International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.89-106
http://dx.doi.org/10.14257/ijsia.2016.10.10.10

Mobile Security and its Application

Jun Hou Chan and Jer Lang Hong

School of Computing and IT, Taylor's University
junhou.chan@taylors.edu.my, jerlang.hong@taylors.edu.my

Abstract

Ownership of a smartphone has never been easier nowadays, and it is supported by the fact that most of the people around us have a smartphone or an equivalent smart device. What is smartphone and why is it a smart? A smartphone by definition is as the name suggests, it is a phone is smart enough to not only be limited to the features and capabilities of a traditional cellular phone but also perform what a "smart" device can. And in recent years, the device that is deemed as the most intelligent device is the computer as it is the most advance piece of technology that is commercially available to the general public. Why this is so, is because in our opinion it has revolutionized how most if not all of the societies of today work. Hence what makes a smartphone is the mobile operating system that it is built upon, which is similar to a computer. It is becoming more and more of a common sight nowadays and this is because they are being offered at a price where more people are able to afford, hence they are reaching the hands of ceiling of the lower income families, all the way up to the higher income families. Back then, pure play devices were mostly simple in terms of how it function and works, hence if possible, we could suggest that the security aspect was never or rather has never been an issue other than the alteration of data after operation such as the tape of video recorders or images captured but never in the process, in the sense that there were no interruptions during operation, most likely is because it was clear and visible, but nowadays when you combine all of those devices into a complex entity, we tend to leave a hole in the cloth somewhere that we did not or rather can't see due to the overwhelming amount of other things that we have. In this paper we discuss the current state of the commercially available operating systems of the two biggest names in smart devices, namely iOS and Android; and measure how secure and/or vulnerable (susceptible) are they to malwares and the nature of the mobile ad hoc network. We first analyze the integrity of the core of a smart device, the operating system and then use it to evaluate the effectiveness of their techniques and defenses of preventing and identifying malwares.

Keywords*: Social Media, Data Extraction, Semantic Analysis*

1. Introduction

The growth of mobile smart devices is virtually endless. Although the meaning for devices that combines telephony and computing has been around as early as 1973 and its concept was already patented. It began sales only in 1994 but it was never referred to as the "smartphone" because the term itself has yet to be coined, not until 1997 with thanks to Ericsson. However the Personal Digital Assistant (PDA) did not take flight when it was introduced, not if it was compared to how the Apple's iPhone (1st generation) did when it was launched in mid-2008. From then on Apple's iPhone sales have been skyrocketing year-by-year and generation-by-generation.

The possibilities and the future of smart devices has peaked our interests immensely as it still has enormous potential for growth despite its current condition but this is unfortunately followed by the fact that it is will be facing a serious threat if not handled

ISSN: 1738-9976 IJSIA

properly. Additionally, with a strong interest in the field of security as well, and with these two interests, we are keen on establishing the barrier that is currently lacking or insufficient that is to protect the users. What we want to accomplish is to join in helping to protect the users, which numbers will only grow in the future. And this could be accomplished either by introducing new concepts perceived or improvements on the existing defense mechanisms, which in our opinion is not sufficient currently, and would only be less in the future. This paper is a revised and expanded version of a paper entitled "A survey on Mobile Security" presented at The 5th International Conference on Next Generation Computer and Information Technology, August 19-20, Harbin, China [14].

2. Background

Mobile security is becoming a major concern in the world today, and it is becoming even more so due to the undeniable fact that the population of smart mobile devices has been growing at alarming rate, and it will become a potentially serious threat if not dealt with properly and quickly. Why it is growing at the rate that it is; it is because it has essentially become an all-in-one device. What this means, is that what once was a feature unique to certain pure play devices, has now been incorporated into a single entity alongside with many other pure play devices. Traditionally from just making and receiving telephone calls, the mobile phone, which was also known as a cellular phone, has evolved. From its first debut in 1973 weighing in at 0.8kg, its purpose and its physique has been changing and evolving since then in order to adapt to and cater for the needs and demands of us, the users. Soon after came the trend of compactness, which made sense as no one appreciates carrying a brick around. Then in 1993, the possibility of text messaging was made available, since then the feature that it offers has never cease to increase, not even today. In 40 years, the mobile phone has evolved miraculously into a device where people back then would have never imagined it possible. With the evolution of the mobile phone, from a single pure play device to a multi-function device and also the affordability being more practical, it has made its' way to the general public, it has also simultaneously made an impact on two thing or rather it has started a chain reaction causing the increase of two things; starting with the number of users, which has exploded over a short period of time since its conception, and also the number of people who are targeting that ever increasing population of mobile users. Smart devices are no longer bounded to the realm of smart phones, but have also expanded onto the realm of tablets and this could only mean one thing and that is that the number of targets has almost doubled. This is so, due to the simple fact that upon the launch of Apple's iPad in year 2010 it had made its mark in human history by making a tremendous impact on the world. Ever since then, people in the society began to own both a smart phone and a tablet, hence promoting the growth of smart devices that is out there and also the number of vulnerable targets if the security for said devices are not kept at an optimal level.

a. Mobile Ad Hoc Network (MANET)

