Volume 5, Issue 12, December 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Security for Mobile Device: Threats and Vulnerability

Khyati Rami*
Ph.D Research Scholar, Mewar University,
India

Dr. Vinod Desai
Dept of Comp. Science, Chikli, Navsari,
India

Abstract*— Nowadays, Mobile devices are obligatory for everyone's daily routine work. In recent years, the availability of these ubiquitous and mobile services has significantly increased due to the different form of connectivity provided by mobile devices, such as GSM, GPRS, Bluetooth and Wi-Fi[1]. Everywhere applications support a wide array of social, financial, and enterprise services for any user with a cellular data plan. In the same trend, the number and typologies of vulnerabilities exploiting these services and communication channels have increased as well. Therefore, Smartphone may now represent an ideal target for malware writers. As the number of vulnerabilities and, hence, of attacks increase, there has been a corresponding rise of security solutions proposed by researchers. In this paper we aim to provide a structured and comprehensive overview of the research on mobile security and surveys the state of the art on threats, vulnerabilities over the period 2004-2014, by focusing on high-level attacks, such those to user applications.

***Keywords*— Security, malware, threats, vulnerability.**

I. INTRODUCTION

The rapid growth of smartphones has direct to a rebirth for mobile services. The applications running on smartphones support vast new markets in communication, entertainment, and commerce. Hardware, access, and software supporting such applications are now widely available and often surprisingly inexpensive, e.g., Apple's App Store [1], Android's Market [2], and BlackBerry App World [3]. As a result, smartphone systems have become pervasive. Application markets such as Apple's App Store and Google's Android Market provide top and tick access to hundreds of thousands of paid and free applications. Markets streamline software marketing, installation, and update—therein creating low barriers to convey applications to market, and even lower barriers for users to obtain and use them.

2014 saw an astounding 75% increase in Android mobile malware encounter rates in the United States compared to 2013 (a 4% vs. 7% encounter rate), an increase driven largely by prolific mobile threats that hold victims' mobile devices hostage in exchange for payment, using a variety of coercion schemes6.[4].Even if global sales of smartphones will pass 420 million devices in 2011 (according to a recent report by IMS research [5]), the number of mobile malware is still small compared to that of PC malware [6]. Nonetheless, we can expect malware for smartphones to evolve in the same trend as malware for PCs: hence, in the next incoming years we will face a growing number of malware. As an example, as more users download and install third-party applications for smartphones, the chances of installing malicious programs increases as well. Furthermore, since users increasingly exploit smartphones for sensitive transactions, such as online shopping and banking, there are likely to be more threats designed to generate profits for the attackers. As a proof that attackers are starting to focus their efforts on mobile platforms, there has been a sharp rise in the number of reported new mobile OS vulnerabilities [7]:from 115 in 2009 to 163 in 2010 (42% more vulnerabilities) Section II we present the literature review from different researcher. They describes different types of mobile malware, along with some predictions on future threats, and outlines the differences among security solutions for smartphones and traditional PCs. Section III discusses current threats targeting smartphones:firstly, it analyzes the different methodologies to perform an attack in a mobile environment; then, it investigates how these methodologies can be exploited to reach different goals. In Sec. IV we present security solutions, focusing on those that exploit intrusion detection systems and trusted platform technologies

II. LITERATURE REVIEW

Mariantonietta La Polla[8] surveys the state of the art on threats, vulnerabilities and security solutions over the period 2004-2014, by focusing on high-level attacks, such those to user applications. We group existing approaches aimed at protecting mobile devices against these classes of attacks into different categories, based upon the detection principles, architectures, collected data and operating systems, specially focusing on IDS-based models and tools. With this categorization we aim to provide an easy and concise view of the underlying model adopted by each approach. Sujithra M.[9] focused on various threats and vulnerabilities that affect the mobile devices and also it discusses how biometrics can be a solution to the mobile devices ensuring security. These systems are proved highly confidential portable mobile based security systems which is much essential. Comparing various biometric traits such as fingerprint, face, gait, iris, signature and voice. Iris is considered as the most efficient biometric trait due to its reliability and accuracy.

