Review of Short Messaging Service Security

Gurjeet Kaur,Pawansupreet Kaur/Students of M.Tech
M.Tech Students, Department of computer science.
S.B.S.College of Engg. & Technology,PTU
Ferozepur, India
gurjeetrandhawa4@gmail.com, meens399@gmail.com,

Dr. Krishan Kumar Saluja/professor
Associate Professor, Department of computer science.
S.B.S. College of Engg. & Technology,PTU
Ferozepur, India
k.saluja@rediffmail.com, k.saluja@ieee.org

***Abstract*— Short Message Service (SMS) has grown in popularity over the years and it has become a common way of communication. SMS is usually used to transport unclassified information, but with the rise of mobile commerce it has become a popular tool for transmitting sensitive information between the business and its clients. By default SMS does not guarantee confidentiality and integrity to the message content. Therefore SMS is not totally secure and reliable.**

The Short Messaging Service (SMS) is global wireless service that is used to send and receive the messages over Global System for Mobile Communication (GSM).There is no built –in procedure to authenticate and offer security for text transmitted over GSM network. The reason behind it is most of the applications for mobile devices are designed and developed without taking security into consideration. This paper describes all the existing security mechanisms in SMS and security shortfalls and various attacks on GSM networks which include Authentication, Encryption, Equipment Identification and Subscriber Identity Confidentiality, Denial of service Attacks, Brute force attack, Replay Attack as well as the manifestation of network vulnerabilities including SMS attacks, encryption attacks and security measures to prevent GSM network from these attacks.

***Keywords*- Short message service security, mobile communication, Global System for Mobile Communication, Wireless Messaging API**

I. INTRODUCTION

Short Message Service (SMS) can be defined as any text, voice, sound or image message sent over a public communications network, which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient [1]. Although SMS was originally meant to notify users of their voicemail messages, it has now become a popular means of communication by individuals and businesses. Banks worldwide, including in South Africa, are using SMS to conduct some of their banking services [2]. For example, clients are able to query their bank balances via SMS.

When sensitive information is exchanged using SMS, it is crucial to protect the content from eavesdroppers. By default, SMS content is sent over the *Global System for Mobile communications* (GSM) network in clear text form, or in a predictable format [3]. This allows an attacker with the right equipment to eavesdrop on the information that is being sent. Another problem with SMS is that the *originating address* (OA) field in the SMS header can be forged, thus allowing masquerading and replay attacks. Therefore SMS is not totally secure and cannot always be trusted. For example, there has been at least one case in the UK where SMS information has been abused by the operator employees [3].

SMS has become a popular wireless service throughout the world as it facilitates a user to be in touch with any mobile phone subscriber anywhere in the world, instantaneously and without any hassle [4].hence, it is important to prevent the SMS content from being illegally intercepted/interrupted by illegal sources as well as to ensure the origin of the message from the legitimate sender. Additionally, unencrypted SMS content during the transmission allows the mobile operator employee to read and modify the SMS content. Unfortunately, the SMS does not have any built in vetting procedure to authenticate the text or provide security for the data/text transmitted. All SMS facilities should incorporate some form of basic security mechanism in terms of confidentiality, integrity, authentication and non-repudiation of the messages before it can deemed suitable for use by the government, commercial and military services [5].

The Short Messaging Service, or SMS, is a bi-directional service to send text over wireless communication systems. It consists of a message that can be up to 160 alphanumeric characters in length. Though originally a GSM service, SMS messages are now a globally accepted service. The messages can be stored in that network until they are collected by the recipient's terminal equipment

II. SMS PACKET FORMAT

An SMS packet contains a header and a payload (see Fig. 1). The header contains information that enables the cellular network to route the SMS message to the correct recipient. The originating address (the mobile phone number of the sender) is also included in the header. The payload is the message content that is displayed on the mobile handset. The size of the payload is 140 bytes, consisting of 160 seven-bit characters, or 140 eight-bit characters, depending on the

provider [6]. Those 140 or 160 characters can comprise of alphanumeric characters or binary bytes.

