International Journal of Research and Innovations in Science & Technology*,*
©SAINTGITS College of Engineering, INDIA
www.journals.saintgits.org
Research paper

Data and Voice Signal Intelligence Interception Over The GSM Um Interface

Vincent N. Omollo[1]*, Silvance Abeka[2], Solomon Ogara[3]

Jaramogi Oginga Odinga University of Science & Technology, Bondo – Kenya.
** vincentyoung88@gmail.com*

Abstract

The Enhanced Data rates for GSM Evolution (EDGE) is a digital mobile phone technology that permits enhanced data communication rates as a backward-compatible annex of the Global System for Mobile communications (GSM). It delivers increased bit-rates per radio channel, which results to a threefold increase in capacity and performance compared with an ordinary GSM/General Packet Radio Service (GPRS) connection. It has found many applications in packet switched communication scenarios, such as internet connections. In a GSM environment, owing to its cellular nature, the communication signals are sent over the air interface. Therefore, it is less secure than in a wired network because it is prone to eavesdroppers equipped with appropriate radio receivers. To address the various security challenges, several security functions were built into GSM to safeguard subscriber privacy. These functions include: authentication of the registered subscribers only; secure data transfer through the use of encryption; subscriber identity protection; making mobile phones inoperable without a subscriber identity module (SIM); disallowing duplicate SIMs on the network; and securely storing the individual subscriber authentication key (KI). However, as demonstrated in this paper, the EDGE signals can still be intercepted, re-routed or modified over the GSM Um interface.

Keywords: ***Encryption, GSM, Security, Signal interception, Um Interface***

1. Introduction

In a cellular network, a service coverage area is divided into smaller hexagonal areas referred to as cells and each cell is served by a base station. The base station is fixed and is able to communicate with mobile stations such as cellular telephones using its radio transceiver. The base station is connected to the mobile switching center (MSC) which is, in turn, connected to the public switched telephone network (PSTN). Figure1 illustrates a typical cellular network, where the triangles represent base stations.

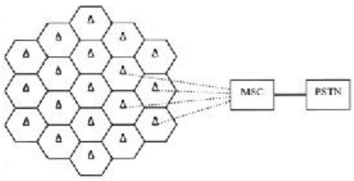


Figure 1: Cellular Network Concept

The frequency spectrum allocated to wireless communications is very limited, so the cellular concept was introduced to reuse the frequency. Each cell is assigned a certain number of channels. To avoid radio interference, the channels assigned to one cell must be different from the channels assigned to its neighboring cells [1]. However, the same channels can be reused by two cells that are far apart such that the radio interference between them is tolerable. By reducing the size of cells, the cellular network is able to increase its capacity, and therefore to serve more subscribers.

For the channels assigned to a cell, some are forward (or downlink) channels that are used to carry traffic from the base station to mobile stations, and the others are reverse (or uplink) channels that are used to carry traffic from mobile stations to the base station. Both forward and reverse channels are further divided into control and voice (or data) channels [2]. The voice channels are for actual conversations, whereas the control channels are used to help set up conversations. To route a call or data through the GSM network is a complicated affair, involving a number of network devices as illustrated in Figure 2. Every GSM mobile station (MS) has a Subscriber Identity Module (SIM) that provides the mobile phone with a unique identity through the use of the International Mobile Subscriber Identity (IMSI). Without this SIM card, the mobile phone is rendered inoperable. It is capable of storing personal phone numbers and short messages. It also stores security related information such as the A3 authentication algorithm, the A8 ciphering key generating algorithm, the authentication key (KI) and IMSI. The mobile station stores the A5 ciphering algorithm [3]. The SIM can be protected with a Personal Identification Number (PIN) chosen by the subscriber. The PIN is stored on the card and if entered incorrectly thrice, the card blocks itself. At this point, the cellular provider needs to be contacted to unblock the mobile phone by entering an eight digit Personal Unblocking Key (PUK), which is also stored on the card.

