Proceedings of the
International Conference on E-Commerce
ICoEC 2015
20-22 October 2015. Kuching, Sarawak, MALAYSIA

Available online at www.icoec.my

The Influence of User Mobility in Mobile Virus Propagation: An Enterprise Mobile Security Perspective

Suhizaz Sudin[a]*, R Badlishah Ahmad [a], Azremi Abdullah Al Hadi[a], Phak Len Eh Kan[a], Syed Zulkarnain Syed Idrus[b], Mohd Mustafa AlBakri Abdullah [c]

[a]*School of Computer and Communication Engineering (SCCE), Universiti Malaysia Perlis*
[b]*School of Human Development and Technocommunication (iKOM)*
[c]*Center of Excellence Geopolymer & Green Technology (CEGeoTech), School of Material Engineering, Universiti Malaysia Perlis*

Abstract: *In this paper, the authors review the usage of mobile devices in the enterprise and also the major impact from the infected mobile devices. Then the authors highlight the virus threat to enterprise mobile security and how critical the problems are. The authors then discuss the mobile virus infection dynamics which are the Bluetooth infections, mobile emails infections and mobile internet infections which are the threats to the enterprise mobile security. Then the authors discuss on the influences of user mobility issue in spreading mobile viruses before concluded this article.*

Keywords: Mobile network, virus threat, user mobility

1. INTRODUCTION

The growing ubiquity of mobile computing networks is leading to new security challenges. As fixed wired computer networks became more popular, the amount of malicious code which used them as its transmission mechanism was increasing. Similarly, as mobile networks become more common, mobile network devices become a target for virus writers (Mickens & Noble, 2005) . Just as boot sector viruses were replaced by viruses that propagated via electronic attachments and other Internet vectors (Bridwell, 2004), the rise of widespread mobile networking leads to the emergence of new types of malicious code.

The blend of susceptible platforms (Mulliner, Vigna, Dagon, & Lee, 2006), security-unaware users and consumers (Wang, 2005), and the explosive growth in the numbers potential victims will unavoidably attract propagating viruses (Dagon, Martin, & Starner, 2004; Hypponen, 2006). The potential damage from mobile viruses is ranging from simple vandalism to identity and information theft, mobile device spam, denial-of-service attacks (DDoS) and mobile bots. The potential effects of virulent malware proliferation on consumers and mobile device providers are acute, including fraudulent charges to customers, aggravation of mobile services, public relations failures, and ultimately - loss of revenue for mobile device providers (Fleizach, Liljenstam, Johansson, M. Voelker, & Mehes, 2007).

In this paper, we address the background of the problem: risks resulting from mobile device usage to the enterprise and the mobile virus infection dynamics. Then, we discuss how user mobility helps in spreading the viruses in enterprise mobile environment before concluded our work.

2. BACKGROUND OF THE PROBLEM

2.1 Security Vulnerabilities Resulting from Mobile Access

Mobile devices have evolved for years from analog traditional walkie-talkies to full-scale internet-enabled computers. These have been upgraded and enhanced. Many are even more powerful than personal computers of the late 1990s. These devices are increasingly moving toward an (Dagon, Martin,

*Corresponding author.
E-mail address: suhizaz@unimap.edu.my

& Starner, 2004) "always connected" form of connectivity, where users can obtain data continuously through the Internet Service Provider. Increasingly, mobile devices also incorporate IEEE 802-based networking technologies such as Wireless Fidelity (Wi-Fi) and Bluetooth (Dagon, Martin, & Starner, 2004), which enable direct connections between mobile devices and make them intermittent members of nearby fixed networks. Increases in connectivity compound the potential security problems.

Users and consumers might think that because their mobile devices are constantly with them, they are more secure compared to PCs. Users and consumers tend to carry false sense of security with mobile devices, leading them to trust these devices with sensitive and personal information. Mobile device attacks can harm a person's most private data such as numbers, names, contacts, appointments, passwords, and even identities (Ruitenbeek, Courtney, H. Sanders, & Stevens, 2007). Even though such personal information is also present on fixed networked PCs, it's more diluted, distributed, and less organized than it is on mobile devices. As the result, private information on mobile devices is easy for intruders to find (Dagon, Martin, & Starner, 2004).

The evolving attacks on mobile devices not only affect individual who own mobile devices but also affect large organizations where mobile devices are employed. Viveros, (2003) and Jain, Asgekar, Chalke, Kumar, & Rao (2006) identified major impacts on the organizations resulting from infected mobile devices. First, organizations may experience financial loss when viruses on mobile devices make unnecessary calls.

Second, work performance of employees relying on infected devices may decrease because processing capabilities of infected devices tend to deteriorate. Viruses create unnecessary processes and files. This uses up available memory and delays processing.

Third, infected devices may allow remote control by unauthorized users. Important data may be stolen (Ruitenbeek, Courtney, H. Sanders, & Stevens, 2007), such as personal information, customer information, and mobile banking information.

2.2 End User Security Behaviours

While in the past information security research primarily focused on technology-based countermeasures, there is a growing interest in the role of user security behaviours. Albrechtsen (2007), reported a qualitative study of users' perceptions of information security at an IT company. The study revealed a wide range of attitudes, with many of the respondents acknowledging low security awareness.

Stanton, Stam, Mastrangelo, & Jolton, (2005) introduced taxonomy of end user security behaviours, and validated it by conducting a large-scale survey of password-related behaviours. The taxonomy is presented as two dimensional maps with user technical sophistication and user intentionality as dimensions.

D'Arcy & Hovav (2007) conducted a survey intended to assess the impact of security countermeasures (security policies, security awareness programs, computer monitoring, and preventive security software) on information systems misuse intention. Security awareness programs were demonstrated to have the greatest impact.

Ruighaver, Maynard, & Chang (2006) proposed a framework for security-relevant aspects of organizational culture, based on a multiple case study. The framework suggests that user security behaviour is ultimately determined by organizational culture.

August & Tunca (2006) conducted a simulation study of the impact of economic incentives on user behaviour with respect to applying security patches to software. The study compares patching policies, to suggest the ones that maximize value generated from the software and vendor profits.

Aron, O'Leary, Gove, Azadegan, & Schneider (2002) addressed the impact of user awareness of an impending virus threat on computer security. They conducted a survey and used the results as a basis for creating a simulation model. High levels of notification were associated with considerable reduction of virus threat.

3. MOBILE VIRUS INFECTION DYNAMICS

Mobile devices offer a fertile ground for the development and spread of malicious code. Therefore in this paper, we focused on the mobile viruses dynamics as our main concern of mobile security issues.

Users might think that because their mobile devices are constantly with them, they are more secure compared to PCs. But, physical control offers little protection against malware. The false sense of

security may lead users to trust these devices with sensitive and personal information. Attacks targeting mobile devices may compromise private data such as phone numbers, names, appointments, passwords, and even identities. Even though such personal information is also present on fixed networked PCs, it's more diluted and less organized than it tends to be on mobile devices. As the result, attackers targeting mobile devices can easily locate private information.

3.1 Bluetooth Infection Dynamics

Bluetooth, originally created as a cable replacement alternative, is a short-range radio technology that connects mobile devices wirelessly. It makes itself different from other similar radio technologies such as IEEE 802.11 by operating at low power usage and cost. Bluetooth has been used for ranges of applications, including wireless entertainment devices, peer-to-peer file exchanges, and data synchronization.

There are two ways in which a device can initiate a Bluetooth connection by:

1. Directly contacting the address of another device,
2. Broadcasting "inquiry" messages to discover other devices.

Most of today's Bluetooth devices provide the user with the option to make them discoverable. Upon receiving an "inquiry" message, a discoverable Bluetooth device will reply with an answer that includes its user-configurable device name and its device type.

A work by Carettoni, Merloni, & Zanero (2007) has found out that a popular form of virus attack is to use a carefully chosen device name when pairing with the target device. To complete the pairing process, the target device must ask for its user's permission while displaying the attacking device's name. A well-chosen device name "Secret Admirer") could convince the user to authorize the pairing. This type of attacks is known by the term of "bluejacking". More recently, there have been reports of a Bluetooth virus outbreak.

Cabir is a software program that repeatedly scans for nearby Bluetooth-enabled devices. Upon discovering a new device, Cabir transmits an installation file disguised as a security management utility. Once target users accept the incoming file, their devices become infected (Mickens & Noble, 2005). Because it requires user intervention, Cabir has not been able to reach and infect a large device population. However, there are reports of Cabir-infected Bluetooth devices found in stores selling cell-phones and cell-phone accessories.

Several attacks exploiting Bluetooth implementation vulnerabilities have been reported. In these attacks, a malicious device can gain access to data on a vulnerable device, issue AT modem commands, or establish an unauthorized "pairing" relationship. As an example, a study from Bose & G. Shin (2006) has measured the prevalence of some of these software vulnerabilities in a trace of Bluetooth-enabled phones captured at CeBIT 2004, a large IT exhibition taking place in Hanover, Germany. Their trace has captured 1,269 discoverable Bluetooth devices over a period of four days. This study found that many devices (i.e. between 6% and 33% depending on the phone type) exhibit exploitable software vulnerabilities. This software vulnerability allowed the authors to retrieve the Bluetooth devices' address books.

An infected device can easily transfers the virus to another mobile device via Bluetooth. Since the behaviour of software vulnerabilities can create unauthorized pairing between Bluetooth devices, the virus can be transferred to another device. Regardless the behaviour of users in transferring files, synchronizing calendars and address book, the mitigation in likely to happen. Once connection is paired for transferring files, synchronizing calendars and address book, the mobile device is vulnerable to the mobile virus.

The longer time taken to accomplish the said task, the higher possibilities of infection occurs. The frequency of vulnerable task performed using mobile device also helps in mitigates virus.

Another issue to consider while analysing the Bluetooth infection dynamics is the social interaction between users using mobile device. Social interactions can be divided to two main categories (Miklas, Gollu, Chan, Saroiu, Gummadi, & de Lara, 2007). One category is interactions between strangers that are people who meet that are people who meet sporadically. The other category is interactions between friends, that is people who meet more regularly and for longer periods of time. If the user interact with friends, the chances of viruses mitigate is higher compared to interact with strangers.

3.2 Mobile Internet Infection Dynamics

As mobile device become more advance and sophisticated, they are capable of surfing the Internet, sending emails and downloading software like most PCs do. The establishment connectivity between Internet and phone networks also boost the usage of mobile networks since it can works as good or even better than personal computer with the mobile capabilities.

Therefore, the mobile user demanding of rich data while accessing the internet makes the mobile devices a popular targets for viruses hence the security is low. The mobile device developer also tend to develop devices that capable or producing the rich data for users. This is achieved by producing the mobile devices that capable of a processing rich data. Rich data sometimes are sensitive and personal, so it becomes a target for attack to occur. Based on work from Fang, Chan, Brzezinski, & Xu (2006), mobile users more likely to use mobile internet to perform general task suck as reading news and entertainment, transactional task such as online trading and gaming task.

The internet infection also influences by the time mobile devices is connected to the Internet Service Provider (ISP). The longer devices is connected the higher possibilities the device being infected. Frequency of usage also influences the virus mitigation. Frequent usage makes device more likely to be infected by viruses. There are two major form of virus attack via Internet access is the virus in a file and social network virus.

3.3 Virus in an Infected File

Internet services coupled with always on connectivity to the Internet that mobile network allows, the technology is potentially vulnerable to increasing number of virus attack and some downloaded files may be infected. A work from Guo, Wang, & Zhu (2004) mentioned that enabling interoperation with the Internet bring tremendous new services and extensive information access, the virus threat resulted from the Internet connection also need to be look into. The user sometimes doesn't notice that their mobile device is connected to the Internet Service provider or another Bluetooth enable device. This make their device is enable for attack since the connectivity is always established between two parties.

Ruitenbeek, Courtney, H. Sanders, and Stevens (2007), found that mobile devices can be infected by downloading infected files using the devices internet browser. The current mobile device is equipped with browser that allows users to download application through the internet. This makes the devices vulnerable to attack if the user accidentally downloads the infected file from other entrusted parties. Sometime the user doesn't aware even the file is infected or not. By the time user realize the device is infected, the viruses already tend to affect the device performance, create unnecessary processes and tend to make the device unusable.

The infected downloaded file is not restricted to application files but also the gaming file. For example, the first Symbian based Trojan has recently been discovered in a popular downloaded game software. Since current high capabilities mobile devices becoming more popular in market, the trend of game downloading also is increasing. There are many websites offer free downloading for gaming files, so the possibility of mobile devices being infected also increased.

3.4 Social Network Virus

While connecting to the internet also, user is exposed to social network viruses. The viruses' attempts to fraudulently obtain sensitive personal information from a node by imitate the appearance of a trusted third party. As an example of attack, the viruses will create a message or pop-up identifying itself as a large banking organization or famous online auction site acquire mobile user to disclose their personal or important data. Once the user click or enter the required data, the viruses will propagate into the node.

3.5 Mobile Email Virus

As most of Smartphones can be used to surf the web, so do the emails. Mobile emails have become tremendous trends in current working environment. The emerging of Smartphone email technology also can helps virus mitigation.

Viruses can use mobile email as a propagation vector is 2 ways:

1. Sending email at high rate
In order for a virus to spread it needs to create a fake email and send itself to different address in the address book. This email is send at high rate and affects the network traffic.

2. Attachments

Mobile virus also can propagate through attachments in email sends and receives through mobile device. User behaviour in opening an email attachment in mobile device helps in propagates viruses. Anonymous attachments are attached together with the email and send to recipient with 'friendly email subjects'. The recipient list is compromised by viruses and the email will auto generate by the virus itself. Comparing to Bluetooth infection vector, the email infection vector is much bigger. The time taken to receive and download emails from mail server also helps in propagating virus to mobile devices. The longer time taken to download emails, the higher possibilities of mobile device being infected.

4. THE INFLUENCE OF USER MOBILITY

The user mobility means the user accesses its work environment based on his records information by any mobile terminal devices. And the user can do the same work at different places. It is said that the mobile user can store his work state in a place and he can continue his previous work in a new place he moved. Mobility is the essential features of mobile computing. In generally, the research about mobility includes several directions, such as user mobility, terminal mobility and resources assess mobility.

In mobile networks, there are no such as user-triggered event. Generally, mobile nodes automatically detect and join local mobile networks whilst the user does not necessarily even know it happen. Mobile networks are becoming increasingly common, and mobile advocates are working diligently towards a world with nearly ubiquitous coverage and transparent mobility from one physical network to another.

According to Wei, Zhao-Hui, Zeng-Qiang, & Zhu-Zhi (2007) the mobility of mobile devices as well as users influence the virus propagation in two states namely intra-cluster and inter cluster. Intra cluster here means within one Mobile Personal Area Network (MPAN). Inter cluster explain how infected device from one MPAN propagate to another MPAN and infect another device. Mobile nodes automatically detect and join another MPAN whilst the user does not necessarily even know it happen. Mobile networks are becoming increasingly common, and mobile advocates are working diligently towards a world with nearly ubiquitous coverage and transparent mobility from one physical network to another. Therefore, user mobility and sharing of access points are the main drivers behind the mitigation of mobile worm (Anderson, Eustice, Markstrum, Hansen, & Reiher, 2005) and mobility also does provide a back door even into or else protected networks, and mobile networks is to make the problem.

Arbaugh (2003), also claims that device can be infected when move from one physical connection to another physical connection. If the mobile node is infected, there is a probability of the new physical connection being infected as well. For example, a sales person transferring data using Wireless Local Area Network (WLAN), sending attachments via emails or downloading a file from the enterprise server to his laptop without realizing the files are already infected. Then he transfers the same file to his smart phone using Bluetooth connections and the worm propagates to his smart phone and has the ability to infect another device which is Bluetooth enable.

An enterprise can be protected by any means of security such as firewalls and anti-viruses. But the propagation still has a chance when user mobile from the enterprise connection to home connection because many home user connects to another MPAN via cable or DSL without protection. User moderately mobile, for example using laptop while travelling and use Virtual Private Network to connect to enterprise when at home. This mobility creates a potential vector for virus propagation.

Enterprise mobile networks are becoming increasingly common and there is a clear trend towards a world with nearly ubiquitous coverage. As the user moves around, the same device is likely to be exposed to a variety of networks with different security standards, resulting in security risks. Problems acquired on less secure networks can be carried over to more secure networks bypassing their security mechanisms (Anderson, Eustice, Markstrum, Hansen, & Reiher, 2005).

The user space also plays a role when discussing user mobility. The place where the infection device located makes different in virus mitigation. For example, if an infected mobile device is sitting in the corner of a room, the infection vector is smaller compared to the infected device is sitting in the middle of the room.

5. CONCLUSION

The usage of mobile devices in enterprise invites new challenge in network security. Since the demand of mobile businesses is increasing, virus

threat on mobile devices needs to be considered by mobile user. As the development of new mobile technology is growing rapidly, the devices become more sophisticated and this will create new threat and attract virus writers. The advance mobile devices store important data and sensitive information in the device. The virus threat can create many losses to the enterprise by disrupting the device operations. Bluetooth is becoming a popular medium in transferring data among mobile user and this makes the Bluetooth enable devices vulnerable to the mobile viruses. User interactions and behaviours also play an important role in the virus threat. The user mobility, user connecting time and user actions when downloading or receiving infected files are taken into account when exploring the mobile virus threat.

In our further research we intend to investigate the interaction between different spreading mechanisms and the effectiveness of various security policies. This will rely on a survey of user behaviour that will be used to determine the range of values for the model parameters.

REFERENCES

Albrechtsen, A. (2007). A qualitative study of users' view of information security. Computers & security, 276-289.

Anderson, E., Eustice, K., Markstrum, S., Hansen, M., & Reiher, P. (2005). Mobile Contagion: Simulation of Infection & Defense. 19th Workshop on Principles of Advanced and Distributed Simulation, 2005.

Arbaugh, W. A. (2003). The Convergence of Ubiquity: The Future of Wireless Security. 2003 USENIX Annual Technical Conference.

Aron, J., O'Leary, M., Gove, R., Azadegan, S., & Schneider, M. (2002). The benefits of a notification process in addressing the worsening computer virus problem: Results of a survey and a simulation model. Computers & Security, 142-163.

August, T., & Tunca, T. (2006). Network software security and user incentives. Management Science, 1703-1720.

Bose, A., & G. Shin, K. (2006). On Mobile Viruses Exploiting Messaging and Bluetooth Services. SecureComm and Workshops, 2006.

Bridwell, L. (2004). Ninth Annual Computer Virus Prevalence Survey. ICSA Laboratory.

Broustis, I., Faloutsos, M., & Krishnamurthy, S. (2006). Overcoming a Challenge of Security in a Mobile Environment. Performance Computing and Communication Conference.

Bryman, A., & Bell, E. (2007). Business research methods. Oxford university press.

Carettoni, L., Merloni, C., & Zanero, S. (2007). Studying Bluetooth Malware Propagation. IEEE SECURITY & PRIVACY.

Carlson, P., & G.B., D. (1998). An investigation of media selection among directors and managers: From "self" to "other" orientation. MIS Quarterly, 335-362.

Chan, S.-C., & Lu, M.-T. (2004). Understanding Internet Banking Adoption and Use Behaviour: A Hong Kong Perspective. Journal of Global Information Management, 21-43.

Coursen, S. (2007). The future of mobile malware. Network Security, 7-11.

Dagon, D., Martin, T., & Starner, T. (2004). Mobile phones as computing devices: the viruses are coming! IEEE Pervasive Computing, 11-15.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. Communications of the ACM, 113-117.

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: A comparison of two theoretical models. Management Science, 982-1003.

Davis, J., Eisenhardt, K., & Bingham, C. (2007). Developing theory through simulation methods. Academy of Management Review, 480-499.

Fang, X., Chan, S., Brzezinski, J., & Xu, S. (2006). Moderating effects of task type on wireless technology acceptance. Journal of Management Information Systems, 123-157.

Fleizach, C., Liljenstam, M., Johansson, P., M. Voelker, G., & Mehes, A. (2007). Can You Infect Me Now? Malware Propagation in Mobile Phone Networks. WORM'07.

Guo, C., Wang, H. J., & Zhu, W. (2004). Smart-Phone Attack and Defenses. Proceedings of HotNets III.

Harrison, J., Lin, Z., & Carley, K. (2007). Simulation modeling in organizational and management research. Academy of Management Review, 1229-1245.

Hsu, M.-H., & Chiu, C.-M. (2004). Predicting electronic service continuance with a decomposed theory of planned behaviour. Behaviour & Information Technology, 359-373.

Hypponen, M. (2006). Malware Goes Mobile. Scientific American, 70-77.

Jain, A. K., Asgekar, A., Chalke, J., Kumar, M., & Rao, R. (2006). Mobile Worms and Viruses. Mumbai: Kanwal Rekhi School of Information Technology.

Law, A. (2007). Simulation Modeling & Analysis. McGraw Hill.

Leavitt, N. (2005). Mobile phones: The next frontier for hackers. Computer.

Mannan, M., & van Oorschot, P. C. (2005). On Instant Messaging Worms, Analysis and. 2005 ACM workshop on Rapid Malcode, 2005.

Mickens, J. W., & Noble, B. D. (2007). Analytical Model for Epidemics in Mobile Networks. Third IEEE International Conference on Wireless and Mobile Computing.

Mickens, J., & Noble, B. (2005). Modeling epidemic spreading in mobile environments. WiSE'05, (pp. 77-86). Cologne, Germany.

Miklas, A. G., Gollu, K. K., Chan, K. K., Saroiu, S., Gummadi, K. P., & de Lara, E. (2007). Exploiting Social Interactions in Mobile Systems. UbiComp, Springer 2007.

Mulliner, C., Vigna, G., Dagon, D., & Lee, W. (2006). Using Labeling to Prevent Cross-Service Attacks against Smart Phones. DIMVA '06.

Nekovee, M. (2007). Worm Epidemics in Wireless Adhoc Networks. New Journal of Physics.

Ruighaver, A., Maynard, S., & Chang, S. (2006). Organizational security culture: Extending the end-user perspective. Computers & Security, 56-62.

Ruitenbeek, E. V., Courtney, T., H. Sanders, W., & Stevens, F. (2007). Quantifying the Effectiveness of Mobile Phone Virus Response Mechanisms. 37th AnnualIEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07).

Sarat, S., & Terzis, A. (2007). On Using Mobility to Propagate Malware. Modelling & Optimisation Adhoc and Wireless Network Workshop, (pp. 1-8). Limassol, Cyprus.

Shirey, C. B. (2004). Modeling the Spread and Prevention of Malicious. Florida: Florida Institute of Technology.

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & security, 124-133.

Viveros, S. (2003). The Economic Impact of Malicious Code in Wireless Mobile Networks. The Institution of Electrical Engineers.

Wang, R. (2005). Symbian OS-Mysterious playground for new malware. Virus Bulletin.

Wei, X., Zhao-Hui, L., Zeng-Qiang, C., & Zhu-Zhi, Y. (2007). The Influence of Smart Phone's Mobility on Bluetooth Worm Propagation. Wireless Communications, Networking and Mobile Computing.

Zheng, H., Li, D., & Gao, Z. (2006). An Epidemic Model of Mobile Phone Virus. 1st International Conference of Pervasive Computing and Application.