III. MOBILE THREATS AND VULNERABILITIES

Security support is mandatory for any database system. For mobile database systems, security support is even more important to protect the users and devices as well as the database. In mobile communication, since wireless medium is available to all, the attackers can easily access the network and the database becomes more vulnerable for the user and the data in the mobile device.

Mobile threats

Mobile threat is defined as any malware that targets smart phones and PDA. Various security threats that can affect mobile devices are categorized as follows in Figure 1.

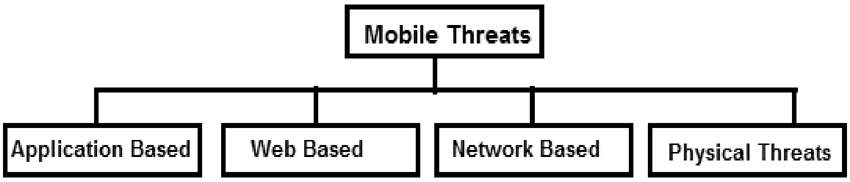

Fig.1 : Various Mobile Threats

□ Application-based threats
□ Web-based threats
□ Network-based threats
□ Physical threats

Application Based threats	**Malware**	**Software is designed to engage in malicious behavior on a device. Malware can also be used to steal personal information from a mobile device that could result in theft or financial fraud.**
	Spyware	Designed to collect or use data without knowledge or approval of user. Targeted data might be phone call history, text message, location, browser history, contact list, email and camera pictures.
	Privacy Threats	Caused by the applications that is not necessarily malicious , but gathers or uses more sensitive information than is necessary to perform their function or than a user is comfortable with.
	Vulnerable applications	It allows an attacker to access sensitive information, perform undesirable actions, stop a service from functioning correctly, and automatically download additional applications.
Web Based Threats	**Phishing Scams**	Use web pages or other user interfaces designed to trick a user into providing information such as account login information to a malicious for the user.
	Party Posing as a Legitimate service	Attackers often use email, text messages, Face book, and Twitter to send links to phishing sites
	Drive by Downloads	Automatically begins downloading an application when a user visits a web page.
	Browser Exploits	It can be launched via a web browser such as a Flash player, PDF reader, or image viewer.
Network-based threats	**Network Exploits**	Takes advantage of software flaws in the mobile operating system or other software that operates on local (e.g., Bluetooth, WI-Fi) or cellular (e.g., SMS, MMS) networks.
	Wi-Fi Sniffing	sending the data in the clear (not encrypted) so that it may be easily intercepted by anyone listening across an unsecured local wireless network.
	Mobile Network Services	Cellular services like SMS, MMS and voice calls can be used as attack vectors for mobile devices. It can be phishing attacks. The attacker gains sensitive information from the user by presenting

		itself as a trustworthy entity. Figure 2 represents the diverse usage of applications in mobile devices and their security level.
Physical Threats	**Lost or Stolen Devices**	The mobile device is valuable even the device is lost and can be re-sold on the black market.[10].
	Computing Resources	The increase in computing resources is setting the contemporary mobile devices into focus for malicious attacks with aim to covertly exploit the raw computing power in combination with broadband network access
	Internet Access	Prolonged connection to the Internet also increases the chances of a successful malicious attack.
	Bluetooth	Once the two devices are in range, the compromised device pairs with its target by using default Bluetooth passwords. When the connection is established, the compromised device sends malicious content.

Table 1: Comparison of mobile devices Threats

Threats	***Mobile units***	***Over the air***	***Wired hosts***
Physical Threats	theft, damage	physical disasters	physical disasters
Web-Based	problematic operation	interruptions, bad quality	-
Network –Based	denial of service, interference, covert channels, used by third parties	eavesdropping, denial of service, routing alterations	denial of service, faults in hardware and software
Application-Based	-	Overloading	Improper handling

Thus it is clearly discussed about the various threats, their issues with the mobile devices in this section. The next section discusses about the various vulnerabilities.

