INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

Spy camera attacks on mobile security

Bhagyashree Sonone
bhagyashree.sonone98@gmail.com
Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra

Samrudhi Khond
khondss@rknec.edu
Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra

Pranali R. Dandekar
dandekarpr@rknec.edu
Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra

ABSTRACT

Nowadays, Smartphone security has become a major issue to resolve. All the smart phones have features like camera, touch screen and many more. These may cause attacks on users smart phones. Modern smart phone platforms provide users to customize their device using applications found on app stores. Users are constantly in trouble that they are unaware of installing malicious apps that steal personal data or gain access to other private information. For example, while using such malicious application, the application provider may carry the hidden request to have access to different devices connected to our phone such as camera, smart phone is been attacked, identifying our location through camera as it will show our surrounding area and trying to identify PIN using camera. However, few Works have studied mobile phone multimedia Security. In this survey, we focus on security problems related to mobile phone cameras. Specifically, we discuss several attacks that are based on the smart phone features.

Keywords: *Security, Attack, Malware, Camera, Anti-Thief.*

1. INTRODUCTION

Meanwhile, a number of Android security and privacy issue have been reveal in the past years. Although the Android permission system gives users an opportunity to check permissions of an application before installation, few users have knowledge of what all these permission requests stand for. Mobile phones are becoming major part of people's everyday life, since they are connected with friends, family, and other activities.

Doing business using internet and other activities. Generally, when we talking about privacy protection, emails, safety of SMS, contact lists, location, calling histories, and important files are considered. The Phone camera could also become a spy; for example, attackers could take pictures and record videos by using the phone camera. For Google Play store, almost 100 spy camera apps are available, using this users take pictures or record videos of other people without their permission. Attackers can execute spy cameras in dangerous apps such that users phone camera is activate automatically without the Device owner's permission, and the pickup photos and videos are sent out to these attackers.

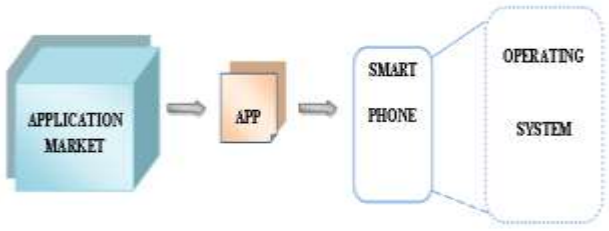

Fig: Getting Application into Phone

2. LITERATURE STUDY

As, all the smart phone uses the application from app store and run them within a middleware environment. Smart phones are possible to get attacked through malicious application. The details about such security threats are as below:

3. MOBILE DEVICE THREATS

Numerous attack happen which decreases security of mobile devices. Some types of attacks could be defined over mobile devices which also includes malware attacks described as:-

4. MALWARE

These kinds of attacks steal personal data from mobile devices and damage devices. With device vulnerabilities and user to install additional apps, attacker can obtain unauthorized access to devices. Some of the attacks are listed below:-

i. Bluetooth Attacks:
In Bluetooth attack, attacker could add or delete contacts or SMS, take user's data from their devices and can track user's mobile location**.** Blue-bugging is a technique that allows hackers to access Bluetooth enabled devices by which attacker can listen conversations by activating software containing malicious data.

ii. SMS Attacks:
In this attack, attacker can advertise and distribute phishing links. SMS service can also be used by attackers to exploit vulnerabilities.

iii. GPS/Location Attacks:
In this attack, current location of the user can be accessed with Global Positioning System i.e. GPS. Hardware and then information can be sold to other companies involved in advertising.

iv. Phone Jail-Breaking:
In phone jail-breaking, an attacker can harm security system in operating system as it allows operating system to install additional and insecure applications. Users usually install them for getting additional functionality.

v. Premium Rate Attacks:
In premium rate attacks, fraud directly attacks subscribers by getting them to make calls and premium rate SMS messages could go unnoticed until attacker faces thousands of dollars of bill on his device as they don't need permissions to send SMS on premium rated numbers.

vi. Gray ware:
Gray ware includes applications which collect the data from mobile devices for marketing purposes. Their intention is make no harm to users but annoy them.

vii. Spyware:
In Spyware, it collects personal information about user from his smart phone such as contacts, messages, call history and location. Personal spyware are able to take physical access of the device by installing software without user's involvement. By collecting information about user from phone, they send it to outside attacker.

