International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:11, 2015

Suggestion for Malware Detection Agent Considering Network Environment

Ji-Hoon Hong, Dong-Hee Kim, Nam-Uk Kim, Tai-Myoung Chung

***Abstract*—**Smartphone users are increasing rapidly. Accordingly, many companies are running BYOD (Bring Your Own Device: Policies to bring private-smartphones to the company) policy to increase work efficiency. However, smartphones are always under the threat of malware, thus the company network that is connected smartphone is exposed to serious risks. Most smartphone malware detection techniques are to perform an independent detection (perform the detection of a single target application). In this paper, we analyzed a variety of intrusion detection techniques. Based on the results of analysis propose an agent using the network IDS.

***Keywords*—**Android malware detection, software-defined network.

I. Introduction

SMARTPHONES are always under the threat of malware, thus the company network that connected smartphone is exposed to serious risks. According to the malware monitoring results presented at Kaspersky, the number of attacks showed a dramatic growth, increasing nearly 10 times from 69,000 in August 2013 to 644,000 in March 2014 [1].

Because of this increase in malware, APK-based detection, during and rights-based detection, behavior-based detection techniques for the detection malware variety of smartphone that study, most of the single application performs the detection target, and each has the critical point. In addition, the in-house network environment by performing the above-mentioned simple host-based detection network than there is a big disadvantage is independent. In this paper, we propose a smartphone based on the functional optimization in-house malware detection agent in the network environment. Implementation of agent environment is a house or packet reassembly is possible IDS and IPS is installed network environment assume that Tagging is enabled using the reserved field of the TCP header during reassembly.

This paper is organized as follows. Section II analyzes the existing smartphone-based malware detection techniques and Section III, we derive the critical point analysis technique to classify as a key technology. Section IV describes the internal network environment and technology for malware detection algorithm used in agent. Finally, Section V concludes and enables using the reserved field of the TCP header packet during reassembly.

Ji-Hoon Hong and Nam-Uk Kim are with the Department of Computer Engineering, Sungkyunkwan University, Republic of Korea (e-mail: jhhong88@imtl.skku.ac.kr, nwkim@imtl.skku.ac.kr).

Tai-Myoung Chung is with School of Information Communication Engineering, Sungkyunkwan University, Republic of Korea (e-mail: jignoh@naver.com).

II. Existing Malware Detection Method

A. Outline

Smartphone-based malware detection techniques are classified as static/dynamic analysis. How to determine whether a malignant test without running the code through static analysis is malware, dynamic analysis is a method to determine whether malignant and run the malware manually.

B. Based on Signature

Signature-based techniques are to create a signature feature of malware and malware network traffic and compare them to the host detection techniques with techniques for creating the feature of malware by signature detection. The most important is the pattern matching of malware smartphone environment in the CPU, memory, battery, etc. These resources taking into account the restrictive environment lightweight, optimization that would feature.

1.Light-Weight IDS

Xiaoming Kou et al proposed lightweight IDS considering the android environment [2]. For general intrusion detection packet preprocessing, pattern-matching algorithm, such as the Snort to provide a lightweight function was applied. However, this technique is simply a rule-set, etc., because only a mere accept most of the functionality provided by libpcap and snort and optimization in runtime overhead there is a disadvantage that occurs.

Deepak Venugopala et al improvement it is proposed to reduce the memory usage for efficient pattern matching algorithm, which reduces the runtime [3]. This technique was applied to multi-pattern matching algorithm by modifying the pattern-matching algorithm of the existing Snort.

2. Behavioral Signature

Three other Abhijit Bose proposed a process behavior based detection framework, modify the android kernel [4]. Collect system call event of the application layer and create a malignant behavior signature in real time by monitoring the API call, and compared with pre-generated signature. Malignant behavior is a battery usage, memory usage of a particular process. But the advantage of this technique is that you can make more detailed detection of malware by monitoring the existing system call, disadvantage there is that the overhead is large and the data base necessary for the execution of the behavior signature.

C. Based on Behavior

Behavior-based detection techniques are analyzed, comparing the attack pattern of the malware analysis and execution flow of the process that occurs in the system

techniques for detection whether the intrusion.

1.SmartSiren

Jerry Cheng et al proposed saving the attack pattern to the proxy server to reduce the amount of smartphone resources. Method is detecting compare with the malignant behavior [5]. Lightweight agent is working Record and service activities, such as SMS, bluetooth. The log record is sent to the proxy server by using a WCDMA network or a WLAN, such as 3G / 4G. Compared with the average server utilization of existing smartphone users with analysis and detection whether the intrusion.

2.Crowdroid

Iker Burguera et al suggest that detection Crowdroid external attack via the outsourcing of the kernel system log collected by the monitoring call forwarding to the center server, center server [6]. Information passed to the server, the distance is compared with the conventional malware through the partition clustering (Partitional Clustering) algorithm. Finally, the application is the detection infected with malware. This technique detection of malware intrusion whether the segment to the application with the same name as a normal application and system call pattern analysis of this Trojan packaging.

