Benign Defence Application for Android Based Mobile Phone CAM Security

R. Divyabharathi, R. Narmathai, C. Shiva Ranjani, X. Stella Infanta.
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. Eventhough 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.

Figure 1. A Representation of camera threat in android mobile applications

Many multimedia applications are available nowadays which make our workload to be reduced. 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.

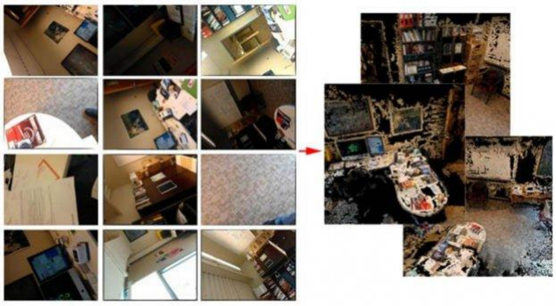


Figure 2.Reconstruction of images to guess private information.

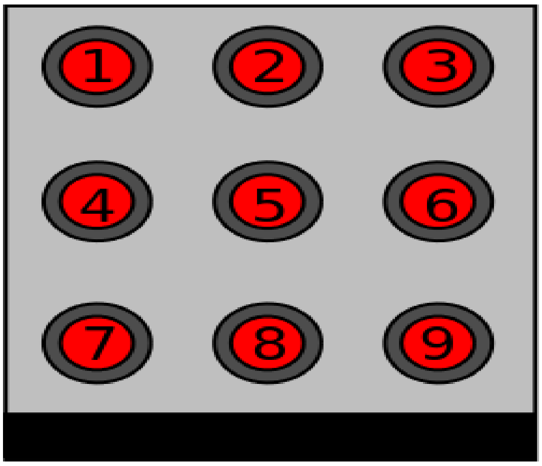
III. RELATED WORK

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.



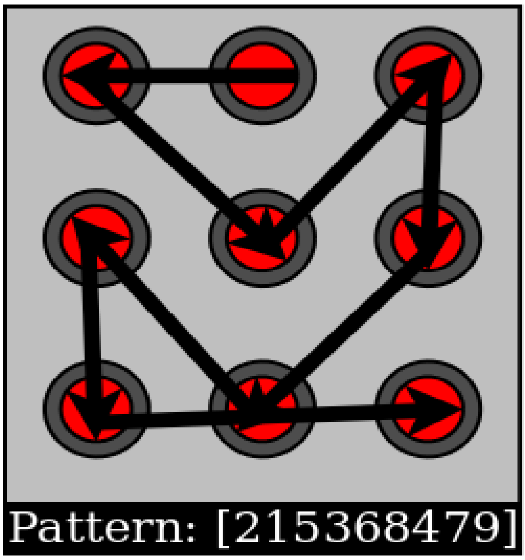


Figure 3.Video smudge pass code attack

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.

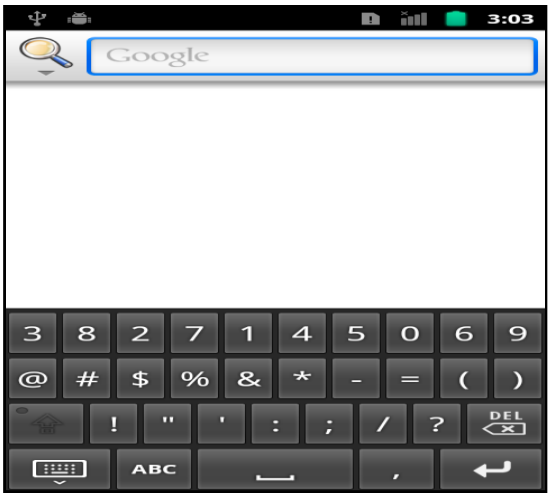


Figure 4. Number keypad in a virtual keyboard.

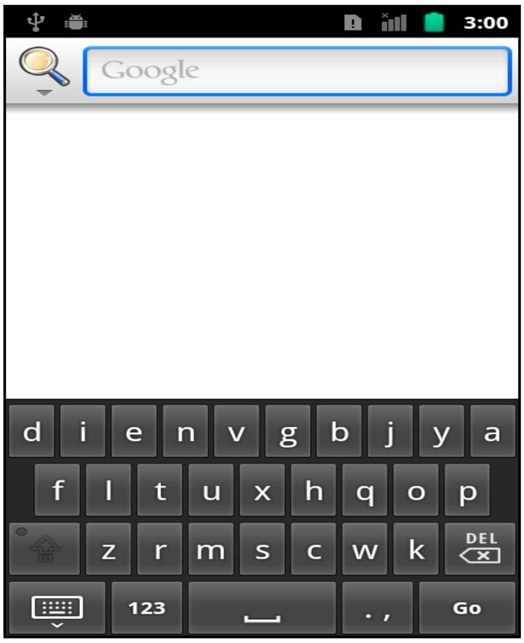


Figure 5. A virtual alphabetic keypad

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.

