ISSN 2319 - 6629

Volume 3, No.2, February – March 2014

International Journal of Wireless Communications and Networking Technologies

Available Online at http://warse.org/pdfs/2014/ijwcnt01322014.pdf

A Survey On Restraining Virus Propagation In Mobile Networks

[1]M.Karpagavalli , [2]K.Mythili

[1]Research Scholar, Hindustan college of Arts and Science, India, mkarpagavalli09@gmail.com
[2]Associate Professor, Hindustan college of Arts and Science, India, mythiliarul@gmail.com

ABSTRACT

Mobile communication systems are becoming increasingly significant and ubiquitous in people's daily lives. Due to the enormous growth in mobile devices, virus propagation in mobile virus is an important security concern. A mobile virus is nothing but malicious computer software that targets mobile phones and causing the collapse of the system and leakage of confidential information. In the wireless communication viruses can even jam wireless services by transmitting thousands of spam messages and diminish the quality of voice communication. Because of the virus propagation, there is leakage of privacy data, additional service charges and exhaustion of battery power. These malware or virus is cell-phone worms that are malicious codes that exploit vulnerabilities in cell-phone software and propagate in networks via popular services such as Bluetooth and Multimedia Messaging Service (MMS). Worms are devastating to both users and network. A user can be instinctively charged for several messages created by the worm and the phone battery will be rapidly drained. Other reported worm damages expand from stealing user data and privacy to destroying hardware. Due to the severe damages of the mobile virus, it is significant for the users to gain a deep understanding of the propagation mechanisms of mobile viruses. So, in these circumstances there is a critical requirement for both users and service providers to further recognize the propagation mechanisms of mobile viruses and to deploy proficient countermeasures.

Key terms: Mobile Networks, Phone virus, virus propagation, security, malware

1. INTRODUCTION

Wireless mobile devices such as cellular phones, Personal digital assistants and headsets are used increasingly in the last decade. The popularity of mobile smart phones with richer wireless communication capabilities permits extensive social interactions in the following aspects. With the increasing number of mobile devices the more and more virus and malwares are also increased. Common to several of the existing mobile viruses and worms is that they influence blue tooth capabilities to propagate themselves. Bluetooth is a short-range radio technology which intends for connecting different wireless devices at low power consumption and at low cost. It has a large range of applications, such as wireless headsets, dial-up networking, and peer-to-peer file sharing.

In the internet computer worms are extensively increasing for more than two decades, are nothing new to us. Actually, Bluetooth worms are dissimilar from internet worms in three ways. Firstly, the transmission range of Bluetooth is restricted that leads to a proximity-based infection mechanism. A Blue-tooth enabled device can only affect the neighbors within its radio range. This can be different from internet worms that often scan the whole IP address space for vulnerable victims. Secondly, the bandwidth obtainable to Bluetooth devices is generally much narrower than those of internet links.

There are three types of mobile viruses which affects the mobile devices. The first one is worm: The major objective of this stand-alone type of malware devices. Worms may also include dangerous and ambiguous instructions. Mobile worms may be transmitted via text messages SMS or MMS and typically do not require user interaction for execution. The second one is Trojan: Unlike worms, Trojan horse always needs user interaction to be activated. This type of virus is generally inserted into seemingly attractive and non-malicious executable files or applications which are downloaded to the device and executed by the user. Once activated, the malware can cause serious damage by infecting and deactivating other applications or the phone itself, rendering it paralyzed after a certain period of time or a certain number of operations. The third one is Spyware: This malware creates a threat to mobile devices by gathering, using and distributing a user's personal or perceptive information without the user consent.

In the following survey, numerous methods have been proposed for restraining mobile virus. Even though some of the simple anomaly detection methods can to a certain extent protect infected phones from sending infected messages based on system calls sequences and application program interfaces [1] [2] , they will not be able to detect new viruses because of the limitation of anti-virus knowledge. To overcome this problem, to make sure that users update their own detection databases, the security companies require for disseminating notifications or patches to smart phones. But due to the limited bandwidth and time it is not possible to broadcast security notifications to all the mobile phones. So, to reduce the number of phones infected there is an urgent requirement for both users and service providers to further understand the propagation mechanisms of mobile viruses and to deploy effectual countermeasures.

