RESEARCH REVIEW JOURNALS
Volume-03
Issue-10
October-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

A Secure Command Based Approach to find Stolen Mobiles

Dr. R. Surendiran

Assistant Professor, Department of Computer Science, Mass College of Arts & Science, Kumbakonam (India)

ARTICLE DETAILS

Article History
Published Online: 10 October 2018

Keywords
Smart Phone, SMS, Commands

***Corresponding Author**
Email: sriparthi.g[at]gmail.com

ABSTRACT

Smart Phone usages increased day by day due to various application and services available in the trendy world. Smart phones provides N number of facilities to the users like internet banking, emails, messages, map, etc. At the same time vulnerabilities also increased in rampant manner. Mobile theft is also a major problem in the modern world. In our research paper we are providing a novel security approach to find the stolen mobiles by remotely. The proposed model implemented and tested with android platform. This approach will be more use full for public sector.

1. Introduction

In Modern world, usage of smart phones has become a vital part of day to day activities of people. Even we can say this decade is called as “Smart Phone Decade”. Smart phones are now at the peak of popularity in their usage of accessing the internet which includes mail access, social networking, mobile shopping and mobile banking.

Smart phones have sensitive and critical data of user like messages, contact details, important mail communications, personal information, call records, videos, photos, etc. So loss of smart phone is a very high amount of dangerous which may not be affordable in many cases. Few surveys about mobile theft in various countries have been studied. To avoid these kinds of issues we need an intelligent application to be run in mobile to eradicate mobile theft and track the mobile even after change of the SIM also.

Remote accessing is more important when we left our mobiles in office, home or stolen by someone. If we left in home there won’t be a major issue but in case of office or some other place or stolen by someone it will make major problem. Third party can steal your information like your contact details, incoming calls, messaging, emails, photos, video’s, etc.

To avoid these kinds of issues we need an effective mechanism to prevent our data’s and mobile information’s and secret data’s. In our research we are introducing a novel SMS based approach for handling remote mobile devices.

2. The Proposed Model

The proposed model introduced full Control over smart phone through Short Message Service (SMS) and we should incorporate some necessary security constraints. It is Start with ‘#’ symbol and following to personal security key. If it matches then proceed the following functionality or else it consider as a normal text message. Another Remote android phone itself can activate this function and access. When SMS is reaching the destination end client node will take full control of another device in terms of functionality.

In normal mobile phones, we couldn’t install the application. In this case, the users will communicate directly through SMS. So the symbols are not matched ignore message to process. That directly show to user visible and that consider as a normal message. If it is matched to take a command. So we process only achieved by authenticated person to access or control a recording Android phones and ‘#’ following password set as a user defined one.

