Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.526 – 532

RESEARCH ARTICLE

Automatic Detection and Restraining Mobile Virus Propagation using Android

S. Chandrasekar, Prof. V. Jayaprakasan

[1]PG Student, M.E Computer and Communication & Anna University

[2]M.E.,(Ph.D) Department of ECE

Ganadipathy Tulsi's Jain Engineering College, Vellore, TamilNadu

chandrugraduate@gmail.com

Abstract— ***The mobile viruses and malwares is difficult that desires to be reported in the future. Today's lot of studies regarding PC viruses and worms, but very less effect has been done concerning the same issues in the mobile environment. But rapid growth of smart phone users, it increasingly become the target of propagating viruses through the Bluetooth and Wi-Fi and spread into the mobile networks. In a mobile viruses and malwares can cause privacy leakage, extra charges, depletion of battery power, remote listening and accessing private short message and call history logs etc., Furthermore, they can scrape wireless servers by sending lot of spam messages or track user positions through GPS [3]. In this we propose a two layer network model for spreading virus through both Bluetooth and SMS/MMS. Our work addressed the effect of human behaviors, i.e., Operational behavior and Mobile behavior, on virus propagation. Moreover, we observe two strategies for avoid mobile virus propagation, i.e., Preimmunization and Adaptive Dissemination strategies represent on the methodology of Autonomy-Oriented Computing (AOC) [13]. So that by using the method it can automatically detect and delete both Bluetooth and SMS virus before enter into the Smartphone operating system.***

Keywords— AOC; Preimmunization; Adaptive Dissemination; Bluetooth; SMS/MMS

I. INTRODUCTION

In recent years, the worldwide market for smart phones has grown dramatically. Smartphone users can now perform many online tasks, including web browsing, document editing, multimedia streaming, Internet banking, and share the documents from one mobile to another through Bluetooth and SMS services. At the same time, the growing use of smartphones for everyday life and business has been attracting the attention of malware writers, whose aim is to theft data confidentiality, integrity, and the ability to use handheld services. Examples of the most infamous threats to mobile phones include the Skull and Mabir worms, targeting at android phone applications. We refer to these malware or viruses as cell-phone worms, which are malicious codes that act susceptibility in cell-phone software and spread in networks through current services such as Bluetooth and Short / Multimedia Messaging Service (SMS/MMS). A user can be automatically exciting for numerous SPAM messages generated by the worm and the phone battery will be quickly exhausted. Many studies reported the damages of mobile viruses [9], [10]. Other reported worm damages extend from robbery user data and privacy to destroying hardware.

In this paper, we propose a two-layer network model, which spreading viruses through Bluetooth and Short/Multimedia Message Services, respectively, in order to specify the above mentioned shortcomings. In our proposed model, viruses are provoked as a result of human behaviours. Two types of human behaviour, i.e., operational behaviour and mobile behaviour (mobility) [3] are considered in our individual-based model. Our work is aimed to gain further insights into how human behaviours affect the propagation mobile viruses and automatically detect and delete the malwares before enter into the smartphone operating system based on the methodology of Autonomy-Oriented Computing (AOC) [13].

II. EXISTING METHOD

Recently, several methods have been proposed to restrain mobile virus propagation based on existing models [2], [3]. Although some straightforward anomaly detection technologies can protect infected phones from sending infected messages based on system calls sequences and APIs, they will not be able to detect new viruses due to the limitation of antivirus knowledge. In order to make sure that users timely update their own detection databases, service providers or security companies need to disseminate notifications or patches to smart phones. However, it would be impossible to spread security notifications or patches to all phones because of the drawback of time and bandwidth [1]. Thus, it would be necessary for us to propose a new strategy that can proficiently forward patches to as many phones as possible, even in large-scale and/or dynamically evolving networks.

III. SMARTPHONE VIRUSES

The Smartphone virus, Cabir, was developed in 2004 by the virus writing group. It can self-replicate but does no damage to the phones. Now a day more than a hundred mobile viruses have come into existence, many of which contain susceptible codes and cause various damages to the smartphones. The growth of smartphone viruses is at a very fast, perhaps the virus writers have gained from the computer and Internet world. Such suddenly growth of smartphones will provide a productive ground for the malware to spread. An affected smartphone can cause severe compensation for both the users and the cellular service provider. In case of users, the damage may contain the loss or theft of private data, the interference of normal smartphone usage and also economic losses (e.g., the virus may secretly use the SMS/MMS services).In the cellular infrastructure side, the mobile viruses present a serious effect of Denial of Server.