2.DEFENSE STRATEGIES AGAINST MOBILE VIRUSES

Hahnsang Kim et.al suggested a method identifying particular malwares by monitoring battery life-time that can discover some unknown energy-depletion threats [3]. Because mobile users are increasing rapidly this adopts battery-powered mobile hand-held devices. The most general method to detect the malware is signature based analysis. But in this method for every particular malware it wants a new signature resulting to that there is high computation cost. A new framework called power-aware malware detection is used to examine, identify and analyze the unknown and energy-greedy threats. This malware-detection method includes power observer and data analyzer. The power samples are gathered by former and builds a power consumption history by utilizing the collected samples and based on the history of the power consumption the power signature is generated. After that the data analyzer distinguishes an anomaly by evaluating the generated power with a database. The main idea of this work is firstly, assuming that in a handheld device one application is executed at a time, and a power consumption history is recorded and then converted into a power signature which is an abstraction of the underlying application behavior. Secondly, a simple and effectual noise filtering and data compression software components enable a lightweight system implementation. By utilizing the process of data compression provides the energy saving is accomplished in the signature database. The drawback of this method is multiprocessing is not supported.

Abhijit Bose et.al have differentiated some malicious behaviors from normal operations by training a classifier based on the support vector machines [4]. Due to the security problem in mobile networks, a behavioral detection scheme is used. In this method, the runtime behavior of an application is scrutinized and this can be compared with the malicious and normal behavior profiles. The malicious behavior profiles can be completed as global rules that associate to whole applications. But the rate of false positives is low. A Support Vector Machines is utilized to effectually decide the virus programs from the incomplete behavior signatures. So that partial signatures for malicious behavior can be classified correctly from those of normal applications running on the handset. For the purpose of real-time deployment, the resulting SVM model and also the malicious signature database are preloaded onto the handset by using either handset manufacturer or a cellular service provider. If the new behaviors are discovered these are updated. The process of updating is same as the anti-virus updation. On the other hand, totally new behaviors are far fewer than new variants; the updates are not predictable to be frequent. But the disadvantage of this method is high computation complexity.

Jerry Cheng et.al suggested a method for detecting single-device and system-wide abnormal behaviors by gathering and sending communization data to remote servers to diminish the detection burden. Because the Smart phones have newly become increased so that the mobile virus is a significant concern. Smart Siren, virus detection and an alert system is used for Smart phones [5]. To detect the viruses, this method gathers the communication activity information from the Smart phones and the joint analysis is performed to detect the abnormal behaviors. One of the main features in Smart Siren is the user privacy protection. Smart Siren concerns the dilemma of privacy by an unidentified and ticketed report submission scheme. However, it avoids the proxy from knowing the behaviors of any user. Also, it prevents a virus attacker from abusing the privacy mechanism and injecting bogus reports in huge amounts to deceive the results of virus detection. The main work is consists of three-fold. Firstly, to show the vulnerability of Window Mobile Smart phones via the development of proof-of-concept viruses. Secondly, by using mutual detection a virus can be detected. Finally, a ticketing method which preserves the user privacy.

Thrasyvoulos Spyropoulos et.al suggested a new time-variant community mobility model. In this method, to define communities that are visited regularly by the nodes to detain skewed location visiting preferences and by using time periods with dissimilar mobility parameters to generate periodical re-appearance of nodes at the same location [6]. Furthermore, this time-variant community model can be mathematically treated to obtain systematic expressions for two significant quantities of interest which decides the performance of mobility-assisted routing schemes the hitting time and the meeting time. The hitting time is defined as the average time before a node moves towards the vicinity of an arbitrarily selected geographical location. The meeting time is an average time defined as before two nodes move to the vicinity of each other. These quantities obtain the time between available communication opportunities under the mobility model, and can be utilized as building blocks to examine the performance of more complex packet forwarding schemes.

Mukund Seshadri et.al suggested a method called Power Track that fits a lesser known but more applicable distribution for the data and track its parameters over time. To consider the analysis of the social network by the calls of users in phone networks [7]. To investigate the mobile call graph and the consequent social networks attained from the network of a huge cellular operator. The major idea of the work is consists of fourfold: Firstly, to identify the distributions in the dataset extensively deviate from those examined in the previous work and the conventional power laws often fall short. Secondly, the power Track method is initiated that presents noticeably better fits using the lesser known but more applicable Double Pareto Log Normal distribution. This method clearly summarizes an examined data distribution by utilizing four parameters. This can be easily evaluate at any given point in time and monitor over time. Finally, this graph changes over time in a way consistent with a generative process which obviously results in Double Pareto Log Normal distributions.

