EXAMINING SECURITY IN MOBILE COMMUNICATION NETWORKS

Johnnes Arreymbi
School of Computing and Technology
j.arreymbi@uel.ac.uk

Abstract: Due to advanced technological developments, mobile phone and other wireless device usage is increasing rapidly. The contents of the multimedia messages may be very important and confidential. Such confidentiality needs to be protected. Any interference and/or interceptions in the communication process would bring reduced system usage and disgruntled stakeholders. This paper discusses the several aspects of security of The Global System for Mobile communication or Group Special Mobile (GSM). In addition it examines how GSM protects the data from interception by authentication, encryption, and ciphering. It furthermore considers some likely flaws in these security methods and suggests possible measures to curb the flaws.

1. Introduction:

In most cases, connecting to other devices in a mobile environment requires wireless networks. Mobile computing has contributed to an increase in productivity and operational efficiency on individuals and businesses. However, the flexibility and ubiquity of such a system comes at a price – that of security.

Security is a major concern for any wireless network. Since radio signals travel through open space, they can be intercepted by individuals with the right equipments, who are constantly on the move, which makes them untraceable. Hackers are scanning airwaves and siphoning off cellular ID numbers for improper use. The security of a mobile network such as GSM includes multiple technologies that attempt to resolve authentication, integrity and identification problems. Some of these are firewalls, authentication servers, biometrics, cryptography, intrusion detection, virus protection and Virtual Private Networks.

The GSM platform which was formed in 1982 [1] is a hugely successful wireless technology. Some research showed that at the end of Jan 2004 [2] there were over 1 billion GSM subscribers across more than 200 countries. Today the world-wide figures are even more, especially in Africa, Asia and other advancing economies where mobile communication uptake has increased by approximately 65% [17, 18].

In the older analogue-based cellular telephone systems such as the Advanced Mobile Phone System (AMPS) and the Total Access Communication System (TACS) [3], cellular drop rate, interference and interception rate and general fraud on such systems were extensive and very rampant. Mostly, without any encryption [4], the voice and user data of the subscriber was in pure raw form and sent over the networks. SIM card cloning too was very easy and they together posed dangerous threat to the users. Such fatal flaws in the mobile phone and wireless technologies were all prevalent [5]. This led to development of GSM.

The prevalence of GSM technologies, together with the introduction of multimedia content delivery, provides a stable, continuous, private and secure environment for communication – audio,

SMS, MMS services - through GSM network systems [18]. But how safe and secure is the GSM technology? Can it really protect vitally important information? In this paper we will provide a brief overview of GSM, its security and encryption technologies. Furthermore, we will attempt to provide a model for GSM security optimization. The third section will look at some GSM flaws and provide possible measures to overcome them. The final section gives an evaluative critique and conclusion to this paper.

2. Encrypting GSM for security

All cellular communication operates using air waves which can fairly easily be intercepted with readily available suitable eavesdropping receivers. Considering this issue, the GSM technology integrated some security controls [6] in order to make the cellular system as secure as a fixed line phone. The system offers some level of physical security such that physical access is needed to the phone line for listening in to be possible. This kind of control measures provides better security for conversation between two mobile phone users. According to GSM specification 02.09 [6], the security functions put in place are: authentication of a user, data and signalling confidentiality and Confidentiality of a user.

Authentication of a user means that a mobile phone needs to prove that it has access to a particular network account with the operator. Data and signalling confidentiality is to make sure that all signalling and user data, such as text messaging and speech are protected against interception by means of ciphering. Meanwhile confidentiality of a user function keeps the unique International Mobile Subscriber Identity (IMSI) and prevents it from being disclosed and displayed in plaintext to avoid leaving tracks of the user. It also means that intruders cannot easily track down certain subscriber of the GSM system.

Besides some of the above security functions, there are other functions that prove to make the mobile phone more secured. The most commonly known protective system is that of the PIN which GSM system provides. In order to distribute the authentication and ciphering information throughout the network, the root key of all ciphering key generation and authentication, Ki [4] have to be distributed by another form known as vectors. This too adds another security level in our proposed security model as would be highlighted below and aims to improve the GSM security.

