptically resilient authorization system. The standard thus became detached. This meant that the authorization was then fully performed on an external processor integrated into a smart card. The resulting solution was called SIM. With the appearance of SIM cards, the subscription was no longer dependent on the devices so a user could change devices as frequently as wished, while preserving the mobile identity.

A SIM card is basically a standard smart card and has no significant difference from other contact based cards, like credit cards. The first SIM even had the same size as a credit card, but the overall trend of shrinking dimensions had led to a newer, more compact form.

1.2 Smart card

As stated, a SIM cad is a smart card and it has no significant difference from other contact based cards. The term smart card refers to whole set of devices that operate under similar principle by using microcontroller and memory allocation. Then this chip is exposed, by contact or wirelessly, to another system in order to exchange data and identity information. Smart cards can provide personal identification, data storage, authentication and application processing. (2) The main reason for using smart cards is definitely the security of the stored data on the card and data protection of other computer systems. Therefore, the hardware on smart card is designed and optimized for these tasks. All of this is followed by appropriate cryptosystems for data protection. Security depends on microcontroller and algorithms performed by the operating systems but it is also important to ensure the security of entire use of smart cards.

1.3 Types of SIM card

Figure 1: Types of SIM card

1.3.1 Full-size SIM

The full-size SIM (or 1FF, 1st form factor) was the first form factor to appear. It has the size of a credit card (85.60 mm × 53.98 mm × 0.76 mm). The form factor was first mentioned in the December 1998 and it represents the size, configuration, or physical arrangement of a computing device.

1.3.2 Mini-SIM

The mini-SIM (or 2FF) card has the same contact arrangement as the full-size SIM card and is normally supplied within a full-size card carrier, attached by a number of linking pieces. This lets such a card be used in a device that requires a full-size card or in a device that requires a mini-SIM card, after breaking the linking pieces. As the full-size SIM is no longer used, the mini-SIM is called a standard SIM or regular SIM.

1.3.3 Micro-SIM

The micro-SIM (or 3FF) card has the same thickness and contact arrangements, but reduced length and width as shown in Figure 1. The micro-SIM was introduced by the European Telecommunications Standards Institute (ETSI) along with some other cards for the purpose of fitting into devices too small for a mini-SIM card. The iPhone 4 was the first smartphone to use a micro-SIM card in June 2010, followed by many others.

1.3.4 Nano-SIM

The nano-SIM (or 4FF) card was introduced in October 2012, when mobile service providers in various countries started to supply it for phones that supported the format. The nano-SIM measures 12.3 × 8.8 × 0.67 mm and reduces the previous format to the contact area while maintaining the existing contact arrangements. A small part of isolating material is left around the contact area to avoid short circuits with the socket. The iPhone 5, released in September 2012, was the first device to use a nano-SIM card, followed by other handsets.

1.4 Structure and authentication

While SIM card is being manufactured, certain information is written into the memory of it: the International Mobile Subscriber Identity or IMSI, in accordance to the carrier who ordered the batch and a 128-bit key called Ki (Key Identification). IMSI and Ki are the subscriber's login and password, respectively, hard-coded into the SIM card chip.

The correspondence between a subscriber's IMSI and the phone number is stored in a special database called HLR (Home Location Register) (3). This data is copied into another database, VLR (Visitor Location Register) in each segment of the network, based on the subscriber's temporary guest registration to another base station. The authorization process is quite simple. When a subscriber is registered to the temporary database, VLR sends a random 128-bit number (RAND) to the phone number. The SIM card processor uses the A3 algorithm to generate a 32-bit signed response (SRES) to VLR, based on the RAND number and Ki. If VLR gets a matching response, the subscriber becomes registered in the network. SIM also generates another temporary ciphering key called Kc. Its value is calculated based on above mentioned RAND and Ki with the help of the A8 algorithm. That key is used to encrypt transmitted data by means of the A5 algorithm. The encryption is always enabled by default, however, in certain circumstances it is switched off, making it possible for an intelligence agency to intercept phone conversations.

