ISSN:0975-9646

Quantifying Response Mechanism for Effectiveness of Hybrid Virus Propagation through BT and SMS Channel-A Review

Harsha Kubade[#1], Deepali Khatwar[#2]

[#1,2]*Computer Science & Technology, RTMNU*
Agnihotri college of engineering,nagthana,Wardha

***Abstract*—A sharply increasing development of mobile network, mobile phones are increasingly becoming the target of Malware. It is nothing but a program which is specifically designed to infect the mobile phone it may be a virus or worm or malware. The potential effects of malware propagation on user and mobile phone providers are severe, including identity and information theft, permanently disabling devices and excessive fees to user or loss of revenue for mobile phone providers. In this paper we are going to review on the qualifying response mechanism effectiveness of hybrid virus propagation through Bluetooth and SMS channel.**

***Keywords*— virus propagation, Bluetooth (BT) and SMS Channel, restraining virus propagation**

I. Introduction

With the growing popularity of mobile devices such as smart phones, handsets and PDAs, the mobile Internet is now a key component of many enterprise and social networks. It is also quickly becoming a major channel for distributing digital media content such as music, video and advertising, and for enabling m-commerce activities. With the proliferation of mobile devices, there is, however, an increasing threat from mobile malware (i.e., viruses, worms, spams and other malicious software), that targets these devices, using traditional social-engineering techniques such as email and file-sharing, as well as vectors unique to mobile devices such as Bluetooth and SMS (Short Messaging Service) messages. Mobile viruses targeting cellular phones, PDAs and Bluetooth-enabled devices have already started to appear [1], [2]. Studying such viruses—their capabilities, infection models and vulnerabilities they typically exploit — is therefore an important area of research. The mobile viruses discovered so far have caused little damage as they require explicit user interaction for installation and activation. However, potential harm from future malicious agents can be severer in the form of handset downtime, service disruption due to Denial-of-Service (DoS) attacks, physical damage to device hardware, and theft of sensitive data on the device. Similar to email viruses, these agents may also target SMS/MMS services for distributing spam and phishing messages. There are several factors that make mobile devices particularly vulnerable to future mobile viruses. First, recognizing customer demand for data-rich cellular services, carriers around the world have been deploying 3G (third generation) cellular systems at a rapid pace. Currently, there are more than 130 3G networks [3] (WCDMA and CDMA2000 1X EV-DO) worldwide. Many of these networks offer real-world data rates of 1.4 Mbps and 128 Kbps for download and upload, respectively. The download data rates are expected to raise to 7.3 Mbps in early 2008, 10.2 Mbps in 2009 and nearly 20-27 Mbps in currently. At these rates, mobile users will be able to run many feature-rich applications on their mobile devices that traditionally require access to a high-speed enterprise network. The processing power (CPU speed and storage capacity) of handheld devices is also increasing rapidly. Many smart phones [4] already contain a full-fledged OS like Symbian, Windows Mobile, Android Mobile and Palm OS, allowing users to download a wide variety of applications. Almost all of these OSs support services such as email, SMS/MMS, and application development in C++ and Java. Consequently, the malware writers increasingly find it easier to generate device-generic but vulnerability-specific malware for mobile devices. As a result, the current count of known mobile malware stands at 100, up from only 10 in previous years combined.

II. Literature Review

Malware is a malicious piece of software which is designed to damage the computer system & interrupt its typical working. Fundamentally, malware is a short form of Malicious Software. Mobile malware is a malicious software aiming mobile phones instead of traditional computer system. With the evolution of mobile phones, mobile malware started its evolution too. When propagation medium is taken into account, mobile viruses are of three types: Bluetooth-based virus, SMS-based virus, and FM RDS based virus [5], [6], [7], [8], [9]. A BT-based virus propagates through Bluetooth & Wi-Fi which has regional impact [5], [7], [8]. On the contrary, SMS-based virus follows long-range spreading pattern & can be propagated through SMS & MMS [5], [6], [8]. FM RDS based virus uses RDS channel of mobile radio transmitter for virus propagation [9]. Operational behavior of user & mobility of a device plays a substantial role in virus propagation. There are several methods of malware detection viz. static method, dynamic method, cloud-based detection method, battery life monitoring method, application permission analysis, enforcing hardware sandbox etc. [10], [11], [12], [13], [14], [15], [16], [17], [18]. Along with the study of virus propagation & detection mechanisms, methods of restraining virus propagation are also vital. A number of proactive & reactive malware control strategies are given in [5], [10].

