GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)

GSM FLAWS IN CONCERN WITH IOT

Ujvalkumar Patel, Pratik Patel

P.G.Student, School of Cyber Security & Digital Forensic, National Forensic Science University, Gandhinagar, Gujarat. (youp64759@gmail.com, https://orcid.org/0000-0001-5166-6775)

Asst.Professor School of Cyber Security & Digital Forensic, National Forensic Science University, Gandhinagar, Gujarat. (pratik.patel@gfsu.edu.in, https://orcid.org/0000-0001-6469-7319)

Abstract

The Global Systems for Mobile Communication(GSM) is really the most boundless versatile Communication innovation existing these days. Its acquaintance goes back to the last part of the eighties, it experiences a few security weaknesses, which have been focused by numerous attacks intended to break the fundamental correspondence convention. A large portion of these attacks related to the A5/1 algorithm used to ensure over-the-air correspondence between the two gatherings of a call. Notwithstanding, it is as yet being used in the GSM networks as a fall-back alternative, in this manner actually putting at hazard the security of the GSM. This standard provides worldwide roaming & Interconnection with any available GSM network including the ones implemented in IOT so that users need to be aware of the possible security issues. The goal of this work is to survey the absolute most applicable outcomes in this field and examine their reasonable possibility.

Key-words: *IoT, GSM, Software Defined Radio, Software Defined Radio, Gnu-radio, GSM Security, Attack, Encryption, Vulnerability.*

INTRODUCTION

The Global Systems for Mobile correspondences (GSM) is actually the vastest adaptable correspondence advancement, representing in excess of around 3.5 billion memberships. GSM standards originally describe a digital, circuit-switched network for full duplex voice telephony. This extended after some time to incorporate information interchanges, first by circuit-switched transport, at that point by parcel information transport by means of GPRS (General Packet Radio Services) and EDGE (Enhanced Information rates for GSM Evolution).
Specifically, the GSM standard experienced the evil impacts of various deficiencies which thought about the headway of a couple of attacks prepared to break mystery and security of subscribers. The goal of this paper is to audit some of the most significant security assaults to the GSM-related innovations.
The structure of the paper is as follows, in the second section, the background of gsm followed by section three, where we have discussed security features. In section four there are attack factors & discussion and final remarks in section five.

THE BACKGROUND OF A GSM

The GSM has been created by the ETSI as a standard to portray conventions for second era computerized cell networks utilized by cell phones.

Network & Switching Subsystem
The GSM framework design contains a variety of components, and is often called the Core Network. It is basically an information network with different substances that give the fundamental control and interfacing for the entire mobile network. The significant components inside the core network include:
Mobile Service Switching Center (MSC): The main element of the core network. Acts like an exchanging hub inside PSTN or ISDN likewise give extra usefulness to empower the necessities of a mobile user to be upheld. Interfaces to different MSCs are given to empower calls to be made to mobiles on various networks.
Home Location Register (HLR): The database contains all the managerial data about every subscriber alongside their last known area.
Visitor Location Register (VLR): This contains chosen data from the HLR that empowers the choice services for the individual endorser to be provided.
Equipment Identity Register (EIR): The EIR is a database that stores lists of MSs International Mobile Equipment Identity (IMEI).
Authentication Center (AuC): It is an ensured information base that contains the secret key likewise contained in the client's SIM card. It is utilized for validation and for encoding on the radio channel.

Gateway Mobile Switching Center (GMSC): The GMSC is the highlight which a ME ending call is at first routed, with no information on the MS's area.
SMS Gateway (SMS-G): The gateway handles messages coordinated in various ways. The SMS-GMSC (Short Message Service Gateway Mobile Switching Center) is for short messages being shipped off a Mobile Equipment. The SMS-IWMSC (Short Message Service Inter-Working mobile Switching Center) is utilized for short messages beginning with a mobile on that network.

Base-Station Subsystem
It is liable for dealing with traffic and signaling between a Mobile Station and Network & Switching Subsystem. It comprises of two components:
Base Transceiver Station (BTS): The BTS utilized in a GSM network involves the radio transmitter collectors, and their related antennas that send and get to legitimately speak with mobiles.
Base Station Controller (BSC): The BSC controls a gathering of BTSs and frequently co-located with one of the BTSs in its group. It deals with the radio assets and controls things, for example, handover inside the group of BTSs, allocates channels.

