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 5, May 2015

A Research on Camera Based Attack and Prevention Techniques on Android Mobile Phones

Anushree Pore, Prof. Mahip Bartere

PG Student, Dept. of CSE, G H Raisoni College of Engineering, Amravati, Maharashtra, India

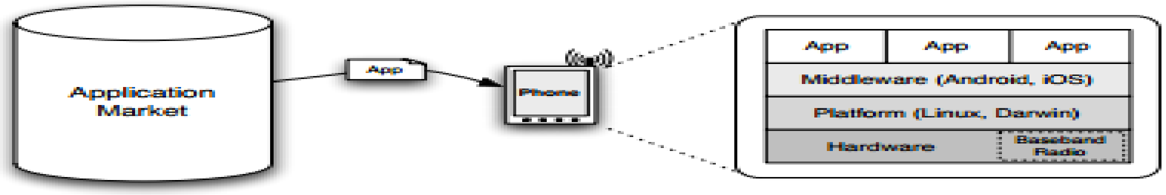
Professor, Dept. of CSE, G H Raisoni College of Engineering, Amravati, Maharashtra, India

ABSTRACT*:* Do we regard our smartphone cameras and speakers as a security threat? We might not, but surprisingly the phone camera could become a traitor; for example, attackers could stealthily take pictures and record videos by using the phone camera. Spy camera apps have also become quite popular. Which allow phone users to take pictures or record videos of other people without their permission. Attackers can implement spy cameras in malicious apps such that the phone camera is launched automatically without the device owner’s notice, and the captured photos and videos are sent out to these remote attackers. 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 paper, we present the attacking application with preventive scheme.

KEYWORDS*:* energy Camera Based Attacks, GPS, Spy-Camera.

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. Meanwhile, a number of Android security and privacy vulnerabilities have been exposed in the past several years. Although 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 malware 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 without 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 requested 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 users’ alertness to camera-based multimedia application attacks. Smart phones retrieve apps from application markets and run them within a middleware environment. Existing smart phone platforms rely on application markets and platform protection mechanisms for security. The Figure 2 shows the general architecture of smart phones.



II. RELATED WORK

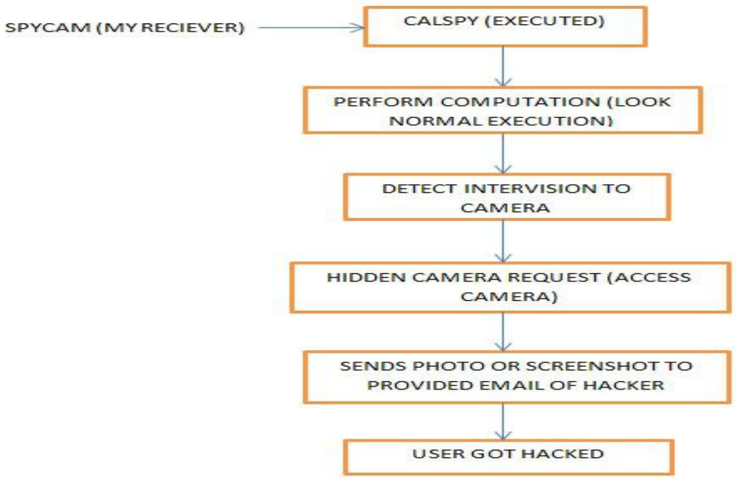
Soundcomber [17] is a stealthy Trojan that can sense the context of its audible surroundings to target and extract highvalue data such as credit card and PIN numbers. Stealthy audio recording is easier to realize since it does not need to hide the camera preview. Xu et al. [18] present a data collection technique using a video camera embedded in Windows phones. Their malware (installed as a Trojan) secretly records video and transmits data using either email or MMS. Windows phones offer a function, ShowWindow(hWnd, SW HIDE), which can hide an app window on the phone screen. However, it is much more complicated (no off-the-shelf function) to hide a camera preview window in an Android system. 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. We also utilize computer vision techniques to analyze recorded videos and infer passcodes from users' eye movements.Several video-based attacks targeted at keystrokes have been proposed. The attacks can obtain user input on touch screen smartphones.

