Interception Methods and GSM

Michal Sustek, Miroslav Marcanik, Milan Oplustil, Pavel Tomasek, Zdenek Urednicek
Faculty of Applied Informatics
Tomas Bata University in Zlin
Zlin, Czech Republic
Email: {sustek, marcanik, moplustil, tomasek, urednicek}@fai.utb.cz

Abstract— **Nowadays, eavesdropping is a real problem, whether it is about the interception of personal or corporate information. Current technologies enable us to use a wide variety of listening devices and methods. It may not be just a recording on a dictaphone, but also the use of vibration. The issue of eavesdropping is very popular today and many people and organizations work on solutions to prevent it. The work of these companies is mostly successful, but a problem still remains related to GSM (Groupe Special Mobile) interception. This contribution provides an insight into the principles of defense against the complex problem of eavesdropping. In any case, people have to be careful and consider what kind of information is communicated using cell phones and other technologies and what are the possibilities of their interception.**

Keywords-eavesdropping; interception; GSM; 5G; wire-tracking.

I. INTRODUCTION

Today, the boom of information and communication technologies contributes to an increasingly connected society. Modern technology surrounds us and it is, therefore, not surprising that almost every one of us owns a cellular phone. We all use it to communicate information. GSM phones are often used to communicate corporate information of critical importance. With the development of technology on transmission, we can see the development options of technologies on sound capturing and interpreting this information back [1]. It leads to a risk of using interception devices. Therefore, it is necessary to know what principles and technologies are used in the implementation of the interception, but also how to prevent it [2]. Eavesdropping can affect everybody in the world.

Countermeasures exist for most eavesdropping methods. However, GSM interception presents a specific issue It is difficult to identify an offender performing the passive form of eavesdropping. It forms part of the problem which must be dealt in the future.

Defense-technical inspection is the primary method [4] used to detect interception devices in a room or on other devices. This method is nondestructive for the device itself. Inspection is performed on suspicion of eavesdropping occurrence. An authorized person performs an initial analysis of space aimed at identifying possible risks and the type of interception device. In an organization, the inspection can be made visible, so that the employees of the company knew, but it can also be done discreetly, outside office hours, in which case the employees are unaware. This systematic inspection is supported by technical facilities [4], both for the detection of interception and subsequent security premises and equipment.

In some areas, it is mandatory to have devices for protecting against interception. Nowadays, with compelling interception devices, it is possible to see several technologies used in wiretaps. These technologies include a contact or non-contact scanning of information from windows, or the use of GSM phones, radio interception, direct recording on a recording unit, as well as passive and active GSM interception.

We should pay attention to protect relevant information, whether by technical means and/or by using common sense.

This contribution presents the basic outline of eavesdropping. It presents some methods of interception and countermeasure. That contains technical, regime measures and identification method including the defense-technical inspection.

Section 1 presents the GSM technology in general including mobile stations, the next generation 5G networks, and their architecture. Section 2 focuses on interception methods and protection methods against interception. The primary part of defense against eavesdropping is a defense-technical inspection. This inspection contains physical control, radio analysis, detection of nonlinearity and other measurements. It is used in protection of meeting places. The main goal is an identification of interception devices and defense against them. Devices against which one must protect are contact and contactless devices, unauthorized use of GSM phones, radio interception and record unit. GSM interception is divided into active and passive form. The active form is reliable, but it is easier to identify. On the other hand, the passive version of GSM interception is almost invisible, but it is not as reliable and it is useless in case of a moving device. The resources, which are used for defense, are GSM jammers, security wallpaper, radio analyzers and more.

II. GSM TECHNOLOGY

GSM technology is based on ETSI (European Telecommunications Standards Institute) standards [8]. The

 ISBN: 978-1-61208-493-0

primary document is standard "GSM - Phase first". In the development of this technology, these were several GSM phases until today's generation was created (Long Term Evolution, hereinafter, the LTE [8]) and for future generations 5G. The GSM network consists of mobile stations, the base station subsystem, a network and switching subsystem and operational subsystems. Subsequently, we will define several types of GSM services, such as telematics services, advanced services, additional services, the Subscriber Identity Module (SIM) card and phone.

