Journal of
Computer Science & Systems Biology

Research Article OMICS International

A Proposed Lower Computational Complexity Secret Key Mirroring System on GSM

Oyinloye OE[1]*, Alese BK[2], Thompson F[2] and Adetunmbi AO[2]

[1]*Department of Computer Science, Ekiti State University, Ekiti State, Nigeria*
[2]*Federal University of Technology, Akure, Ondo State, Nigeria*

Abstract

Global system for mobile communication is a wireless radio technology used mostly on network communication. It is designed to overcome the challenges of analog communication. GSM evolved from generation 1G to 4G LTE and uses protocols to protect transmissions, which have shown to be susceptible to attacks. This fact has been proven based on several attacks ranging from narrow pipe attack, guess, and determine attacks, side channel attacks, time memory tradeoff attacks and correlation attacks which have high computational complexities. The proposed system called GSM Traffic Monitoring System (GTMS) attempts to proffer a lower computational complexity attack. It uses a key retrieval and passive attack module to handle the mirroring of the secret key authentication procedure given a chosen random challenge on a SIM card through the injection of a malware. This research aims at drawing the attention of network providers- SIM configuration; an area that requires protection from attackers.

Keywords: GSM traffic monitoring system; Mirroring; 2-ary malware; Key retrieval; GSM; GTMS$_{\text{RAND}}$; SIM; Authentication; Secret key

Introduction

Mobile communication has become convenient than ever, due to openness of wireless network. One of the applications of mobile communication is in the use of the Global System for Mobile Communication (GSM). The GSM is a digital wireless network standard designed to replace the many existing incompatible cellular system; to overcome the limitations of analog communication network systems. Most users use the GSM network for communication and exchange of very sensitive and private information believing that the GSM System is reliable and secure [1].

The Global system for mobile communication has three sections namely; the mobile station, base station subsystem and network and switching subsystem as described in Figure 1.

The mobile station consists of the mobile equipment and a subscriber identity module card. It authenticates itself to the operator's network and communicates to other users through the base station subsystem. The base station subsystem controls the radio link with the mobile station. It manages the base transceiver station, releases/allocates radio channels, coordinates frequency hopping, channel setup and connection of mobile station to network and switching subsystem [2].

The network and switching subsystem is responsible for the management of mobile services such as authentication, switching of calls profiling and mobility management, call routing between functional entities based on the standard signaling system number 7 (SS7), location update, roaming capabilities, call control, provision of subscribed services for each mobile currently located in a geographical region [2]. The connections between these sections are mostly fiber, microwave, and satellite links [1].

In all, GSM has evolved through several generations; each generation is characterized by its own operational features. The generations include the 1G, 2G, 3G, 3.5/4G. 1G is the analog voice cellular telephony developed in 1980s; it supports one call per channel and hence was inefficient in using limited spectrum. It required large/heavy and expensive analog devices and its power consumption was high. It required large frequency gap to handle interference [3].

In order to deliver mobile voice services to more people in more places, the 2G was designed in the 1990s and it supported more than one user per channel, enabling compression of voice signal. The digital components cost/weight were far less and it delivered more secure signals. It allows multiple users (8 users) per radio with each user talking one at a time via time division multiple access (TDMA) technique; offering a simple data service with General Packet Radio Service (GPRS). It required large frequency gap to reduce interference [3,4].

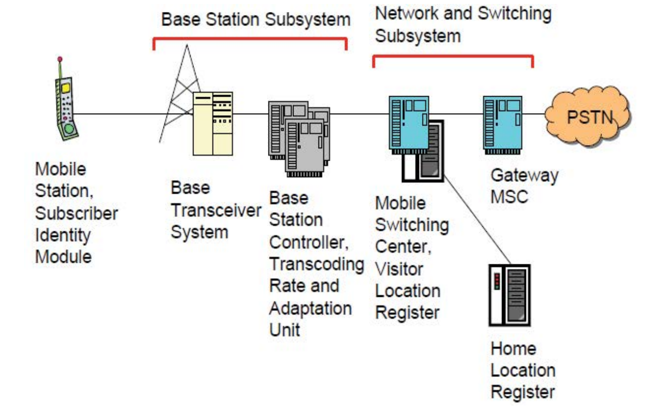
Base Station Subsystem
Network and Switching Subsystem
PSTN
Mobile Station, Subscriber Identity Module
Base Transceiver System
Base Station Controller, Transcoding Rate and Adaptation Unit
Mobile Switching Center, Visitor Location Register
Gateway MSC
Home Location Register

Figure 1: GSM Architecture [3].