Maggi et al. [19] implement an automatic shoulder surfing attack against modern touch-enabled smartphones. The attacker deploys a video camera that can record the target screen while the victim is entering text. Then user input can be reconstructed solely based on the keystroke feedback displayed on the screen. However, this attack requires an additional camera device, and issues like how to place the camera near the victim without catching an alert must be considered carefully. Moreover, it works only when visual feedbacks such as magnified keys are available.iSpy [20], proposed by Raguram, shows how screen reflections may be 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

In this section, we discuss possible countermeasures that can protect Android phones against these spy camera attacks. In an Android system, no application programming interface (API) or log file is available for a user to check the usage of a camera device. Hence, detection of camera-based attacks requires modification to the system. So, the application can be developed which detects the hidden request in the response from the application provider. Such app will check the hidden request and presents an alert dialog including the name of the suspicious app is displayed, and what kind of hidden request is for will be displayed, for e.g. app wants to use camera, this is the hidden request called spy camera attack. Besides, the detailed activity patterns of suspected apps are logged so that the user can check later. In accordance to this we developed two apps one to show the one of the possible attack and one the protecting app.

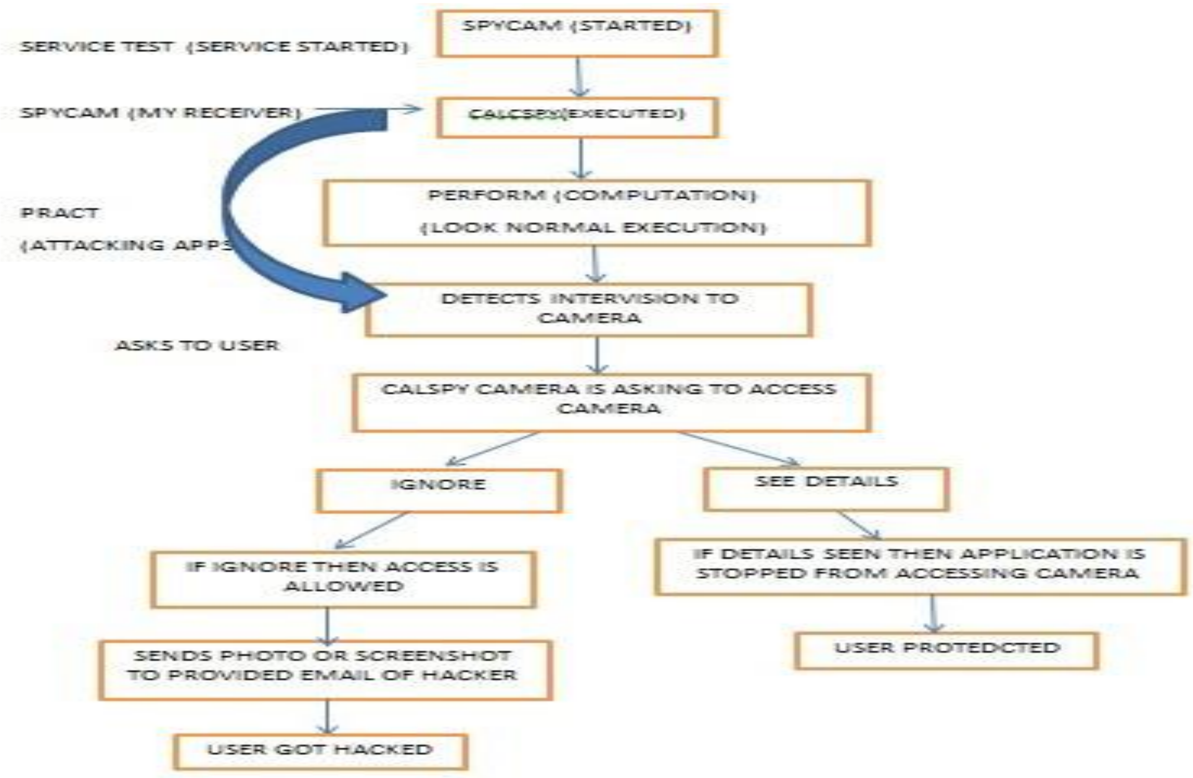
System model for attacking application.