3. Block Diagram

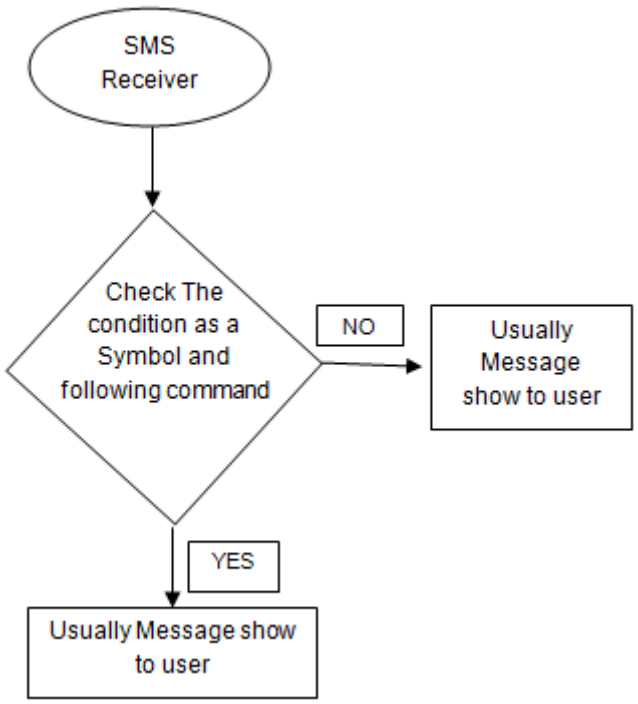

Diagram1: Block diagram of Remote Access

4. Remote Access

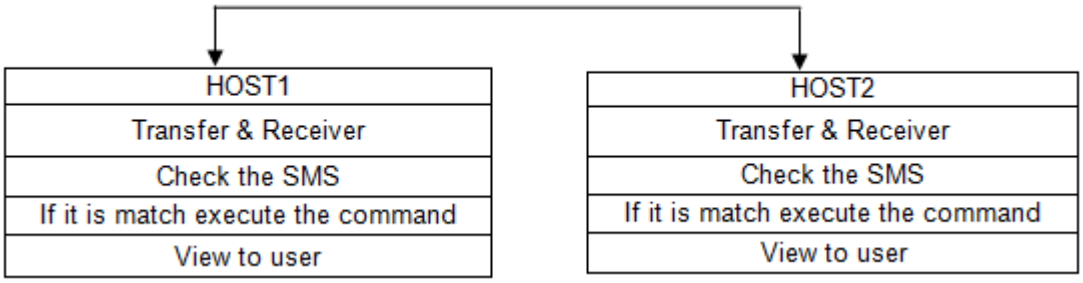

Diagram 2: Working Principle of Remote Access

The important purpose of this application is access a smart phone to remote devices through the SMS and control the full functionality of remote device. Then we have to consider a mobile security. So we have an authentication then only access this application. In case of authentication means "# then followed by personal security key". The remote access diagram clearly explains a method. How to access the one to another device? The host1 is an android phone user and host2 also android phone user.

So host1 wants to access a control of host2. The host1 must require personal security key of host2. Then only able to access a host2 so first thing host1 know as a personal security key and send to SMS vice conversation. If it is match the personal security key then to take a control of mobile. Whatever command host1 send that are present in the database itself that execute and able to operate a mobile phone. The database was presented in the application that contains a predefined function. The SMS commands are invoke corresponding functions. The function is run background of the mobile environment.

"#..."GPS_ON or OFF	Switch ON the GPS. Switch OFF the GPS.
"#..."BLUETOOTH_ ON or OFF	Switch ON the Bluetooth. Switch OFF the Bluetooth.
"#..."SWITCH_ON or OFF	Switch ON the Phone. Switch OFF the Phone.
"#..."MESSAGE_ READ or WRITE	Read or Write SMS to Inbox
"#..."CAMERA_ON or OFF	Switch ON the Camera. Switch OFF the Camera.
"#..."etc…,	Etc….,

Table1: Sample Commands which are executed in background

The above table is describing a functions and methods in the application. The many functions are available in this application. If the key is match then execute the corresponding methods or else show like a normal SMS.

If a send "#2047" GPS_ON message to host2. Then received a host2 and check a # and following personal security key. If it is match to check message content. Then it invokes a corresponding process.

Diagram 3: Enabled GPS location in Victim Node

a. SAMPLE CODE:

```
if(s!=key){
        Intent intent = new Intent
("android.location.GPS_ENABLED_CHANGE");
   intent.putExtra ("enabled", true);
 }
```

So we have successfully GPS ON using remote android phone. That way to proceeds all the function and methods execute. That is a sample code to execute by AVM machine.

5. Conclusion

In this paper we have implemented a novel approach for detecting the theft mobiles or left mobiles based on the SMS command. Since SMS is the basic operation for every mobile, this technique work in all the mobiles. Security features are very important for mobile phones in the trendy world. Most of the valuable information's are available in our mobile phones or tablets. We believe that this approach will help to mobile users and trendy people.

6. Future Work

Since this is very emerging and recent technology, researchers can use their ideas any of mode into to our work.

We couldn't stand in front of the technology improvement and growth but research is the major factor for all innovation and technology growth.

