JOURNAL OF APPLIED SCIENCES RESEARCH

ISSN: 1819-544X
EISSN: 1816-157X
2016 May; 12(5): pages 8-13

Published BY **AENSI Publication**
http://www.aensiweb.com/JASR
Open Access Journal

Detecting Camera Based Traitor and Fraudulent Apps on Smartphone

[1]A. Palaniraj, [2]L. Indu, [3]S. Iniyan, [4]J.S. Umashankar

[1]Information Technology, Panimalar Institute of Technology, Chennai, India.
[2]Computer Science and Engineering, P.B. College of Engineering, Chennai, India.
[3]Computer Science and Engineering, SRM University, Chennai, India.
[4]Information Technology, Panimalar Institute of Technology, Chennai, India.

Address For Correspondence:
A.Palaniraj, Information Technology, Panimalar Institute of Technology, Chennai, India.
E-mail: palaniraj.kpm@gmail.com

ABSTRACT

In recent trends, android smartphones are rapidly in use by more number of users because of its user friendly and open source architecture. There are millions of android applications are assessible in the open market place. But we cannot trust most of the apps, which may steals the user privacy content or any confidential data. However some works have studied mobile phones multimedia securities and also android permissions. In this paper to center of attention on the protection problems regarding camera headquartered assaults on smartphones. The fraudulent application and its traitor can be well identified through utilising the security method that detects the attacks. By use of the defense system the users can be saved before capturing into the vulnerability. To investigate out the safety system we now have scheduled a camera established fraudulent application for feasibility study and likewise we analyzed the performance of the approach with the fraudulent operations from the open android market.

KEYWORDS: Fraudulent application, Defense System, Android, Security on Privacy

INTRODUCTION

Men and women from all round the arena are switching to the smartphones, for the reason that the smartphones performs vital roles in the each day pursuits of probably the most peoples. On considering the collection of smartphones, generally categorized by means of the operating system. A survey on Business Insider [6] says that on 2011 the android users were 51.4%, iPhone 33.0%, Blackberry 8.3%, Microsoft windows phone 3.1%, palm 1.6% and others 2.6% which concludes that most of the users prefer the android smartphones. Another survey recently by the Business Insider [8] says that According to Strategy Analytics, Android devices were sold 81% on most smartphones on 2014. So, the global smartphone market increased 30%, from 1billion to 1.3 billion. More researches have done on android security breaches.

The Android running approach lacks in security, so we must discover the various possible attacks on Android OS to improve the security. [1] Some of the possible attacks are Remote controlled monitoring attack, Application-oriented attack, Screen unlocking attack, Camera based attack model .In this analysis , In this evaluation , we're specializing in the security issues of digital camera established attacks model. A defense system is developed to check the permission of the application to detect the fraudulent application. The camera based attack uses the permission of built-in Camera (com.android.gallery3d). [3] Defense system checks the permission of the installed application using Check Permission () method of Activity Manager Service. Moreover to that we proposed a Camera based attack (fraudulent application) which cannot be detected by major mobile ANTI VIRUS apps and Options to view important points file / do away with the fraudulent app before coming into the attack. Further we detect the traitor (hacker's mail) of the fraudulent apps using manual

reverse engineering and search procedure. The feasibility of the safeguard procedure is measured by detecting the proposed camera headquartered attack application and also with various fraudulent applications from the Android play retailer.

Related Work:

Many analysis have achieved to receive the disorders of hacking the exclusive knowledge and media making use of the mobile camera in an android smartphones [1]. The camera centered assault model has been proposed to hack the user's multimedia via the built in digital camera. The procedure should run silently with none alert so that the consumer can't determine the assault. A gentle weight security scheme was proposed with the aid of Longfei Wu and Xiaojiang Du [1] supplies protection from many vulnerabilities and assaults. However it breaks down to analyze the traitor of the assaults. [2] The Android malware has the fast growth on the open android market place so the security scheme can support to resolve the security problems. The Malware can also be established on the cellular process through making use of Repackaging, replace assault or drive-through download. The main antivirus software like AVG, Lookout, Norton and TrendMicro are fails to notice lots of the digital camera situated attacks and in addition the malwares. Every packages / newly installed Android applications can control the system resources with permissions.