GSM coverage area is divided into bundles. Each bundle consists of 7 cells. Inside each cell, there is a base station assigned to a particular group of channels and provides communication with mobile subscribers. In the event when the area of all the cells is equal to at least the interference area, it is possible to use the same channel group in all cells [6].

To obtain better properties of the system it is possible to use sectorization. The entire GSM area is divided into a smaller number of cells. This leads to the need to increase the number of base stations because the cells are smaller, but the covered area has the same size.

The number of required channels is not changing but the number of base stations growths from 7 to 21. Their number can be reduced again to 7 by placing three separate directional antennas at the intersection of three neighboring cells.

A. *Mobile station*

The GSM user communicates using mobile stations, which means not only the receiver/transmitter (cell phone), but also a SIM module. The SIM card is used as unique identifier for user within the network.

Source coding performs of the encoder source, which digitizes the analog signal and the digital side eliminates redundant data contained in the audio. The main goal of this step is to reduce the data flow to a minimum since each channel has its limitations. For removing these frequencies, a parametric method is used. The signal is divided into 20 msec segments. Then it is used to each segment LPC (Linear Predictive Coding) filter and LRP (Long-Range fading Prediction) to encryption.The resulting signal is composed of 188 bits, which carry information about calling and 72 bits, which carry information about filters. These two parts make up the frame of length 260 bits. There are 50 of these frames in one second, therefore, the bit rate is 13kbps.

To minimize unwanted signals, such as noise, interference, and scattering, channel coding is used, which adds additional bits to the colloquial frame which are used in the decoder to remove and reduce errors. In essence, it is a block of convolution codes that divide the 260-bit blocks colloquial framework into 3 classes (50 major, 132 minor and 78 less important). Based on these codes, it is possible to nearly double the signal and the speed.

The signal is magnified with redundant bits which are added to information binary string. It leads to increasing error detection and correction capabilities. A block, the size of which is 456 bits, is divided into 8 groups of size 57 bits each. These groups are interleaved with the last four groups of the previous block and with the first four groups of the following block.

B. *5G Architecture*

One of the main ideas of designing 5G networks [6] is a separation of internal and external users into two segments. This approach aims to avoid losses resulting from signal passing through the walls, or at least minimize it. It will be realized with a complex antenna system and massive Multiple Input/Multiple Output (MIMO) technology, which will be deploying large antenna arrays with tens or hundreds of antenna segments. While the most common MIMO technologies serve 2 to 4 antennas, the goal of massive MIMO systems is to increase user options by using antenna arrays. Outdoor base stations will be equipped with an extensive antenna array of antenna elements around the cells. These cells will be connected by optical fibers with base stations. Outdoor users are equipped with a limited number of antenna elements, but they can work with others in an extensive virtual network. An antenna array will be installed outside buildings and will communicate with external base stations.

One can use a mobile architecture where internal users need to communicate only with the internal access points with antenna arrays; then, one can use technologies for short-range communication (Wi-Fi [6], the ultra-wide band [6], mm-wave communications [6]).

5G network architecture should also contain heterogeneous macrocells, microcells, small cells, and transmitters. To ensure adequate coverage for users who move too quickly, it will also work with mobile femtocells, which combine the concept of mobile relays and femtocells [6]. In Figure 1, one can see the planned architecture for 5G networks.

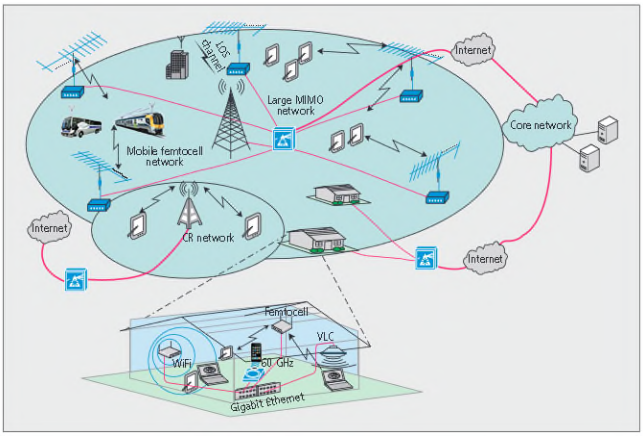

Figure 1. 5G Network [6].