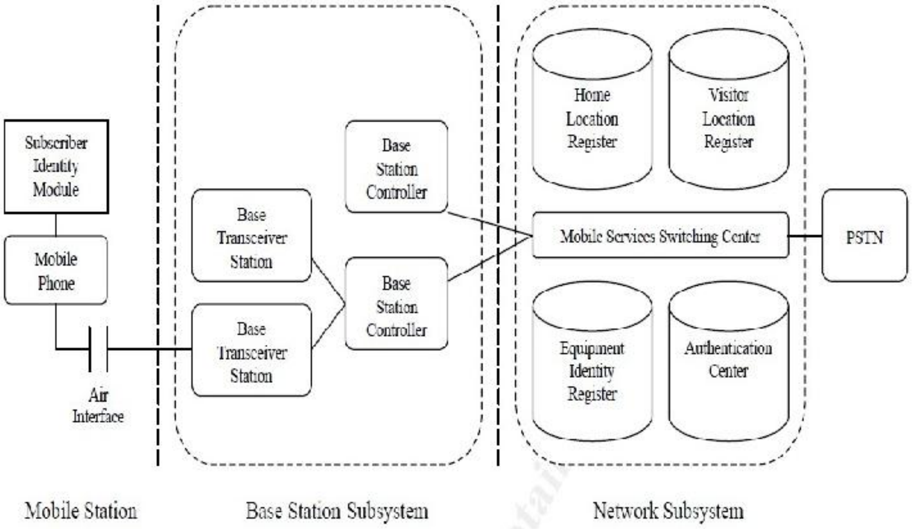


Figure 2: The GSM Architecture

The responsibility of the Base Station Subsystem (BSS) is to connect the user on a mobile phone with other landline or mobile users. The Base Transceiver Station (BTS) is in direct contact with the mobile phones via the air interface (Um). The Base Station Controller (BSC) is responsible for the control of the several BTS. It monitors each call and decides when to handover the call from one BTS to another, as well as manages radio frequencies allocated for the calls through the BTS.

The Network Subsystem (NSS) is a complete exchange, capable of routing calls from a fixed network via the BSC and BTS to an individual mobile station. The Mobile Services Switching Center (MSC) interconnects the cellular network with the Public Switched Telephone Network (PSTN). The MSC also serves to co-ordinate setting up calls to and from GSM users [4]. The Home Location Register (HLR) stores information of all subscribers belonging to an area served by a MSC. It stores permanent data such as the IMSI, services subscribed by the user, subscriber’s number from a public network, KI and some other temporary data. The HLR has to provide the MSC with all the necessary information when the call is coming from a public network.

The Visitor Location Register (VLR) contains relevant information for all mobiles currently served by a MSC. The permanent data stored in the VLR is also stored in the HLR. In addition, it also stores the Temporary Mobile Subscriber Identity (TMSI), which is used for limited intervals to prevent the transmission of the IMSI via the air interface [5]. The VLR has to support the MSC during call establishment and authentication when the call originates from a mobile station.

The Equipment Identity Register (EIR) stores all the International Mobile Equipment Identities (IMEI) of mobile equipment and their rights on the network. The EIR maintains a white, gray and black list. Those on the white list are permitted on the network while those on the black list are blocked from the network [6]. The gray list consists of faulty equipment that may pose a problem on the network but are still permitted to participate on the network. The IMEI reveals the serial number of the mobile station, manufacturer, type approval and country of production. The Authentication Center (AuC) is a protective database that houses the KI, the A3 authentication algorithm, the A5 ciphering algorithm and the A8 ciphering key generating algorithm. It is responsible for creating the sets of random numbers (RAND), Signed Response (SRES) and the Cipher key (KC), though the created sets are stored in the HLR and VLR.

2. Related Work

Various studies have shown that GSM is very insecure. The cryptographic algorithms, such as A3, A5and A8 that are used in GSM have been broken [7]. The data communication protocols added to GSM after its initial deployment, such as GPRS and EDGE, have all along been suspected of being just as insecure as GSM itself [8]. Before the network can permit a subscriber, the authentication procedure checks the validity of the subscriber's SIM card and then decides whether the mobile station is a legitimate user. This is done suing the challenge-response method as shown in Figure 3. As the figure shows, the authentication procedure starts by sending a 128 bit random number (RAND) to the MS over the Um interface. This random number is then passed to the SIM card, where it is sent through the A3 authentication algorithm together with the individual subscriber authentication key (KI).

