Using an approximated One-Time Pad to Secure Short Messaging Service (SMS)

N.J Croft and M.S Olivier
Information and Computer Security Architectures (ICSA) Research Group
Department of Computer Science
University of Pretoria
Pretoria
South Africa
Email: ringtingting@gmail.com

***Abstract*— Short Message Service (SMS) is a hugely popular and easily adopted communications technology for mobile devices. Yet due to a lack of understanding in its insecure implementation, it is generally trusted by people. Users conduct business, disclose passwords and receive sensitive notification reports from systems using this communication technology. SMS was an "after-thought" in the Global System for Mobile Communication (GSM) design which uses SS7 for signalling. SMSs by default are sent in cleartext form within the serving GSM's SS7 network, Over The Air (OTA), and potentially over the public Internet in a predictable format. This allows anyone accessing the signaling system to read, and or modify the SMS content on the fly.**

In this paper, we focus our attention on alleviating the SMS security vulnerability by securing messages using an approximate one-time pad. A one-time pad, considered to be the only perfectly secure cryptosystem, secures an SMS message for transport over any medium between a mobile device and the serving GSM network. Our approach does not alter the physical underlying GSM architecture.

I. Introduction

The Global System for Mobile Communications (GSM) is a common standard issued by the European Telecommunications Standards Institute (ETSI). Phase I of the GSM specification was published in 1990 and is currently the most widely used mobile phone system in the world.

The initial Short Message Service (SMS) standard was first discussed in the early 1980s but the world's first commercial SMS service was not introduced until 1992. SMS was created as part of Phase I of the GSM standard. SMS is widely adopted with approximately 1 billion SMS messages sent every day worldwide [1].

The wireless network signaling infrastructure is based on SS7. This enables signalling between functional entities in the network system and is more commonly known as the SS7 network [2]. SMS makes use of the Mobile Application Part (MAP) [3], which defines methods and mechanisms of communication in wireless networks between peer entities. However, MAP is an unencrypted protocol allowing anyone with access to the signalling system the ability to read and or modify SMS messages. With an increase of SMS messages being used to communicate sensitive information, such as banking information, and now also being used in search queries [4], the need arises to find a solution to ensure these SMS messages are secure and the content remains private.

A one-time pad [5] is a very simple yet completely unbreakable symmetric cipher where the same key is used for encryption and decryption of a message. To use a one-time pad, you need two copies of a "pad" or key which is a block of truly random data. To encrypt a message each bit of each letter in the plaintext is combined with the corresponding letter's bit in the pad in sequence using a transformation called the bitwise exclusive or (XOR). This means that two bits are taken as input and produce a single bit as output. If the key is truly random, an XOR-based one-time pad is perfectly secure against ciphertext cryptanalysis. A pad is only used once and discarded, hence the name one-time pad.

In this paper we provide a solution to the SMS security problem. Our approach is to secure an SMS message using one-time pads using shared information between the communicating peers and the serving GSM network. The keys generated from this shared information using hashing techniques, is sufficiently random for use in our approximated one-time pad. In our approach, the physical underlying GSM architecture remains unchanged.

This paper is structured as follows: Section II provides an overview of the GSM architecture and user authentication and identification. Section III outlines details of Short Message Service (SMS). In Section IV we discuss cryptosystems, focusing on hashing functions and one-time pads. We illustrate the use of hashing functions and discuss the benefits of using one-time pads and its suitability for use in securing an SMS message. In Section V we provide an approach to securing an SMS using one-time pads. Section VI concludes this paper.

II. Background

The Global System for Mobile Communications (GSM) [6] [7] is a common standard issued by the European Telecommunications Standards Institute (ETSI). The most basic service

supported by GSM is telephony; however GSM also allows data to be transported (both synchronous and asynchronous) as a bearer service [8]. The GSM standard is considered to be a "second generation" or 2G cellular system and was designed to be secure, have strong subscriber authentication and Over The Air (OTA) transmission encryption [8]. In order to understand the authentication process in GSM the respective underlying architecture needs to be understood.