In managing mobile access to network system resources, it is very essential to enforce security measures. The system should be able to know who is accessing resources at what point and know the purpose of each access. Controlling access to systems is best illustrated in the AAA framework: *Authentication*, *Authorisation* and *Accounting* [20, 21]. Authentication is the ability to identify network or system users through the validation of a set of assigned credentials such as user identification number and passwords. Authorisation defines the ability of a specific user to perform certain tasks, such as creating, modifying and deleting, after authentication has taken place. And, Accounting allows it to measure and record the consumption of network or system resources. This framework adapts well in a mobile or wireless environment. The most challenging amongst the three issues in the AAA framework is authentication. The increased complexity of attacks has pushed the network society

to build up strong authentication techniques. Rather than only relying on the inadequate use of usernames and passwords, different and efficient technologies have been developed for improve security, such as RADIUS (Remote Authentication Dial up User Service), Token-based Strong authentication, 802.11i Security, Secure Socket Layer (SSL), Virtual Private Networks (VPN) and Media Access Control (MAC) Filtering. In most Instances, GSM networks utilises encryption for three purposes: authentication, encryption and key generation [7].

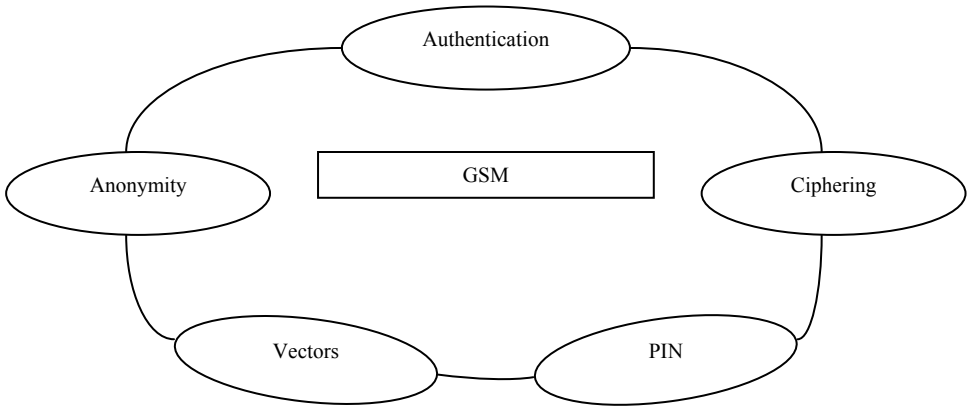

Figure 1. Proposed Model for improve GSM Security

2.1. Authentication:

Authentication service within a system is concerned with assuring that a communication is authentic. It can prohibit an unauthorized user claiming to be a bonafide mobile subscriber logging into the network [6]. In order to ascertain the position, some kind of challenge needs to be issued by the network, for which the mobile station (MS) such as mobile phone, must respond to correctly. And if all fails, the unauthorized user therefore fails to personate the bonafide subscriber because of the challenge provided in connecting to the network. Others techniques include such as the SIM card, A3 Algorithm IMSI and Ki.

The Subscriber Identity Module (SIM) card is a small smartcard with embedded micro-chip which is inserted into the GSM phone and provides the appropriate details of an account. The SIM card contains information which is necessary to gain access to a particular account. Some of which are: International Mobile Subscriber Identity (IMSI), and Individual Subscriber Authentication Key (Ki) etc. The IMSI is a sequence of 15-digit code, used to identify an individual GSM mobile station (MS) to a GSM network [9].

Ki is utilised as a highly protected secret key shared between the MS and the Home Location Register (HLR) of the subscriber's home network [10]. It is a randomly generated 128-bit number and all keys and challenges used in the GSM system are generated according to Ki. Also used in authentication is the A3 algorithm [6]. In this procedure, two 128-bit input

codes are calculated by A3 algorithm and then a 32-bit output code is generated. The most common implementations for A3 are COMP128. The authentication procedure can simply be described as: mobile phone provides the Ki to network and the latter could verify the Ki to prove the mobile phone is not the impersonated one. But, this is highly insecure because the Ki could be intercepted by an eavesdropper. If Ki is lost, the authentication will disappear because the eavesdropper will personate that subscriber by providing the same Ki.
In such situations, the GSM technology provides a better method to resolve such a problem. The network generates a 128-bit random number, RAND [10] which is 128-bit random challenge generated by the Home Location Register (HLR). It then uses the A3 algorithm to generate an authentication sign, SRES [10] which is the 32-bit Signed Response (SRES) generated by the MS and the Mobile Services Switching Center. After the generation of SRES, the network then sends the RAND to the phone. The phone respond by doing the same, generating a 32-bit SRES and then transmitting the SRES back to the network for comparison. Authentication is complete and becomes successful only when the two values of SRES are the same. This enables the subscriber to then join the network. If authentication fails the first time, the network may choose to repeat the authentication procedure with the IMSI. If that too fails, the network releases the radio connection. The mobile then considers that SIM to be invalid. Therefore, the protection of Ki is provided. And just in case an eavesdropper manages to intercept the RAND, no relevant information can be retrieved by listening to the channel because, each time, a new RAND number is generated.

