GSM Security Process: its Operating and Weaknesses allowing Interception

Cécile Duthoit
Department of Electrical Engineering, Faculty of Engineering
University of Indonesia
Depok, Indonesia
&
Department of Networks and Telecommunications
INSA Toulouse
Toulouse, France
E-mail: duthoit@etud.insa-toulouse.fr

***Abstract*— GSM is a second-generation mobile standard standardized by ETSI (European Telecommunications Standards Institute) in the 80s. Since the beginning of its deployment in the early 90, the number of compatible mobile devices has been increasing. In 2011, more than 6 billion mobile connections are identified worldwide.**

The GSM network has long remained immune to intrusions, especially because of the high cost of interception equipment. However, due to the democratization of technological software and hardware tools, this financial barrier is no longer, making exploitable flaws in the GSM system.

Considering the popularity of this medium and the number of vulnerable users, it seemed necessary to focus on the technical interception and ways to implement them.

This paper aims to make a review of the GSM system and network, its objectives, its implementation, its evolutions and its weaknesses, the potential solutions to improve its security system, and presents the operating and role of interception in that context.

Keywords— GSM, security, weaknesses, interception.

I. Introduction

GSM is a second-generation mobile standard standardized by ETSI (European Telecommunications Standards Institute) in the 80s. Since the beginning of its deployment in the early 90, the number of compatible mobile devices has been increasing. In 2011, more than 6 billion mobile connections are identified worldwide.

The GSM network has long remained immune to intrusions, especially because of the high cost of interception equipment. However, due to the democratization of technological software and hardware tools, this financial barrier is no longer, making exploitable flaws in the GSM system.

Considering the popularity of this medium and the number of vulnerable users, it seemed necessary to focus on the technical interception and ways to implement them. The role of this paper is to make a review of the GSM system and network, its objectives, its implementation, its evolutions and its weaknesses, the potential solutions to improve its security system, and presents the operating and role of interception in that context.

First we will look at the GSM standard and present it. Then we will analyze its security system to further identify and understand his weaknesses. Finally we will study the different types of interceptions and conclude about the current state of the GSM security system.

II. Related Works

Wilayat Khan and Habib Ullah, in their paper titled “Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography”[9], describe, explain and analyze the processes of authentication and encryption of the GSM network. Indeed, mobile communication and especially 2G has been facing many security problems. With its three nodes-architecture, encryption and decryption is managed by the mobile station (MS), Visitor Location Register (VLR), and Home Location Register or Authentication Center (HLR/AuC). Since the GSM encryption mechanism has been moved from symmetric cryptography to asymmetric cryptography, in order to provide security services like authentication and secure communication, they analyze these both mechanisms and propose a new generalized approach of encryption, based on asymmetric cryptography for user and network authentication and communication encryption in GSM. Indeed, the public key cryptographic approaches are very secure but they are computationally extensive as well as have more signaling overhead, and do not provide integrity of the initial authentication messages and authentication of the network. The enhanced model they propose is based on the public key cryptography, using the real benefits of public key encryption, but with fewer signals reducing the signaling overhead and by nuancing its computational extensiveness.

Luka Perkov, Ana Klisura, and Nikola Pavkovic, in their paper titled "Recent advances in GSM insecurities"[16], discuss the privacy and the different threats such as interception and theft of service which are raising significant interest in GSM community. They expose the issues in both GSM standard and implementations and evoke the popularization of available hardware and software capable of various attacks on GSM networks. They give a theoretical overview of the GSM network architecture, and describe different attack vectors, as well as both hardware and software tools available.

Francisco J. González-Castaño, Javier Vales-Alonso, José M. Pousada-Carballo, Fernando Isasi de Vicente, and Manuel J. Fernández-Iglesias, in their paper titled "Real-Time Interception Systems for the GSM Protocol"[14], present the concept of interception, its operating in GSM systems, its application and threats. A GSM protocol interceptor is a device located in a closed area that listens to information exchanged between base stations and mobile stations. They present three new interception systems for security purposes: detectors, to force all idle Mobile Stations nearby to generate activity; selective interceptors to exchange between Mobile Stations and Base Stations; and enhanced selective interceptors to combine the previous two systems and therefore improve blocking performance. They also present real tests and simulations they made in order to demonstrate the feasibility of the systems.