2 Security

A SIM card uses the Personal Identification Number or PIN code to provide security and usually after three wrong attempts it requests PUK (PIN Unlock) code. User then gets usually ten opportunities to type PUK correctly, after that SIM makes itself useless by refusing local access to its privileged information and authentication functions.

Authentication and confidentiality of user data are in deposit of the secrecy of IMSI and Ki. With disclosure of such numbers, anyone can imitate a legitimate user. A3 and A8 algorithms are also implemented on every SIM. This means that each operator can determine and change such algorithms independent of other operators and hardware manufacturers. Therefore, the authentication will work when a user is roaming on other countries or operators since the local network will query the HLR of the home network for the results and does not need to know the A3/A8 algorithm of the home network.

2.1 A3 Algorithm

The A3 algorithm is used to generate a signed response which is sent from Mobile Station Equipment (MSE) to base transceiver station (BTS) to authenticate the identity of the MSE: The MSE retrieves the 32-bit Signed Response (SRES) by issuing a command to the SIM. This command includes the 128-bit random challenge (RAND) generated by the Home Location Register. The SIM uses the RAND, its 128-bit Ki and the A3 algorithm to calculate a 128-bit response which is returned to the MSE, then passed on to the BTS, Mobile Switching Center (MSC) and finally verified by the Authentication Center.

Only the first 32 bits are used as SRES. A3 is completely implemented in the smart card, so Ki never leaves the SIM. Most GSM networks use a version of the COMP128 algorithm as implementation of A3.

2.2 A8 Algorithm

The key generation algorithm A8 is very similar to A3. In fact, the same COMP128 algorithm is used to create the 64-bit ciphering key (Kc) which is subsequently used in A5: Taking the 128-bit RAND received from MSC and the 128-bit Ki stored in the SIM as input, A8 calculates 128 bits of output. Figure 2 shows a schema of this data flow. The same key Kc stays active until the MSC decides to request a new one, which rarely happens and is therefore an issue concerning attacks.

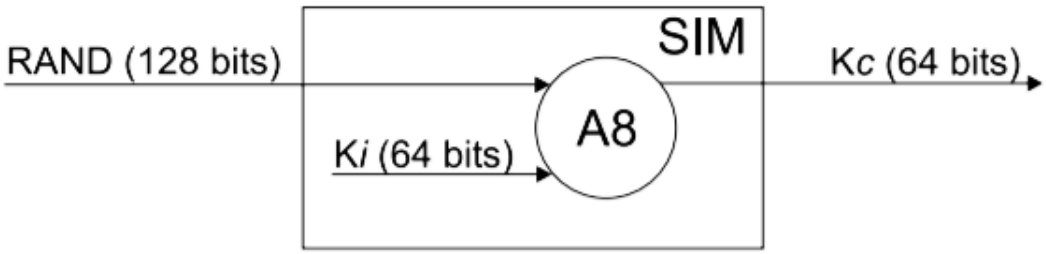

Figure 2: Data flow of A8

As have been said before, the COMP128 algorithms are implementations of the A3 and A8 algorithms defined in the GSM standard. The first version (COMP128-1) is poorly structured. The actual length of the Kc, which is obtained at the output, is only 54 bits. The last 10 bits are always empty, which is a security defect in further use for encryption. Because of a leaked document the first version of COMP128 was made public in 1997 and shortly later was successfully attacked. Nowadays, with improved attacks it is possible to extract the Ki in less than a minute, given physical access to the SIM and knowing the PIN. The extracted Ki can then be used to break authentication security and for example clone SIM. Therefore GSM network providers have switched to COMP128-2, COMP128-3 and COMP128-4 (for 3G networks) algorithms.