Operation and Support Subsystem (OSS)
OSS is a component inside the general GSM mobile communication network architecture that is associated with segments of the NSS & BSC. It is used to control and screen the overall GSM network and it is likewise used to control the traffic load of the BSS.

SECURITY FEATURES

GSM security is tended to in two perspectives: Authentication & Encryption. Authentication avoids fraudulent access by cloning MS. Encryption avoids unauthorized listing. At whatever point ME attempts to join a GSM network, it needs to go through a validation method needed to confirm the character of the subscriber utilizing it. At the point when connected, the signaling and information channel over the radio path between a base station and the ME are ensured by an encryption scheme. These schemes don't need touchy data to be sent over the radio channel. All things being equal, the confirmation is performed utilizing a challenge response component. The conversations are encrypted utilizing a temporary, haphazardly created encoding key (Kc). The cell phone recognizes itself by means of the Temporary Mobile Subscriber Identity (TMSI), which is given by the network and might be changed intermittently for extra security.

Authentication
As examined in Margrave 1995, the cycle of Authentication in GSM standard is as per the following.
The Authentication Center (AuC) generates a 128 bit random number (RAND) and sends it to the ME [1].
The mobile phone generates the 32 bit signed response (SRES) based on the encryption of RAND with A3 algorithm using Authentication Key (Ki) [6]. The calculation is completely done inside the SIM.
On the network, after getting a signed response (SRES) from the subscriber, the AuC contrasts its estimation of SRES and the value it has gotten from the cell phone. In the event that the two qualities coordinate, the verification is effective and the subscriber joins the network.

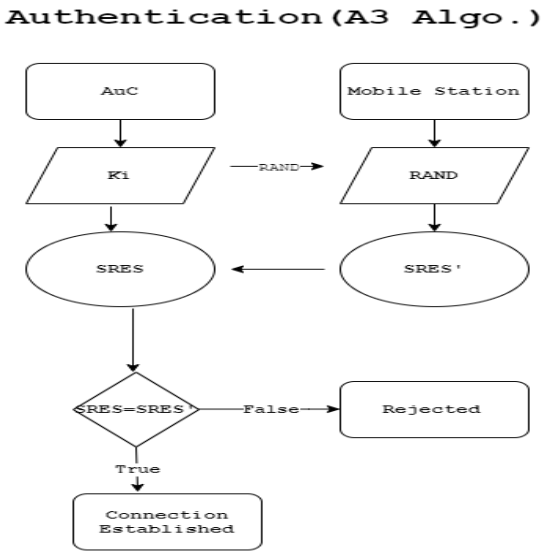

fig.1

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)

Encryption

In the event that the MS is acknowledged for access, an encryption key generated by A8 algorithm with KI & RAND as input. The SIM contains the execution of the algorithm A8 which is utilized to produce the 64-bit ciphering key (Kc) to be utilized to encryption also, decode the information between the ME and the base station. Encoded communications between the MS and the organization are finished using A5 Encryption algorithm. Encryption algorithm started by an encoding mode from the GSM network. The versatile station starts encryption and decryption of information using the chosen encoding algorithm and the encoding key (Kc). The A5 algorithm is implemented in the ME, as they have to encrypt and decrypt data over the air.

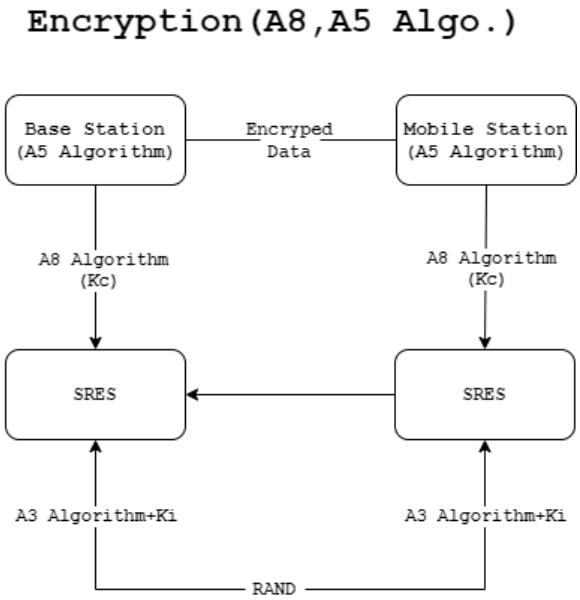

fig.2

Since GSM has been around for over 10 years there have been few changes in the quality of a portion of the algorithms.