C. *Encryption for data protection*

Current encryption is used to protect against unwanted eavesdropping. The GSM network calculates the secret key, which length is 64 bits, after verifying the mobile phone in the mobile station. A key figure of TDMA (Time Division Multiple Access) frame lengths of 22 bits is input to the cipher algorithm A5 [6]. The A5 algorithm generates a pseudo-random sequence which, along with 114-bit bursts used XOR function. It leads to data encryption. The A5 algorithm is relatively fast and it establishes a 228-bit sequence during TDMA frame.

After encryption, the modulation signal has a carrier wave using GMSK (Gaussian Minimum Shift Keying) modulation. GMSK is two-state modulation which is based on the frequency keying stroke.

III. INTERCEPTION

Interception of mobile phones and monitoring the flow of information are current topics of great interest. With the available technologies, it is possible to eavesdrop on almost any form of communication. On the other hand, however, it remains the issue of cryptography and steganography [1]. Wiretapping is usually conducted by a third party (i.e., not the operator, but he can know about eavesdropping and allow it). Wiretapping is divided into active and passive forms. The operator knows about the active form and sees it in the system, however, a passive form is not known to the operator. The passive form is based on the capture of radio signals and then decoding them.

The passive way has very significant limits in terms of reach and effectiveness, because, when the phone is in motion, these interceptions have problems with receiving the signal. For this type of interception, a computer equipped with a GSM antenna, receiver, and special software is used. This software enables the device to identify all phones within range and can focus on one or multiple phones. Then, it can record, decode and eavesdrop the cell phones (in the case of short message service and multimedia messaging service). The interception of conversation is not possible to find or identify. Consequently, it is necessary to focus on defense rather than detection.

A. *Defense-technical inspection*

Defense-technical inspection is the basic form for detecting interception devices in a room and also it is not destructive to the device. The inspection is conducted on the grounds of suspicion. An authorized person performs an initial analysis of the room aimed at identifying possible risks of the type of interception, determination of inspection techniques and inspection frequency. As with all steps, it is necessary to select the date, time, method and inspection techniques themselves. The inspection can be made visible, so that the employees of the company knew, but also discreetly outside office hours, by which employees are not aware [4].

Most companies that provide the inspection to be carried out require the constant presence of a responsible person from the part of the applicant, which is to prevent further irregularities and accusations that might occur. Once an interception is found in an area, there are basically three options to deal with it. These options are its liquidation, inform the police or use it for disinformation the offender. The inspection consists of four steps:

- Physical control
- Radio Analysis
- Detection of nonlinearity
- Other measurements

1) *Physical control*

In the first step of defense-technical inspection, all the equipment and other resources, which could contain the interception, will be disassembled. Examples include outlet detectors, telephones, lights, switches, and other similar devices.

2) *Radio Analysis*

The second step performs spectral analysis [3] in the room. It scans all frequencies that occur at that place and subsequently verifies if each frequency has a reason for its existence. The principle of this method is to detect the presence of radio equipment which is designed for the interception. Figure 2 shows the radio analysis output. Each frequency indicates radio signals of potential interception hardware.

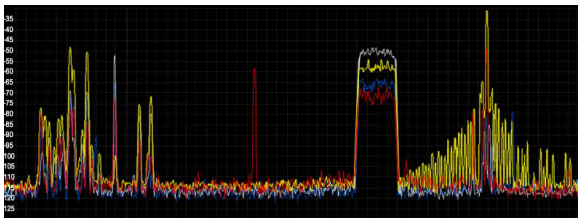

Figure 2. Radio Analysis [3].

3) *Detection of nonlinearity*

After identifying the presence of a radio detector, the inspection checks nonlinearities. The method is based on the fact that each intercepted device includes semiconductor components. It allows the discovery of semiconductors in the transmitted electromagnetic field. This detection method is used for walls, construction equipment etc.

