IOSR Journal of Mobile Computing & Application (IOSR-JMCA)
e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 3, Issue 4 (Jul. - Aug. 2016), PP 11-16
www.iosrjournals.org

Securing Short Message ServiceUsing Vernam Cipher in Android Operating System

Andysah Putera Utama Siahaan
Faculty of Computer Science, Universitas Pembangunan Panca Budi
Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia

Abstract: *Although many ways to communicate with someone, SMS is still one of the popular media to send a message to someone. Not unlike the others, the messages sent can be known by the third party either tapping or the investigation. Unencrypted SMS can be easily obtained from communication providers so that they may be misused. Since the communication devices have been using Android operating system, they are programmable. There is various script can be inserted to devices to protect the data. One of them is Vernam Cipher. This method offers how to protect personal messages sent via SMS easily. It converts the message into an encrypted message shortly before sent. At the moment there tapping on the outside, the information is not easily understood its contents. The message is entirely secure.*

Keywords: *Vernam, Mobile, SMS, Cryptography, Security, Encryption, Decryption*

I. Introduction

Information security means securing information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction [7].Despite the emergence of digital media to communicate, SMS is still used as a system that is popular among social media. SMS has a major role in communication. Not everyone has a sophisticated device that supports internet facility. For owners of older model devices, SMS is a way that always used to deliver the message to the listener. The security of data on SMS delivery is not guaranteed. Everyone can steal the message. Although the message is personal, the message can be retrieved from a provider. When there is an investigation, the message might be generated from the database. Whatever happens at the talks, if everyone wants, the message is still readable. This method does not teach how to send the crime message, but it explains how to keep a secret message is not misused by the irresponsible parties. This research tries to modify the bits order by encrypting and providing a password.

II. Theories

2.1 Android Short Message Service

SMS stands for Short Message Service. It is a facility to send and receive a short text message via the wireless devices or cellular phone communication device. One of the advantages of SMS is cost. SMS is a service that is widely applied in wireless communication system. SMS enables sending messages in alphanumeric. SMS mechanism is sending a short message from one subscriber terminal to another terminal. Short Message Service Centre (SMSC) is the device that handles this operation. It is also known as Message Centre (MC). It includes the determination of search or sorts the final destination of the message.Figure 1 illustrates how the GSM Network handles the SMS.

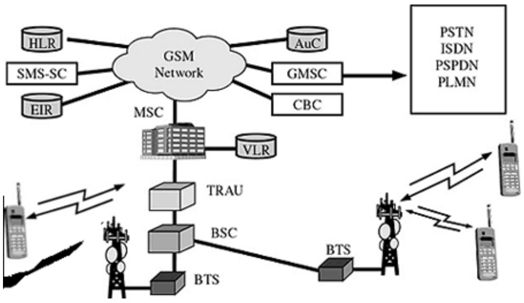
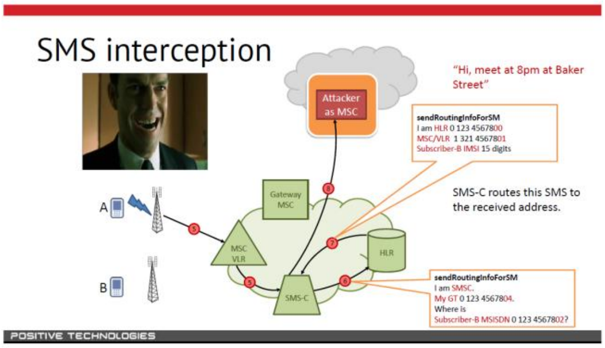


Figure 1.SMS Architecture

SMS service is a non-real time service where a short message can be submitted to a destination, no matter if the destination is ready or not. When it is not active, the system will delay the delivery to the destination until the destination is active again. The SMS system guarantees the delivery of a short message to get to the destination. Temporary delivery failures always identified as a pending message. Short retransmission message will always be possible unless the applicable rules that the short message has exceeded a certain limit should be removed and otherwise failed to send.

In Android Operating System, we can use SMSManager API or devices Built-in SMS application to send SMS. However, it uses a phone number system to find people and send them a message. SMS using the conventional phone is similar to using the Android one. The difference is that the Android phone is programmable. We can build a script to monitor the activity of the phone or maybe we can filter the SMS content which is delivered to the inbox. The Android SMS is more flexible than the predecessor. We can attach them to the function that we wish such as auto send, block, and many other functions.