Like most if not all of the current technologies, the concept of mobile ad hoc network (MANET) was conceived and used only for military purposes since its birth, in the 1970's. Back then it was better known as PRNET (Packet Radio Networks). Sufficient to say, it was the first generation of the ad hoc network system that we know today as mobile ad hoc network. Later on, sometime during the 1980's came the second generation, where it was enhanced further and used as a part of the SURAN (Survivable Adaptive Radio Networks) program. Since it was still being used for combat purposes, the main aim for the ad hoc networks remained the same; however the developments of the second generation primarily focused on the advancement of

the first generation's structure. What the second generation offered was a packet-switched network to the mobile battlefield, which was an environment incapable of having and without an infrastructure of any kind. The results of the SURAN program was positive as it proved that it was beneficial in improving the radios' performance when it was made to be more compact, cheaper and resilient to electronic attacks. After two generations of military usage, finally in the 1990's came the commercial ad-hoc networks, which is third generation of this technology. It did not come alone as it came accompanied with notebook computers and other viable communications equipment. The mobile ad hoc network consists of multiple routing protocols, namely reactive, reactive routing, and hybrid routing protocols. Despite the unfortunate fact that no system is perfect, the existences of loopholes, bugs and defects in any system, that is made by man is inevitable, and this does not apply only to operating systems of smart devices but also to the very core of ubiquitous computing. The very nature of ubiquitous computing itself has made it necessary that wireless network is to act as the interconnection method. This is because it is not practical or rather not feasible for ubiquitous devices to get a wired connection anywhere and whenever they need to connect with other ubiquitous devices. To name a few of the vulnerabilities of the mobile ad hoc network, it would be the unreliability of the wireless links between the nodes, ever changing dynamic topologies, lack of both a secure and clearly-defined boundaries and centralized management, and also restricted power supply. However there are always two sides to a coin, the upside of the mobile ad hoc network includes providing availability, integrity, confidentiality, authenticity, authorization, and also anonymity.

b. Mobile Malware

Back to the other matter at hand, the defense against malwares that is aimed at these vast amounts of potential prey. Alike the battle between good and evil, the battle with malwares is a never ending battle and also a tough one at that. The authors of malware are people coming from varying backgrounds and with different intentions of doing so. Initially malwares, for computers, were made for joy and excitement for novice authors as the numbers of experts back then were small in size. However that mindset has passed its prime and now a much more common set of intentions is has come about and is likely to stay for quite some time. The common intentions right now is, either financial gain through exploiting un-expecting users, popularity and/or leaving the author's mark in history, or even for the pure simple joy of fun although the number of people doing it for fun has depleted over time but a number still remains. This common set of intention has not only inspired a remarkable amount of people to get active and join for unethical reasons, but it has also done the same in inspiring people who would want to join for ethical reasons. In the very beginning malwares existed only in the world of laptops and desktop computers; hence mobile malware was merely a proof-of-concept. Like any other type of threats, it was harmless or rather not serious enough to make a point to begin with, however with time, mobile malware has begun to move forward and it is no longer just a concept, therefore turning into a real threat. Computer malwares has been around since its debut back in the early 70's with the Creeper, which is known to be the very first computer virus [13]. Then it slowly evolved into the many variants of malwares that we have today. As for mobile malware, its story starts from almost a decade ago back in 2004. In 2004, the first mobile malware known as Cabir, made its first appearance. Cabir is in fact a worm that was developed merely as a simple proof-of-concept by author, Vallez, who was part of a team of virus writers. The Cabir worm was written to infect Symbian-based devices and its primary method of getting other similar devices infected was via Bluetooth. Even though it was not meant for anything harmful, unfortunately it was inevitable that the proof-of-concept was soon to be picked up by others with mischievous intent. Soon enough there was

already new and more powerful variants of Cabir by the end of that very year. [12] As the field of malware itself is vast and broad, and it can perform a large variety of harm reflecting each individual author's intention and also it may varies across platforms such as Android and iOS. This is because each platform would have their own security schemes hence making certain actions viable in one platform but rendered useless in the other therefore in this paper we chose to survey and observe the number of malware, types of malware in existence, malwares that had caused a major impact, and see how each of the respective operating system had mitigated each and every one of them in 2012 or earlier if there are none in 2012.

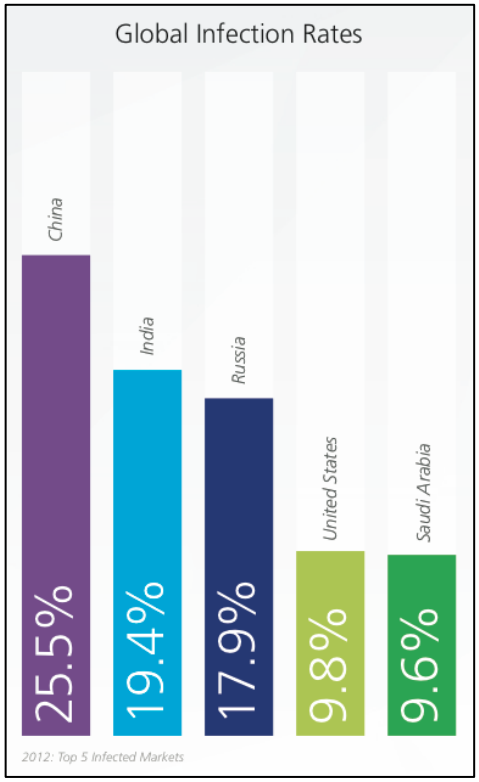

Figure 1. Supporting Information Illustrating the Global Malware Infection Rate [92].

3. Related Work

Back in 2004, Guo *et. al.*, forecasted that mobile malware would be used to launch attacks such as spam, identity theft, and wiretapping against telecom networks and call centers [7]. Similarly, there have been others who have surveyed and discussed about mobile malwares sighted throughout 2005 and 2008 [8-11]. Here we present a discussion of the feasibility of mobile-based attacks, especially when given modern smartphone capabilities. Evaluation of the incentives that lies behind the different types of attacks is also done. In 2009, Enck *et. al.*, presented potential incentives for mobile malware and we follow their work but with a twist of a more in-depth consideration of mobile malware incentives and a survey that validates their predictions that premium SMS and information-gathering malware would become prevalent. In more recent work, Becher *et. al.*, and Vidas *et. al.*, discuss potential mobile attack vectors, such as the web browser and physical access. They focus on describing attack mechanisms, whereas we survey malware.