Mobile Vulnerabilities

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface. [11].Various vulnerabilities that can affect mobile devices are categorized as follows in Figure 3.

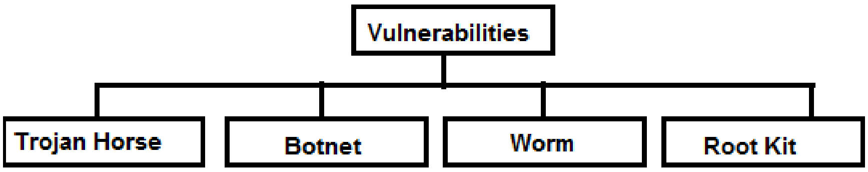

Fig 3 Mobile Device Vulnerabilities

Trojan Horse	**Trojan can be used to gather private information or to install other malicious applications like worms or botnets. In addition, Trojans can be used to commit phishing activities. For example, a false banking application could collect sensitive data from the user. Such applications can easily spread through unsupervised application stores or through social networks.**
Botnet	Botnet is a set of compromised devices which can be controlled and coordinated remotely. This attack strategy is used to utilize the computing power of compromised devices in order to commit various activities ranging from sending spam mail to committing Dos attacks.
Worm	Worm is a self-replicating malicious application designed to spread autonomously to uninfected systems. A more recent example of a worm type malware for mobile devices is Ikee.B which is used to steal financially sensitive data from jail broken iPhones.[12]
Rootkit	Rootkit is a malicious application which gained rights to run in a privileged mode. Such malicious applications usually mask their presence from the user by modifying standard operating system functionalities.

Name	Time	Type	Method of Infection	Effects	OS
Liberty Crack	2000	Trojan	Pretend to be a hack	Remove third-party software	Palm OS
Cabir	2004	Worm	Bluetooth connection and copies itself	Continuous scan of Bluetooth, drain phone's battery	Symbian OS
Dust	2004	Virus	File Infector	Infect all executables in root DIR	Windows Mobile
Brador	2004	Trojam	Copy itself in to the startup folder	Open a backdoor	Windows Mobile
Mosquitos	2004	Trojan	Embedded in a game	Send SMS to premium-rate numbers	Symbian OS
Skulls	2004	Trojan	Vulnerability in overwriting system files	DoS	Symbian OS
MetalGear	2005	Worm	Vulnerability in overwriting system files	Disable virus scanner	Symbian OS
CommWarrior	2005	Worm	Replicates via Bluetooth and MMS	MMS charging	Symbian OS
Doomboot	2005	Trojan horse	Doom 2 video game	Prevents booting and installs Cabir and CommWarrior	Symbian OS
Lasco	2005	Virus	File Infection	Add itself to install packages	Symbian OS
Locknut	2005	Trojan	Vulnerability in OS	Create entries for a new application	Symbian OS
Feakk	2005	Worm	SMS message	Send SMS to all contacts	Symbian OS
Cardblock	2005	Virus	Fake SIS application	Encrypt memory card with a random password	Symbian OS
CardTrap	2005	Cross-Platform Virus	Auto-start of removable storage	Copy Wukill on the phone	Symbian/Windows OS
Blankfont	2005	Trojan	Replace font files	Fonts not displayed	Symbian OS
Letum	2006	Worm	E-Mail spreading	Infect registry	Windows Mobile
Fontal	2006	Trojan	Vulnerability in overwriting system files	Copy to/from mobile/PC	Windows/Mobile OS
Mobler	2006	Cross-Platform Worm	Dropping Mechanisms	Disable antivirus and infect removable storage	Symbian/Windows OS
Redbrowser	2006	Trojan	Fake Browser	Send SMS continuously	OS-Independent (J2ME)
Wesber	2006	Trojan	Fake Browser	Send SMS to premium-rate numbers (Russia only)	OS-Independent (J2ME)
Acallno	2006	Spyware	Fake Commercial Software	Gather and send information about user's activities	Symbian OS
Lasco	2007	Worm	A worm that spreads over Bluetooth networks	Searching and infecting other phones	Symbian OS
Feak	2007	Worm	Proof-of-concept worm	Sending SMS to contact list with URL	Symbian OS
Flocker	2007	Trojan	It claims to be an ICQ application to trick the user	Sending SMS to a hard coded phone number	Symbian OS
Beselo	2008	Worm	Via MMS and Bluetooth	SMS charging	Symbian OS
InfoJack	2008	Trojan	Attach itself to installation packages	Disable security settings	Windows Mobile

