Permission Manager: Application to secure the Smartphone

Prof. Ghule Sheetal, Ambre Vijaya, More Priti, Tiwari Utkarsh, Yadav Manoj

Department of Computer Engineering,University of Pune,

Shri ChhatrapatiShivaji College of Engineering, Rahuri Factory. (Shrishivajinagar)

Abstract: - **Nowadays, Smartphones are very powerful, and many its applications use wireless multimedia communications. The prevention from the outside dangers (threats) has become a big concern nowadays for the experts. Android operating system has become one of the most popular operating system for Smartphone; Android security has become a big problem nowadays. Because of the free application it provides and the feature which makes it very easy for anyone to develop it. However, there are many systems proposed to provide the security by number of researchers working to solve this problem. In this article, we focus on security issues related to Android Smartphone. Specifically, we discuss several new attacks that are based on the use of phone. We implement the attacks on real phones, and demonstrate the feasibility and effectiveness of these kinds of attacks. Furthermore, we implemented a simple defense scheme that can effectively detect these attacks.**

Keywords: Smartphone, Android, security, attack, permission

ISR

I. INTRODUCTION

From 2007, the Android operating system (OS) has successfully enjoyed an unbelievable rate of popularity. As of 2014, the Android OS achieved a major part of global Smartphone market shares. For a certain time, a number of Android protection and privacy injuries have been exposed in the past several years. Although the permission system provides users an option to check the permission request of an application (app) before installation, some users have the knowledge of what all these permission requests support for, as a result, they fails to warn users of protection risks. For a certain time, arising number of apps thoroughly explained to enhance security and protect user privacy have appeared in Android app markets. Much of large anti-virus software companies have announces their Android-version security apps, and attempt to provide a protection for smart phones by discovering and blocking harmful apps. In addition, there are data securing apps that provide users the ability to conceal information, decrypt, sign, and conform signatures for private credentials, emails, and data. However, mobile malware and privacy leakage remain a big threat to mobile phone security and privacy.

Normally, when discussing about protection, many Smartphone users think to the safety of SMS, emails, contact lists, calling logs, location information, and private data. They may be unexpected that the phone camera could become a violates, for example, attackers could furtively take pictures and record videos by using the phone camera. In recent days, many types of camera-based applications have come in Android app markets. Spy camera apps have also become more famous. As in Google Play, there are nearly 100 spy camera apps, which allow users to take pictures or record videos of other people without their permission and attention and 1000 or more application that accessing personal data of the users. However, trust it or not, phone users themselves could also become victims. Attackers can create spy cameras in harmfulapps such that the phone camera is launched automatically without the device the knowledge of owner, and the taken photos and videos are sent out to these background attackers. Even worse, according to a statistical survey on Android malware study, camera permission ranks 12th of the most regularly requested permissions among benign apps, while it is out of the top 20 in malware. The popularity of camera usage in benign apps and relatively less usage in malware lower users' alertness to camera-based multimedia application attacks.

In recent days, people take their phones everywhere, and because of that their phones see lots of private information. If the phone camera is exploited bay harmful spy camera app, it may cause thoughtful security and privacy problems. For example, the phone camera may record a user's regular day to day activities and conversations, and then send these out through the Internet or multimedia messaging service (MMS). Hidden photography is not only crime but also illegal in some countries due to the invasion of privacy. However, 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 anybody has used his/her phone without permission and knowledge, the phone camera could be used to capture the face of an unknown user. In addition, it can also assist the owner to find a lost phone. In this paper, we first conduct a survey on the threats and benefits of spy cameras. Then we show the basic attack model and two camera based attacks. And then we introduce our defense system.

II. RELATED WORK

Many researchers has made a number of defense scheme to solve the security problem. A number of works have focused on the issue of getting the private information on the Smartphone using the android operating system. For example, Soundcomber [2] is a stealthy Trojan that can sense the context of its audible surroundings to target and extract highvalue data such as credit card and PIN numbers. Stealthy audio recording is easier to realize since it does not need to hide the camera preview. Xu*et al.* [3] present a data collection technique using a video camera embedded in Windows phones. Those malware (installed as a Trojan) silently records video and transmits data using either email or MMS. Windows phones offer a function, ShowWindow(hWnd, SW HIDE), which can hide an app window on the phone screen. However, it is much more complicated (no off-the-shelf function) to hide a camera preview window in an Android system. In this work, we are able to hide the whole camera malware app in Android. Moreover, we had implemented the advanced forms of attacks such as remote-controlled and real-time monitoring attacks. We can also utilize computer vision techniques to analyze recordedvideos and infer passcodes from users' eye movements. With this it can obtain user input. Maggi *et al.* [4] implement an automated shoulder surfing attack against modern touch-screenSmartphone. The attacker deploys a video camera that can record the victim's screen while thevictim is entering text. Then user input can be reconstructed solely based on the keystroke feedback displayed on the screen. However, these kind of attack requires an additional camera device, and the camera should be placed near the victim without catching an alert must be considered carefully. Moreover, it works only when visual feedbacks such as magnified keys are available. As many of the application provides the capabilities to get to know the information about anyother system or number with the cost of the personal data. For example,with the help of a single application which is having the permission of internet and the personal information anyone can get the data of any other person or the user who installed the application. And as we have provided the permission to the application, while the installation it is quite easy for the bad guy to get the information.