Some of the permissions are BLUETOOTH, READ_CONTACT CAMERA, WRITE_SETTINGS, CHANGE_WIFI_STATE and CALL_PHONE, etc. [3] Android version 2.2, categorizes 134 permission into three stages of threats:

1. Typical permissions
2. Dangerous permissions
3. Signature/System permissions

Erika Chin [4] offered an instrument known as ComDroid, that discover the vulnerabilities on inter application communication. It can be utilized by builders to research the functions. From Play retailer 20 functions had been analyzed with ComDroid instrument which detects 34 vulnerabilities.

Proposed Work:

To resolve the issues and protection breaches, we have projected an improved defense system with the ability of detecting the fraudulent application and its traitor. The traitor could be found only on the application with inter communication attacks (i.e.) having access to mailing the multimedia contents to the hackers mail account.

Problem Description:

The employment of the improved defense system needs a fraudulent application with traitor. So we have developed a camera based spy camera (CALC) to catch the users face and to mail it to the traitor without any background experiences. The fraudulent app turns off the sound and vibration of the mobile, using the system setting. To mute the sound and vibration, set the flag to 0 for FLAG_REMOVE_SOUND_AND_VIBRATE permission of the system. And the camera takes the picture of the victim without their knowledge then it will be mailed to the traitor

System Architecture:

We provide SQLite database entry for the improved defense approach to avoid intrusion from malwares.

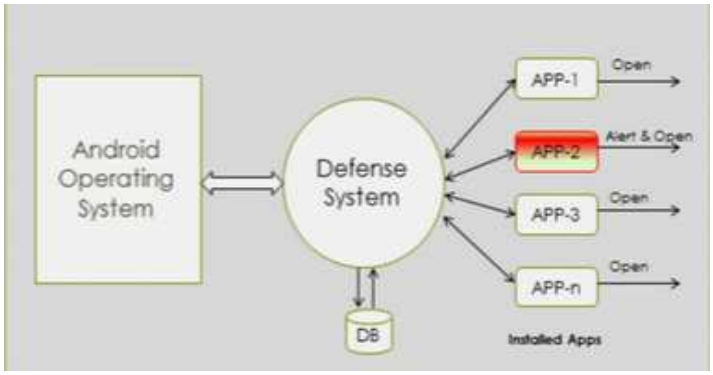

Fig. 1: Detecting fraudulent Application using improved Defense System

The safeguard process is acting like a firewall between the android working system and with the mounted system functions. Fig 1 demonstrates that an alert will arise if the any application access the constructed in

camera (com.Android.Gallery3d) and likewise studies the traitor via utilizing the reverse engineering mechanism [7] beneath the alert information.

Improved Defense System Development:

We have advanced and upgraded the defense system with three major actions: (1) Application is authenticated with SQLite database to avoid malware attacks. (2) Improved the defense scheme with options to report or uninstall the fraudulent apps. (3) The traitor's information (mail id) is retrieved using the Adro Guard reverse engineering process [9]. As Fig 1 demonstrates that the system will alert a message only for the fraudulent applications. And the alert will be as a dialog message with detailed note of the package information (ex: com.example.calcspy) and also vibration, voice alert. The permission level of the applying is detected with the aid of modifying the DEX file as shown in Fig 2.

Fig. 2: Checking Fraudulent APK permissions

By checking the permission of the packages we can encounter the fraudulent application. The traitor of the fraudulent application can only be found if the permission of the fraudulent APK has both android Permission ACCESS_CAMERA and also INTERNET.

Implementation of Fraudulent Application:

To analyze the utility of the proposed extended safety structure, we have advanced camera centered fraudulent software [1]. The user interface of the fraudulent software is a straightforward calculator which runs the digicam venture heritage and does now not cause any consumer alert. Fig 3 shows the calculator fraudulent app's digicam assault. The structure involves the next steps.

