International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 4, July - August 2015 ISSN 2278-6856

Preventions and Features of Camera Based Attacks on Smart Phones

Prof.Mahip Bartere, Miss. Anushree Pore

G H Raisoni, College of Engineering Anjangao Bari Road Amravati, Maharashtra, India

Abstract

Generlly when talking about privacy protection ,most smart phone users pay attention to the safety of SMS, emails, contact lists, calling histories, location information, and private files. Since they are mobile and used as everyday gadgets, they are susceptible to get lost or stolen. Hence, access control mechanisms such as user authentication are required to prevent the data from being accessed by an attacker. However, commonly used authentication mechanisms like PINs, passwords, and Android Unlock Patterns suffer from the same weakness: they are all vulnerable against different kinds of attacks, most notably shoulder-surfing. In this paper, we focus on the Android platform and aim to systematize or characterize existing Android malware. As a result mobile security is no longer immanent, but imperative. This survey paper provides a concise overview of mobile network security, attack vectors using the back end system and the web browser, but also the hardware layer and the user as attack enabler.

Keywords: Malware, Security, Preventions.

1.Introduction

To implement an android based attacks detection and prevention system from camera based attacks on mobile phone. To develop an 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. And demonstrate the feasibility and effectiveness of the attacks detection and prevention. smartphones offer different authentication mechanisms like passwords, PINs, or Android Unlock Patterns. Since passwords and PINs are cumbersome to enter into the device, alternative solutions are needed.The goals and contributions of this paper are threefold. First, we fulfil the need by presenting the first large collection of 1260 Android malware samples1 in 49 different malware families, which covers the majority of existing Android malware, ranging from their debut in August 2010 to recent ones in October 2011. However, we recently saw the first real attacks against smartphones: In March 2010, Iozzo and Weinmann demonstrated a drive-by download attack against an iPhone 3GS that enabled an attacker to steal the SMS database from the phone. In November 2010, one of the first public exploits to perform an attack against the mobile browser shipped with Android was released. Indeed, in recent years there have been a rash of attacks (typically focused on bank ATMs and gas stations) in which the user's payment card stripe is acquired via a "skimmer" while a pinhole camera is used to capture the associated PIN as it is entered.

Table 1: Specifications of selected smartphones
Model Touch Screen

Model Sample	Touch Screen Size (pixels)	Acc. Sample Rate	Ori. Sample	Rate Android
Aria	!(320)×"(480)	~ 50"	~ 50"	v2.3
Nexus	!(480)×"(800)	~ 25"	~ 25"	v2.3
Atrix	!(540)×"(960)	~ 95"	~ 8"	v2.3

As motion sensors are considered as insensitive resource, TapLogger does not require any security permission to access the accelerometer and orientation sensors. As mentioned in the introduction, thermal cameras have a clear advantage over conventional cameras for the purposes of capturing codes: conventional cameras need to film the code as it is being typed, whereas thermal cameras can recover the code for some time afterwards.

1) GSM: Global System for Mobile communications (GSM) is the first and most popular standard in Europe for mobile telecommunication system and is part of the secondgeneration (2G) wireless telephone technology. We raise awareness of the di_culty of properly design- ing a trusted path. Speci_cally, all shared resources need careful consideration when reasoning about their security. Mobile applications use and depend on sensors more extensively. Moreover, users tend to carry mobile devices wherever they go. A shoulder surfer would only obtain a subset of the potential PIN, but she could reconstruct the PIN with an intersection analysis if she would be able to watch the entry process several times.

2. METHODOLOGY

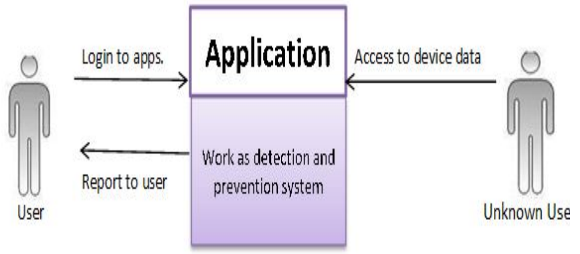


Figure. 1 Camera Based Attack Detection and Prevention

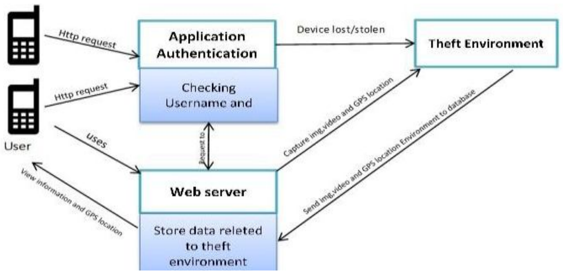

Http request
Application Authentication
Device lost/stolen
Theft Environment
Http request
Checking Username and
User
uses
Request to
Capture img,video and GPS location
Send img,video and GPS location Environment to database
View information and GPS location
Web server
Store data releted to theft environment

