Benign Defence Application for Android Based Mobile Phone CAM Security

Mr. M. B. Bose,
M.E Assistant Professor
Department of Information Technology,
Parisutham Institute of Technology and Science,
Thanjavur, Tamilnadu

Abstract - The most widely used mobile operating system as of 2013 is android with more around 79.3 percent of global Smartphone market share. Even though it has several multimedia applications, security has become a major threat. Many honest users are suffering due to the attacks caused by phone cameras. Several applications are able act as a traitor in accessing all user data. Therefore we design a background scanning algorithm to detect those applications which use the camera as well gallery, contacts, and emails of the user without their knowledge. Since all threats occur when internet access is available, the application provides the user with a checklist of applications that the user wants to give access to.

I. INTRODUCTION

Android mobile plays a major role in the mobile market and sells more than that of the windows, iOS and other mobile phones. The applications are also available as open source. Android has the ability to download and install the application in APK file, or downloading through Application store like GooglePlayStore that allows users to install them in their devices. Google Play Store in these devices complies with Google's compatibility requirements and license the Google Mobile Services software. Several applications are arriving day to day since many of the developers prefer Android Application development due to its popularity.

Android devices incorporate many optional hardware components, including still or video cameras. Many of the users do not know that their mobile devices are the major traitors in leaking their private information's obtained by the spy camera which is nothing but the mobile phone's own camera when the user enables Wife or they access internet for any other applications.

Even when the mobile is locked the malicious applications stealthily capture the images and also records videos. The remote attackers engage themselves in remote reconnaissance called a virtual theft completely through the use of phone’s camera and other sensors. The images obtained secretly during the normal use of phone generate 3D models of the user’s surrounding. A surveillance platform is available to the remote attackers so that reconstruction of the 3D models into mark able detail of user can be found.

The main problem is that the user itself becomes victims of such attacks. Even though Android permission system asks the user to check the permission request of an application, they do not warn the users about any security risks.

Several security applications have also been developed to provide dataprotection. When talking about data protection these applications focus only only on contacts, email, messages etc., and fail to concentrate on the mobile’s camera some of the attacks include Remote controlled monitoring attack, video-passcode Inference attack, etc., Therefore the applications must be given access to any data only with the knowledge of user. For that we are going to use a background scanning algorithm which checks the utilization of camera by any of the applications when the mobile is in use as well as the mobile is in locked state.

II. CHALLENGES

The most challenging fact is the severity of the attacks caused by the camera. The cameras can collect huge amount of data very rapidly, and gives it to the attacker. For example, a 10-megapixel camera can easily record 100 megabytes of data per minute if taken at high rate [1].The Place Rider is an application that performs Virtual Theft...
attack in a Stealthy way and extracts many private information’s.

III. RELATED WORK

RANSOM WARE ATTACK

The ransomed ware attack locks the mobile device and overlays a message on the screen and illegal pornography and malicious activities. It will ask for hundreds of dollars to unlock our mobile.

VIDEO SMUDGE PASSES CODE ATTACK

There are two types of threat models active and passive. The passive attacker operates the mobile from remote place and collects the smudges of password through the camera. The attacker controls the angle and lighting setup of the camera. The attacker could guess the possible pass code. Active attacker has the Capability of controlling the lighting conditions and can alter the touch screen in a way to improve he retrieval rate.

KEY STROKE INFERENCE ATTACK

Many smart phones are enabled with virtual keyboard. The operating system is able to understand all the user activities on the window. The Layout of user input is made available with the help of key logger activities. The motion changes can thus infer user data. If it is to be avoided a change in the inner core of the operating system is required which intern is not an easy task. It is hard to set the range of reduction in such attacks.
SCREEN UNLOCKING ATTACK

This Attack occurs when the screen turns on. It turns on when the screen turns on and ends up immediately when the screen turns off. It includes two keys:
ACTION SCREEN-ON: When the user turns on the mobile.
ACTION USER_PRESENT: When the user guards up.

THE REMOTE-CONTROLLED REAL-TIME MONITORING ATTACK

It is one of the most aggressive attacks in the android mobile and the remote user controls the spy camera and sends a READY message and turns the application into an Android Eye to dynamically launch the captured video using NanoHttpd.

IV. EXISTING SYSTEM

In the existing system when camera is called the malicious app will turn off the mobile phone sound and vibration in the audio manager by making changes to STREAM_SYSTEM and FLAG_REMOVE_SOUND_AND_VIBRATE
And hides the camera preview through LayoutInflater.inflate().

Without causing any abnormal behaviour the spy camera apps transmit the user’s data once the Wi-Fi is enabled. Even when antivirus and security application are available the user will only be provided with warning message which the user may sometimes do not notice.

Sometime this warning message may be provided along with the vibration. But that may also remain unnoticed by the user. Even though the overall security of mobile is been provided by the pass codes there occurs many attacks that cause malicious activities to be carried out by the spy cameras.

Also no Application Programming Interface(API) is available to check the log and determine the activities or applications running in the mobile.

Most of the mobile phones have pattern as pass codes which include only 9 dots. With pattern conventional one time pass codes cannot be generated. Therefore the attacker tracks different and possible patterns which are sent to the remote attacker.

In the existing system a change is been made in the ActivityManagerService and a warning message can be generated only for camera and thus when camera is been called by any application it provides a warning message as shown in Fig 6.

Many scanning applications are available in android system but they need to check for the malpractice each time the user wants to-do so. For each and every application the scan needs to be performed and the malicious will not show any change in their normal behaviour.

So even when scanning is performed there occurs some issues with providing permission to access applications like camera. Inturn these applications can root the Android device and have control the operating system. After that gaining the root Access becomes more difficult.
In our proposed system we design a background scanning algorithm that checks the Activity Manager and when camera is called by any of the applications when the user’s mobile is locked the further operations will not take place. The same can be used for gallery also. Whenever camera is called without users knowledge the user the camera will turn off automatically and whenever the user is unlocking the device a warning message will alert the user about the malicious app so that the user can take corrective measures to avoid any kind of possible attacks in their device.

Most of the attacks occur mainly when internet is available. The user’s data is sent to the remote attacker without any abnormal behaviour. Therefore whenever Wi-Fi is enabled the user will be provided with a checklist of all the installed applications Fig:9,10 and ask the user to select the applications for which the user wants to give access to.
VII. CONCLUSION

In this article, we study about the various camera based attacks and how the attackers theft the user information. Eventhough there is security provided for the android mobile phones the malware and the privacy leakage became a big threat. We proposed the defence application for the camera security.

REFERENCE


