Hybrid Compression Encryption Technique for Securing SMS

Tarek M. Mahmoud Tarek@minia.edu.eg
Faculty of science/ Department of Computer Science Minia University El Minia, Egypt

Bahgat A. Abdel-latef Dr_bahgat2005@yahoo.com
Faculty of science/ Department of Computer Science Minia University El Minia, Egypt

Awny A. Ahmed awny_ahmed70@yahoo.com
Faculty of science/ Department of Computer Science Minia University El Minia, Egypt

Ahmed M. Mahfouz AhmedMahfouz@minia.edu.eg
Faculty of science/ Department of Computer Science Minia University El Minia, Egypt

Abstract

Mobile communication devices have become popular tools for gathering and disseminating information and data. When sensitive information is exchanged using SMS, it is crucial to protect the content from eavesdroppers as well as ensuring that the message is sent by a legitimate sender. Using an encryption technique to secure SMS data increases its length and accordingly the cost of sending it. This paper provides a hybrid compression encryption technique to secure the SMS data. The proposed technique compresses the SMS to reduce its length, then encrypts it using RSA algorithm. A signature is added to the encrypted SMS for signing it to differentiate it from other SMS messages in SMSINBOX. The experimental results which are based on Symbian OS show that the proposed technique guarantees SMS data security without increasing its size.

Keywords: Mobile Communication Devices, Short Message Service, compression, encryption, Symbian Operating System

1. INTRODUCTION

Mobile communication devices have become commonplace during the past few years, integrating multiple wireless networking technologies to support additional functionality and services. One of the most important developments that have emerged from communications technology is SMS. It was designed as part of Global System for Mobile communications (GSM), but is now available on a wide range of network standards such as the Code Division Multiple Access (CDMA) [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 are using SMS to conduct some of their banking services. For example, clients are able to query their bank balances via SMS or conduct mobile payments. Also, people sometimes exchange confidential information such as passwords or sensitive data amongst each other [2].

SMS technology suffers from some risks such as vulnerabilities, eavesdroppers and unauthorized access [3]. So, we need to find a solution to ensure that these SMS messages are secure and their contents remain private, without increasing their lengths.

This paper provides a solution to this SMS security problem. Our approach is to secure the SMS message using Hybrid Compression Encryption (HCE) system. The proposed technique compresses the SMS to reduce its length, then encrypts it using RSA algorithm. A signature is added to the encrypted SMS for signing it to differentiate it from other SMS messages in SMSINBOX.

This paper is structured as follows: Section 2 gives an overview of Short Message Service (SMS). Section 3 provides some details of SMS security. The Proposed Technique used for Securing SMS is introduced in section 4. Section 5 shows our experimental results. Finally, conclusion and future work are presented in section 6.

2. Short Message Service (SMS)

SMS is a communication service standardized in the GSM mobile communication systems; it can be sent and received simultaneously with GSM voice, data and fax calls. This is possible because whereas voice, data and fax calls take over a dedicated radio channel for the duration of the call, short messages travel over and above the radio channel using the signaling path [4]. Using communications protocols such as Short Message Peer-to-Peer (SMPP) [5] allow the interchange of short text messages between mobile telephone devices as shown in Figure 1 that describe traveling of SMS between parties.

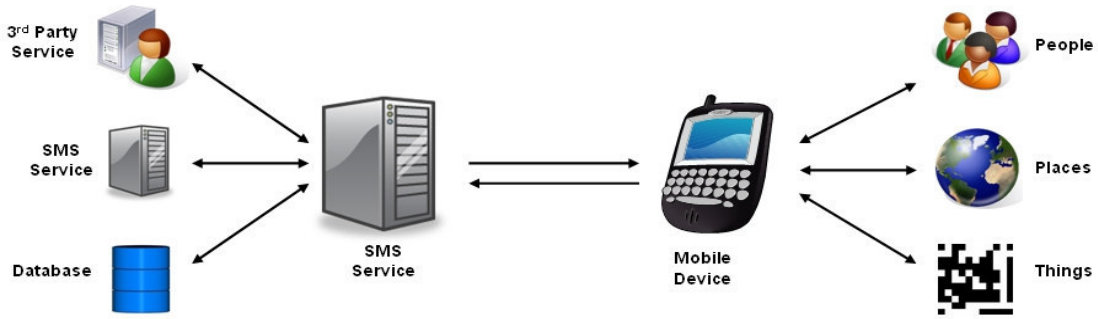

FIGURE 1: The basic of SMS system.

