Modeling and Automatic Detection 0f Virus in Mobile Environment

Lakshmi.D[1], Thamizharasi.H[2], Prakash.R[3], Divyalakshmi.C[4]

[1, 2, 3]Scholar, Department of Computer Science and Engineering, Dr. Pauls Engineering College, Vanur Tk., Villupuram Dt

[4]Assistant Professor, Department of Computer Science and Engineering, Dr. Pauls Engineering College, Vanur Tk., Villupuram Dt

Abstract

In this thesis present a new way to assess and restrain virus propagation by proposing the concepts of two-layer network model for simulating virus propagation through both Bluetooth and SMS. An efficient autonomy-oriented computing (AOC) based patch dissemination strategy to restrain the mobile virus. In this strategy, some entities are deployed in a mobile network to search for mobile devices according to some specific rules and with the assistance of a center. Mobile networks, formed by the connection of mobile devices following some relationships among mobile users, provide good platforms for mobile virus spread. Quick and efficient security patch dissemination strategy is necessary for the update of antivirus software so that it can detect mobile virus, especially the new virus under the wireless mobile network environment with limited bandwidth which is also large scale, decentralized, dynamically evolving, and of unknown network topology. Our simulation results provide further insights into the determining factors of virus propagation in mobile networks.

KEYWORDS: *Mobile computing, security, AOC, pre-immunization, adaptive dissemination.*

1. INTRODUCTION

Many studies have reported the damages of mobile viruses in smart phones . For example, an outbreak of mobile viruses occurred in china in 2010. The ‘zombie’ virus attacked more than 1 million cell phones, and created a loss of $300,000 per day. Among many potential damages, mobile viruses can cause private data leakage and disturb conversation by remote control. In some more serious situations, viruses can even jam wireless services by sending thousands of spam messages, and reduce the quality of voice communication. In view of this situation, there is an urgent need for both users and service providers to further understand the propagation mechanisms of mobile viruses and to deploy efficient countermeasures. In order to help researchers observe and predict potential damages of a virus, some models have been used to study the dynamic process of virus propagation.

Notifications or patches to smart phones. However, it would be impractical to disseminate security notifications or patches to all phones because of the limitation of time and bandwidth. Some strategies attempt to forward security notifications or patches based on the short-range communication capabilities of intermittently connected phones, but their impact will be affected by human mobility patterns and inter-contact frequencies among phones. It would be difficult to acquire signature files in a timely manner.

2. RELATED WORKS

In the last few years, the growing popularity of mobile devices has made them attractive to virus and worm writers. One communication channel often exploited by mobile malware is the Bluetooth interface. In this paper, we present a detailed analytical model that characterizes the propagation dynamics of Bluetooth worms. Our model captures not only the behavior of the Bluetooth protocol but also the impact of mobility patterns on the Bluetooth worm propagation. Validation experiments against a detailed discrete-event Bluetooth worm simulator reveal that our model predicts the propagation dynamics of Bluetooth worms with high accuracy. We further use our model to efficiently predict the propagation curve of Bluetooth worms in big cities such as Los Angeles. Our model not only sheds light on the propagation dynamics of Bluetooth worms, but also allows to predict spreading curves of Bluetooth worm propagation in large areas without the high computational cost of discrete-event simulation.

Mobile malware is rapidly developing, but current anti-virus products in mobile devices still use the signature-based solutions, which usually need a large database and cannot detect malware variants. In this paper, we proposed a behavior-based malware detection system for Windows Mobile platform called WMMD (Windows Mobile Malware Detection system). WMMD uses API interception techniques to dynamic analyze application's behavior and compare it with malicious behavior characteristics library using model checking. The experiment results show that

WMMD can effectively detect the obfuscated or packed malware variants that cannot be detected by other main stream anti-virus products.

5. PROPOSED APPROACH

We have presented a two-layer network model for simulating and analyzing the propagation dynamics of SMS-based and BT-based viruses. Our model characterizes two types of human behavior, i.e., operational behavior and mobile behavior, in order to observe and uncover the propagation mechanisms of mobile viruses. Our simulation-based studies have contributed to the understanding of interactions between human behaviors and the propagation dynamics of mobile viruses. If users have higher security awareness, they would not be infected even if they receive infected messages. If a user opens an infected message, the phone of this user is infected and automatically sends viruses to all phones based on its address book. If a user does not open an infected message, it is assumed that the user with higher security awareness deletes this infected message. An infected phone sends out viruses to other phones only once, after which the infected phone will not send out viruses anymore; If a phone is patched (immunized), it will not send out viruses even if a user opens an infected message. In order to reflect the real transmission of short messages, we add some parameters to simulate the states of short messages and smart phones in our model.