***Corresponding author:** Oyinloye OE, Department of Computer Science, Ekiti State University, Ekiti State, Nigeria, Tel: +2348033897728/+2349053120280; E-mail: rukkivie@yahoo.com

Received December 19, 2016; **Accepted** January 12, 2017; **Published** January 20, 2017

Citation: Oyinloye OE, Alese BK, Thompson F, Adetunmbi AO (2017) A Proposed Lower Computational Complexity Secret Key Mirroring System on GSM. J Comput Sci Syst Biol 10: 006-011. doi:10.4172/jcsb.1000239

On top of the foregoing, the development of the Code Division Multiple Access (CDMA) GSM in year 2003 yielded 3G. It provided increased voice capacity by more efficient use of spectrum resources and better security. With 3G the high-speed internet access was introduced and it surpassed 2G connections in 2013 [3,4]. Since year 2010, the 4G Long Term Evolution (LTE) is evolving to provide more data capacity for faster and better mobile broadband. The multimode 3G/LTE is the foundation on which the 4G LTE thrives [3,4]. These GSM generations proffer several levels of security and excellent services; however, the security services are operated on cryptographic devices.

In recent years, several kinds of attacks on cryptographic devices have become public. The goal of these attacks is to reveal the secret key of cryptographic devices. Techniques used to achieve this goal are manifold; hence attacks on cryptographic devices differ significantly in terms of cost, time, equipment, and expertise needed. Consequently, there are also several ways of categorizing these attacks. Attacks may be classified as either passive or [5,6].

Passive attacks are attacks in which the cryptographic device is operated largely or even entirely within its specification. The secret key is revealed by observing physical properties of the device, for example; execution time, power consumption. With active attacks, the cryptographic device, its inputs, and /or its environment are manipulated (tampered with) in order to make the device behave abnormally. The secret key is revealed by exploiting this abnormal behavior of the device [5].

Receptivity is one of the characteristics of GSM network, thus anyone could use a receiver to passively monitor the radio waves. Therefore, it is important that reasonable security measures should be employed to ensure privacy of user's data from unauthorized use of the service, avoid misuse of resources by impersonators and eavesdropping on information. Security measures have been put in place to safe guard a subscriber's privacy ranging from personal identification numbers, pin unblocking key codes, several protocol algorithms for communication. Despite the availability of these security measures, a test of the provided security measure is regularly required to determine the strength of the security mechanism deployed by network operators. Researches show that these security measures may be susceptible to several attacks such as cryptographic attacks, power analysis attacks and correlation attacks as confirmed by the studies of [7-10]. Although these attacks and many more have successfully cracked the security algorithms they also have shown to have high computational complexity. As researches expose some of the weaknesses, designers of GSM have attempted to handle these weak points, more attacks have been proposed on the newer approaches.

Review of Existing Studies

The GSM is used by millions of users [11]. These millions entrust their privacy at the mercy of the network provider's security mechanism.

GSM deploys several security measures to protect the radio link and communication in general. They include:

(i) A3 algorithm

(ii) A8 algorithm

(iii) A5 algorithm

The use of these algorithms is seen in user authentication, protection of transmitted data over-the-air among others. The efficiency of these algorithms, hinge on the high degree of security on secret key privacy. A study by Brienco et al. showed that network vulnerability is possible by revealing the secret key, since the secret key is central to the security algorithm [7]. This was proved by recovering the secret key from a SIM card through reverse engineering gathered data from the reference algorithm, based on 150,000 challenge queries. The study further showed that possession of the secret key leaves each of the algorithms used in GSM susceptible to an attacker's manipulation [2]. Brumley reported on a narrow pipe attack technique that exploited the weakness of the COMP-128 and which was said to have been used to recover the secret key [12]. This left the card clone-able and allowed eavesdropping, but it requires at least eight hours completing the attack.