SMS interception

"Hi, meet at 8pm at Baker Street"

sendRoutingInfoForSM
I am HLR 0 123 4567800
MSC/VLR 1 321 4567801
Subscriber-B IMSI 15 digits

SMS-C routes this SMS to the received address.

sendRoutingInfoForSM
I am SMSC.
My GT 0 123 4567804.
Where is
Subscriber-B MSISDN 0 123 4567802?

Via: The 3G4G Blog - blog.3g4g.co.uk

Figure 2. SMS Interception

There are many attacks possible to SMS [2]. Figure 2 shows how the SMS can be attacked in the air. Since SMS is wireless signal, everyone can intercept the signal and turn into the original information.

2.2 Vernam Cipher

The data security is the most significant issue in networking problem. A specific cryptography algorithm must protect the data to maintain the integrity. One of them is Vernam Cipher. It produces the ciphertext by doing modulo in its bits. Every character is turned into an 8-bit binary and converted into cipher bits. The SMS will work if combined with this algorithm. In producing the ciphertext, we must provide a key to keeping the ciphertext unbreakable. Vernam Cipher uses a very simple formula as showed next.

$$CT = PT \oplus Key \qquad (1)$$

$$PT = CT \oplus Key \qquad (2)$$

Where:

CT : bit of aftercode message
PT : bit of original message
Key : bit of password

PT is filled with the bit of the plaintext. For example, the character "A" is 65 where the binary is 01000001. To produce the ciphertext, it performs an 8-time looping. It carries out from bit 1 to bit 8. Every bit is calculated. Formula 1 and 2 are identical. They are using the same technique to manipulate the bits. XOR is used to encrypt and decrypt the bit.

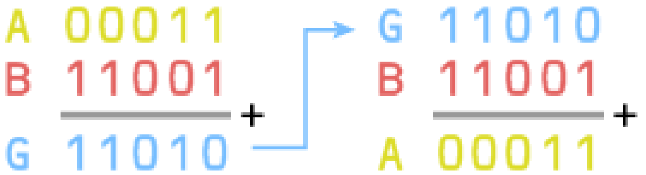


Figure 3. Vernam Cipher bit operation

Vernam uses XOR operation to produce the ciphertext. The resulting bit "1" if the input bits are different while "0" if they are same. Figure 3 shows the result of the bit operation. It describes how the set of binary (A) are encrypted (G) and return to plain binary back.

III. Proposed Work

SMS sent will be forwarded to a cellular provider. GSM network will search for the destination number and then send the message to the number. When the message arrives at the destination, the number sends an acknowledgment back to the operator. This research proposes the method encrypts the message before broadcasted. The message must be encrypted when the user has finished typing the content. By encrypting the message, it is hard to convert it back without knowing the algorithm and password used before. The attacker must know at least some of the plaintext character.

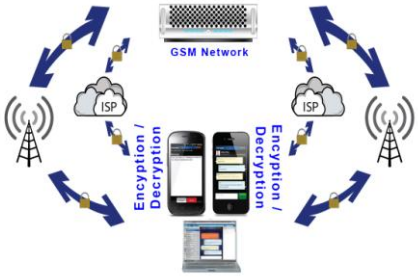


Figure 4. GSM encryption and decryption

Figure 4 describes the flow of sending and receiving a message. It must be encrypted before sent to a destination and must be decrypted as well when receiving it. When the message is in the air, it is entirely secure. Every attacker can steal the information, but they will have got nothing since the message is encrypted.

IV. Interface Design

The interface is designed to put the application in the mobile system. Figure 5 shows the home screen of the application. The display consists of the message, password, phone number text boxes and three buttons of command buttons. The application is build by using Basic4Android version 4. It is a very familiar interface to construct the Android application. We can build either using the designer mode or even generating a toolbox script.

