Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Camera Based Attacks On Mobile Phones

Security in wireless multimedia communications

Geeta Nage[1], Ashwini Jadhav[2], Azar Kazi[3] ,Sandesh Mundhe[4]
[1,2,3,4]*Computer, PGMCOE*

Abstract— Now a days mobile smartphones are very powerful,and many smartphone applications use wireless multimedia communications. Mobile phone security is important security issues in wireless multimedia communications.In mobile operating system, Android security has been extensively studied by researchers. However, few works have studied mobile phone multimedia security. We mainly focus on security issues related to mobile phone cameras. Several new attacks are discovered based on the use of phone cameras. We implement the attacks on real phones, and show the possibility and efficiency of the attacks. moreover, we propose a lightweight defense scheme that can proficiently detect these attacks.

Keywords— Smart phone , Spy camera , Wifi , Passcode

I. INTRODUCTION

The Android operating system(OS) has gain an unbelievable rate of popularity. since 2013, the Android OS has 79.3 percent of smartphone market shares.Android security and privacy vulnerabilities have been uncovered in large numbers. Even if,before installation the Android permission system gives an opportunity to user to check the permission of an application(app), many users don't have knowledge of all these permission requests ; so, they not able to notify to the users about security risks. In recent years,in Android app markets number of apps are precise to provide security and protect user privacy. Android-version security apps have been published by anti-virus software companies, and tried to protect smartphones by detecting and blocking msalicious apps. There are also the data protection apps which provide means to the users to encrypt, decrypt, sign,and verify signatures for private texts, emails and files. For mobile phone security and privacy mobile malware and privacy leakage become a big issue.Generally, when we talking about privacy protection,safety of SMS, emails, contact lists, calling histories,location information, and private files are considered.The phone camera could also become a spy; for example, attackers could take pictures silently and record videos by using the phone camera. In this days,different types of camera-based applications have available in Android app markets (photography,barcode readers, social networking, etc.). Spy camera apps become most popular. For Google Play,almost 100 spy camera apps are available, using this phone users take pictures or record videos of other people without their permission. but,it is also possible that phone users itself become victims. Attackers can implement spy cameras in malicious apps such that the phone camera is activate automatically without the device owner's permission, and the captured photos and videos are sent out to these remote attackers. Nowadays, people carry their phones everywhere;hence, then lots of private information is being captured. If the phone camera is exploited by a malicious spy camera app, it may cause serious security and privacy problems. For example, the phone camera may record a user's daily activities and conversations, and then send these out via the Internet or multimedia messaging service(MMS). Secret photography is considered as a illegal in some countries due to the security attack. A phone camera could also play vital role if it is well controlled by the device owner. For example,when the owner wants to check if someone has used his/her phone without permission, the phone camera could be used to record the face of an unauthorized user. as well, it can help the owner to find a lost phone. In this paper we present the basic attack model and two camera based attacks: the remote-controlled real-time monitoring attack and the passcode inference attack. We implement these

attacks along with popular antivirus software to test their stealthiness, and conduct experiments to assess both types of attacks. The results show the possibility and use of these attacks. Finally, we propose a lightweight defense scheme.

II. LITERATURE SURVEY

Now a days many problems are occurred while obtaining private information on smartphones using multimedia devices such as microphones and cameras. For example, Xu et al. [1] present a data collection technique using a video camera . Their malware secretly records video and transmits data using either email or MMS. In this work, we are able to hide the whole camera app in Android. Moreover, we implement advanced forms of attacks such as remote controlled and real-time monitoring attacks.Several video-based attacks targeted at keystrokes have been proposed. The attacks can obtain user input on touch screen smartphones. Maggi *et al.* [5] realize an automatic shoulder surfing attack on smartphones.The attacker use a video camera to record the target screen when the victim is entering text. User input can be again constructed from keystroke feedback displayed on the screen. but, this attack needs more camera device, and issues like how to place the camera near the victim without knowing must be considered carefully. It works only when magnified keys are available. iSpy [4], proposed by Raguram, shows how screen reflections is used for reconstruction of text typed on a smartphone's virtual keyboard. Similarly, this attack also needs an extra device to capture the reflections, and the visual key press confirmation mechanism must be enabled on the target phone. In contrast, our camera-based attacks work without any support from other devices.

