Volume 5, No. 5, May 2014
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

AN APPROACH TO ENHANCE THE MOBILE SMS SECURITY

Sharad Kumar Verma[1] and Dr. D.B. Ojha[2]

[1]Research Scholar, Department of CSE, Mewar University, Chittorgarh, Rajasthan, India
sharadverm@gmail.com
[2]Director Research, Mewar University, Chittorgarh, Rajasthan, India
ojhabrat@gmail.com

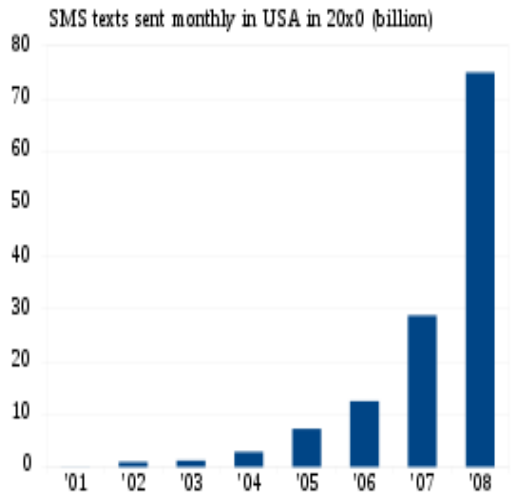
Abstract: Short Message Service (SMS) is a text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages. SMS does not have any built-in procedure to authenticate the test and offer security for the text transmitted as data, because most of the applications for mobile devices are designed and developed without taking security into consideration. In this paper, we combine two security schemes i.e. Caesar Cipher and one time pad that provide much more security for the text transmitted between different mobile phone subscribers

INTRODUCTION

Various types of tools have been created to make human communications simpler and faster. The most significant communication tool is the modern telephone which was first invented by Sir Alexander Graham Bell in the 19th century. Since then, communication devices have evolved into very advanced and sophisticated tools. Mobile technology is mostly preferred by 6 Billion mobile subscribers equating to more than 87% of world population. There are various functions provided by Mobile phones such as make and receive call, SMS, MMS, video calling, Internet, mp3, camera, games etc.

Short Message Service (SMS) is getting more popular now-a-days. SMS was first used in December 1992, when Neil Papworth, a 22-year-old test engineer used a personal computer to send the text message "Merry Christmas" via the Vodafone GSM network to the phone of Richard Jarvis in the UK. The GSM is optimized for telephony, since this was identified as its main application. The key idea for SMS was to use this telephone-optimized system, and to transport messages on the signaling paths needed to control the telephone traffic during time periods when no signaling traffic existed. In this way, unused resources in the system could be used to transport messages at minimal cost.

Short message service is a mechanism of delivery of short messages over the mobile networks. It is a store and forward way of transmitting messages to and from mobiles. The message (text only) from the sending mobile is stored in a central short message center (SMS) which then forwards it to the destination mobile. This means that in the case that the recipient is not available, the short message is stored and can be sent later. Each short message can be no longer than 160 characters. These characters can be text (alphanumeric) or binary Non-Text Short messages. An interesting feature of SMS is return receipts. This means that the sender, if wishes, can get a small message notifying if the short message was delivered to the intended recipient. Since SMS used signaling channel as opposed to dedicated channels, these messages can be sent/received simultaneously with the voice/data/fax service over a GSM network. SMS supports national and international roaming. This means that you can send short messages to any other GSM mobile user around the world. With the PCS networks based on all the three technologies, GSM, CDMA and TDMA supporting SMS, SMS is more or less a universal mobile data service.



© JGRCS 2010, All Rights Reserved

Figure1: SMS messages sent monthly in USA (billion)

The figure below shows a typical organization of network elements in a GSM network supporting SMS.

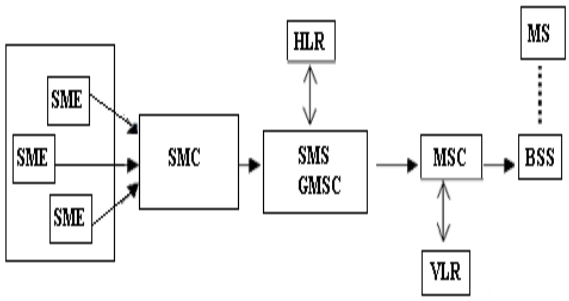


Figure2: SMS Architecture

The SMC (Short Message Center) is the entity which does the job of store and forward of messages to and from the mobile station. The SME (Short Message Entity) which can be located in the fixed network or a mobile station, receives and sends short messages.