III. Mobile Malware Evalution

Although, first mobile malware, 'Liberty Crack', was developed in year 2000, mobile malware evolved rapidly during years 2004 to 2006 [19]. Enormous varieties of malicious programs targeting mobile devices were evolved during this time period & are evolving till date. These programs were alike the malware that targeted traditional computer system: viruses, worms, and Trojans, the latter including spyware, backdoors, and adware. At the end of 2012, there were 46,445 modifications in mobile malware. However, by the end of June 2013, Kaspersky Lab had added an aggregate total of 100,386 mobile malware modifications to its system [20]. This shows that there is a dramatic increase in mobile malware. Arrival of 'Cabir', the second most mobile malware (worm) developed in 2004 for Symbian OS, dyedin-the-wool the basic rule of computer virus evolution. Three conditions are needed to be fulfilled for malicious programs to target any particular operating system or platform:

The platform must be popular: During evolution of 'Cabir', Symbian was the most popular platform for smart phones. However, nowadays it is Android, that is most targeted by attackers. These days' malware authors continue to ponder on the Android platform as it holds 79.3% of the total market share in mobile phones and tablet devices.

There must be a well-documented development tools for the application: Nowadays every mobile operating system developers provides a software development kit & precise documentation which helps in easy application development.

The presence of vulnerabilities or coding errors: During the evolution of 'Cabir', Symbian had number of loopholes which was the reason for malware intrusion. In this day and age, same thing is applicable for Android [21]. The pie chart illustrates the operating system wise distribution of mobile platform [22]:

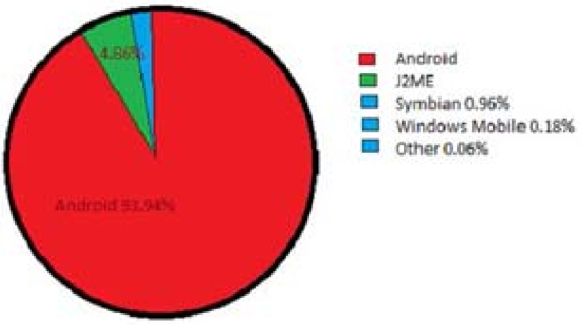

Fig. 1 Operating System wise distribution

IV. Mobile Malware Propgation

There are 3 communication channels through which malware can propagate. They are: SMS / MMS, Bluetooth / Wi-Fi, and FM Radio broadcasts.

A. *SMS/MMS Viruses*

Viruses that use SMS as a communication media can send copies of themselves to all phones that are recorded in victim's address book. Virus can be spread by means of forwarding photos, videos, and short text messages, etc. For propagation, a long range spreading pattern is followed which is analogous to the spreading of computer viruses like worm propagation in e-mail networks [6]. For accurate study of SMS-based virus propagation, one needs to consider certain operational patterns, such as whether or not users open a virus attachment. Hence, the operational behavior of users plays a vital role in SMS-based virus propagation [8].

Process: If a phone is infected with SMS based virus, the virus regularly sends its copies to other phones whose contact number is found on the address book of the infected phone. After receiving such distrustful message from others, user may open or delete it as per his alertness. If user opens the message, he is infected. But, if a phone is immunized with antivirus, it will not send out viruses even if user opens an infected message. Therefore, the security awareness of mobile users plays a key role in SMS-based virus propagation. Same process is applicable for MMS-based virus propagation whereas MMS carries sophisticated payload than that of SMS. It can carry videos, audios in addition to the simple text & picture payload of SMS.

B. *Bluetooth/ WiFi*

Viruses that use Bluetooth as a communication channel are local-contact driven viruses since they infect other phones within its short radio range. BT-based virus infects individuals that are homogeneous to sender, and each of them has an equal probability of contact with others [7]. Mobility characteristics of user such as whether or not a user moves at a given hour, probability to return to visited places at the next time, traveling distances of a user at the next time etc. are need to be considered [8].