SPYCAM (MY RECIEVER)
CALSPY (EXECUTED)
PERFORM COMPUTATION (LOOK NORMAL EXECUTION)
DETECT INTERVISION TO CAMERA
HIDDEN CAMERA REQUEST (ACCESS CAMERA)
SENDS PHOTO OR SCREENSHOT TO PROVIDED EMAIL OF HACKER
USER GOT HACKED

CalcSpy:

* Application Look like a Calculator.
* As the application is started, it performs normal computations like calculator.
* But internally an Image is Captured Automatically without user intervention.
* The Captured Image along with the text is being sent to the Attackers email Id.
* The user feels that only there is some lag in the running of application but in reality he/she is hacked.

System model for protecting application


SERVICE TEST (SERVICE STARTED)
SPYCAM (STARTED)
SPYCAM (MY RECEIVER)
CALCSPY(EXECUTED)
PERFORM (COMPUTATION)
(LOOK NORMAL EXECUTION)
PRACT
(ATTACKING APPS
DETECTS INTERVISION TO CAMERA
ASKS TO USER
CALSPY CAMERA IS ASKING TO ACCESS CAMERA
IGNORE
SEE DETAILS
IF IGNORE THEN ACCESS IS ALLOWED
IF DETAILS SEEN THEN APPLICATION IS STOPPED FROM ACCESSING CAMERA
SENDS PHOTO OR SCREENSHOT TO PROVIDED EMAIL OF HACKER
USER PROTEDCTED
USER GOT HACKED

SpyCam:

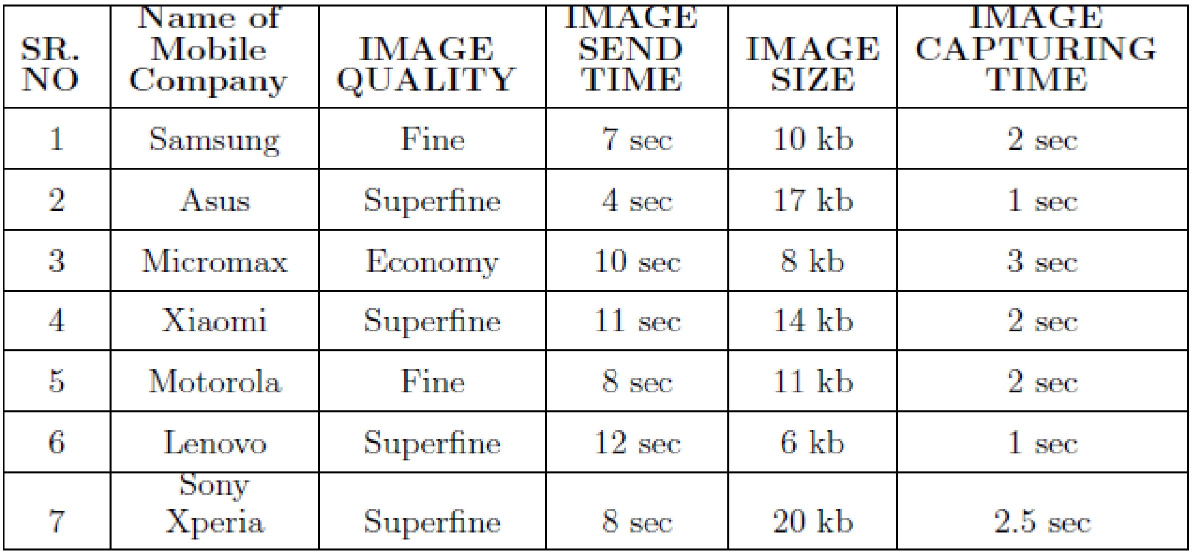
* As the application starts it gives some basic Introduction about what actually is the purpose of the application.
* The next window is the Login Window here user needs to register himself for only once the user gets here an Login Id and the Password for Logging in.
* After Successfully Logging In, the application prepares the Complete List of all installed applications in the Phone that can access Camera or that can access Camera.
* Now the user is ready to Safely Use any Application.
* As user clicks on any Application the App checks whether that Particular app is accessing the camera at the time if yes then It Pops up a notification window telling the user about the camera access.
* Now the user has the power to allow or reject the application to access the camera.
* If any app uses camera but is not currently the app allows the application.
* Thus the user is protected from any camera based attack.