III. PROPOSED SYSTEM

We want to discover possible attacks based on a spy camera. The attacks should appear normal to user experience. Attacks should run stealthily and silently so that they do not cause a user alert.Attacks have a translucent view, make no sound or vibration, and check phone resource utilization before launching themselves. The general architecture should contain the following six parts. Figure 1 shows the architecture of a basic spy camera attack.

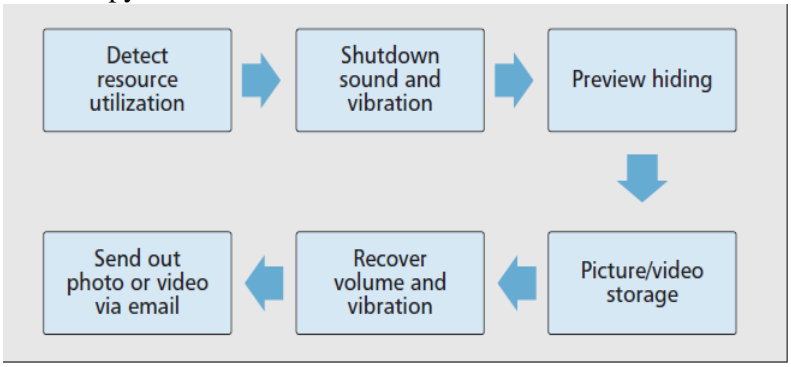

Figure.1 basic architecture of camera attack model

3.1. The remote-controlled real-time monitoring attack

The basic camera attack can be improved to more violent attacks. For example, the attacker can remotely control the spy camera app such that the time of attack launch and end is under control. The remote control is implemented using socket.Then app can be controlled using orders like "launch" and "stop" or specify.Many android apps are availiable that provide security in phone.Videos are capture through the front-face camera, even if the phone's screen is screening its app menu.Remote-controlled real-time monitoring attack could create a big threat to a phone user's privacy: daily activities and surrounding environment are all under the eye of the attacker. Camera-based attacks can be detected when multiple apps request the camera device at the same time or if the camera is being used by another app. But this can easily be avoided by selecting the time to launch attack. The malicious camera app can regularly check the screen status and run the quiet video recording only

when the screen is off, which means that the user is not using the phone and the camera device is idle.

3.2.The video-based passcode inference attack

we talk about two types of camera attacks for inferring passcodes.

3.2.1.Application oriented attack

Smart App Protector is a locker app which is used to lock apps (i.e., Gallery, messaging,dialing apps). provide extra protection. In passcode inference attack,the video is captured during user authentication.Poll the running task list and launch the attack as soon as the target app appears on top of the list. It opens the camera and takes videos of the user's face (especially the eyes)secretly with a front-face camera for a time long enough to cover the entire authentication process,when attack conditions are met. The view is totally transparent to users in mobile phone attack, so that not need to worry. but, frequency need to maintain at about two scannings per second;or else the attack may take place after the user starts entering the password.

3.2.2.Screen unlocking attack

When a user is entering a password to unlock the screen,attack is launched.Until a user not entering the correct password android system would not show the user interface,for achieving privacy. This provides a protection for spy camera attacks besieged at the screen unlocking process. Users is unaware of camera is working, even though the camera preview is right under the unlocking interface.When screen turns on attack should start and when the screen is unlocked it should end.

IV. CONCLUSION

We study camera-related problems in Android phones for mobile multimedia applications.We studied some advanced spy camera attacks, with the remote-controlled real-time monitoring attack and two types of passcode inference attacks.To secure a smartphone from all these spy camera attacks we propose an effectual defence scheme. In the upcoming years,we will investigate the possibility of performing spy camera attacks on other mobile operating systems.

REFERENCES

[1] 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.

[2] Longfei Wu and Xiaojiang Du,"Security Threats to Mobile Multimedia Applications: Camera Based Attacks on Mobile Phones", University of Massachusetts Lowell,March 2014

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

[4] 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.

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