Process: Unlike SMS based viruses, if a phone is infected by a BT-based virus, it spontaneously & atomically searches another phone through available Bluetooth services. Within a range of sender mobile device, a BT-based virus is replicated. For that reason, users' mobility patterns and contact frequency among mobile phones play crucial roles in BT-based virus propagation. Same process is followed for Wi-Fi where Wi-Fi is able to carry high payload in large range than that of BT.

C. *FM-RDS*

Several existing electronic devices do not support data connectivity facility but include an FM radio receiver. Such devices are low-end mobile phones, media players, vehicular audio systems etc. FM provides FM radio data system (RDS), a low-rate digital broadcast channel. It is proposed for delivering simple information about the station and current program, but it can also be used with other broad range of new applications and to enhance existing ones as well [9]. Process: The attacker can attack in two different ways. The first way is to create a seemingly benign app and upload it to popular app stores. Once the user downloads & installs the app, it will contact update server & update its functionality. This newly added malicious functionality decodes and assembles the payload. At the end, the assembled payload is executed by the Trojan app to uplift privileges of attacked device & use it for malicious purpose. Another way is, the attacker obtains a privilege escalation exploit for the desired target. As RDS protocol has a limited bandwidth, we need to packetize the exploit. Packetization is basically to break up a multi-kilobyte binary payload into several smaller Base64 encoded packets. Sequence numbers are attached for proper reception of data at receiver side. The received exploit is executed. In this way the device is infected with malware [9].

V. Mobile Malware Detection

Once the malware is propagated, malware detection is needed to be carried out. In this section, various mobile malware detection techniques are explained.

A. *Static Analysis Technique*

As the name indicates, static analysis is to evaluate the application without execution [10], [11]. It is an economical as well as fast approach to detect any malevolent characteristics in an application without executing it. Static analysis can be used to cover static pre-checks that are performed before the application gets an entry to online application markets. Such application markets are available for most major Smartphone platforms e.g. 'Play store' for Android, 'Store' for windows operating system. These extended pre-checks enhance the malware detection probabilities and therefore further spreading of malware in the online application stores can be banned. In static analysis, the application is investigated for apparent security threats like memory corruption flaws, bad code segment etc. [10], [12].

Process: If the source code of application is available, static analysis tools can be directly used for further examination of code. But if the source code of the application is not available then executable app is converted back to its source code. This process is known as disassembling. Once the application is disassembled, feature extraction is done. Feature extraction is nothing but observing certain parameters viz. System calls, data flow, control flow etc. Depending on the observations, anomaly is detected. In this way, application is categorized as either benign or malicious. Ded, a Dalvik decompiler, is used to dissemble the code. It generates Java source code from .apk image. Feature extraction is done by using Fortify SCA. It is a static code analysis suite that provides four types of analysis; control flow analysis, data flow analysis, structural analysis, and semantic analysis. It is used to evaluate the recovered source code & categorize the application as either benign or malicious.

B. *Dynamic Analysis Technique*

Dynamic analysis comprises of analyzing the actions performed by an application while it is being executed. In dynamic analysis, the mobile application is executed in an isolated environment such as virtual machine or emulator, and the dynamic behavior of the application is monitored [10], [11], [13]. There are various methodologies to perform dynamic analysis viz. function call monitoring, function parameter analysis, Information flow tracking, instruction trace etc. [13]. Process: Dynamic analysis is usually more complex than the static analysis. In this, the application is installed in the standard Emulator. After installation it will be executed for a specific time and penetrated with random user inputs. Using various methodologies mentioned in [13], the application is examined. On the runtime behavior, the application is either classified as benign or malicious. Example: Fig. 3 shows Android Application Sandbox (AASandbox) [14], the dynamic malware detection technique proposed by Blasing et al. for Android. It is a two-step analysis process comprising of both static & dynamic analysis. The AASandbox first implements a static pre-check, followed by a comprehensive dynamic analysis. In static analysis, the application image binary is disassembled. Now the disassembled code is used for feature extraction & to search for any distrustful patterns. After static analysis, dynamic analysis is performed. In dynamic analysis, the binary is installed and executed in an AASandbox. 'Android Monkey' is used to generate runtime inputs. System calls are logged & log files are generated. This generated log file will be then summarized and condensed to a mathematical vector for better analysis. In this way, application is classified as either benign or malicious.

VI. Conclusions

This paper reviews the detail study of mobile malware. Rapid growth in smart phone development resulted in evolution of mobile malware. In this paper, first of all we have discussed evolution & current scenario of mobile malware. Then propagation & detection methods of mobile malware are discussed.

