ISSN:2320-0790

An International Journal of Advanced Computer Technology

DETAINING AND AVOIDING MOBILE VIRUS PROPAGATION BY CONSIDERING HUMAN BEHAVIOR

[1]Anagha C M, [2]Dr. S. Uma, [3]Mr. M. Mathan Kumar

[1]PG Scholar, [2]Professor and Head, [3]Asst. Professor,
Dept. of PG-CSE
Hindusthan Institute of Technology, Coimbatore

ABSTRACT: Malware, short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is designed to cause damage to a standalone computer or a networked pc. So wherever a malware term is used it means a program which is designed to damage your computer it may be a virus, worm. So, in order to overcome this problem we propose a two-layer network model for simulating virus propagation through both Bluetooth and SMS. We examine two strategies for restraining mobile virus propagation, i.e., preimmunization and adaptive dissemination strategies drawing on the methodology of autonomy-oriented computing (AOC). This method can effectively restrain virus propagation in a large-scale, dynamically evolving, and/or community based network. In order to increase the effectiveness of inhibiting the propagation of mobile phone viruses, we introduce an innovative approach called a virus detection model based on the Danger Theory. This model includes four phases: danger capture, antigen presentation, antibody generation and antibody distribution. Due to the distributed and cooperative mechanism of artificial immune system, the proposed model lowers the storage and computing consumption of mobile phones. By using this system, we can effectively inhibit and delete the virus files.

Keywords

Mobile networks, phone virus, human mobility, autonomy-oriented computing, Danger Theory, preimmunization, adaptive Dissemination.

1. INTRODUCTION

Mobile security or mobile phone security has become increasingly important in mobile computing. It is of particular concern as it relates to the security of personal information now stored on the smart phone. More and more users and businesses use smart phones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smart phones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

In June 2004, computer scientists released a proof-of concept mobile virus named Cabir, used Bluetooth to send itself over the airwaves to unsuspecting victims who thought they had received a security program and proceeded to infect themselves upon installation. In August 2010, the first malicious program for smart phones running the Google's Android operating system named Trojan-SMS. Android OS Fake Player has been detected. By April 2012, according to Kaspersky virus database, there are more than 5000 mobile phone viruses. 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.

The damages of mobile viruses in the smart phones are an important problem. 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 observe and predict potential damages of a virus, some models have been used to study the dynamic process of virus propagation. Valid propagation models can be used as test beds to: 1) estimate the scale of a virus outbreak before it occurs in reality and 2) evaluate new and/or improved countermeasures for restraining virus propagation.

We propose a two-layer network model for characterizing BT-based and SMS-based viruses, which propagate through Bluetooth and Short/Multimedia Message Services, respectively, in order to address the abovementioned shortcomings. In our proposed model, viruses are triggered as a result of human behaviors, rather than contact probabilities in a homogeneous model. Two types of human behavior, i.e., operational behavior and mobile behavior (mobility) are considered in our individual- based model. Different from existing work that focuses on the effects of network structures on virus propagation; our work is aimed to gain further insights into how human behaviors affect the propagation dynamics of mobile viruses. In order to delete the virus files we use a technique called a novel analytical model to efficiently analyze the speed and severity for spreading the hybrid malware such as Commwarrior that targets multimedia messaging service (MMS) and BT. This can estimate the damages caused by the hybrid malware and aids in the development of detection and containment processes.

2. MODELING MOBILE VIRUS PROPAGATION

A two-layer network model simulates mobile virus spreading through different communication channels. Different from others, this work addresses the issue of how human behaviors, i.e., operational and mobile behavior, affect virus propagation. Based on the analysis of propagation mechanisms, we note that a primary factor contributing to SMS-based virus propagation lies in users' operations after receiving infected messages. If users have enough knowledge about the risk of mobile viruses (i.e., with a high security awareness), they will not open suspicious messages and their phones will not be easily infected.

In addition to operational patterns, mobility patterns play a key role in BT-based virus propagation. This is because BT-based viruses can only infect local neighbors (whether or not they know these neighbors) within a certain range.

2.1 Two-Layer Network Propagation Model

The basic ideas behind our two-layer network propagation modeling are shown in Fig. 1. 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. SMS-based viruses propagate in this layer following the social relationships among mobile users.