The SMS GWMS (SMS gateway MSC) is a gateway MSC that can also receive short messages. The gateway MSC is a mobile network's point of contact with other networks. On receiving the short message from the short message center, GMSC uses the SS7 network to interrogate the current position of the mobile station form the HLR, the home location register.

HLR is the main database in a mobile network. It holds information of the subscription profile of the mobile and also about the routing information for the subscriber, i.e. the area (covered by a MSC) where the mobile is currently situated. The GMSC is thus able to pass on the message to the correct MSC.

MSC (Mobile Switching Center) is the entity in a GSM network which does the job of switching connections between mobile stations or between mobile stations and the fixed network.

A VLR (Visitor Location Register) corresponds to each MSC and contains temporary information about the mobile, information like mobile identification and the cell (or a group of cells) where the mobile is currently situated. Using information from the VLR the MSC is able to switch the information (short message) to the corresponding BSS (Base Station System, BSC + BTSs), which transmits the short message to the mobile. The BSS consists of transceivers, which send and receive information over the air interface, to and from the mobile station. This information is passed over the signaling channels so the mobile can receive messages even if a voice or data call is going on.

APPLICATIONS

Some of the common applications of SMS are:

- Exchanging small messages like "See you at 8.30 tonight at xyz". SMS is particularly suited for these kinds of short messages because SMS is much cheaper than calling someone and giving the same message. Calling someone to give the same message would invariably take more time and hence more cost.
- Many operators offer e-mail service over SMS. Every user is assigned an e-mail address at signup and any message delivered to that email is converted to short messages and delivered to the mobile.
- It is possible to send e-mail messages (less than 160 characters) from a mobile phone to any e-mail address via SMS.
- Information services like news, weather, entertainment and stock prices etc. can be availed just by sending a keyword like NEWS, WEATH etc to the short message center number.
- SMS can be used by the network operators to provide services like balance enquiry in case of prepaid cards using SMS.
- Mobile chatting is one more hot application of SMS
- SMS can be used to notify users that they have received new voice-mail or fax messages.
- It provides an alternative to alphanumeric paging services
- Using SIM-Toolkit, now a part of GSM specifications, SMS can be used to have on the air activation of features. By sending codes embedded in short messages from the server network operators can remotely provision the user's wireless terminal
- Internet e-mail alerts.
- Downloading new ring tones.

SMS SECURITY ISSUES AND VULNERABILITIES

Two important aspects for any entity using consumer technologies such as SMS for business purposes:

a. SMS is not a secure environment.
b. Security breaches often occur more easily by concentrating on people rather than technology.

The contents of SMS messages are visible to the network operator's systems and personnel. Therefore, SMS is not an appropriate technology for secure communications. Most users do not realize how easy it is to intercept messages. It would likely be a relatively complex to hack into a telecom provider's systems to obtain the content of SMS messages, but finding staff privileged to look at SMS messages and persuading them to reveal the contents is much easier. The

© JGRCS 2010, All Rights Reserved

underlying specifications and technology for SMS transmission leave many security gaps. These gaps make SMS vulnerable to –

- ***Snooping:*** - On device, at the store and forward network elements
- ***SMS Interception:***-Over the air, in wired network
- ***Spoofing:*** - Using commercial tools, own SMS gateway
- ***Modification:*** - Using conventional hacking techniques
- ***Attacks on GSM, the SMS Carrier Technology:*** - Often the weakest link in security is the mobile phone itself. Even leaving the mobile phone unattended inadvertently could expose your private and confidential messages to snooping.

Short message service (SMS) will play an important role in the future business areas, which are popularly known as m-commerce, mobile banking, governmental use, and daily life communication. Up to now many business organizations use SMS for their business purposes. SMS's security has become a major concern for business organizations and customers. There is a need for an end to end SMS Encryption in order to provide a secure medium for communication. Security is main concern for any business company such as banks who will provide these mobile banking services. Currently there is no such scheme that provides complete SMSs security. In this paper we will combine two encryption scheme i.e. Caesar Cipher and one time pad to enhance the security.

