IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

CYBER MOBILE HACKING APP CODE SURVEY AND DETCTION METHOD

Mr.M.Sakthivel,M.C.A,M.Phil(Phd)
Head and Assistant professor,
Department of Computer Science,
DR.R.K.Shanmugam College of Arts And Science,
Kallakuruchi

Mr.C.Anbarasan,M.Sc.MPhil.,
Assistant professor,
Department of Computer Science,
DR.R.K.Shanmugam College of Arts And Science,
Kallakuruchi

***Abstract*—** Nowadays people are eagerly waiting to peep into the others personal details, it's all about curiosity, passiveness or steeling the data. This may be for creating fun or sometimes in order to protect them from the different set of obstacles. With the help of the latest technology one can able to easily hack up the others phone but also it is not as easy as possible. The use of Smart phones has become very popular around the globe in this digital area and in recent days its user's number has increased at indefinite level, as everyone rush to explore the digital world. For experiment analysis, we used 90% of the data for training and the rest 30% for testing. Different experiments are conducted for each tagger independently. Having tested on the same data the performance analyses of the taggers are 86.56%,84.46% and 88.42% for CS, HMM tagger and Hybrid tagger respectively. Result from our experiment shows that adding of rule-based tagger performs better result than alphabet AZ Anti and TRF tagger alone. This paper describes the vulnerabilities found in Android based Smart phones and also describes the attacks like privilege escalation, privacy attack and other threats which are associated with these particular devices. In last section we discuss the possible countermeasure against the attacks and threats due to that, the Android Smart phones become vulnerable.

Keywords-Android Hack code, AlphabetAZAnti code,Signal Tool, Security password,virus code,TRF

I. INTRODUCTION

The Time signal app application stays topper in hacking someone's phone**.** It is extreme popular app that had been widely used in the United States. It would offer you more than 40 different features which makes you to achieve your goal. By using this you can hack up someone's smart phone easily. When you installed this application in the targeted device then through that sure you can start hack someone phone

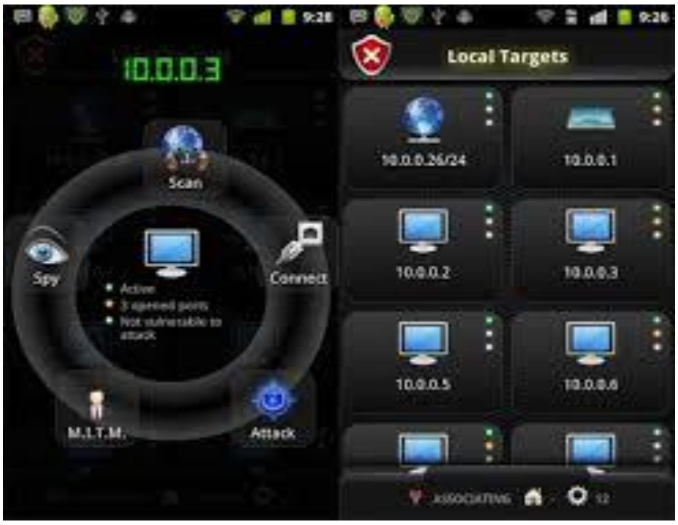


Fig 1: Timer Root hacking Function Target

Fig 2. AZAnti Virtual Hacking

Hacker Authentication

Two-factor authentication via WhatsApp Security Settings. With the end-to-end encryption and two-factor.

Wi-Fi Pass hacker

For example, you can use Cyclones Password Generator. Cyclones is a free password manager tool, and it comes with a number of features that can make your life easier. It can generate a strong password A@###^5&@@.

Fig 3. WhatsApp WIFI Hacker

First, if you suspect that someone hacked your WhatsApp account, you might want to remove the app, and then reinstall it several times. Some security experts say that reinstalling the app at different times of the day would also stop the WhatsApp hack from causing you more trouble. Removing and reinstalling the application is burdensome

Game App

SCAN APP 1 SYS
Add the ID to your Computer connect the scan App
ID1- 87654320859876@##$@
ID2-78543769546$$#@[10]##1064
SCAN APP2 SYS
File moving ##loop
Setting-Additional 10mns
Long Input-Keyboard
Dictionary-delete lean words board
2065-Enter the password
Switch key Board-Clear typing data
App Play store-download the App
Victims Account Successfully