Step 1: Resource utilization by considering the power consumption, CPU and memory usage to intrude into the camera and gallery without user's knowledge.

Step 2: Setting flag 0 to sound and vibration

Step 3: Hiding preview of the camera.

Step 4: Capture the front camera and save in Storage.

Step 5: Recover the sound and vibration.

Step 6: Send out the photo via mail.

To experiment the efficiency of fraudulent app, we set up AVG cell antivirus app. The Antivirus does not file/ warns the person about the vulnerability of the fraudulent utility for the duration of hidden digicam assault.

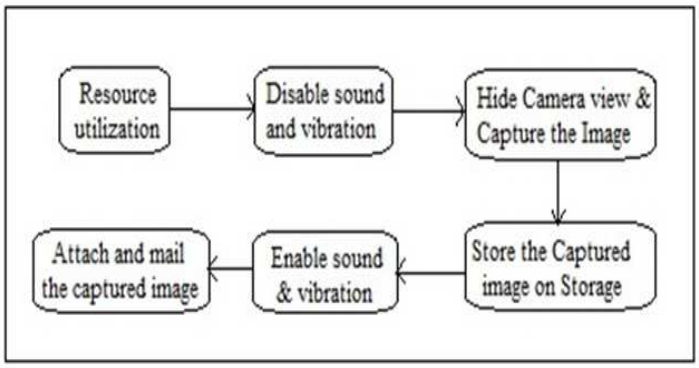

Fig. 3: Fraudulent Application work Process (calculator)

Feasibility of Defense system with proposed fraudulent app:

Since android play store has more number of fraudulent apps [2]. We have chosen some of them like Simple Notepad, Spy Camera, Hidden Camera, etc. We tested the utility of the improved defense system by opening the fraudulent applications. When the fraudulent apps started through the system, it will alert the user with a message along with detailed note. The alert will be in terms of a vibration and also voice clip. To detect the traitor of the fraudulent application which is proposed, we further doing a reverse engineering process to identify the mailing address from the package. The defense system is feasible than the mobile antiviruses to

detect the camera based attacks on android phones.

Reverse Engineering:

Reverse Engineering to APK [10], which is the course of decompiling and repackaging the executable apk file. As a way to observe the traitor of the fraudulent application, we are focusing on to retrieve the supply of the false app to become attentive of the hacker's mail id. As we know android is open supply, anyone can recreate the purposes by using enhancing the prevailing code. The following is the steps clever algorithm for repacking an executable apk file for detecting the traitor

Step1: Open the manifest.xml file included in the apk
Step2: Modify the file by injecting attribute "android: name" to "somename.class"
Step3: Convert the binary xml to text and repackage it to apk using apk tool.
Step4: Detect the source packages using decompilation.
Step5: Identify the traitor information from the source file by search procedure.

Experimental Results And Description:

Both Improved Defense System and CalcSpy (Fraudulent App) are successfully tested on front end camera equipped Android Phone (Galaxy Note) Fig 4. Indicates the alert message of fraudulent application calcspy (fraudulent application) seeking to launch from the defense procedure. Alternative can be used to ignore the message and likewise can view the detailed happen of the appliance launching the digital camera. The happen file comprises the package knowledge of the applying. Considering that the android system makes usage of targeted programs of the system level and hooked up applications, we are able to become aware of the malwares or false applications through determining the title of the package deal com.example.Calcspy

To notice the fake utility, the improved safety procedure tests the take place file of the functions. The show up has all knowledge concerning the package and the permissions. We used checkPermission() method to get the digital camera based attacks and the alert message is projected toward the consumer. Due to the fact that the attackers hacks the camera without person notification, the defense approach will provide such mechanism of alert to restrict silent camera entry with the aid of the fraudulent apps.