SMS contains some meta-data [6]:

- Information about the senders (Service center number, sender number)
- Protocol information (Protocol identifier, Data coding scheme)
- Timestamp

SMS messages do not require the mobile phone to be active and within range, as they will be held for a number of days until the phone is active and within range. SMS are transmitted within the same cell or to anyone with roaming capability. The SMS is a store and forward service, and is not sent directly but delivered via an SMS Center (SMSC). SMSC is a network element in the mobile telephone network, in which SMS is stored until the destination device becomes available. Each mobile telephone network that supports SMS has one or more messaging centers to handle and manage the short messages [4].
SMS message packets are simple in design. The structure of SMS packet is shown in Figure 2 [2].

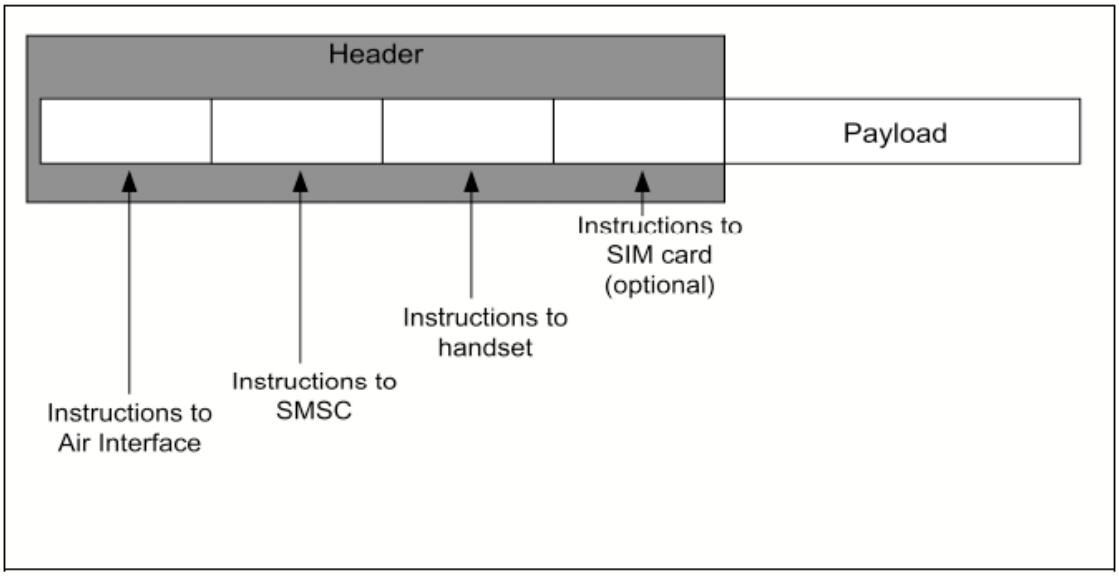

FIGURE 2: SMS Message structure

An SMS comprises of the following elements, of which only the user data is displayed on the recipient's mobile device:
• Header - identifies the type of message:
- Instruction to Air interface
- Instruction to SMSC
- Instruction to Phone
- Instruction to SIM card

• User Data - the message body (payload).
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].

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

USC2, 16 bits	70 complex characters

TABLE 1: Relation between coding scheme and text length.

3. SMS security

SMS travels as plain text and privacy of the SMS contents cannot be guaranteed, not only over the air, but also when such messages are stored on the handset. The contents of SMS messages are visible to the network operator's systems and personnel. The demand for active SMS based services can only be satisfied when a solution that addresses end-to-end security issues of SMS technology is available, where primary security parameters of authentication, confidentiality, integrity and non-repudiation are satisfied [9,13].

Authentication is concerned with only specific users with specific combination of device, application, memory card, and SIM card that are allowed to access corporate data. This way the users or unauthorized persons cannot change any part of the combination to obtain access to sensitive data. Confidentiality is about ensuring that only the sender and intended recipient of a message can read its content. Integrity is concerned with ensuring that the content of the messages and transactions not being altered, whether accidentally or maliciously. Non-repudiation is about providing mechanisms to guarantee that a party involved in a transaction cannot falsely claim later that he/ she did not participate in that transaction[14].

An end-to-end key based encryption technology for SMS plugs the gaps in transit security of SMS. Authentication added for resident SMS security access together with encryption, addresses the confidentiality issue of SMS technology. Added features of message integrity and digital signing of SMS address integrity and Non Repudiation for SMS technology[15].

4. The Proposed Technique for Securing SMS

In this section, we describe the proposed technique used to secure SMS without increasing its length. The two main steps of this technique are the compression and encryption processes. SMS Compression is the process of encoding SMS information using fewer bits than an unencoded representation. The purpose of this step in the proposed technique is reducing the consumption of expensive resources and reducing SMS length. SMS encryption is the art of achieving security by encoding messages to make them non-readable.

