Actas de XIV Jornadas de ARCA
Sistemas Cualitativos y sus Aplicaciones en
Diagnosis, Robótica e Inteligencia Ambiental
F. J. Ruiz, N. Agell, J. A. Ortega (Eds.)

Wireless location: A survey about GSM in location techniques

Ismael Cuadrado Cordero, Luis Miguel Soria Morillo, Pedro Gallego Torrecilla, Juan Antonio Ortega Ramírez
{icuadrado@cica.es, lsoria@us.es, kafka.g@gmail.com, jortega@us.es}
University of Seville
Computer Languages and Systems Dept.,
41012, Seville, Spain

Abstract

Security has become one of the most important features in modern computation, especially due to the point of view of the user. Security issues (like privacy or secure use of the application) will be taken into account during the evaluation of the system by the final user. Also, it is an important issue for the developer, due to the reason that the developer should be sure about the correct performance of the system. The purpose of this paper is to offer a deep survey on existent attacks to GSM location adapting them from common GSM attacks to location attacks.

1 Introduction

Location is a much studied field, and has become popular due to the appearance of new location techniques and algorithms. Nowadays, the user can be accurately located without overly effort or energy consumption. Thanks to the popularity GSM technologies and the low resources requirements, this technology has experienced a boom of users and researchers in the last years.

GSM is a standard set developed in order to describe all technologies for second generation digital cellular networks and can be used in order to locate a device capable of use a GSM network. In the beginning, this type of location could only be accomplished using a computer connected to Internet and a contract with a mobile operator enterprise (in order to obtain data).

The main advantage of GSM location is its popularity. Due to the fact that is only needed a mobile phone it has been rapidly extended. However, without the help of the network or the help of other kind of location (such as WiFi) it has a low accuracy (Error of over 300 meters).

From the GSM cell can extracted different information that can be used in order to calculate the position of the target.

Thanks to the appearance of new generation mobile phones and the ease to install services, competences between applications have been increased. Also, it is not usual in users to take care about security issues, until the moment of a break in security. Then, the user could ask for responsibilities to the owner of the service. Therefore, it is necessary to establish a set of basic security standards, in order to protect both the user and the developer.

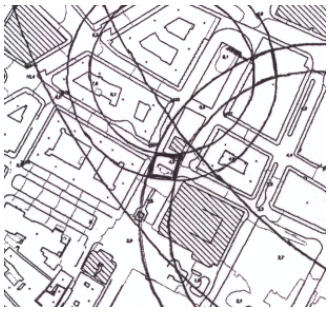


Figure 1: Location

Nowadays, there is not a deep survey about GSM location systems which could be complete enough about those threats on GSM location systems. Furthermore, the current surveys on GSM (not location but GSM methods) are not youth enough.

2 GSM Network

Cell phones connect to the network by searching for “cells” in the immediate vicinity. A “cell” is defined as the coverage area provided for an antenna. Same antenna can include from 1 to 3 different cells.

Cell radius varies depending on antenna height, gain and propagation conditions from a couple of hundred meters to several tens of kilometers. In practical use, the longest distance the GSM specification supports is 35 kilometers (22 mi). But a cell can be detected even from hundred of meters.

The GSM network includes the following elements:

• *Mobile Station (**MS):*** A Mobile Station is a mobile device capable to communicate with the cell. That means a mobile device with a SIM card.

• *Base Transceiver Station (**BTS):*** Is the part of the Base Station Subsystem in charge of communications. It is integrated with the antenna.

• *Mobile Switching Center (**MSC):*** Is the part of the Base Station Subsystem in charge of management and growth of a wireless telecommunications network. It is integrated into a circuit switching platform, in the antenna.

• *Visitor Location Register (**VLR):*** Is a database that contains information about the subscribers roaming within on the area. It has information about devices temporary connected to the cell.

• *Home Location Register (**HLR):*** Is the main database of permanent subscriber information for a mobile network. It has information about devices permanently connected to the antenna.

• *Authentication Center (**AuC):*** It validates any security information management (SIM) card attempting network connection when a device has a live network signal.

• *Base Station Controller (**BSC):*** Is an automatic coordinator (controller) that permits one or more Base Transceiver Stations (BTS) to communicate with a mobile switching center.