A. GSM Architecture

The GSM system has two major components: the fixed installed infrastructure (network) and the Mobile Station (MS) [9]. Mobile users make use of the serving GSM network's services by communicating over a radio interface. Figure 1 illustrates the GSM architecture.

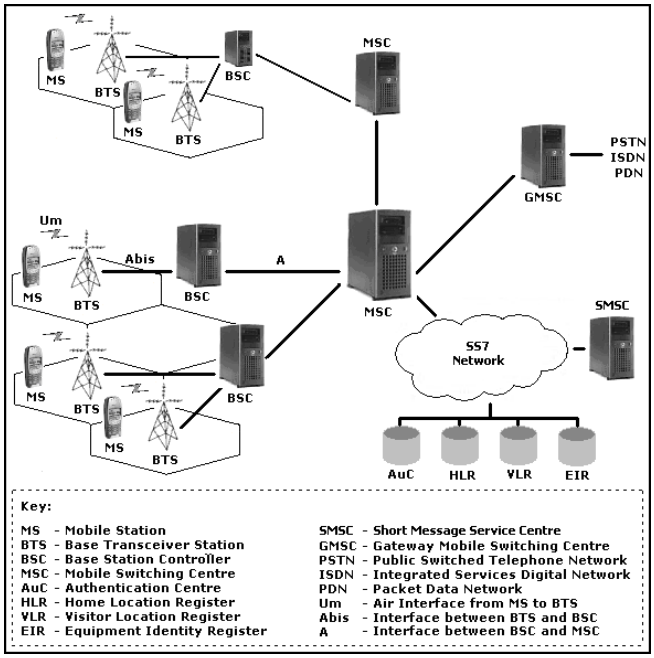

Fig. 1. GSM Architecture (adapted from [8])

The Mobile Station (MS) is the mobile phone or GSM compliant device. The Base Transceiver Station (BTS) is a radio tower or pico (single) cell with which the Mobile Station communicates. The Base Station Controller (BSC) acts as a common node between multiple BTSs and the network's backbone. The Mobile Switching Centre (MSC) performs the switching functions of the network. The MSC has an interface to one or more BSCs and to external networks. Several databases are available for control and network management. The following are usually considered to be part of the MSC:

- Home Location Register (HLR) - contains permanent (user's profile) and temporary (location information) data for all registered users with a network operator
- Visitor Location Register (VLR) - is responsible for a group of location areas and stores the data of those users who are currently in its area of responsibility
- Authentication Centre (AuC) - provides for authentication of an MS on the network and encryption of communication transmissions
- Equipment Identity Register (EIR) - registers equipment data

Signalling between functional entities in the network system uses the Signalling System Number 7. The Short Message Service (SMS) is a store and forward service, in other words, short messages are not sent directly from sender to recipient, but always via an SMS Centre (SMSC) instead. Each mobile telephone network that supports SMS has one or more messaging centers to handle and manage the SMS messages. The service center is responsible for the collection, storage, and delivery of short messages, and is outside the scope of GSM [7]. Thus the provider of the SMS service does not necessarily have to be the serving GSM operator. However, a default SMSC number is usually provided by the network operator and this number is stored at the Mobile Station (MS).

B. GSM Authentication and Identification

The Subscriber Identity Module (SIM) is a small smart card which contains both programming and information. The SIM plays an important role in identifying a user and is placed inside a GSM Mobile Station (MS). This card is issued by the network operator and contains two sorts of information namely USER-DATA and NETWORK-DATA. One of the pieces of information is the International Mobile Subscriber Identity (IMSI) which is stored securely within the SIM [10] under NETWORK-DATA. This is the unique number assigned to each GSM mobile user and is up to 15 digits long [11].

When a user switches on his or her mobile device, the International Mobile Subscriber Identity (IMSI) is used for connection to the network. The initial connection is the only time the IMSI is used, as after the connection the network assigns the user a ***random*** temporary identifier known as the Temporary Mobile Subscriber Identity (TMSI), thus hiding a user's true identity. The TMSI has local purpose, as the temporary identifier is valid only for a specific area. If the user moves to another area, the network allocates the user a new TMSI. When a new TMSI is allocated to an MS, it is transmitted to the MS in ciphertext [11]. The MS stores the TMSI on the SIM card so that when the MS is switched off the this data is not lost. The TMSI is also stored at the VLR and not at the HLR and consists of up to 32 bits (4 octets [11]). The main purpose of the TMSI is to retain the anonymity of the subscriber since the IMSI can reveal the user's true identity.

