ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

Defence Mechanism for Camera Based Attacks in Android Phones

BabySyla L
Assistant Professor, Dept. of Computer Applications, College of Engg., Trivandrum, Kerala, India

Abstract
This paper aims at presenting camera based attack on android phones and implement a defense scheme to eliminate the threat against attacks. As the most popular mobile operating system, Android security has been extensively studied by researchers. Although the Android permission system gives users an opportunity to check the permission request of an application (app) before installation, few users have knowledge of what all these permission requests stand for as a result, they fail to warn users of security risks. Secret photography is not only immoral but also illegal in some countries due to the invasion of privacy. A phone camera could also provide some benefits if it is controlled well by the device owner.
The research work is divided into has 2 phases. First through a malware app take the pictures, and record videos of user secretly and send those to a remote server without user's attention which explains the remote attack. Second part is a defense mechanism against camera based attack. By installing the defense app will let the user know that if he/she is a victim of camera based attack. If it founds that the user's phone is under attack user can uninstall the app.

Keywords
Android, Camera based attacks Detection, Défence, Malwares, Threats

I. Introduction

The aim of this paper is to implement remote controlled real time monitoring attack on android phones and to propose a defence scheme against that attack. The entire work is divided into two parts. The first part is to implement camera based attack using malicious app which can work remotely as well as by user interaction. The second part is to implement defence mechanism for detecting camera based attacks on android phone and take necessary action against those kinds of apps.

II. Problem Definition

Since 2007, the Android operating system (OS) has enjoyed an incredible rate of popularity. As of 2016, the Android OS holds 96.8 percent of global Smartphone market shares. Meanwhile, several Android security and privacy vulnerabilities have been exposed in the past several years. Although the Android permission system gives users an opportunity to check the permission request of an application (app) before installation, few users have knowledge of what all these permission requests stand for; as a result, they fail to warn users of security risks. Generally, when talking about privacy protection, most Smartphone users pay attention to the safety of SMS, emails, contact lists, calling histories, location information, and private files. They may be surprised that the phone camera could become a traitor; for example, attackers could stealthily take pictures and record videos by using the phone camera. Nowadays, various types of camera-based applications have appeared in Android app markets (photography, barcode readers, social networking, etc.). Spy camera apps have also become quite popular. As for Google Play, there are nearly 100 spy camera apps, which allow phone users to take pictures or record videos of other people without their permission. Phone users themselves could also become victims. Attackers can implement spy cameras in malicious apps such that the phone camera is launched automatically without the device owner's notice, and the captured photos and videos are sent out to these remote attackers.

III. Methodology

The project is divided into 2 modules. In the first module, a spyware application is developed which looks and functions like a normal app but in the background, it acts like a spy cam that can take pictures, videos capture sound, detect GPS coordinates of the victim and send these details to hacker or whoever it may concern. The main idea behind this first module is to give an idea that how remote attack is implemented and though which all techniques hacker hijacks a user's personal data's.
Second Module is used to show how user can bypass camera based attack. After installation app scans for malware apps which steals user's data and alerts the user. User can then uninstall the application if he founds that the app is not safe.

IV. Requirement Analysis And Specifications

Requirement definition is the high abstract description of requirements. Requirements may be functional or non-functional.

i. Functional Requirements

- Malware App Functions includes the following
- Stealthily Record videos
- Find if screen is off and captures Images
- Stealthily Records sounds
- Stealthily Detects GPS coordinates of Users
- Can be controlled remotely and can be launched and stopped in a certain timeframe
- Can send data to web server
- Defense App Functions
- Stealthily run in background
- Report to user whenever a camera hacking malware functions
- Can produce popup messages and alert the user by producing sounds and vibrations.

ii. Non-Functional Requirements

Non-functional requirements define the general qualities of the software product. Non-functional requirement is in effect a constraint placed on the system or on the development process. They are usually associated with the product descriptions such as maintainability, usability, portability, etc. It mainly limits the

solutions for the problem. The solution should be good enough to meet the non-functional requirements. The system must be capable for offering speed as well as accuracy. Quality requirements such as reliability, availability, safety, security must be checked.

V. System Architecture

The system architecture for the project, it gives out an overall idea about the project. The proposed method includes two main phases 1) Explaining Camera based Remote Attack 2) Defence Mechanism against Camera based attack.