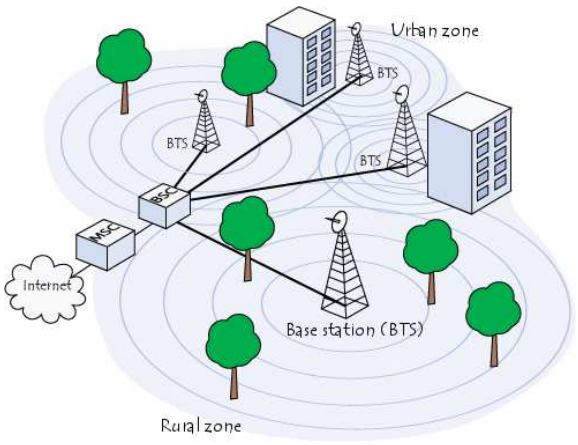
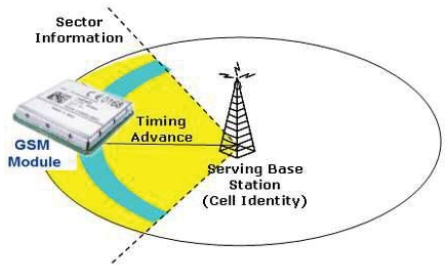


Figure 2: GSM network

3 GSM Location

Of those elements, the main two components are mobile stations (i.e., mobile terminals) and so-called base stations, which communicate with mobile terminals directly. Each of these base stations is associated with various "cells". A cell is a sector that is covered by the base station. Each terminal that is connected to a cell has an associated frequency, the way that two terminals never have the same frequency at the same time. So, the mobile terminals are informed of the cells that are near and which receive signal, as they will have to partner with one of these cells.



From the GSM cell can extracted different information that can be used in order to calculate the position of the target.

• The identification of the source cell, which is composed of:

• *Mobile country code (MCC**):*** A number that indicates which country the cell belongs to.

• *Mobile network code (**MNC):*** A number indicating what network the cell belongs to.

• *Location Area Code (**LAC):*** A number that indicates which area the cell belongs to.

• *Cell Identification (**Cell ID):*** A number that uniquely identifies the cell within its area. On this number, the first digit indicates whether it is directional or omnidirectional. Is 0 if it is omnidirectional or 1 if not.

• Temporal parameters involved in the communication:

• *Timing advance (**TA):*** Parameters related to the time it takes to communicate with the base station terminal. This time is necessary in order to establish the correct synchronization between them.

- *Time of Arrival (**TOA):*** Time it takes for a signal to travel from the base station to terminal or vice versa. Is measured by the base stations.

- *Time Difference Of Arrival (**TDOA):*** TOA difference between the terminal and one or most of other base stations.

- *Enhanced Observed Time Difference (E**-OTD):*** Similar to the TDOA but in this case the times are measured by the mobile terminal.

- *Round**-Trip-Time-of-Flight (RToF):*** Time it takes the signal to go from the base station to terminal and back.

- *Angle of arrival of the signal.*

- *Angle of Arrival (AOA**):*** The angle with which comes the signal from the base station to terminal.

- *Intensity of the incoming signal.*

Currently it is very difficult to get most of the parameters described above, requiring the collaboration of the owner of the mobile network or the inclusion in the mobile device of some special hardware.

The parameters that can be obtained more easily (and are most of times used) are:

- The identification of GSM cells nearby the terminal. This information can be usually obtained from up to 80 or 100 different cells.

- The power of the signal arrival of each of those cells.

Using an appropriate mathematical and statistical treatment over the retrieved data, it is possible to get a higher accuracy. Depending on the technique used, which also depend on the hardware, it can get more or less precisely.

According to these parameters, a usual mobile device can get:

- *Cell Of Origin (COO):* 100m-35km

- *COO with CS and Received Signal Strength:* 100m - 20 km

- *Timing Advance (TA):* 550 m

- *Round-Trip-Time-of-Flight (RToF):* 50m-150m

- *Time Difference Of Arrival (TDOA):* 50m - 150m

- *Enhanced Observed Time Difference (EOTD):* 50m - 150m

Angle Of Arrival (AOA): 50m-150m

4 GSM Communication

The process of connection with a network can be described as follows:

1. The Mobile Station obtains the IMSI (International Mobile Subscriber Identity, which is unique, with at most 15 digits uniquely devoted to every mobile subscriber in the world) from the SIM card (subscriber identity module or subscriber identification module, which is an integrated circuit designed in order to securely store), and sends a message to the mobile operator with this number requesting access and authentication.