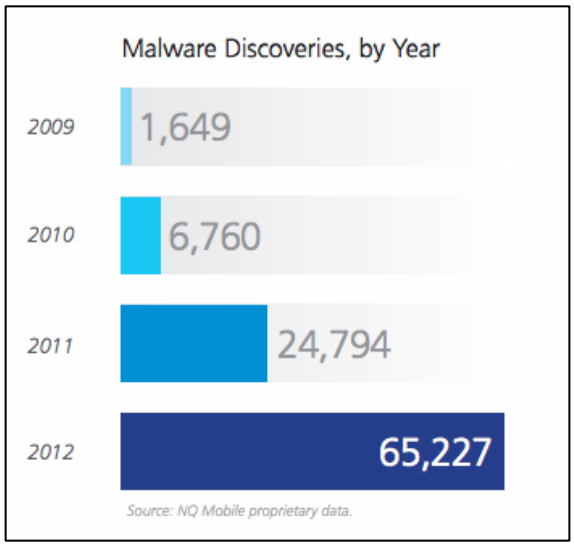

Figure 2. Supporting Information Illustrating the Malware Discoveries on a Yearly Basis [92].

a. Problem Overview

We first look into what are some of the problems that corresponds to mobile security, which for this research, it includes the vulnerabilities of the mobile ad hoc network and secondly, malicious software, which is also known as malwares, that is designed for smart devices

b. Vulnerabilities of Mobile Ad Hoc Networks

For this part of the paper we talk about some of the vulnerabilities that exist in the mobile ad hoc networks currently. As stated previously, because of the freedom and convenience that ubiquitous computing offers there exists drawbacks to such advantages as well. This is due to the simple fact that there will always a tradeoff between performance (convenience in this matter) and security in almost everything. With the subject of mobile ad hoc networks in hand, the convenience it offers have far outweighs its security aspects. As compared to its predecessor, the traditional wired network, mobile ad hoc networks have far more vulnerabilities. Furthermore more on that point, the security aspect of mobile ad hoc networks is much more challenging to maintain than wired connections. In the following sub-sections, we discuss further on the various existing vulnerabilities of the mobile ad hoc networks.

i. Absence of Secure Boundaries

The definition of this vulnerability is self-defining in itself. This is much clearer in the sense that since there is no actual physical connection, the proper form of defense required cannot be properly defined. The birth of this vulnerability lies within the concept of the mobile ad hoc network itself, which is the freedom to join, leave and traverse along inside the network when joined successfully. Unlike the traditionally wired network, the perpetrator is no longer restricted by the need to attain a physical access to the target network initially in order to execute any form of malicious activity to the intended target [3]. What's more is that the perpetrator can be as far away as the radio range of any of the nodes in the mobile ad hoc network. The need to bypass through the several line-of-defenses that was set-up to prevent such an entry, such as firewall and gateway is also neglected. As a result, it does not have a clearly defined boundary that can be used to protect the network from potentially dangerous network

accesses. With the absence of secure boundaries, it renders the network susceptible to attacks; this means that the network can suffer from all kind of attacks at any time, originating from any one of the nodes and possibly targeting the remaining nodes that are inside the network. Some common types of attack include leakage of confidential information, eavesdropping, direct interfering, data alteration, message replay, message contamination and denial-of-service.

ii. Threats from Compromised Nodes within the Network

As stated earlier regarding the vulnerability emerging from the fact of the absence of secure boundaries in the mobile ad hoc network, this present perpetrator the opportunity to gain access inside the network. This could have been accomplished by many ways, and one of which is the overtaking over a node entirely. Then using the compromised nodes the perpetrator can perform further undesirable actions to certain nodes or to the network entirely. This vulnerability can be classified as threats that are coming from certain compromised nodes inside the network. Since all of the nodes are independent entities that have the choice and freedom to join or leave at any time they like, it makes the establishment of policies that is to be enforced by nodes to prevent malicious behaviors from the nodes that it interacts with, significantly hard because of the diversity of behaviors that different nodes possesses. In addition to that, with the mobility of the network that ad hoc network offers, compromised nodes can change its attack pattern along with its targets frequently in order to avoid tracking and tracing, especially if it is in a large scale ad hoc network. Henceforth threats from within the network are far more dangerous as compared to external attacks, attacking coming from outside the network, this is much more so because they are much harder to detect as they are coming from compromised nodes which acts and behave normal and well.

iii. Lack of Centralized Management Facility

As ad hoc networks lack a piece of management machinery that is centralized, therefore it will have several vulnerability issues. To start off, the absence of this crucial machinery makes the detection of attacks very difficult, this is because monitoring the traffic in a highly dynamic and also a large-scale ad hoc network is no easy feat [4]. The ad hoc network is also known to encounter several benign failures, such as path breakage, transmission impairments, packet dropping and several others, and this is known to happen quite often. With the knowledge of these two facts alone, we are able to see why intentional and malicious failures is that much harder to detect, especially when the attacker changes their attack pattern and target in varying periods of time. With each and every victim, because we can only observe the failure that occurs in itself, we are unable to conclude, at least not from this short duration observation, that it was an intentional failure caused by an adversary. However all is not lost, as we can also easily conclude that all the failures is malicious instead of benign failure because we are able to notice that the adversary has performed a significant amount of misbehavior when we are looking from the vantage point of the system, even though should all the failures occur in different nodes at different time. From the scenario described, we can see the severity and the problems that the lack of centralized management machinery will lead to, especially when we are attempting to detect any form of attacks that could occur inside in the ad hoc network. Secondly, the lack of centralized management machinery will cause problem with the trust management for the nodes in the ad hoc network [1]. In the mobile ad hoc network, the cooperation of nodes in required for network operations, even though while no security associations (SA^2) exists for all the network nodes, therefore the practicality of performing a priori classification is questionable, and as a result the of establishment of

a line of defense which will assist in distinguishing where if nodes are trustworthy of not cannot be achieved here in the mobile ad hoc network.