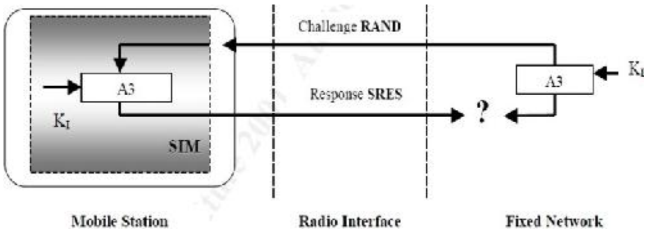


Figure 3: MS Authentication In GSM Network

The output of the A3 algorithm is the signed response (SRES) which is transmitted via the Um interface from the MS back to the network. Once in the network, the AuC compares its value of SRES with the value of SRES it has received from the MS. If the two values of SRES match, authentication is successful and the subscriber joins the network. The key to GSM's security is keeping KI unknown. However, using a chosen-challenge attack (which works by forming a number of specially-chosen challenges) and querying the SIM card for each one, the value of the secret key that is used for authentication can be established by analyzing the responses from these queries[9].

When a new GSM subscriber turns on his MS for the first time, its IMSI is transmitted to the AuC on the network, which results to a Temporary Mobile Subscriber Identity (TMSI) being assigned to the subscriber MS. The IMSI is rarely transmitted after this point. This is to deter a potential adversary from identifying a GSM user by their IMSI. The user keeps on using the same TMSI till location updates occur. Each time a location update happens, the network assigns a new TMSI to the MS. The MS employs the TMSI to report to the network or during call initiation. Similarly, the network uses the TMSI, to communicate with the mobile station. The Visitor Location Register (VLR) performs the assignment, the administration and the update of the TMSI [10]. When it is switched off, the mobile station stores the TMSI on the SIM card to make sure it is available when it is switched on again. However, in this paper, we showed that it is possible to establish the IMSI, which could then be used to identify the GSM user.

To protect both user data and signaling on the vulnerable Um interface, GSM employs a ciphering key. Once the MS is authenticated, the RAND (delivered from the network) together with the KI (from the SIM) is sent through the A8 ciphering key generating algorithm, to produce a ciphering key (KC) as shown in Figure 4. The 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 [11].

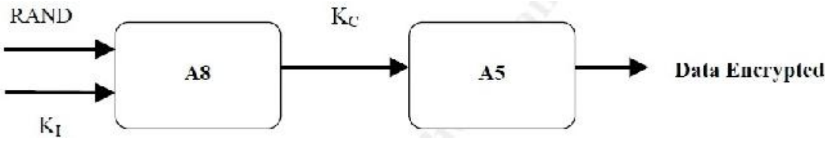


Figure 4: Data And Signaling Encryption Using Ciphering Key

The A5 algorithm is implemented in the hardware of the mobile phone, as it has to encrypt and decrypt data very fast. However, A5 has been cryptographically broken []. Moreover, the COMP128 algorithms, which are implementations of the A3 and A8 algorithms defined in the GSM standard have been shown not to be strong enough to prevent fraud [12].

3. Methodology

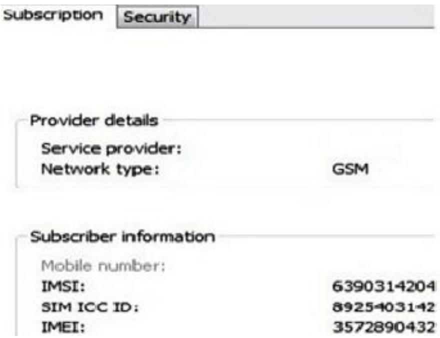
In this paper, we demonstrate how one can be able to make a call on another subscriber's bill, how to break into the GSM network and determine the absolute radio-frequency channel number (ARFCN), how to accomplish packet sniffing, and how to intercept EDGE signals over the Um interface. This is the air interface between the GSM MS and the base transceiver station.

3.1 Making Calls On Another Subscriber's Bill

To carry out this attack, the researchers exploited the COMP128 weakness that allowed them to establish the value of the secret key that was used for authentication purposes over the GSM network. To accomplish this, both hardware and software tools were required. The hardware tools that were employed included SIM card reader, SIM programmer, silver pic 2 card and unregulated adapter. On the other hand, the software tools included Cardinal Sim Editor, CardMaster and SIMEMU.