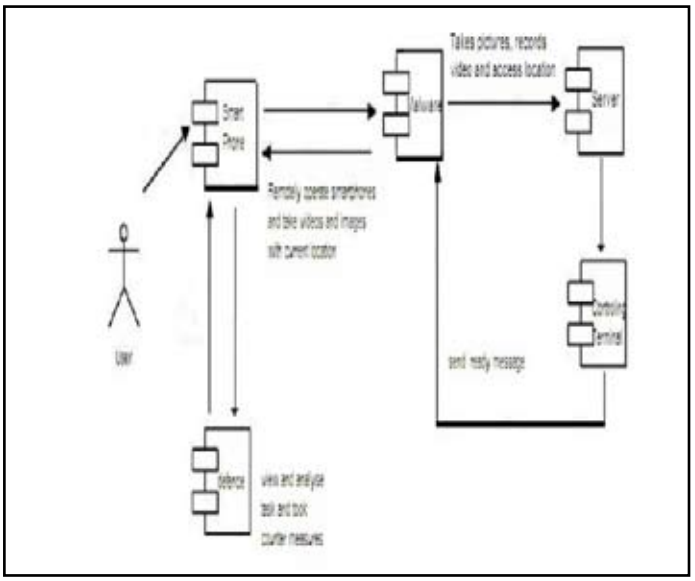


Fig 1: System Architecture

A. Camera Based Remote Attack

For explaining camera based Remote attack there is an android application as well as a java server webpage console. Android application in first look will be looking like a normal calculator. It also performs the function of a normal calculator. But malicious codes are written in the backend of the calculator. To start the process web server is started using Apache Tomcat v.7.0. the URL of the webpage is copied from clipboard and pasted to a browser's clipboard. Then on the android application set the IP address of the Machine. This can be done by long pressing the tile selection in the android phone. After that long press button 4 in the calculator in the same way long press 5, 6 and 7. Long pressing 4 will take picture anonymously without any notification or sound. In the same way 5,6 is used to record the sound. Long pressing 7 will start video recording. After few seconds long press 7 again to cut the recording. After doing this go to server page. This is where anonymous data are collected. Web server indicates that a hacker is accessing these data from a remote location. On the connect to phone option it can see different options like take picture record videos, record audio etc. in this way hacker can view and download these data's and perform camera based attack remotely.

B. Defence Mechanism Against Camera Based Remote Attack

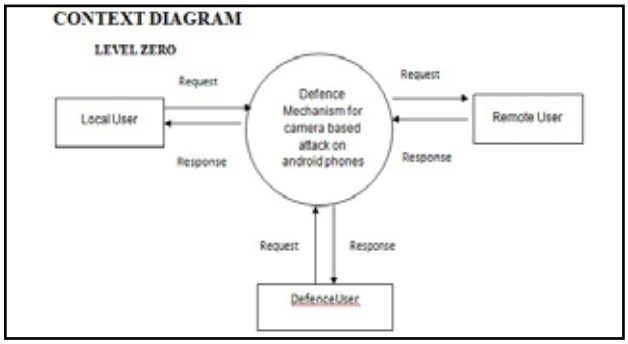
If the user feels like his phone is under camera based attack user can install this app and remove those spyware applications. Normal antivirus apps does not detect camera based remote attacking spyware applications and that's where defence app plays a major role. Scanning is based of 3 ways based on malware package names, permissions, signatures. After installing this app user can scan his/her phone and if it detects any threat it will alert the user by popping an alert box. User can either ignore the warning or simply uninstall the app.

4.3 UML DESIGN

The Unified Modelling Language (UML) is a standard language for writing software blue prints. The UML may be used to visualize, specify, constructs, and document the artifacts of a software-intensive system. UML is a very expressive language, addressing all the views needed to develop and then deploy all types of systems. It is only a language and so is just one part of a software development method. The UML is process independent, although optimally it should be used in a process that is use case driven, architecture-centric, iterative, and incremental.

C. Context Diagram

The Context Diagram shows the system under consideration as a single high-level process and then shows the relationship that the system has with other external entities (systems, organizational groups, external data stores, etc.).



VI. System Implementation

Successful system implementation requires good leadership and careful planning. A good understanding of every component of the system is critical in putting together an implementation strategy. Implementation is the process of converting a system into an operational one. The designed system is converted to an operational one using a suitable programming language Installation of the system takes place only after it is found to be error free. Implementation walkthroughs ensure that the completed system accomplishes the original requirement. This walkthrough occurs just before the system goes into use, and it includes careful review of all manuals, training materials and system documentation.

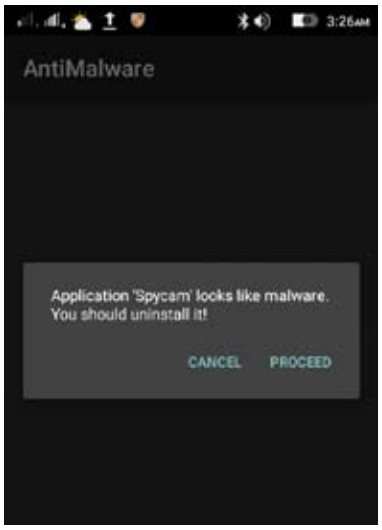


Fig 2: Defense android app interface

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

VII. Conclusion

Now days more than 1 million Android devices activated Android has very few restrictions for developer, increases the security risk for end users. A spy camera can play to attack or benefit phone users. Now, several advanced spy camera attacks have been detected, including the remote-controlled real-time monitoring attack using the detection mechanisms. I have proposed an effective defense scheme to secure a smart phone from all these spy camera attacks. As well as I have found some of the security issues related to the loss of mobile device or theft of mobile device, so I am going to develop the secure scheme for that also using GPS location tracking and capturing video recordings remotely. In the future, I will investigate the feasibility of performing spy camera.

References

[1] *Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," IEEE Symp. Security and Privacy 2012, 2012, pp. 95–109.*

[2] *R. Schlegel et al., "Soundcomber: A Stealthy and Context Aware Sound Trojan for Smartphones," NDSS, 2011, pp. 17–33.*

[3] *N. Xu et al., "Stealthy Video Capturer: A New VideoBased Spyware in 3g Smartphones," Proc. 2nd ACM Conf. Wireless Network Security, 2009, pp. 69–78.*

[4] *F. Maggi, et al.,"A Fast Eavesdropping Attack against Touchscreens," 7th Int'l. Conf.Info. Assurance and Security, 2011, pp. 320–25.*

[5] *R. Raguram et al., "ispy: Automatic Reconstruction of Typed Input from Compromising Reflections," Proc18th ACM Conf. Computer and Commun. Security,2011, pp. 527*

Author's Profile

The author is working as Asst. Professor, CSE in department of Computer Applications, CET. She has more than 10 years of teaching.