ATTACK ON SPY CAMERA AND FINDING FRAUD APPLICATIONS ON GOOGLE STORE

Prachi Chaskar[1], Pooja Dangat[2], Divya Guldhekar[3], Shubhangi Sukale[4] , Gore Swati[5]

ABSTRACT

System focus on the security issues related to camera based attacks on smart phones. The fraudulent application and its traitor can be detected by using the defense system that detects the attacks. To evaluate the defense system we have proposed a camera based fraudulent application for feasibility study and also we analyzed the performance of the system with the fraudulent applications from the open android market. To download application smart phone user has to visit play store. When user visit play store then he is able to see the various application lists. This list is built on the basis of promotion or advertisement. User does not have knowledge about the application. So user looks at the list and downloads the applications. But sometimes it happens that the downloaded application wont work or not useful. That means it is fraud in mobile application list. We are going to find the applications those are fraud, from Google play store. We are providing sentiment analysis on the reviews, for finding true positive and false negative of the reviews and also working on NLP algorithm from which we are finding positive comments, negative comments and neutral comments.

***Index Terms*—attacks, fraudulent ,Google Play Store, NLP**

I. INTRODUCTION

The Android operating system (OS) has enjoyed an incredible rate of popularity. Android OS holds 79.3 percent of global smartphone market shares. Meanwhile, a number of Android security and privacy vulnerabilities have been exposed in the past several years. Although the Android permission system gives user an opportunity to check the permission request of an application before installation, few users have knowledge of what all these permission requests stand for; as a result, they fails to warn users of security risks. Meanwhile, there are increasing number of apps specified to enhance security and protect user privacy have appeared in Android app markets. Most large anti-virus software companies have published their Android-version security apps, and tried to provide a shield for smartphones by detecting and blocking malicious apps. In addition, there are data protection apps that provide users the capability to encrypt, decrypt, sign, and verify signatures for private texts, emails and files. However, mobile malware and privacy leakage remain a big threat to mobile phone security and privacy.

Nowadays, people carry their phones everywhere; and, their phones see lots of private information. If the phone camera is exploited by a malicious spy camera app, there may occur serious security and privacy problems. For example, the phone camera may record a user’s daily activities and conversations, and then send these out via

the Internet or multimedia messaging service (MMS). Secret
capturing photography is not only immoral but also illegal in some countries due to the invasion of privacy. Nevertheless, a phone camera could also provide some benefits if it is controlled well by the device owner. For example, when the owner wants to check if someone has used his/her phone without permission, the phone camera could be used to record the face of an unauthorized user. Besides, it can also help the owner find a lost phone. Can also use to take faster back up generation of the applications available in android system. And can be share easily with another user easily.

II. PROBLEM DEFINITION AND SCOPE

A. Problem Statement

Although in the existing approaches can be used for anomaly detection from rating and review records, they are not able to extract fraud evidences for a given time period (i.e., leading session) and are not able to detect ranking fraud happened in Apps historical leading sessions. There is no existing benchmark to decide which leading sessions or Apps really contain fraud. So our system helps to overcome this problems.

B. Goals and Objectives

- Natural Language Processing
- Background processes detection
- Mobile location tracking
- Fraud app detection
- Detecting Attack on camera

C. Statement of Scope

It is difficult to develop a system that makes all requirements of the user. User requirements keep changing as the system is being used. Some of future enhancements that can be done to this system are:

- As the technology increasing, it is possible to upgrade the system and can be adaptable to desired environment.
- Because it is based on object- oriented design, any further change can be easily adaptable.
- Based on the future security issues, security can be improved using emerging technologies.
- Mobile Tracking module can be added
- Face Detection module can be added
- Fraud App module can be added.

III. PROPOSE SYSTEM

We are going to develop system in which we done android applications for the security purpose (i.e. unwanted activates) which occur on the mobile phone.

In which system contain four type of security issues like camera hacking, mobile tracking, fraud apps detections on the basis of NLP and backup generations.