3.1.1 Procedure

The SIM card reader was plugged into the computer com port and the Cardinal SIM editor was run. On the editor's settings, the com port where the SIM card was inserted and the transmission baud rates were selected. On the smartcard item, SIM editor was picked and the program was thereof started. Afterwards, SIM Info item was clicked to bring forth the load button. This allowed us to determine the IMSI and IMEI codes as shown in Figure 5. For security reasons, only part of these codes is shown and the name of the service provider has also been hidden.

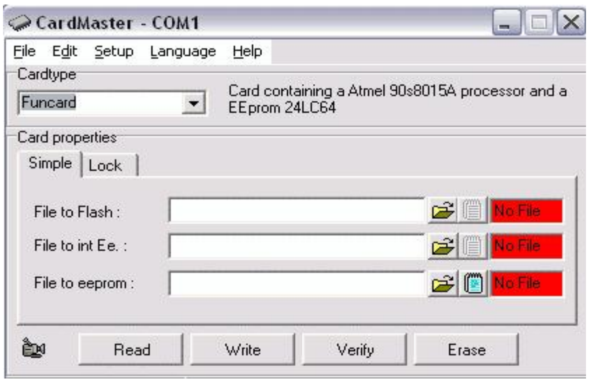


Provider details
Service provider:
Network type: GSM

Subscriber information
Mobile number:
IMSI: 6390314204
SIM ICC ID: 8925403142
IMEI: 3572890432

Figure 5: IMSI Code Determination

The SIM Info dialog box was closed and the Security/Find key KI option was selected. Upon opening, the start key was clicked and after sometime, the KI key was found. The SIM programmer was then connected to the com port and from the CardMaster program setup menu, the appropriate port to where the programmer was attached to was selected. When the card was ready, the card type was chosen by clicking on silvercard. In the silvercard, there were two files, namely SEE50s.hex (EEPROM) and SEF50sEN.hex (PIC). In the CardMaster menu, the item 'File to Pic' field was picked and SEF50sEN.hex was uploaded. Similarly, 'File to Eeprom' item was picked and SEE50s.hex uploaded as shown in Figure 6. This figure shows card type as Funcard, which was changed to silvercard as already stated. Afterwards, on the Edit menu, 'Auto Program' was selected. The SIM card was then resized so as to fit into the MS.



Cardtype: Funcard

Card containing a Atmel 90s8015A processor and a EEprom 24LC64

Card properties

File to Flash : No File

File to int Ee. : No File

File to eeprom : No File

Figure 6: CardMaster Uploading

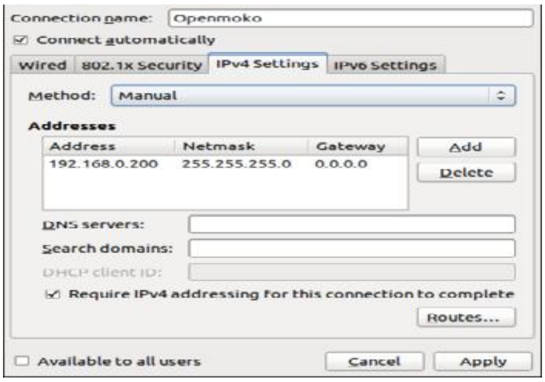
This silvercard was then inserted into the phone and the personal identification number (PIN) entered. From the Sim-Emu menu, the Set Phone # was clicked, then GSM #1 slot, followed by Configure and finally Edit#. The GSM #X was edited to any name and the ok key pressed. From the Config.Pos menu, PIN2 was inserted and position 1 was selected as the card position. Afterwards, the setup asked for the IMSI, which was then entered as shown in Figure 5. Moreover, the setup required the KI, which was then entered as obtained from the Cardinal software. The personal unlocking number (PUK) was also entered.

3.2 Absolute Radio-Frequency Channel Number

The absolute radio-frequency channel number is a code which indicates a pair of physical radio carriers employed for land mobile radio system transmission and reception of signals. One of this pair is used for the uplink signals while the other one is used for the downlink signals. Hence it is important if one has to intercept the signals over the Um interface.

3.2.1 Procedure

The Openmoko and wireshark software were used to determine the absolute radio-frequency channel number (ARFCN). The Openmoko software captured the GSM packet while wireshark was used to analyze it and hence determine the ARFCN. Figure 7 shows the Opnmoko interface that was used to edit and capture the packets. Wireshark is a powerful tool that is used to troubleshooting networks, both wireless and wired, network analysis, and also for software and communications protocol development.