The IMSI consists of three parts, namely [12]:

1) Mobile County Code (MCC) - 3 decimal digits
2) Mobile Network Code (MNC) - 2 decimal digits
3) Mobile Subscriber Identification Number (MSIN) - 10 decimal digits

The MSIN is unique for a MCC/MNC combination.

The International Mobile Station Equipment Identity (IMEI) uniquely identifies a Mobile Station (MS) internationally (a unique serial number). The IMEI is allocated by the equipment manufacturer and registered by the network operator who stores it in the Equipment Identity Register (EIR). The EIR contains a list of all valid mobile equipment on the network and each MS is identified and authenticated by its IMEI.

The Location Area (LA) is a group of BTSs within a particular region and has its own identifier, known as Location Area Identifier (LAI). The LAI consists of the following:

- Country Code (CC)
- Mobile Network Code (MNC)
- Location Area Code (LAC)

The LAI is broadcast by the base station. The MS can determine this information by listening for the LAI and update the information in the HLR/VLR if required. Thus each user, based on location of connection to the serving GSM network, has an associated LAI which is stored at the MS on the SIM card under NETWORK-DATA information. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI to avoid ambiguities [13]. According to the GSM standards (GSM 03.04 [14] and GSM 09.02 [3]) the unencrypted SS7 communication protocol (MAP) needs to use a Mobile Network Code (MNC) to assure the reception of messages from MSs.

III. Short Message Service (SMS)

Short Message Service (SMS), is a universal text messaging system, allowing the transmission of messages up to 160 alphanumeric characters to be sent to or from a GSM Mobile Station (MS). SMS is characterized by an out-of-band packet delivery and low-bandwidth message transfer, which results in a highly efficient means for transmitting short bursts of data. Every Short Message has to pass via a Short Message Service Centre (SMSC).

The benefit of an SMS to a user centers around convenience, flexibility and the seamless integration of a complete messaging solution. SMS works on a store-and-forward basis and when received, is stored on the SIM card or on the MS's internal store.

An SMS is transferred in a connectionless packet mode over the signalling channel of the serving GSM network. Once a message is sent, it is received by a SMSC (refer to Figure 1), which must then get it to the appropriate recipient mobile device via the MSC.

Figure 2 illustrates the elements comprising an SMS message.
An SMS comprises of the following elements, of which only the User Data (the message) is displayed on the recipient's mobile device:

- Header - identifies the type of message

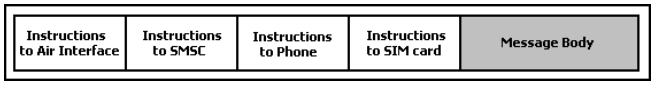

Fig. 2. An SMS Packet

- Service Center TimeStamp
- Originating Address - mobile number of the sender
- Protocol Identifier
- Data Coding Scheme
- User Data Length - the length of the message
- User Data - the message (***140 bytes***: 160 7-bit characters, or 140 8-bit characters)

Those 140 / 160 characters can comprise of words or numbers or an alphanumeric combination. Non-text based short messages (for example, in binary format) are also supported.

SMS messages travel between several network nodes before being delivered. We now describe the process flow when an SMS message is sent from one sender MS to a recipient MS.

1) The SMS message is submitted from the sender MS to the SMSC
2) After the message is processed at the SMSC, it sends a request to the HLR and receives routing information for the recipient MS
3) The SMSC sends the SMS to the MSC
4) The MSC retrieves the recipient's information from the VLR. This may include an authentication operation between the MSC and VLR
5) The MSC forwards the message to the recipient MS
6) If delivered successfully, the SMS is stored on the recipient MS's SIM card under USER-DATA
7) The MSC returns to the SMSC the outcome of the SMS delivery status
8) If requested by the sending MS, the SMSC reports delivery status of the SMS back to the sender

We now shift our attention to the intricacies of cryptography in order to provide detail on how we approach securing an SMS message.