4) *Other measurements*

The last step is to check the other elements, such as telephone lines, checking in infra-specter, control of leadership in the over-voice band.

Due to a large amount of work, it is an approximate speed of inspection 10 m^2 per hour for a couple of technicians. After the inspection is completed, the authorized person of the contracting authority receives a verbal report follows by a written report on the results of the inspection and the list of used methods. Of course, as in all sectors of security, the best protection is a combination of

 ISBN: 978-1-61208-493-0

technical means to human disturbance, because the technology is not always reliable and can be a failure [4].

B. Technique for protection meeting places

With the increasing diversity of eavesdropping devices also grows a diversity of protection devices against the interception. These safeguards are mandatory in some areas. Today, after the expansion of eavesdropping devices it is possible to see several technologies that are used for wiretapping (contact or contactless sensing information from windows, the use of GSM phones, the radio interception, direct recording on the recording unit).

1) Protection against contact and contactless information gain from windows or walls of the building

The interception is performed on the basis of vibration of the glass panel or the wall of a building. The method/devices used to protect these surfaces are white noise generators [4]. The white noise vibrates on the window panels and in the walls. Optionally, one can add speakers, from which the noise is able to superimpose a recording of the voice recorder. Due to the frequency range of the white noise, it is clear that it passes all frequencies of human speech. The white noise is a mechanical wave. It leads to interference with the signal and then it cannot be deleted with the available technology. It protects reliably before interception using stethoscopic and laser microphones. Despite all the advantages it also has one major disadvantage, especially for the comfort of the people on negotiations. The frequencies are in the audible spectrum and can thus interfere with the comfort of each person in the room [4].

2) Protection for unauthorized use of GSM phones

Under this type of protection, it is possible to use two devices (Identification GSM operation and the GSM jammer). The identification of the GSM operation uses sensitive devices that detect signals in the GSM band, and inform both acoustically and visually about the unauthorized transmissions. The disadvantage is the necessity to set it to a sensitivity to avoid false alarms announcement [4].

The second option is a GSM jammer, which operates in the GSM phones. GSM jammers jam the receiver, which subsequently cannot log into the network. There are many types of jammers, which vary in reliability. However, the problem remains that, in fact, it is illegal to interfere with the operators signal [4].

3) Protection against radio interception

The most common type of interception is radio interception [10]. It has good possibilities for capturing and sending the signal. However, as in all other cases, these are ways to prevent it. For protection, they are used in radio analyzer, jammer, safety foil, and wallpapers.

Radio analyzer saves all radio frequencies, which are active in the area. After subsequent scanning of the radio spectrum, the results can be compared with the new scan and the error detected. This deviation indicates a new radio receiver/transmitter that can be tapped in space and display the field strength (relative distance of the transmitter). These devices have a difference in bandwidth with which they are able to operate and control the speed. Like with all other devices, there are also certain disadvantages. In particular, these disadvantages include the relatively high demands on the operation and the high coverage area of different radio signals. Only in London, the scan of a single site can detect 600 active frequencies. That is the reason why is it necessary to carefully adjust the sensitivity of these because not of all the disturbing frequencies comes from listening devices [4].

The second possibility is a jammer; whose function is very similar to GSM jammers. The main advantage is the fact that they produce no false signals. But, as with the GSM version, there is questionable legality and yet unknown effects on human health by prolonged exposure. Some types of jammers are nowadays used as protection against remotely charge attacks that have initiated igniter radio signal.

The third measure, which operates on the principle of Faraday's cage (inhibits the passage of radio signals from the protected area) are security stickers, wallpapers, and foils. Its application is technically very demanding. Wallpaper itself contains a copper layer. It is necessary to completely cover each element of the room (doors, windows, line filters for 230 V line). The use of a protective element is rather rare due to the complexity [4].

4) Protection from obtaining information direct entry to the recording unit

In the context of digitization, it is no longer possible to use some methods for protecting before recording the acoustic signal to a recording device, which was used earlier. Today's equipment for direct recording does not radiate. It is necessary to choose methods that have an effect on the quality of recorded sound. The solution is the noise generator with speakers. The noise binds to the signal and degrades it. Nowadays, there are no technical possibilities to effectively eliminate the noise from the recording [4].