THE CAESAR CIPHER

In cryptography, a Caesar cipher, also known as a Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals.

For example:

```
Plain:    ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:   DEFGHIJKLMNOPQRSTUVWXYZABC
```

Deciphering is done in reverse.

ONE TIME PAD

A one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly. In this technique, a plaintext is paired with random, secret key (or pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, at least as long as the plaintext, never reused in whole or in part, and kept completely secret, the resulting ciphertext will be impossible to decrypt or break.[1][2] It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys. However, there are several key conditions that must be met by the user of a one time pad cipher, or the cipher can be compromised.

a. The key must be random and generated by a non-deterministic, non-repeatable process. Any key generated by an algorithm will not work. The security of the OTP relies on the randomness of the key. Unfortunately, the randomness of a key cannot be proved.

b. The key must never be reused. Use of the same key to encrypt different messages, no matter how trivially small, compromises the cipher.

c. The key must not fall in the hands of the enemy. This may seem obvious, but it points to the weakness of system in that you must be able to transmit large amounts of data to the reader of the pad. Typically, one time pad cipher keys are sent via diplomatic pouch.

A typical one time pad system works like this: Generate a long fresh new random key. XOR the plaintext with the key to create the ciphertext. To decrypt the ciphertext, XOR it with the original key. The system as presented is thus symmetric. Other functions (e.g., addition modulo n) could be used to combine the key and the plaintext to yield the ciphertext, although the resulting system may not be symmetric.

For example:

Plaintext : T H E B R I T I S H

Keys : D K J F O I S J O G

It follows the formula "(plaintext + key) MOD alphabet length":

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Perform encryption:

© JGRCS 2010, All Rights Reserved

(T(19)+D(03)=22) MOD 26 = 22 = W

(H(07)+K(10)=17) MOD 26 = 17 = R

(E(04)+J(09)=13) MOD 26 = 13 = N

(B(01)+F(05)=06) MOD 26 = 06 = G

(R(17)+O(14)=31) MOD 26 = 05 = F

(I(08)+I(08)=16) MOD 26 =16 = Q

(T(19)+S(18)=37) MOD 26 = 11 = L

(I(08)+J(09)=17) MOD 26 = 17 = R

(S(18)+O(14)=32) MOD 26 = 06 = G

(H(07)+G(06)=13) MOD 26 = 13 = N

Ciphertext : W R N G F Q L R G N

Decryption is also quite straightforward. It follows the formula "(ciphertext - key + alphabet length) MOD alphabet length":

(W(22)-D(03)= 19 +26) MOD 26 = 19 = T

(R(17)-K(10)= 07 +26) MOD 26 = 07= H

(N(13)-J(09)= 04 +26) MOD 26 =04 = E

(G(06)-F(05)= 01 +26) MOD 26 =01 = B

(F(05)-O(14)=-09 +26) MOD 26 = 17= R

(Q(16)-I(08)= 08 +26) MOD 26 = 08 = I

(L(11)-S(18)=-07 +26) MOD 26 = 19 = T

(R(17)-J(09)= 08 +26) MOD 26 = 08= I

(G(06)-O(14)=-08 +26) MOD 26 = 18= S

(N(13)-G(06)= 07 +26) MOD 26 = 07= H

We can see the original message here: "The British"

OUR APPROACH

In our approach we combine both of the above mention encryption scheme i.e. Caesar Cipher and one time pad. When a short message entity (SME) sends an SMS (only text message), it will be encrypted by Caesar cipher means each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet for first time encryption then will use one time pad encryption technique to perform encryption again. Now the generated ciphertext is more secure than the generated by individual Caesar cipher or one time pad scheme. When the SMS is received at the receiver end, it will be decrypted first. Decryption follows reverse operations performed during encryption.