The steps of the proposed technique can be described as follows:

Step 1: Get SMS.
Step 2: Determine the SMS recipient.
Step 3: Compress the SMS.
Step 4: Check the compressed SMS length.
4.1 If it is greater than 145 characters then divide it into more than one according to its length such that each message is 145 characters to satisfy the message length limit imposed by the proposed technique.
Step 5: Encrypt the compressed SMS using RSA algorithm.
Step 6: Add signature to the SMS.
Step 7: Send the SMS.

In Step 4, restricting the SMS length in the proposed technique to 145 characters is necessary for the encryption process. We have conducted many experiments to determine the length of SMS cipher (encrypted) text. Table 2 illustrates the experimental results for the relation between the RSA Modulus bits, maximum number of SMS plain text and length of output encrypted characters. According to these results, we selected the RSA Modulus size to be 1248 bits as optimal value for the proposed technique, so the output cipher text will be 156 characters and the

maximum input characters will be 145. As mentioned in section 2, the standard SMS length is 160 characters.

RSA Modulus Size (bits)	Number of Input Characters Range	Length of Output Encrypted Character
256	1 – 21	32
512	1 – 53	64
1024	1 – 117	128
1248	1 – 145	156
2048	1 – 245	256

TABLE 2: The relation between RSA Modulus bits, maximum number of Input characters and length of output encrypted characters

In step 5, encrypting the SMS is based on RSA algorithm [10] [11].
The steps of this algorithm can be described as follows:

Step 1: choose two large primary numbers P and Q
Step 2: calculate N=P*Q
Step 3: select the public key (i.e. the encryption key) E, such that it is not a factor of (P-1) and (Q-1)
Step 4: Select the private key (i.e. the decryption key) D, such that the following equation is true (D*E) mod (P-1) * (Q-1) =1
Step 5: For encryption, calculate the cipher text CT from the plain text PT as follows CT=PT^E mod N
Step 6: Send CT as the cipher text to the receiver
Step 7: For decryption, calculate the plain text PT from the cipher text CT as follows PT=CT^D mod N

Figure 3 illustrates the SMS format after applying the proposed technique. It contains 4 characters as a signature and 156 characters as encrypted SMS data.

4 Signature	156 Cipher text

FIGURE 3: SMS Format after applying the proposed technique.

5. Experimental Results

This section presents the results of evaluating the efficiency of the proposed technique that is based on Symbian OS [12]. We consider the SMS length as a criterion to evaluate the performance of the proposed technique. The main purpose of the proposed technique is to secure SMS. We achieved this by compressing the SMS data to reduce its length then encrypting it to guarantee its security.

Table 3 shows a comparison between SMS length before and after the compression step. The 1st column contains some SMS samples, the 2nd column represents the total number of SMS characters before the compression process, and the 3rd column contains the total number of SMS characters after compression.

SMS Sample	Total number of SMS characters before compression	Total number of SMS characters after compression
#There are "men" like mountains "high" friend "honor" comradely "warranty" communicate with them "right and duty of the length of time" forgotten "impossible".	160	125
Source, Name : ahmed Mahfouz Password : 02034112 Card Number : 2400139 Account Number : 0111149 Operation : withdrawal Value : 1000$ Destination, Name : MobiTech Account Number : 0111133	185	142
Dear Sir this data are important for you so take your precautions-- ----------name : ahmed Muhammad balance : 100000 your password : 02710101 ----------	225	119

TABLE 3: Comparison between SMS length before and after Compression

Table 4 illustrates the results obtained after applying the proposed technique. The 1st column contains SMS samples, the 2nd column represents the total number of SMS characters before the encryption process, the 3rd column contains SMS length after the compression process, the 4th column contains the percentage of compression phase, and the 5th column contains message length using the proposed technique.

Message	Length of original Message	Length of compressed Message	Percentage of compression phase	Message length using the proposed technique
#There are "men" like mountains "high" friend "honor" comradely "warranty" communicate with them "right and duty of the length of time"	160	125	22%	156