IV. IMPLEMENTATIONS

Face Detection Algorithm:

It is assumed that by combining the detected regions from algorithms, skin region is extracted. Thus, three algorithms are combined assuming that their combination gives the skin region from the image and from the skin detected image face is extracted by first extracting facial features and then drawing a bounding box around the face region with the help of facial features.

Spyware Algorithm:

Spyware collects personal information from user's phone such as contacts, call history and location. Personal spyware are able to gain physical access of the device by installing software without user's consent. By collecting information about user's phone, they send that information to attacker who installed the app rather than the author of the application.

Fraud App Detections Algorithm:

Fraudulent behaviors in Google's Android app market fuel search rank abuse and malware proliferation. We investigate three types demonstrations through our system that is Ranking base demonstration, Rating base demonstration, Review base demonstration, by developing the system which combines ranking, rating and review behaviors through statistical mining base assumptions test. We block the malware when the application is downloading.

Camera Based Attacks on Smart Phones Algorithm:

Generally when talking about privacy protection, most smart phone users pay attention to the safety of SMS, emails, contact lists, calling histories, location information, and private files. Since they are mobile and used as everyday gadgets, they are susceptible to get lost or stolen. Hence, access control mechanisms such as user authentication are required to prevent the data from being accessed by an attacker. However, commonly used authentication mechanisms like PINs, passwords, and Android Unlock Patterns suffer from the same weakness: they are all vulnerable against different kinds of attacks, most notably shoulder-surfing. The system focus on the Android platform and the aim is to systematize or characterize existing Android malware. As a result mobile security is no longer immanent, but imperative. This survey paper provides a concise overview of mobile network security, attack vectors using the back end system and the web browser, but also the hardware layer and the user as attack enabler

V. SYSTEM

A. Figures

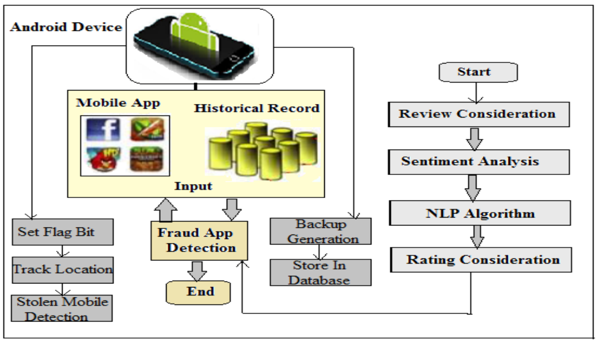

Figure 1 System Architecture

1. User Registration

The users of the system have to firstly register with the application before going ahead and logging into it. The registration consists of firstly choosing the set of alphanumericcharactersthattheuserdesiresforsettingthepasswordandUserbasic information i. e. Email-id, Name etc. For more security the user also gives a image password which will in turnbe hidden in the set of images that the user had selected. During logging in the user is asked to type the text password which is matched to the text which will be retrieved from the images which was stored during the registration.

2. Camera Access Module

We use picture method of camera to detect attack on cameras. Our system check that when this method is called and by whom this method is called.

3. Fraud App Detection Module

We have chosen some of them like Simple Notepad, Spy Camera, Hidden Camera, etc. We tested the feasibility 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 antivirus to detect the camera based attacks on Android phones.

4. Stolen Mobile Detection

We are going to develop an Android application such that when a user loses his/her phone, the spy camera could be launched via remote control and capture what the thief looks like as well as the surrounding environment. Then the pictures or videos along with location information (GPS coordinates) can be sent back to the device owner so that the owner can pinpoint the thief and get the phone back. We conduct a survey on the threats and benifits of spy cameras.

5. Review Ranking

In addition ratings, most of the App stores also permit users to write some textual comments as App reviews. Such reviews can indicates the individual perceptions and usage experiences of existing users for particular mobile Apps. Indeed, review manipulation is one of the most valuable perspective of App ranking fraud. Specifically, before downloading or purchasing a new mobile App, users usually first read its historical reviews to ease their decision making, and a mobile App contains more encouraging reviews may captivate more users to download.