A. Types Of Viruses

It is mainly to observe and catalog the various smartphone viruses in survival today, because such an understanding would enable us to choose what type of virus is most critical for our result to target. There are many ways to categorize smartphone viruses. These smartphone viruses are categorized based on the targets that the virus attacks (e.g. the call center, the cellular base station) [14]. Instead of focusing on what the viruses seek to attack or achieve, we choose to categorize the smartphone viruses based on the multiple infection vectors that the virus enters and/or exits the device. The benefit of our approach is that it provides a generic view on how a virus penetrates into a smartphone and how easily it can spread in the smartphone population. We have identified the categories of infection vectors for smartphone virus, which are listed in Table 1 gives some descriptive viruses at present in existence for each infection vector. Below, we will describe these infection vectors in more detail.

B. Cellular Network

Smartphone viruses can use Multi-media Messaging System (MMS) to spread within the traditionally virus-free cellular network. The most well-known virus of such a kind is *CommWarrior*. By the virtues of its core telephony functionalities, every smartphone is almost always on and always connected to the cellular network, making this infection vector extremely contagious.

INFECTION VECTOR	***EXAMPLES***
Cellular Network	CommWarriors, Mabir
Bluetooth	Cabirs, CommWarrior
Internet over WiFi/GPRS/EDGE	Skulls, Doomboot
USB/ActiveSync/Docking	Crossover, Mobler
Peripherals	Cardtrap

Table 1: Smartphone virus Categorization based on infection vector

C. Bluetooth

Bluetooth virus is innovative in that its spreading does not rely on the existence of any network infrastructure. Instead, it leverages the mobility of the mobile users and the short range wireless connectivity to directly infect nearby Bluetooth users. It is especially contagious in a dense environment, as demonstrated the incidents of *Cabir* outbreak in the World Athletics Championships.

D. Internet

Most smartphones are capable of accessing the Internet (via Wi-Fi, GPRS/EDGE or 3G network access),and run the risk of contracting viruses through downloading from the Internet much like the desktop computers. However, a few distinctions from the desktop computer set this infection vector less potent than the above. However, a smartphone user can still be lured into downloading such as *Skulls* and *Doomboot*, disguised as games, and end up getting infected by a smartphone virus.

E. USB/ActiveSync/Docking

Frequently, smartphones are connected to a desktop computer in order to synchronize calendar events and new contacts. A smartphone virus could potentially penetrate the smartphone in the event of a synchronization as demonstrated by the *Crossover* virus . However, to take this infection vector, the virus must compromise the desktop computer before an attempt can be made onto the smartphone. This requirement makes it significantly more difficult for the smartphone virus to reach a large audience.

F. Peripherals

Similar to desktop computers where viruses used to exploit the floppy disk to spread, smartphone viruses also demonstrated that they are capable of going the same route, as shown by *Card trap*. However, similar to the floppy disk virus, this infection vector has limited spreading capability and most likely will fade out before a major outbreak. In this work, we focus on two categories, i.e., those viruses that spread through cellular messaging systems or Bluetooth. These two infection vectors are not only the most popular ones among existing smartphone viruses, but also the most dangerous ones, because they are unique to smartphones and have strong spreading capability. Thus, it is critical to have a security solution that can effectively combat these viruses.

IV. PROPOSED METHOD

In the system we are implementing a two layer network model for spreading virus through Bluetooth and SMS/MMS channel. The spreading of viruses is addressed by the operations of human behaviors such as mobile behavior and operational behavior [3]. Moreover we examine two strategies to avoid virus in mobile phones. i.e., Preimmunization and Adaptive Dissemination strategies through the methodology of Autonomy-Oriented Computing (AOC) [1].In this method it can automatically detect the virus before when virus enter into the smart phones and delete it.

V. AUTONOMY-ORIENTED COMPUTING

Autonomic computing alludes to the self-managing physical appearance of distributed computing resources, adapting to irregular changes while beating intrinsic difficulty to operators and users [13]. Started by IBM in 2001, this enterprise finally aims to develop computer systems capable of self-management, to overcome the quickly growing difficulty of computing systems management, and to decrease the obstacle that complexity stances to further growth. The system makes conclusion on its own, using high-level policies; it will constantly check and enhance its status and automatically modify itself to changing conditions. An autonomic computing framework is collected of autonomic components (AC) interacting with each other.