2.3 A5 Algorithm

The cryptographic algorithms are implemented on the hardware of mobile phones. To protect privacy all over-the-air transmissions on a GSM network are encrypted with a stream cipher known as A5. Three algorithms are generally available: A5/1, A5/2, and A5/3. A5/1 and A5/2 are two stream ciphers originally defined by the GSM standards. A5/1 is stronger but it is subject to export control and can be used by those countries that are members of The European Conference of Postal and Telecommunications Administrations. A5/2 is deliberately weakened to be used by the other countries. A5/3 is a block cipher based on the Kasumi algorithm that is defined by the 3GPP (The 3rd Generation Partnership Project) and can be supported on dual-mode phones that are capable of working on both 2G and 3G systems. The GSM authentication, session key generation, and encryption processes are depicted in Figure 3.

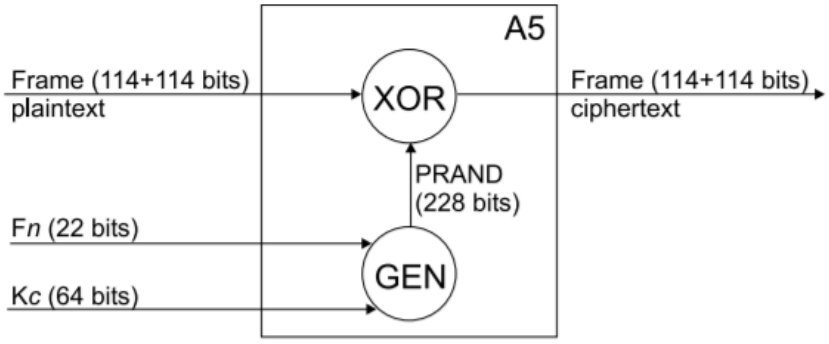

Figure 3: GSM Authentication, Session key generation, and Ciphering

A5 is a stream cipher (4). It operates on 228-bit blocks called frames which are sent and received over the air every 4.6 milliseconds. 114 bits represent data sent from the MSE and the other 114 bits are data received by the MSE, both mainly containing digitized audio signals. Taking the ciphering key Kc produced by A8 and a frame counter Fn, A5 generates 228 pseudo random bits (PRAND) which are XOR-ed with the plaintext frame resulting in 228 bits of ciphertex (5)t. The most important part in A5 is generating the pseudo random bits (function GEN in figure 3).

In 2010, Dunkelman, Keller and Shamir published an attack that allows an adversary to recover a full A5/3 key by related-key attack (5). The time and space complexities of the attack are low enough that the authors carried out the attack in two hours on an Intel Core 2 Duo desktop computer even using the unoptimized reference Kasumi implementation. The authors note that this attack may not be applicable to the way A5/3 is used in 3G systems, but their main purpose was to discredit 3GPP's assurances that their changes to MISTY wouldn't significantly impact the security of the algorithm.

3 Attacks

3.1 IMSI Catcher

An International Mobile Subscriber Identity-catcher, or IMSI-catcher, is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users. Basically it is a fake mobile tower acting between the target mobile phone and the service provider's real towers, it is considered a man-in-the-middle attack. The GSM specification requires the handset to authenticate to the network, but does not require the network to authenticate to the handset. The IMSI catcher has took advantage of this well-known security hole. It masquerades as a base station and logs the IMSI numbers of all the mobile stations in the area, as they attempt to attach to the IMSI-catcher. It allows forcing the mobile phone connected to it to use no call encryption or to use easily breakable encryption (A5/1 or A5/2), making the call data easy to intercept and convert to audio.

This vulnerability was designed to be there from the start so intelligence services could perform Man-In-The-Middle attacks when appropriate for the case. IMSI-catchers are often deployed by court order without a search warrant. They can also be used in search and rescue operation for missing persons (6). This procedure has raised significant civil liberty and privacy concerns and is strictly regulated in some countries, while od the other hand in some countries data traffic is not even encrypted or it has very weak encryption thus rendering an IMSI-catcher unnecessary.

3.2 Clone attack

One of the first vulnerabilities in SIM cards that was ever discovered was the possibility of cloning. In this case, cloning means reading the contents of a SIM card and writing them into the memory of another SIM card. It is quite understandable, given the fact that a SIM card, from the hardware perspective, is just an ordinary smart card which are available anywhere and are cheap as chips (7).