1) The message delivery latency and failure.

Statistical results in have shown that 91% of delivered messages have a latency period less than 5 minutes (95% of messages have a latency less than 1 hour from Fig. 2 in , and 5% of delivered messages have a latency longer than 1 hour. Meanwhile, 5.1% of messages fail to reach their estimations. Internet service providers can apply the throttling technology, which has been used in computer networks, to slow down the speed of virus propagation by increasing the delivery latency of messages. By doing so, we can gain some time to disseminate security patches to subscribers, hence to restrain mobile virus propagation.

2) Power on or off.

Mobile phones may be turned off when users sleep. Here, we simulate the power on or off period based on the awake or sleep time of a user, respectively, as reported in the existing studies2; that is, the period of power on (awake time) is between 14 to 18 hours, whereas the period of power off (sleep time) is between 6 to 10 hours.

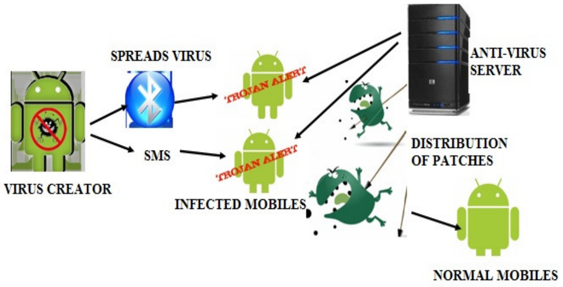

Figure.1. System model for modeling and restraining mobile virus

6.1TWO-LAYER NETWORK PROPAGATION

The basic ideas behind our two-layer network propagation modeling are The lower layer represents a geographically-based cell tower network. BT-based viruses spread in this layer to various positions of mobile phones The upper layer corresponds to a logical network constructed from the address books of phones.

6.2 SMS-BASED PROPAGATION

Social relationships are embodied in mobile networks based on the address books of smart phones. If a phone is infected by an SMS-based virus, the virus automatically sends its copies to other phones based on the address book of the infected phone. When users receive a suspicious message from others, they may open or delete it based on their own security awareness and knowledge about the risks of mobile viruses. Therefore, the security awareness of mobile users is one of the dominant factors that determine SMS-based virus propagation. In our model, we simulate one type of operational behavior, i.e., whether or not a user opens a suspicious message. The probability of clicking on a suspicious attachment can be used to reflect and quantify the security awareness of a user. Analogous behavior has been used to simulate email virus propagation [3], [1]. Briefly, once the sample size goes to infinity, the message-clicking probabilities among different users will follow a Gaussian distribution , If users have higher security awareness, they would not be infected even if they receive infected messages.

If a user opens an infected message, the phone of this user is infected and automatically sends viruses to all phones based on its address books. If a user does not open an infected message, it is assumed that the user with higher security awareness deletes this infected message. An infected phone sends out viruses to other phones only once, after which the infected phone will not send out viruses anymore;

If a phone is patched (immunized), it will not send out viruses even if a user opens an infected message.

7. PROPOSED SYSTEM TECHNIQUES

My proposed system consists of following techniques:

MOBILE CLIENT

Mobile Client is an Android application which created and installed in the User's Android Mobile Phone. So that we can perform the activities. The Application First Page Consist of the User registration Process. We'll create the User Login Page by Button and Text Field Class in the Android. While creating the Android Application, we have to design the page by dragging the tools like Button, Text field, and Radio Button. Once we designed the page we have to write the codes for each. Once we create the full mobile application, it will generated as Android Platform Kit (APK) file. This APK file will be installed in the User's Mobile Phone an Application.

SERVER

The Server is Server Application which is used to communicate with the Mobile Clients. The Server can communicate with their Mobile Client by GPRS or Bluetooth Technology. In the Project we are using Bluetooth technology to access with the Client. The Server Application can be created using Java/ DotNet Programming Languages. The Server will monitor the Mobile Client's accessing information and Respond to Client's Requested Information. The Server will not allow the Unauthorized User from entering into the Network. So that we can provide the network from illegitimate user's activities. Also the Server will identify the Malicious Nodes activities.

VIRUS GENERATION AND DISTRIBUTION

In this Module we will create the Mobile Virus which is malicious code that will perform malicious activities in the User's Mobile Phones. In this Project we are creating a New Folder Virus which will create a Folder inside the Folder virus by developing malicious codes. So that we can generate the Mobile Virus. Once the attackers created the Virus, they will spread the Virus via Bluetooth or SMS technique, So that the virus will be spread to other Users Mobile Phones. While sending via Bluetooth technique, the User's has to be present within the communication range. The Attacker can send the virus file via Mobile Application that was installed in their Mobile Phones.