Side channel attacks ranging from differential power analysis attack, simple power analysis attack, partitioning attacks requiring queries ranging from eight to thousands, has also been used. These query requirement makes the approach have a high data complexity and furthermore not implementable in real-time. Studies show that these side channel attacks can be guarded against by using hiding and masking of power measurements [5,13].

Other attacks types were further proposed on the algorithms used for confidentiality. These attacks were based on the fact that the protocols used on GSM also called algorithms use the shared secret key as their security baseline. So, the attacks placed on these protocols were used to recover the secret key, session key and even establish connection. The algorithms include the A5/1, A5/2, A5/3 and a not in use but already proposed A5/4 [14].

Biryukov et al. proposed a time memory data tradeoff approach by reconstructing the linear feedback shift registers used in the A5/1 algorithm [15]. This approach does not foster real time attack since a large amount of known key stream, a large data for pre-computation and storage is required for a successful attack. Although the study proposed a possible online phase of the attack, by analysis it can be said that a possible online phase of the attack would give a very low success rate due to the computational requirement and will require very expensive machines with very high speed.

More attacks were further proposed on the network signaling. Margave claims that access to the signaling network will reveal sensitive information for key recovery [16]. This claim is based on the fact that the traffic within a network operator's environment is sent as plaintext. This attack requires the presence of the attacker at the base station and very expensive equipment for implementation. On the part of the network operators, physical protection of base stations is always provided, so that access to the signaling equipment may be difficult and hence this attack can be guarded against. But, if it happens that an attacker gets access to the base station; then, this attack will be successfully carried out and used for a long time undetected.

Barkan et al. proposed an attack on A5/2 to exploit the GSM error/correction scheme. GSM uses error/correction before encryption; this makes the data have linear dependencies and by observing cipher-text the study showed that the session key could be recovered [10]. However, the pre-computational phase of the attack requires a huge amount of data more than is required for a time memory tradeoff attack. These practical obstacles make actual implementation of the attack difficult.

Dunkelman et al. proposed a related key attack on Kasumi used in A5/3 to recover the key from block cipher [17]. The study obtained the 128-bit key using chosen and related messages that may not be applicable in the specific way in which Kasumi is used on the A5/3 encryption in the 3G GSM telephony. The break was not operated in real time meaning the conversation must be intercepted, recorded, and then run through a system to break the encryption to have a suitable *.wav* file output. A5/3 used in 3G calls is not generally known to be broken outside of the intelligence agency circles. However various known cell phone vulnerabilities can make it susceptible to passive attack. With downward compatibility issues attack possible on A5/1 and A5/2 can be mounted on A5/3**.**

Gendrullis et al. proposed and implemented also time memory tradeoff attack to generate the linear feedback shift registers content for reconstructing the 64-bit session key by using generated states and discarding only possible wrong states thereby reducing the level of unsuccessful result [18]. This technique required many checking possibilities. The study revealed that the approach produced the same number of 64 bits output for more than one state. In the study, it is claimed that this occurrence is negligible but for real time implementation this may lead to a lack of confidence in this approach.

Session keys have also been recovered using brute force attack; although, with a high data complexity and almost not realizable in real time, as a large amount of input data is required to make it feasible. The required data is said to be time bound, so that if the data captured is not used to recover the key within the data validity period, then the approach must be repeated with a new captured data. Cases of this are seen in Golic, who proposed brute force attacks [19] and Kumar who investigated further [20]. It was observed that these approaches resulted in exhaustive search, which generally is known to have a high time complexity [19,20].

The result of these attacks implies that the security of networks is highly vulnerable, but most of these attacks also require a large amount of data, time and some others, expensive equipment. Hence, this research focused on secret key recovery using a malware based approach by mounting an active attack on the SIM card, performing a passive attack for validation and evaluating the computation complexity, with the hope to reduce the computational complexity.

Furthermore, this research was carried out to help network operator determine a possible vulnerable point on the SIM card and also to act as a test tool for network operators determine the extent of vulnerability on the SIM card and network.