2.2. Ciphering:

It is vitally important that providers keep user data and signaling data secure from interception by ciphering. The GSM system uses symmetric cryptography. In symmetric cryptography, the data is encrypted using an algorithm and the ciphering key. In GSM systems, the ciphering key is named Kc. Kc is the 64-bit ciphering key [10] and used as a Session Key for encryption of the air channel. Kc is generated by the MS from the RAND presented by the GSM network and the Ki from the SIM utilising the A8 algorithm. Like symmetric cryptography, this same Kc is needed by the decryption algorithm to decrypt the data. The idea is that the Kc should only be known by the phone and the network. If this is the case, the data is meaningless to anyone intercepting it. As earlier mentioned, the A8 algorithm uses the RAND and Ki as input to generate a 64-bit ciphering key Kc which is then stored in the SIM and readable by the phone [11]. Like the SRES, the network also generates the Kc and distributes it to the base station (BTS) handling the connection.
The A5 algorithm uses the 64-bit cipher key [12] derived from the 128-bit authentication key by the A8 algorithm in the SIM card to perform the encryption. The A5 algorithm is also 'seeded' by the value COUNT [6], which is sequentially applied to each 4.615ms GSM frame (see figure 4). Currently there are 3 algorithms defined for ciphering algorithms – A5/1, A5/2 and A5/3 [6]. A5/1 and A5/2 were the original algorithms defined by the GSM standard. A5/2 was a deliberate weakening of the algorithm for certain export regions, where A5/1 is used. In countries such as the US, UK and Australia, A5/3 was added in 2002 and is

based on the open Kasumi algorithm defined by 3GPP. The output of A5 algorithm is the cipher text which is very secure and cannot be easily decrypted by eavesdroppers.

2.3. Anonymity:

Anonymity is a process set to make it difficult to track a mobile phone user of the system. According to Srinivas [13], when a new GSM subscriber switches on their phone for the first time, its International Mobile Subscriber Identity (IMSI), for example real identity, is used and a Temporary Mobile Subscriber Identity (TMSI) is issued to the subscriber, which from then on is always used. Once ciphering has commenced the initial TMSI is allocated. The VLR controlling the LA in which the TMSI is valid maintains a mapping between the TMSI and IMSI such that, the new VLR (if the MS moves into a new VLR area) can ask the old VLR who the TMSI (which is not valid in the new VLR) belongs to [6]. The use of TMSI prevents the recognition of a GSM user by the potential eavesdropper. To track a GSM user via the TMSI, an eavesdropper must intercept the GSM network communication where the TMSI was initially negotiated. In addition, because the TMSI is frequently changed, the eavesdropper must intercept each additional TMSI changing session.
The TMSI is updated at least during every location update procedure such as when the phone changes location area (LA) or after a set period of time. The TMSI can also be changed at any time by the network. The new TMSI is sent in ciphered mode whenever possible so an attacker cannot maintain a mapping between an old TMSI and a new one [6]. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) [14] is necessary in addition to the TMSI

2.4. Authentication vectors:

In the GSM communications, the AuC (Authentication Centre), which is a part of HLR (Home Location Register), as it is well known, stores the SRES, Kc and RAND for every particular subscriber. And if the subscriber is roaming, the foreign GSM database known as VLR (Visitor Location Register) would learn and source the Ki from HLR [13]. This process is very insecure because the Ki transfers directly from HLR to VLR and can be intercepted. However, the HLR distributes authentication vectors [6], including a valid SRES, Kc and RAND for the particular IMSI, which the VLR has specified. So therefore, the transmitted data are not Kis but other authentication and ciphering information, and given protection to the Ki.

