4th International Conference on E-Commerce
ICoEC 2017
18-20 SEPTEMBER 2017. PUTRAJAYA, MALAYSIA

Mobile Network Virus Infection Dynamics: A Threat to Enterprise Information Security

Suhizaz Sudin[a]*, R Badlishah Ahmad [a], Syed Zulkarnain Syed Idrus [b]
[a] School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia
[b] School of Human Development and Technocommunication, Universiti Malaysia Perlis, Malaysia

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. The risks to the enterprise from mobile devices are also being explained. In this section, the impact towards organizations is taken into consideration as well as the vulnerabilities of mobile networks. 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.*

Keywords: Mobile Network, Vulnerabilities, Mobile Personal Area Network

1. 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 used, the mobile network devices as well become a massive target for virus writers (Peng, Yu, & Yang, 2014) . Just as cancel sector viruses were returned by viruses that infected and propagate at the hand of electronic attachments and distinctive Internet vectors (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015), the rise of widespread mobile networking will focused to 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 dressed to the teeth boundary for hard code. The became lost in of conditional platforms (Enck et al., 2014), distrusting users and consumers (Sudin et al., 2015), and explosive growth in potential victims will unavoidably attract propagating viruses (Khan, Abbas, & Al-Muhtadi, 2015). 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 weight effects of virulent malware proliferation on consumers and mobile stylistic allegory providers are acute. This including illegitimate charges to customers , aggravation of mobile stylistic allegory services, crowd relations failures, and at the end of the day loss of piece of the pie for mobile antithesis providers (Singh, Sangal, Jain, Traynor, & Lee, 2010).

As the fixed attitude of soaring antithesis in increasing in businesses, the stake is such of the having to do with aspects that crave to be catch a glimpse of into. Several reasons are identified that makes mobile networks are in a superior

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

way vulnerable to hard attacks than solid 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 method have been developed for fixed networks, the above differences of mobile networks needs new security practices such as network topology that change dynamically, creates new set of security challenges (Faruki et al., 2015). The main idea here is that a node may disperse its true identity, but it can give the false location. Consequently, it can urge the absorb by conform the electronic message routes, monitoring bodily secured impression etc. In decide, the generally common manage of wireless augur makes soaring networks sweat to be infected for watchful and stoic attacks (Sudin et al., 2015).

Passive attacks means the attacker does not actively threat the network, but it mainly performs as a spy, and identifies the loop hole 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.

2. THE RISK TO THE ENTERPRISE FROM MOBILE DEVICE

Mobile devices have evolved for years as analog traditional walker-talkie to full-scale Internet-enabled computers. It has been upgraded and enhanced even many are more powerful than personal computers of the late 1990s. These devices are also moving toward an "always connected" form of connectivity, where users can obtain data continuously through the Internet Service Provider. Increasingly, the mobile devices specifically mobile devices also incorporate IEEE 802-based networking technologies namely the Wireless Fidelity (Wi-Fi) and Bluetooth.

On the other hand, having such powerful networked computers creates path for the threat of a new class of malware: viruses, worms, and trojans which purposely designed for the mobile environment. Most consumers and users think of Wi-Fi and Bluetooth as short-range communication tools. Therefore, most manufacturers consider the threat to mobile devices are less compared to fixed network because users would have to be physically near a malicious node to be attacked (Khan et al., 2015).

However, a Bluetooth connection with a standard mobile device more than one mile away with a 19dbi panel antenna has been developed .In addition, because Bluetooth devices are often carried, an attacker can attack the mobile devices even a truly short-range distance in the area of high-concentration, anonymous pedestrian traffic such as railway stations and bus stations. Threats against mobile devices are more dangerous and critical than traditional malware. Mobile devices, such as phones and PDAs, are often richer in personal data compared to personal computers.

Users and consumers might search for pot of gold that for their on the wing devices are invariably mutually them, they are more beg borrow or steal compared to Personal Computers. But physical approach mechanism of a personal digital assistant doesn't swear a have control. Users and consumers sweat to am a foundation for a false tenor of security by the whole of mobile devices, dominant them to invest these devices with more confidential and mortal information. Mobile device attacks can harm a person's most private data such as numbers, names, contacts, appointments, passwords, and even identities (Zhu, Cao, Zhu, Ranjan, & Nucci, 2012) . Even though such personal information is also present on fixed networked PCs, it's more diluted, distributed, and less organized than it must be on restricted mobile devices. As the result, threats on mobile devices are often get an easy access in finding private information (Khan et al., 2015).