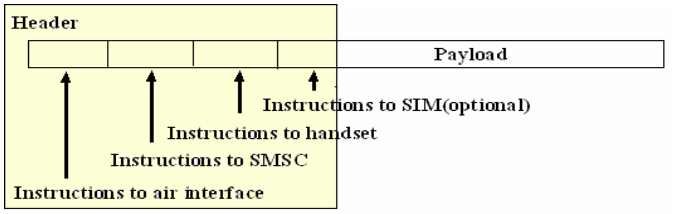

Fig.1 SMS message structure (adopted from [Clements 2003])

As shown in Table 1, each SMS is up to 140 bytes, which represents the maximum size of SMS, and each short message is up to 160 characters in length when Latin alphabets are used, where each character is 7 bits according to the 7-bit default alphabet in Protocol Data Unit (PDU) format, and 70 characters in length when non-Latin alphabets such as Arabic and Chinese are used, where 16-bit messages are used [7] [8].

TABLE I SMS LENGTH

Coding scheme	Text length per message segment
GSM alphabet, 7 bits	160 characters
8-bit data 140 octets	140 octets

III. OVERVIEW OF GSM NETWORK ARCHITECTURE

SMS messages being sent in a two-way direction between a Mobile Station1 (MS) and the Authentication Center (AUC) over a GSM network. The AUC could be the backend server belonging to an issuing bank or a merchant where it verifies the authenticity of the person who is in possession of the MS. Assuming that a user wishes to transfer money to some other account, he/she would send an SMS that will initiate this process. Therefore the SMS in this particular scenario would be sent from the MS first. The SMS message reaches the BSS via the air interface. The BSS composes of an base transceiver station (BTS) and a Base Station (BS) where a number of these base stations that form a coverage area can be connected to a Base Station Controller (BSC). The BSS transfers the SMS message to the MSC over the A interface.
It plays a major role in subscriber roaming by providing all the necessary functionality involved in registering, authentication, location updating, SMS routing and call routing for a roaming subscriber. The MSC routes the SMS to the SMSC that the AUC is connected to over the SS7 network. The connection between the AUC and the SMSC is facilitated by a GSM modem or a TCP/IP connection. It is possible to have more than one SMSC within the service provider to improve scalability.

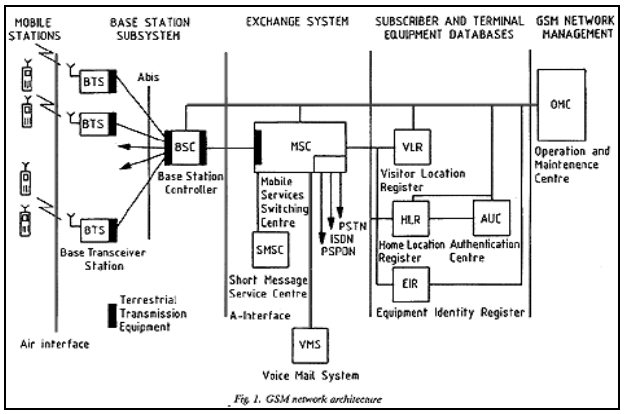

Fig.2(a) GSM Network Architecture

Once the AUC has verified the MS, it will send an acknowledgement SMS message back to the MS. Once receiving the message at the SMSC, the contents of the incoming packets are examined and if necessary, converted into the SMS packet structure (see Fig. 1).The SMSC queries a Home Location Register (HLR) to determine the location of the target MS. When the HLR locates the MS, it forwards the address of the MSC to the SMSC; otherwise the text is stored in the SMSC, until the target MS is located. The MSC then forwards the acknowledgement message to the BSS that serve the coverage area of the MS.

In case of SMS diagram of a GSM is depicted in Figure 2(a), followed by a simplified SMS message flow in Figure 2(b).

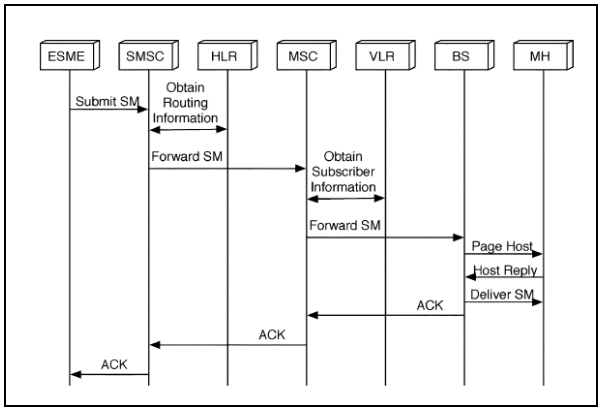

Fig.2(b)SMS Flow

IV. WMA PACKAGE FORMAT

The Wireless Messaging API (WMA) - an optional package for Java 2 Micro Edition that enables SMS messaging on Java-enabled cellular phones.WMA enables an application developer to develop an application that sends and receives an SMS. Fig.3 illustrates the components within the WMA package. None of these components includes any encryption mechanism to protect the confidentiality content of an SMS message during transit.