Connection name: Openmoko

☑ Connect automatically

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.0.200	255.255.255.0	0.0.0.0

DNS servers:

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

□ Available to all users

Figure 7: Openmoko Interface

On wireless networks, it is possible to employ the Aircrack wireless security tools to incarcerate IEEE 802.11 frames and read the resulting dump files with Wireshark. Figure 8 shows the wireshark interface. In this section, we demonstrate how the GSM packets can be captured and the encryption /decryption algorithm used determined. The GSM algorithms include A3, A5 and A8.

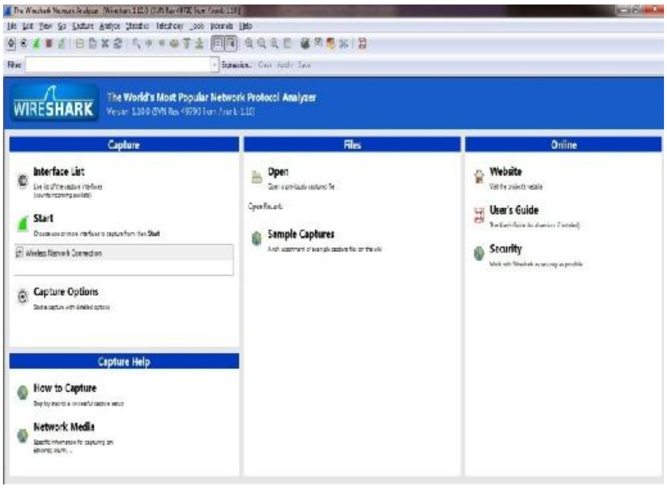


Figure 8: Wireshark Network Analyzer Interface

As this figure shows, among the details on this diagram are the interface list and start option. This list specifies from which network the packets are to be captured from and analyzed. These interfaces can be wireless or wired, such as a local area network. Since the data to be captured resided in the Um interface, the wireless option was selected and the start button pressed to commence the data interception and analysis.

3.3 GSM Packet Decoding

The A3 It is operator-dependent and is an operator option. The A3 algorithm is a one-way function, meaning that it is easy to compute the output parameter SRES by using the A3 algorithm but very multifaceted to recover the input parameters (RAND and KI) from the output parameter. A5 has various implementations, such as A5/0, A5/1 and A5/2. The rationale for the diverse implementations is due to export restrictions of encryption technologies. Whereas A5/1 is the strongest version, the A5/0 comes with no encryption, and hence is the weakest.

3.3.1 Procedure

Since all the above GSM algorithms have been cryptographically broken, determining which one is in use is important in deciding the attack mechanism to be used to decrypt the data. Once again, the tools of choice were Openmoko and Wireshark. Similar procedures were adopted as the ones for ARFCN determination.

3.4 GSM Traffic Interception

Whereas any GSM data can be captured over the GSM Um interface, this paper settled on the EDGE data because the Universal Mobile Telecommunications System **(**UMTS) and High-Speed Packet Access (HSPA) (both High-Speed Downlink Packet Access -HSDPA and High-Speed Uplink Packet Access- HSUPA) use UMTS authentication, which is relatively strong, owing to its mutual authentication nature. However, most devices also GSM/EDGE capable, and are configured to try and connect to a GSM/EDGE network whenever a suitable MTS/HSPA network is not available.

3.4.1 Procedure

To accomplish both data and voice interception over the Um interface, both hardware and software components were needed: The hardware included a mobile phone jammer, a base transceiver station (BTS), hub, a laptop computer and a modem/ADSL ; while the software included Linux operating system, OpenBSC, OpenGGSN and OsmoSGSN. The hardware connections were done as shown in Figure 9. The experimental BTS was placed very close to the ADSL so that the radiated power from the BTS could reach it. The radio spectrum for transmission was set to be that of the target Public Land Mobile Network (PLMN).