2. The operator network searches its database for the incoming IMSI and its associated K_i (a 128-bit value used during the authentication of the SIM on the network. Each SIM holds a unique K_i assigned to it by the operator during the personalization process. The K_i is also stored in the Authorization database (AuC). During the process of authentication, the SIM card provides a function, *Run GSM Algorithm*, that allows the phone to pass data to the SIM card to be signed with the K_i).

3. The network then generates a Random Number and signs it with the K_i associated with the IMSI, computing another number known as Signed Response 1 (SRES_1) and send the random number to the Mobile Station, which passes this information to the SIM card. This way, the network is protecting the K_i from observers.

4. The SIM card signs it with its K_i, producing SRES_2, which it gives to the Mobile Station along with encryption key K_c. The Mobile Equipment passes SRES_2 on to the network.

5. The network then compares its computed SRES_1 with the computed SRES_2 of the Mobile Station. If the two numbers match, the SIM is authenticated and the Mobile Equipment is granted access to the network of the operator.

K_c is used to encrypt all further communications between the Mobile Equipment and the network. In figure 1, there is described the process of generation the code.

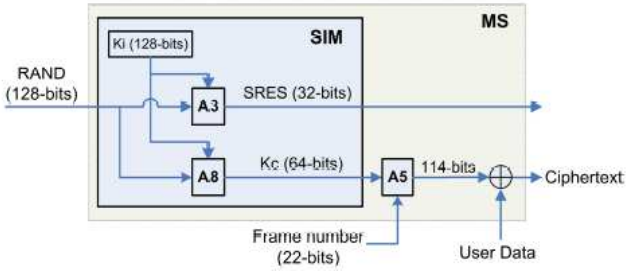


Figure 4: Codification of Ki

6. After user authentication, the network can order the phone to start the encryption by using the generated session key Kc. The cryptographic algorithms are implemented on the hardware of mobile phones. The network can choose from up to 7 different encryption algorithms (or the mode of no ciphering) but it should choose an algorithm that is implemented on the phones. A classmark message has been earlier specified the phone's capabilities to the network. 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 CEPT. A5/2 is deliberately weakened to be deployed by the other countries. The use of such algorithms is controlled by the GSM *Memorandum of Understanding* (MoU). A5/3 is a block cipher based on the Kasumi algorithm that is defined by the 3GPP at 2002 and can be supported on dual-mode phones that are capable of working on both 2G and 3G systems.

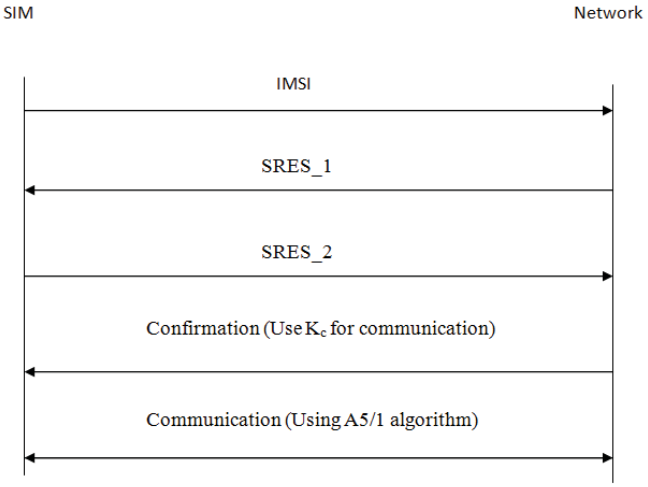


Figure 5: GSM communication

4.1 GSM included security mechanisms

GSM incorporates some security mechanisms on its standard, which must be implemented both for the providers and the clients. These security mechanisms protect the privacy of the customer and the network, not allowing the authentication on the network to third parties and encrypting the calls while they travel over the air.

These security mechanisms are separated on three different encryption methods. The first (and most important one) is A5, which encrypts the information over a stream cipher method. The two other methods are A3 and A8 which are used as authentication algorithm and key agreement respectively. These two last methods were not standardized in the GSM specifications.