However, the opportunity to clone SIM cards could be used for malicious activities. Having received short-term access to the victim's SIM card, an adversary could clone it and thus compromise the legitimate SIM card. If a cloned SIM card is active during the time when the legitimate subscriber is registered in the mobile network, the latter would get its connection cut off and still remain totally unaware of it. In that case, all inbound calls and messages will be directed to the adversary, and they, in turn, would be able to make calls, send messages and browse the Internet on the victim's behalf. The unsuspecting victim would even see the normal network indicators and the name of the carrier on the screen, which would create the illusion of connection, however, the targeted subscriber would not be able to make calls until the handset is rebooted or the mobile network obligatory refreshes the registration status and that typically happens automatically once every few hours.

A clone could be registered basically anywhere, even on another continent. Then carriers introduced some primitive means of security such as: if a subscriber suddenly registers far from the location he was registered recently, administrators would get a corresponding notification as a warning. Still attacker may register in a location pretty close to the victim, which renders the abovementioned security approach useless.

The Ki key, which is used to authorize a subscriber in the network, is normally never read from the SIM card. A SIM card processor calls it on the inside, so the key is not meant to be shared over the air. It is stored in a protected segment of the memory and there are no application programming interfaces which could read it. But here is where cryptanalysis methods come into use.

If an attacker employs a software which repeatedly runs the A3 algorithm on a SIM card, making it to process random RAND passwords and to produce SRES responses in return, certain weaknesses could be discovered and thus the Ki key could be calculated. Even more then 10 years ago, PC performance levels were enough to complete such a task in just a few minutes. However, it is not that simple. Any SIM card has a kind of self-destruction timer counting how often the algorithm is run. For instance, the card's limit may be 50 000 times. As soon as this limit is reached, the SIM card processor would stop calculating SRES responses. If one has not succeeded in calculating Ki, the SIM card becomes totally useless and should be replaced. Sometimes it happens in real life with a legitimate SIM card, provided that it was used for quite a while and the value of the limit was initially low.

Also cryptanalysis can be used to obtain Ki value only on those SIM cards which support the first version of A3 algorithm – COMP128-1. Those are still used by some carriers, and such cards can indeed be cloned. More advanced carriers have already switched to COMP128-2 and COMP128-3 algorithms which increase the number of RAND-SRES bundles so the Ki key cannot be calculated with the use of the abovementioned method.

German cryptographer Kristen Nohl (8) and his team experimented on more than 1000 SIM cards during a two-year investigation. In 2013 he said that he has found a way to discover SIM card's digital keys by sending a special text message to it and in that way exposes chip to manipulation. This means that SIM card can work against user. The hacker starts by sending a text message to the SIM card that the user doesn't even get to see, and the SIM card in some cases responds with data that can be run through with cryptanalysis. Once an attacker cracks the key, he can commit premium SMS fraud, circumvent caller-ID checks, manipulate voice-mails, redirect incoming calls and text messages, abuse payments, track users, install malware on their devices, or perform any other browser-based attack. With data access enabled, Nohl claims that an attacker can clone SIM cards, decrypt 2G, 3G, and 4G traffic, clone NFC takers and future SIM applications.

Also, in 2015 a Jiao Tong University (9) researcher has exploited side-channel attack techniques to crack the encryption codes. Side-channel attacks measure things like power consumption, electromagnetic emissions and heat generation to work out what is going on in a chip. They cracked eight commercial SIM cards in between 10 and 80 minutes.

4 Future SIM cards

4.1 Virtual SIM card

Virtual SIM cards are cards that appeared mostly because of urge to have several SIM cards available at the same time and because of inconvenience of user while roaming.

On virtual SIM card there is a protected section in the internal memory of a handset, just like in any regular SIM card. However, all the data is downloaded through the radio channel, including identifiers which are usually stored in the HLR database on the carrier's side, which the handset gets via a secure channel. From the technology standpoint, the deployment is very simple as well. A SIM card remains in its place but it's just an imitation which contains no data, and some of its memory can be rewritten. This capability is supported in the newest iPads where one can just buy an Apple SIM imitation and write any carrier's data onto it.