IV. Cryptosystems: Hash Functions and One-Time Pad

A cryptosystem is a mechanism that allows two or more users to communicate in a secure manner, that is nobody but these users must be able to learn the content of the communication message. Every message, denoted by m, is subject to an encryption operation, denoted by E. The encrypted message is often referred to as ciphertext. In order to recover the original message from a given ciphertext a decryption operation, denoted by D is performed.

A hash function H is a transformation that takes a variable size input and returns a fixed-size output, often referred to as the hash value or $h = H(x)$. The basic properties of a hash function are:

- The input can be any length

- The output has a fixed length
- $H(x)$ is relatively easy to compute for any given x
- $H(x)$ is one-way meaning its difficult to invert

The MD5 [15] and SHA1 [16] algorithms are two popular algorithms for generating cryptographic hash functions. SHA1, considered the successor to MD5, produces 160-bit output while MD5 produces 128-bit output.

A perfect, or unconditionally secure cryptosystem, is an encryption technique that can not be broken even if unlimited time and computational power were present. A common example of a perfect cryptosystem is the Vernam cipher, often referred to as one-time pad.

At a character-level, all the bits in the first letter of the message m are XORed with all the bits in the first letter of the key k. This produces a binary pattern of the encrypted letter. So for example the first letter of the message m is the letter "b" and the first letter of the key k is "#" the resultant encrypted letter is the character "A" (see Figure 3).

bit sequence for [b]	bit sequence for [#]	Bitwise XOR for [A]
1	0	1
1	1	0
0	0	0
0	0	0
0	0	0
1	1	0
0	1	1

Fig. 3. Example: letter [b] XORed with letter [#] produces encrypted letter [A]

The one-time pad has the following requirements, namely:

- Each key k is used only once
- The key k used to encrypt a message m is at least as long as m, that is $length(k) \geq length(m)$
- Each key k is random and unpredictable

If these requirements are satisfied, the one-time pad is an unconditionally secure cryptosystem. However, the one-time pad has some associated difficulties in its practical implementation. These include the fact that a new truly random secret key must be issued prior to every communication and must be significantly long for large messages. Again, once a key is generated it must be distributed between the communicating parties. This aspect is commonly referred to as the key distribution problem, as the key k used in the encrypting and decrypting of messages m must only be shared between the communicating parties.

An SMS is short in nature and the key distribution problem is alleviated by the underlying serving GSM network architecture (using TMSI) thus making one-time pads an ideal candidate for the securing of an SMS.

V. Securing an SMS using One-Time Pads

It is important to understand that security features Over The Air (OTA) interface and those present in the GSM fixed network are independent of each other. The network security features do not continue past the BTS. This contrasts to the air interface which is a medium accessible by anyone with the right air interface equipment available to them. The only alternative to protect data privacy in SMS messages involves encrypting the message body at the sending device and then decrypting the message at the receiving device. Such an approach protects the data for the entire duration of its transit through the network, although such an implementation of such a system is highly difficult. In order to be compliant with the all flavours of SMS, the encryption algorithm must possess three attributes, namely:

1) The encrypted message must be in the form of ciphertext in order to meet the SMS message body standards
2) The encryption algorithm cannot alter the size of the message, since that would cause initially large messages to exceed the maximum allowed size after encryption
3) Simple and computationally inexpensive

One-time pads comply with all these requirements, however a random pad computation is needed that exists at both the MS and the serving GSM network in order to encrypt and decrypt the SMS message.