4.2 Ciphers

The GSM communications are encrypted using a family of algorithms collectively called A5. Ordered, there are 4 different kind of algorithms used during communication, each one is known by a number. The first one is A5/0, which uses a communication with no encryption. Then, A5/1 is the mostly common used cipher method in Europe and the United States. A5/2 is the "exported" version of the A5/1 algorithm. This algorithm was a deliberate weakening of the initial one for certain export regions. The A5/3 is a new algorithm based on the UMTS/WCDMA algorithm Kasumi

All of these algorithms are based on the same 64-bit key derived mechanism. A5/1 and A5/2 has been deeply cracked, and A5/3 has not been developed anywhere yet.

5 Existent surveys on GSM attacks

First approach to security on distributed location services and the considerations to take into account on this kind of systems was done by Leonhardt and Magee in 1997 [10]. In this paper, authors discuss about security requirements faced by a location service in different organizational contexts. They argue that fine-grained access control requires a symbolic location model over which access control is specified. They outline the salient features of a location service supporting such a location model. The two main security models, Lampson's access matrix and the security labels of Bell-LaPadula, are analyzed focusing on their application to location information. They argue that those schemes need to be generalized to deal with multiple targets in order to be applicable to location information. Based on the generalized models, they propose a concrete security model for location information which protects both personal and organizational privacy.

The importance of the work of Leonhardt and Magee could be hidden by its time. However, even if this paper is old, it offers an interesting and complete work in order to get a full overview about location problems associated to distributed location services. Many of the problems evaluated on this work are still relevant nowadays.

Like most of papers in the bibliography, Pesonen worked on 1999 in GSM security as a complete field [11]. It was not until some years after when researchers notice the need of separating different fields of action and research. At this paper, the author studies GSM standard security, showing some of the possible attacks. Following the author idea, an attacker can go through the security model or even around it, and attack other parts of a GSM network, instead of the actual phone call. Although the GSM standard was supposed to prevent phone cloning and over-the-air eavesdropping, both of these are possible with little additional work compared to the analog mobile phone systems and can be implemented through various attacks. One should not send anything confidential over a GSM network without additional encryption if the data is supposed to stay confidential. Even if this paper was written in 1999, which makes it a bit outdated, it is still interesting for the present work due to the reason that this paper is one of the reference papers for the security problems on GSM standard. Furthermore, as happened with the previous paper, many of the problems shown on this paper should be taken into account nowadays.

Since 2000, the fashion of GSM weaknesses turned into a fashion of encryption. From this year, many authors have focused in showing the weaknesses of the encryption algorithms. Biham and Dunkelman [12] performed one of the first and most known works on this field. They focused on A5/1 encryption of GSM communication. At this paper, authors describe an attack on cipher A5/1 with total work complexity 239.91 of A5/1 clockings, given 220.8 lines of known plaintext. With this work, authors proposed a very good solution, which was the best known result with respect to the total work complexity. This work, performed with the current technologies, could mean a not so big computation time and shows the biggest weak point of the GSM technology.

Ekdahl and Johansson continue with the same field of research, [13] 3 years later. In this paper, authors present a different attack on A5/1, based on ideas from correlation attacks. Whereas time-memory tradeoff attacks have a complexity which is exponential with the shift-register length, the complexity of the proposed attack is almost independent of the shift-register length. This attack breaks A5/1 in a few minutes using 2–5 min of conversation plaintext. Once again, with the current technology, this attack can be performed with few computation time and effort. Both papers show the weaknesses of A5/1, which could be the biggest point of access to the data of the user. Using this encryption for the communication, a potential attacker can obtains and decrypts the information associated to the location (which is send using the same standard) and breaks the privacy of the user. Threats associated to this kind of attack are evaluated on the next chapters.

Barkan et al. [14] worked on encrypted communications and possible attacks in GSM standard authors discuss about attacks based on Cyphertext-Only. Following the definition of the authors, "These attacks can even break into GSM networks that use 'unbreakable' ciphers". In this paper, authors described a ciphertext-only attack on A5/2. This attack requires a few dozen milliseconds of encrypted off-the-air cellular conversation and finds the correct key in less than a second on a usual personal computer. A potential attacker could obtain all the associated user information, which means a complete break on the privacy of the standard. However, A5/2 is not a very frequently used cipher for GSM communications. It is only used when it is necessary to decrease the information transmitted through the medium. The weaknesses of this encryption are known and public.