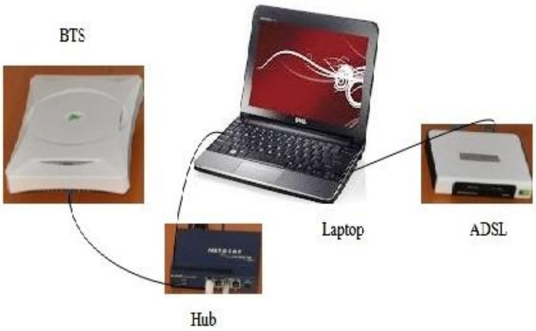


Figure 9: GSM Traffic Interception Setup

The laptop had Linux operating system installed, together with three additional software, namely OpenBSC, OpenGGSN and OsmoSGSN. OpenBSC includes functionality usually accomplished by the following components of a GSM network: BSC (Base Station Controller), MSC (Mobile Switching Center), HLR (Home Location Register), AuC (Authentication Center), VLR (Visitor Location Register), and EIR (Equipment Identity Register). Both OpenGGSN nad OsmoSGSN were utilized to add GPRS/EDGE capabilities to the OpenBSC.

The setup BTS was tuned to emit signals in the frequency of the target PLMN. It was also configured to masquerade the target PLMN by setting its MCC (Mobile Country Code) and MNC (Mobile Network Code) codes to those of the target PLMN. Moreover, it was set to accept the connection of the target MS, identified by his IMSI code and IMEI. The procedure for obtaining both IMSI and IMEI was outlined in section (A) above. The laptop computer had an operational uplink to the Internet an ADSL connection and the OsmoSGSN, OpenGGSN, and her routing tables were configured in such a way that the traffic from the target were forwarded to the Internet or redirected to some other machines and the replies from the Internet get back to the target MS.

The set up BTS was then powered to provide network coverage to the victim. Since the setup BTS was closer to the target MS, the power level from this BTS was stronger than that from the real PLMN. Hence the target MS was meant to desert its connection to the real PLMN and connect to the set up BTS. To force the ADSL to switch to EDGE connectivity, a mobile phone jammer became handy to by causing interference in the UMTS frequency bands used at that location such that the target MS lost its 3G connectivity and resort to the 2G connectivity. Thereafter, the target MS was instructed to utilize GEA0 as the encryption algorithm, which had no encryption at all.

4. Results And Discussions

In this section, we discuss the results of the four attacks whose procedures were given in the previous section. These included making calls on another subscriber’s cost, determining the absolute radio-frequency channel number of the target MS, decrypting GSM data over the Um interface and intercepting the GSM user traffic.

4.1 Making Calls On Another Subscriber’s Bill

It was demonstrated that it is possible to make a call on the expense of another subscriber by masquerading his SIM card details given in section (A) above. However, some networks are configured to detect and terminate calls originating simultaneously from same SIM card. Hence one cannot initiate a call when the victim is also calling. This can be addressed by blue -bugging the victim and employing the BT Info software to turn off his MS as shown in Figure 10. Once the victim MS is off, the attacker can make calls at the victim’s bill.

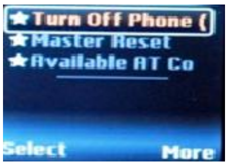
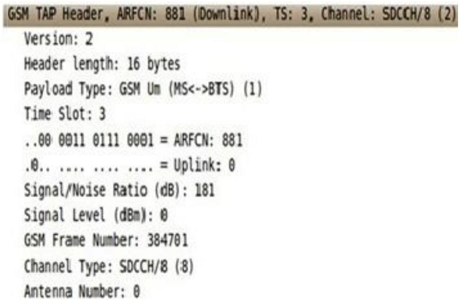


Figure 10: Turning Off The Target MS

4.2 Absolute Radio-Frequency Channel Number

This attack was carried out using Openmoko and Wireshark software. Whereas the Openmoko software was employed to capture the GSM packet, Wireshark software was utilized to analyze it, revealing the information shown in Figure 11.



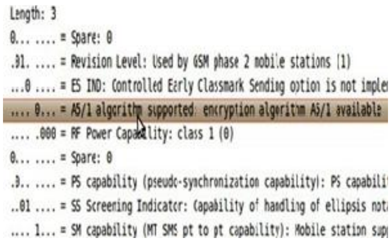
```
GSM TAP Header, ARFCN: 881 (Downlink), TS: 3, Channel: SDCCH/8 (2)
  Version: 2
  Header length: 16 bytes
  Payload Type: GSM Um (MS<->BTS) (1)
  Time Slot: 3
  ..00 0011 0111 0001 = ARFCN: 881
  .0.. .... .... .... = Uplink: 0
  Signal/Noise Ratio (dB): 181
  Signal Level (dBm): 0
  GSM Frame Number: 384701
  Channel Type: SDCCH/8 (8)
  Antenna Number: 0
```

Figure 11: Downlink ARFCN Determination

It shows that the absolute radio-frequency channel number that was in use for downlink connections in this GSM network was 881. This value is important because it is a key determinant of both the uplink and downlink frequencies.