Fig 4. Game Survey hacker

STEP 1

Cash App-Setting-Account Setting

Details 1012 hacking

Remove(no)fast 23

STEP 2

Remove Accounting

Setting-Account Setting

Managing Account

My Account SB112

Remove Account SB32

Fig 5. Identify online virus code

Fig 6. Cash app hacker

II. APP SETTING

ANDRORAT(APPLE)

MyAircell my jio App

Sign in to Myapp Samsung
Tap on 'Settings icon' from the Menu
Select 'Manage Accounts' VO
Tap on the 'Remove' icon5847 to remove the respective linked account(Apple)

Managing Account Setting

Login into the My Jio app.
Go to Settings > Add S=Set Manage Accounts.
All your accounts will be displayed there together in a list.
Tap on the delete icon/trash bin icon to remove the account add after the confirmation it will be removed.

Password Setting

Go to settings app > device settings display > manage device and remove any devices shown here
Change your password
Email at xxxcare@*jio*.com to log you out of all devices.

Fig 7. Password lock

The child involved can be your son or daughter. The major dilemma in this aspect is that children tend to become scared and hide their SMS' from their parents.

A tracking app would allow you to retrieve, check and read text messages of one another, thereby saving your kids, wife or husband from the trauma of going through the experience verbally

Spyic syn msg

Spyic is the answer to all your questions (and mine). It is an Android hacking tool that gives you complete control over the target device REMOTELY.

Fig 8. KiK Manager

Cocospy

Cocospy is an awesome Android mobile hacking tool that can work from any Android mobile phone.You can use your mobile phone to view what the other person is up to. You will get every bit of information about the target device, from pictures to messages to call records.With Cocospy.

Android hacking will feel like a piece of cake. You don't even need to have any technical knowledge of hacking at all!

Sensor No Root over Root:

If an app can hack an Android phone without rooting it, always go for it.

While rooting makes hacking an Android phone easy, it also compromises its security and yours. The data can be leaked to third-party sources. Also, the app can download many other virus-infected apps on the phone.

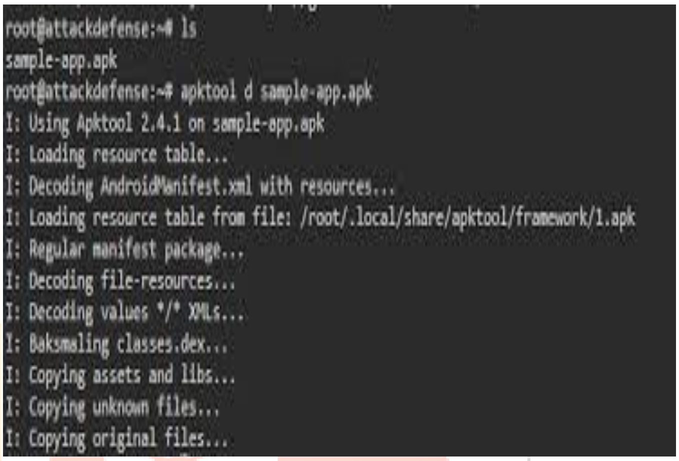
Rooting any phone can also make it prone to anonymous hackers who can then exploit the device.

III Spyware Detector - Anti Spy Privacy Scanner

TeamViewer for Android

Remotely control computers as well as transfer files to and from the remote computer. For commercial use, please observe these licensing notes.

Install TeamViewer QuickSupport on your mobile device to enable Windows, Mac, and Linux computers to connect to your Android, Windows 10 Mobile, or iOS device to provide you with assistance.



```
root@attackdefense:~# ls
sample-app.apk
root@attackdefense:~# apktool d sample-app.apk
I: Using Apktool 2.4.1 on sample-app.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Fig 9. Sensing run time code program

HP-613056

3DB Data MydataApp-link
My Idea(Port Number @##$$*#
Commend dump calling
IMEI Number
Setting Accessible unknown source
Zeal spy-Aclmslation-Enable
Pass-##$$@@@-7 hours
Call Log Enable

Fig 10.Spyware Root virus app

Scanning Process

A monitoring app must be detectable on the target device. Many wonder if it is possible to detect a spy app on Android devices.

Yes, there are some signs, which mean that you've got spying software installed on your device

Click on the "Tools" option, and then head to "Full Virus Scan."

When the scan is complete, it will display a report so you can see how your phone is doing and if it has detected any spyware in your cell phone. Use the app every time you download a file from the Internet or install a new Android app

Android Dummper

AndroDumpper is an application that you can use to find out if your access point is vulnerable to WPS protocol.

As usual, the application lets you carry out this check on any network, but it's recommended to use it exclusively on your own.

Fig 11.Dumpper Reader

To use the application correctly, you'll need to have a rooted device and the app Busybox installed. Even if this is not the case, you can still use the application, but the check without rooted privileges

AndroDumpper is an application with some really interesting features. Not only does it let you verify the security of your point of access, but it also lets you see all the passwords for all the WiFi networks that you have connected to from that Android device.