A. Random Key Generation

From section III we recall that an SMS User Data (the message) is 140 bytes long. The message body thus contains 1120 bits (140 x 8) of data which exists in cleartext form. From section IV, the SHA1 hash algorithm from variable length input produces 160-bit output. For the simple reason that one-time pads require the key k used to encrypt a message m to be at least as long as m, we conveniently segment the SMS User Data into seven sections (160-bit blocks)$(1120 \div 160 = 7)$. We generate an approximate one-time pad as the key generation is based on random and known, shared network information. If the message body is less than 140 bytes in length, we apply padding techniques so as to ensure 160 bit blocks upon message segmentation. This is however outside the scope of this paper. The first approximate one-time pad is generated as follows,

$$k_1 = SHA1(IMSI;\, TMSI;\, IMEI;\, LAI) \qquad (1)$$

where k_1 is the output of the SHA1 hash of inputs IMSI, TMSI, IMEI and LAI. The TMSI remains the only random input into the key generation and thus the key is considered an approximated one-time pad. Although a 32-bit random key is insufficient for a strong cryptosystem, with the addition of shared information between the MS and GSM network (only known by the user and the network), the probability of an interception from an eavesdropper is minimal.

Once a TMSI has been used in the generation of the approximate one-time pad, the serving GSM network must discard the used TMSI and allocate a new TMSI number which is transmitted to the MS in ciphertext [11]. Thus for each new SMS message sent, a new approximated one-time pad is generated (k_1).

We use key expansion techniques in generating the remaining keys required to encrypt the six segmented 160-bit blocks. The remaining expanded keys are generated as follows,

$$k_i = SHA1(k_{i-1}) \quad (2)$$

where ($i = [2; 7]$). We have generated an approximated 160-bit one-time pad and six expanded keys in order to encrypt the seven segments of the SMS message body.

B. Applying the One-Time Pad

By XORing the first User Data segment, denoted by s_1, with the approximate one-time pad k_1 we produce an encrypted segment, denoted by e_1. Each encrypted segment e_1 is a 160-bit block of ciphertext. We repeat this process for the remaining six segments and six expanded keys, refer to Figure 4.

Fig. 4. Encrypting the segmented SMS User Data using an approximated one-time pad and six expanded keys

In order to decrypt the SMS message, the k_1 to k_7 is replicated at the serving GSM network. The serving GSM network is able to do this as it shares IMSI, TMSI, IMEI, LAI with the MS.

C. Secure SMS Flow Path

To provide a secure end-to-end SMS solution in the current GSM architecture is extremely difficult given its current infrastructure. MSs are unable to authenticate each other in GSM communications and rely on the serving GSM network for authentication (AuC) and switching (MSC) of messages. GSM requires that a subscriber trusts his/her service provider [17]. Therefore our secure SMS flow path is subdivided into a link from the sender MS to the GSM network and from the GSM network to the recipient MS. These two individual links are encrypted specifically for each MS. The sender and recipient of an SMS are required to generate an approximate one-time pad and encrypt/decrypt the SMS using this pad as well as the six expanded keys. By the same token, the GSM network generates the same key set for each MS (sender and recipient) in providing a virtual end-to-end secure path.

Figure 5 illustrates the process flow when a sender MS sends a secure SMS to a recipient MS. The MSC is an intermediary which decrypts the incoming SMS message. It then locates the recipient via an HLR request (and VLR request if required) and encrypts the SMS message specifically for the recipient (IMSI; TMSI; IMEI; LAI). Upon receiving the SMS message the recipient must generate the approximate one-time pad and six expanded keys in order to decrypt the message, after which the message is decrypted and stored on the MS's SIM card. An acknowledgement of the received SMS is returned to the MSC. The MSC may forward the delivery status of the SMS message back to the sender's MS upon request.

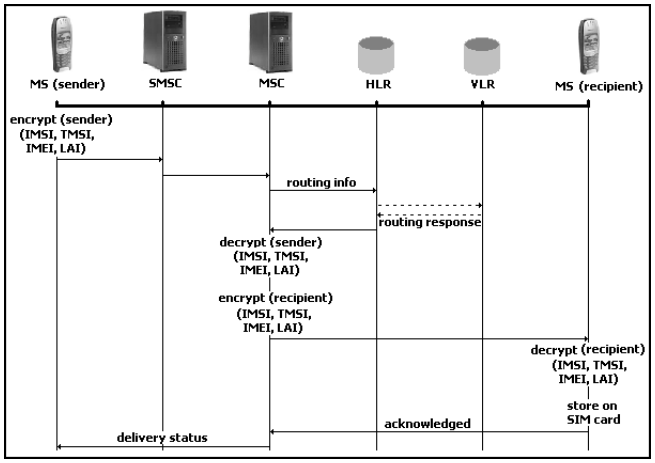

Fig. 5. Secure SMS Flow path (MS_{sender}-to-MSC, MSC-to-$MS_{recipient}$)

The SMS message resides as a plaintext message at the MSC, this allows legal authorities access to the message if required. The MSC is thus prone to attacks, however, as the MSC is core to any GSM network operator we assume the MSC is sufficiently secure from outside attacks.

