International Journal of Computer Trends and Technology
, Volume 3 Issue 6 – 2012, ISSN: 2231 - 2803

A Novel Tree Based Security Approach for Smart Phones

[(1)]R.Surendiran,
Research Scholar,
Dept of MCA, Computer Center,
Madurai Kamaraj University, Madurai.

[(2)] Dr.K.Alagarsamy,
Associate Professor
Dept of MCA, Computer Center,
Madurai Kamaraj University, Madurai.

Abstract:

Mobile phones play a major role in every human being. Last one decade mobile phones and related devices usage has developed in tremendous manner. Smart devices and its applications used in many ways like financial, entertainment, communication, etc. It also increases the lot of security threats and vulnerabilities. This paper we are going to provide a novel tree based security approach for mobile phones. Tree is data structure concept which is used to make the security level much more complicated.

Keywords: Tree, Smart phones, Encryption, Decryption.

I. Introduction:

Information and Communication Technology is not equally distributed in our world: developed countries represent about 70 per cent of all Internet users while its percentage of Internet hosts has risen from 90 per cent in 2012 to about 99 per cent in 2016.

Things change dramatically if we look at mobile and wireless technology: developing countries already represented about 60 per cent of mobile connections in 2010, with a foreseen growth rate that is faster for developing countries than that for the developed one in the period 2010-2012.

This growth depends on the new point of view of mobile electronic technology applications, making in principle convenient to do business with their clients located anywhere in the world by passing the poor telecommunication infrastructure still common in many developing countries. On the other hand, in the developed countries has a technique under the name of electronic mobile is becoming much and more essential in electronic business transactions. The use of smart mobile phones will enable different kind of services and new business models, overcoming time and space limitations.

A). SMS:

Short Message Service 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 [6].

Short messages [7] are now used for both personal and business communications. Some common examples are:

1. Alerts and notifications to customers from service point, vendor, banks, service provider on transaction status, credit card details, NEFT transactions status, system administrators in some organizations if critical events occur in IT systems, etc.

2. One-time passwords (OTP) being sent to the customers of banks or organizations via SMS messages for authorizing or confirming high risk online transactions. With this onetime password, the customers can be authenticated by the online transaction system before transactions are completed.

3. Text message used by people for chatting and information sharing via their mobile phones, who provide a convenient way for targeted clients to request and respond to products, services like downloadable ringtones , wallpapers and other commercial activities.

II. SMS Security Threats:

a). Message Disclosure

Basically encryption is not applied to short message transmission by default; messages could be interrupted and traced during transmission. In addition, SMS messages are stored as plain text by 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.

Spying programs like FlexiSpy7 enable intruders to automatically record all incoming and outgoing SMS messages and then upload the logs to a remote server for later viewing and analysis.

B). Spamming

Probably most of e-business is using SMS as a valid marketing medium; many people have had the inconvenience of receiving SMS spam. The availability of bulk SMS broadcasting utilities makes it easy for virtually everyone to send out mass SMS messages.

C). Denial of Service Attacks

DoS attacks are made possible by sending sequence of unwanted messages to a target mobile phone, making the victim's mobile phone inaccessible. Weaknesses in the SMS protocol could be overcome to launch a DoS attack on a cellular phone network.

D). SMS Phone Crashes

Some vulnerable mobile phones may crash if they receive a particular type of malformed short message. Once a malformed message is received, the infected phone becomes inoperable.

E). SMS Viruses

Mobile phones are getting more powerful and programmable; the potential of viruses being spread through SMS is becoming greater. In addition, the ability of SIM application toolkits that allows applications to access the dialing functions and phone book entries might make SMS suitable platform for spreading self-replicating virus.

F). SMS Phishing

It is a combination of SMS and phishing. Similar to an Internet phishing attack using email, attackers are attempting to fool mobile phone users with bogus text messages. When users are taken in by a bogus text message, they may connect to a website provided in the SMS message, and be tricked into download a malware application into their mobile phones.

There are numerous threats available in the market. To avoid these kinds of issues and problems, we have proposed a novel tree based approach for sms communication.

III. Proposed Method:

Algorithm:

1) Fetch the client SMS as plain Text
2) Make a tree formation
3) Arrange the left node in array format
4) Form key table
5) Apply permutation based on key values
6) Add encryption key
7) Send cipher text

PROPOSED METHODLOGY (MRS Algorithm)

a.encryption.

Example text " **android** ".

Android is convert to equalant ascii value

a->97, n->110, d->100, r->114, o->111, i->105, d->100.