IV. PERFORMANCE ANALYSIS

We have developed two applications as SpyCam and CalcSpy and done the Computational analysis by considering following points:

1. Image Quality
2. Mail Send Time
3. Image Size
4. Image Capturing Time

Table 1: Performance analysis



SR. NO	Name of Mobile Company	IMAGE QUALITY	IMAGE SEND TIME	IMAGE SIZE	IMAGE CAPTURING TIME
1	Samsung	Fine	7 sec	10 kb	2 sec
2	Asus	Superfine	4 sec	17 kb	1 sec
3	Micromax	Economy	10 sec	8 kb	3 sec
4	Xiaomi	Superfine	11 sec	14 kb	2 sec
5	Motorola	Fine	8 sec	11 kb	2 sec
6	Lenovo	Superfine	12 sec	6 kb	1 sec
7	Sony Xperia	Superfine	8 sec	20 kb	2.5 sec

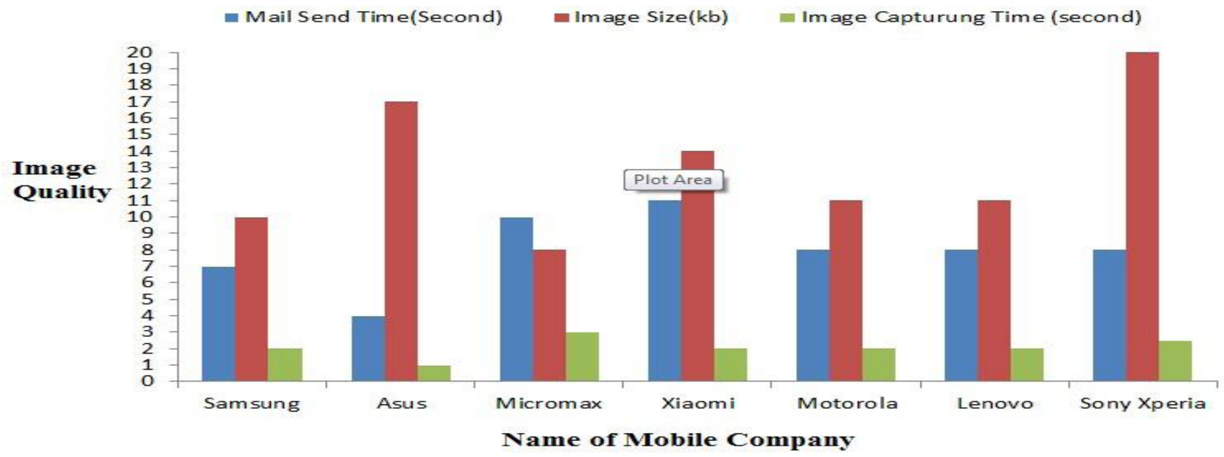


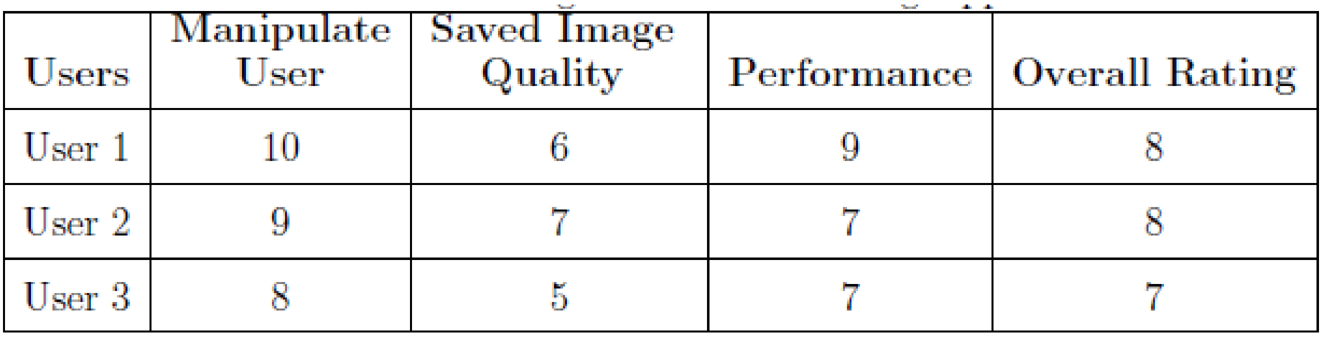
Figure 4.1.1: Performance Analysis

Average Analysis
Quality: Fine
Mail Send Time: 7 Sec
Image Size: 13 kb
Image Capture Time: 1.5 Sec

V. USER RATING BASED ATTACKING APPLICATION