Because of this, authors extend afterwards the original attack to a (more complex) ciphertext-only attack on A5/1. They describe new attacks on the protocols of networks that use A5/1, A5/3, or even GPRS. These attacks are based on security flaws of the GSM protocols, and work whenever the mobile phone supports A5/2. They even show active attacks, such as call hijacking, altering of data messages and call theft. Once again, a potential attacker could gain access to the location information encrypted by this standard with not so much effort.

Information discussed in [14] was extended by the research provided the year after by Meyer and Wetzel [15]. This paper discuss the impact of GSM encryption attacks, that recover the encryption key, and the man-in-the-middle attack on the security of networks, which employ UMTS and GSM base stations simultaneously. Authors suggest protecting UMTS connections from GSM attacks by integrating an additional authentication and key agreement on intersystem handovers between GSM and UMTS. Authors show that it is possible to mount a man-in-the-middle attack in GSM during authentication which allows an attacker to make a victim mobile station authenticate itself to a fake base station which in turn forwards the authentication traffic to the real network, thus impersonating the victim mobile station to a real network and vice versa, which could be a very important problem due to privacy of the user.

More recently, in 2009, Nohl and Paget [16] surveyed most of the problems of GSM communications, using an example of broken the A5/1 cipher. The work is centered on ciphers used during communication, with a special attention on A5/1. After all works presented criticizing A5/1 encryption during more than 6 years, GSM standard has kept using the same cipher. Even after the existence of an enhanced version of this cipher (A5/3) most of GSM networks keep using the weak version. At this work, authors offer an interesting and complete work which shows how GSM can fail and how A5/1 is broken. The work performed by Nohl and Paget shows one more time the impropriety of using this kind of cryptography. Nowadays, it is still being used on most of the networks.

Finally, in 2012 Kune et al. [17] authors investigate techniques to test if a user is present in a small area, or absent from a large area by simply listening on the broadcast GSM channels. With a cheap and easy combination of readily available hardware and open source software, they demonstrate practical location test attacks that include circumventing the temporary identifier designed to protect the identity of the end user. Finally, they propose solutions that would improve the location privacy of users with low system impact.

6 GSM solutions

Many authors have proposed solutions to different GSM problems or attacks. Due to the novelty of the GSM location services and research, most of those solutions have been proposed to GSM communications, but the solutions shown on this section should be adapted to the goal of protecting GSM location. Most important solutions provided by authors are evaluated in this section.

In 2001, Pelecrinis et al. [18] wrote the first relevant paper evaluated due to GSM location. Authors show the threats of a denial of service attack in wireless networks. The risks of this kind of attacks are enhanced in wireless networks. According to the authors, “The shared nature of the medium in wireless networks makes it easy for an adversary to launch a Wireless Denial of Service (WDoS) attack”. The most common denial of service attack in wireless networks is provided by a malicious node transmitting a radio signal. This signal blocks any legitimate access to the network and/or interferes with the reception of the original signal. This kind of attack has been deeply investigated and is called jamming. Furthermore, the malicious nodes are referred to as jammers. Jamming includes a set of techniques, which vary from attacks based on the continual transmission of interference signals (simple attack, in the hand of the usual attacker), to more complicated attacks which try to explore vulnerabilities of the protocol. The risk associated to this last subset of attacks is not as high as the risk associated to the first one, because of the explicit need of knowledge of the specific protocol. Authors present a survey on the jamming attacks, and techniques proposed for detecting the presence of jammers. Furthermore, they offer some existent mechanisms in order to protect the network from this kind of attacks. Even if this survey is from 2001, most of techniques and attacks proposed on it are still up to date.

A year later, Alkassar and Stiible [5] introduce an identification scheme in order to solve the problem of mafia fraud in communications by hiding the conversation channel between the participants using Channel Hopping (CH) techniques. According to the definition of the authors, “Mafia fraud is a known problem in GSM communications. Common identification schemes are vulnerable against real-time attacks that are known as mafia frauds: An active adversary relays unnoticed all messages between the participants - causing a misidentification with fatal consequences. No convincing practical solution is known so far, and even common security proofs explicitly omit such scenarios”. Mafia fraud has been a weak point in all kind of communications technologies. The problem with mafia fraud in communication technologies is that attacker does not lay on the technology in order to provide the attack. This kind of attack is independent of the technology used. It means that the attacker does not make use of some weaknesses of the technology, but directly attacks the reliance of the users. Mafia fraud has been deeply studied, but authors propose an efficient solution which is still useful. This kind of attack can be used in order to know the location of the user. Once the attacker obtains access to the network, location can be obtained by acting as one member of the network and directly asking to one of the nodes.