VI. Conclusion

In this paper we have presented a means to securing SMS messages, which at present are inherently insecure. We devised an approach using approximated one-time pads and illustrated the secure flow of an SMS message between the sender and recipient MS. With one-time pads considered an unbreakable symmetric cipher, and the key distribution problem eliminated, our approach allows for secure messaging at an acceptable level while not physically altering the underlying GSM network.

Future work includes investigating the speed and computational complexity for a Mobile Station in generating the approximated one-time pad and the six expanded keys.

References

[1] GSM Association, "SMS (Short Message Service)," Web reference, http://www.gsmworld.com/yechnology/sms. Accessed May 2005.
[2] Y. B. Lin, "Signaling System Number 7," *IEEE Potentials*, pp. p. 5–8, August 1996.
[3] GSM Recommendation 09.02, "Mobile Application Part (MAP) Specification," European Telecommunications Standards Institute.
[4] K. R. R. Schusteritsch, S. Rao, "Mobile Search with Text Messages: Designing the User Experience for Google SMS," in *Technology, Safety, Comminity (CHI)*, Conference on Human Computer Interaction. Portland, Oregon, USA: ACM, April 2005, pp. 1777–1780.
[5] B. Schneier, *Applied Cryptography: Protocols, Alorithms and Source Code in C*. Wiley Computer Publishing, John Wiley and Sons, Inc, 1996.
[6] M. Mouly and M. Pautet, "The GSM system for mobile communications, cell & sys," 1992.
[7] M. Rahnema, "Overview of GSM system and protocol architectures," *IEEE Communications magazine*, April 1993.

[8] N. Croft, “Secure Interoperations of Wireless Technologies,” Masters Dissertation, University of Pretoria, School of Computer Science, October 2003.
[9] E. T. . 929, “Digital cellular telecommunications system (Phase 2); Security related network functions,” European Telecommunications Standards Institute, November 1999.
[10] GSM Recommendation 02.09, “European Digital Telecommunications System (Phase 2+); Security Aspects; (GSM 02.09 version 6.1.0 Release 1997),” European Telecommunications Standards Institute.
[11] GSM Recommendation 03.03, “European Digital Telecommunications System (Phase 2+); Numbering, addressing and identification (GSM 03.03),” European Telecommunications Standards Institute.
[12] V. K. Garg, *Principles and applications of GSM*. Prentice Hall PTR, 1999.
[13] GSM Recommendation 03.03, “European Digital Telecommunications System (Phase 2+); Security related network functions (GSM 03.20 version 8.0.0 Release 1999),” European Telecommunications Standards Institute.
[14] GSM Recommendation 03.04, “Signaling Requirements Related to Routing of Calls to Mobile Subscribers,” European Telecommunications Standards Institute.
[15] R. Rivest, “The MD5 Message-Digest Algorithm,” Internet Engineering Task Force, RFC 1321, April 1992.
[16] National Institute of Standards and Technology, NIST FIPS PUB 180-1, “The Secure Hash Algorithm (SHA-1),” US Department of Commerce, Tech. Rep., April 1995.
[17] N. Croft and M. Olivier, “Using a Trusted Third Party Proxy in achieving GSM Anonymity,” in *South African Telecommunication Network and Applications Conference*. SATNAC, September 2004.

Neil Croft Neil Croft is a PhD Computer Science student at the University of Pretoria. His research interests include security and privacy in current and next generation wireless communication networks. He completed his Masters degree at the University of Pretoria in October 2003 and undergraduate studies at the Rand Afrikaans University in 2001.