ATTACK FACTORS

There is a wide classification of attacks against versatile correspondence that doesn't rely upon network shortcomings. These include SIM cloning, phishing with SMS and may exploit human factors as well. [Castiglione et al. 2009] has written a good review on such security issues. The majority part of the attack focuses on the A5 algorithm. The careful definition of these algorithms is still authoritatively mysterious. However, the research has been able to reverse the algorithm and did crypt-analysis. Basic structure of A5/1 was disclosed in 1994. First crypt-analysis has been performed by Golic [Golic 1997]. In this segment we survey probably the most intriguing assaults proposed up until now, recognizing by passive, handover and active attacks.

Passive Attack

Let's talk about history, after the overall plan of A5/1 was released, a few shortcomings of this algorithm have been uncovered by mainstream researchers. The main attack focusing on the A5/1 algorithm has been proposed by Golic [Golic 1997], which presented a compelling Time-Memory Trade-Off (TMTO) attack. This procedure is relevant to any cryptosystem with a generally modest number of inner states like A5/1, which has 264 states characterized by three move registers. The proposed attack would be practicable just having 15 TB of pre-determined information or three long stretches of known discussion, which isn't extremely sensible [Biryukov et al. 2001].

Biryukov introduced two assaults dependent on a TMTO [Biryukov et al. 2001]. The main attack requires two minutes of known-discussion information and one moment of handling time, while the second attack requires two seconds of plaintext information and a few minutes of handling time. The amount of required storage changes from around 140 GB to 290 GB. Sadly, the execution season of the proposed attack develops dramatically with the diminishing of the information succession. The significant downside of this attack is that it requires a lot of known-discussion information, which is practically speaking not generally accessible.

Barkan proposed an improvement of this technique in [Barkan et al. 2003]. The creators initially depict a cipher text just attack on A5/2 that requires two or three dozen milliseconds of encoded behind closed doors cell discussion and finds the right key in under a second on an individual PC. At that point, their proposition is reached out to a more-mind boggling cipher text as it was attacked on A5/1 abusing a shortcoming of the GSM convention. Specifically, the creators saw that mistake adjustment codes are utilized in GSM frames.
After all of this in 2009 Nohl found out a way to do an attack almost in real time where attackers need 2TB of pre-calculated data.
Whatever mentioned above, attacks need pre-calculated data then only attack can be performed. So in practical manner and as an example of passive attack, a passive attack gadget would just catch IMSI numbers. This is basic includes playing out the initial steps of interfacing with a BS.

Active Attack
Active attack is making a full network connection with the cell tower so Men in the Middle (MITM) can be accomplished. As mentioned before for fake base stations, it will forward the acknowledgment and authenticated traffic to real BS. A5/1(weak) or A5/0 (disabled) algorithm used in fake BS so that incoming and outgoing traffic can be easily captured and read.
When the GSM Technology is implemented in an IoT system. the system becomes vulnerable to these attacks, compromising the integrity of the system. The below mentioned methods have been tested and successfully exploited, as a result the SMS and voice calls were decrypted and were available to the attacker in plain text.

Method (I)
In this method researchers can create their own network and test it. So that real services do not get interrupted.
Equipment: BladeRF x40, HackRF, HTC Desire HD, Nokia 6021.
Blade RF is the full duplex software defined radio which is used to build fake base stations. These can transceiver on a frequency of 300MHz to 3.8GHz [6]. It is a full duplex that means it can receive and transmit at the same time. This is necessary for running BS.
HackRF is utilized to investigate the radio signs created by the Blade RF. It is a half duplex handset and it has a recurrence of 1MHz to 6GHz.
HTC Desire HD and Nokia 6021 are utilized to test the base station.
Methodology: First step of this method is setting up the base station on the spectrum of GSM 900. For Sniffing and decoding purposes GR-GSM (open source tool for analysis of gsm signals) will be used.
After setting up these things Jamming will perform to check whether a phone jumps to the fake base station [6].
Now, start the live monitoring of the GSM radio signals using gr-gsm and capture it using Wireshark (Packer analyzer tool that enables us to capture packets at an interface and analysis of various procedures at packet level). Check all the packets in wireshark and check which algorithm is implemented in live connection.
Configure the YateBTS and try to connect with fake BS using Nokia or HTC. So that SMS, GPRS & voice traffic can be sniffed.