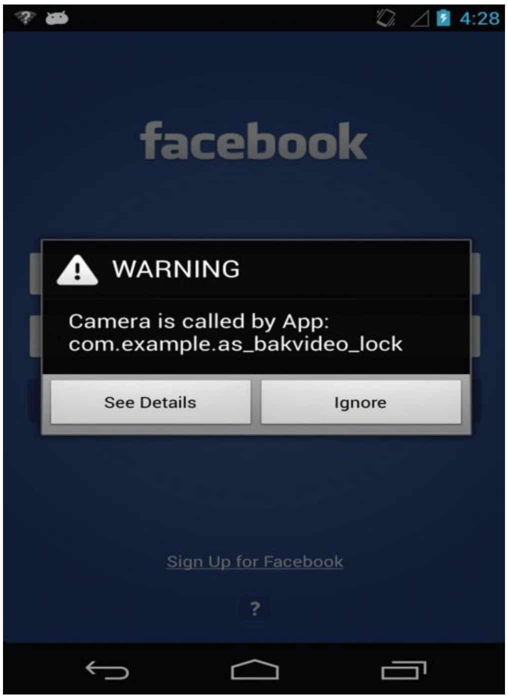
THE REMOTE-CONTROLLED
REAL-TIME MONITORINGATTACK

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 Layout Inflater.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.



WARNING

Camera is called by App:
com.example.as_bakvideo_lock

Figure 6. Warning message given by the existing system.

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.

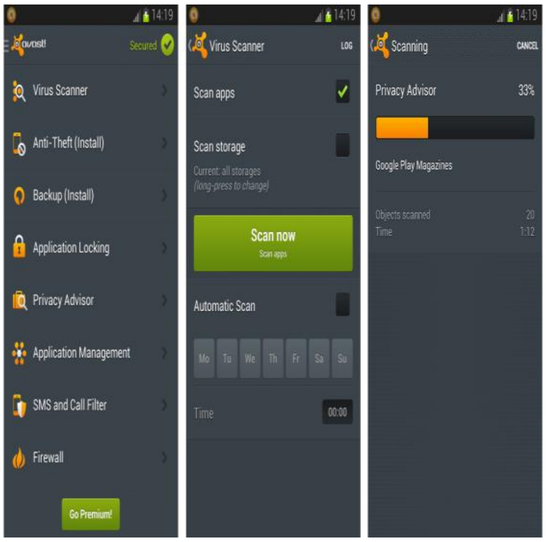


Figure 7. Scanning done by antivirus

V. PROPOSED SYSTEM

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.

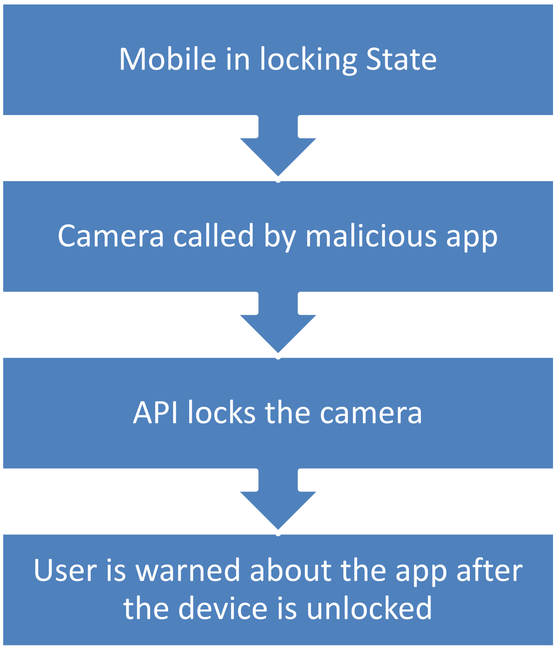
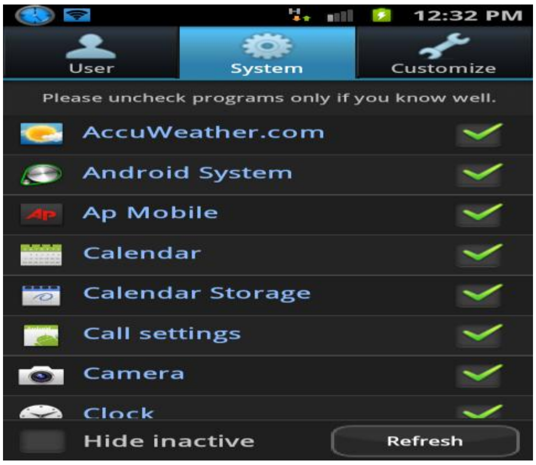