190

Existing GSM Architecture

Establishing a connection between the phone and the network begins with the mobile station sending the International Mobile Subscriber's Identity (IMSI) number to the network operator. This number is attached to a copy of the card's secret key and a set of random challenges (RANDs) at the network provider's authentication center. The network provider sends a Random Challenge (RAND) to the SIM. This random challenge is combined with the secret key on the SIM card using the COMP-128 algorithm to generate a signed response and a session key, K_c. The generated signed response is sent to the network provider, who compares the result of the signed response (SRES) from the SIM and the copy resident at its (Network Operator) authentication center. If it matches, the network provider allows the SIM card to connect on the network, otherwise authentication is rejected.

In some cases, a temporary mobile subscriber's identity (TMSI) number can be sent to the network address in other to protect the IMSI from attackers. If the result of the SRES does not match using the IMSI in the event that the TMSI did not derive the correct signed response, the authentication process may be repeated or an authentication reject message is sent to the subscriber. Figure 2 shows the GSM authentication procedure.

Design

The proposed system is tagged GSM traffic Monitoring System (GTMS). It is designed as a simple tool with less computational complexities, to reconstruct the secret key used by a SIM card. GTMS uses a malware injection approach to intercept SIM card authentication operation. This approach does not attempt to recover the secret key when the SIM card is not carrying out the SIM card authentication, contrary to the work of researchers who attempt to crack the triple DES algorithm, because the secret key is protected with triple DES when not in use. Rather the process of mirroring begins when the secret key carries out the authentication procedure in order to mirror the authentication process.

The injection process gives way to the required authentication and communication process with the mobile station. Figure 3 describes the GTMS authentication architecture on the mobile station.

The malware performs the responsibility of the network provider by providing the required random challenge called $\mathrm{GTMS}_{\mathrm{RAND}}$. The designed system does not disregard the GSM standard. This standard ensures that certain regulations are followed before any authentication is performed.

Architecture of the proposed system

The GTMS is single tier architecture that uses the malware activities and the passive attack to mirror data. Figure 4 illustrates the connection structure of the GTMS system.

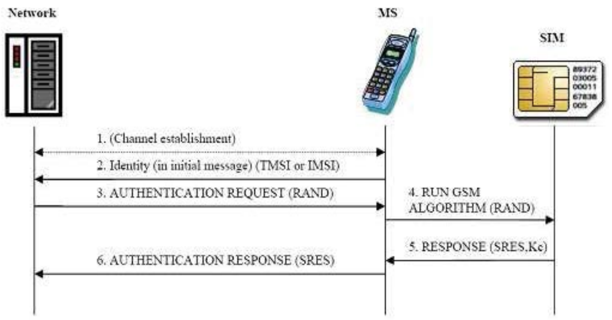
Network
MS
SIM
89372 03005 00011 67838 005
1. (Channel establishment)
2. Identity (in initial message) (TMSI or IMSI)
3. AUTHENTICATION REQUEST (RAND)
4. RUN GSM ALGORITHM (RAND)
5. RESPONSE (SRES,Kc)
6. AUTHENTICATION RESPONSE (SRES)

Figure 2: GSM authentication procedure [2].

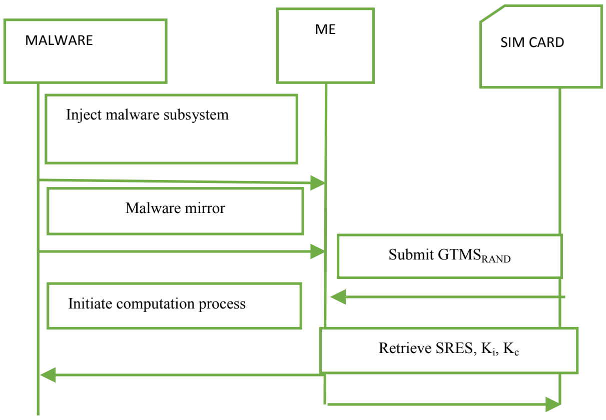

Figure 3: GTMS Communication Architecture.

The malware: The malware is first injected into the mobile equipment (ME) and then the SIM card. When this is done, the malware attempts to inject itself into the required environments manipulating the activities of the SIM/ME functionalities. Figure 5 shows the malware injections on the SIM and the mobile equipment.

The GTMS mathematical model

It applies the standard practice of a SIM/ME. However, in order to suit the expected and desired attributes for the GTMS to achieve its purpose, attempts are made to manipulate the standard characteristics of each of these functions. The GTMS is attempting to recover the secret key stored on the SIM.