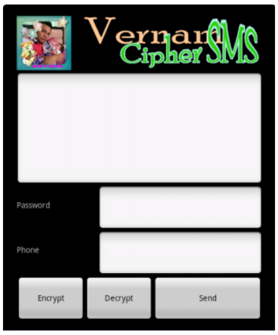
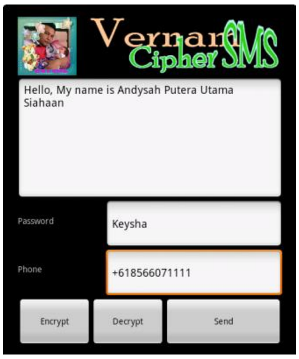


Figure 5. Vernam Cipher SMS display

V. Software Testing

Now we test the apps with serveral characters. Assume we have "**Hello, My Name is Andysah Putera Utama Siahaan**". Figure 6 explains that the input characters are put in the message box.



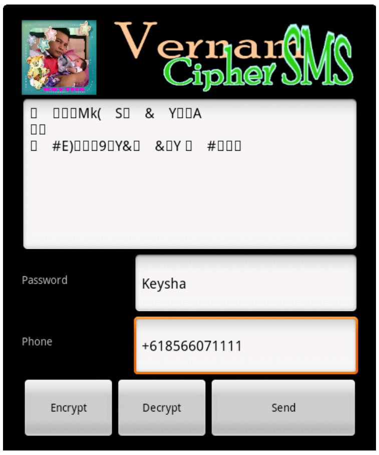
Hello, My name is Andysah Putera Utama Siahaan

Password: Keysha

Phone: +618566071111

Figure 6. Initial input (message, password and phone number)

There are two more input boxes such as password and phone number. The password is a set of characters provided to protect the encryption. It is used to decrypting the message back to plain text after it has arrived at the destination. The phone number is the destination itself.



□ □□□Mk(S□ & Y□□A
□□
□ #E)□□□9□Y&□ &□Y □ #□□□

Password: Keysha

Phone: +618566071111

Figure 7. Encrypted Message

After the Encrypt Button is pressed, the algorithm converts the plain text into cipher text by using the separated password provided earlier. Figure 7 shows the message box is showing the illegible characters. Some of them are illustrated like boxes. Separate applications do not show the same shape. Pressing the Decrypt Button will get the text back to its original information. When the text is in a cipher mode, the Send Button is to send the message to the destination number. Both participants must have the same applications to communicate each other. Otherwise, the receiver will not understand the word that has been displayed.

VI. Evaluation

Let's take a look at the previous example. Tabel 1 is some of the plaintext ASCII code.

Table 1. Plaintext ASCII code

H	e	l	l	O	,		M	y
72	101	108	108	111	44	32	77	121

Table 2. Key ASCII code

K	e	y	s	h	a	K	e	y
75	101	121	115	104	97	75	101	121

Table 2 is the code of the key. The key is repeated until the length of the plaintext is met. Formula 1 is to encrypt the plaintext into the ciphertext. To reconstruct it back to the plaintext, we can apply Formula 2.

The encryption calculation:

$$\begin{aligned} CT[1] &= PT[1] \oplus K[1] \\ &= 72 \oplus 75 \\ &= 3 \end{aligned}$$

$$\begin{aligned} CT[2] &= PT[2] \oplus K[2] \\ &= 101 \oplus 101 \\ &= 0 \end{aligned}$$

$$\begin{aligned} CT[3] &= PT[3] \oplus K[3] \\ &= 108 \oplus 121 \\ &= 21 \end{aligned}$$

$$\begin{aligned} CT[4] &= PT[4] \oplus K[4] \\ &= 108 \oplus 115 \\ &= 31 \end{aligned}$$

$$CT[5] = PT[5] \oplus K[5]$$

$= 111 \oplus 104$
$= 7$

$CT[6] = PT[6] \oplus K[6]$
$= 44 \oplus 97$
$= 77$

$CT[7] = PT[7] \oplus K[7]$
$= 32 \oplus 75$
$= 107$

$CT[8] = PT[8] \oplus K[8]$
$= 77 \oplus 101$
$= 40$

$CT[9] = PT[9] \oplus K[9]$
$= 121 \oplus 121$
$= 0$

After the above calculation, the ciphertext is obtained. There are several characters are illegible. It shows on the screen. The ASCII 0 – 31 are usually unprinted. They are marked as or any other character. The ASCII 32 – 127 are printed and primarily used. The ASCII 128 – 255 are the extended characters that show like symbols.Table 3 shows the result after being encrypted.