Then process a tree structure model

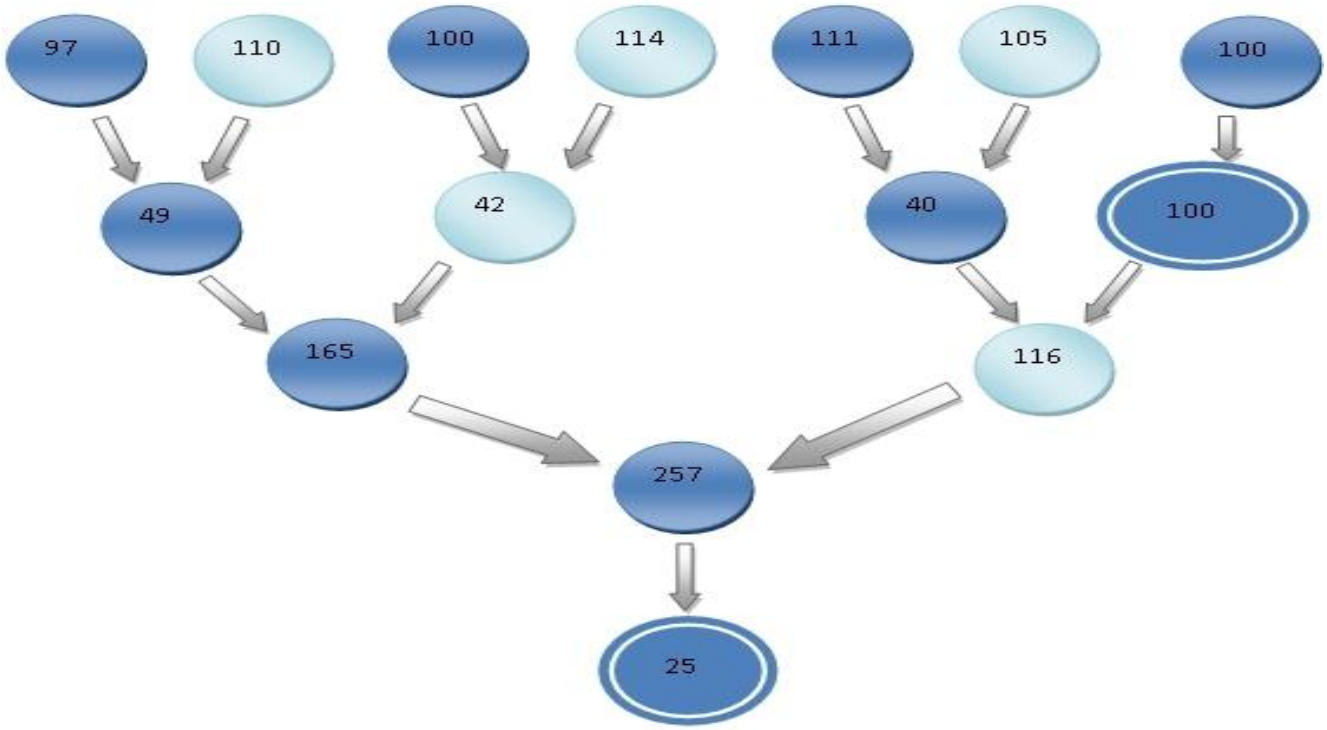

Diagram 1. Tree Structure of source Text

Take a left node of tree.

25
257
165
49
97
100
40
111

Left node array

Let we take the key size is 256 bit's.

So that key range up to 0 to 315 characters

Get the two Key from user. One is adding to text and other is performed permutation. Permutation key range is 0 to 40320.

Each table have a 8 characters, every character will take 8 bit so 64 – bit's

A	B	C	D	E	F	+	-

Table-1

G	H	I	J	K	L	*	/

Table-2

M	N	O	P	Q	R	#	@

Table-3

S	T	U	V	W	X	Y	Z

Table-4

User given a key is 20 and hi

Permutation key is "20"

Normal key is "hi"

Result

A	B	C	D	-	F	E	+

Table-5

G	H	I	J	/	L	K	*

Table-6

M	N	O	P	@	R	Q	#

Table-7

S	T	U	V	Z	X	W	Y

Table-8

So above all are results of permutation.

Then apply this formula.