VII. Future Scope

In Future work we are going to develop application to increase the effectiveness of the reducing the propagation of mobile phone viruses by increasing time delay, work proposes a novel analytical model to efficiently analyze the accuracy for spreading the hybrid malware that targets multimedia messaging service (MMS)/ (SMS) and BT. And extend model to incorporate additional characteristics of human mobility and operations. In particular future computational model will consider the dynamic changes of users' behaviors in the course of mobile virus propagation.

References

[1] Symantec,"Symbos.mabirwormdescription," http://securityresponse.symantec.com/avcenter/venc/data/symbos.mabir.html, April 2005

[2] "Symbos.commwarrior worm description," http://securityresponse.symantec.com/avcenter/venc/data/symbos.commwarrior.a.html, October 2005

[3] In-Stat, "3g cellular deployment report," http://www.instat.com, March 2006.

[4] "Worldwidesmartphonemarket," http://www.canalys.com/pr/2005/r2005102.htm, 2005.

[5] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation", IEEE transactions on mobile computing, Vol. 12, No. 3, March 2013.

[6]] C. Gao, j. Liu, and N. Zhong, "Network immunization and virus propagation in Email networks: experimental evaluation and

analysis," Knowledge and information systems, vol. 27, no. 2, pp. 253-279, 2011.

[7] G. Yan and S. Eidenbenz, "Modeling propagation dynamics of Bluetooth worms (extended version)," IEEE transactions on Mobile Computing, Vol. 8, No. 3, pp. 353-368, March 2009.

[8] M. C. Gonzalez, C. A. Hidalgo, and A. L. Barabasi, "Understanding individual human mobility patterns," Nature, Vol. 453, No. 7196, pp. 779-782, 2008.

[9] E. Fernandes, B. Crispo, and M. Conti, "FM 99.9, Radio virus: Exploiting FM radio broadcasts for malware deployment",Transactions on information forensics and security, Vol. 8, No. 6, June 2013.

[10]] M. Chandramohan, H. Tan, "Detection of mobile malware in the wild", IEEE early access, 2012. [11] Q. Yan, Y. Li, T. Li, and R. Deng, "Insights into Malware Detection and Prevention on Mobile Phones", Springer-Verlag Berlin Heidelberg 2009.

[11] W. Enck, D. Octeau, P. Mcdaniel, S. Chaudhuri,"A study of android application security", In: Proceedings of the 20th Usenix security symposium, August 2011.

[12] M. Egele, T. Scholte, E. Kirda, C. Kruegel, "A Survey on Automated Dynamic Malware-Analysis Techniques and Tools", CSUR4402-06 ACM-TRANSACTION February 8, 2012.

[13] T. Blasing, A. D. Schmidt, L. Batyuk, S. A. Camtepe, and A. Albayrak, "An android application sandbox system for suspicious software detection", In 5th International Conference on Malicious nd Unwanted Software (Malware 2010), Nancy, France, 2010.

[14] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid Android: Versatile protection for smartphones", In ACSAC'10, Dec. 2010.

[15] G. Jacoby, N. Davis, "Battery-based intrusion detection", In Proceedings of the Global Telecommunications Conference (2004).

[16]] L. Liu, G. Yan, X. Zhang, and S. Chen, "VirusMeter: Preventing your cellphone from spies", In Proceedings of RAID, volume 5758 of Lecture Notes in Computer Science, pages 244-264, 2009.

[17] W. Enck, M. Ongtang, P. McDaniel,"On Lightweight Mobile Phone Application Certification", In: Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS) (Nov 2009).

[18] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices", IEEE Communications Surveys & Tutorials, IEEE 2012.

[19] Kaspersky Lab IT Threat Evolution: Q2 2013, [online] http://www.kaspersky.co.in/about/news/virus/2013/kaspersky_lab_it_threat_evolution_q2_2013.

[20] A. Gostev, "Mobile Malware Evolution: An Overview, Part 1", [online], http://www.securelist.com/en/analysis ?pubid=200119916.

[21] D. Maslennikov, "Mobile Malware Evolution: Part 6" [online], http://www.securelist.com/en/analysis/204792283/Mobile_Malware_Evolution_Part_6.