III. What is GSM

a. Overview of the GSM system

Global System for Mobile Communications (GSM) is the most widely used cellular standard, designed in 1982, and developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile phones. It has been first deployed in Finland in July 1991.

Figure 3.1: GSM Standard logo[6]

It has become the default global standard for mobile communications thanks to over 90% market share and its use by over 2 billion people across more than 212 countries. Most of the users are located in Europe and Asia because of the limited coverage and support in USA.

b. Evolution of the mobile communications

From its beginning, mobile communications have known many evolutions. We can usually consider that one new generation of mobile communications appears about each decade. 2G networks have been developed in the beginning of the 90s, as a replacement for first generation (1G) analog cellular networks, developed in the early 80s. Those 2G networks, more commonly known as GSM, use a standard that originally described a digital, circuit-switched network optimized for full duplex voice telephony. That digital network marked the beginning of the SMS (Short Message Service).

It has been extended later in the 90s to include data communications, first by circuit-switched transport, then by packet data transport via GPRS (General Packet Radio Services), known as the 2.5G, and EDGE (Enhanced Data rates for GSM Evolution or EGPRS), known as the 2.75G. These evolutions allowed to get a better data rate (from up to 9.05Kb/s for the first 2G to a theoretical data rate of 384Kb/s for the 2.75G). The 2.5G also marked the beginning of the MMS (Multimedia Messaging Service).

At the beginning of the 2000s, the third generation (3G) cellular networks has been developed. It is also known as the Universal Mobile Telecommunications System (UMTS) and is a system for networks based on the GSM standard. It has been developed and is maintained by the 3GPP (3rd Generation Partnership Project). Later, it evolved to the 3.5G or 3G+, using the HSDPA (High-Speed Downlink Packet Access) or HSUPA (High-Speed Uplink Packet Access) standards and the 3.75G with HSPA+ (Evolved High-Speed Packet Access) and DC-HSPA+ (Dual Carrier/Channel High-Speed Packet Access) standards to reach data rates up to 42 Mb/s. This last evolution announced the 4G.

Around 2010, the 3.9G has been developed, also known as Long Term Evolution (LTE), with theoretical data rates of 300 Mb/s. It is commercially called 4G, although it does not respect all the technical specifications decided for the 4G.

Nowadays, the 4G LTE Advanced, which is the second generation of 4G LTE, and correspond to the real announced 4G, is being developed, with announced theoretical data rates of about 1Gb/s.

c. *GSM network architecture and protocols*

GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate area. A cell is a part of a base station, and several base stations form the cellular network.

A typical GSM network contains Base Stations, a Base Station Concentrator, various databases (MSC, VLR, etc.), switches and terminals. Those part of the GSM network are presented in figure 2.1.

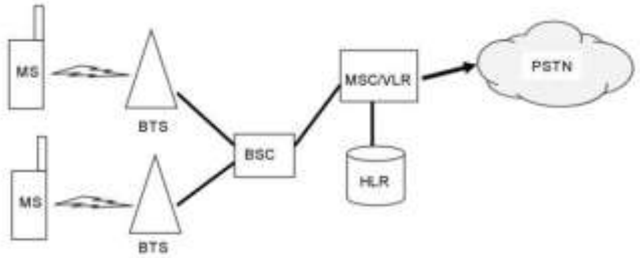

Figure 3.2: Key elements of a GSM network[5]

The Mobile System (MS) includes the Mobile Equipment (ME) and a Subscriber Identity Module (SIM), which contains the subscriber International Mobile Subscriber Identity (IMSI), to carry various kind of information such as the area code, the country code, the identity, ect..

The Base Transceiver Station (BTS), which is basically a radio receiver, handles functions related to radio access between the mobile phone and the BTS. Each BTS covers a cell, which is a radio access area. We usually use the term of “site” to mention a group of BTSs.

The Base Station Controller (BSC) offloads the MSC of radio-related items, such as radio call setup, administration of channels, and handover (roaming) between cells (BTS coverage).

The Mobile Switching Center (MSC) is the actual traffic or call route switch and performs the switching between the 64-kbps channels. The MSC is also responsible for monitoring and registering calls.

The Visitor Location Register (VLR) is a database located in the MSC to maintain a list of the subscribers for those mobile phones that currently exist within the MSC coverage area.

The Home Location Register (HLR) is the main database that maintains a list of each GSM operator’s subscribers. The HLR performs several functions related to maintaining and administering mobile services and is supported by other databases.