Pmcryptic	2008	Worm	Memory card spreading	Dialing premium-rate numbers	Windows Mobile
Yxe	2009	Worm	SMS containing malicious URL	Send contact lists to external server	Symbian OS
Yxes	2009	Worm/Bootnet	SMS containing malicious URL	Send contact lists to external server	Symbian OS
Ikee	2009	Worm	Scanning a IP ranges and SSH	Alter wallpaper	iPhone
FlexiSpy	2009	Spyware	Fake Application	Tracking/log of device's usage	Symbian
Curse of Silence	2009	SMS Exploit	Vulnerabilities in e-mail parsing	Disable SMS functionalities	Symbian OS
ZeuS MitMo	2010	Worm	Fake SMS	Steal bank account information	Cross-platform
iSAM	2011	Multifarious malware	Scanning IP and connecting to SSH	Collect private information, send malicious SMS, DoS	Iphone

IV. EVOLUTION OF MOBILE MALWARE

Several papers discuss the evolution of mobile malware: for instance, [13] describes the evolution of malware on smartphones from 2004 to 2006. For an overview on the state of the art of mobiles viruses and worms up to 2006, see Hypponen [14]. In the period 2004-2008, the number of types of mobile malware has increased significantly: as of March 2008, F-Secure has categorized 401 distinct types of mobile malware worldwide, whereas McAfee has counted 457 kinds of mobile malware [15]. In the period 2004-2010, 517 families of mobile viruses, worms and Trojans have been categorized by F-Secure [16]. For a complete list of mobile malware in the period 2000-2008 see [17]; see [18] for mobile malware that spread from January 2009 to June 2011.The first virus (a Trojan) for mobile phones, developed for Palm devices [19], was discovered in 2000 by F-Secure [20]. In June 2004, the first worm that could spread through mobile phones with Symbian OS appeared: this worm, called Cabir [21], was only a prototype developed by the 29A Eastern European hacker group. Cabir is considered the first example of malicious code that can spread itself exploiting the networking technologies on mobile devices (in this case, Bluetooth) to infect other devices.

Recently, a growing number of viruses, worms, and Trojans that target smartphones have been discovered. As we have already pointed out, the reason of the growing number of mobile malware is due to the widespread use of smartphones. Furthermore, we have to consider that most of the smartphones lack any kind of security mechanisms and are not well prepared against new threats. Within the 2006-2013 periods, security issues exploiting several attack vectors have increased [21], and there has been a dramatic escalation of complex attacks targeting lower-level device functionality: early security threats have turned into sophisticated, profit-oriented, attacks driven by experienced criminals. A discussion of mobile malware, based on OSes and infection routes, is presented in Toyssy and Helenius [22] that describe and cluster mobile malware with respect to: the *OS*: Symbian, Palm OS, Linux, Windows Mobile; the *infection routes*: MMS, Bluetooth, IP connections via GPRS/EDGE/UMTS, WLAN, copying files, removable media. The authors propose some prevention solutions and countermeasures, by considering: the *users*, which have to be educated to utilize the device in a secure way; the *software developer*, which can develop security protection targeted at smartphone; the *network operator*, which can enhance the network infrastructure with mechanisms to avoid intrusions; the *phone manufacturers*, which should update the devices automatically so that for attackers it would be harder to exploit security holes; new *epidemiological models*, to forecast if an already detected virus can initiate an epidemic.