D. Based on Taint Analysis

Dynamic analysis technique is based Taint analysis, Taint tracking technique referred to as the marking to certain data and to monitoring the process by which this data is transferred within the program log ram tracking code data flow. The smartphone applications are suitable to apply the Taint analysis because it runs in Dalvik virtual machine, but it is difficult to lower the overhead for tracing command-level data flow to the actual usable level.

1.SCanDroid

Adam P et al suggest that SCanDroid performing static taint analysis targets Java code [7]. The SCanDroid consists of a bytecode loader, Inflow filter, analizing of string data and flow, outflow filter and so on. Inflow filter checks whether the Attach a tag to the data based on the permissions set by checking it in the outflow filter. Coverage of static analysis is high advantage compared to dynamic analysis, did not apply to the actual android platform.

2.Taintdroid

William Enck et al. proposed a TaintDroid platform applying dynamic taint analysis on the android platform to prevent personal information from being leaked [8]. Modify the stack frame of the android was a technique to track the propagation process by adding the taint tag on local variables, functions, and parameters. In addition, the taint tracing in order to increase the efficiency of the resources used file-level, fuction-level, each divided into parameter-level storage, native system library, were to be applied to the virtual machine. TaintDroid is showed the overhead 14% in normal operations, and 27% in IPC.

III. Existing Malware Detection Methods Analysis

Existing smartphone malware detection techniques are classified as signature-based and behavior-based used in traditional intrusion detection system. In this chapter, it shall be classified as shown in Fig. 1, according to the key technologies used in each detection technique conversely differently.

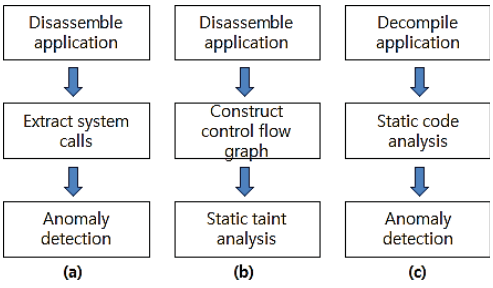

Fig. 1 Critical technique of malware detection

Each detection techniques can be classified in accordance with the core technology that will. (a) Extract system call: application to virtual machine to install the drive to try System Call OK, (b) Construct control flow graph: application of resources used, including the execution flow branch every generation that event the test, (c) Static code analysis: checking whether a combination of the application or permission is a violation of Intent, such as a specified Security Rules.

Critical point represented by the classification on Table I. Commonly, existing smartphone malware detection techniques are mostly single application performs the detection target. In addition, account the environment of the network simple host-based detection technique has the critical point.

TABLE I
Existing Detection Method Analysis

Detection method	Quantity
(a) Extract system calls	The use of a lot of system resources due to the installation and operation of the virtual application
(b) Construct control flow graph	This decision malignant impossible to scan a single event, in addition Taint analysis is necessary
(c) Static code analysis	Android third party property not considered in (optionally install the application users)

IV. Suggestion for Malware Detection Agent Considering Network Environment

Malware detection techniques for smartphones perform an independent detection (perform the detection of a single target application). Therefore, intrusion detection system offers a smartphone-based malware detection agent is considering building a large network environment such as a network, corporate network. The network operating system configuration is also the same as that proposed (Fig. 2). The border of the network has been built intrusion detection system, and performs equally signature/behavior-based intrusion detection and existing IDS. If it is determined in malware packet discards the packet, otherwise the packet forwarding in

case, if a determination of malware packet difficult to add functionality using the reserved field of the TCP header doubt packet tagging.

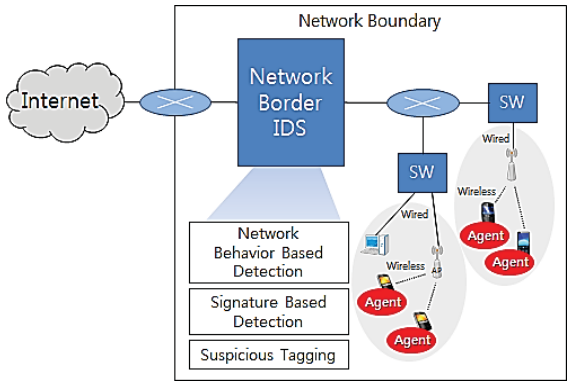

Fig. 2 System Architecture

Agent is installed on any smartphone connected via the wireless LAN to the network. The basic system modules are shown in Fig. 3.

Packet Tag Inspection Module to determine whether the use of the tagging suspects Libpcap. And use a proxy server to run without modification or platform administrator privileges.

Module checking the tag, and use the port number to find the destination process. In addition, classifies and manages the process to a suspect process. Next, a process is performed to track behavior, a typical system call, access to the device information, file access, memory access, access to the other process, and monitoring whether the API call is not allowed.