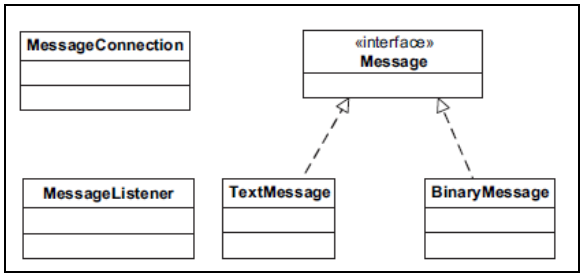

Fig .3 WMA Pavkage

V. EXISTING SECURITY MEASURES IN GSM

A. Authentication

When a new subscriber is registered in the GSM network, the mobile system is given a 128 bit subscriber authentication key K_i , and the telephone number or international Mobile Subscriber identity (IMSI) which are used in the network to identify the Mobile System. The Authentication algorithm is A3 algorithm[8].The K_i and the IMSI are stored in both the mobile and Authentication Center (AUC). This uses the K_i and IMSI, which are inputs to the A3 algorithm to calculate the 32-bit identification parameter called the Signal Response (SRES).

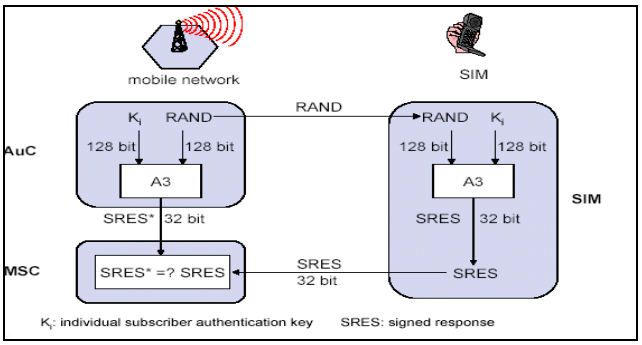

Fig .4 Authentication in GSM

In actual sense, A3 generates 128-bit output but only the first 32-bit form the SRES. SRES is calculated as a function of K and a 128-bit random number (RAND) generated by AUC as shown in Figure 4 and then stored in the HLR for use in set-up procedures. Set-up or registration will not be accepted until authentication, as in Figure 0 has been performed. Using the mobile system's IMSI, the MSC fetches the corresponding RAND and SRES from the HLR. RAND is sent to the mobile system, which uses its stored K value to calculate SRES. It then returns the calculated SRES to the MSC, where it is compared with the SRES value received from the HLR. If the values tally, the set up is accepted, if not, it is rejected.

B. Encryption.

GSM, which is a form of radio communication, can be intercepted by practically anyone in the immediate surroundings. Therefore, protection against eaves dropping is an important service in a mobile network. This is done by using an encrypted air interface both for traffic and control channels. Since encryption of voice requires digital coding, it cannot be used in analog mobile networks [9].

The encryption algorithm used in GSM voice ciphering is a stream cipher known as the A5 algorithm. Multiple versions of A5 exists which implement various levels of encryption. They are

- A5/0 which utilizes no encryption
- A5/1 which is the original A5 algorithm used in Europe
- A5/2 which is a weaker encryption algorithm created for export and used in the United States.
- A5/3 which is a stronger encryption algorithm created as part of the Third Generation Partnership Project (3GPP)[10].

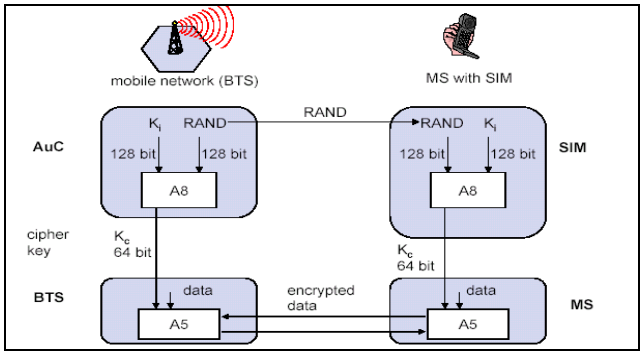

Fig.5 Encryption in GSM

In A5/1 and A5/2, voice encryption is done using the calculated session key K_c , based on K_i and RAND by the AuC, in addition to the SRES it generates as shown in Figure 7. This key is stored in the HLR together with the RAND and SRES.