iv. Limited Power Supply

As in the ad hoc network the individual nodes is mobile, it is highly likely that their primary source of power is relying on battery, whereas traditionally, nodes in the wired network has no concern in terms of power supply as they are able to obtain electric power supply directly from the outlets, which also implies that it is almost infinite. With power supply being a concern, nodes in the mobile ad hoc network will need to face problems that restricted power supply will bring. One of many problems presented by limited power supply is denial-of-service attack [1]. In the ad hoc network, since the perpetrator knows that the target node depends on battery power, which suggests limited power supply, the perpetrator can perform a variety of actions which includes, sending additional packets to the target node and requesting it to route said packets continuously or it can deceive and trap the target node into performing some computations which could possibly be intractable, and as a result wasting valuable resources and time. By doing so, it can significantly exhaust the target node's battery power as it performs meaningless task and it will be out of commission as it runs out of power. Another problem that arises from the issue of having limited and/or restricted power supply comes from within where when a node in the mobile ad hoc network misbehaves; to be more precise it might behave in a selfish manner when it realizes that it has a limited power supply and this behavior could cause problems especially when the need for this particular node to cooperate with other nodes to support certain functions in the network come about. However, even so we must not view all selfish nodes as malicious nodes. This is because some nodes could possibly encounter restricted power supply issues therefore behaving the way that it is, which is tolerable if it was genuinely the case, but then there exists some other nodes that would intentionally declare that it is running out of battery power and therefore refuses to cooperate with other nodes in for cooperative operations, even though it has enough battery power left to support the operation. All in all, as true as it may be, selfish behavior does not necessarily denote malicious behavior, but we need to know if the selfishness is genuinely a result caused by limited battery power or by intentional uncooperativeness.

v. Scalability

Last but not least, scalability; it is something that we must address especially when we discuss of the vulnerabilities in the mobile ad hoc network [1]. With the traditional wired network, the scale was something that was predefined when it was designed and is highly unlikely to change during usage, however that no longer adhere to the mobile ad hoc network as its scale changes and varies during operation, and because of the mobility of the nodes in the network, it is hard to predict or estimate an approximate amount of nodes that will be in the network in the future. As a result, protocols and services that are to be used such as routing protocols should be compatible to the ever changing scale of the ad hoc network, which could very well range from a handful of nodes and off to hundreds and/or ever possible thousands of nodes. With this in mind, this would then require the said protocols and services to be able to scale up and down efficiently.

vi. Vulnerabilities of the Mobile Ad Hoc Network: Summary

From the discussion in the previous sections of this chapter, it is suffice to conclude with stating that the mobile ad hoc network is insecure to begin with. This is supported by firstly, the fact that there is an absence of secure boundaries, due to the freedom

given to individual nodes to join, leave and move within the network, secondly the lack of required centralized machinery, thirdly the limited power supply that leads to selfish behavior and therefore problems, lastly, the scale of the network which is an ever changing phenomenon has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network. In the end, when the mobile ad hoc network is brought back to back with its predecessor, the wired network, the mobile ad hoc network certainly requires a higher level of robustness in regards to its security scheme to ensure and maintain the security of it.

c. Security Solutions For The Mobile Ad Hoc Networks

As we discussed in the previous section, there exist several vulnerabilities has is able to render the MANETs (Mobile Ad Hoc Networks) insecure. Even so, we are far from securing the mobile ad hoc network, if we only know of the existing vulnerabilities. Therefore in order to achieve our goal of securing the mobile ad hoc network we need to first know of the existing security solutions. In this section, we will survey some of the existing security schemes that can be useful in protecting the mobile ad hoc network from malicious behaviors.

i. Security Criteria

First we have to define the criteria and conditions which we can use to judge if a mobile ad hoc network is secure or not. In other words, we need to know what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network. Following this section, we will briefly introduce the widely used criterion that is used to evaluate a mobile ad hoc network as secure or not.

1. Availability

Availability by definition means that a node should maintain its ability to provide all the designed services regardless of the security state of it [1]. Availability by itself is a criterion that is mostly challenged during denial-of-service attacks, where all the nodes in the network have the possibility of being the attack target. Therefore selfish nodes that exist in the network will make some of the network services unavailable (*e.g.*, routing protocol or key management service) [2].

2. Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised in many ways; an example of some would be [5]:

1. Malicious altering
2. Accidental altering

A message is prone to attacks by an adversary with malicious goals, where it can be removed, replayed or revised; this is known as malicious altering. There are also cases where messages can be lost or having its content altered not by malicious altering but due to certain benign failures, which may be caused either by encountering transmission errors during communication or hardware errors such as hard disk failure.

3. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In short, in order to maintain the confidentiality of some certain information, we need to keep their existence a secret from all those entities that are not allowed access or do not have the privilege to access them.

4. Authenticity

Authenticity assures participants who are in communication are genuine and are not impersonators [1]. It is vital for the participants who are in communication to prove their claimed identities using some techniques so as to ensure authenticity. Should there not be any authentication mechanism, the attacker could potentially impersonate a benign node and therefore obtain access to confidential resources, or even send fake messages to disrupt normal network operations.

5. Nonrepudiation

Nonrepudiation means that the sender and receiver cannot deny that they have both sent or received such message. This is especially useful when we need to justify if a node that is exhibiting abnormal behavior is compromise or not. However, if a node recognizes that is has received a message that is suspicious or wrong, then it can use that fact as an evidence to notify other nodes of the node that is sending out the improper message might have been compromised.

6. Authorization

Authorization is a process where a particular entity is issued a credential that specifies the privileges and permissions that it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to users of different levels. For instance, we need to ensure that network management function is only accessible by the network administrator, therefore should be an authorization process before the network administrator accesses the network management functions.