Normal key each character ascii should add.

n=>normal key , p=> position,

h->104

i->105

n=104+105

n=209

p= n mod 8;

p= 209 % 8

p= 5

if (left node array[] =! 257)

encrypted []=left node array+ table[p];

encrypted[]='a' + '-';

encrypted[]=97 + 45;

encrypted[]=142;

encrypted[]='n '+ 'E'

encrypted[]=179;

encrypted[]='d' + 'F'

encrypted[]= 170

encrypted[]= 'r' + '+'

encrypted[]=157

encrypted[]='o' + 'A'

encrypted[]=182

encrypted[]='i' + 'H'

encrypted[]=177

encrypted[]='d' + 'I'

encrypted[]=173

142
257
179
170
157
182
177
173

Encrypted array

Encrypted array should convert a equitant characters and send.

b. Decryption

Decryption always the reverse process of encryption..

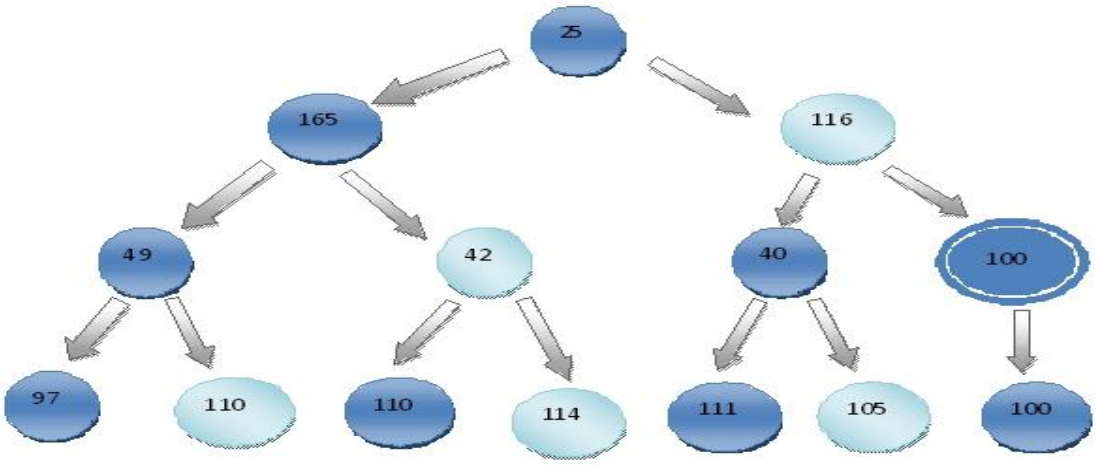

Diagram 2. Hence child nodes all are "original" data.

Comparison Analysis:

There are lot standard techniques were implemented in smartphone security applications like RSA, DES, SHA, etc. Here we are taking some of those for our comparison analysis. Performance analysis has been taken in various aspects like speed, performance, sustainability, etc.

In comparison analysis we have taken 162 characters as plain text because the maximum size of single SMS is 162 characters. We have analyzed the algorithm in various aspects like key complexity, key size, cipher text size, Transfer Rate.

Algorithm	Key complexity	Key size	Cipher Text size	Transfer Rate	Time Taken
MRS (Proposed Algorithm)	98	256 bit	n	15.13	3.51
AES	80	256 bit	n^2	19.25	4.92
DES	83	256 bit	n^2	20.31	5.432
Blowfish	81	448 bit	n^2	64.326	3.572

Table 9 – Comparison Analysis with Existing Algorithm

Conclusion:

This paper we have discussed about novel approach in the smart phone security issues era. Since tree is a complex data structure from the origin, it's most difficult to decrypt the data. Our MRS algorithm will provide the efficient and secured way for information transmission between the communication clients. We trust that our work will be the highly useful for society and research sector.

References:

[1] A Novel Scheme of Data Hiding in Binary Images IEEE, International Conference on Computational Intelligence and Multimedia Applications 2007

[2] Elliptic Curve Cryptography, an Implementation Guide,Anoop MS.

[3] Data Hiding in Binary Image for Authentication and Annotation Min Wu, Member, IEEE, and Bede Liu, Fellow,IEEE

[4] Williams Stallings, Cryptography and Network Security,Prentice Hall, 4th Edition, 2006.

[5] Steganography in MMS, Mohammad Shirali-Shahreza, Sharif University of Technology, Tehran, IRAN.

[6]http://en.wikipedia.org/wiki/Short_Message_Service

[7] Short Message Service Security, February 2008 , The Government of the Hong Kong Special Administrative Region

[8] Huang, D.-L., P.-L. P. Rau and G. Salvendy (2008). Perception of Information Security. Behavior and Information Technology

[9] Image Based Steganography Using LSB Insertion Technique,M. S. Sutaone. IEEE.

[10] Implementation of Text based Cryptosystem using Elliptic Curve Cryptography s. Maria Celestin Vigila , K.Muneeswaran