The process of recovering the secret key with the use of the GTMS is a 3-tuple system Ŧ;

Ŧ={₥, ƻ, ℓ}| ₥, ƻ, ℓ are complex functions (1)

these functions have a relationship that is a nonhomogeneous second order linear differential equation as described in Equation 1.

Ŧ=f (₥)+f (ƻ)+f (ℓ) (2)

where ₥ is the malware function, ℓ is the emulator function, ƻ is the Reversing function. Each of these functions has several components that aid achieving their operations.

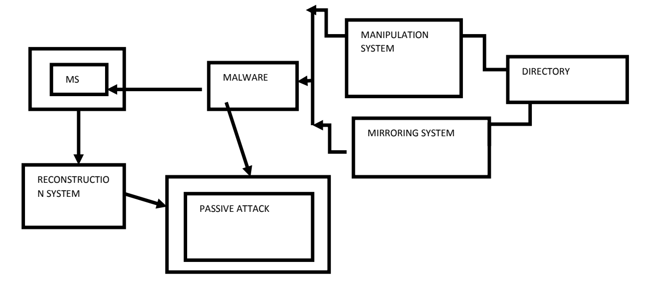

Figure 4: Connection structure of the GTMS.

The GTMS operations are broken into two main modules, namely: The key retrieval and Passive attack. Each module holds a dependent relation with each other. This paper emphasizes the key retrieval process.

The key retrieval module: The GTMS begins by firstly recovering the key using the key retrieval module. The key retrieval module is built on a 2-ary malware with characteristics of definite finite automata. The 2-ary malware is based on the theorem of a k-ary malware.

Definition: A k-ary malware is a family of k-files (some of them may not be executable), whose union constitutes a computer malware and its code operation can be sequential (serial mode) or parallel, depending on how k-constituent parts are acting either one after the other or together respectively [21].

However, in this research a 2-ary non-monolithic binary entity malware is proposed with a set of binary and non-executable files, working in a serial mode to produce the desired capture of the 128-bit secret key property. The entities of the malware are given in the relation as described in equations 3 to 7 and their attributes are transparent and silent, so that their activities are not seen as foreign to the SIM. This attribute is built in through the use of through the use of the Libthor programme resident in m_n

₥=$m_g \cup m_r$ (3)

$m_r=\{f,g\}$ (4)

$m_g=\{\{m_v \in m_g\}|m_n>m_v< m_g\}$ (5)

$m_g=m_v \cup m_n$ (6)

$m_v=\{b, c, d\}$ (7)

m_g, m_r, f, g, are the set of binary files used by the malware and m_n is the non-executable files. Here m_r indicates the mirroring system, whose