C. Techniques to protect communications media

The advent and subsequent development of GSM technology have created a new risk, which involves interception of mobile phones and information communication in this way. It is important to recognize that the GSM network protects information with encryption only on the way to a GSM cell and back to the phone, the rest is unprotected.

Currently, there is a wide variety of devices that are able to decrypt the signal in real time and perform it in this way of the interception. These elements can be active or passive.

1) Active

Active devices are essentially fake GSM cells. The device convinces its target that the device is the best cell, which should be used with the cell phone. The signal is duplicated. One copy is forwarded to a GSM network and

 ISBN: 978-1-61208-493-0

the second copy is decrypted. These systems are active and they are detectable on the side of the operator. By default, this method is used in urban residential areas, approximately 500 meters from their target. Generally, these methods are more reliable than passive methods of eavesdropping [4].

2) Passive

The capturing signal takes place on the side of the cell phone. The attacker must be in urban areas about the same distance. The main advantage of this method is "invisibility". On the other hand, if the target moves, the interception is essentially impossible because the device is not able to quickly re-tune the frequency in order to capture the tapped signal.

The best method of defense of communications equipment is their encryption. Therefore, many cell phone manufacturers have started to produce versions of their phones, which are equipped with encryption devices. The basis is the principle on which the information is digitized, encrypted and in such form goes with the device. On the receiver side, one must also use an encrypted phone for which it is possible to decrypt the information [4].

3) GSM interception

As in the case of radio interception, it is a small device that senses ambient sounds, but, unlike classical radio interception, it does not intercept the broadcast signal locally on discrete frequency, but it is transmitted using the same principle as talking on a cell phone. Actually, the interception is logged into base transceiver station as well as cell phone and from a signal transmitted. Nowadays, this type of interception is widespread for several reasons. First, it has a virtually unlimited range; the attacker can be anywhere there is a phone signal coverage. Second, the main supply is operating almost unlimited. The last point is called costs. The costs are minimal (advantageous monthly fee) and it is almost impossible to capture the conventional methods for detecting interception (Radio frequency detectors, radio spectrum analyzers). The findings of this type of the interception device are problematic for several reasons. First, the signal is not transmitted on a usual frequency and analog modulation, but it uses GSM network infrastructure itself with FDMA/TDMA (Frequency Division Multiple Access/ Time Division Multiple Access). The entire eavesdropping is not conducted continuously, but it is invoked to "request" call on the device. In principle, the device is logged into the network. The device is hidden, if it does not launch an active interception, it looks like others cell phones.

Although finding of these devices is difficult it is not impossible. One can use a spectrum analyzer and a strict adherence to procedures. If one wanted to avoid installation of interception device, one must have 24-hour control over all daily routines in the room. This approach is costly and unsustainable.

IV. CONCLUSION AND FUTURE WORK

Nowadays, the interception issue affects all people, even if they do not realize it. Due to the technical progress of society, there are many means of communicating information, but also a lot of resources for their capture.

This technology creates a risk of misuse of critical information. Currently, there is a large amount of communication through people's cell phones. Cell phones are often used to communicate critical corporate information. Fortunately, despite the technical capabilities of the attacker, there are countless ways to resist interception.

Defense-technical inspection is the basic form for detection of interception devices in a room and that is also non-destructive to the device. The inspection is conducted on the grounds of suspicion. An authorized person performs an initial analysis of the room aimed at identifying possible risks of the type of interception, determination of inspection techniques and inspection frequency. As with all steps, it is necessary to select the date, time, method and inspection techniques themselves. The inspection can be made visible, so that the employees of the company knew, but also discreetly outside office hours, by which employees are not aware.

For technical resources, in addition to physical control, spectral analysis is also performed. This is a scan of all frequencies and their subsequent comparison with a reference measurement. Based on this comparison, it is possible to identify suspect signals that could potentially come from interception devices. Another method that is used is the control of nonlinearities. The method is based on the fact that each previously produced interception includes semiconductor components. The nonlinearities detection method can detect the presence of semiconductors in a sensing area because the electromagnetic field in the area is affected by these semiconductors. The authorized person must not forget to check the other elements, such as telephone lines, checking in infra specter, control of the over-voice band.