```
 Start
   My Jio 4G Data MydataApp-link
     My Idea (Port Number @##$$*#
     Commend dump calling
      IMEI Number own
     Setting Accessible unknown source
     Zeal spy-Aclmslation-Enable/24 hours
     Pass-##$$@@@-7 hours
     Call Log Enable
End
```

IV.CONCLUSION

Hacking has both its benefits and risks. Hackers are very diverse. They may bankrupt a company or may protect the data, increasing the revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end

In this work, at first, we discussed the current authentication problems, data protection and privacy problems. We investigated the vulnerabilities in smartphones and attacks that can occur in smartphones. Secondly, we have characterized identified attacks in contradiction of smartphones, concentrating on why attacks occur and what are their effects on smartphones. Finally, we have studied existing security results to prevent smartphones from infections, malicious codes and intruder's attacks.

REFERENCES

Gupta, A. (2014, March). Learning Pentesting for Android Devices (1st ed.).

Packtpub. (2015). Practical Mobile Forensics. Retrieved March 06, 2016, from https://www.packtpub.com/packtlib/book/ApplicationDevelopment/9781783288311/pref05

Casey, E., 2011, Digital evidence and computer crime: Forensic science, computers, and the internet, Academic press

Bommisetty, S., Tamma, R., & Mahalik, H. (2014, July). Practical Mobile Forensics (1st ed.). Birmingham, UK: Packt Publishing.

Ballano, M. (2014, August 11). Mobile Attacks: Cybercriminals' New Cash Cow. Retrieved March 06, 2016, from http://www.symantec.com/connect/blogs/mobile-attacks-cybercriminals-new-cash-cow

Chell, D., Erasmus, T., Colley, S., & Whitehouse, O. (2015). The Mobile Application Hacker's Handbook.

Lessard, J., & Kessler, G. (2010, September). Android Forensics: Simplifying Cell Phone Examinations. In Small Scale Digital Device Forensics Journal, vol. 4, no. 1.

Kaspersky. (2014, October). Mobile Cyber Threats. Retrieved March 06, 2016, from http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf

Hoog, A. (2011). Android Forensics Investigation, Analysis and Mobile Security for Google Android.

Wikipedia. (2015). WhatsApp. Retrieved March 06, 2016, from https://en.wikipedia.org/wiki/WhatsApp

Buchanan, I. (2015, September 9). 200 million Whatsapp users open to attack. Retrieved March

Global Positioning System. (2007, January 11). Countermeasures against GPS trackers. Retrieved March 06, 2016, from https://globalpositioningsystem.wordpress.com/2007/06/11/countermeasures-against-gps-trackers/

Statista. (2015). Number of monthly active WhatsApp users worldwide from April 2013 to September 2015 (in millions). Retrieved March 06, 2016, from

http://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/

TechAdvisor. (2011, September 12). WhatsApp Android app review. Retrieved March 06, 2016, from

http://www.pcadvisor.co.uk/review/android-tablet-apps/whatsapp-android-app-review-3302802/

The FORGE. (2015). Whatsapp: Overview. Retrieved March 06, 2016, from https://theforgecoc.wordpress.com/whatsapp-overview/

Wikipedia. (2015). Global Positioning System. Retrieved March 06, 2016, from https://en.wikipedia.org/wiki/Global_Positioning_System

Developers. (2015). Location Strategies. Retrieved March 06, 2016, from http://developer.android.com/guide/topics/location/strategies.html

Wu, X., & Li, X. (2013, October). Hack android application and defense. In Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on (pp. 676-680). IEEE.