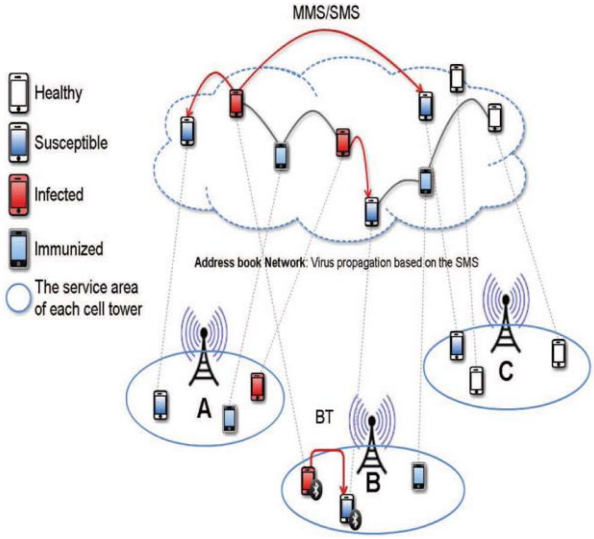

Fig. 1. A two-layer network model for simulating mobile virus propagation.

2.2 SMS-Based Propagation Process

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. 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. In order words, the lower the message-clicking probabilities among different users are, the higher the security awareness will be. In order to better characterize the SMS-based virus propagation, we assume that. 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.

2.3 BT-Based Propagation Process

Different from SMS-based viruses, if a phone is infected by a BT-based virus, it automatically searches another phone through available Bluetooth services within a certain range, and then replicates the BT-based virus to that phone. Therefore, users' contact frequency and mobility patterns play key roles in BT-based virus propagation. In our model, we integrate a stochastic local infection dynamics among phones with the mobile behavior of each user in a geographical network, taking into account prior research on human mobility.

2.3.1 Human Mobility

Although we have used a homogenous model to simulate BT-based virus propagation in each tower, users' different traveling patterns will cause different dynamic spreading processes. Several studies have found that users' traveling patterns play a key role in virus propagation similar to contact-based epidemics (e.g., SARS) in humans. The more accurate the mobility patterns of users are, the better predicting results about virus propagation will be. Based on existing studies, four characteristics of mobility have been observed from the real-world data:

- The traveling distances of a user follow a truncated power-law distribution.
- People move with a probability at each time.
- People trend to devote most of the time to only a few locations in their daily life where they can meet a lot of other people.
- Intercontact times (i.e., the time elapsed between two consecutive contacts of the same two phones) follow a power-law distribution.

3. COUNTERMEASURES AGAINST MOBILE VIRUSES

Based on our analysis, a smart phone can avoid a BT-based attack by turning off the Bluetooth service. However, SMS-based viruses often propagate through the trust relationships among friends. Previous experiments also show that SMS-based viruses are more dangerous than BT-based viruses in terms of propagation speed and scope. In this section, we describe two strategies to restrain SMS-based virus propagation.

3.1 Preimmunization Strategy

Recently, one of the commonly adopted methods for restraining virus propagation is network immunization, which cuts epidemic paths by preimmunizing a set of nodes from a network following some defined rules. The immunized nodes are selected to protect computers or social networks based on the measurements of degree or between's. Some strategies have been proposed to restrain virus propagation by dividing a mobile network into small clusters. However, it would be difficult for these strategies to deal with large-scale, decentralized and/or highly dynamic networks.

In the real world, different companies may release security patches at different time because of the response delays for new viruses. Therefore, the AOC-based preimmunization strategy will be deployed into a network at different times. The deployment delay determines when security patches are distributed to the selected phones based on our strategy.

3.2 Patch Dissemination Strategy

In reality, we detect certain viruses and then allocate patches or antivirus programs into networks only after these viruses have already propagated (e.g., Melissa). Due to the network bandwidth constrains, the security notifications or patches cannot be sent to all users simultaneously. Therefore, we propose an adaptive dissemination strategy based on the methodology of AOC in order to efficiently send

security notifications or patches to most of phones with a relatively lower communication cost.

On the other hand, the AOC-based dissemination strategy that we will discuss below is concerned with how to route security notifications or patches to as many phones as possible with a relatively lower communication cost and a higher coverage rate (i.e., a route selection problem). Initially, we only deploy a few dissemination entities into a mobile network. Each entity with the security patch will be first routed to the highly connected phones based on the local information in order to efficiently disseminate the security notification to other phones.

4. MOBILE PHONE VIRUS DETECTION MODEL (MPVDM) BASED ON THE DANGER THEORY

According to the distribution and resource limitation characteristics of mobile phones, in order to inhibit the propagation of virus, a mobile phone virus detection model (MPVDM) based on the Danger Theory is proposed. The model contains three parts: mobile phones, the Decision Center and database including the Antibody Bank and the Self Set.

Mobile phones are installed with agents, which collect and analyze local information, communicate with Decision Center, receive antibodies and protect mobile phones from viruses.

The Decision Center is a high-performance server, which manages the whole mobile phone network. It is responsible for processing the danger signal, building danger zone, receiving antigens, generating and distributing antibodies.

The Antibody Bank stores all the signatures that are utilized for detecting and removing mobile phone viruses, and newly generated antibodies will be added to this bank. It can reduce the time delay of generating antibody for already detected virus.

