ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Survey on Camera Based Attack Detection and Prevention Techniques on Android Mobile Phones

Ashish S.Kale, Prof.Ramesh G. Patole

Master of Engineering Student, Dept. of Computer Engineering, G.H.Raisoni College of Engineering, Wagholi, Pune, Maharastra,India

Assistant Professor, Dept. of Computer Engineering, G.H.Raisoni College of Engineering, Wagholi, Pune, Maharastra, 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 these attacks. 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 inference, limbus, eye tracking, remote controlled

I.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 vulnerabilities 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.

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 [1], 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

II.RELATED WORK

1. Threats and benefits of spy camera:
(a) Leaking private information: A spy camera works as a thief if it steals 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 obscure names in a directory that is seldom visited. Then these data are sent out to the attacker when Wi-Fi (fast and usually unlimited) access or other connection is available.
(b) Watchdog: A spy camera can stealthily take pictures of the phone user and determine those who use or check other people's phones.
(c) Anti-thief: 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.
2. The Remote Controlled Real Time Monitoring Attack:
The basic camera attack can be further enhanced to more aggressive attacks. The spy camera can easily be extended to a stealthy real-time monitor based on the way an IP camera is built. NanoHttpd is a lightweight HTTPserver that can be installed on a phone. In our case, we can start an HTTP server at a given port which supports dynamic file serving such that the captured videos can be played online upon requests from a browser client.
3. The Video Based Pass code Inference Attack:
In this system, we discuss two types of camera attacks for inferring pass codes. We also discuss the computer vision techniques for eye tracking that can be utilized in the attacks.
(a) The Application-Oriented Attack: The first type of attack is the application-oriented attack, which aims at getting the credentialsof certain apps. Most apps (like Face book) that require authentication containletters, which need a complete virtual keyboard. There are two other types of popularpass codes, pattern and PIN. Smart App Protector is a locker app by which a user is ableto lock apps that need extra protection (i.e., Gallery, messaging, and dialing apps).For asuccessful pass code inference attack ,the video must be captured during user authentication.
(b) The Screen Unlocking Attack: In this subsection, we discuss another type of attack. The attack is launched when a useris entering a screen unlocking pass code. We categorize this scenario as a different attackmodel since it is unnecessary to hide the camera preview under this circumstance.

III.PROPOSED ALGORITHM

To implement the attacks on real phones, and demonstrate the feasibility and effectiveness of the attacks. 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.In this paper we are using Viola-Jones forFace Detection.
TheViola-Jones Object Detection Framework is a generic framework for object detection, which is particularly successful for face detection. In this assignment, we provide a simplified version of Viola-Jones face detection algorithm, implemented by our colleague Francesco Comaschi. The simplified implementation does not include the training part of the framework. The cascade classifier in the simplified implementation uses pre-trained parameters for the cascade classifier. Although the provided code is not meant to be an optimal implementation, yet it provides reasonable detection rate for a wide range of input images. The image below is an example that is included in the package.

IV.PSEUDO CODE

Viola-Jones Face Detection:

```
Begin:
for number of scales in image pyramid do
   downsample image by one scale
   compute integral image for current scale
   for each shift step of the sliding detection window do
      for each stage in the cascade classifier do
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

```
        for each filter in the stage do
          filter the detection window
        end
        accumulate filter outputs within this stage
        if accumulation fails to pass per-stage threshold do
          break the for loop and reject this window as a face
        end
      end
      if this detection window passes all per-stage thresholds do
        accept this window as a face
      else
        reject this window as a face
      end
    end
end
```

V.ACKNOWLEDGEMENT

We would like to take this opportunity to express my sincere gratitude to my Project Guide Prof Ramesh G Patole (Assistant Professor, Computer Engineering Department) for his encouragement, guidance, and insight throughout the research and in the preparation of this dissertation. He truly exemplifies the merit of technical excellence and academic wisdom.

VI.CONCLUSION AND FUTURE WORK

In this paper, we study camera related vulnerabilities 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 defence 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 the using various attack how to implement android app for to find mobile thief and its location using ksoap2 protocol.ksoap2 protocol is very secure to transfer information because it uses envelope to transfer data.

REFERENCES

[1]. Y. Zhou and X. Jiang, ―Dissecting Android Malware: Characterization and Evolution,‖ IEEE Symp. Security and Privacy 2012, 2012, pp. 95–109.
[2]. R. Schlegel et al., ―Soundcomber: A Stealthy and Con- text-Aware Sound Trojan for Smartphones,‖ 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. Conf.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 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]. D. Li, D. Winfield, and D. Parkhurst, ―Starburst: A Hybrid Algorithm for Video-Based Eye Tracking Com- binning Feature-Based and Model-Based Approaches,‖ IEEE Computer Soc. Conf. Computer Vision and Pattern Recognition — Workshops, 2005, p. 79.
[10]. P. Adrian, ―Fast Eye tracking,‖ http://www.math- works.com/matlabcentral /file exchange/25056-fast-eye- tracking, 2009.