SPY CAMERA ATTACK PREVENTION TECHNIQUE AND ANTITHEFT TECHNIQUE FOR ANDROID MOBILE PHONE

Gadakh Komal Navnath[1], Jadhav Chhaya Vitthal[2], Varpe Kalyani Babasaheb[3], Varpe Akshada Dinkar[4].

[1,2,3,4]Department of Computer Engineering
SPCOE College of Engineering Dumbarwadi, Pune-412409
Savitribai Phule Pune University, India

ABSTRACT

Mobile phone security has become an important aspect of security issues in wireless multimedia communications. In this paper, we focus on security issues related to mobile phone cameras. Specifically, we discover 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 theseattacks.In this paper, we are going to develop an Android application such that when a user loses his/her phone, the spy camera could be launched via remote control and capture what the thief looks like as well as the surrounding environment. Then the pictures or videos along with location information (GPS coordinates) can be sent back to the device owner so that the owner can pinpoint the thief and get the phone back. We conduct a survey on the threats and benefits of spy cameras. Then we present the basic attack model and two camera based attacks: the remote- controlled real time monitoring attack and the pass code inference attack. We run these attacks along with popular antivirus software to test their stealthiness, and conduct experiment to evaluate both types of attack.

Keywords*: Passcode inferences, eye tracking, remote controlled.*

1. INTRODUCTION

An Android operating system (OS) has enjoyed an incredible rate of popularity. As of 2013, the
Android OS holds 79.3 percent of global smartphone market shares. Mean-while, a number of Android security and privacy vulnera-bilities have been exposed in the past several years. Al-though 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 fails to warn users of security risks. Meanwhile, an increasing number of apps specified to enhance security and protect user privacy have appeared in Android app markets. Most
Large anti-virus software companies have published their Android-version security apps, and tried to provide a shield for smart phones by detecting and blocking malicious apps. In addition, there are data protection apps that provide users the capability to encrypt, decrypt, sign, and verify signatures for private texts, emails, and files. However, mobile mal-ware and privacy leakage remain a big threat to mobile phone security and privacy.
Nowadays, people carry their phones everywhere; hence, their phones see lots of private information. If the phone camera is exploited by a malicious spy camera app, it may cause serious security and privacy problems.
In this article, we first conduct a survey on the threats and benefits of spy cameras.Attackers can implement spy cameras in malicious apps such that the phone camera is launched automatically with-out the device owner's

notice, and the captured photos and videos are sent out to these remote attackers. Even worse, according to a survey on Android malware analysis, camera permission ranks 12th of the most commonly re-quested 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 us-ers' alertness to camera-based multimedia application at-tacks.

2 .THREATS AND BENEFITS OF SPY CAMERA

Now we discuss some threats and benefits of using a spy camera.

2.1 Leaking Private Information

A spy camera works as a thief if it flogs private information from the phone. First, the malware finds a way to infect the victim's smart phone it runs a background service to secretly take pictures or record videos, and store the data with mysterious names in a directory that is seldom visited. Then these data are sent out to the attacker when Wi-Fi or other connection is available.

2.2 Watchdog

A spy camera can stealthily take pictures of the phone user and determine those who use or check other people's phones.

2.3 Antitheft

When a user loses his\her phone, spy camera can be activated by using remote control and record How the thief looks like & as well as places &environment and landmark. Then by using collected information we can track the phone by GPS CO-ORDINATES and get the phone back. To send all recorded data we use newly developed light weight Ksoap2 protocol.All information sends through Ksoap2 envelope.

3. THE REMOTE CONTROLLED REAL TIMEMONITORING ATTACK

The basic camera attack can be further raise to higher degree to more aggressive attacks.
For example the spy camera app can remotely control by attacker such that it can
launch& end the attack. Socket is the simplest way to implement the remote control. After the malicious app is downloaded & installed on a victim's phone, the app send a ready message along with the ip address ad port number the attacker's server. Then attacker can control launch and stop of app or specify a time schedule. There are many android apps that turn phone into a security surveillance camera. Such as android eye. The based on way an ip camera is built the spy camera can easily be extended to a stealthy real-time monitor. Nano is a lightweight HTTP server that can be in-stalled on a phone. In our case the captured videos can be played online upon requests from a browser client, can be done by starting HTTP server at a given port which support dynamic file serving. Figure 1 shows the video taken by a real-time spy cam- era of a mobile phone. an Android phone is located In environment figure 1A. Videos can be recorded through front camera, although the phone's screen is showing its app menu. Figure 1b is the view of the phone camera, which is accessed from a PC browser. The address is the the port number of the server and the IP address of the phone. In this section, we discuss the remote-controlled real-time monitoring attack.which could pose a big threat to a phone user's privacy daily activities and surrounding environment are all under the eye of the attacker.when multiple apps request the camera device at the same time or if the camera is being used by another app Camera-based attacks can be detected.By selecting the time to launch attack this can easily be avoided.The malicious camera app can periodically check the screen status and run the privately video recording only when the screen is off, which means the camera device is idle and the user is not using the phone.The status of the phone screen can be obtained by registering two broadcast receivers, ACTION_ SCREEN_ON and ACTION_SCREEN_OFF.