2.5. SIM card security:

Most often, the SIM itself is protected by an optional PIN code which resembles that of an ATM PIN card system [8]. Typically if a user inputs the wrong PIN code three (3) times, the system will automatically lock out and block the user from using the system again. In such instance, a PIN Unlock called PUK is required to unlock the system before any use, if the PUK is correct. And incorrectly entering the PUK code 10 times, the SIM card would be permanently blocked and refusing local access to privileged information making the SIM useless.

3. Systems vulnerabilities and Solutions:

Some of the security algorithms discussed above tend to provide the GSM system with some security, and it may seems that such a GSM system is protected absolutely. However with such technologies commonly available, the systems in turn become vulnerable and complicated and as such, the more people begin to find flaws in the GSM security.
Recently, some of these flaws are gradually been resolved by specialists in line with the improved GSM specifications. Other new technologies such as GSM 1800, HSCSD, GPRS and EDGE have been added to enhance GSM system [3]. And, the 3rd generation (3G) technologies such as UMTS [6] have also been used to improve the security in GSM. The next section will explore some of the network security issues.

3.1. Security in UMTS technology:

In the GSM network systems, it is unbelievable that the authentication procedure does not require the network to prove its knowledge of the Ki or any other authentication context to the mobile phone. Therefore, it is possible for an attacker to setup an impersonated mobile base station with the same Mobile Network Code as the user's network. And with this, all calls or text messages sent by the subscriber could easily be intercepted.
The Universal Mobile Telecommunications System (UMTS) is the world's choice for 3rd Generation wireless service delivery [15], as defined by the International Telecommunications Union (ITU). With the UMTS technology, it is near impossible for an attacker to mimic or imitate the network in terms of a 2-way authentication procedure. The procedure for which the mobile authenticates itself to the network is almost the same as GSM. But in UMTS, the network also sends an Authentication Token known as AUTN along with the RAND. The AUTN contains the MAC code, which works much like the GSM SRES but in the opposite direction. Therefore, if the MAC sent by the network does not match the MAC calculated by the SIM, the phone respond by sending an authentication reject message to the network and the connection is then terminated.

3.2. Enhancing implementation of A3/A8 Algorithms:

As earlier discussed, the common implementation of the A3 and A8 algorithms is concerned with a single algorithm - COMP128; which generates the 64-bit Kc and the 32-bit SRES from the 128-bit RAND and the 128-bit Ki input. This algorithm has been found to be insecure, because, as it is, the RANDs can provide enough information for an attacker to determine the Ki in significantly less than the ideal number of attempts. Earlier attacks based on repeated 2R attacks [6] could typically crack a SIM in approximately 217 RANDs. Increasingly, and even more so, some users have found it useful to 'clone' several of their SIMs [16] onto a single programmable smartcard with easily available technology.
The common implementation of A3/A8, COMP128 has another flaw, in that, when generating the 64-bit Kc, it always sets the least significant 10 bits of the Kc to 0 [3] this is almost certainly a deliberate weakening. This effectively reduces the strength of the data ciphering algorithm to 54 bits, regardless of which ciphering

algorithm is used. Therefore, faced with the above insecurity, the newer implementations of A3/A8 have been introduced such as COMP128-2 and COMP128-3 [6] to help alleviate the problems. So far, these algorithms have held up reasonably well, however, they are still a mystery as they are developed in secret. COMP128-2 still has the deliberate 10-bit weakening of the ciphering Kc however. COMP128-3 is the same basic algorithm without this weakening, such as a truly 64-bit Kc. In fact, the new algorithms of COMP128-2 and COMP128-3 have managed to stop SIM cloning somehow and have also made the serious over-the-air Ki extraction difficult and unfeasible, even if they do not approach the ideal strength of 2128.

3.3. Exploring A5/3, A5/1 and A5/2 algorithms:

The A5/1 output is based on the modulo-2 which is performed using an exclusive OR known as xor operation summed output of 3 LFSRs whose clock inputs are controlled by a majority function of certain bits in each LFSR. However, the attack exploits flaws [15] in the algorithm and A5/1 could be cracked in less than 1 second on a typical PC. A5/2 is a deliberately weakened version of A5/1, which has been demonstrated to be also flawed. A5/2 can be cracked on the order of about 216, and thus is even weaker than A5/1. GSM supports up to 7 different algorithms for A5 ciphering. Until recently, only the A5/1 and A5/2 algorithms were used. In 2002, GSM added a much stronger algorithm A5/3 which is based on the Kasumi core which is the core encryption algorithm for UMTS [6]. However, only few networks and handsets support this algorithm currently.