7. Anonymity

With anonymity, it means that all the information that can potentially be used to identify the owner or the current user of the node should be by default, be kept private and not to be distributed by the node itself or the system software. This is closely related to privacy preserving, where we try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

8. Security Criteria: Summary

Up till with this section, we have noted and discussed several key requirements is to be enforced in order to ensure the security of the mobile ad hoc network. Despite this, there are also other security criteria that are much more specialized and application-oriented, which includes location privacy, self-stabilization and Byzantine Robustness, which are correlated to the routing protocol in the mobile ad hoc network. Upon settling the main security criteria, we can move on, and begin discussion on the main threats that violates the security criteria, which is commonly known as attacks.

ii. Type of Attacks in Mobile Ad Hoc Networks

When it comes to the range of possible attacks on the mobile ad hoc network, there are too much to count. However, almost of all them can be classified under one of the following types [3]:

1. External attacks; where the objective of the attacker is to cause congestion, propagate fake routing information or disrupt nodes from providing services.
2. Internal attacks; where the objective of the adversary is to participate in the network activities, but first require gaining access to the network either by

malicious impersonation and access the network as a new node or by a direct approach where they directly compromise a current node and using it as a basis to carry out its malicious intent.

As described by the two categories above, external attacks are considerably similar to how normal attacks would be in the traditional wired networks, where the adversary is in the proximity but it is a not a trusted node in the network, therefore, this type of attack can be prevented and detected by security methods such as membership authentication or firewalls, which are conventional security solutions. However, internal attacks are far more dangerous if compared to with external attacks and this is because of the pervasive communication nature and open network media that is in the mobile ad hoc network. Internal attacks begin with having nodes that are originally benign users of the ad hoc network and they can easily pass the authentication and get protection from the security mechanisms. This method allows adversaries to make use of the compromised nodes to gain access to the services, which is supposedly only available to authorized users in the network, and then they can use the legal identity provided by the compromised nodes to conceal their malicious behaviors. With this, it tells us that internal attacks requires more attention as they are performed by malicious insiders, when we are considering the security issues in the mobile ad hoc networks. In the following, we discuss on the most common and main type of attacks that emerges in the mobile ad hoc networks.

9. Denial of Service (DoS)

One of the many types of common attacks is denial of service. The objective of performing a DoS attack is to rob the availability of certain nodes or even the services of the entire ad hoc network. Traditionally with the wired network, DoS attacks are carried out by flooding the target with network requests causing heavy network traffic and also exhausting the processing power of the target, and with the goal of rendering the services that is offered by the target being unavailable to genuine requests. However with the mobile ad hoc network, DoS attacks are not practical due to the distributed nature of the services. However, even with DoS attacks being impractical, mobile ad hoc networks are still more vulnerable than wired networks; some reasons include the interference-prone radio channel and the limited battery power. In practice, attackers uses radio jamming and battery exhaustion techniques to conduct DoS attacks on the mobile ad hoc networks.

10. Impersonation

A second type of attack is conducted solely by impersonation, and it is a serious threat to the security of the mobile ad hoc network [1]. As discussed previously regarding authentication, should there not be a proper authentication mechanism that can be used by the nodes, then this provides the adversary an opportunity to capture some nodes in the network then making them look like benign nodes. With this method, nodes that are compromised will be able to join the network by passing off as normal nodes, and then begin to perform malicious activities such as propagating false routing information and possibly gaining inappropriate priority to access confidential information.

11. Eavesdropping

Eavesdropping by itself is considered to be another kind of attack that is not to be uncommon in mobile ad hoc networks. With eavesdropping, our adversary hopes to obtain certain confidential information, which should be kept out of reach from unauthorized individuals during communication. Confidential information varies and

can range from information such as location, encryption keys and up to the password of nodes. Because such important data is vital to the security state of the nodes, they should therefore be kept away and out of reach from unauthorized individuals with unauthorized access.

12. Attacks against Routing

As routing is considered to be one of the more important services that are offered in the network, therefore it is also unavoidable that it has become one of the more common and main targets by attackers to conduct their malicious intent. With regards to the mobile ad hoc network, routing-targeted attacks can generally be classified into two (2) difference categories:

1. Attacks on routing protocols and,
2. Attacks on packet forwarding/delivery [3]

The objective of routing protocols attacks is to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. On the other hand, for packet forwarding attacks, the objective is to disrupt the packet delivery along a predefined path.

The main influences brought by the attacks against routing protocols include network partitioning, routing loop, resource deprivation, and route hijack [3]. Some of the many attacks that are against routing have had been researched on and well known [10-13]:

1. Impersonation of another node to spoof route message.
2. Propagating a false route metric to misrepresent the topology.
3. Sending a route message with wrong sequence number to suppress other legitimate route messages.
4. Flooding Route Discover excessively as a DoS Attack.
5. Modifying a Route Reply message to inject a false route.
6. Generating fake Route Error to disrupt a working route.
7. Suppressing Route Error to mislead others.

Due to the nature of mobile ad hoc networks, it is not easy to validate all of the route messages [3]. Other routing attacks do exists, and they are much more sophisticated, some examples would be Wormhole, Rushing and Sybil attacks [14-16]. Another form of attack is the attack on packet forwarding/delivery and it is not easy to detect nor prevented [3]. There are two ways to go about it with this form of attack: one of which is selfishness, where the malicious node selectively drop route messages that is supposed to be forwarded, in the interest of conserving its own battery power; the other is denial-of-service, where the attacker floods the victim's network traffic which as a result drains the victim's battery power.

13. Type of Attacks in Mobile Ad Hoc Networks: Summary

We have covered and discussed on the type of attacks in mobile ad hoc networks. The attacks can be categorized under one of the two (2) categories: external attacks and internal attacks, with the latter posing as a greater threat for the mobile ad hoc network. Furthermore, we introduced some of the main attack types in the mobile ad hoc network, which comprises of attacks such as denial-of-service (DoS) attacks, impersonation attacks, eavesdropping attacks, and as well as attacks against routing.

iii. Security Schemes for Mobile Ad Hoc Networks

After a discussion on some of the better-known type of attacks that exists with the mobile ad hoc network, it is only proper that now we discuss on some of the security

schemes that can deal with such attacks. In the following subsection we will discuss on several security schemes that is well known to be able to handle the variety of different attacks as discussed previously.