4. THE VIDEO BASED PASS CODE INFERENCE ATTACK

When the keys is being touched A user's eyes move along with, which means that tracking the eye movement could possibly tell what the user is entering.Thus, it is of great importance By tracking the eye movements we can Thus, it is of great importance or not. As computer vision techniques are advancing and becoming more accurate, an offline processing of the video can extract the eye position in each frame and draw the path of eye movements,which means that an attacker could figure the passcode based on the video captured by a spy camera

app.In this section, we discuss two types of camera attacks for assuming passcodes.We also discuss the computer vision techniques for eye tracking that can be utilized in the attacks.

4.1 The Application-Oriented Attack

The application oriented attack is first type of attack, which aims at getting the rights of certain apps . Figure 2 gives some examples of app passcodes. Most apps (like Facebook) that require authentication contain letters, which need a complete virtual keyboard, as shown in Fig. 2A. Figures 2b and 2c show two other types of popular passcodes, pattern and PIN, which we discuss in detail later. Smart App Protector is a locker app by which a user is able to lock apps that need extra protection (i.e., Gallery, messaging, and dial-ing apps). the video must be captured during user authentication, For a successful passcode inference attack. to poll the running task list and launch the attack as soon as the target app appears on top of the list is an effective way. Specifically we can get the name of the most recently launched app by using getRunningTask () function of activity manager. Meanwhile the running apps and resource utilization must be scan by the detection service. When attack conditions are met, it opens the camera and secretly takes videos of the user's face (especially the eyes) with a front-face camera for a time long enough to cover the entire authentication process.
to ensure the attack is effective and efficient There are several other factors we need to considered.

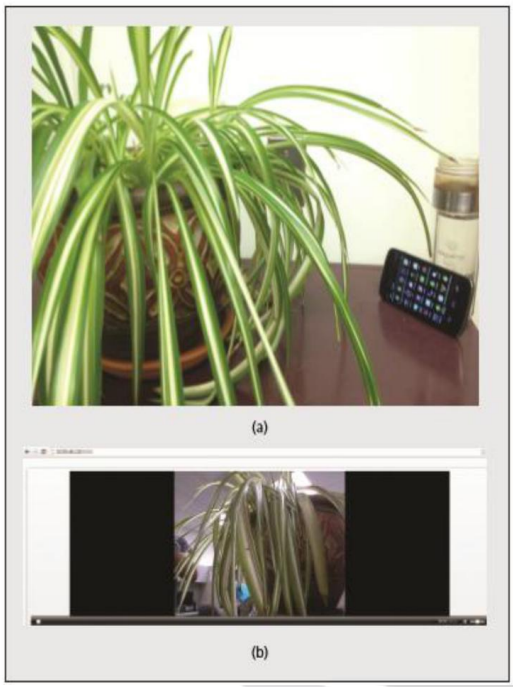

Fig 1: Demo of the real–time monitoring attack: a) Overallview of phone environment b) Scene captured by phone camera.

First, the detection service of a spy camera app must be launched beforehand, by either appetizing the user to run the app or registering an ACTION_BOOT_COMPLETED re-ceiver to launch when booting is finished.The RE-CEIVE_BOOT_COMPLETED permission is a commonly requested permission that would not be considered danger-ous.Second, polling task lists repeatly leads to extra con-sumption of energy resource.the detection service is active only when a user is using the phone to improve the efficiency of scanning.As mentioned before, this can be deter-mined by screen status.The detection service will break off when the screen is off and continue when the screen lights up again.

4.2 The Screen Unlocking Attack

In this subsection, we discuss another type of attack.when a user is entering a screen unlock-ing passcode the attack is launched .We categorize this plan as a different attack model since it is unnecessary to hide the camera pre-view under this condition. If the device owner does not show the user interface by entering the correct credential An-droid system would not allow user to interface to achieve privacy. This accidentally provides a shield for spy cam-era attacks goaled at the screen unlocking process.Users never know that the camera is working, even though the camera preview is right below the unlocking interface.We demonstrate the screen unlocking
Passcode inference attack.. Its difference from the application-oriented attack is the condition to launch the attack and the time to stop. Initially the attack should start as soon as the screen turns on and should end immediately as the screen is unlocked.This can be achieved in two key steps:

Registering a Broadcast Receiver to receive ACTION_SCREEN_ON when a user lights up the screen and begins the unlocking processregistering another broadcastreceiver to receive
ACTION_USER_PRESENT when a passcode is confirmed and the screen guard is gone.The second step guarantees that the camera service would stop recording and end itself immediately when the user interface is switched on. In addition, the attack should con-sider the situation with no screen locking passcode.