Elizabeth Van Ruitenbeek et.al suggested the propagation model of mobile phone viruses to study the effect of the dependability of mobile phones. Because of the attacks through the virus the mobile phone get damage and also it compromise personal information, delete the data, battery drained problem and capture the phone services [8]. Due to the effects of mobile virus in phones the customer complaints are also enlarged and additional network congestion because of the virus-related traffic. The response mechanisms and the models are used to attain insight on the effectiveness of the virus mitigation techniques. Particularly, the effects of multimedia messaging system (MMS) viruses are taken into account which spreads by transmitting infected messages to other phones. The six response mechanisms are utilized that give responds to the viruses at three response points in the propagation process: which is called the point of reception, the point of infection on target phones, and the point of distribution from polluted phones. But the disadvantage of this method is there is less accuracy.

Shin-Ming Cheng et.al suggested a new differential equation-based model to examine the mixed behaviors delocalized infection in the mobile phones [9]. Because of the increasing popularity of the mobile phones, the social interactions are also increased. In personal area network, the communication between an individual and the friends are interconnected by call records and contacts are facilitated by portability of handset. Secondly, Smart phones are equipped with short-range wireless communication technology such as Wifi, Bluetooth which permits peer-to-peer communication individuals that builds a spatial social network. This work proposes a new analytical method to effectually examine the speed and harshness for spreading the hybrid malware such as Commwarrior that targets multimedia messaging service (MMS) and BT.

Pradip De et.al proposed a general framework based on epidemic theory for examining the vulnerability in the transmitting protocols in the wireless sensor networks [10]. Because wireless sensor networks are used in different types of applications so that security is one of the most significant problems. One of the dangerous viruses called Cabir is extensively susceptible to malwares. Cabir utilizes the Blue tooth technology to spread the viruses between the cell phones. So, to conquer this trouble to consider a common scenario for network-wide broadcasting information and instead of looking into particular cryptographic methods to secure broadcast protocols. The working procedure is recognized in terms of speed of propagation and reachability. In the wireless sensor network, suppose if a source node has been compromised and is being utilized along with the communication mechanism of the broadcast protocol to compromise the remaining nodes by propagating a quantity of malware in the network. Particularly, the major idea is a new framework based on epidemic theory serves as a general and flexible platform for capturing and characterizing the malware spreading in various broadcast protocols, thus facilitates a comparative analysis of their vulnerabilities. According to the local spatial interaction of nodes in a neighborhood the epidemic model for propagation of data is to be generated. To map the specific protocol, a spreading rate is used. Additionally, to investigate the dynamics of the malware infection in the particular protocol the spreading rate is used.

Pradip De et.al suggested a technique to examine the the spreading process of node compromise in the wireless sensor networks [11]. Through the wireless communication, an attacker effectually compromise neighbouring nodes and thus threats the entire network. Specifically, in the wireless sensor networks the security schemes are used, to assume that the communication can only be performed when neighbouring nodes can institute mutual trust by validating a common key. Therefore, the compromise of the ode not only decides by the deployment of sensor nodes and also affects the node density, but also decided by the pair wise key scheme employed therein. In the wireless sensor networks, to scrutinize these factors an epidemiological method is used to observe the probability of an outbreak. Additionally, to analyze the effect of node recovery in an active infection scenario and to attain crucial values for these parameters which results in an outbreak. There are two types of node deployment scenarios called uniform arbitrary deployment and group based deployment of nodes. The major limitation of this method is high computation cost.

Liang Xie et.al suggested to handle the security threats in mobile networks [12]. As the increasing number of cell phones the viruses and malwares are also increased this causes problem like loss of privacy data, extra charges and depletion of battery power. A mandatory access control based defence mechanism for blocking malware which launch attacks through generating new processes for execution. This mechanism is effectual in defeating malware that executes malicious nodes in new processes. Also to combat automated malware which gain controls of existing processes to execute malicious codes, and propose a more comprehensive defence that identifies and blocks malware using AI techniques such as Graphic Turing test (GTT). On the other hand this method does not respond on well-known malware signatures.

Pan Hui et.al suggested to examine the problem of optimal distribution of content-based signatures of malware to decrease the number of infected nodes that can help to detect the corresponding malware and to disable further propagation. Because the malware attacks become more recurrent in mobile networks [13]. So, to deploy a proficient defence mechanism for protecting against infection and to help the infected nodes to recover the significant serious spreading and outbreaks. In mobile devices are promiscuous in terms of operating systems. Malware can affect the system in any opportunistic method through local and global connectivity. To model the defence system with realistic postulations addressing all the issues which is not considered. Based on this framework of optimizing the system welfare utility through the signature allotment, to present an encounter-based distributed algorithm based on Metropolis sampler.