VI. GOALS AND MODELING PROCESS OF AUTONOMY-ORIENTED COMPUTING

AOC has three goals [15]:
The first goal is to reproduce life-like behavior in computation. With complete knowledge of the fundamental mechanism, simplified life-like behavior can be used as model for a general-purpose problem solving technique. Replication of behavior is not the end, but rather the means, of these computational algorithms; the second goal is to understand the essential mechanism of a real-world complex system by hypothesizing and frequent experimentation. The conclude product of these simulations is a progress understanding of or explanations to the real working mechanism of the modeled system; the third goal affairs the rise of a problem solver in the absence of human intervention.
To build an AOC-based model, the following is a list of common steps:

- Observe macroscopic behaviors of a natural system;

- Design entities with desired synthetic behaviors as well as an environment where entities reside;
- Observe macroscopic behaviors of the artificial system;
- Validate the behaviors of the artificial system against the natural counterpart;
- modify (ii) in view of (iv);
- Repeat (iii)-(v) until satisfactory;
- Find out a model/origin of (i) in terms of (ii) or apply the derived model to solve problems.

From the above steps, we note that an AOC system mainly contains a population of autonomous entities and the rest of the system is referred to as the environment. Concentrating on entity and environment, the construction of an AOC model involves three phases (see Figure 1) . The first phase, natural system identification, can be viewed as the precursor to actual systems modeling and concerns the selection of an appropriate analogy from the natural and physical world. There are two tasks involved: identify desired system behaviors and identify system parameters. Choosing the right analogy is the key to the success of the AOC-based system and the right system usually presents itself through its behaviors. Once an appropriate analogy is chosen, details such as the number of entities to run and the length of time to run the simulation need to be decided. The second phase, artificial system construction, involves all elements in the AOC-based system. This phase is divided into two major sub-phases: autonomous entity modeling and environment modeling. The identify contributing entities task is the first and the most important task in this phase. Designers are required to choose the level of detail to be modeled that is appropriate to the problem at hand. The define neighborhood task defines a certain measurement (e.g., distance) in the solution space within which local interactions can occur and local information can be collected.

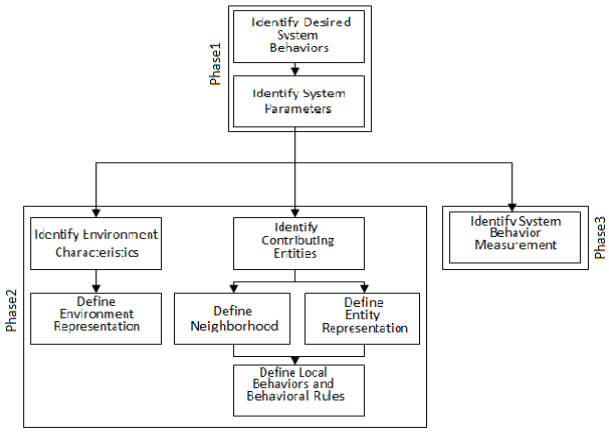

Fig. 1. A block diagram of major components of an AOC model

The *define entity representation* task handles how to characterize an entity, including its states and goals etc. The last task concerning the entities, *define local behaviors and behavioral rules*, defines the ways in which an autonomous entity reacts to various information it has collected within its neighborhood and the ways in which it adapts its local behaviors and behavioral rules. The tasks that concern the environment are *identify environment characteristics* and *define environment representation.* The former task concerns the role the environment plays in conveying the knowledge shared between the autonomous entities. The latter task addresses the characterization of the environment. The third phase, **performance measurement**, concerns the evaluation criteria for comparing the artificial system manifested by the AOC-based system with its natural counterpart. This relates to problem-solving and provides an indication to modify the current set of individual behaviors and behavioral rules

VII. TWO-LAYER NETWORK PROPAGATION MODEL

A. 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.

In order to better characterize the SMS-based virus propagation, we assume that[1]:

- 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.

B. BT-Based Propagation Process

Different from SMS-based viruses, if a phone is contaminated by a BT-based virus, it automatically pursuits another phone through available Bluetooth services within a particular 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. A BT-based virus can only infect its geographically local neighbors with the same OS within a certain range. These geographically local neighbors are homogeneous for a BT-based virus since an infected phone randomly selects a susceptible phone as its target at a time.