4. Conclusions:

Although new measures by which the security of GSM is protected are introduced, with time, hackers may still find ways around these measures. There can be no perfectly secure product, but one can say that GSM is the most secure, globally accepted wireless system, with public standard to date. It can be made more secured by taking appropriate security measures in certain areas of system management. Adequate management of identities in open systems networks is crucial to provide security and improve efficiency. Identity management requires an integrated and often complex infrastructure where all involved parties must be trusted for specific purposes depending on their role and function. In this paper, many algorithms have been implored to demonstrate that the mechanisms of security in the GSM specification maintain some level of security in the cellular telecommunications system. The measures used in the GSM such as authentication, ciphering and anonymity give the mobile phone users some privacy and anonymity, in addition to protecting the system from the fraudulent use. However, we have also seen some weaknesses in the security of GSM. There are flaws such as in COMP128, A5/1 and so on. These vulnerabilities could be used by attacker to intercept the contents of conversations or text messages. Some measures have also been explored to prevent these flaws to an extent and imploring new technologies such as UMTS and others improved algorithm to take care of the weakness in security of GSM.
Furthermore, with increase developments in the GSM technologies, it is very likely that, more secure methods will be

developed and used in 3G and 4G mobile network environments to give it added security.

5. References:

[1] GSM Tutorial, International Engineering Consortium, 2004, http://www.iec.org/online/tutorials/gsm/topic02.html

[2] Today's GSM, 2005, http://www.gsmworld.com/technology/gsm.shtml

[3] Priyanka Agarwal, Security of GSM System, Jan. 2005, Distribution Source: Article Warehouse.

[4] Chengyuan Peng, GSM and GPRS security, (24th Oct. 2004) http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers/peng.pdf

[5] Charles Brookson, Can you clone a GSM Smart Card (SIM)? July 2002, http://www.brookson.com/gsm/clone.pdf

[6] Jeremy Quirke, Security in the GSM system, May 2004

[7] How is encryption utilized in GSM? 2004, http://www.gsm-security.net/faq/gsm-encryption.shtml

[8] SIM card, GSM system, Chapter 7, http://www.mc21st.com/techfield/systech/gsm/g7-4.htm

[9] What is an IMEI? 2004, http://www.gsm-security.net/faq/imei-international-mobile-equipment-identity-gsm.shtml

[10] What are Ki, Kc, RAND, and SRES? http://www.gsm-security.net/faq/gsm-ki-kc-rand-sres.shtml

[11] Secure Mobile Communication, Oct. 2003, http://www.dcs.warwick.ac.uk/~esvvv/docs/specification_10-10-03.pdf

[12] Comparison of Airlink Encryptions, 2003, http://www.qualcomm.com/technology/1xev-do/webpapers/wp_Airlink_Encryption.pdf

[13] Srinivas, The GSM Standard (An overview of its security), Oct. 2004, http://www.sans.org/rr/papers/index.php?id=317

[14] Yong LI, Yin CHEN, Tie-Jun MA, Security in GSM, 2003, http://www.gsm-security.net/papers/securityingsm.pdf

[15] Biryukov, Shamir, Wagner, Real Time Cryptanalysis of A5/1 on a PC, http://www.cs.berkeley.edu/~daw/papers/a51-fse00.ps

[16] Have the A3 and A8 algorithms been broken? http://www.gsm-security.net/faq/gsm-a3-a8-comp128-broken-security.shtml

[17] International Telecommunication Union (ITU) (2004), African Telecommunication Indicators 2004. http://www.itu.int/ITU-D/ict/publications/africa/2004.

[18] Arreymbi, J. (2002), Issues in Delivering Multimedia Content to Mobile devices, In Proceedings of the 6th International Conference on Information Visualization. IEEE, Computer Society, London 2002.

[19] Paul Montague and Rai Safavi-Naini, Eds, (2005), Security workshop 2005, Conferences in Research and Practice in Information Technology, Vol. 44, Australian Computer Society, Inc.

[20] Dimitris N. Chorafas, (1997), *High Performance Networks, Personal Communications and Mobile Computing*, 109-137, Macmillan Press Ltd.

[21] James Arlin Cooper, 281-401, (1989), *Computer and Communications Security, Strategies for the 1990s,* McGraw-Hill Book Company.