Various different signal protocols are used to transfer the information between the key elements of the network. It includes Signaling System No. 7 (SS7), which is a set of telephony signaling protocols developed in 1975, used to set up and tear down most of the world's Public Switched Telephone Network (PSTN) telephone calls.

d. GSM frequency bands

The GSM standard defines GSM frequency bands and frequencies for the different spectrum allocations that are in use around the globe. The air interface usually works on 4 standardized main frequency bands but for some specialist applications, or in countries where spectrum allocation requirements mean that the standard bands cannot be used, different allocations may be required.

There is a total of fourteen different recognized GSM frequency bands, from 380 MHz to 1900 MHz. These are defined in 3GPP TS 45.005. The choice of which bands are used depend upon the regulatory requirements for the country and the ITU (International Telecommunications Union) region in which the country is located. For example, Europe, Middle East, Africa, Asia and Oceania tend to use the GSM 900 and 1800 bands as standard and the USA use both 850 and 1900 MHz bands.

That is the reason why today most phones support operation on multiple bands and are known as multi-band phones (typically most standard phones are dual-band phones). This evolution allow users to keep their mobile phone when they are travelling for instance. Incidentally, foreigners who were going to Japan in the last 90s had to rent mobile phone to be able to communicate because the GSM standards were different from Europe or South-East Asia.

e. GSM modulation

GSM differs from first generation (1G) wireless systems –which used only FDMA- in that it uses a combination of Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) as the method to divide the bandwidth among the users. In this process, the FDMA part divides the frequency of the total 25 MHz bandwidth into 124 carrier frequencies of 200 kHz bandwidth and the TDMA part divides each 200kHz channel into eight 25kHz time-slots.

f. Range of the GSM signal

The range of the wireless signal is usually limited to 35km, with 70 km being possible with special equipment.

IV. GSM Security System

a. GSM security system overview

The GSM network has long remained immune to intrusions, especially because of the high cost of interception equipment. However, due to the democratization of technological software and hardware tools, this financial barrier is no longer, making exploitable flaws in the GSM system. The use of wireless transmission for mobile communications makes GSM Public Land Mobile Networks (PLMN) more sensitive to any kind of attacks. Indeed, the attackers does not need to find the wire medium to interfere with the network. Furthermore, considering the popularity of this medium and the number of vulnerable users, it may be an interesting target for potential attackers. That is why security is extremely important in GSM system. The security features in GSM PLMN are implemented to protect both the access to the mobile services for its users and any relevant item from being disclosed at the radio path, to ensure the privacy of user-related information.

In order to ensure users privacy, various functions were built into the GSM security system. First, authentication is absolutely needed to access the network. Then, all the data is encrypted before transmission. The identity of the users is also protected. A SIM is needed to access the network and it is not allowed to duplicate a SIM. Those security features are described and explained below.

b. Authentication of the users on the GSM network

International Mobile Subscriber Identity (IMSI) authentication has been built in order to protect the network against unauthorized use. It protects the GSM PLMN subscribers of any intrusion on the GSM network by unauthorized users. It uses the A3 algorithm to authenticate the user, as explained below. In the next part about data encryption, the A8 algorithm, which is based on the same paradigm will be explained.

There are several steps in that authentication procedure.

First, the mobile station sends its identity using IMSI to the GSM network. When the network receives it, it has to find the correspondent KI of that identity. Ki is the 128-bit Individual Subscriber Authentication Key utilized as a secret key shared between the Mobile Station and the Home Location Register of the subscriber's home network.

Then, the network generates a 128 bit random number (RAND) and sends it to the Mobile Station (MS) over the air interface. That RAND number is generated by the Home Location Register.

The MS then calculates a SRES with the A3 algorithm using the given challenge (RAND) and the KI residing in the SIM. That SRES is the 32-bit Signed Response generated by the Mobile Station and the Mobile Services Switching Center.

At the same time, the network calculates the SRES using the same algorithm and the same inputs. When the MS sends the SRES to the network, the network tests its validity by comparing with the one it calculated.

IMSI authentication is based on a shared secret KI between the subscriber's home network's and its SIM. This KI is generated and written in the SIM card at a safe place when the SIM card is personalized, and a copy of the key is put to the HLR. That system is based on the theory of public and private key. The secret KI can be associated to the secret key, whereas the RAND number can be compared to the public key. Then, we get the parallel between the encrypted message and the SRES which are both encrypted or calculated using the public key or both public and private keys.