The mobile system also calculates a K_c values based on both the RAND value received from the MSC and on the K_i value stored in the mobile system. If the result of the authentication is approved, the MSC will also store the encryption key in the base station (via the BSC) for use in encryption/ decryption operations. The BSC then sends a "test signal" (encryption mode command) to the mobile system. In response, the mobile system should generate an encrypted signal (encryption mode complete) which if the BSC can interpret it, permits continued signaling and communication.

C. Equipment Identification.

Equipment identification is a form of checking the mobile systems used within in the network. This is to ensure that no stolen or otherwise unauthorized mobile systems are used in the network. To this end, every mobile system in the network is provided with a tamper proof equipment number in the manufacturing process, called International Mobile Equipment

Identity (IMEI). During the set-up phase, the MSC can request this number from the mobile system and then send it on for checking in the EIR [8]**.** If the number is barred or unknown, the set-up attempt is rejected

D. Subscriber Identity Confidentiality

Subscriber identity confidentiality means that the operator tries to protect the users telephone number (the IMSI) from unauthorized tapping. A temporary mobile subscriber number (TMSI) is used in the dialogue between the mobile system and the network, except for the first contact attempt in a set-up phase. The MSC gives the mobile system a random IMSI for each set-[8].

VI. SMS SECURITY ISSUES

The initial idea for SMS usage was intended for the subscribers to send non-sensitive messages across the open GSM network. Mutual authentication, text encryption, end-to-end security, non repudiation was omitted during the design of GSM architecture. In this section we discuss some of the security problems of using SMS.

When the SMS is used as a bearer for mobile business applications which need high security, e.g. payment, shopping or mobile betting, there is a possibility that an attacker might capture the message context which includes user privacy, or amend the message causing a fraudulent transaction.

A. SMS disclosure

With no protection on confidentiality and integrity, SMS messages could be intercepted and snooped during transmission and the user privacy is at stake. Although SMS messages are encrypted when it is sent across the air, the encryption algorithm chosen for SMS message encryption must be the network-specific algorithms, such as A5 for GSM. These algorithms have been susceptible to cryptanalysis and [11] demonstrated that the secret key of A5 could be cracked in minutes. The SMS messages sent over the SS7 networks are unencrypted; moreover, most Service Providers communicate with the SMSC via SMPP SMPP (Short Message Peer to Peer protocol [12] over the Internet, and the cryptographic protection is not available for SMPP protocol. So, the attacker could read or amend the message content in some way. In addition, SMS messages are stored as plain text in the SMSC before they are successfully delivered to the intended recipient, these messages could be viewed or amended by users in the SMSC who have access to the messaging system. Furthermore, lack of protection of the BSS makes it possible to read and/or manipulate SMS messages in transit.

B. SMS spoofing

SMS spoofing is a very feasible threat because an attacker can manage to inject SMS messages into the messaging network with a 'spoofed' originator IDs. An attacker can spoof a legitimate ME by sending a SMS message from the internet with the correct headers. The ME isn't able to detect that it comes from the internet and a transaction will be conducted according to the attacker.

If an attacker knows the authenticating information of a user, he could consist in impersonating the genuine user to conduct a transaction with a legitimate AS. The authenticating information of the user can be eavesdropped easily as mentioned in Section above section.

C. Replay of messages

The possibility exists that an attacker arranges for authentication request and/or authentication response messages to be replayed. Though an attack on the reply of an authentication request message does not seem obvious, replaying an authentication response could be a more serious vulnerability. If such a replay is possible, it can be used to impersonate a legitimate user and hence authenticate a false transaction. Please note that this attack will not work if there exists an authentication request number (anti-replay mechanisms) that must be included in the response.

D. Forging Originator s Address

SMS spoofing is an attack that involves a third party sending out SMS messages that appear to be from a legit sender. It is possible to alter the originator s address field in the SMS header to another alpha-numerical string. It hides the original sender s address [13] and the sender can send out hoax messages and performs masquerading attacks.