Fig 2: Different types of passcodes: a) Password; b) Pattern;c) PIN

The spy camera app should check keyguardmanager with the isKeyguardLocked () function to make sure the screen is locked before launching the attack to avoid being exposed.Alternative authentication methods in addition to the conventional password: pattern and PIN is provided to simplify the screen unlocking process.A pattern is a graphical passcode composed of a subset of a 3 × 3 grid of dots that can be connected in an ordered sequence. There are some rules for the combination of dots.

• The number of dots chosen must be at least 4 and no more than 9

• Each dot can be used only once. A PIN is a pure-digit passcode with length ranging from 4 to 16, and repetition is allowed

In screen unlocking of Android phones both are alternatives used extensively.a user's eye fatigue problem relieves the relatively larger distance between adjacent keys effectively. However, this also brings vulnerability to video based passcode inference attacks since the larger scale of eye movement makes the attack easier.

5. VIDEO-BASED EYE TRACKING TECHNIQUES

Two types of imaging approaches are commonly used In the eye tracking field :visible and infrared spectrum imaging.Visible spectrum imaging passively utilizes the ambient light reflected from the eye, while infrared spectrum imaging is able to eliminate uncontrolled specular reflection with active infrared illumination.Although infrared spectrum eye tracking is more accurate, most smartphones today are not equipped with infrared cameras.Hence, we focus on visible spectrum eye tracking.

Fig 3: Demo of existing eye tracking techniques: a) Starbursteye tracking demo; b) fast eye tracking demo.

For images captured by visible spectrum imaging, often the best feature to track is the contour between iris and sclera known as the limbus.Li et al propose the Starburst eye tracking algorithm, which can track the limbus of the eye.As we can see from Fig. 3a,they can locate where the eye is looking in a real-time manner, in visible spectrum, in visible spectrum they can locate where the eye is looking in a real-time manner.However, Starburst requires calibration by manually map-ping between eye positions coordinates and scene-image coordinates. This can be performed only by the phone owner, which makes it infeasible in spy camera attacks.
Aldrian presents a method to extract fixed feature points from a given face in visible spectrum, which is based on the Viola Jones ad boosted algorithm for face detection. But it is able to track pupil movement without scene image and calibration, as shown in Fig. 3b. We adopt this eye tracking algorithm in our research to extract eyes from videos.

6. FEATURE ANALYSIS OF THE PASSCODEINFERENCE ATTACK

An important feature that enhances the effectiveness of a passcode inference attack is that it can be launched repeatedly, which allows certain passcodes to be attacked many times. In this way, an attacker could get a set of possible passcodes and keep launching attacks until the correct one is found. The passcode inference attack depends on the vic-tim's eye movement instead of analyzing videos containing the screen or its reflection, which makes it harder to achieve high and stable one-time success rates. In addition, there are complex factors that may influence its performance, such as the distance between face and phone, light-ing conditions, velocity of eye movements, pause time on each key, and head/device shaking when typing. Among these experimental conditions, only the lighting condition can be kept constant during our experiments. To test the effectiveness of the passcode inference attacks with different types of passcodes, we use the conventional password, pattern, and PIN in our experiments. By comparing the rules of pattern and PIN, we find that pattern combination is actually a subset of PIN. In addition, the outlines of the two passcodes are similar (both are squares). Hence, we present their results and discuss their performance together. Another consideration for experiments is the length of pat-tern and PIN. In fact, people rarely use long PINs and com-flex patterns since they are hard to memorize and impractical for frequent authentications such as screen unlocking. This can be best illustrated by Apple iOS's four-digit PIN for screen unlocking. Hence, in our experiments we choose a four-digit pattern/PIN for testing.

7. CONCLUSION

In this paper, we study camera related vulnera- bilities in Android phones for mobile multimedia applications. We discuss the roles a spy camera can play to attack or benefit phone users. We discover several advanced spy camera attacks, including the remote-controlled real-time monitoring attack and two types of passcode inference attacks. Meanwhile, we propose an effective defense scheme to secure a smartphone from all these spy camera attacks. In the future, we will investigate the feasibility of performing spy camera attacks on other mobile operating systems. We study theusing various attack how to implement android app for to find mobile thief and its location using ksoap2 protocol. It is very secure to transfer information because it uses envelope to transfer data.

8. REFERENCES

[1] R. Schlegel et al., ―Sound comber: A Stealthy and Con-text-Aware Sound Trojan for Smartphones,‖ NDSS, 2011, pp. 17–33.

[2] 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.

[3]Android-eye,https://github.com/Teaonly/ android-eye, 2012.

[4].Nanohttpd,https://github.com/NanoHttpd/ nanohttpd.

[5].A. P. Felt and D. Wagner, ―Phishing on Mobile Devices,‖ Proc. WEB 2.0 Security and Privacy, 2011.

[6].P.Aldrian,―FastEye tracking,‖ http://www.math-works.com/matlabcentral /file exchange/25056-fast-eye-tracking, 2009.