Mobile device security is a major concern for organizations. The sizes of mobile devices, its memory capability and ease of use, which information can be downloaded and removed easily, drives risk to organizations when used and move outside physical boundaries (Delac, Silic, & Krolo, 2011). The evolving attacks not only affect persons who own mobile devices but also affect large organizations where mobile devices are used but susceptible (Seo, Gupta, Sallam, Bertino, & Yim, 2014). (Sudin et al., 2015) identify major impact to the organizations resulted from the infected mobile device.

Firstly, the organizations can experience a financial loss when viruses on mobile devices make unnecessary call to predefine unknown devices in the mobile environment. Big organizations which use a lot of mobile devices in the business processes may face a big loss when the infected devices tend to make unimportant calls to any potential devices in the network. The false call can be generated through the contact in the mobile device address book and also by roaming independently in the mobile environment (Sudin et al., 2015).

Second, performance of work will be decreasing since infected devices tend to slow down the processing capabilities. The viruses will create unnecessary processes and files in the mobile devices. This will use up the existing memory of the mobile devices and will delay the mobile devices processing time. Indirectly the work performances of organizations employee who are using those devices tend to slow down due to these infected devices.

Third, infected devices will allow remote control which can be assessed by unauthorized user. The important data will be viable to unauthorized user since current mobile user stores sensitive information on mobile devices (Zhu et al., 2012) such as personal information, mobile business information, mobile banking information etc.

Infected devices do not only give impact to individuals and organizations but also the service provider. As the service given on mobile devices portray the credibility of service provider, delay and problems of services caused by viruses made some impact to the service provider as well. The customer complaints regarding infected phones will be increased and the network will be congested due to virus related traffic (Zhu et al., 2012).

2.1 Vulnerabilities of Mobile Network

How mobile computing works resulted an expose environment to malicious attacks. Firstly, the use of wireless linkage makes the network vulnerable to attacks ranging from passive eavesdropping to active network interfering (Delac et al., 2011). Unlike fixed wired networks where an attacker must has a physical connectivity to the network connections or get through several defense mechanisms at firewalls and gateways, mobile network can be attacked from any directions and target any node. This will resulted damages that include secretive information leakage, a contaminant message, and impersonation of mobile node. All these show that a mobile network will not have clear defense mechanisms, and every single node must be prepared for confrontation with an attacker either directly or indirectly.

Second, mobile nodes are autonomous which have the ability of roaming independently. This means that nodes with insufficient physical protection are exposed of being captured, compromised, hijacked and infected. Since tracing a particular mobile node in a global scale network is hard to perform, attacks by a compromised node from within the network are far more damaging and much harder to detect. Therefore, mobile environment containing nodes, the infrastructure and policies must be in place to work in a mode that trusts no peer (Thompson & Morris-King, 2016).

Third, decision and policy making in mobile environment is sometimes distributed and some wireless network security algorithms rely on the cooperative participation of all nodes and the infrastructure (Zhu et al., 2012). The absence of centralized authority means that the attackers can use this susceptibility for new types of attacks designed to break the cooperative algorithms.

In addition, mobile computing has evolved new type of computational and communication processes that rarely appear in fixed or wired environment. For instance, mobile users and consumers tend to be stingy about communication due to slower links, limited bandwidth, higher cost, and battery power constraints; mechanisms like disconnected operations (Seo et al., 2014) and location-dependent operations only appear to mobile wireless environment. Unsurprisingly, security measures developed for wired network are likely incompetent to attacks that exploit these new applications.

Applications and services provided in a mobile wireless network can be an irresolute link as well (Peng et al., 2014). In these networks, there are always proxies and software agents running in base-stations and intermediate nodes to obtain the performance gains through caching, content transcoding, or traffic shaping, etc. Potential threat may target these proxies or agents to obtain important sensitive information or to launch DoS attacks, for instance doing cache flushing by using bogus references, or get the content transcoder do useless and expensive computation.