The Self Set is a database which stores the self or normal signatures of mobile phones. This set is used to tolerate immature lymphocytes which generate antibodies using negative selection algorithm.

4.1 Phases of MPVDM

A. Danger capture

Once a mobile phone is infected by a virus, there will be some abnormal behaviors, which indicate that the mobile phone is in danger. Because users' operations have influence on the danger signatures, as the mobile phones are in standby state most of the time, we only extract and evaluate danger signatures of mobile phones when they are in standby state.

B. Antigen presentation

When the Decision Center receives a danger signal, it will build a two-dimensioned danger zone both for SMS/MMS and Bluetooth, centered with the mobile phone which sends out the danger signal. The first dimension is measured by hop (suitable for SMS/MMS viruses), and the second dimension is measured by physical distance (suitable for Bluetooth viruses). After the danger zone is built, the Decision Center sends antigen presentation command to all mobile phones that are located in the danger zone. The agents running in mobile phones collect local system information that is useful in preventing virus intrusion and removing virus. We focus on five kinds of system information, including SMS/MMS, Bluetooth, internet connection, local file operation and process creation. Encode these kinds of information to receptors, which are the basic units of antigen/antibody. Mainstream encoding methods include binary encoding and real-value encoding. In this model we use real-value encoding method, that every kind of system information is encoded to a real number.

C. Antibody generation

The Decision Center is responsible for analyzing antigens and generating antibodies of the virus. Based on traditional self/non-self discrimination to avoid autoimmunization, antibody is generated by tolerating the Self Set using negative selection algorithm. The Self Set consists of self-elements which present normal signatures of the mobile phones.

D. Antibody Distribution

The antibody has two functions. First, self-defending, for a healthy mobile phone, antibody can protect the mobile phone from infected by corresponding virus, and that is the concept of vaccine. Second, self-cleaning, for a mobile phone that has already been infected by a virus, the antibody can be utilized for removing the virus. The Decision Center is responsible for distributing antibodies to mobile phones. Both Internet and SMS can be used

as distribution ways. Agent running in mobile phone receives the antibody, loads it and takes effect. The distribution targets can be mobile phones that are in danger zone both infected ones and susceptible ones. In order to inhibit the propagation of virus more effectively, the key nodes of the network will also receive the antibody.

5. CONCLUSION

A two-layer network model is used for simulating and analyzing the propagation dynamics of SMS-based and BT-based viruses to mitigate the viruses and malwares in the mobile networks. 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. In this method it can effectively restrain the virus propagation. To increase the effectiveness of the reducing the propagation of mobile phone viruses, we introduce an innovative approach called a virus detection model based on the Danger Theory. The concept of the Danger Theory is proposed in this paper to resolve the problem of detecting virus in resource limited mobile phones. This model provides a way to detect and response to mobile phone virus more effectively and faster. Based on the spreading and damaging characteristics of virus, danger signal is generated and sent out by infected mobile phones. After antigen is collected, the Decision Center generates corresponding antibody based on traditional self/non-self algorithm. By using this method we effectively detect the virus files and this can increase the virus response efficiency. In addition to that we detect the virus and deleting the virus file.

For future work proposes a novel analytical model to efficiently analyze the speed and severity for spreading the hybrid malware such as Commwarrior that targets multimedia messaging service (MMS) and BT.

REFERENCES

[1]. Chao Gao and Jiming Liu, "Modeling and Restraining Mobile Virus Propagation," Ieee Transactions On Mobile Computing, Vol. 12, No. 3, March 2013. (Base paper)

[2]. Cheng .J, S.H.Y. Wong, H. Yang, and S. Lu, "Smartsiren Virus Detection and Alert for Smartphones," Proc. Fifth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '07), pp. 258-271, 2007.

[3]. De .P, 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.

[4]. Lee .K, S. Hong, S.J. Kim, I. Rhee, and S. Chong, "SLAW: A Mobility Model for Human Walks," Proc. IEEE INFOCOM, pp. 855-863, 2009.

[5]. Mei .A and J. Stefa, "SWIM: A Simple Model to Generate Small Mobile Worlds," Proc. IEEE INFOCOM, pp. 2106-2113, 2010.

[6]. Ruitenbeek .E.V 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.

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

[8]. Zhu .Z, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A Social Network Based Patching Scheme for Worm Containment in Cellular Networks," Proc. IEEE INFOCOM, pp. 1476-1484, 2009.

[9]. Zou .C.C, D. Towsley, and W. Gong, "Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 2, pp. 105-118, Apr.-June 2007.

[10]. Zyba .G, G.M. Voelker, M. Liljenstam, A. Mehes, and P. Johansson, "Defending Mobile Phones from Proximity Malware," Proc. IEEE INFOCOM, pp. 1503-1511, 2009.