We have done this experimental analysis for our Attacking Application named as Calc-Spy. We have done this analysis by giving application to the different users for use. They have used our application and give their rating based on the parameters given in the following table.

Table 2: User Rating Based on Attacking Application



Users	Manipulate User	Saved Image Quality	Performance	Overall Rating
User 1	10	6	9	8
User 2	9	7	7	8
User 3	8	5	7	7

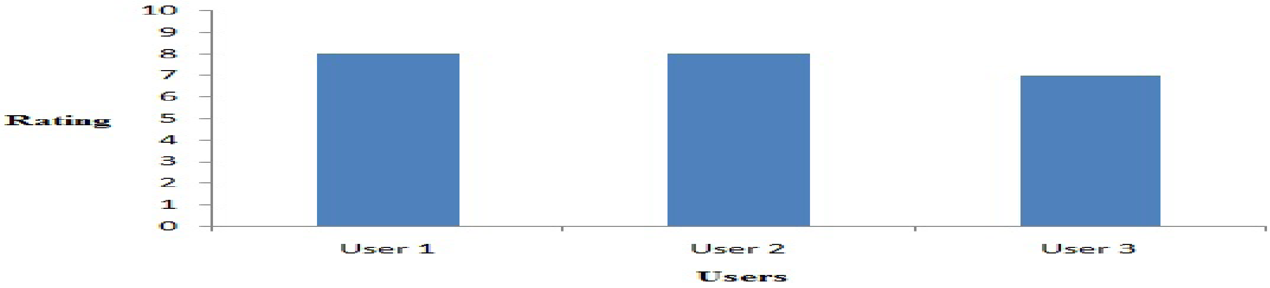
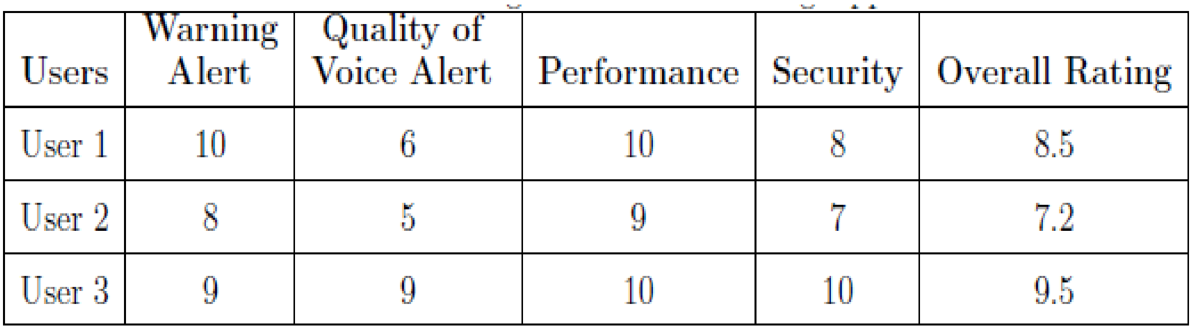


Figure 4.2.4: Average Rating of Users

VI. USER RATING BASED ON PROTECTING APPLICATION

We have done this experimental analysis for our Protecting Application named as SpyCam. We have done this analysis by giving application to the different users for use. They have used our application and give their rating based on the parameters given in the following table.