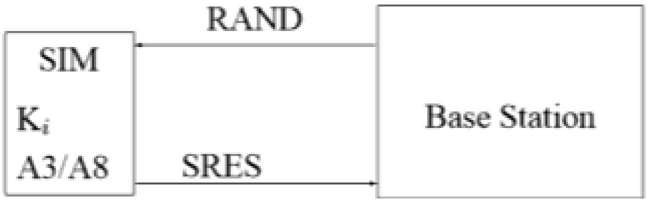

Figure 4.1: IMSI authentication[8]

The problem that can be emphasized is that if the user's identity is always sent before accessing the network, this IMSI may be gotten by someone who is eavesdropping. To answer this issue, a system of temporary identity has been developed. When a user buy a new SIM card and turns on his phone for the first time, its IMSI is transmitted to the Authentication Center (AuC) on the network. But after that first identification, a Temporary Mobile Subscriber Identity (TMSI) will be assigned to the subscriber and the true IMSI will be rarely transmitted, except for extreme necessity. The TMSI is saved with the IMSI in the network.

The MS will continue to use that temporary identity, which will be update by the Visitor Location Register (VLR) each time the user changes his/her location for example. The TMSI will also be stored on the SIM card when the MS is switched off, to be sure of its availability for the next time it will be switched on.

All this process consists in the A3 algorithm process.

c. Encryption of the data

To ensure the protection of the data sent and received by the subscribers, these data need to be encrypted. Then, it can only be decrypted by the receiver and the privacy of the communication is respected.

The GSM system uses a ciphering key to protect both user data and signal from potential attacks that could occur due to the vulnerability of the air interface. After IMSI authentication steps as explained above, both RAND number and KI are sent through the A8 ciphering key generating algorithm, in order to produce a ciphering key (KC).

This A8 algorithm is stored on the SIM card. The KC created by the A8 algorithm, is then used with the A5 ciphering algorithm to encipher or decipher the data.

Those algorithms form the COMP128 algorithm, whose design is completely private. It is used by almost all the GSM operators for both authentication and generation of KC (using respectively A3 and A8 algorithms).

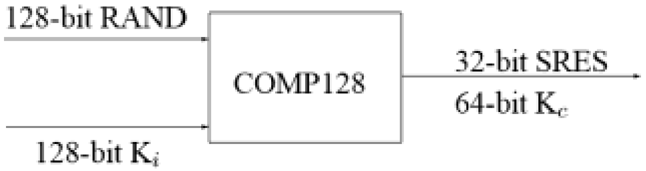

Figure 4.2: COMP128 algorithm schema[8]

The encrypted communication is initiated by a ciphering mode request command from the GSM network. When the MS receives this command, the A5 algorithm, which is implemented in the hardware of the mobile phone, is initialized using both KC and number of frames to be encrypted. Then, each frame will be encrypted by using a different key-stream. The encryption is done by mobile because SIM does not have enough power and processing capacity. The same KC is used as long as the MSC does not authenticate the MS again. If a new authentication is needed, for example because the user changed his/her location, a new KC will be generated. In practice, if there is no main change in the MS state, the same KC may be in use for days.

The whole authentication system is schematized on figure 4.3.

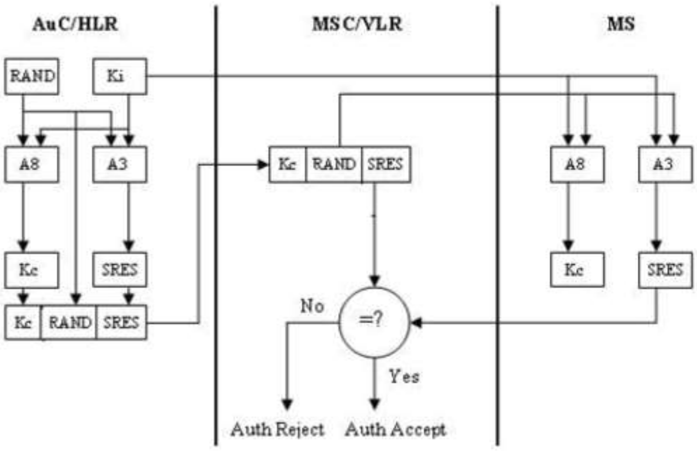

Figure 4.3: The GSM authentication architecture[9]

V. GSM Security Problems

a. Weaknesses of the GSM security system

There are several weaknesses in the GSM system that could be used by attackers.