Fig. 4: Improved Defence system against fraudulent Applications (Tested on CalcSpy)

The Fraudulent Applications runs the camera silently on background task and captures the user front camera image and stores on the storage space using get External Storage Directory method. Fig 5 displays the implementation of the calculator fraudulent application. Once the activity of capturing the front camera image, the Image is compressed to 300 x 300 bitmapped image. The compression process is required to uninterrupted attachments of the secrete images from the storage space. Then it is attached to Mail account of the traitor. We have now experimented the fraudulent application with the elevated protection process to detect the undertaking. And on the whole development, the anti-virus does not warns any alert of the false utility but our proposed procedure has detected the digital camera situated attack and further we examined the traitor making use of the reverse engineering mechanism which we already discussed early.

Fig. 5: CalcSpy (Fraudulent Camera Based Attack)

Performance Evaluation:

In this article, we proposed a CalcSpy fraudulent utility to put in force the digital camera established attack. We proposed the appliance to research the feasibility of the safety method. The system detects the false apps and alerts/ warns person about the digicam recreation is going on the problem software. On present procedure, as a outcome of continues heritage procedure of the security pastime. The procedure annoys the person with alert messages and in addition detects the trusted utility as a fraudulent. Comparing with the prevailing scheme, our proposed architecture acts as a middle layer between the android working approach and the hooked up applications for fraudulent detections. We find a approach to detect the traitor's mail by applying the reverse engineering using the open source apktool. The process converts the application to source code for detecting the traitor's mail id.Another way is to sending a report to the goggle for invalid permission activity of the fraudulent application.

Conclusion:

In this paper, we have proposed an improved defense system to detect the camera based attack and enhanced with reporting mechanism. We further progressed to attain the traitor of the fraudulent application. The feasibility of the improved defense system is analyzed with several fraudulent applications from the Google play store. And we have developed our own fraudulent calculator application to capture the front camera of Galaxy Note Android phone. We further planned to enhance the defense system to detect various intruder attacks like Passcode attack, SMS and Phone conversation attacks.

REFERENCES

1. Longfei Wu and Xiaojiang Du, 2014. "Security Threats to Mobile Multimedia Applications Camera-Based Attacks on Mobile Phones," IEEE Communications Magazine.
2. Zhou, Y. and X. Jiang, 2012. "Dissecting Android Malware: Characterization and Evolution," IEEESymp. Security and Privacy, pp: 95-109.
3. Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, David Wagner, "Android Permissions Demystified" CCS'11, October 17–21, 2011, Chicago, Illinois, USA. Copyright 2011 ACM 978-1- 4503-0948-6/11/10.
4. Vaibhav Wanjale, Abhijit Dhapte, Sarita Morey and Prof. Mrs. Neha Koria, 2014. "AAPS Android Based System for Camera Based Attacks" International Journal of Emerging Technologies and Engineering (IJETE) 1(10): 2348-8050.
5. Erika Chin, Adrienne Porter Felt, Kate Greenwood and David Wagner, 2011. "Analyzing Inter- Application Communication in Android" MobiSys'11, June 28–July 1, 2011, Bethesda, Maryland, USA. Copyright, pp: 978-1-4503.
6. Survey of Smartphones by Business Insider on 2011. http://www.businessinsider.com/smartphone- survey-results-2011-4?op=1
7. Optimization Routing Using Secure Reverse Multicast Bellman Ford Adhoc Routing and Ant Protocol in Manet, 2015. Australian Journal of Basic and Applied Sciences, 9(2).
8. Strategy analytics of Android by Business Insider on 2015."http://www.businessinsider.com/android-1-billion-shipments-2014-strategy-analytics.

9. Andro Guard for reverse engineering “https://code.google.com/p/androguard/wiki/RE”
10. Patrick Schulz, Felix Matenaar 2013. “https://bluebox.com/wp-content/uploads/2013/05/AndroidREnDefenses201305.pdf.
11. Carlos A. Castillo “Android Malware Past, Present, and Future” Mobile Security Working Group, McAfee
12. UNICODE, 2016. Text Security Using Dynamic and Key-Dependent 16x16 S-BOX, Australian Journal of Basic and Applied Sciences, 10(1): 26-36.