VI. DESIGN AND ANALYSIS

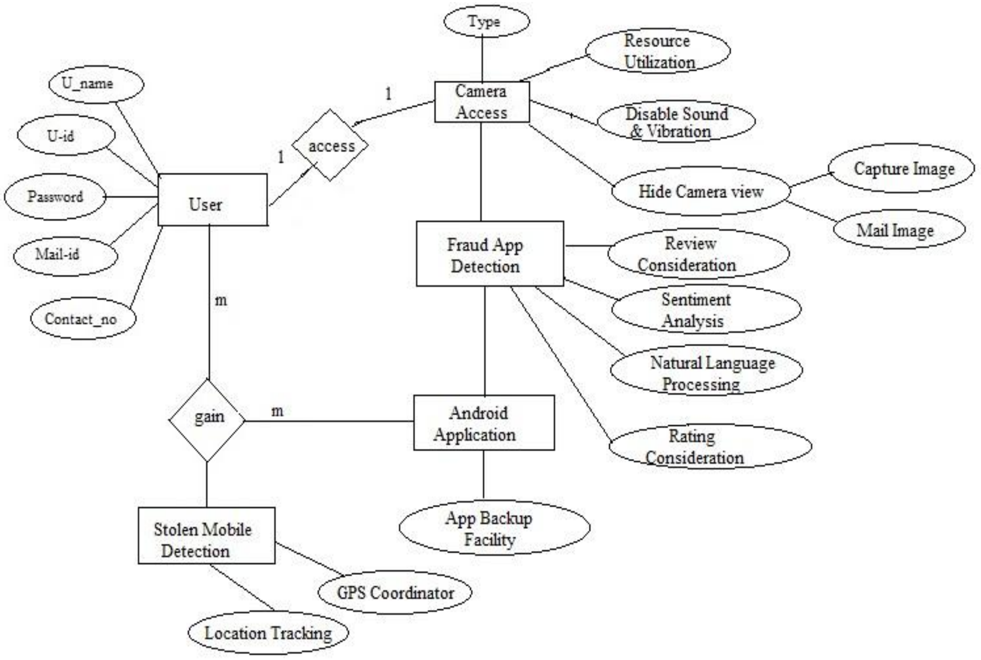

Figure 2 System ER Diagram

VII. RELATED WORK

Fraud behaviors in Android app market fuel search rank abuse and malware proliferation. We present Fair Play, a novel system that uncovers both malware and search rank fraud apps, by picking out trails that fraudsters leave behind. To identify suspicious apps, Fair Plays PCF algorithm correlates review activities and uniquely combines detected review relations with linguistic and behavioral signal from longitudinal Google Play app data. We contribute a new longitudinal app dataset to the community, which consists of over 87K apps, 2.9M reviews, and 2.4M reviewers, collected over half a year. Fair Play achieves over 95 per accuracy in classifying gold standard datasets of malware, fraudulent and legitimate apps. We show that 75per of the identity malware apps engage in search rank fraud. Fair Play discovers hundreds of fraudulent apps that currently evade Google Bouncers detection technology, and reveals a new type of attack campaign, where users are harassed into writing positive reviews, and install and review other apps.

Generally when talking about privacy protection, most smart phone users pay attention to the safety of SMS, emails, contact lists, calling histories, location information, and private files. Since they are mobile and used as everyday gadgets, they are susceptible to get lost or stolen. Hence, access control mechanisms such as user authentication are required to prevent the data from being accessed by attacker. However, commonly used authentication techniques does not provide that much security to the user mobile phone: they are all being perform vulnerable activities against different kinds of attacks. In this system, we focus on the Android platform and aim to systematize or characterize existing Android malware. As a result mobile security is no longer immanent, but imperative. For that, this system provides concise overview of mobile network security, attack vectors using the back end system and the web browser, but also the hardware layer and the user as attack enabler