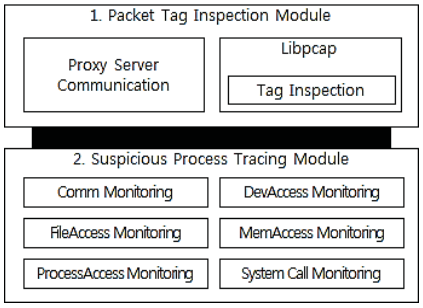

Fig. 3 System Module

The core of the agent, which is to offer a system call Sequence analysis of malignant behavior, a series of operation procedures as follows:

- Process is the primary component used to operate the Activity, Service, Content Provider, Broadcast Receiver inde all four kinds of components are implemented as JNI, libc, libstdc such acts as the library type.
- Process is also suspected to operate using threads and handlers receive, transmit the basic components and messages.
- Message is stored in the message queue, and performs transmission and FIFO operation by the module called Looper (accessible from the Application layer) present in the thread is received.
- Agent and hooking a message via the PID for the observed defaults table Looper Module suspect process (Process IDentifier).
- After analyzing the message and performs the malignant behavior scoring.

Malignant behavior scoring process that is used in the operation of the agent as follows:

- Table II shows a well-known malignant behavior of the feature. Sequence signature and generates a system call for library-call and in accordance with the feature.

TABLE II
MALIGNANT BEHAVIOR FEATURE

Malignant Behavior Feature
Replace the smartphone system application to another file
Function key failure and stop transmission and reception functions of telephony
Continuous scanning Bluetooth
SMS sent at random targets of the Java platform
Delete user data and stored text
Access address book, and then converted into a text SMS sent
Terminal information (IMEI, phone number, etc.) SMS sent
Telephony records, access to letters sent by the log recording screen text
Transfer the log information to a text by accessing the GPS information
memory card access, tried to force a written

- Measure the similarity of the signature and is, where reference signs are used for monitoring algorithm [9]. The algorithm operates in the background with minimal resources in smartphone market share, to determine the malignant behavior according to the number of system call. The default number of the system call (default) is present, the average number of the system call is used (mean) is calculated by (1):

$$M = \alpha * M_{new} + (1-\alpha) * M_{old} \quad (1)$$

α denotes the update coefficient, M_{new} represents the average number of the last system call. M_{old} is the average number of system call earlier, when the average update factor α is 0.5 or more in calculating the average value of the system call number of the last weight put on the system call number. max, is calculated by the (2).

$$\frac{\text{The maximum number of system calls}}{\text{The minimum number of system calls}} \quad (2)$$

It is possible to calculate the median value of the mean and max. The median value by calculating the average process values(*mean*) is the distance ΔM take the point *fallingM* relative to the mean. Total distance is $\triangle 2M$ system call number shall be placed between the $\triangle 2M$. If, falls below *fallingM* a suspected malignant behavior will increase if the system call number at a time until *risingM* in *fallingM* is confirmed as malignant behavior.

V. Conclusion

In this paper, we analyze intrusion detection techniques for a variety of research-based smartphone. Based on the results we propose an agent using the IDS network. Proposed agent in this paper is a lightweight feature to reduce the share of resources smartphone. Agents are a key signature for the library call, system call sequences of malware. Therefore, future research will generate a malware signature in the module for communication with and implement priority stored in a separate storage via a proxy server. This will be done after an analysis of the false positive for malware in accordance with the behavior of the agent.

Acknowledgment

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012-0005681).

This research was funded by the MSIP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2014 [2014044072003, Development of Cyber Quarantine System using SDN Techniques].

References

[1] Mobile Cyber Threats, Kaspersky Lab & INTERPOL Joint Report, http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf, 2014.

[2] Xiaoming Kou, Qiaoyan Wen, "Intrusion detection model based on android," Broadband Network and Multimedia Technology(IC-BNMT), 2011.

[3] Deepak Venugopala, Guoning Hub, "Efficient signature based malware detection on mobile devices," Mobile Information Systems, 2008.

[4] Abhijit Bose, Xin Hu, Kang G. Shin, Taejoon Park, "Behavioral Detection of Malware on Mobile Handsets", MobiSys '08 Proceedings of the 6th international conference on Mobile systems, 2008.

[5] Jerry Cheng, Starsky H. Y. Wong, Hao Yang, Songwu Lu, "SmartSiren Virus Detection and Alert for Smartphones", MobiSys '07 Proceedings of the 5th international conference on Mobile systems, 2008.

[6] Iker Burguera, Urko Zurutuza, Simin Nadjm-Tehrani, "Crowdroid Behavior-Based Malware Detection System", SPSM '11 Proceedings of the 1st ACM workshop on Security and privacy in smartphones, 2011.

[7] Adam P. Fuchs, Avik Chaudhuri, and Jeffrey S. Foster, "Scan -Droid Automated Security Certification of Android Applications", SPSM '11 Proceedings of the 1st ACM workshop on Security and privacy in smartphones, 2011.

[8] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, "Anmol N. Sheth, TaintDroid An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones", OSDI'10 Proceedings of the 9th USENIX conference on Operating systems design and implementation, 2010.

[9] W. L. Cholter, et al., "IBAN: Intrusion Blocker based on Active Networks" Proceedings of the DARPA Active Networks Conference and Exposition, May, 2002.