4.2 Embedded-SIM (eSIM)

eSIM (10) is the step forward. In previous solutions, a SIM card profile is downloaded remotely, but on the device level, this profile is stored on a SIM card's substitution which could be reused in a different handset. In case of eSIM, there are no replaceable substitutions at all, and the chip itself is embedded into the handset. eSIM is a non-replaceable embedded chip that is soldered directly onto a circuit board. The surface format provides the same electrical interface as the full size, 2FF and 3FF SIM cards, but is soldered to the circuit board as part of the manufacturing process.

The European Commission has selected the Embedded SIM format for its in-vehicle emergency call service known as eCall. All new car models in the EU must have one by end of this year to instantly connect the car to the emergency services in case of an accident.

A regular SIM card is easily disposed of when a person's handset is stolen or lost. In this case an outsider can use the newly obtained device with a different SIM card. But this trick would not work on eSIM. The one would not be able to download a new profile without the legitimate owner's password; moreover, on each reboot, the handset will download the previous profile, making it possible to locate the device.

Conclusion

In this project SIM card's background is shown together with its past and future. Structure of a card and security algorithms are explained as well as the attacks that can be performed. Although new technologies have tendencies to use less and less physical equipment in phones, SIM cards were and continue to be very efficient. Security of SIM card is proven not to be very high but providers are trying to improve it in upcoming generations. As already stated, some attacks are used in intelligence agencies in ordered to catch culprits, but there are speculations that agencies use these attacks on ordinary people in order to find out identification keys for every SIM card that is made. However, no one has ever acknowledged usage of attacks in these purposes and we, as ordinary citizens, can hope we will not become their persons of interest for security matter.

Bibliography

1. *The evolution of the SIM card.* **Shatilin, Ilja.** s.l. : Kaspersky, 2016. https://www.kaspersky.com/blog/sim-card-history/10909/.

2. *Pametne kartice in varnost.* **Jurišić, Aleksandar and Tonejc, Jernej.** 2001. http://lkrv.fri.uni-lj.si/~ajurisic/sc/m1.pdf.

3. *Solutions to the GSM Security Weaknesses.* **Toorani, Mohsen and Beheshti, Ali A.** 2009. https://arxiv.org/ftp/arxiv/papers/1002/1002.3175.pdf.

4. **Stockinger, Thomas.** *GSM network and its privacy - the A5.* 2005. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.8718&rep=rep1&type=pdf.

5. **Dunkelman, Orr, Keller, Nathan and Shamir, Adi.** *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony.* 2010. https://eprint.iacr.org/2010/013.pdf.

6. *THE GREAT SIM HEIST.* **Scahill, Jeremy and Begley, Josh.** 2015. https://theintercept.com/2015/02/19/great-sim-heist/.

7. *SIM cards: attack of the clones.* **Shatilin, Ilja.** 2016. https://www.kaspersky.com/blog/sim-card-history-clone-wars/11091/.

8. *Sim card flaws leave millions of mobile phones open to attack, hacker finds.* 2013. https://www.theguardian.com/technology/2013/aug/01/sim-card-flaw-cellphone-hackers-karsten-nohl.

9. *Cracking SIM cards with side-channel attacks.* 2015. https://www.rambus.com/blogs/cracking-sim-cards-with-side-channel-attacks-2/.

10. *eSIM: what is it for?* **Shatilin, Ilja.** 2016. https://www.kaspersky.com/blog/what-is-esim/11400/.

11. **GSMA.** *Generic Overlay SIM Security Assessment.* 2014. https://www.gsma.com/publicpolicy/wp-content/uploads/2014/08/GSMA-Security-Group-Overlay_SIM_Security_Assessment_August_18_2014.pdf.

12. **Wikipedia.** https://www.wikipedia.org/.