E. SMS Encryption

The default data format for SMS messages is in plaintext. The only encryption involved during transmission is the encryption between the base transceiver station and the mobile station. End-to-end encryption is currently not available. The encryption algorithm used is A5 which is proven to be vulnerable [14].Therefore a more secure algorithm is needed.

F. Brute Force Attack

Brute Force Attack comes under cryptography technique for find an secure key from encrypted data. I.e. a brute force attack consists of trying every possible code, combination, or password until you find the right one.

In brute force attack it systematically checks all possible keys until the correct key is found. So it totally depends upon the key length as longer keys exponentially more difficult to crack the password than shorter ones. This is the most used method for cracking password [15].

G. Denial-of-Service Attack

Traditionally a denial-of-service (DoS) attack is an attempt to make a computer resource unavailable to its intended users.

One such method is to flood a network, thereby preventing legitimate network traffic. Typically the targets are high-profile web servers, and the attack attempts to make the hosted web pages unavailable on the Internet. Such an attack is extendable to any mobile environment. A mobile device is rendered ineffective should a mobile device be flooded with

this type of SMS messages. Furthermore, should a "Silent" SMS DoS attack [16] takes place on the handset; the intended victim would be oblivious to the attack. The only visible symptom would be an abnormal decline in battery charge capacity and the inability to receive calls etc. This ineffectiveness of the handset is due to SMS messages making use of the signaling layer, also used in performing other network events. Not only will a "Silent" SMS consume battery power but it will clog the signaling channel. This may be the reasoning behind the motivation in performing a "Silent" DoS attack. Primarily it may be done for economic advantage to elude another party to communicate, or may be used to ensure that a given party is not notified of some events. As another example, consider an Intrusion Detection System (IDS) that informs a network administrator via mobile phone if an attack occurs. By launching a DoS attack on the mobile phone, the network intrusion may occur for much longer without the knowledge

VII. SECURITY MEASURES FOR SECURE SMS

The following subsections describe how the Secure SMS protocol conforms to the general security requirements.

A. Confidentiality

This is achieved by encrypting the message using a symmetric secret one-time password. The one-time password is only shared between the user and the bank server. The strength of the confidentiality depends on the security strength of the passwords generation algorithm used and the strength of the ciphering algorithm used. It is assumed that only the authorized user will know his/her list of passwords and the passwords are never shared with other people.AES algorithms were considered to perform the message encryption. NSA15 has conducted a review and analysis of using AES to protect classified information. AES is an NSA approved cryptographic algorithm to be used for United States national security information and system at all classification levels. The use of 128 bits key length is approved to be sufficient to protect classified information up to the US national secret level.

B. Integrity

The message digest is the hashed value of the message content calculated server application and the mobile phone application. If the content is altered during transmission, the hashing algorithm will generate a different digest value at the receiver side. If the digests mismatch, the receiver will know that the integrity of the message has been compromised. The strength of the integrity checks depends on the strength of the algorithm used to generate the digest value and it also depends on the strength of the encryption algorithm used to hide the confidential data. A message digest is use to maintain the message integrity for each SMS message. The speed of calculating the message must be efficient and it must calculate the message digest relatively fast in the mobile phone environment. The message digest calculation algorithm used for this project is SHA1.

C. Authentication

For the receiver to authenticate the user, the user must provide his/her authentication detail(s) to the receiver. This authentication process is performed by validating the message PIN with the receiver stored PIN. The PIN is previously selected by the user when the user registers for a mobile banking account. The strength of the authentication depends on the password selection strategies used. The authentication detail (PIN) of the user is protected within the encrypted banking details. The attacker cannot read the authentication detail of the user therefore the attacker cannot use the authentication detail to perform masquerading attacks.

D. Non-Repudiation

Only the account holder and the bank server are supposed to have the one-time password. The bank server does not generate the same one-time password more than once. Therefore every onetime password is unique in the server s database. Each pair of one-time password and sequence number is only allowed to be used for a single user. Therefore the user cannot deny not sending the message because only that specific user has that unique pair of password and sequence number to encrypt the message. If the
Bank server can use the same sequence-password pair to decrypt the message, then it indicates that user must have sent the message.

E. Availability

The availability of this protocol depends on the availability of the cellular network. The time it takes for a message to be delivered depends on the density of network operator base towers.