Mobile in locking State
Camera called by malicious app
API locks the camera
User is warned about the app after the device is unlocked

Figure 8. Design of Proposed Algorithm

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.



12:32 PM

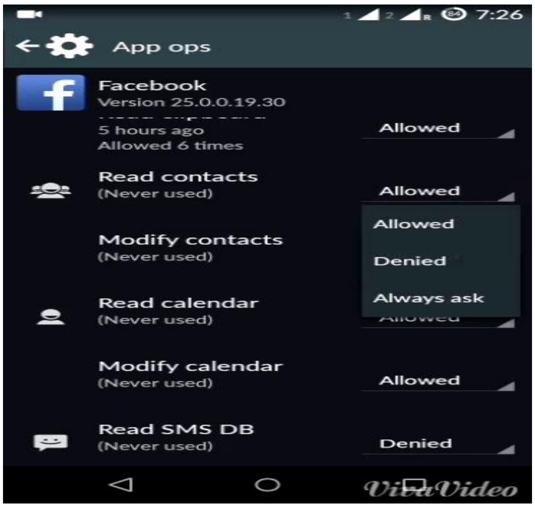
User | System | Customize

Please uncheck programs only if you know well.

- AccuWeather.com ✓
- Android System ✓
- Ap Mobile ✓
- Calendar ✓
- Calendar Storage ✓
- Call settings ✓
- Camera ✓
- Clock ✓

Hide inactive | Refresh

Figure 9. Checklist for the applications.



7:26

App ops

Facebook
Version 25.0.0.19.30
5 hours ago
Allowed 6 times
Allowed

Read contacts
(Never used)
Allowed

Modify contacts
(Never used)

Allowed
Denied
Always ask

Read calendar
(Never used)

Modify calendar
(Never used)
Allowed

Read SMS DB
(Never used)
Denied

VivaVideo

Figure 10. The choices for application which can access internet.

VI. FUTURE ENHANCEMENT

Through the internet access only our information like contact list, gallerys, messages and other data get tracked by the attackers.Inorder to overcome this problems we can allow the internet access for the particular applications alone. And the various applications provide the advertisements when user using their applications through that also the threats are formed.

So the user can deny the particular applications which cause the malicious and user can use the non malicious applications.

VII. CONCLUSION

In this article, we study about the various camera based attacks and how the attackers theft the user information.Eventhough the 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

[1] Suhas Holla, Mahima M Katti. "Android Based Mobile Application Development and its Security", Department of Information Science & Engg, R V College of Engineering Bangalore, India. *International Journal of Computer Trends and Technology- Volume3issue3-* 2012.

[2] Enck, W., Octeau, D., Mcdaniel, P., and Chaudhuri, S. *A Study of Android Application Security*. Tech. Rep. Nastr- 0144-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, Pa, USA, January 2011.

[3] Kasperskey Lab. *First sms Trojan Detected for Smart phones Running Android*.Http://Www.Kaspersky.Com/News?Id=207576158, August 2010.

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

[5] I Ker Burguera,Urko Zurutuza, Simin Nadjm-Tehrani "Crowdroid: Behaviour-Based Malware Detection System for Android".Inproceedings of the 1st Acm Workshop on *Security and Privacy In Smart phones and Mobile Devices* (Spsm'11), Pages 15-26, 2011, Acm New York, Ny, USA ©2011. Chicago, Il, USA, October 17, 2011.

[6] Gianluca Dini, Fabio Martinelli, Andrea Saracino, and Daniele Sgandurra. "Madam: A Multi-Level Anomaly Detector for Android Malware".In Proceeding Mmm-Acns'12 Proceedings Of The 6th International Conference on *Mathematical Methods, Models And Architectures for Computer Network Security*:Computer Network Security, 2012.

[7] Http://www.scribd.com/doc/219864151/attacks-on-android.

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