First, the security of the algorithms used by the GSM communication system is based on the concept of security by obscurity. That means that, in order to protect it, the code is kept secret and inaccessible to anyone who is not allowed to access it. This concept is not the most secure since once the hidden data is discovered, the security system is down.

Another point is that the GSM system only provides access security. All communication between the Mobile Station (MS) and the Base Transceiver Station (BTS) are encrypted, but all communications and signaling is generally transmitted in plain text in the fixed network. That means that only the air part of a GSM communication is encrypted and the signal is decrypted at the BS and then transmitted in clear text across the network. If someone manages to eavesdrop the wire network, there will be no need to decrypt it since it will be in plain text.

One of the most dangerous weaknesses is that only the mobile authenticates itself to the network. The Base Station (BS) can easily be imitated and it will be difficult for the MS to differentiate the true BS from the false one. An attacker may impersonate a BS and explicitly demand mobiles to send their IMSIs. Then the privacy and anonymity of the user is no longer maintained.

There are also some flaws in the algorithms, such as the one discovered in the COMP128 by the Smartcard Developer Association (SDA) and the ISAAC security research group. That flaw enabled them to retrieve the secret key, KI, from a SIM card. Indeed, the COMP128 algorithm is broken in such a way that it reveals information about the KI when the appropriate RANDs are given as arguments to the A8 algorithm. Retrieving the key (KI) from the SIM card is considered as the most dangerous attack.

The estimated level of security in the GSM system is extremely different depending on the area or the country we are considering. Figure 4.4 is a GSM Security Map which compares the protection capabilities of mobile networks around the world. Networks are rated in their protection capabilities relative to a reference network that implements all protection measures that can be implemented. This reference is regularly updated to reflect new protection ideas becoming commercially available.

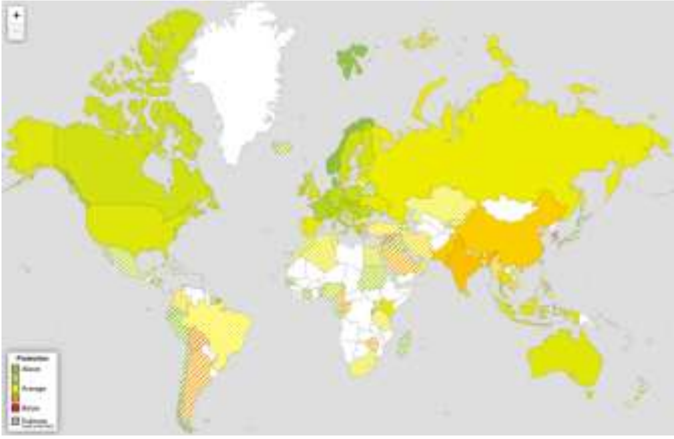

Figure 4.4: GSM Security Map[12]

According to this map, most of the countries which present certified data are from North America, Europe and Asia. Among those countries, only a few North European countries such as Norway or Denmark as considered as having a high protection system.

b. Different types of possible attacks

There are several types of possible attacks. We can distinguish four main types.

The eavesdropping is when the attackers are able to intercept the signaling and user’s data. In that case, they can listen the communication, but if the data are encrypted they will not be able to read it (unless if they manage to decrypt it).

The usurpation of the user’s identity is a process in which the attackers are able to send signaling or user’s data to the GSM network, by pretending they come from the user’s MS.

The usurpation of the network’s identity is the exact contrary: sending data to the user by pretending they come from the network.

The man-in-the-middle process is when the attackers place them between the MS and the network and are able to listen, modify, delete, and resend signaling or user’s data between the two entities.

c. Some solutions and possible improvements

In order to improve the security of the algorithms used in the GSM system, some evolutions have been implemented. For example, a new security algorithm, known as A5/3, has been developed by a joint working party between the GSM Association Security Group and the 3rd Generation Partnership Project (3GPP), to provide users of GSM mobile phones a higher level of protection against eavesdropping. This A5/3 algorithm is based on the Kasumi algorithm, specified by 3GPP for use in 3rd generation mobile systems as the core of confidentiality and integrity algorithms. This solution propose to use another cryptographically secure algorithm for A3, such as A5/3 or COMP128-2. New SIM-cards for all subscribers and an updated HLR software would be required, but it would not be extremely difficult to instore since it could be the role of the operators to make the changes for their own subscribers. This solution would disable the possibility of cloning SIM-cards, which is considered as the most dangerous attack.