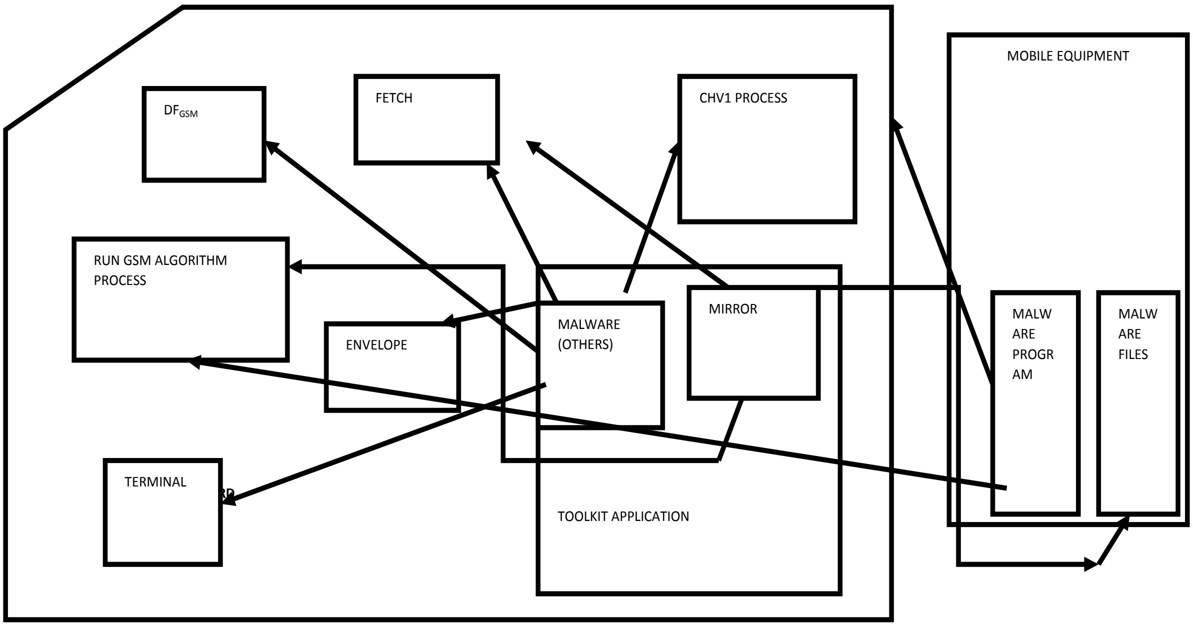

Figure 5: Malware injection on mobile station.

member properties are given asf andg . M_g is the set of executable binary m_v and non-executable file m_n, and $m_n \neq 0$.

The malware $\not{m}$ is defined such that all transparent and silent binaries and the main legal program is said to constitute the only parts of the malware. The set m_v whose members are shown in Equation 7 is the set of binary that have distinct properties. M_n, Non-executable further carries the attributes to ensure that m_v are not detectable by an antivirus, the SIM card's security system and the mobile equipment.

m_v operation: The set m_v whose members are its properties given in Equation 7 all work together to achieve the initiation of the Run GSM algorithm. This algorithm request is usually initiated by the mobile equipment after the card holder's verification 1 (CHV1) procedure is successful. It further generates the required RAND; this RAND is the input parameter for the authentication procedure. The generated RAND by the malware is tagged $GTMS_{RAND;}$ it is known to the attacker.

Assuming all properties of elements of m_v have a general property name, say P, then it can be said that the object b who is a member of m_v has the property say: kernel-land code injection. This property forces the injection of code into the mobile phone. The injected code allows the mobile equipment to listen to the malware, assuming that the malware is the subscriber's network's base transceiver station (BTS). This assumption makes the malware a fake base station, without physical structure.

The mobile equipment receives the RAND from the malware; which poses as a network. The property information of b as P(b) as shown below: P(b) → accept_network_Receive_GTMS$_{\_RAND}$.

Another member of m_v is c. Let c be a property say: the generation of the $GTMS_{RAND}$ and initiator of the next binary file. The $GTMS_{RAND}$ given to the mobile station through the mobile equipment is usually a randomly generated 128 bits value. This value is generated by the home location register (HLR) in a standard GSM setting without any integrity parameter for the SIM to validate the source of the RAND, hence the SIM card does not have any means of verifying the validity of the RAND sent. With this RAND characteristic the GTMS system uses the binary file c to generate the $GTMS_{RAND}$. The RAND generated follows the EAP-SIM authentication given by Arkko and Haverinen [22].

The value of the attribute contains two reserved bytes followed by one $GTMS_{RAND}$ that is 16 bytes long. The reserved bytes are set to zero upon sending and ignored upon reception and represents the number of $GTMS_{RAND,}$ which in the case of this research n=1. The $GTMS_{RAND}$ value was generated using the Lehmer multiplicative congruential algorithm, based on the standard minimum parameters as described in Equation 9 and 10 and the initial value called S_0.

$$X=S_{i+1}=Z \times S_i+G \bmod N \tag{8}$$

Where Z, G, N are integer parameters; Z=16807; G=1, N=128; $S_0 \geq 1$. So that S_i is given to be the sunset of the natural numbers and $S_0 \neq 0$, then there is a natural number (t)

$$T=S|S_0 \leq S_i \forall S_i \leq S \tag{9}$$

S_0 being the least element of S. the generator performs this operation eight times to generate eight hexadecimal number, which is concatenated to produce the 128 bits $GTMS_{RAND}$ as described in Equation 10

$$GTMS_{RAND} = \sum x_h \forall h=\{1,2,3,\ldots,8\} S_i \leq S; x_h=\text{hexadecimal value} \tag{10}$$

The $GTMS_{RAND}$ is stored in m_n as given

m_n=store_$GTMS_{RAND}$

Here, only a copy is stored for attack verification purpose.

