Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2016, 3(3): 26-29

Research Article ISSN: 2394 - 658X

Analysis on Camera Attacks and their Defenses on Android Smartphones

Supriya Deshpande and SC Dharmadhikari

Department of Information Technology, Pune Institute of Computer Technology, Pune, India
supriya.deshpande36@gmail.com

ABSTRACT

All smart phones have features like camera and touch screen, these features may lead to different types of attacks on smart phones. Modern smart phone platforms let users customize their device via third-party applications found on "app stores" or traditional websites. Application originality is a problem so users are constantly at risk of installing malicious apps that stealthily take away personal data or gain root access to devices. This paper reviews new security threats that occur frequently for mobile. It also shows novel user interface attacks on Android-based cell phones focusing on showcasing the conceivable alleviation strategies for such attacks. This Paper also discusses various attacks on different computer components like browser and ad libraries, such as UI Readdressing attack and Sidewinder attack.

Keywords: Camera Based Attacks, Sidewinder attack, UI Readdressing attack

INTRODUCTION

Mobile phones are becoming important part of our day to day life specially the android based smart phones, since they are involved in playing an important role with friends and family, doing business, accessing the internet and other activities. The small size of android devices, attached with people's careless usage, increases the chances of malicious software injection onto smart phones. They can be compromised in three respects: confidentiality, integrity, and availability [1-4]. Various types of camera-based applications are seen in Android app markets (photography, barcode readers, social networking, etc.). Spy camera apps have also become quite popular. As for Google Play, 100 spy camera apps are available, which allow phone users to take pictures or record videos of other people without their permission that is compromising the privacy of the users. Although little malware has been found in Google Play, both Android apps and the Android system itself contain vulnerabilities. Aggressive ad libraries also leak the user's private information. By leveraging all these vulnerabilities, an attacker can conduct more targeted attacks, which we call Sidewinder Targeted Attacks [5]. As, all the smart phone uses the applications from the market, it is possible that smart phones fall prey to attacks through malicious applications.

The organization of the paper includes threats to mobile devices &various types of attacks on smart phones discussion in Literature Review. Various types of analysis performed on the android mobile phones are discussed in Conceptual Analysis part of the paper. Next part is the countermeasures suggested against the types of attacks along with the conclusion of the paper.

LITERATURE SURVEY

The Survey carried out by MacAfee showed that the Android mobile operating system solidified its lead as the primary target for new mobile malware. The amount of malware targeted at Android devices jumped nearly 37 percent [6]. There is very less difference between PCs, Laptops, Note Pads & Smart phones as all these are connected technologies. Various services like Social networking & gaming provided by smart phones with the help of applications, these are exposed to gain confidentiality [7]. Sidewinder Targeted Attacks use basic ad libraries to infect android phones. They use non android services to target a machine to infect it which is an android Smartphone. Intensity of this attack is high because no user thinks that a non android service may infect an android phone [5]. UI Redressing attacks mostly target the browsers in the desktop as well as mobiles. There are ways in which attacks can be counter measured and their details are discussed further. Various Types of Attacks and Threats are discussed in upcoming section.

Mobile Device Threats

A threat is an expression to do harm to someone or something. In our scenario we interpret threat as something that causes the normal functioning of the mobile device either to malfunction or to stop functioning**.** There are different Types of threats present in the market today. The Risk factor a mobile phone has is due to presence of threats. Some of them can be summarized as follows:

- Interception of Communications: Man in middle attacks comes under this category. When communication between two Computers is interpreted is called as the man-in-middle attack [3].
- Loss, Theft or Seizure: When a Smartphone is used by unauthorized person the security gets compromised.
- Location Logging and Tracking: Mobile phones can be easily tracked by service providers.
- Bugging: It is possible on some mobile phone brands to call and answer the phone without causing it to ring or react in any overt way. This presents a challenging risk.
- Targeted Data Acquisition: Bluetooth slurping- It takes place when Bluetooth is enabled [4].
- Other Threats: Spam, Viruses, Malware, etc.