Method (II)
In this method researchers can create their own network using IOT devices and test it.
Equipments: Arduino, gsm module sim900, RTL-SDR.
Arduino is the microcontroller that enables us to control our hardware with a serial connection.
Gsm module sim900 is a device which is able to make calls using AT commands.
RTL-SDR enables a wide range reception of signals up to 2100MHz.
Methodology: Initiate a call to a number using Arduino board and gsm module. Simultaneously set the RTL-SDR to capture the live packets using gr-gsm.
Spare the caught record and interpret this spared .cfile utilizing gr-gsm with same boundaries as were when catching and open Wireshark, tune in to loopback and subsequent to unraveling save the record as a .pcap augmentation.
Pass parameter of TMSI in wireshark, save the output in .txt format and find out repetition of TMSI.
Method (III)
In this method researchers don't have to build their own network. It is directly plug and play the gsm radio frequency.
Equipments: RTL-SDR
Methodology: The first thing to find out is frequency. Primary GSM band is 900MHz. Kalibrate (an open source project used to scan the gsm frequencies) will give us an output of the number of frequencies around us.
Select the frequency from the output list of Kalibrate. Now, start capturing the GSM traffic of particular frequency.
Using airprobe python script the frequency will be captured in real-time. Simultaneously start wireshark and dump the data of the airprobe.

Now, Data has been captured as packets in wireshark. So as of now analyze the pacp file for more information about the frequency.
By analyzing the file, IMSI, TMSI, and the Ciphering algorithm can be found.
For the next step, connect the phone with the computer in media transfer protocol and use it as an abstract modem which supports AT- Commands, which used to get Kc and TMSI.
Note down the TMSI & Kc. This is an important value of the encryption method of gsm. So use it to decrypt the voice channel and sms.

DISCUSSION

IoT is a vast topic and can be implemented in various domains of engineering, commerce and medical science. The organizations use GSM with IoT to communicate remotely with their substations and servers.
Due to the lack of technical assistance, organizations often buy and implement insecure/poorly configured hardware or outdated technology. Since GSM has already been compromised it is highly recommended to avoid using outdated technology and upgrade to newer technology and tools such as SIM7600EI, SIM7100A (4G LTE High speed modems) for secure communication.

"Conflict of Interest: The authors declare that they have no conflict of interest."

REFERENCES

[1] Arjunsinh Parmar, Kunal M. Pattani (2017), "Sniffing GSM Traffic Using RTL-SDR and Kali Linux OS", [Journal] IRJET e-ISSN: 2395-0056, p-ISSN: 2395-0072
[2] Sanjeev Saharan, Jitender Kumar (2017), "Exploiting GSM Vulnerabilities: An Experimental Setup And Procedure To Map TMSI And Mobile Number", [Journal] IJARCS ISSN: 0976-5697
[3] Nicolae Crisan, Maria Condrea (2017), "GSM Wireless Sniffer using Software Defined Radio", [Journal] CJECE ISSN: 1844-9689
[4] [Event] Black Hat (2008), "Intercepting GSM Traffic", [Online] Available: https://www.blackhat.com/presentations/bh-dc-08/Steve-DHulton/Whitepaper/bh-dc-08-steve-dhulton-WP.pdf
[5] Muhammad Talha Choudary ,Arish Yaseen , Muhammad A Javaid , Abeer R Khan1 , Bilal A Khawaja , Sajid Saleem and Muhammed Mustaqim (2017), "Sniffing Decoding and Decryption GSM signals using Open Source Software and Low Cost Hardware" , [Journal] IEEC
[6] Kenneth van Rijsbergen (2016), "The effectiveness of a homemade IMSI catcher build with YateBTS and a BladeRF", [Online] Available: https://rp.delaat.net/2015-2016/p86/report.pdf
[7] Santiago Aragon, Federico Kuhlmann and Tania Villa, "SDR-based network impersonation attack in GSMcompatible networks", [Journal] IEEE ISSN: 1550-2252
[8] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext only cryptanalysis of gsm encrypted communication", [Journal] Cryptology [Online] Available: https://link.springer.com/content/pdf/10.1007/s00145-007-9001-y.pdf
[9] GSM Structure Diagram [Online] Available: https://en.wikipedia.org/wiki/GSM