3. VIRUS THREAT ON MOBILE DEVICE

Seo et al. (2014) 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.

He 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 (Khan et al., 2015).

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 (La Polla, Martinelli, & Sgandurra, 2013). 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 (Enck et al., 2014)

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 world-wide, whereas only half of it in 2004 (Papaleo, Cambiaso, Patti, & Aiello, 2016) .

The wide-spread usage of Bluetooth devices has attracted the virus propagation. (Mtibaa, May, & Ammar, 2010) 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 advance 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 device worldwide which makes these devices being targeted by the viruses writer (La Polla et al., 2013). Here we highlight a few virus spreading mechanism in mobile network namely the Mobile Personal Area Network, Internet Access and Messaging.

3.1 Mobile Personal Area Network

Thompson and Morris-King (2016) explained that a compromised mobile device can 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 being infected by a fixed devices 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 being 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 in increased, the standardization of networks and devices are becoming more connected (Zhao, Zhang, & Zhang, 2014). 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 to fixed wired PCs and vice versa (Seo et al., 2014).

3.2 Internet Access

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 (Sicari et al., 2015) while accessing the internets makes the mobile devices a popular target for viruses hence the security is low. The mobile device developer also tend 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 attack via Internet access is the virus in an attachment and social network virus.

3.2.1 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 (Faruki et al., 2015).

Papaleo et al. (2016) 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.

According to Zhu et al. (2012) 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 (Papaleo et al., 2016). 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.

3.2.2 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 (Cheng, Ao, Chen, & Chen, 2011). 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.

The study from Cheng et al. (2011) also claims that about 19% of all those surveyed reported having clicked on a link in a 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.

3.3 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.

3.3.1 Worm Infection

The worm infection is autonomous. The user's behavior of transferring message or information through short range Bluetooth connectivity (Singh et al., 2010) 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 equip 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 allocate 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 (Peng et al., 2014).

The entry level mobile devices which don't have the internet connectivity make fully used of this 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.

3.3.2 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 Enck et al. (2014), 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 an enormous quantities of SMS traffic. Multimedia Messaging System (MMS) is an advance 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 opening the multimedia files sent through MMS (Vecchiato, Vieira, & Martins, 2016).

SMS address spoofing also is an emerging threat that allows viruses to make a 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 (Delac et al., 2011).

4. EXPLAINING THE INFECTION DYNAMICS

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

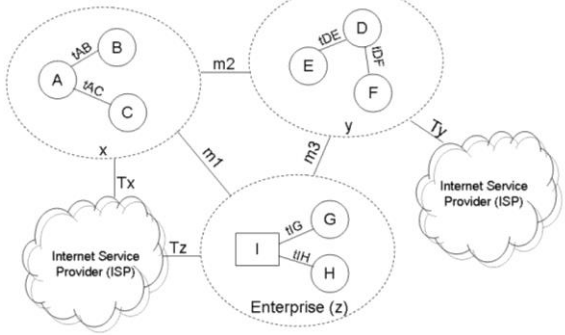
tAB
B
A
tAC
C
x
m2
tDE
D
E
tDF
F
y
Ty
m1
m3
Tx
Internet Service Provider (ISP)
Tz
I
tIG
G
tIH
H
Enterprise (z)
Internet Service Provider (ISP)

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 is connected, the possibility of B being infected is high. The same assumption is apply 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 an 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 x being infected by virus.

5. CONCLUSION

Mobile networks security is important in an organizations. Since many organizations going mobile, virus threat on mobile is an issue that need 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 advance 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

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.

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.

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.

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 defenses. *IEEE Communications Surveys & Tutorials*, *17*(2), 998–1022.

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.

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

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.

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.

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

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.

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.

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.

Sudin, S., Ahmad, R. B., Al Hadi, A. A., Kan, P. L. E., Idrus, S. Z. S., & Abdullah, M. M. A. (2015). The Influence of User Mobility in Mobile Virus Propagation: An Enterprise Mobile Security Perspective, *Proceedings of the International Conference on E-Commerce 2015*, 20-26.

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.

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.

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.

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.

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.