AUTOMATIC DETECTION OF VIRUS:

Once the attack spread the Virus File to other User's Mobile Phone the content of the message of the file will be analyzed by the Server to detect whether the file contains that Malicious Behavior or not. If the file contains the malicious behavior, then the Server will detect the file as Virus file. Once the Server detected that the Virus file it will deliver the patches to the User's Mobile Phone and deletes the Virus File.

DISTRIBUTION OF PATCHES

Once the Server identify virus file was sent to the User's Mobile Phone, the Server will provide the patch files to delete the Virus file. Using an Android Application the patches will be distributed to the User's Mobile phone automatically to clear the Virus.

8. NETWORK MODEL

8.1 Two-Layer Network

The basic ideas behind our two-layer network propagation modeling are shown in Fig.3.1The lower layer represents a geographically-based cell tower network. BT-based viruses spread in this layer to various positions of mobile phones The upper layer corresponds to a logical network constructed from the address books of phones. SMS-based viruses propagate in this layer following the social relationships among mobile users.

8.2The Structure of a Geographical Network

Mobile phones connect with each other through wireless signals provided by cell towers. In our study, we is built based on geographical information, whereas the social relationship network is constructed from the address books of mobile users. model the geographical network of cell towers using a 2-dimensional grid .

9. CONCLUSION

Based on our proposed two-layer network model, we have examined two strategies for controlling SMS based virus propagation that are based on the methodology of autonomy-oriented computing (AOC). As revealed in our experimental results, the AOC-based pre immunization strategy is capable of restraining mobile virus propagation by protecting some highly-connected phones, whereas the AOC-based dissemination strategy can forward security notifications or patches to as many phones as possible with a low communication cost in order to help them recover or avoid the potential damages of mobile viruses. Our experimental results have also indicated that our strategies can restrain virus propagation in a large-scale, dynamically-evolving, and/or community-based network

As for our future work, we will investigate the hybrid viruses that propagate through both BT and SMS channels some assumptions about human mobility and operational patterns in this paper have been based on some empirical studies and statistical data. In our next step, we will extend our model to incorporate additional characteristics of human mobility and operations. In particular, our future computational model will consider the dynamic changes of users' behaviors in the course of mobile virus propagation.

Be helpful to send security notifications to as many users as possible in order to improve their security awareness, which can in turn play a key role in restraining virus propagation. Meanwhile, our simulation results have shed light on the effects of human mobility on BT based virus spreading, in terms of infection dynamics and spatially localized spreading patterns. Based on our proposed two-layer network model, we have examined two strategies for controlling SMS based virus propagation that are based on the methodology of autonomy-oriented computing (AOC). As revealed in our experimental results, the AOC- based pre-immunization strategy is capable of restraining mobile virus propagation by protecting some highly-connect ted phones.

10.REFERENCES

[1]D.-H. Shi, B. Lin, H.-S. Chiang, and M.-H. Shih, "Security aspects of mobile phone virus: A critical survey," Industrial Management and Data System, vol. 108, no. 4, pp. 478–494, 2008.

[2]H. Kim, J. Smith, and K. G. Shin, "Detecting energy greedy anomalies and mobile malware variants," Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services(mobisys08), pp. 239–252, 2008.

[3]L. Xie, H. Song, T. Jaeger, and S. Zhu, "A systematic approach for cell-phone worm containment," Proceedings of the 17th International World Wide Web Conference (WWW08), pp.1083–1084, 2008.

[4]N. Xu, F. Zhang, Y. Luo, W. Jia, D. Xuan, and J. Teng, "Stealthy video capture: A newvideo-based spyware in 3G smartphones," Proceedings of the 2nd ACM Conference on Wireless Network Security (wisec09), pp. 69–78, 2009.

[5]G. Yan and S. Eidenbenz, "Modeling propagation dynamics of bluetooth worms (extended version)," IEEE Transactions on Mobile Computing, vol. 8, no. 3, pp. 353–367, 2009.

[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]P. Wang, M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi, "Understanding the spreading patterns of mobile phone viruses," Science, vol. 324, no. 5930, pp. 1071–1076, 2009.

[8]S. Cheng,W. C. Ao, P. Chen, and K. Chen, "On modeling malware propagation in generalized social networks," IEEE Communications Letters, vol. 15, no. 1, pp. 25–27, 2011.

[9]P. De, Y. Liu, and S. K. Das, "An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 8, no.opp.413–425, 2009.