VIII. **STRATEGIES**

A. 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. 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. This section examines the performance of the AOC-based preimmunization strategy [3], which has been restraining SMS-based virus propagation. In order to cut the epidemic path and reduce the infection rate as low as possible, the AOC-based preimmunization strategy selects a group of phones, with the highest degrees and larger transmission capabilities in a mobile network, for protection (e.g., patching). Furthermore, we evaluate the robustness and scalability of the AOC-based preimmunization strategy and show how it works with large-scale and/or highly dynamic mobile networks. In the real world, different companies may release security patches at different time because of the response delays for new viruses. Therefore, different from our previous work in, 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. This result suggests that security software companies should improve their abilities to detect viruses and release patches as fast as possible. That is because a certain number of immunized phones can divide the whole network into small blocks and cut the epidemic paths, and then restrain virus propagation.

B. Adaptive Patch Dissemination Strategy

However, 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.

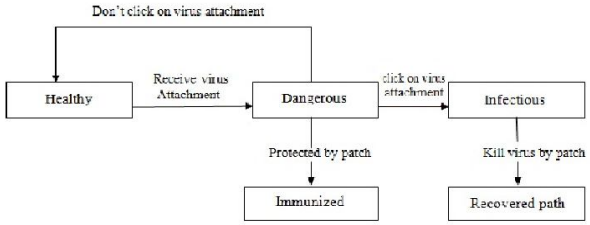

Fig. 2. The state transition of smartphones in the AOC-Based dissemination Strategy

Different from the moving behavior of immunization entities , a dissemination entity will still move to another no resided highly connected neighbor (i.e., this neighbor is not resided before) at the next time step even though it has already resided in the highest degree phone in a network. Fig. 2 introduces the state transition of phones in the face of SMS-based viruses[1]:

- If a phone receives a message with a virus embedded attachment, it is likely to be infected, i.e., Healthy! Dangerous;
- If a phone has received an infected message, there are two types of operational behavior: the user of this phone does not open the infected message, Dangerous! Healthy; or open it, Dangerous! Infectious;
- The autonomous entities are deployed into a network for distributing patches to phones. If an infected phone receives the patch, it will recover from the infected state, i.e., Infectious! Recovered.
- If a phone is in Healthy or Dangerous state, the patch will protect the phone from the attacks of viruses, i.e., Dangerous! Immunized, Healthy! Immunized.

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.

IX. CONCLUSION AND FUTURE WORK

In this paper, we have showed a two-layer network model for analyzing the spreading of SMS-based and BT-based viruses [3]. Our result shows that we protect the smartphones in spreading of viruses. This is support in android smartphones and accurately detect and delete the virus of the content before enter into the mobile operating system. Future work can be enhanced the virus content of data's enter into the smartphones through Bluetooth and SMS channels it automatically filter the virus and data separately and delete the virus but not the data.

REFERENCES

[1] C.Gao and J. Liu, "Modeling and Restraining Mobile Virus Propagation (Supplementary File)," IEEE Trans, Mobile Computing, vol.12, pp. 529-541, mar 2013.

[2] C.Gao, J.Liu, and N.Zhong, "Network Immunization with Distributed Autonomy-Oriented Entities", IEEE Trans. Parallel and Distributed Systems, vol.22, no.7, pp. 1222-1229, July 2011.

[3] C,Gao and J.Liu, " Modeling and Predicting the Dynamics of Mobile Virus Spread Affected by Human Behavior", Proc. IEEE 12th Int'l Symp. A World of Wireless, Mobile and Multimedia Networks (WoWMoM '11), pp, 1-9,2011.

[4] F.Li,Y.Yang, and J.Wu,"CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks," Proc. IEEE INFOCOM, pp.2811-2819,2010.

[5] F.Li,Y.Yang, and J.Wu,"CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks," Proc. IEEE INFOCOM, pp.2811-2819,2010.

[6] 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.

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

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

[9] 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.

[10] 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.

[11] M.C. Gonzalez, C.A.Hidalgo, and A.L.Barabasi,"Understanding Individual Human Mobility Patterns",Nature, vol.453, no.7196,pp. 779-782,2008.

[12] 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.

[13] J.Liu, " Autonomy-Oriented Computing(AOC): The Nature and Implications of a Paradigm for Self-Organized Computing."Proc. Fourth Int'l Conf.Natural Computation(ICNC '08),pp.3-11,2008.

[14] J.Cheng, 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.

[15] Jiming Liu, Xiaolong Jin, Kwok ching Tsui, " Autonomous Oriented Computing(AOC): Formulating Computational Systems with Autonomous Components." IEEE Trans on system, man and cybernetics,pp.879-902,nov 2005.

