DETECTION OF CAMERA BASED ATTACKS ON MOBILE PHONES USING LIGHTWEIGHT DEFENSE APPLICATION

M. REVATHI, R. ROJA, S. SOWMIYA
Department Of Computer Science
Adhiparasakthi Engineering College, Melmaruvathur

ABSTRACT Now a day's several new attacks that are based on the use of phone cameras. We implement the attacks on real phones, and demonstrate the feasibility and effectiveness of the attacks. Furthermore, we propose a lightweight defense scheme that can effectively detect these attacks. The defense app is able to decide the dynamic launch pattern of camera related apps by polling the task list. If a camera app calls camera without user permission or it calls with a different app name, the defense app would give warnings to the phone user as several notifications.

EXISTING SYSTEM

In existing system the detection of spy camera is done but it does not provide sufficient detail about the spy camera activities .After detection it is not uninstall from the device .Hence there is no privacy for the mobile user. It continues to running in the background without user knowledge and it makes the mobile to run abnormally. These disadvantages can be overcome by implementing the lightweight defense application.

PROPOSED SYSTEM

Light weight Defense application is installed in the device after getting user's permission and it silently runs in the background without interrupting the user's activities. It detects the Spy cam app which is hidden in any of the running application that calls the camera service. The defense app gives notifications to the user about the malicious app installed unknowingly. After giving the notifications it uninstalls the malicious app from the user's device. The notifications are Beep sound, Voice message, Alert message

Advantages

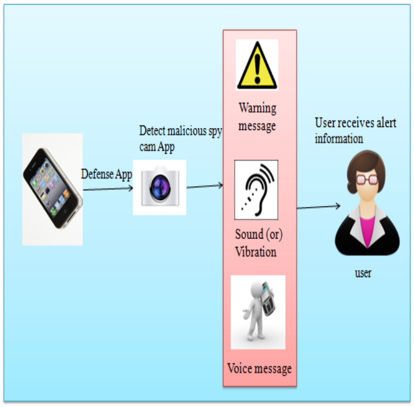
- It provides privacy and protects the user's information from hacker.
- It secures Smartphone from all malicious spy camera attacks.
- The performance and memory storage of mobile phone is increased.

FAST EAVESDROPPING ATTACK

This paper "**A Fast Eavesdropping Attack Against Touch screens**" the attack against the Apple iPhone2010's most popular touch screen device although it can be adapted to other devices that employ similar key-magnifying keyboards. Our attack processes the stream of frames from a video camera and recognizes keystrokes online, in a fraction of the time needed to perform the same task by direct observation or offline analysis of a recorded video, which can be unfeasible for large amount of data. Our attack detects, tracks, and rectifies the target touchscreen.The device or camera's movements and eliminating possible perspective distortions and rotations In real-world settings, our attack can automatically recognize up to 97.07 percent of the keystrokes with 1.15 percent of errors (3.16 on average) at a speed ranging from 37 to 51 keystrokes per minute.

SYSTEM ARCHITECTURE

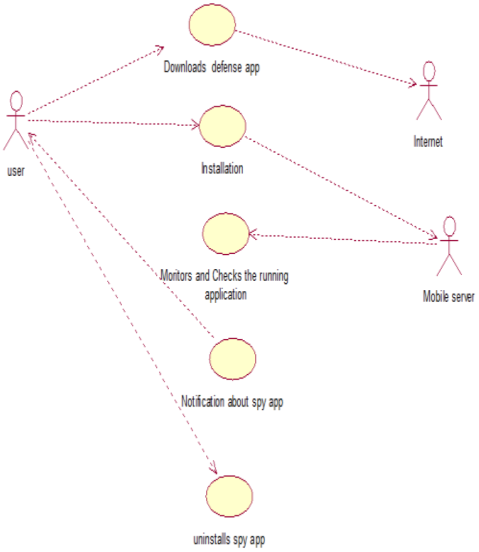
A system architecture is a conceptual design that defines the structure and behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured and systems developed, that will work together to implement the overall in a way that supports reasoning about the structural properties of the system. The system architecture of MMS based anti-theft application is given.



System Architecture

USE CASE DIAGRAM

A Use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases).Use cases focus on the behavior of the system from the external point of view. The actor is outside the boundary of the system, whereas the use cases are inside the boundary of the system.