The number of transactions that the server can handle at once depends on the hardware capability. If the server s hardware can handle multiple incoming messages then the server can perform multiprocessing to accommodate for more requests. The protocol has no restriction on the type of hardware needed. Therefore it is up to the developers to decide the hardware specifications.

F. Replay Attacks

Assuming the attacker managed to get hold of the transmitting message and he/she performs replay attacks. For every received message, the bank server needs to check for the sequence number for the specific account identifier given in the received message. If the message s sequence number does not match the sequence number from the bank database, then the message is discarded.

To further enhance replay attacks prevention, the bank server stores every received message into the database16. When a new message is received, the bank server can check it against those messages that are stored in the database.

To test for replay attacks, we deliberately send the same messages to the bank server multiple times. The server received the first message and performed the transaction, when the next identical message is received; the message is

ignored and discarded because of the received message is already exist in the database.

G. Masquerading Attacks

Masquerading attack is when the attacker pretends to be a legitimate account user. It is assume that the attacker managed to get hold of the legitimate account identifier. The attacker cannot perform banking transaction because he does not have the account identifier s PIN. We further assume the attacker managed to get hold of the user s PIN.

The attacker still cannot perform bank transaction because the attacker does not have the required One-Time Password to correctly encrypt the banking details for the bank to interpret.

To test for masquerading attacks, we created a message with a valid account identifier.

We then used an invalid One-Time Password to encrypt the banking message. When the message gets delivered to the bank server, the server cannot decrypt the message using the database password, therefore the message decryption failed. Since the message cannot be decrypted by the bank server, the bank server does not have to check for the message

PIN because it cannot be read.

H. Increasing Security against a Brute Force Attack

From the example above, PIN security could be increased by:

- Increasing the PIN's length
- Allowing the PIN to contain characters other than numbers, such as * or #
- Imposing a 30 second delay between failed authentication attempts
- Locking the account after 5 failed authentication attempts

A brute force attack will always succeed, eventually. However, brute force attacks against systems with sufficiently long key sizes may require billions of years to complete.

REFERENCES

[1] HAMMONDS, M. B. 2003. Spam – the meat of the problem. *Computer Law & Security Report* vol 19, issue 5, 388 – 391.

[2] BROWN, I., CAJEE , Z., DAVIES, D., AND STROEBEL, S. 2003. Cell phone banking: predictors of adoption in South Africa – an Exploratory study. *International Journal of Information Management*, volume 23, issue 5, 381 – 394.

[3] LORD, S. 2003. Trouble at Telco: When GSM Goes Bad. *Network Security*, issue 1, 10 – 12.

[4] C Zhang F, Yang HW, Song C (2005). A security scheme of SMS system. pp. 1333.

[5] Hossain M, Jahan A, Hussain S, Amin MM, Newaz MR, Shah SH (2008). A proposal for enhancing the security system of short message service in GSM. pp. 235-240.

[6] Croft NJ, Olivier MS. "Using an approximated one-time pad tosecure short messaging service (SMS)". In: Proceedings of thesouthern African telecommunication networks and applications conference (SATNAC); 2005. p. 71–6.

[7] G. Le Bodic, "*Mobile Messaging Technologies and Services SMS, EMS and MMS*", 2nd ed., John Wiley & Sons Ltd, (2005).

[8] (**www.ericsson.com/support/telecom/part-d/d-6-4.shtml)**

[9] (**www.ericsson.com/support/telecom/part-d/d-6-4.shtml**

[10] (**www.gsmsecurity.com/faq.shtml)**

[11] A. Biryukov, A. Shamir, D. Wagner, Real Time Cryptanalysis of A5/1 on a PC, 2000 http://cryptome.org/a51-bsw.htm. Accessed on: 13 February 2007.

[12] SMS Forum, Short Message Peer-to-Peer Protocol Specification version 5.0, http://www.smsforum.net.)

[13] Steve Lord, X-Force Security Assessment Services, and Internet: Trouble at the Telco When GSM goes bad. In *Network Security*, 2003(1):10 12, 2003

[14] Wagner, D. *GSM Cloning*. Smartcard Developer Association and ISAAC security research group. http://www.isaac.cs.berkeley.edu/isaac/gsm.html (1998); accessed 28 October 2006.

[15] http://www.tech-faq.com/brute-force-attack.html

[16] N.J Croft, M.S Olivier "A Silent SMS Denial of Service (DoS) Attack" Information and Computer Security Architectures (ICSA) Research Group South Africa