Table 3: User Rating Based on Protecting Application



Users	Warning Alert	Quality of Voice Alert	Performance	Security	Overall Rating
User 1	10	6	10	8	8.5
User 2	8	5	9	7	7.2
User 3	9	9	10	10	9.5

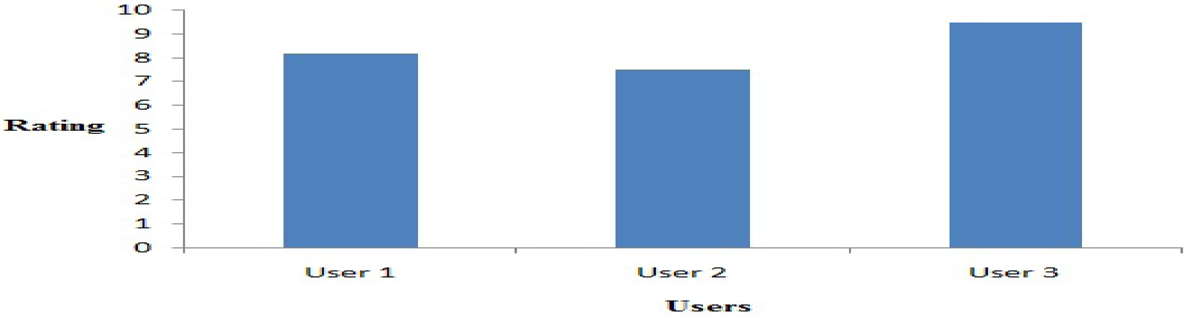


Figure 4.2.8: Average Rating of Users

VII. ATTACKING APPLICATION

This is an User Interface of the attacking application. We named this application as CalcSpy. This application is look like the real normal calcultor application but internally it will capture the image and as soon as you press equal to button it will send the capured image and text to the hackers email id.

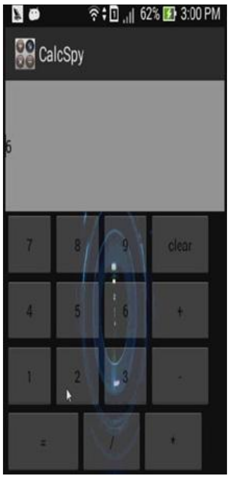
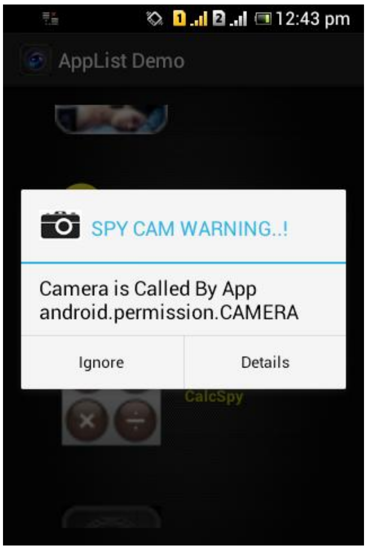


Figure 4.6.5: CalcSpy (Fake Application)

VIII. PROTECTING APPLICATION

The application shows list of all the application installed in the mobile phone. User can click on any of the application from the list. If user click on Ignore button then fake application will perform its intended work. And if user press Details button the app will show all the information about application which is trying to access camera.



SPY CAM WARNING..!

Camera is Called By App android.permission.CAMERA

Figure 4.6.4: Camera is Called by App

IX. CONCLUSION

In this article, 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 defense scheme to secure a smartphone from all these spy camera attacks. In the future, we will investigate the feasibility of performing spy camera.

REFRENCES

[1] Google bets on Android future. http://news.bbc.co.uk/2/hi/technology/7266201.stm

[2] D.Stites, A.Tadimla :A Survey Of Mobile Device Security: Threats, Vulnerabilities and Defenses./urlhttp://afewguyscoding.com/2011/12/survey-mobile-device-security-threats vulnerabilities-defenses.

