（様式５）

学 位 論 文 要 旨

平成 28 年 8 月　　日

学位申請者
Noor Afiza Binti Mat Razali　　印

学位論文題目

Remote Detection Method of Operating Environment in Cyber Security Attack and its Countermeasure

学位論文の要旨

Virtual machines (VM) provide ease of use through its on-demand characteristics and benefits in terms of lowering costs and improving scalability. Additionally, VMs are also used as security systems such as malware detection systems. Recently, with the rapidly expanding usage of mobile devices, VMs are now commonly used as emulators for scanning and detecting malwares that are embedded in mobile applications. Applications for mobile devices is checked by first running them in VM environments before being released to the public or end users. Such security checking for mobile application is done on VMs due to the constrained resources in mobile devices such as processing power, memory etc., that prohibited high end malware scanners to be executed in mobile devices. However, scanning and detecting malwares process using VMs may cause serious security threats to the end users. In particular, if a piece of malware can detect its current running environment, it may change its behavior in such a way that it doesn't perform malicious operations if it detected that it is running on VM environment as an emulator. This is a potential security hazard to end users, especially mobile device users. Therefore, security tests aimed against applications for mobile devices on VMs may not be effective in detecting malwares.

In this dissertation, based on the problem statement discussed above, remote detection method of operating environment is presented. This research shows that the operating environment could be remotely detected by using IP and ICMP timestamps information in network packets. The remote detection is done by analyzing the patterns of IP and ICMP timestamps in replies packets received from the target environment. In the method, the following characteristic patterns of IP and ICMP timestamps from target environment are analyzed.

1) Differences between two successive timestamps in the replied packets
2) How many times identical timestamps are stamped between the packets

In this research, experiments were done to validate the detection scenario of full virtualization technology using VMWare vSphere, Oracle VirtualBox and Xen Hypervisor as the virtualization software. High performance servers were used in the experiment to emulate the actual VM environments in real life situations. High performance real machine was also used in the experiments as a comparison to the VM environments. Based from the analysis results of two measurements mentioned above, this research has successfully differentiated and detected the target operating environment. Differences in IP and ICMP timestamps behavior patterns has clearly been seen in the experiments data. By comparing the numbers of how many times the identical timestamps are replied in the received packets from real environment and VM environments, the results shows that more than 60% of the identical timestamps are stamped for 5 times in the continuously replied packets in real machine. In contrast, there are no identical timestamps stamped 5 times in the replied packets from VirtualBox, Xen and VMWare ESX. The reason is that, in VM environment,

timestamp operations are sometime interrupted to complete other operations and takes more time to complete job than real machine. The results validates the operating environment remote detection method using IP and ICMP timestamps characteristic that are proposed in this dissertation. Moreover, the detection method does not require any installation of software on the target machine which further increase its potential harm if it were to be used by malware to detect VM environments.

Based from the results, a countermeasure technique to disguise IP and ICMP timestamps characteristic from real machine such that it shows similar IP and ICMP timestamp patterns as the VMs are proposed. By using this technique, malware may not be able to differentiate between a real machine and VMs, thus providing protection to end users that are using real machine.

In the case of mobile devices, this research has also analyzed on the IP and ICMP timestamp characteristic pattern using 4 versions of Android operating systems. Android operating system was chosen as the target mobile device operating system because Android are commonly being used by majority of mobile devices and it is based on Linux platform that are open to public. Experiments results on mobile device running Android in this research shows that the differences between two successive timestamps in mobile device is 2, 3 and 4 milliseconds in 4 versions of Android that were tested. Meanwhile, for the latest version of Android running on hypervisor products, this research found out that the differences are either 0 or 1 millisecond for timestamps differences between two successive timestamps. This means that, more identical timestamps are frequently stamped for Android that is installed on VM environment. Conversely, identical timestamps are never stamped for Android on real mobile device environment.

As a conclusion, this dissertation proposed that network timestamps could be used as potential tools to remotely detecting operating environment that could be manipulated in cyber security attack. One potential usage of the method is by implementing it into video streaming application that hide the actual purpose of the application in detecting target machine operating environment using the method. Countermeasure mechanism to disguise the differences were also presented in this dissertation.

For future work, more test should be conducted to gather more data to determine more characteristic patterns that could be used as detection methods and in proposing mitigation methods to resolve those remote methods. Mechanism to identify and analyze malware that attached this remote detection method into applications installed on a mobile device could also be proposed. Also, behavior analysis of real malware could be done to determine how the malware behavior changed according to the running environment. The remote detection method and relationship with malware behavior could be implied in bigger framework during security policy implementation to avoid cyber security attack by taking consideration of malware behavior could change based on the detection of the operating environment.