The binary file c initiates the next binary file tagged; a. It employs the system of virtual machine for malware, which was developed by Anthony Desnos. These virtual machines are said to offer a powerful protection for an algorithm or anything else that would require protection against reverse engineering. It takes a piece of assembly instructions and has a simple dynamic metamorphic virtual machine very quickly to interpret.

The GTMS embeds this machine into different parts of the malware to protect them. The virtual machine is totally independent from the program. It runs an algorithm into an encapsulated object, for protecting every binary file instructions. The virtual machine uses a malicious pseudo-random number generator to hide the $GTMS_{RAND}$ stored on the mobile equipment by XORing the sequence with a 128 bit sequence. The integer constants in the $GTMS_{RAND}$ generator are protected using LibThor internal junk package.

LibThor has been proven to be useful in hiding operation code values, register offsets or anything which represents an invariant in a program [21]. The property of the binary file c is given as:

$(x_h, a)=\{\{c|P(c)\} \text{with } x_h, a \in c\}$

x_h represents the $GTMS_{RAND}$ and a is the initiation of the next binary file attribute.

The property d who is a member of the set m_v is said to have three attributes:

a) Force the SIM to perform CHV1 verification for a successful return

b) Change the SIM card's directory to DF_{GSM}, to allow initiation of the Run GSM algorithm.

c) Initiate the algorithm.

The particular binary property of P(d) is given as-

$d=\{d_i|P(d_i)$ where $i=(1,2,3,)\}$, and i represent the attributes of binary d.

The malware manipulates the standard operation in the following functionality:

Envelope:

Input: data string #content of data string "instruction to add malware functionality part of toolkit"

Output: The SIM data download is activated, meanwhile the SIM acknowledges with a 16 bytes of data.

The manipulated Envelope initiates a point-to-point download of properties c of m_v, properties g of m_r into the SIM card. It further enables changing of file directory as given in property d_i.

Terminal: The malware manipulates the function of the terminal used by the SIM card to transfer from the mobile equipment the SIM toolkit application g, b, c, d_1 and d_2.

Thus, the SIM card is expected to perform a CHV1 and present it to the mobile equipment, after this verification the mobile phone is meant to initiate the RUN GSM algorithm; if this does not begin the binary file d_3 will force the process to begin. Before the RUN GSM algorithm is initiated the b must have provided the $GTMS_{RAND}$ to the mobile equipment to transfer to the SIM card. However, d_2 should have changed the active directory to the dedicated file for GSM.

Upon initiation of the algorithm for authenticating a subscriber to the network given as:

Input: $\mathrm{GTMS}_{\mathrm{RAND}}$

Output: SRES, K_c, C

Where C is the mirrored content from the authentication process and is 128 bits based on the $\mathrm{GTMS}_{\mathrm{RAND}}$; x and the secret key K_i tagged as y.

Authentication procedure:The manipulated fetch command is used to initiate the mirror operation whose result is C and other properties. This fetch command with its characteristics described in GSM Specification allows the mirrored data to be saved in m_n and protected by LibThor internal junk packaging.

The components of m_v can hence be written as described, using the set property system, shown below,

$P(m_n)=P(b)+P(c)+P(d)$

Where,

$$P(d) = \sum_{(i=1)}^{3} Pd_i \qquad (11)$$

m_r operation: The set as given in Equation 4 are the functions for manipulating the SIM security. The f function injects the necessary code into the SIM card to manipulate the SIM card security, for the purpose of allowing the mirroring capability of the malware, g to be active. The mirroring function

$$g = \mathrm{Ref}_1(\mathrm{v}) = 2\frac{v.1}{1.1}1 - v \qquad (12)$$

$$f(\mathrm{x}) = \{\mathrm{x}, \mathrm{y} \mid \mathrm{AXx} + \mathrm{By} = \mathrm{C}\} \qquad (13)$$

$$(\mathrm{x}, \mathrm{y}) \mid \mathrm{y} = \frac{C}{B} - \left(\frac{A}{B}\right) X \qquad (14)$$

Here x and y represent the $\mathrm{GTMS}_{\mathrm{RAND}}$ and the secret key, A and B are real numbers; A, B=1, v denotes the vector of the result C being reflected, l represents any vector in the line being reflected in and v.l denotes the dot product of v with l. Using this function the malware mirrors the SIM card.