Table 3. Ciphertext ASCII code

					M	k	(	
3	0	21	31	7	77	107	40	0

Table 4. Complete process of Vernam Cipher

PT	A	Key	A	CT	A
H	72	K	75		3
e	101	e	101		0
l	108	y	121		21
l	108	s	115		31
o	111	h	104		7
,	44	a	97	M	77
	32	K	75	k	107
M	77	e	101	(	40
y	121	y	121		0
	32	s	115	S	83
N	78	h	104	&	38
a	97	a	97		0
m	109	K	75	&	38
e	101	e	101		0
	32	y	121	Y	89
i	105	s	115		26
s	115	h	104		27
	32	a	97	A	65
A	65	K	75		10
n	110	e	101		11
d	100	y	121		29
y	121	s	115		10
s	115	h	104		27
a	97	a	97		0
h	104	K	75	#	35
	32	e	101	E	69
P	80	y	121	)	41
u	117	s	115		6
t	116	h	104		28
e	101	a	97		4
r	114	K	75	9	57
a	97	e	101		4
	32	y	121	Y	89
U	85	s	115	&	38
t	116	h	104		28

a	97	a	97		0
m	109	K	75	&	38
a	97	e	101		4
	32	y	121	Y	89
S	83	s	115		32
i	105	h	104		1
a	97	a	97		0
h	104	K	75	#	35
a	97	e	101		4
a	97	y	121		24
n	110	s	115		29

Table 4 is the complete process of encryption and decryption. The text “Hello, My Name is Andysah Putera Utama Siahaan” turns into encrypted message and return back to the plaintext.

VII. Conclusion

PlainSMS is very dangerous. If the content does not consist of any important thing, it does not matter. Otherwise, it brings into trouble. Encrypting the message is the only way to secure the information personally. The cellular network provides the mobile encryption as well, but it does not guarantee the message safely. The attacker can intercept the message at any time. Vernam Cipher is the great common encryption method to implement. It does not need the complex mathematical calculation. It provides the ciphertext by doing XOR operation. The text after encryption is completely secure to transmit.

References

[1]. B. Forouzan, Cryptography and Network Security, McGraw-Hill, 2006.

[2]. Z. Ghadialy, “The SS7 Flaws that Allows Hackers to Snoop on Your Calls and SMS,” The 3G4G Blog, 29 12 2014. [Online]. Available: http://blog.3g4g.co.uk/2014/12/the-ss7-flaws-that-allows-hackers-to.html. [Diakses 15 7 2016].

[3]. H. M. E. Bakry, A. E. T. E. Deen dan A. H. E. Tengy, “Implementation of a Hybrid Encryption Scheme for SMS / Multimedia Messages on AndroidI,” International Journal of Computer Applications, vol. 85, no. 2, pp. 1-5, 2014.

[4]. S. Jha dan U. Dutta, “Review on SMS Encryption using MNTRU Algorithms on Android,” International Journal of Computer Science and Information Technologies, vol. 6, no. 4, pp. 3855-3858, 2015.

[5]. A. P. U. Siahaan, “RC4 Technique in Visual Cryptography RGB Image Encryption,” International Journal of Computer Science and Engineering, vol. 3, no. 7, pp. 1-6, 2016.

[6]. A. P. U. Siahaan, “Three-Pass Protocol Concept in Hill Cipher Encryption Technique,” International Journal of Science and Research, vol. 5, no. 3, 2016.

[7]. R. Rayarikar, S. Upadhyay dan P. Pimpale, “SMS Encryption using AES Algorithm on Android,” International Journal of Computer Applications, vol. 50, no. 19, pp. 12-17, 2012.

Author Profile

Andysah Putera Utama Siahaan was born in 1980, Medan, Indonesia. He received the S.Kom. degree in computer science from Universitas Pembangunan Panca Budi, Medan, Indonesia, in 2010, and in 2012, he obtained M.Kom. from the University of Sumatera Utara, Medan, Indonesia. In 2010, he joined as a lecturer at the Department of Engineering, Universitas Pembangunan Panca Budi. He has been a researcher since 2012. He has studied his Ph. D. degree from 2016. He is now active in writing international journals and conferences.