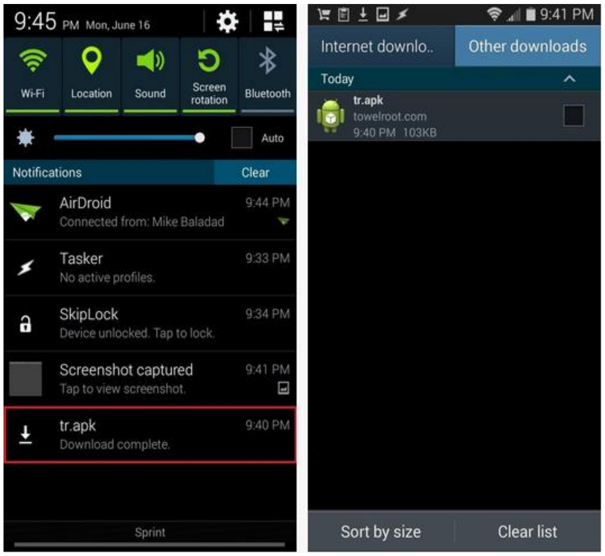


Use case diagram

IMPLEMENTATION

Implementation is the most crucial stage in achieving a successful system and giving user's confidence that the new system is workable and effective. This type of conversation is relatively easy to handle, provide there are no major changes in the system .Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly. Initially at the first step the executable form of the application is to be created and loaded in the common server machine which is accessible to all users and the server is to be connected to a network. The final stage is to document the entire system which provides components and the operating procedures of the system.

STEP 1



AirDroid 9:44 PM
Connected from: Mike Baladad

Tasker 9:33 PM
No active profiles.

SkipLock 9:34 PM
Device unlocked. Tap to lock.

Screenshot captured 9:41 PM
Tap to view screenshot.

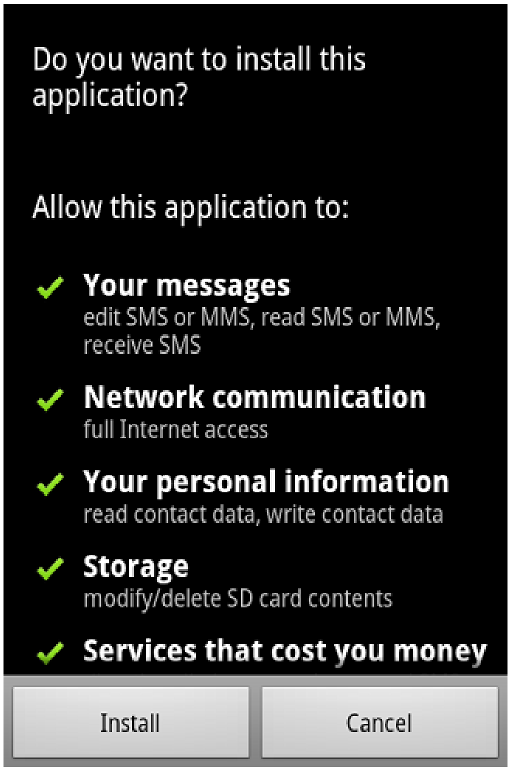
tr.apk 9:40 PM
Download complete.

tr.apk
towelroot.com
9:40 PM 103KB

Download Application

The lightweight Defense app is downloaded from the Google play store by the user to protect their mobile from spyware.

STEP 2



Do you want to install this application?

Allow this application to:

✓ **Your messages**
edit SMS or MMS, read SMS or MMS, receive SMS

✓ **Network communication**
full Internet access

✓ **Your personal information**
read contact data, write contact data

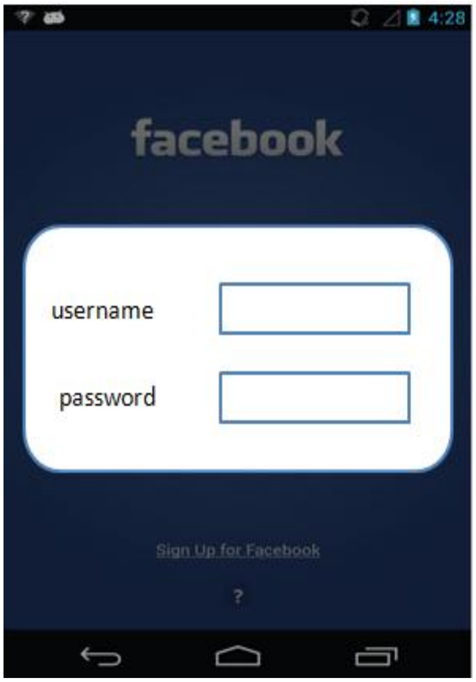
✓ **Storage**
modify/delete SD card contents

✓ **Services that cost you money**

Permission Page Of The Application

The downloaded defense application request for user's permission before installation into device.