The next year (2003) was a very prolific year for the field of research in GSM attacks. For example, at [19], Wullems et al. introduce location-based security services and discuss a new model for tamper-resistant location acquisition using GSM cell phones and related to two types of security ser-

vices, location-based Access control and audit. They also provided a basic set of criteria from which future research into 3rd generation cellular location and other location technologies can be pursued. Authors demonstrated these location-based security services in terms of a framework for both WAP and web-based Internet applications, which facilitates the acquisition of location using the proposed model for tamper-resistant location determination. This work is focused on GSM location. At this time, privacy GSM location methods started being an important research of study. Because of this, authors started worrying about security in GSM location.

Another good example of the prolific nature of this year and the worried atmosphere about location trust can be found in [20]. Here, authors identify a number of critical infrastructure applications that are reliant on location services from cooperative location technologies such as GPS and GSM. Authors perform a vulnerability analysis on these components of GSM and GPS location systems as well as a number of augmentations to these systems. Authors propose a generalized model for the vulnerability assessment of active location technologies with cooperative infrastructure, grouping the characteristics of GSM, GPS and various augmentations to these location systems. The model reduced the technologies to the fundamental characteristics of Infrastructure, Devices, Signaling and communications. Based on these characteristics, they perform a vulnerability assessment of these technologies. Authors offer another good example of the concern about location. They identified a set of GSM location weaknesses and offer solutions for some of them. Furthermore, at this work, it is possible to see some attacks that can be modified from GPS location to GSM location. That way, a researcher focus on GPS location can use his knowledge on this technique in order to propose solutions to GSM location attacks.

Another known problem on GSM networks is cloning. Brawerman and Copeland [4] propose an anti-cloning framework for software defined radio mobile devices (SRD) in 2005. The main idea of this framework is that the mobile device, together with the Wireless Operator, is responsible for detecting if it has been cloned or not. The weak point of the framework is that new pieces of hardware and new protocols are necessary to avoid network services being used by cloned units. The main problem of the work of Brawerman and Copeland is that their framework was only tested in the paper, so they offered no experimental data from the use of the framework. However, solution proposed by them was based on solid statements.

The SDR main idea is that it is not focused on the mobile phone of the user, but is used by this in order to establish communications. Due to this characteristic, cloning could be detected easily and with no interferences. The idea of separating the clone detection from the phone was really useful, and is the best solution to this problem. One of the more dangerous threats in SDR wireless communication is cloning. Besides illegal billing, cloned units increase the competition of shared resources, the network congestion and degrade network services. Even if the network enterprise can provide mechanisms in order to avoid cloning (like enhanced versions of the encryption algorithm COMP128-2 and COMP128-3), is still important to detect cloning when it happens. Problems of location associated with cloning will be explained on next chapter but, most common location problems associated to cloning of a mobile device are collisions on the location and fake data.

Even if most of the GSM problems have been solved due to these researches, there are still many possible attacks to GSM technology. In 2008, Toorani and Shirazi [21] propose an updated survey on those threats. In this paper authors make a briefly presentation of the most important security flaws of the GSM network and its transport channels. Due to the advance of technology, attacks have been improved too. The emergency of new technologies has meant the emergency of new threats and attacks. Authors noticed those changes and evaluated new possible attacks. The most important change in GSM communications was the release of smartphones. This kind of phone has a substantial difference of computation power than usual phones. Furthermore, it allows the execution of complex external applications, which could contain a potential threat to the user or the service. This way, attackers obtained a new set of gates to the service.

Work of Toorani and Shirazi is not only focused on the survey of new threats. At this paper, authors provide some practical solutions to improve the security of currently available 2G systems. They offered solutions for most of the proposed problems, at the same time that they leave an open window for new works on the field. This work is a good and updated overview about most common problems on GSM technology communications. However, this work is very general in terms of GSM location and is focused on GSM communications. Furthermore, it does not contemplate modern technologies associated to modern smartphones or 3G technologies.