4.3 GSM Packet Decoding

The rationale of this attack was the establishment of the GSM algorithm that was in use in the communication between the target MS and the GSM network. Knowing this algorithm was important so that an attacker would decide which vulnerability to exploit in order to decrypt the GSM data, since these algorithms have varying cryptographic strength. Figure 12 gives the results obtained.



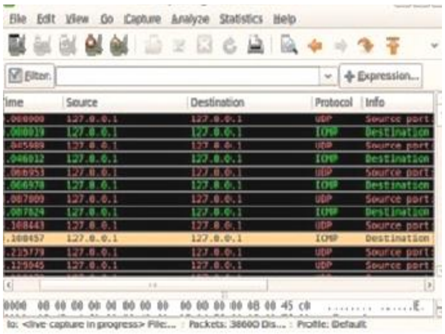
```
Length: 3
0... .... = Spare: 0
.01. .... = Revision Level: Used by GSM phase 2 mobile stations (1)
...0 .... = ES IND: Controlled Early Classmark Sending option is not imple
.... 0... = A5/1 algorithm supported: encryption algorithm A5/1 available
.... .000 = RF Power Capability: class 1 (0)
0... .... = Spare: 0
.0.. .... = PS capability (pseudo-synchronization capability): PS capabili
..01 .... = SS Screening Indicator: Capability of handling of ellipsis not
.... 1... = SM capability (MT SMS pt to pt capability): Mobile station sup
```

Figure 12: GSM Packet Decoding

Figure 12 displays the GSM algorithm in use as A5/1. This algorithm employs an extremely weak encryption key of only 64 bits. The consequences are that the short length of this key makes it susceptible to rudimentary attacks such as brute forcing and dictionary attacks.

4.4 GSM Traffic Interception

The results indicate that by employing the setup in section (D) above, it was easy to establish a GSM network monitoring point as shown in Figure 13. It is clear from this figure that one can determine the transmission period, packet source, packet destination, the protocol in use as well as other miscellaneous data concerning the MS data communications.



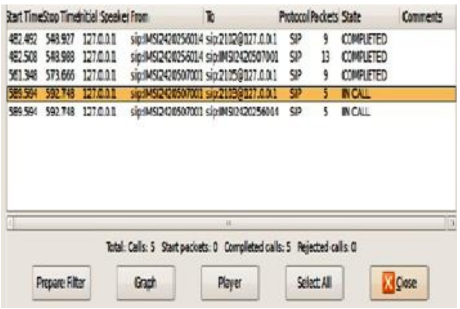
```
ime        Source      Destination   Protocol  Info
.000000    127.0.0.1   127.0.0.1     UDP       Source port
.000019    127.0.0.1   127.0.0.1     ICMP      Destination
.045689    127.0.0.1   127.0.0.1     UDP       Source port
.046012    127.0.0.1   127.0.0.1     ICMP      Destination
.066953    127.0.0.1   127.0.0.1     UDP       Source port
.066978    127.0.0.1   127.0.0.1     ICMP      Destination
.087009    127.0.0.1   127.0.0.1     UDP       Source port
.087024    127.0.0.1   127.0.0.1     ICMP      Destination
.108443    127.0.0.1   127.0.0.1     UDP       Source port
.108457    127.0.0.1   127.0.0.1     ICMP      Destination
.215779    127.0.0.1   127.0.0.1     UDP       Source port
.219045    127.0.0.1   127.0.0.1     UDP       Source port

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 c0   ........ ......E.
lo: <live capture in progress> File... : Packets: 38600 Dis... : Profile: Default
```

Figure 13: GSM Network Monitoring

Moreover, by placing the setup BTS in close proximity to the intended target, the target MS's voice and signaling traffic were intercepted successfully. This was made possible by the fact that all the traffic was routed through the setup laptop.

It was possible to employ Wireshark's built-in SIP analyzer, to play back voice traffic in real-time or to be recorded for malicious activities as shown in Figure 14.



Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
482.492	548.927	127.0.0.1	sip:IMSI242025056014	sip:2102@127.0.0.1	SIP	9	COMPLETED	
482.508	548.988	127.0.0.1	sip:IMSI242025056014	sip:IMSI242050507001	SIP	13	COMPLETED	
561.348	573.666	127.0.0.1	sip:IMSI242050507001	sip:2105@127.0.0.1	SIP	9	COMPLETED	
589.594	592.748	127.0.0.1	sip:IMSI242050507001	sip:2103@127.0.0.1	SIP	5	IN CALL	
589.594	592.748	127.0.0.1	sip:IMSI242050507001	sip:IMSI242025056014	SIP	5	IN CALL	

Total: Calls: 5 Start packets: 0 Completed calls: 5 Rejected calls: 0

Figure 14: Wireshark Conversation Interception

5. Conclusion

In this paper, it has been demonstrated that it is possible to carry out data and voice interception in the GSM network. This was possible by the determination of useful MS details such as the IMSI, IMEI and KI. Using this technique, one can gain full control over the target's data and voice communications. This attack exploited three major GSM vulnerabilities. The first vulnerability was that there is absence of mutual authentication in EDGE (2G), which makes EDGE devices completely vulnerable to this attack. Moreover, the GSM standard's requirement that MS support the GEA0 encryption algorithm, which essentially means no encryption at all makes GSM devices prey for this kind of attack. Finally, the system implemented on most UMTS and HSPA (3G) devices that makes them cascade to EDGE when UMTS or HSPA are not available, which perpetuates this attack to these 3G devices. To curb this, the MS's must be configured to only connect UMTS/HSPA networks so that they do not switch to EGDE when network connectivity deteriorates. Alternatively, higher level protocols (that protect GSM data in transit even though the principal communication channel is insecure) such as Secure Sockets Layer (SSL) and Internet Protocol security (IPSec) that grant endpoint authentication and encryption should be employed.

References

[1] G. Sai and A. Kakkar, "Generations of Mobile Communication", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.6, No.3, (2016), pp. 320-324.

[2] U. Gawas, "An Overview on Evolution of Mobile Wireless Communication Networks: 1G-6G", *International Journal on Recent and Innovation Trends in Computing and Communication*, Vol. 3 No.5, (2015), pp. 3130 – 3133.

[3] M. Toorani and S.Beheshti, "Solutions to the GSM Security Weaknesses", *Proceedings of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies*, Vol. 88, (2014), pp. 576-581.

[4] [M. Kamel and E. George, "Secure Model for SMS Exchange over GSM", I. *J. Computer Network and Information Security*, Vol.1, (2016), pp. 1-8.

[5] M. Ramadan, D. Guohong, L. Fagen, and X.Chunxiang, "A Survey of Public Key Infrastructure-Based Security for Mobile Communication Systems", *MDPI*, (2016), pp. 1-17.

[6] D. Brake, "5G and Next Generation Wireless: Implications for Policy and Competition", *Information Technology & Innovation Foundation*, (2016), pp.1-22.

[7] J. Cichonski, J. Franklin , and M. Bartock, "Architecture Overview and Security Analysis", *National Institute of Standards and Technology*, (2016), pp. 1-49.

[8] E. Donald, and O. Nosa, "Analysing GSM Insecurity", *International Journal of Research and Scientific Innovation*, Vol.3, (2016), No. 10, pp. 10-18.

[9] B. Ravishankar, "Authentication and relate threats in 2G/3G/4G Networks", *Department Of Computer Science*, Oxford, (2016), pp. 1-64.

[10] M. Ramadan, G.Du, F. Li, C. Xu, "End-to-End Encryption Scheme over GSM System", *Int. J. Secur. Appl*, Vol. 10, (2016), pp. 229–240.

[11] M. Inayat, M. Siddique, and A. Asadullah, " A Survey on the Encryption Algorithms Used in Cell Phone Messages", *International Journal of Emerging Technology and Advanced Engineering*, Vol.6, No.2, (2016), pp. 36-39.

[12] Z. Jabr, S. Taha and I. Aly Saroit, "Seps-Aka: A Secure Evolved Packet System Authentication And Key Agreement Scheme For Lte-A Networks", *Computer Science & Information Technology*, (2014), pp. 57–70.