14. Intrusion Detection Techniques

Intrusion detection (ID) is not a new concept in the field of networking and by definition is a type of security management system that is for computers and networks. Generally speaking, an Intrusion Detection System (IDS) gathers and analyzes the information from various areas in the context that it is in, such as a computer or network, to deduce if there are any breaches in security of any form or if there are any unwanted manipulations done to the system. Such security breach includes both intrusion (external attacks) and misuse (internal attacks). As stated, it is not a new concept as it is already implemented with the traditional wired network. Despite some of the key differences of the traditional wired network and mobile ad hoc network, the technique of intrusion detection has undeniably gained the attention of researchers who were in search of security solutions for the mobile ad hoc network.

15. Intrusion Detection Techniques in MANET

In regards to intrusion detection techniques in MANETs, it was presented in the paper written by Zhang *et. al.*, [6]. In this paper a framework for intrusion detection in MANET was proposed, which was able to meet the needs of MANET. The architecture of the intrusion detection system is illustrated below in Figure 3.

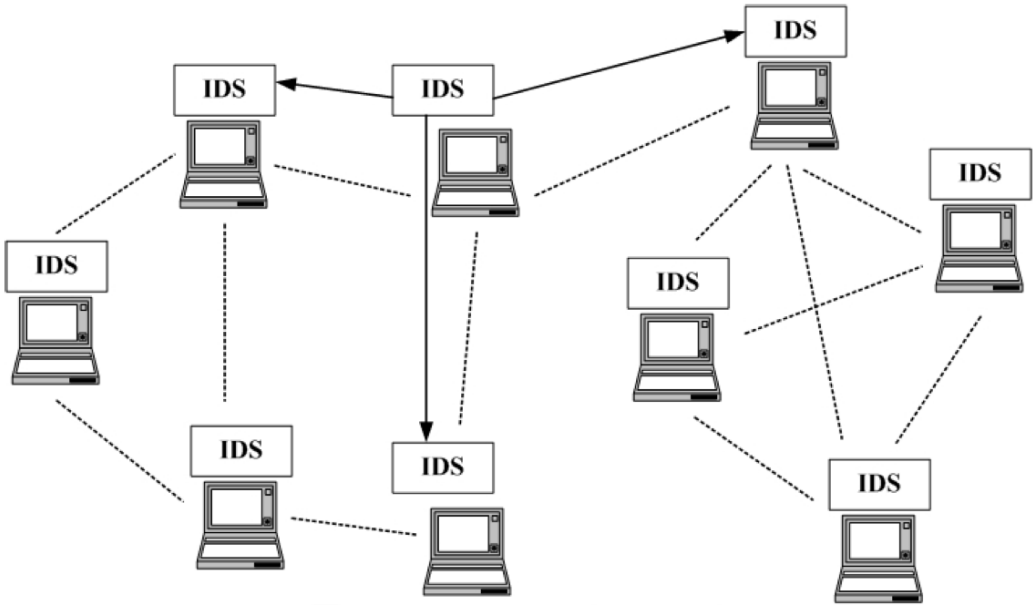

Figure 3. Architecture of an Intrusion Detection System (IDS) for MANETs

As illustrated in Figure 3, with this architecture there are built-in IDS agents in all of the nodes that are in the MANET as all of them play a role as they take part in the intrusion detection and response activities when signs of an intrusion are detected. Additionally, adjacent nodes have the ability to share results obtained from investigations with each other hence cooperating in a broader range. However, the call for cooperation occurs only when the node that detects an anomaly has insufficient information and is not able effectively determine out what kind of intrusion it is. In this scenario, the node that made the discovery of such an anomaly would then require all of the other nodes that are within its range of communication to search their individual

security logs and possibly find traces of the intruder by tracking them. The internal structure of a typical IDS agent is as shown in Figure 4.

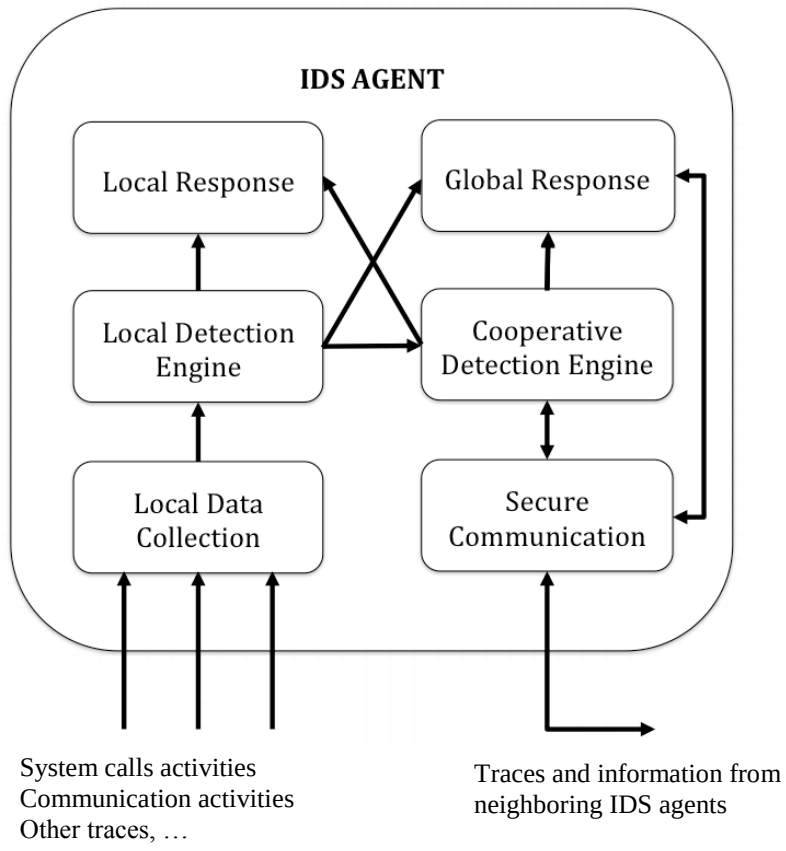

Figure 4. A Conceptual Model of an IDS Agent

There are four (4) main functional modules in this model:

1. Local data collection – this module handles data collection and any issues that might arise during operation.
2. Local detection engine – this is the next module in line that examines the local data after it is collected by the local data collection module. It then examines the data to check if there is any sort of anomaly that is shown in the data. As the IDS are able recognize most if not all of the known type of attacks, it has promoted the constant birth of new attack types. By knowing this, the detection engine should not expect to only perform pattern recognition between known attack behaviors and the anomalies that resemble intruders, but instead it should utilize statistical anomaly detection techniques, in which it differentiates anomalies from normal behaviors on the basis of the deviation between the current observation data and the normal profiles of the system.
3. Cooperative detection engine – this particular module works hand-in-hand with other IDS agents when the need for consolidation of evidence when suspicious anomalies are detected in certain nodes. When the need for a cooperated detection process arises, all the participants will propagate the intrusion detection state information of themselves to all of the neighboring nodes. By sharing resources all of the participants now partake in the calculation of the new intrusion detection state after receiving all of the new information from

their neighbors by using algorithms such as a distributed consensus algorithm with weight.

4. Intrusion response – this module as the name suggests, handles the responses to intrusions when the intrusion has been confirmed. The response can be in many forms, such as reinitializing communication channels or reorganizing the entire network where compromised nodes will be removed. As there is no one optimal solution for all problems, hence the response to the intrusion behavior will also vary with difference kind of intrusions.

In the paper, it also briefly discussed about a multi-layer integrated intrusion detection and response technique, where the intrusion detection module will be included in each of the nodes in all of the layers of the MANET. This is to provide a wider range of coverage and also obtain better performance when it comes to certain attacks. This is because some attacks are often passed off to be legitimate in the lower layers (MAC protocol), but not when in higher layers (e.g. application layer). This multi-layer technique can drastically improve the performance of the IDS especially when there are large amount of attacks that can be easily identified in the higher layers, but not so in the lower layers. However, as the paper only covers the basics of the multi-layer integrated intrusion detection and response technique, it does not include details of the implementation.

16. Cluster-Based Intrusion Detection Technique in MANET

Thus far, we have discussed about intrusion detection technique architecture for the ad hoc network that is cooperative, which was presented by Zhang *et. al.*, unfortunately, this technique comes at a high cost of precious battery power for all of the participating nodes. With limited power supply in the ad hoc network being an important issue, this may cause certain nodes that are running low on power to behave in a selfish manner in order to conserve their battery, hence not being cooperative with other nodes. In this scenario, this very act of selfishness has compromised the original intention of the cooperative intrusion detection architecture. As a resolution to the problem, Huang *et. al.*, has presented another technique for ad hoc networks, a cluster-based intrusion detection technique. In the remaining part of this section we will aim focus on the what's and how's of the technique as we briefly discuss on the cluster-based technique without going into details and specifics.

In this paper, it states that a MANET can be reorganized into a number of clusters, where no one node is left out as each and every node is a member of at least one cluster, and for every cluster there is at least one node that will be responsible for issues monitoring in a certain period of time, it is known as "clusterhead". As defined in the paper, the definition of a cluster is a collection of nodes that is within the same radio range with each other. This also means that whenever a particular node is selected as the role of being the "clusterhead", all of the nodes that are in the same cluster should be within the vicinity of 1-hop.

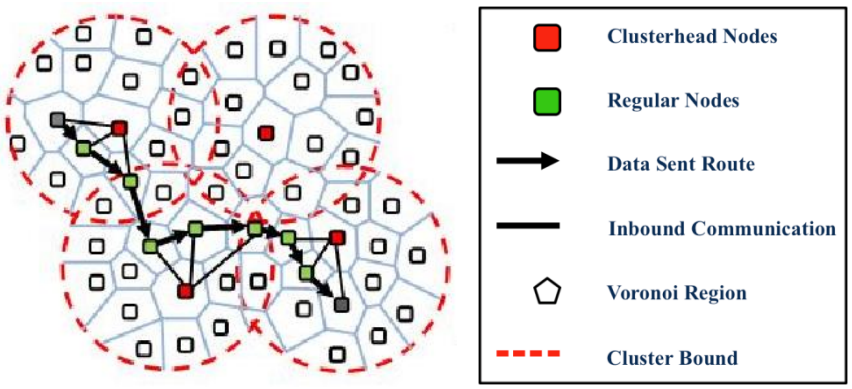

Figure 5. Sample illustration of a Cluster-based Intrusion Detection

It is vital for the cluster selection process to be efficient and fair. Efficiency reflects the process of some methods when it comes to choosing a node from the cluster every time with optimal efficiency. There are two (2) definitions of being fair in this context:

1. The probability of a node being chosen as the "clusterhead" should be the same across for all nodes, and
2. The time of each node being the "clusterhead" should be the same or identical.

Experiments have been carried to justify on the cluster-based intrusion detection technique, as the experiments evaluates on performance. The results obtained from the experiments shows that by comparison, the cluster-based IDS technique the CPU speedup is higher than that of the per-node based IDS technique and the network overhead for the cluster-based IDS technique is lower than the per-node based IDS technique, which is to be expected. Despite the promising results obtained which is in favor of the cluster-based detection technique, the detection rate for the cluster-based IDS technique is slightly lower than the per-node IDS technique. However, this is understandable, because from the vantage point of an entire cluster, there is only one node that is monitoring the traffic for the every one cluster, and therefore it is definitely prone to making less than precise judgment because of the limited processing power of just a single node.