forgotten "impossible".				
Source, Name : ahmed Muhamed Password : 02034112 Card Number : 2400139 Account Number : 0111149 Operation : withdrawal Value : 1000$ Destination, Name : MobiTech Account Number : 0111133	185	142	23%	156
Dear Sir this data are important for you so take your precautions ---------- name : ahmed Muhammad balance : 100000 your password : 02710101 ----------	225	119	47%	156
Your account 'Save 1' was credited with $999.98 on Wed 22 Nov 2006 Ref.2390809CR Call 800800 for assistance, if required. Thank you for SMS Banking with ABC Bank.	165	145	12%	156
Salary has been credited to your A/C BAL A/C NO. Balance in A/C xxxxx3329 as of 06 Aug 2009 is INR /908.8/. Thank you for SMS Banking with ABC Bank.	150	135	10%	156
xyzBank, user test Account Number:9820209954 Available balance in A/C xx310 On 04-Nov 2008 05:30 Is Rs. 50000 Thank you for SMS Banking with ABC Bank	158	141	11%	156
Peace be upon you Dear,Muhammed Key 1 : A2HBN - 3SJKL - 7HBN6 - OIKML - YPL9N - OPF8V - TRDCV - 7HJ4D Key 2 : K8DFF - BN4KI - KSLOM - QPOCD - AOPED -\x01\x33IOMN - 8GVFD	166	144	13%	156
Peace be upon you Name : Ahmed Muhamed Account Number : 056789034 Operation type : withdrawal Balance : 60000 Value : 10000 Outstanding Account : 40000	241	163	32%	Split into two messages

on 15-Aug 2009 06:45 ---------- SMS services center.				

TABLE 4: Comparison between SMS lengths using compression and the proposed technique

It is clear from Table 4 that using the proposed technique for securing SMS messages caused a considerable reduction in their lengths equal 21% approximately on average. Also, the length of compressed message depends on its contents. It should be noted that the last message in this table has been split into two messages because its length is greater than 145 characters.

6. Conclusion and future work

In this paper a new hybrid technique for securing SMS is introduced. The proposed technique combines the compression and encryption processes. The proposed technique compresses the SMS data using a lossless algorithm. After this step the compressed SMS data is encrypted using RSA algorithm. The advantage of this technique is achieving the protection criteria such as confidentiality and authenticity between two communication parties and at the same time decreasing the message lengths. The experimental results show that SMS length does not exceed the standard SMS length using the proposed technique compared with the technique that uses only the RSA encryption process to secure SMS. Future work is required to apply the proposed technique to other mobile operating systems and services.

REFERENCES

1. SMS document, Nokia, (2009, June). Available:http://wiki.forum.nokia.com/index.php/SMS
2. J. Li-Chang Lo, J. Bishop and J. Eloff. *"SMSSec: an end-to-end protocol for secure SMS"*, Computers & Security, 27(5-6):154-167, 2007.
3. P. Traynor, W. Enck, P. McDaniel and T. La Porta. *"Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks"*, IEEE/ACM Transactions on In Networking, 17(1):40-53, 2009
4. GSM document, Short Message Service, (2009, July). Available: http://www.gsmfavorites.com/documents/sms/
5. SMS peer-to-peer protocol, Wikipedia, (2009, May). Available: http://en.wikipedia.org/wiki/Short_message_peer-to-peer_protocol
6. PDU-encode-decode, thought works, (2009, July). Available: http://twit88.com/home/utility/sms-pdu-encode-decode
7. N. Croft and M. Olivier, *"Using an approximated One Time Pad to Secure Short Messaging Service (SMS)"*, In Proceedings of the Southern African Telecommunication Networks and Applications Conference. South Africa, 2005
8. G. Le Bodic, "*Mobile Messaging Technologies and Services SMS, EMS and MMS*", 2nd ed., John Wiley & Sons Ltd, (2005).
9. SMS vulnerabilities and XMS technology, Network Security Solutions, (2009, July). Available: http://www.mynetsec.com/files/xms_mobile/SMS_Vulnerabilities_XMS_Technology_White_Paper.pdf
10. Atul Kahate, "*Cryptography and network security*", 3rd ed., Tata McGrawHill, (2003).
11. David Pointcheval, RSA Laboratories' CryptoBytes, "*How to Encrypt Properly with RSA*", Volume 5, No.1, Winter/Spring 2002, pp. 9-19.
12. Symbian developer library, Symbian Software Ltd, (2006, January). Available: https://developer.symbian.com/main/documentation/sdl/;jsessionid=D059D9E1944BD96B3FAA3A61E42E7FD7.worker1
13. Anita & Nupur Prakash, *"Performance Analysis of Mobile Security Protocols: Encryption and Authentication"*, International Journal of Security, Volume (1) : Issue (1), June 2007.
14. Bhadri Raju MSVS, Vishnu Vardhan B, Naidu G A, Pratap Reddy L & Vinaya Babu A, *"A Noval Security Model for Indic Scripts - A Case Study on Telugu"*, International Journal of Computer Science and Security, (IJCSS) Volume (3) : Issue (4), August 2009.

15. Jayaprakash Kar & Banshidhar Majhi, *"An Efficient Password Security of Multi-Party Key Exchange Protocol based on ECDLP",* November 2009.