5. SPY CAMERA ATTACK WORKFLOW

Step 1:

Detect Resource Utilization

- When CPU memory usage high after launching the attack and make the phone performance abominable.

Step 2:

Shutdown Sound and Vibration

- For launching attacks a malicious camera app can continuously observe remaining action after ensuring limited resources. After the attack, the app can change the current volume level of the phone and current vibration condition and other parameters.

Step 3:

Preview Hiding

- It is difficult to hide the preview of camera .so set the view parameter by changing the attribute of the window manager .by addViewFunction finally the app can add the hidden preview dynamically.

Step 4:

Picture or Video Storage

- Using filename and seldom visited directories, the photos or videos are store in hidden Mode

Step 5:

Recover Volume and Vibration

- After previous action the app can release the camera and set the audio volume and vibration back to original state without knowing owner.

Step 6:

Send Out Photo or Video via Email

- After this step, via cellular network the transmission of collection of data is outside

This all steps are gives some idea about what spy camera works on smart phone for giving personal information. Some based architecture of these steps is as follows:

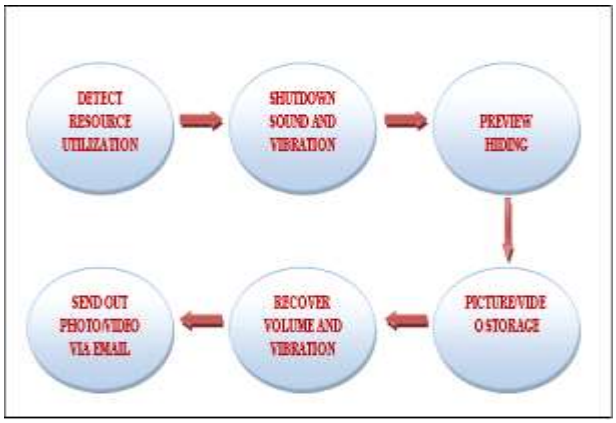

Fig: Spy Camera Attack Workflow

6. DISADVANTAGES

As mentioned above, the role a spy camera plays depends on the way it is used and who is in control of it. In the following, we discuss some threats and benefits of using a spy camera.

- **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 harm the user's phone. For example, it appears to be a normal app with legitimate use of a camera and the Internet. On one hand, it performs the function it claims. On the other hand, it runs an application in background to secretly record videos or capture pictures, and store them with hidden names in a directory that is rarely visited. Then these data are sent out to the outside attacker over Wi-Fi access or other fast or unlimited network connection.

- **Watchdog**

Watchdog is a thing that spy camera can do. Nobody wants other people to use or check their phone without permission. A spy camera can take pictures of the phone user stealthily and allocate them who use or check other people's phones.

7. ADVANTAGE

- **Anti-Thief**

A spy camera could play a completely different role if it is used properly. When a user loses their 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 catch the thief and get the phone back.

8. CONCLUSION

We study camera based problems in smart phones for mobile based multimedia applications. We studied some advanced spy camera attacks based on android phones. To secure an android phone from all of these spy camera based attacks we propose an effectual defense scheme. In the upcoming years, we will research the possibility of Performing spy camera attacks on user's mobile operating systems. We discuss the roles a spy camera can play to attack or benefit Phone users. We introduced effects of spy camera while using smart phones security. In the future, we will research the practicability of performing spy camera.

9. REFERENCE

[1] A Review on Camera Based Attacks on Android Smart Phones http://www.ijcst.com/vol61/1/17-Anushree-Pore.pdf
[2] Threats and Attacks Based on Smart phones Camera https://www.onlinejournal.in/IJIRV3I3/023.pdf
[3] Attack on spy camera and finding fraud Applications on Google store
http://www.ijarse.com/images/fullpdf/1510225837_817ijarse.pdf
[4] Camera Based Attacks On Mobile Phones https://www.ijmter.com/papers/volume-3/issue-3/camera-based-attacks-on-mobile-phones.pdf