REFERENCES

[1] Apple Inc., "Apple App Store," http://www.apple.com/ iphone/appstore/, June 2009.

[2] Google Inc., "Android Market," http://www.android.com/market/, June 2009.

[3] Research In Motion Ltd., "Blackberry App World," http://na.blackberry.com/eng/services/appworld/, June 2009

[4] https://www.lookout.com/resources/reports/mobile-threat-report

[5] MS Research, "Global Smartphones Sales Will Top 420 Million Devices in 2011, Taking 28 Percent of all Handsets, According to IMS Research," July 2011. [Online]. Available: http://imsresearch.com/ press-release/Global Smartphones Sales Will Top 420 Million Devices in 2011 Taking 28 Percent of all Handsets According to IMS Research.

[6] Q. Yan, Y. Li, T. Li, and R. Deng, "Insights into Malware: Detection and Prevention on Mobile Phones," in *Security Technology*, D. ´Slzak, T.-h. Kim, W.-C. Fang, and K. P. Arnett, Eds. Springer Berlin Heidelberg, 2009, vol. 58, ch. 30, pp. 242–249.

[7] S. Coorporation, "Symantec Internet Security Threat Report Volume XVI," *Whitepaper*, vol. 16, Apr 2011.

[8] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra," A Survey on Security for Mobile Devices", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 1, FIRST QUARTER 2013.

[9] Sujithra M," Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism", International Journal of Computer Applications (0975 – 8887) Volume 56– No.14, October 2012.

[10] Mavridis I., Pangalos G “Security Issues in a Mobile Computing Paradigm”2012.

[11] Paul Ruggiero and Jon Foote “Cyber Threats to Mobile ”, Produced for US-CERT, a government organization, Carnegie Mellon University-US, 2011.

[12] http://www.rsasecurity.com/products/securid/Last accessed in January 2008.

[13] A. Gostev, “Mobile malware evolution: An overview,” *Kaspersky Labs Report on Mobile Viruses*, 2006.

[14] M. Hypponen, “Malware Goes Mobile,” *Scientific American*, vol. 295, no. 5, pp. 46–53, 2006.

[15] G. Lawton, “Is It Finally Time to Worry about Mobile Malware?” *Computer*, vol. 41, pp. 12–14, May 2008.

[16] M. Hypponen, “Mobile Security Review September 2010,” F-Secure Labs, HelsinkiFinland, Tech. Rep., September 2010.

[17] A.-D. Schmidt and S. Albayrak, “Malicious Software for Smartphone s,” Technische Universit¨at Berlin - DAI-Labor, Tech. Rep. TUBDAI 02/08-01, February 2008, http://www.dai-labor.de.

[18] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, “Survey of Mobile Malware in the Wild,” 2011. [Online]. Available: http://www.eecs.berkeley.edu/ ∼afelt/malware.html

[19] N. Leavitt, “Mobile Phones: The Next Frontier for Hackers?” *Computer,*vol. 38, pp. 20–23, April 2005.

[20] F-Secure, “Liberty (Palm),” Aug 2000. [Online]. Available: http: //www.f-secure.com/v-descs/lib palm.shtml

[21] “Bluetooth-Worm:SymbOS/Cabir,” Jun 2004. [Online]. Available: http://www.f-secure.com/v-descs/ cabir.shtml

[22] McAfee Labs, “Mobile Security Report 2009,” 2009. [Online]. Available: http://www.mcafee. com/us/resources/reports/ rp-mobile-security-2009.pdf

[23] S. T¨oyssy and M. Helenius, “About malicious software in smartphones,”*Journal in Computer Virology*, vol. 2, no. 2, pp. 109–119,2006.