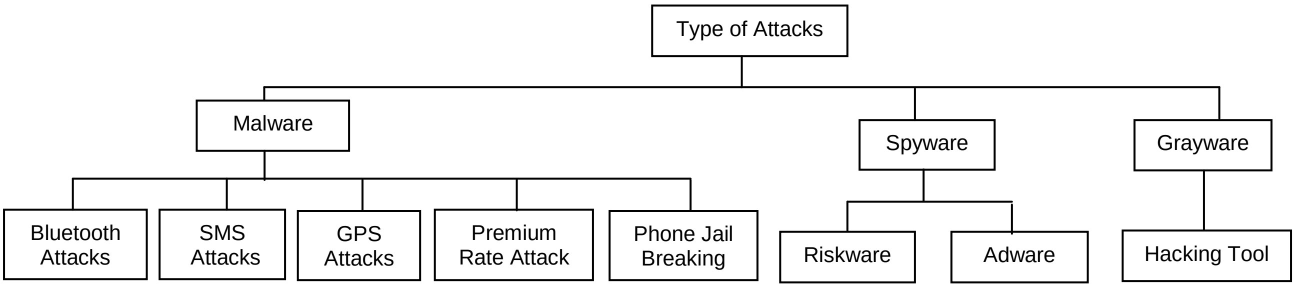

Fig. 1 Types of Attacks

Types of Attacks

Three main categories of attacks could be listed as- malware attacks, gray ware attacks and spyware attacks described in following Table. Hierarchical structure of various attacks is shown in Fig. 1. Various Types of Attacks can be described in the Table -1.

Table -1 Description of Attacks

Type of Attack		**Description of Attack**	**Examples**
	1. Bluetooth Attacks	Bluetooth attack sat taker can pullout contacts or SMS messages, steals prey's data from their devices and can track user's mobile location [5].	Bluejacking, Bluesnarfing
	2. SMS Attacks	SMS attacks; attacker can advertise and spread phishing links. SMS messages can also be used by attackers to exploit vulnerabilities [2].	SMS Fuzzing, Silent DoS SMS Attack.
Malware	**3. GPS/Location Attacks**	User's location and movement can be retrieved with global positioning system (GPS) hardware and then information can be sold to other companies involved in advertising [2].	GPS Spoofing attack
	4. Phone Jail-Breaking	In jail-breaking, security implication scan be removed of operating system. It allows OS to install unspecified applications. [2].	YiSpecter malware *attack*
	5. Premium Rate Attacks	Premium rate SMS messages could go unnoticed until attacker faces thousands of Rupees of bill. They do not need permissions to send SMS on premium rated numbers [2].	Attack on premium rate numbers.
Spyware	**1.Adware**	Displays advertisements and gathers data, such as user web surfing preferences, through a web browser [24].	SpyFalcon
	2. Riskware	The applications that can be modified for another purpose and used against the computer user or owner [24].	VNC (Antivirus)
Grayware	**Hacking Tools**	Helps hackers gain unauthorized access to computers [24].	NMap, Nessus

CONCEPTUAL ANALYSIS

Analysis is the investigation of a particular thing or a concept. In our scenario we discuss the static, dynamic and permission based analysis of android smart phones that can be detailed as follows. There is a comparative analysis of various parameters of attacks in form of a table -2.

Static Analysis

Static analysis scrutinizes copied app by inspecting its software properties and source code. However, complication and encryption techniques embedded in software makes static analysis difficult. Static analysis is further categorized into two categories- signature-based detection and behaviour-based detection traditionally used by anti-viruses. Framework for detection and monitoring of energy greedy threats by building power consumption from the collected samples is one method of analysis, after generating power signatures; data analyzer compares them with signatures present in a database [7].

Dynamic Analysis

Dynamic analysis involves execution of application in remote location to track its execution behaviour. In contrast to static analysis, dynamic analysis enables to disclose natural behaviour of malware as executed code is analyzed, therefore immune to confusion attempts. By collecting 350 apps from the Amazon Android Market, results found that about 82 applications leak private data. Apps-playground framework for automatic dynamic analysis of android applications. Designed approach is able to analyze malicious applications in addition to applications leaking private data from smart-phones without the user's consent[10].Automatic analysis code integrates the detection, exploration and disguise techniques to explore android applications effectively. Detection techniques detect the malicious functionality while app is being executed. Automatic exploration techniques are helpful for code coverage of applications by simulating events such as location changes and received SMS so that all application code is covered. Another type is Fuzzy testing and intelligent black box execution testing that can be used for automatic exploration of android applications. Disguise techniques create realistic environment by providing data such as International mobile equipment identity (IMEI), contacts, SMS, GPS coordinates etc.

Permission-Based Analysis

Listed permissions in manifest.xml help to detect applications malicious behaviour [2]. These permissions have the ability to limit application behaviour by controlling over privacy and reducing bugs and vulnerabilities. Few controls tools are "Architecture for automatic downloading of android applications from the android market"&"Droid Ranger for systematic study on overall health of both official and unofficial Android Markets with the focus on the detection of malicious apps. Droid Ranger leverages a crawler for collection of apps from the Android Market and saved into local repository". Features extracted from collected apps include requested permissions and author information. Two different detection engines are used for detection of known and unknown malwares. First detection engine is permission-based behavioural foot-printing scheme able to distil apps requiring dangerous permissions such as SEND_SMS and RECEIVE_ SMS PERMISSIONS.

Comparison-Based Analysis

It compares various parameters of Attacks such as the work done by the attack on the object of attack along with the intensity of damage caused due to that attack**.**

Table -2 Comparing Parameters of Attacks

Parameters	UI Redressing Attack [10]	Side-winder attack [5]	Camera-based Attacks [8]
Work done	Discussing which UI redressing attacks can be transferred from desktop- to mobile- browser field.	Using non-android service to get control of android services.	A control to defend against camera based attacks.
Contribution	demonstration of a browser less tap-jacking attack.	Way of attack by non-based services.	Keeps scanning through the memory for checking camera access.
Object Of Attack	Browser	Ad libraries	Camera
Type of Attack that does not work on android phones	• Cursor jacking • Cookie jacking • Double click jacking • Pop up blocker bypass	Ad libraries using HTTPS with proper SSL certificate.	-
Countermeasures	• Android touch filter • Tap jacking Security Layer	• Backporting of new release of security patches. • Training to programmers for awareness of security.	• Check Permissions. • Active Camera App Scanning.
Damage caused	Unauthorized home screen navigation.	Sensitive information disclosure. Unauthorized root access.	Real time audio and video disclosure.
Intensity Of Damage	Low(Because it can be detected by user)	High (Because of complete root access)	Medium (because of real time)

COUNTER MEASURE

In this section, we discuss possible countermeasures that can protect Android phones against these spy camera attacks. In an Android system, API or log file is not available for a user to check the usage of a camera device [15]. 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 [19].

Tap jacking Security Layer (TSL) is another approach which is developed to restrict Camera Based Attacks. In this approach, TSL opens automatically once a user fires an application it is crucially important that it is always in the background and remains opened until the application in its forefront gets closed. Further, a touch gesture on the TSL will be blocked; this assures that no touch gesture on part of a victim will be unintentionally forwarded to another application. Therefore, classic click jacking-related browser less attack scenarios can no longer be carried out [10].

CONCLUSION

Currently more than a million Android devices, activated Android has very few restrictions for developer, increases the security risk for end users. In this paper we have reviewed security issues in the Android based Smartphone. The integration of technologies into an application certification process requires overcoming logistical and technical challenges. Android provides more security than other mobile phone platforms.

Moreover, 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. This paper discusses Various Threats, Attacks, their countermeasures and the different parameters that affect the android smart phones. We propose to find out an innovative prevention method for all the types of attacks discussed in the paper. We also suggest finding out different ways to countermeasure these attacks if at all it could happen after applying the preventive measures to android Smartphone's.

REFERENCES

[1] Google bets on Android Future, *http,// news.bbc.co.uk/2/hi/technology/7266201.stm*, **2008**.

[2] D Stites and A Tadimla, A Survey of Mobile Device Security, Threats, Vulnerabilities and Defences, *http//afewguyscoding.com/2011/12/survey-mobile-device-security-threats vulnerabilities-defences*, **2011**.

[3] W Enck, P Gilbert, BG Chun, LP Cox, J Jung, P McDaniel, AP Sheth and Taint Droid, An Information on Tracking System for Real Time Privacy Monitoring on Smart-Phones, *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation*, USENIX Association Berkeley, CA,USA, **2010**, 1-6.

[4] T Blasing, L Batyuk, AD Schimdt, SH Camtepe and S Albayrak, An Android Application Sandbox System for Suspicious Software Detection, *Malicious and Unwanted Software (Malware)*, **2010** 55 – 62.

[5] *https//www2.fireeye.com/WBNR-14Q4SidewinderAndroid.html*, **2015**.

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

[7] V Rastogi, Y Chen and W Enck, Apps Playground, Automatic Security Analysis of Smartphone Applications, *Proceedings of the Third ACM Conference on Data and Application Security and Privacy*, ACM, New York, **2013**, 209-220.

[8] Henry B Wolfe, The Insecurity of Mobile Phones, Proceedings of Informing Science & InformationTechnologyEducat ion Conference, **2010**, 119-131.

[9] AD Schmidt, JH Clausen, SH Camtepe and S Albayrak, Detecting Symbian OS Malware through Static Function Call Analysis, *Proceedings of the 4th IEEE International Conference on Malicious and Unwanted Software*, **2009**, 15-22.

[10] *http//docs.trendmicro.com/all/ent/imsva/v8.2/enus/imsva_8.2_olh/imsx_ag_va/imsx_ch_01/about_spyware_grayware.htm*, **2015**.

[11] H Kim, J Smith and KG Shin, Detecting Energy-Greedy Anomalies and Mobile Malware Variants, *Proceeding of the 6th International Conference on Mobile Systems, Applications and Services*, ACM, New York, **2008**, 239-252.

[12] A Bose, X Hu, KG Shin and T Park, Behavioural Detection of Malware on Mobile Handsets, *Proceeding of the 6th International Conference on Mobile Systems, Applications and Services*, ACM, New York, **2008**, 225-238.

[13] L Min and Q Cao, Runtime-based Behaviour Dynamic Analysis System for Android Malware Detection, *Advanced Materials Research*, **2012**, 2220-2225.

[14] DJ Wu, CH Mao, TE Wei, HM Lee, KP Wu and Droid Mat, Android Malware Detection through Manifest and API Calls Tracing, *IEEE Seventh Asia Joint Conference on Information Security*, Tokyo, **2012**, 62-69.

[15] R Jhonson, Z Wang, C Gagnon and A Stavrou, Analysis of Android Applications, *IEEE Sixth International Conference on Software Security and Reliability Companion*, **2012**, 45- 46.

[16] Y Zhou, Z Wang, W Zhou, X Jiang and Hey, *Get of My Market, Detecting Malicious Apps in Official and Alternative Android Markets*, International Journal of Distributed and Parallel Systems, **2014**, 5(4), 1-13.

[17] L Batyuk, M Herpich, SA Camtepe, K Raddatz, AD Schmidt and S Albayrak, Using Static Analysis for Automatic Assessment and Mitigation of Unwanted and Malicious Activities within Android Applications, IEEE 6th International Conference on Malicious and Unwanted Software, **2011**, 66-72.

[18] M Ongtang, SE McLaughlin, W Enck and PD McDaniel, Semantically Rich Application-Centric Security in Android, Proceedings of the 25th Annual Computer Security Application Conference, **2009**, 340-349.

[19] L Xie, X Zhang, JP Siefert and S Zhu, pBMDS a Behaviour-based Malware Detection System for Cell phone Devices, *Proceedings of the Third ACM Conference on Wireless Network Security*, Hoboken, USA, **2010**, 37-48.

[20] R Schlegel , Kehuan Zhang, Xiaoyong Zhou, Mehool Intwala, Apu Kapadia and Xiao Feng Wang, Sound comber, A Stealthy and Context-Aware Sound Trojan for Smartphone's, *NDSS*, **2011**, 17–33.

[21] N Xu, Weijia Jia, Yisha Luo, Fan Zhang, Dong Xuan and Jin Teng, Stealthy Video Capturer, A New Video Based Spyware in 3G Smartphone's, *Proceedings of the* 2nd ACM *Conference on Wireless Network Security*, **2009**, 69–78.

[22] F Maggi, S Gasparini and G Borachhi, A Fast Eavesdropping Attack against Touch screens, *7th International Conference on Information, Assurance and Security*, **2011**, 320–325.

[23] R Raguram, Andrew M White, Dibenyendu Goswami, Fabian Monrose and Jan-Michael Frahm, Automatic Reconstruction of Typed Input from Compromising Reflections, *Proceedings of the 18th ACM Conference on Computer and Communication Security*, **2011**, 527– 536.

[24] Longfei Wu and Xiaojiang Du, Security Threats to Mobile Multimedia Applications, Camera-Based Attacks on Mobile Phones, Security in Wireless Multimedia Communications, *IEEE Communications Magazine*, **2014**, 80-87.