Defense against GSM interception is difficult because its identification is not easy. Its signal is not broadcasted on a frequency and analog modulation but uses GSM network infrastructure itself with FDMA/TDMA access. The entire interception is not carried out continuously, but it is invoked to "request" call on the device. In principle, the device is logged into the network. The device is hidden, if it does not launch an active interception, it looks like others cell phones.

The next steps of research will lead to a deeper understanding of wiretaps in terms of features and options for defense against them. Following this understanding will be appropriate to conduct a testing and measuring for available wiretaps. On the other hand, the most interesting methods of interception, the GSM interception is probably the best option for a creation of any external encryption applications.

 ISBN: 978-1-61208-493-0

ACKNOWLEDGMENT

This work was supported by Internal Grant Agency of Tomas Bata University under the project No. IGA/FAI/2016/25.

REFERENCES

[1] S. Fisman, Wiretapping, and Eavesdropping. Clark Boardman Callaghan, 1978. ISBN 068559856X.

[2] J. Losert, Infosafe - Protection against eavesdropping, special technology [Online]. Olomouc:, 2016. Available from: http://www.infosafe.cz/ 2016.5.17

[3] J. Mudroch, Mudroch Labs s.r.o [Online]. Bánská Bystrica, Available from: http://www.triangulace.cz/ 2016.5.17

[4] F. Kucera, Mobile interception. Android World [Online]. Praha: VSHosting, 2012 Available from: http://www.svetandroida.cz/ mobilni-odposlechy-jak-funguji-a-lze-se-jim-branit-201201 2016.5.17

[5] N. Kokesova, Principles of operations of contemporary mobile communication networks . Brno, 2006. Supervisor Doc. Ing. J. Saudek, CSc.

[6] Ch. Wang and F. Haider, "Cellular Architecture and Key Technologies for 5G wireless Communication Networks" IEEE Communications Magazine. 2014, (2): 9. Available from: http://cms.comsoc.org/SiteGen/Uploads/Public/Docs_TC_5GMWI/Cellular_Architecture_and_Key.pdf 2016.5.17

[7] I. Poole, 5G Mobile / Cellular Technology. Radio-Electronics [Online] Available from: http://www.radio-electronics.com/info/ cellulartelecomms/5g-mobile-cellular/technology-basics.php 2016.5.17

[8] J. Kacerovsky, GSM Networks. Semestral paper, Communication systems and services, Brno, 2002. Available from: http://www.uai.tode.cz/stud_mat/GSM/it420_gsm.pdf 2016.5.17

[9] M. D. Renzo et al., "Spatial Modulation for Generalized MIMO: Challenges, Opportunities, and Implementation," Proc. IEEE, vol. 102, no. 1, Jan. 2014, pp. 56–103.

[10] C.-X. Wang and S. Wu, "Massive MIMO Channel Measurements and Modeling: Advances and Challenges", IEEE Wireless Communication.

[11] WWRF, L. Sorensen and K. E. Skouby, User Scenarios 2020, report, July 2009; http://www.wireless-world-research.org. 2016.5.29

[12] N. Jamaly., A. Derneryd and Rahmat-Samii, Y. "Spatial Diversity Performance of Multiport Antennas in the Presence of a Butler Network", Antennas and Propagation, IEEE Transactions on, On page(s): 5697 - 5705 Volume: 61, Issue: 11, Nov. 2013.

[13] Kempe D. and F. McSherry, A decentralized algorithm for spectral analysis, Journal of Computer and System Sciences, v.74 n.1, p.70-83, February 2008

[14] X. Li, H.-N. Dai, Q. Zhao and Q. Wang. "Eavesdropping Attacks in Wireless Ad Hoc Networks under a Shadow Fading Environment" Proceedings of the 2014 International Conference on Internet of Vehicles (IOV 2014)

 ISBN: 978-1-61208-493-0