Significance of the Study

Some methods that have been used by authors include correlation attacks, side-channel attacks, guess-and-determine attacks, memory tradeoff attacks. These attack designs are dependent on solving complex mathematical equations with a number of assumptions. They recover materials essential to intercept communication, but these attacks are characterized by high computational complexities in terms of time or storage. This research worked on proffering a reduced computational complexities approach to recovering secret key required for authentication. It is a promising candidate of attack and an obvious point of concern for network operators in the security of secret key and SIM cards. This became evident as a simple point to point download of newer functionalities into a SIM card makes the SIM card vulnerable to cloning and traffic eavesdropping without having to attack the triple DES cryptographic system used to protect secret key.

References

1. Mohamed E, Agarwal B, Obkircher O, Vasa J, Vdkerti M (2009) Single-Chip multiband in CDMA/HSDPA/HSUPA/EGPRS transceiver with diversity receiver and 3G receiver paths. Solid state circuits conference digest of technical papers IEEE International, pp: 16-17.
2. Quirke J (2004) Security in the GSM system. AusMobile.
3. Qualcomm (2014) The evolution of mobile Technologies 1G to 4GLTE. 1-41.
4. Hardik M, Darpt P, Bhaumik H, Hardik M (2014) 0G to 5G mobile technology: survey. J Basic Appl Eng Res 1: 56-60.
5. Mangard S, Elisabeth O, Thomas P (2008) Power analysis attacks: Revealing the secret key of smart cards. Springer Science and Business Media, pp: 3-5 and 11-12.
6. Alese BK, Adu MK, Owa VK (2015) Cyber security in Nigeria: A collaboration between community and professionals. World Acad Sci Eng Technol - Inter J Comp Electric Auto Cont Info Eng 9: 1344-1348.
7. Brienco M, Goldberg I, Wagner D (1999) A pedagogical implementation of the GSM A5/1 and A5/2 voice privacy encryption algorithm.
8. Skorobogatov SP, Anderson RJ (2002) Optical Fault Induction attacks. Crypto Hard Embed Syst 2002: 2-12.
9. Ekadhl P, Johansson T (2003) Another attack on A5/1. Information Theory IEEE Transactions 49: 284-289.
10. Barkan E, Biham E, Keller N (2003) Instant cipher text only cryptanalysis of GSM encrypted communication. Adv Cryptol 2003: 600-616.
11. Arber C (2011) GSM Security Cryptanalysis of A5/1. Int Cent Info Tech, pp: 30-57.
12. Brumley B (2014) A3/A8 and COMP128. Special course on Cryptology T-79.514.
13. Rao JR, Rohatgi P, Scherzer H, Tinguely S (2002) Patitioning attacks: or how to rapidly clone some GSM cards. Security and Privacy proceedings IEEE symposium, pp: 31-41.
14. Barkan E, Biham E, Keller N (2008) Instant cipher text only cryptanalysis of GSM encrypted communication. J Cryptol 21: 392-429.
15. Biryukov A, Adi S, Wagner D (2001) Real time cryptanalysis of A5/1 on PC. Fast Software Encryption, pp: 1-18.
16. Margrave D (1999) GSM security and encryption. George Mason University, pp: 1-5.
17. Dunkelman O, Nathan K, Adi S (2010) A practical time attack on A5/3 cryptosystem used in third generation GSM telephony. Inter Asso Cryptol Res, p: 13.
18. Gendrullis T, Martin N, Rupp A (2008) A real world attack breaking A5/1 within hours. Crypto Hard Embed Syst, pp: 266-282.
19. Golic J (1997) Cryptanalysis of alleged A5 stream cipher. Proceeding of Eurocrypt LNCS. Springer Verlag, pp: 239-255.
20. Kumar N (2011) Investigations in bruteforce on cellular security based on DES and SAES. Inter J Comput Eng Manage 14: 50-52.
21. Eric J (1999) Report on limiting smart card constraints on UTMS. Advance security for personal communication techniques.
22. Arkko J, Haverinen H (2006) Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA).