A Model of Virus Infection Dynamics in Mobile Personal Area Network

Suhizaz Sudin[1], R Badlishah Ahmad [2], Syed Zulkarnain Syed Idrus[2]
[1]*School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia*.
[2]*School of Human Development and Technocommunication, Universiti Malaysia Perlis, Malaysia.*
suhizaz@unimap.edu.my

***Abstract*—In this paper, the authors explore the mobile network security focused on the virus threat. Firstly, the authors explain the importance of mobile network security which sometimes not really takes into considerations by users. This paper then explains the virus threat of mobile devices virus where it explains how the viruses spread. The threats can be in three major forms namely the virus spreading via mobile personal area network, virus spreading via internet access and virus spreading via messaging. Lastly a model explains the dynamics of the infection on Mobile Network is introduced.**

***Index Terms*—Mobile Devices; Mobile Network; Mobile Personal Area Network; Vulnerabilities.**

I. INTRODUCTION

With the continuing production of portable wireless devices such as laptops and Personal Digital Assistants (PDAs), mobile networks are becoming an important part of our everyday networking infrastructure. However, the growth of mobile computing network is leading to new security challenges. As the fixed wired network became more popular, the amount of malicious code which used the Internet as its transmission mechanism is increasing. Similarly, as mobile networks become more in use, the mobile network devices as well become a massive target for virus writers [1]. Just as boot sector viruses were replaced by viruses that infected and propagate through electronic attachments and other Internet vectors [2], the rise of widespread mobile networking will focus on new types of malicious code. Moreover, IBM's 2004 Business Security Report forecast that malware propagation amongst mobile devices would be an increasingly dangerous problem.

Mobile devices are the new boundary for malicious code. The blend of susceptible platforms [3] distrusting users and consumers [4], and explosive growth in potential victims will unavoidably attract propagating viruses [5]. Ranging from simple vandalism to identity and information theft, mobile device spam, denial-of-service attacks (DDoS) and potentially mobile bots, are the possible damages that can be done by mobile viruses. The potential effects of virulent malware proliferation on consumers and mobile device providers are acute, including extreme charges to customers, aggravation of mobile device services, public relations failures, and ultimately loss of revenue for mobile device providers [6].

As the usage of mobile device in increasing in businesses, the security is one of the important aspects that need to be looked into. Several reasons are identified that makes mobile networks are more vulnerable to malicious attacks than fixed networks:

The nature of broadcast medium, which exposes information to a passive listener.

- The lack of an authoritative certification source.
- The limited battery supply, which to exclude overhead and computational rigorous solutions.
- The mobility.

These reasons make tracing infected node more complex. Even though many detection and prevention methods have been developed for fixed networks, the above differences of mobile networks need new security practices such as network topology that change dynamically, creates new set of security challenges [7]. The main idea here is that a node may disperse its true identity, but it can give the false location. Consequently, it can affect the network by modifying the transmission routes, monitoring all secured information etc. In detail, the widely common use of wireless medium makes mobile networks tend to be infected for active and passive attacks [4].

Passive attacks mean the attacker does not actively threaten the network, but it mainly performs as a spy, and identifies the loophole of the network. A passive attacker also can trigger an active attack, by passing this information to active attackers. In active attacks, the attacker can disperse various topology information, drop or modify transmission packets, fabricate false messages or flood the existing network.

Generally, most attacks or threat can be categorized into either one of the above cases. As a result, any defense mechanism requires extensive evidence gathering to make the defense system works well.

II. VIRUS THREAT ON MOBILE DEVICE

[8] identify four main types of mobile viruses' attack using which can be distinguished based on their damages that caused:

- The viruses make the mobile device partially or totally can't be used.
- The viruses generate unwanted messages sending to unknown recipient, fake call and increasing in data billing.
- The viruses disclose private data to unauthorized parties.
- The viruses try to attract the user to disclose private data then stole the sensitive information.

[8] also again named preconditions for serious attacks to develop:

- Very few significant software platforms that make the knowledge to accumulate. This made attackers easier to write new code.

- Development tools are publicly available and well-documented for any particular platforms that create the competence in the invention of new mobile viruses.
- Platform susceptibilities, like errors on coding provide holes to for the viruses to mitigate without user's notice.

Since the mobile devices said to be less secure compared to fixed network, it has been targeted by the virus writer. The code will perform some form of scan trying to locate target machines which are susceptible to infection and attempt to exploit any target machines found. If successful, the exploit will concede the mobile code to replicate itself to the target machine, which will itself begin its own exploit or transfer cycle [5].

However, security concerns over viruses that spread on mobile networks are hard to overstate: once a virus has compromised a device, it can easily place fake calls, distribute spam emails, and steal sensitive or private information that is stored on the device [9]. More enhanced version of viruses might derive control over a huge number of mobile devices in which they implant malicious code. These make mobile botnets could be in place to execute Distributed Denial of Service (DDoS) charge against mobile base stations, cellular switches, specific IP addresses or phone numbers such as emergency numbers [3].

Bluetooth as one of popular communication medium, was originally created as a cable replacement alternative, is a short-range radio technology that connects wireless mobile devices. It makes itself different from other similar radio technologies such as IEEE 802.11 by operating at low power usage and cost. Bluetooth has a huge range of applications, including wireless entertainment devices, peer-to-peer file exchanges, and data synchronization. The market for Bluetooth devices has been growing rapidly in recent years. In 2005, there are 272 million Bluetooth devices have been shipped worldwide, whereas only half of it in 2004 [10].

The widespread usage of Bluetooth devices has attracted the virus propagation. [11] state that the first mobile device virus named Cabir which hit mobile devices in 2004, used Bluetooth connectivity channels on devices running the Symbian Operating System to mitigate onto other devices. They also mention that the Cabir successor Mabir and the CommWarrior are both have the abilities of spreading themselves through the Bluetooth interfaces of mobile devices. While these viruses created considerable problems by draining the batteries of infected devices resulted from intensive scanning operations and probably also by congesting the mobile network transmission, they have not imposed any serious security failure as none of them actually carried a malignant payload.

Malicious viruses place attack on the device running on Symbian OS due to the popularity and advanced features. The virus can scan for in-range Bluetooth-enable device using proximity scanning. A recent study conducted estimates that by 2008, there will be more than 922 million Bluetooth-enable devices worldwide which make these devices being targeted by the viruses writer [9]. Here we highlight a few virus spreading mechanism in mobile network namely the Mobile Personal Area Network, Internet Access and Messaging.

III. Mobile Personal Area Network

[12] explained that a compromised mobile device could actively scan and detect peer devices through its Mobile Personal Area Networks (MPAN) interface such as Bluetooth or UWB (ultra wideband). Due to the mobility, they can detect new node at different locations.

MPAN is not restricted for mobile device only; it also can contain a fixed device as well. Virus can mitigate from one device to another within this cluster from one cluster to another.

Mobile device also exposed to the risk of being infected by a fixed device in the same cluster. In an organization, both mobile and fixed devices are used for certain purposes. Mobile device is used by the mobile workers whereas fixed devices normally used by the enterprise system. Again, once the device is connected, the risk of virus propagation is there.

From the report of Network Associates & Mercer, viruses propagate on mobile devices because of the current protection of mobile network is poor or non-existent, the computing power is increased, the standardization of networks and devices are becoming more connected [13]. Since the usage of mobile device is increasing, many applications are developed to be used in mobile environment. Many organizations tend to use mobile devices in their daily operation. These mobile devices again will be connected to the organization fixed network in term of updating data, managing resources and retrieving messages. By placing a virus on the mobile device, an attacker can take control of fixed wired PCs and vice versa [8].

A. The Impact of User Mobility

According to [14] 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 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 [11] and mobility also does provide a backdoor even into or else protected networks, and mobile networks is to make the problem.

[4] also claims that device can be infected when moving 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 salesperson transferring data using Wireless Local Area Network (WLAN) from the enterprise server to his laptop without realizing the files are already infected. Then he transfers the same file to his smartphone using Bluetooth connections and the worm propagates to his smartphone and has the ability to infect another device which is Bluetooth enabled.

An enterprise can be protected by any means of security such as firewalls and anti-viruses. But the propagation still has a chance when using 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.

B. Internet Access

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

Therefore, the mobile user demanding of rich data [2] while accessing the internets makes the mobile devices a popular target for viruses hence the security is low. The mobile device developer also tends to develop devices that capable of 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. There are two major form of virus attacks via Internet access; the virus in an attachment and social network virus.

C. Virus in an Infected Attachment Files

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 [7].

[10] 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 looked into. The user sometimes doesn't notice that their mobile device is connected to the Internet Service provider or another Bluetooth enabled device. This makes their device enabled for attack since the connectivity is always established between two parties.

According to [15], 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. Sometimes the user doesn't seem 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 [10]. 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 increasing.

D. Social Network Virus

While connecting to the internet also, user is exposed to social network viruses. The viruses attempt to fraudulently obtain sensitive personal information from a node by imitating the appearance of a trusted third party [16]. 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 clicks or enters the required data, the viruses will propagate into the node.

The study from [16] also claims that about 19% of all those surveyed reported having clicked on a link in an untrusting email or messages, and 3% admitted to giving up financial or personal information. It is worth noting that propagation of social viruses is getting better. In conjunction with trends in other online crimes, it is inevitable that future generations of social virus attacks will incorporate greater elements of context to become more effective and thus more dangerous for society.

E. Messaging

Another popular medium for threats is the messaging. It can happen from one mobile device to another, fixed device to mobile device and mobile device to a fixed device. There to major form of infection that can occur through messaging; worm infection and trojans infection.

F. Worm Infection

The worm infection is autonomous. The user's behavior of transferring message or information through short-range Bluetooth [6] also influences the attack of worm to mobile device. The Bluetooth technology becoming a most popular transfer medium since most of current mobile devices are equipped with the Bluetooth technology and there are a lot of cheap Bluetooth portable dongle in market that can be used with fixed devices.

For example, the Brador virus infects Pocket PCs running Windows CE, creating a backdoor which allocates a remote attacker unlimited access to the device. The Cabir worm infects cell phones running the Symbian operating system. It takes control of the phone's Bluetooth interfacing; Cabir continuously scans for other Bluetooth-enabled devices and tries to contaminate any such device which enters the scanning range. The Mabir and Symbos Comwar worms use comparable scanning techniques and also spread via MMS messages [1].

The entry-level mobile devices which don't have the internet connectivity make fully used of these capabilities to transfer files and share application with peers. Worm which use Bluetooth as the transfer medium use proximity scanning to scan the enable devices than mitigate itself without the user even notice. Once the connection is established between two parties, the mitigation occurs and creates new harm to the infected nodes.

G. Trojans Infection

Trojan infection needs human action to mitigate. A human action such as opening attachment file in a message is a propagation vector for trojans infection via messaging.

According to [3], Short Message Services (SMS), a paging-like service for mobile devices works at 168 characters which the data capacity is very small thus may not be useful to mitigating mobile viruses, but it has the ability to generate enormous quantities of SMS traffic. Multimedia Messaging System (MMS) is an advanced type of SMS for mobile device that based on General Packet Radio Service technology. MMS messages are similar to text messages between mobile devices, but MMS messages are capable of including attached files, much like email with attached files MMS which carries up to 50Kb of data is a target medium for virus writer. The

data allows in MMS is large enough to carry viruses and mitigate to the receiving node. The viruses can infect receiving node when user is opening the multimedia files sent through MMS [17].

SMS address spoofing also is an emerging threat that allows viruses to make an SMS message pop-up as though it came from a different user and network. Many mobile system providers allow Internet users to send short text messages directly to their mobile device subscribers via a web-based SMS gateway. When not designed correctly, such a gateway opens the door to send large volumes of SMS spasm and other malicious content [18].

IV. The Infection Dynamics Model

We have come out with a model illustrating the virus threat scenarios of a mobile network. A threat can be either online connected to the Internet or offline with the Internet. It also can be either within the MPAN or inter-MPAN.

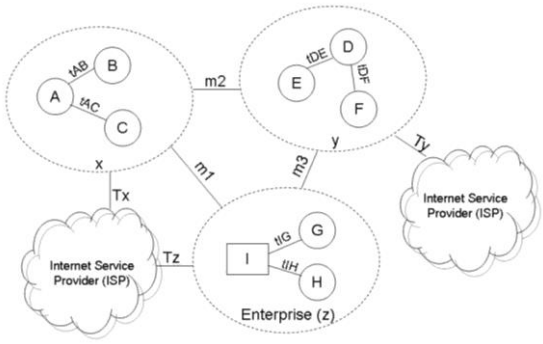

Figure 1: Infection Dynamics of Mobile Virus

As depicted in Figure 1, MPAN x which contains mobile node A, B, and C, MPAN y contain mobile node D, E and F and MPAN z, the enterprise contain mobile node G, H and also fixed node I. All of the MPAN are connected to the Internet through Internet Service Provider, ISP.

In x, A is connected to B and C. The connection time between A and B is represented by tAB. Assuming A is already infected, the longer A and B are connected, the possibility of B being infected is high. The same assumption applies for connection between A and C. The longer tAC, the higher possibility C will be infected. Mobile node A, B or C can also move to another MPAN z(m1) or y(m2) or both z(m1) and y(m2). If the node that moved is infected, then there is a possibility an infection occurred in z or y or both z and y. MPAN x also is connected to the ISP. The longer x is connected to ISP, represent by Tx, the higher possibility x being infected by virus.

In y, D is connected to E and F. The time D and E connected is representing by tDE. If D is infected, the possibility of E being infected also is high if tDE is high. The same assumption is applied for connection between D and F. The longer tDF, the higher possibility F will be infected. Mobile nodes in y can also move to another z(m3) or x(m2) or both z(m3) and x(m2). If the node that moved is infected, there is a possibility of infection occurred in z and x. MPAN y also is connected to the ISP. The longer y is connected to ISP, represent by Ty, the higher possibility y being infected by virus.

In z, I is connected to G and H. The connection time between I and G is represent by tIG. Assuming fixed node, I is already infected from the enterprise, the longer I and G is connected, the possibility of G being infected is high. The same assumption is applied for connection between I and H. The higher tIH, the higher possibility H will be infected. Mobile I or H or both can also move to another MPAN x(m1) or y(m3) or both x(m1) and y(m3). If the node is infected, then there is a possibility an infection occurred in x and y. MPAN z also is connected to the ISP. The longer z is connected to ISP, represent by Tz, the higher possibility of x being infected by virus.

V. Conclusion

Mobile networks security is important in an organizations. Since many organizations going mobile, virus threat on mobile is an issue that needs to be considered by mobile user. As the technology is rapidly developing, mobile devices become more sophisticated and this will create new threat and attract virus writers. The advanced mobile devices store important data and sensitive information in the device. The virus threat can create many losses to the organization by disrupting the device operations. User behaviours play an important role in the virus threat for mobile device. 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.

References

[1] Cheng, S.-M., Ao, W. C., Chen, P.-Y., & Chen, K.-C. (2011). On modeling malware propagation in generalized social networks. *IEEE Communications Letters*, *15*(1), 25–27.

[2] Delac, G., Silic, M., & Krolo, J. (2011). Emerging security threats for mobile platforms. In *MIPRO, 2011 Proceedings of the 34th International Convention* (pp. 1468–1473). IEEE.

[3] Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., … Sheth, A. N. (2014). TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*, *32*(2), 5.

[4] Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2015). Android security: a survey of issues, malware penetration, and defences. *IEEE Communications Surveys & Tutorials*, *17*(2), 998–1022.

[5] Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. *Procedia Computer Science*, *56*, 376–383.

[6] La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. *IEEE Communications Surveys & Tutorials*, *15*(1), 446–471.

[7] Mtibaa, A., May, M., & Ammar, M. (2010). On the relevance of social information to opportunistic forwarding. In *Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS), 2010 IEEE International Symposium on* (pp. 141–150). IEEE.

[8] Papaleo, G., Cambiaso, E., Patti, L., & Aiello, M. (2016). Malware Development on Mobile Environments. In *Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on* (pp. 270–275). IEEE.

[9] Peng, S., Yu, S., & Yang, A. (2014). Smartphone malware and its propagation modeling: A survey. *IEEE Communications Surveys & Tutorials*, *16*(2), 925–941.

[10] Seo, S.-H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014). Detecting mobile malware threats to homeland security through static analysis. *Journal of Network and Computer Applications*, *38*, 43–53.

[11] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164.

[12] Singh, K., Sangal, S., Jain, N., Traynor, P., & Lee, W. (2010). Evaluating Bluetooth as a medium for botnet command and control. *Detection of Intrusions and Malware, and Vulnerability Assessment*, 61–80.

[13] Sudina, S., Ahmada, R. B., Al Hadia, A. A., Kana, P. L. E., Idrusb, S. Z. S., & Abdullahc, M. M. A. (2015). The Influence of User Mobility in Mobile Virus Propagation: An Enterprise Mobile Security

Perspective.

[14] Thompson, B., & Morris-King, J. (2016). The impact of hierarchy on Bluetooth-based malware spread in mobile tactical networks. In *Proceedings of the Summer Computer Simulation Conference* (p. 34). Society for Computer Simulation International.

[15] Vecchiato, D., Vieira, M., & Martins, E. (2016). Risk Assessment of User-Defined Security Configurations for Android Devices. In *Software Reliability Engineering (ISSRE), 2016 IEEE 27th International Symposium on* (pp. 467–477). IEEE.

[16] Xia, W., Li, Z.-H., Chen, Z.-Q., & Yuan, Z.-Z. (2007). The Influence of Smart Phone's Mobility on Bluetooth Worm Propagation. In *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on* (pp. 2218–2221). IEEE.

[17] Zhao, T., Zhang, G., & Zhang, L. (2014). An overview of mobile devices security issues and countermeasures. In *Wireless Communication and Sensor Network (WCSN), 2014 International Conference on* (pp. 439–443). IEEE.

[18] Zhu, Z., Cao, G., Zhu, S., Ranjan, S., & Nucci, A. (2012). A social network based patching scheme for worm containment in cellular networks. In *Handbook of Optimization in Complex Networks* (pp. 505–533). Springer.