Steps Description

a. When mobile devices compose and send the SMS, the SMS will be first encrypted by Caesar Cipher scheme. The encrypted SMS will again encrypted by one time pad scheme and then send to the nearest base station (BS) using on- the-air (OTA) interface, which is the standard for the transmission and reception of application-related information in wireless communications devices,

b. In case of internal exchange process, the BS forwards the secure or encrypted SMS content to the mobile's home short message service centre (SMSC), over SS7.

c. But in case of external exchange process, the sender's SMSC reformats the encrypted SMS message to the short Message Peer to Peer Protocol (SMPP) format and then sends it to the SMS gateway using TCP/IP over the public or private internet which links to the mobile recipient's SMSC. The SMPP is the telecommunication industry protocol for exchanging SMS messages between SMS centers.

d. After completing its internal or external processing, and interrogation of the destination location, the SMSC sends the message over SS7 to the nearest BS around the final mobile destination.

e. Through the OTA protocol again when the BS station forwards the SMS to the final Mobile reception first it will be decrypted. Decryption follows reverse operations performed during encryption and then the delivery acknowledgements will follow the reverse path.

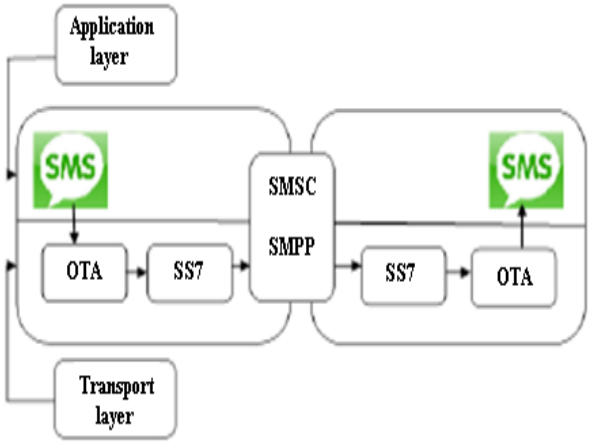


Figure3: Transmission Layer

For example:

© JGRCS 2010, All Rights Reserved

Suppose the mobile device compose and send the SMS: “Hello Sharad”.

Step-1 : Guess the Cipher key

Cipher Key : 3

Stept-2 : Perform Caesar Cipher Encryption Scheme and generate ciphertext using cipher key.

Plaintext : HELLOSHARAD

Ciphertext : KHOORVKDUDG

Step-3 : Perform one time pad encryption scheme on the cipher text generated by Caesar Cipher Scheme .

Plaintext : KHOORVKDUDG

Keys : DKJFOISJOGH

Perform encryption:

(K(10)+D(03)=13) MOD 26 =13= N

(H(07)+K(10)=17) MOD 26 =17= R

(O(14)+J(09)=23) MOD 26 =23 = X

(O(14)+F(05)=19) MOD 26 =19= T

(R(17)+O(14)=31) MOD 26 =05= F

(V(21)+I(08)=31) MOD 26 =03= D

(K(10)+S(18)=28) MOD 26 =02 = C

(D(03)+J(09)=12) MOD 26 =12 = M

(U(20)+O(14)=34) MOD 26 =08 = I

(D(03)+G(06)=09) MOD 26 =09 = J

(G(06)+H(07)=13) MOD 26 =13 = N

Ciphertext: NRXTFDCMIJN

The ciphertext is send to the nearest base station (BS) using on- the-air (OTA) interface, which is the standard for the transmission and reception of application-related information in wireless communications devices.

Step-4: After completing its internal or external processing, and interrogation of the destination location, the SMSC sends the message over SS7 to the nearest BS around the final mobile destination. Through the OTA protocol again when the BS station forwards the SMS to the final Mobile reception first it will be decrypted. Decryption follows reverse operations performed during encryption. First perform one time pad decryption scheme to decrypt the ciphertext.

Decryption is also quite straightforward. It follows the formula "(ciphertext - key + alphabet length) MOD alphabet length":

(N(13)-D(03)=10+26) MOD 26 =10= K

(R(17)-K(10)=07+26) MOD 26 =07= H

(X(23)-J(09)=14+26) MOD 26 =14 = O

(T(19)-F(05)=14+26) MOD 26 =14= O

(F(05)-O(14)=-09+26) MOD 26 =17= R

(D(03)-I(08)=-05+26) MOD 26 =21= V

(C(02)-S(18)=-16+26) MOD 26 =10= K

(M(12)-J(09)=03+26) MOD 26 =03= D

(I(08)-O(14)=-06+26) MOD 26 =20 = U

(J(09)-G(06)=03+26) MOD 26 =03 = D

(N(13)-H(07)=06+26) MOD 26 =06 = G

Plaintext : KHOORVKDUDG

Step-5 : We consider plaintext generated by one time pad decryption scheme as ciphertext for deciphering using Caesar Cipher scheme. Deciphering is done in reverse.