Figure. 2 Working under mobile lost/stolen situation

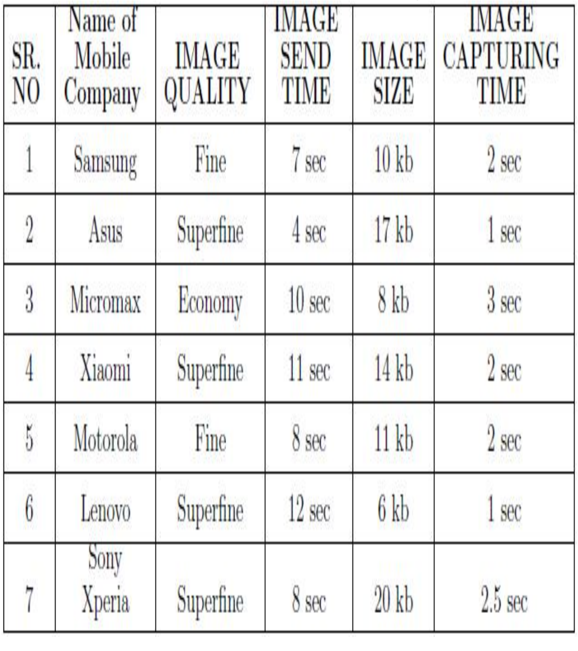
we perform an evolution-based study of representative android malware, which shows that they are rapidly evolving and existing anti-malware solutions are seriously lagging behind. For example, it is not uncommon for Android malware to have encrypted root exploits or obfuscated command and control (C&C) servers. The adoption of various sophisticated techniques greatly raises the bar for their detection. In fact, to evaluate the effectiveness of existing mobile anti-virus software The PIN login mechanism is a special case of the aforementioned passwords. Whenever any application is accessing mobile camera then this application will give us such pop-up message that which application is requesting for camera access. Such way user get alert and user have to decide whether to give permission or reject that request for camera access. However, the overall attack scenario of side channel analysis is not very likely in the case of SIM cards. Here, an attacker needs physical access to the SIM card to perform some measurements. While possible, this is not very plausible since users typically take their devices with them. As mentioned in the introduction, thermal cameras have a clear advantage over conventional cameras for the purposes of capturing codes: conventional cameras need to film the code as it is being typed, whereas thermal cameras can recover the code for some time afterwards. The stealthiness depends on the type of components that is exploited to root the phone. For example, some Android root exploits like do not need any permissions while others might. After exploitation, the rootkit can tamper with the relevant OS components to hide itself entirely from the victim. Malware detection on smartphones is a difficult task. Although in principle not different from malware detection on desktop computers, the limited processing power of such devices poses a hugechallenge.

3.RESULT

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. Longfei Wu [21] implemented the attacks on real phones, and demonstrate the feasibility and effectiveness of the attacks. Furthermore, they propose a lightweight defense scheme that caneffectively detect these attacks. 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 2: 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

4.DISCUSSION/ANALYSIS

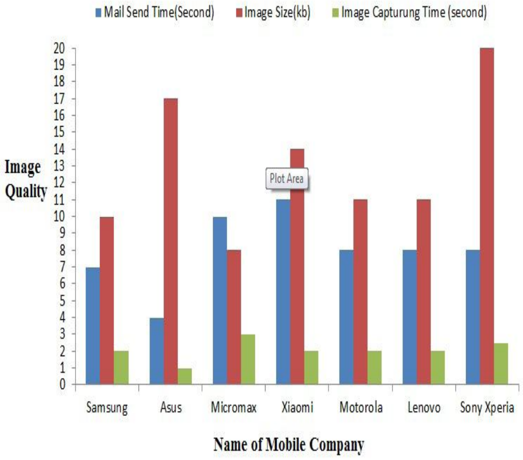
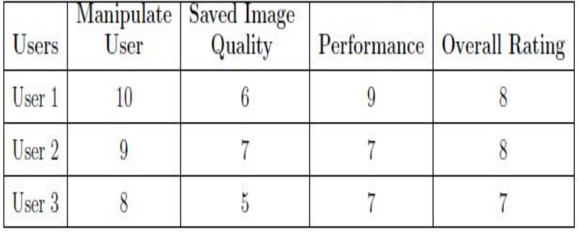


Figure. 3: Performance Analysis

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

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 3: 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

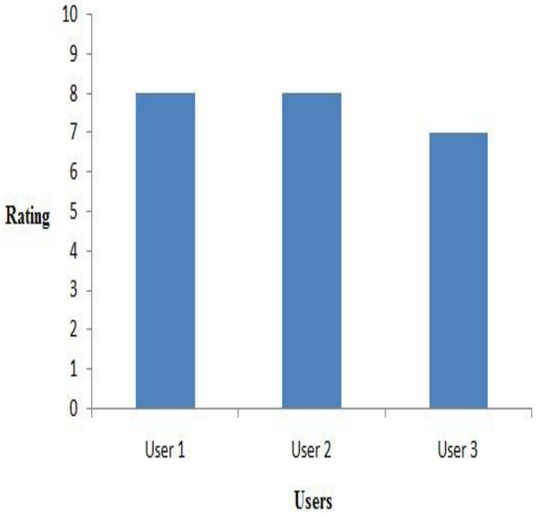


Figure. 4: Average Rating of Users

5.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.

References

[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.

[22]. A. Portnoy, “Pwn2Own 2010,” 2010,http://dvlabs. tippingpoint.com/blog/2010/02/15/pwn2own-2010.

[23]. M. Keith, “Android 2.0-2.1 Reverse Shell Exploit,” 2010, http://www.exploit-db.com/exploits/15423/.

[24]. R.-P. Weinmann, “All Your Baseband Are Belong To Us,” hack.lu, 2010, http://2010.hack.lu/archive/2010/ Weinmann-All-Your-Baseband-Are-Belong-To-Us-slides.pdf.

[25]. A. Greenberg, “Google pulls app that revealed Android flaw issues x,” 2010, http://news.cnet.com/8301-27080 3-20022545-245.html.

[26]. P. Zheng and L. M. Ni, “The Rise of the Smart Phone,”IEEE Distributed Systems Online, vol. 7, no. 3, 2006.

[27]. S. C. Guthery and M. J. Cronin, Developing MMS Applications- Multimedia Messaging Services for WirelessNetworks. McGraw-Hill Professional, Jun. 2003.