[3] W.Enck, P. Gilbert, B.G. Chun, L.P.Cox, J.Jung, P.McDaniel, A.P.Sheth: TaintDroid: an information on tracking system for realtime privacy monitoring on smart-phones.:In OSDI'10 Proceedings of the 9th USENIX conference on Operating systems design and implementation,pp.1-6 ,USENIX Association Berkeley, CA,USA (2010)

[4] T.Blasing, L.Batyuk, A.D.Schimdt, S.H.Camtepe, S.Albayrak,:An Android Application Sandbox System for Suspicious Software Detection.

[5]McAfee Labs Q3 2011 Threats Report Press Release, 2011,http://www.mcafee.com/us/about/news/2011/q4/20111121-01.aspx

[6] A.D.Schmidt, J.H.Clausen,S.H.Camtepe, S.Albayrak: Detecting Symbian OS Malware through Static Function Call Analysis: In Proceedings of the 4th IEEE International Conference on Malicious and Unwanted Software,pp.15-22.IEEE(2009).

[7] H.Kim, J.Smith, K.G.Shin,:Detecting energy-greedy anomalies and mobile malware variants: InMobiSys 08: Proceeding of the 6th international conference on Mobile systems, applications, and services,pp.239-252.ACM,NewYork(2008).

[8] A. Bose,X.Hu, K.G.Shin, T.Park: Behavioral detection of malware on mobile handsets:In MobiSys08: Proceeding of the 6th international conference on Mobile systems, applications, and services,pp.225-238.,ACM,NewYork(2008).

[9] L.Min,Q.Cao: Runtime-based Behavior Dynamic Analysis System for Android Malware Detection:Advanced Materials Research,pp.2220-2225.

[10] V.Rastogi, Y.Chen, W.Enck: AppsPlayground: Automatic Security Analysis of Smartphone Applications: In CODASPY'13 Proceedings of the third ACM conference on Data and application security and privacy,pp.209-220.ACM,NewYork(2013)

[11] D.J.Wu,C.H.Mao,T.E.Wei,H.M.Lee,K.P.Wu: DroidMat: Android Malware Detection through Manifest and API Calls Tracing.: In Information Security (AsiaJCIS), 2012 Seventh Asia Joint Conference ,pp.62-69.IEEE,Tokyo(2012)

[12] R.Jhonson, Z.Wang, C.Gagnon, A.Stavrou,: Analysis of android applications' permissions.:In Software Security and Reliability Companion (SERE-C) Sixth Inter-national Conference,pp.45- 46.IEEE(2012)

[13] Y.Zhou,, Z.Wang, W.Zhou,X.Jiang: Hey, You, Get o_ of My Market: Detecting Malicious Apps in O_cial and Alternative Android Markets: In Proceedings of the 19th Network and Distributed System Security Symposium,San Diego,CA(2012).International Journal of Distributed and Parallel Systems (IJDPS) Vol.5, No.4, July 2014.

[14] L.Batyuk,M.Herpich,S.A.Camtepe,K.Raddatz,A.D.Schmidt,S.Albayrak:Using static analysis for automatic assessment and mitigation of unwanted and malicious activities within Android applications.: In 6th International Conference on Malicious and Unwanted Software,pp.66-72.IEEE Computer Society(2011)

[15] M.Ongtang,S.E.McLaughlin,W.Enck,P.D.McDaniel,:Semantically rich application-centric security in android:In Proceedings of the 25th Annual Computer Security Application Conference (ACSAC),pp.340-349(2009)

[16] L.Xie, X.Zhang, J.P.Siefert, S.Zhu: pBMDS: a behavior-based malware detection system for cellphone devices.:In Wisec'10 Proceedings of the third ACM conference on Wireless network security,Hoboken,pp.37-48.ACM,USA(2010).

[17] R. Schlegel et al., "Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones," NDSS, 2011, pp. 17–33.

[18] N. Xu et al., "Stealthy Video Capturer: A New VideoBased Spyware in 3g Smartphones," Proc. 2nd ACM Conf. Wireless Network Security, 2009, pp. 69–78.

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

[20] 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.

[21] Longfei Wu et. al., "Security Threats to Mobile Multimedia Applications: Camera-Based Attacks on Mobile Phones", Security in Wireless Multimedia Communications, IEEE Communications Magazine, March 2014, pp. 80-87.