Ciphertext : KHOORVKDUDG

Plaintext : HELLOSHARAD

We can see the original SMS here: "Hello Sharad”.

CONCLUSION

Short message service (SMS) will play an important role in the future business areas, which are popularly known as m-commerce, mobile banking, governmental use, and daily life communication. SMS’s security has become a major concern for business organizations and customers. The method implemented above is an innovation of new technique which is a better option for telecommunication industry to enhance the privacy of SMS.

REFERENCES

[1] antis, A. Castiglione, A. Cattaneo, G. Cembalo, M. gna, F. Petrillo, U.F, "An Extensible Framework for ient Secure SMS," Complex, Intelligent and Software sive Systems (CISIS), International Conference, 15-eb.2010, pp. 843-850, doi:10.1109/CISIS.201081

[2] ain, A.; Jahan, S.; Hussain, M.M.; Amin, M.R.; Shah az, S.H.; "A Proposal For Enhancing The Security

© JGRCS 2010, All Rights Reserved

em Of Short Message Service In GSM", Anti-terfeiting, Security and Identification, 2nd national Conference, ASID 2008, doi: 109/IWASID.2008.4688386.

[3] //en.wikipedia.org/wiki/Encryption

[4] yi, Mary; Seral, Devrim; "SMS Security: An nmetric Encryption Approach," Wireless and Mobile munications (ICWMC), 6th International Conference, , pp. 448-452, doi: 10.1109/ICWMC.2010.87

[5] nek, David.; Drahansky, Martin.; "SMS Encryption Mobile Communication", Security Technology, TECH '08, International Conference, 2008, .0.1109/SecTech.2008.48

[6] er Hasan Al-Bakri, M. L. Mat Kiah, A. A. Zaidan, B. idan and Gazi Mahabubul Alam: "Securing peer-to- mobile communications using public key graphy: New security strategy", International Journal e Physical Sciences Vol. 6(4), pp. 930-938, 18 ary, 2011.

[7] n Khozooyi, Maryam Tahajod, Peyman khozooyi, rity in Mobile Governmental Transactions", 2009 d International Conference on Computer and ical Engineering, 978-0-7695-3925-6/09 $26.00 © IEEE, pp 168-172.

[8] allings, "Cryptography and Network Security 4th Ed," ce Hall, 2005, PP. 58-309.

[9] sh Saxena and Ashish payal, "Enhancing Security n of Short Message Service for M-Commerce in ", International Journal of Computer Science & eering Technology (IJCSET), ISSN: 2229-3345 Vol. 4, April 2011, pp. 126-133.

[10] Siddique, and M. Amir, "GSM Security Issues and enges," 7th IEEE International Conference on are Engineering, Artificial Intelligence, Networking Parallel/Distributed Computing (SNPD'06), pp.413-une 2006@IEEE.

AUTHOR'S BIOGRAPHY

Sharad Kumar Verma, received his Bachelor of computer application (BCA) degree from MCRPV,

Bhopal(MP), INDIA in 2004, Master of computer application (MCA) degree from UPTU Lucknow(UP), INDIA in 2007, and currently pursuing Ph.D in computer science (Network Security) from MEWAR University, Rajasthan, INDIA. He has more than six years of teaching experience in Meerut Institute of Engineering & Technology, Meerut (UP) INDIA. He is the author/co-author of more than 11 publications in reputed journals. The research fields of interest are Coding Theory and Time Synchronization in Wireless network.

Dr. Deo Brat Ojha, Birth Place & date –Bokaro Steel City, (Jharkhand), INDIA on 05/07/1975. Ph.D

from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varanasi (U.P.), INDIA in 2004. The degree field is Optimization Techniques In Mathematical Programming. The major field of study is Functional Analysis. He has more than 12 year teaching experience as PROFESSOR & more than eight year research experience. He is working at MEWAR Institute of Technology, Ghaziabad (U.P.), INDIA. He is the author/coauthor of more than 50 publications in technical journals and conferences.

© JGRCS 2010, All Rights Reserved