Ranking fraud in the mobile App market refers to fraudulent or deceptive activities which have a purpose of bumping up the Apps in the popularity list. It becomes more easy to android app developer to use different shady means, such as in flating their Apps sales or posting phony App ratings, to Commit ranking fraud. Where there is limited scope in ranking fraud has been widely recognized, there is limited understanding and research in this area.At the end of system, we provide a holistic view of ranking fraud and propose ranking fraud detection system for mobile Apps. Specifically, we first propose to accurately locate the ranking fraud by mining the active periods, namely leading sessions, of mobile Apps. This is one of the leading topic which is playing important role in detecting fraudulent apps in applications store. Furthermore, we investigate three types of evidences, i.e., ranking based evidences, rating based evidences and review based evidences, by modeling Apps ranking, rating and review behaviors through statistically prostheses tests. In addition, we are going to design system in that an optimization based aggregation method to integrate all the evidences for fraud detection. Finally, we evaluate the proposed system with real-world App data collected from the iOS App Store for a long time period. We increase effectiveness of the proposed system, and shows the increased scalability of fraud app detection algorithm and some regularity of ranking fraud activities.

VIII. CONCLUSION

Now day’s lots of Android device used Android has very less restrictions for developer team, increases the security risk for People. Reviewed security issues in the Android based Smartphone. The integration of technologies into an application certification process requires overcoming logistical and technical challenges. Android provides more security than other mobile phone platforms. Moreover, in this project study camera-related vulnerabilities ,fraud apps and face detection in Android phones for mobile multimedia applications. We develop the system which plays important role that help to find detection of attack on camera that will benefit mobile users.

REFERENCES

[1] Longfei Wu and Xiaojiang Du, Temple University Xinwen Fu, University of Massachusetts Lowell, Security Threats to Mobile Multimedia Applications: Camera-Based Attacks on Mobile Phones IEEE Communications Magazine March 2014.

[2] Ezra Siegel. Fake Reviews in Google Play and Apple App Store. Appentive, 2014

[3] Zach Miners. Report: Malware-infected Android apps spike in the Google Play store. PCWorld, 2014.

[4] Stephanie Mlot. Top Android App a Scam, Pulled From Google Play. PCMag, 2014 .

[5] Daniel Roberts. How to spot fake apps on the Google Play store. Fortune, 2015.

[6] Andy Greenberg. Malware Apps Spoof Android Market To Infect Phones. Forbes Security, 2014.

[7] Jon Oberheide and Charlie Miller. Dissecting the Android Bouncer. SummerCon2012, New York, 2012. [8] VirusTotal - Free Online Virus, Malware and URL Scanner. https://www.virustotal.com/, Last accessed on May 2015.

[8] AsafShabtai, Uri Kanonov, Yuval Elovici, ChananGlezer, and Yael Weiss. Andromaly: a Behavioral Malware Detection Framework for Android Devices. Intelligent Information Systems, 38(1):161–190, 2012

[9] Michael Grace, Yajin Zhou, Qiang Zhang, ShihongZou, and Xuxian Jiang. Riskranker: Scalable and Accurate Zero-day Android Malware Detection. In Proceedings of ACM MobiSys, 2012

[10] BhaskarPratimSarma, Ninghui Li, Chris Gates, Rahul Potharaju, Cristina Nita-Rotaru, and Ian Molloy. Android Permissions: a Perspective Combining Risks and Benefits. In Proceedings of ACM SACMAT, 2012

[11] Chia-Mei Chen, Je-Ming Lin, Gu-HsinLai,National Sun Yat-sen University Kaohsiung, Taiwan "Detecting Mobile Application Malicious Behaviors Based on Data Flow of Source Code,2014 International Conference on Trustworthy Systems and their Applications.

Divya S. Guldhekar:
Perceiving BE in Department of Computer Engineering, Jaihind College of Engineering, kuran, Maharashtra, India.

Shubhangi R. Sukale:
Perceiving BE in Department of Computer Engineering, Jaihind College of Engineering, kuran, Maharashtra, India.

Prof. Swati Gore:
Department of Computer Engineering, from SavitriBai Phule Pune University,5 year Experience teaching, Working Assistant Professor in Jaihind College of Engineering, kuran, Maharashtra, India.

Prachi D.Chaskar:
Perceiving Department of Computer Engineering, Jaihind College of Engineering, kuran, Maharashtra, India.

Pooja A. Dangat:
Perceiving BE in Department of Computer Engineering, Jaihind College of Engineering, kuran, Maharashtra, India.