17. Misbehavior Detection through Cross-Layer Analysis

As discussed earlier in regards to the multi-layer intrusion detection technique, it is a potential research area as pointed out by Zhang *et. al.,* in their paper [6], but in spite of that they did not go into detail with it. Therefore in this section we will discuss an analysis method that is presented by Parker *et. al.,* which is the cross-layer analysis method. In this paper, observation of the attack behaviors in MANET is performed and the findings tells us that there are some attackers that exploits several vulnerabilities at multiple layers simultaneously and keeping the severity of each attack low enough to not pass the detection threshold in order to avoid being identified and captured by the single-layer misbehavior detector. As the single-layer misbehavior detector does not detect this form of cross-layer attack, it makes it a far more dangerous threat than the single-layer attacks. However, this cross-layer attack can be detected with a corresponding cross-layer misbehavior detector. The cross-layer misbehavior detector works by initially gathering and compiling all of the inputs from all the layers of the network, then analyzing them in a comprehensive way by the cross-layer detector.

18. Intrusion Detection Techniques in MANET: Summary

In summary, with this chapter we have covered several typical intrusion detection techniques that are in the MANETs. With this we can say that because of the constantly changing topology and as well as with limited battery power, the intrusion detection mechanisms should be of a cooperative nature and also energy-efficient, which is as shown in the papers presented by Zhang *et. al.*, and Huang *et. al.*, respectively [6] [8]. With the topology constantly changing, and the mobility of nodes in the ad hoc network, it is relatively hard for a single node to gather enough of the information that is required if it depends solely on the single-layer detection method as it may be vulnerable due to the threshold that is configured.

4. Conclusion and Future Works

In this paper, we have attempted to inspect the security issues that reside in mobile ad hoc networks, which may very well be the main disturbance to the operation of it. With thanks to the mobility and open media nature of the mobile ad hoc network, it has similarly render the mobile ad hoc networks to be more susceptible to all sorts of security risks, such as information disclosure, intrusion or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher in demand as compared to those in the traditional wired networks. Firstly we briefly introduce the basic characteristics of the mobile ad hoc network. Due of the emergence of the concept pervasive computing, the need for network users to get connection with the world anytime at anywhere increases exponentially, which then also inspires the emergence of the mobile ad hoc network. With the convenience that the mobile ad hoc networks offer, they are also increasing security threats for the mobile ad hoc network, which deserves much attention. We then discussed some typical and dangerous vulnerabilities in the mobile ad hoc networks, most of which are caused by the possibilities that mobile ad hoc network offers us, such as mobility, constantly changing topology, open media and limited battery power. These vulnerabilities have made it necessary and vital for us to find effective security solutions in order to protect the mobile ad hoc network from all kinds of security risks. Lastly we introduce the current security solutions for the mobile ad hoc networks, which we started off with the discussion on the security criteria in mobile ad hoc network, which acts as a guidance for us in this area. We then also covered some of the main attack types that threaten mobile ad hoc networks. In the end, we discuss about several security techniques that can be used to aid with the protection of the mobile ad hoc networks from external and internal security threats. As mobile malware is currently growing and evolving, it is just a matter of time when it eventually rivals desktop malware. In this paper, we surveyed the behaviors of the current mobile malware. As part of our survey, we performed a thorough examination on the permissions of Android malwares. One of the common requests for Android malware is for the ability to send SMS messages without the user’s consent and this is something that is not a common sight among non-malicious applications. Despite that sole fact, we were unable to identify any other patterns that is permission-based that can be used for effective malware classification. During our observation noticed that none of the malware in that is in our data set was approved by the Apple App Store. This indicates that human review may be an effective malware deterrent. However, we were also able to witness that Symbian's automated review-and-sign process fared worse out of the three as almost one-third of the Symbian malwares that was in our data set was approved by or evaded this process. Apparently both malware authors and smartphone users currently are eager and motivated to find root exploits. And the root exploits are easily available as they are published by the homebrew community with the intent to help smartphone owners

customize their phones. Despite the good intent that the homebrew community has, malware can also utilize the same root exploits to circumvent smartphone security mechanisms, as it is displayed with four (4) of the malware in our data set did just this.

Acknowledgements

This paper is a revised and expanded version of a paper entitled "A survey on Mobile Security" presented at The 5th International Conference on Next Generation Computer and Information Technology, August 19-20, Harbin, China [14].

References

[1] A. Mishra and K. M. Nadkarni, "Security in Wireless Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, **(2003)**.
[2] L. Zhou and Z. J. Hass, "Securing Ad Hoc Networks", IEEE Networks Special Issue on Network Security, **(1999)** November/December.
[3] Y. Zhang and W. Lee, "Security in Mobile Ad-Hoc Networks", in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, **(2005)**.
[4] P. Papadimitraos and Z. J. Hass, "Securing Mobile Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, **(2003)**.
[5] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.
[6] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-hoc Networks", in Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, Massachusetts, **(2000)** August, pp. 275–283.
[7] J. Hamada, "New Android Threat Gives Phone a Root Canal", Symantec, http://www.symantec.com/connect/blogs/ new-android-threat-gives-phone-root-canal, **(2011)**.
[8] C. Peikari, "PDA attacks, part 2: airborne viruses-evolution of the latest threats", (IN) SECURE Magazine, **(2005)**.
[9] A. Schmidt, H. Schmidt, L. Batyuk, J. H. Clausen, S. A. Camtepe and S. Albayrak, "Smartphone Malware Evolution Regisited: Android Next Target?", In MALWARE, **(2009)**.
[10] A. Shevchenko, "An overview of mobile device security", http://www.viruslist.com/en/analysis.
[11] S. Toyssy and M. Helenius, "About malicious software in smartphones", Journal in Computer Virology, **(2006)**.
[12] Trend Micro, A Brief History of Mobile Malware; http://countermeasures.trendmicro.eu/wp-content/uploads/2012/02/History-of-Mobile-Malware.pdf
[13] Evolution! From Creeper to Storm; http://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/07ws/malware/evolution_report.pdf
[14] J. H. Chan and J. L. Hong, "A survey on Mobile Security", 5th International Conference on Next Generation Computer and Information Technology, Harbin, China, August 19-20.