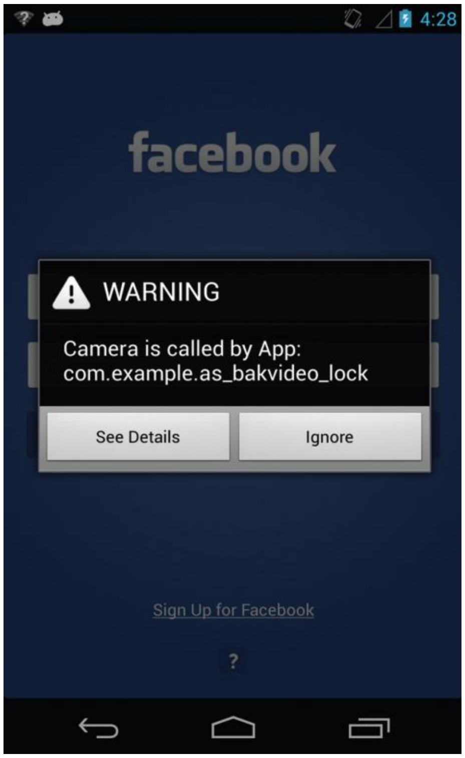
STEP3



Monitoring Background Running Process

In this Figure 8.3, the snapshot shows the monitoring process of the defense application, i.e the chat application is monitored.

STEP 4

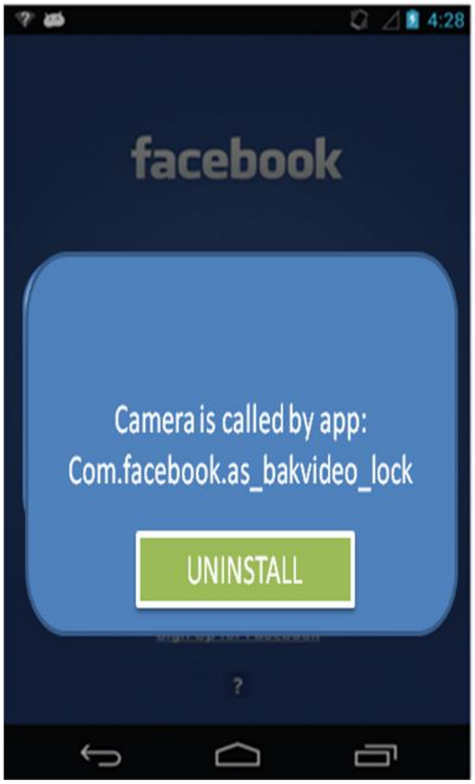


Camera is called by App:
com.example.as_bakvideo_lock

Defense against spy camera attack

In this the defense application detects the spy camera app in the chat application and it provide details of the spy camera app.

STEP 5



Camera is called by app:
Com.facebook.as_bakvideo_lock

Uniinstall Spy Application

In this Figure 8.5 the defense application asks user permission to uninstall the spy camera app from the user’s device.

CONCLUSION

In this paper, the proposal is the advanced detection of spy camera application with enhanced features. Lightweight defense application is one of the android applications which enable the user to protect their mobile from hackers. This application automatically detects the spy camera application. This application is user friendly and it can be installed without any technical knowledge for the user. It is also cost effective and it utilizes the minimal resources from the mobile. The installation of this application is a simple process and takes only a few minutes. Hence the user can protect their personal data and privacy from the hacker. It does not involve any difficult task to identify the spy camera application.

FUTURE ENCHANCEMENTS

With the advent of time, technology is evolving every day. Our application will further be developed and improved. Currently this application is available for android based mobile phones. Future work involves development of the application for iOS, Symbian, Windows Mobile OS etc.The extra feature can be done is the mobile from hangout and while login to the device either using pattern or PIN Number. If the user is an unauthorized person then the camera should take the picture and send mail to the mobile owner. So they can protect their mobile.

REFERENCES

[1] Y. Zhou and X. Jiang, “Dissecting Android Malware: Characterization and Evolution,” *IEEE Symp. Securityand Privacy 2012*, 2012, pp. 95–109.
[2] R. Schlegel *et al.*, “Sound comber: A Stealthy and Context- Aware Sound Trojan for Smart phones,” *NDSS*,2011, pp. 17–33.
[3] D. Li, D. Winfield, and D. Parkhurst, “Starburst: A Hybrid Algorithm for Video-Based Eye Tracking Combining Feature-Based and Model-Based Approaches,”*IEEE Computer Soc. Conf. Computer Vision and PatternRecognition — Workshops*, 2005, p. 79.
[4] F. Maggi, *et al.*,“A Fast Eavesdropping Attack against Touchscreens,” *7th Int’l. Conf.Info. Assurance andSecurity*, 2011, pp. 320–25.
[5] R. Raguram*et al.*, “ispy: Automatic Reconstruction of Typed Input from Compromising Reflections,” Proc.18th ACM Conf. Computer and Commun.Security,2011, pp. 527–36.
[6]“Android-eye,”
https://github.com/Teaonly/android-eye, 2012.
[7] “Nanohttpd,”
https://github.com/NanoHttpd/nanohttpd.
[8] A. P. Felt and D. Wagner, “Phishing on Mobile Devices,”Proc. WEB 2.0 Security and Privacy, 2011.
[9] N. Xu *et al.*, “Stealthy Video Capturer: A New Video- Based Spyware in 3g Smartphones,” *Proc. 2nd ACMConf. Wireless Network Security*, 2009, pp. 6978.