Another way to improve data security would be to encrypt the traffic on the operator's backbone network between the network components. Indeed, as we saw above, only the wireless communication is encrypted. Encrypting the data sent across the fixed network would disable the attackers from wiretapping the backbone network. The implementation of that solution would also need the co-operation of the hardware manufacturers.

Obviously, the security processes must not have bad efficiency consequences, such as adding more delay, increasing the bandwidth of the channel, increasing error rates or error propagation, adding excessive complexity to the rest of the system, or being too expensive. This is the challenge of security processes: balancing between the cost (financial costs and costs of efficiency) and the highest level of security that can be implemented.

VI. GSM Interception

a. Indiscriminate jamming

In some cases, jamming can be used as a security measure to fight malicious transmissions. It happened in Spain during the late 1990s for example, when temporary indiscriminate frequency jamming has been a successful security measure against malicious transmissions which used general-purpose bands. Unfortunately, indiscriminate jamming of GSM networks is not a solution, because it may cause severe problems in urban areas. Interception may be a solution to these problems, since it can allow us to be selective in jamming targets.

b. Three types of interceptors

A GSM protocol interceptor is a device located in a closed area that listens to information exchanged between base stations (BS) and mobile stations (MS). There as several ways to implement GSM interception. Three of them will be presented below.

The first one is called "detector". It makes all idle MS nearby generate activity. This technique can be used to detect the presence of MS in a certain radius for example.

The second one is called "selective interceptor". It monitors information exchange between MS and BS (while the MS is active). It extracts messages containing MS identifiers and checks identifiers in a local cache to decide if an external jamming unit should block individual calls (either incoming or outgoing).

The third system is called "enhanced selective interceptor". It combines the previous two systems to improve blocking performance.

c. Detectors

The operating of detectors is quite simple. First, a jamming device has to block all downlink signaling carriers. Then the detector offers a signaling pseudo carrier, whose broadcast control channel (BCCH) carries a location area identifier (LAI) different from those in the jammed signaling carriers. The BCCH (Broadcast Control CHannel) carries a repeating pattern of system information messages that describe the identity, configuration and available features of the base transceiver station (BTS). The LAI (Location Area Identity) is a code transmitted on the BCCH by a BTS, to indicate which area it belongs to. This identifier is stored in the SIM card and is updated each time the location changes. Each location area of a public land mobile network (PLMN) has its own unique: the LAI. It is an internationally unique identifier.

When an idle MS enters the influence area of the jamming unit, it loses contact with the active carrier of its current BS. After MS downlink signaling failure counter (DSC) expires, which takes a time, the MS considers a failure has taken place.

Therefore the MS is going to search for an alternative carrier and will only be able to find the pseudo carrier we propose. The MS will synchronize with our pseudo carrier and read its BCCH data. Because of the different LAI, the MS will have to proceed to its identification again. This process will show the presence of that MS and can be used to detect the presence of all the MS in a certain range.

d. Selective Interceptor

The selective interceptor monitors GSM protocol exchange between BS and MS. When the interceptor obtains MS identifiers, there are two different possible scenarii depending on how the identification has proceeded.

The first one is called "Remote Identity Check and Blocking". With this scenario, the MSC and the interceptor must be linked in a metropolitan-area network (MAN) because this method requires a continue communication between the MSC and the interceptor. A fast and reliable connection is also necessary to implement a real-time blocking, which makes this method difficult to execute. When MS identifiers are transmitted to the corresponding mobile switching center (MSC), it informs the MSC of the presence of the MS in the monitored target area. Then the MSC can block its activity during a period of time.

The second possibility is called "Local Identity Check and Blocking". In this scenario, a local jamming device generates interferences that affect active carriers and blocks MS activity. Communication between the MSC and the interceptor is also required but the continuity of the connection is not important. The interceptor obtains MS identifiers and checks them in a local identity repository (accessed through the MSC). Therefore, selective interception allows to block only some chosen MS, by checking their identifiers.

e. Enhanced Selective Interceptor

The enhanced selective interceptor combines both detector and selective interceptor features. It forces the MS to proceed to its self-identification in order to captures its identity.