III. SYSTEM ARCHITECTURE

The system architecture of our system is very easy to understand about the application's working. Our application resides in between the application and the system. And it is dealing with the problem of getting access or denying the permission to access the system components or restricting the same.

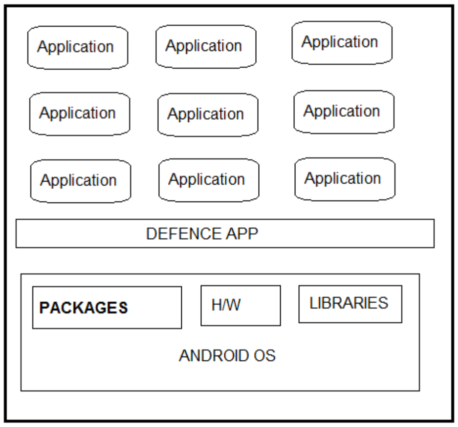

Fig.: (A) System architecture

III. THE BASIC ATTACK MODEL

We want to discover possible attacks based on a spy camera. The attacks should appear normal to user experience.

The challenge is to make it workable and get the data from the mobile with malicious application.

Step 1: To make the attack look normal to the user, the malware should consider the current CPU, memory usage, and battery status. Launching the attack when CPU and memory usage are already high could make a phone's performance even worse. Users would guess that the system is working slowly because of the no. of application, and it won't panic much. Similar concern will be taken to the user about the draining of the batteries and the other resources.

Step 2: After ensuring sufficient resources for launching attacks, a malicious app can continue on the remaining actions. First, the app can turn off the phone's sound and vibration, which can be achieved by setting the system sound *Audio Manager. STREAM_SYSTEM* to 0 and the flag to *FLAG_REMOVE_SOUND_ AND_VIBRATE*. The app can log the current volume level and vibration status, and resume it after the attack.

Step 3: If it is the attack to get the data than there is no such difficulty but, If the attack is based on video or camera than difficulty of the attack will occurs, when it will start the video recording or camera because it will take the maximum of the battery and live streaming can cause the speed of the data connections. And for that it have to get to the video and camera to run on the background. And for that it will require to setting up the layout.

Step 4: After setting up the layout, the attack could be launched as follows:

1. For the camera/video attack, initialize the *SurfaceHolder*, choose which camera (front or back) is used, and open the camera to take pictures or record videos.
2. For the data based attack the all data will be copied in to a zipped file.

3. Data are supposed to be stored in disguises, including using confusing filenames and seldom visited directories. The app releases the camera after the all Actions in the attack.

Step 5: After finishing the attack, the app sets modified status back to its original values. This way, the owner will not have any clue about the attack.

Step 6: In the final step of the attack the app have to send the collected data to the attacker. The best option for using the transmitting the data will be the Wi-Fi if available or the data connection. For example, it could use the *javax.mail*to send the data as an email attachment. Most email systems limit the maximum size of attachments, so the document should be within the size. If it is video, the length of a video should have an upper bound specific to the email service.

IV. COUNTERMEASURES

As we know that it is a very easy to implement the application but at the same time it is very difficult to implement it. As we are working solely with the main system packages not with the used-installed application. In this section we will discuss about the possible ways that can protect Android Smartphone's against these kind of attack.

The architecture of the system is very simple. It works same as the application lock which is provided to the user to lock the files that are having the sensitive credentials. Whenever a lock application is called-up the lock check and asks for the password or pattern.

In an Android system, whenever an application programming interface (API) is available for a user to check the usage of a Hardware component of our device. Our application will check if the application which is calling for the hardware component likewise for camera it will check in the database if the application is allowed for the access. Then it will provide the permission information to the system. Now the system will check it and response accordingly. If it is not allowed, it will send the error message to the system along with the package name of the application,which requested. The Application Package Name is a unique identifier in Android, and third party apps cannot reuse the name of built-in apps like a Camera (com.android.gallery3d). By looking at the app name, we are able to identify the built-in camera app (that is known to be safe), and no alert will be generated. Then we design a further checking mechanism for third party camera-based apps.

V. RESULT

We implemented the application with the proposed methodology. The application checks the permission records of all the application those are installed on the smartphone. The application is working effectively. And apart from that, it also makes battery life better and at some point stops the unnecessary data usage. The methodology or mechanism is working effectively and efficiently. The testing has done on the application with no. of malware app in many different scenario. The results are better and as expected.

VI. CONCLUSION

In this paper, we focused on the unnecessary vulnerabilities in Android phones for mobile multimedia applications. We discuss the problem of the data theft or the lost of the personal information. We discover several advanced attacks that can cause the data-theft problem and the live video-streaming attack that can compromise the security of the users. Meanwhile, we propose an effective defense scheme to secure a Smartphone from all these attacks. In the future, we will investigate the feasibility of performing attacks on other mobile operating systems.

REFERENCES

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

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

[3] N. Xu*et al.*, "Stealthy Video Capturer: A New Video-Based 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. Conference .Info. Assurance and Security*, 2011, pp. 320–25.

[5] R. Raguram*et al.*, "ispy: Automatic Reconstruction of Typed Input from Compromising Reflections," Proc. 18th ACM Conf. Computer and Communication Security, 2011, pp. 527–36.