CONCLUSION

Due to the enormous growth in the mobile devices, viruses and malwares are also increased. So, the propagation of virus causes some problems like leakage of data, user privacy, and charge depletion in battery. In wireless communication, by transmitting several spam messages the wireless services are corrupted through malwares. So that diminishes the quality of voice communication. So, there is a significant challenge for both users and service providers to obviously understand the propagation mechanisms of viruses and malwares in the mobile networks. To detect the viruses and malwares several schemes are proposed such as, monitoring battery life-time which discovers some unknown energy-depletion threats. Based on epidemic theory, a common framework is used to examine the susceptibility in the sending protocols in the wireless sensor networks. At the end of the survey, it is concluded that an effective detection mechanism is proposed to reduce the number of infected phones by viruses and malwares in mobile networks.

REFERENCES

[1] L. Xie, H. Song, T. Jaeger, and S. Zhu, “A Systematic Approach for Cell-Phone Worm Containment,” Proc. 17th Int’l World Wide Web Conf. (WWW ’08), pp. 1083-1084, 2008.

[2] N. Xu, F. Zhang, Y. Luo, W. Jia, D. Xuan, and J. Teng, “Stealthy Video Capturer: A New Video-Based Spyware in 3G Smart phones,” Proc. Second ACM Conf. Wireless Network Security (WiSec ’09), pp. 69-78, 2009.

[3] H. Kim, J. Smith, and K.G. Shin, “Detecting Energy-Greedy Anomalies and Mobile Malware Variants,” Proc. Sixth Int’l Conf. Mobile Systems, Applications, and Services (MobiSys 08), pp. 239-252, 2008.

[4] A. Bose, X. Hu, K.G. Shin, and T. Park, “Behavioral Detection of Malware on Mobile Handsets,” Proc. Sixth Int’l Conf. Mobile Systems, Applications, and Services (MobiSys ’08), pp. 225-238, 2008.

[5] J. Cheng, S.H.Y. Wong, H. Yang, and S. Lu, “Smart siren Virus Detection and Alert for Smartphones,” Proc. Fifth Int’l Conf. Mobile Systems, Applications, and Services (MobiSys ’07), pp. 258-271, 2007.

[6] W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, “Modeling Time-Variant User Mobility in Wireless Mobile Networks,” Proc. IEEE INFOCOM, pp. 758-766, 2007.

[7] M. Seshadri, S. Machiraju, A. Sridharan, J. Bolot, C. Faloutsos, and J. Leskovec, “Mobile Call Graphs: Beyond Power-Law and Lognormal Distributions,” Proc. 14th ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining (KDD ’08), pp. 596-604, 2008.

[8] E.V. Ruitenbeek and F. Stevens, “Quantifying the Effectiveness of Mobile Phone Virus Response Mechanisms,” Proc. 37th Ann. IEEE/IFIP Int’l Conf. Dependable Systems and Networks (DSN ’07), pp. 790- 800, 2007.

[9] S. Cheng, W.C. Ao, P. Chen, and K. Chen, “On Modeling Malware Propagation in Generalized Social Networks,” IEEE Comm. Letters, vol. 15, no. 1, pp. 25-27, Jan. 2011.

[10] P. De, Y. Liu, and S.K. Das, “An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks,” IEEE Trans. Mobile Computing, vol. 8, no. 3, pp. 413-425, Mar. 2009.

[11] P. De, Y. Liu, and S.K. Das, “Deployment Aware Modeling of Node Compromise Spread in Wireless Sensor Networks Using Epidemic Theory,” ACM Trans. Sensor Networks, vol. 5, no. 3, pp. 1-33, 2009.

[12] L. Xie, X. Zhang, A. Chaugule, T. Jaeger, and S. Zhu, “Designing System-Level Defenses against Cell phone Malware,” Proc. IEEE 28th Int’l Symp. Reliable Distributed Systems (SRDS ’09), pp. 83-90, 2009.

[13] A. Bose, X. Hu, K.G. Shin, and T. Park, “Behavioral Detection of Malware on Mobile Handsets,” Proc. Sixth Int’l Conf.Mobile System.