VII. Conclusions

GSM is the mobile communication standard used in the second generation of mobile technologies (2G), first developed in the 80s but still daily used nowadays since it provides very good vocal transmissions for phone calls. Since its beginning, the number of compatible mobile devices has been increasing, with more than 6 billion mobile connections identified in 2011. However, its security system is not extremely satisfying, because of issues in both GSM standard and implementations. The security processes it provides cannot entirely ensure anonymity and confidentiality to its users, and in the same time, the democratization of technological software and hardware tools makes attacks even easier. Interceptions are becoming more and more accessible to anyone, particularly with the high number of tutorials on the Internet and the costs of hardware becoming lower and lower.

Many studies about GSM security are made, and I think its security system can be highly improved, thanks to the huge progresses we make in the fields of telecommunications and computer science. Because of its use worldwide, we should not just let the GSM standard in its current state to only focus on the next mobile generations. The half encryption, only for the wireless part of the GSM network, should for example be extended to the full network. Although many improvements have already been done, such as the extension of the size of the cypher-key, from 64bits at the beginning to 128bits, the encryption and more generally the security process can still be improved. Obviously, encryption, authentication, and all security processes which are extended consume more bandwidth and minimize the capacity. But I suppose that the higher and higher data rates we manage to achieve with all the technical progresses we make will allow to use better encryption (with more and more secure keys for example) among the whole network.

References

[1] Ian Poole, "GSM Frequencies and Frequency Bands", Radio-Electronics.com. http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/gsm-frequency-frequencies-bands-allocations.php (accessed on 12/12/2015)

[2] GSMA official website. http://www.gsma.com/aboutus/gsm-technology/gsm (accessed on 12/12/2015)

[3] University of Colorado, “GSM Tutorial”, Electrical, Computer and Energy Engineering. http://ecee.colorado.edu/~ecen4242/gsm/index.htm (accessed on 12/12/2015)

[4] Tutorials Points, “GSM –Specifications”. http://www.tutorialspoint.com/gsm/gsm_specification.htm (accessed on 12/12/2015)

[5] What-When-How, In Depth Tutorials and Information,“Case Study IP RAN and Mobile Backhaul QOS Part 1”. http://what-when-how.com/qos-enabled-networks/case-study-ip-ran-and-mobile-backhaul-qos-part-1/ (accessed on 12/12/2015)

[6] Official Website of Satpro Company. http://www.satpro.org/ (accessed on 12/12/2015)

[7] GSM Security. “What Are Ki, Kc, RAND, and SRES?”. http://www.gsm-security.net/faq/gsm-ki-kc-rand-sres.shtml (accessed on 12/13/2015)

[8] Billy Brumley, “A3/A8 &COMP128”, Special Course on Cryptology” www.tcs.hut.fi/Studies/T-79.514/slides/S5.**Brumley**-comp128.pdf (accessed on 12/13/2015)

[9] Wilayat Khan and Habib Ullah, “Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography”, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 9, May 2010 ISSN

[10] David Margrave, “GSM Security and Encryption”, George Mason University. https://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html (accessed on 12/13/2015)

[11] “The GSM Security Technical Whitepaper for 2002”, January the 10th, 2002. https://www.hackcanada.com/blackcrawl/cell/gsm/gsm_security.html (accessed on 12/13/2015)

[12] GSM World Map project website. https://gsmmap.org/#!/ (accessed on 12/13/2015)

[13] Yubo Song, Kan Zhou and Xi Chen,“Fake BTS Attacks of GSM System on Software Radio Platform”, JOURNAL OF NETWORKS, VOL. 7, NO. 2, FEBRUARY 2012

[14] Francisco J. González-Castaño, Javier Vales-Alonso, José M. Pousada-Carballo, Fernando Isasi de Vicente, and Manuel J. Fernández-Iglesias, “Real-Time Interception Systems for the GSM Protocol”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 51, NO. 5, SEPTEMBER 2002

[15] Kan Zhou, Aiqun Hu, Yubo Song, “A No-jamming Selective Interception System of the GSM Terminals”, Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference

[16] Luka Perkov, Ana Klisura, Nikola Pavkovic, “Recent advances in GSM insecurities”, MIPRO 2011, May 23-27, 2011, Opatija, Croatia