An example of the appearance of new technologies and the repercussion on user's privacy could be found on the work of Grech and Eronen [22]. This work takes into account new technologies of communication. Even if is not the goal of the present work, Grech and Eronen researched on this paper about communication through internet. Unlicensed Mobile Access (UMA) is a technology that provides access to GSM services over Wireless LAN or Bluetooth. It also challenges the assumption of closed platforms, since it is relatively easy to implement a UMA phone purely in software running on standard PC hardware and operating systems. This paper examines the security implications of UMA for

GSM security, focusing especially on the impact of open terminal platforms. Authors identify several areas where open platforms may increase risks to both honest users and network operators, and propose countermeasures for mitigating those risks. This is only an example of how important technologies are into location services. An attacker could use the gate provided by this technology in order to hack the service of location of the user. Furthermore, some researches can be focused on providing this service of location through this kind of technology.

Conclusions

GSM is a very used technology and, therefore, a critical technology into security issues. Related with the security into GSM location, a possible attacker could have access, blocks or modify the location associated to a specific user or a location service. Furthermore, those attacks could be performed without a big invests on technology or computation, which makes it an attractive point for attackers.

Nowadays, existent surveys on GSM attacks are only focused on general possible attacks to GSM technology, but not on location risks. In this paper it has been shown that surveys on GSM attacks are not concrete enough for location issues.

Along this paper, a survey of the operation of GSM communication, as well as the weaknesses of this technology has been shown. Through the evaluation of the operation of GSM technology and its weaknesses, it is easier to understand the performed attacks and the risks associated to them. A survey of the operation of the location services based on GSM technology has been shown as well. The purpose of this survey is to provide a complement for the information given in the paper, as the basis for a deeper study in the field. Also, this survey helps in order to establish the framework of application of this technology of location, being as GSM location is not possible or has no sense to apply in every field.

However, current work on the field is not concluded yet. GSM based location techniques are not safe enough. As shown on the bibliography, there are still so many ways to perform an attack to the location blocking, modifying or obtaining the value of the provided location. GSM standard has not changed in the last years, mostly because of economic issues related to the companies that make use of this standard.

During this paper, it has been shown that cryptographic issues, as well as some issues related with the technology, could be solved so much time ago, but it could mean changing many things in both parts of the network, and many conflicts with old versions.

As a general conclusion, this technology is not safe enough for its use as the only location service in critical services. At the other hand, this technology offers a much extended, low consumption and user friendly method to locate people. Due to this reasons, besides the extension of the technology and the economic saving related to the companies providing those services, it is necessary to perform more researches in security. With this goal, this work tries to be a starting point, in order to facilitate the work for a researcher interested on this topic.

Acknowledgments

Thanks to Dr. Hugo Jonker and Dr. Jun Pang of University of Luxembourg for his help and advice during the development of this paper.

References

[1] Heikki Laitinen, Jaakko Lahteenmaki, Tero Nordstrom. Database Correlation Method for GSM Location. IEEE VTS 53rd Vehicular Technology Conference, 2001. VTC 2001 Spring. Vol 4. 2504 – 2508. 2001

[2] Chris Wullems, Oscar Pozzobon, Mark Looi, and Kurt Kubik. Enhancing the Trust of Location Acquisition Systems for Critical Applications and Location-based Security Services. Proceedings of the Forth Australian Information Warfare and Security Conference (AIWSC 2003). 391–405. 2003.

[3] M. Brinceno, I. Goldberg, and D. Wagner. GSM Cloning, 1998. http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html

[4] Alessandro Brawerman, and John A Copeland. An AntiCloning Framework for Software Defined Radio Mobile Devices. 2005 IEEE International Conference on Communications, 2005. ICC 2005. Vol. 5. 3434 – 3438. 2005

[5] Ammar Alkassar, Christian Stüble. Towards Secure IFF: Preventing Mafia Fraud Attacks. MILCOM 2002. 21st Century Military Communications Conference. IEEE. volume 2, pages 1139--1144, 2002

[6] L. Lopes, E. Villier, and B. Ludden, "GSM Standards Activity on Location," IEE Colloquium on Novel Methods of Location and Tracking of Cellular Mobiles and Their System Applications. 1999.

[7] Emiliano Trevisani and Andrea Vitaletti. Cell-ID location technique, limits and benefits an experimental study. WMCSA, *Workshop on Mobile Computing Systems and Applications.* IEEE Computer Society. 51-60.2004.