References

1. R.Surendiran, K.Alagarsamy: An Extensive Survey on Mobile Security and Issues, International Journal of Computer & Organization Trends – Volume2 Issue1 -2012, ISSN: 2249 - 2593, Page 39 - 46
2. Bo Li and Eul Gyu Im: Smartphone, promising battlefield for hackers, Journal of Security Engineering , vol: 8 no: 1, 2011, pages 89-110
3. R.Surendiran, K.Alagarsamy: Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption, International Journal of Engineering Trends and Technology (IJETT) - Volume4 Issue5 - May 2013, ISSN: 2231-5381, Page 2217 - 2224
4. Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. 2011. Android permissions demystified. In Proceedings of the 18th ACM conference on Computer and communications security (CCS '11). ACM, New York, NY, USA, 627-638
5. Hossein Falaki, Ratul Mahajan Srikanth Kandula, Dimitrios Lymberopoulos, Ramesh Govindan, Deborah Estrin: Diversity in smartphone usage, Proceedings of the 8th international conference on Mobile systems, applications, and services, ISBN: 978-1-60558-985-5
6. R.Surendiran, K.Alagarsamy: A Crtitical Approach for Intruder Detection in Mobile Devices, SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – Volume1 Issue4 - June 2014, ISSN: 2348 – 8387, Page 6 - 14
7. W. Enck, M. Ongtang, and P. McDaniel. Understanding Android Security. IEEE Security and Privacy, 7(1):50–57, 2009.
8. Mcafee Wave secure: https://market.android.com/details?id=com.wsandroid
9. Survey about mobile theft in UK: http://news.bbc.co.uk/2/hi/uk_news/1748258.stm
10. Kyungwhan Park, Gun Il Ma, Jeong Hyun Yi, Youngseob Cho, Sangrae Cho, Sungeun Park:Smartphone Remote Lock an d Wipe System with Integrity Checking of SMS Notification, Consumer Electronics (ICCE), IEEE International Conference on 9-12 Jan. 2011 pages 263-264.
11. Survey about mobile theft in USA: http://www.symantec.com/about/news/release/article.jsp?prld=20110208_01
12. Online SMS sending portal: http://en.wikipedia.org/wiki/Way2SMS.com
13. Survey about mobile theft in India:http://asiarelease.asia/norton-survey- eveals-1-in-2-indians-is-avictim-ofmobile- phone-loss-or-theft/
14. Patrick Traynor et.al, "From mobile phones to responsible devices" in "Security and Communication Networks", Wiley Publications, Vol 4 , Issue 6, 2011
15. Dr.R.Surendiran: Secure Software Framework for Process Improvement, SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume 3 Issue 12 – December 2016, ISSN: 2348 – 8387,Page 19 – 25
16. Operating System: http://en.wikipedia.org/wiki/Android_%28operating_system%29
17. R.Surendiran, K.Alagarsamy: A Novel Tree Based Security Approach for Smart Phones, International Journal of Computer Trends and Technology, Volume 3 Issue 6 – 2012, ISSN: 2231 - 2803, Page 787 - 792
18. Karsten Sohr, Tanveer Mustafa, and Adrian Nowak. 2011. Software security aspects of Java-based mobile phones. In Proceedings of the 2011 ACM Symposium on Applied Computing (SAC '11). ACM, New York, NY, USA.
19. Android Emulator: http://developer.android.com/guide/developing/tools/emulator.html
20. Dr.R.Surendiran: Development of Multi Criteria Recommender System, SSRG International Journal of Economics and Management Studies (SSRG-IJEMS) – volume4 issue1 January 2017, ISSN: 2393 - 9125, Page 28 – 33
21. G. McGraw. Software Security: Building Security In. Addison-Wesley, 2006
22. Semantec Anti-theft: https://market.android.com/details?id=com.symantec.anti.theft
23. Android SDK: http://developer.android.com/sdk/android-2.3.html
24. S.Gavaskar, R.Surendiran, E.Ramaraj: Three Counter Defense Mechanism for TCP SYN Flooding Attacks, International Journal of Computer Applications, Volume 6– No.6, September 2010, ISSN: 0975 – 8887, Page 12 - 15

