http://dx.doi.org/10.6109/ijice.2011.9.6.695

Effective Evaluation about the Antivirus Solution for Smart Phone

Suk-Jo Shin, Seon-Joo Kim, Chun-Yan Jiang, and In-Jun Jo, *Member, KIICE*

***Abstract*— Smartphone has formed a new market and introduced a new environment. They have an operating system like PCs, enabling free installation and removal of application programs. As the number of Smartphone users is increasing, more personal information is also exposed to malicious codes. There are problem of modification and deletion of files, battery consumption, and information leakage due to malicious codes. As the needs of Smartphone antivirus solutions are increasing, the antivirus solutions should be evaluated with quality characteristics. In this paper, we propose an effective evaluation method for functionality and performance of Smartphone antivirus solutions, and the best practices for evaluation.**

***Index Terms*— Antivirus Solution, A Derivation of Evaluation Item, Smart Phone**

I. INTRODUCTION

ACCORDING to the Korea Communications Commission report, the one out of five new domestic subscribers uses Smartphone, and the number of Smartphone users are over 1 million, and by 1002 million. Google Android operating system took up 59%, and Apple iOS had 26.5%.[1]

As Smartphones becomes popular, various security issues are raised due to protect data in Smartphone. Smartphone's performance has already reached the stage where PC-like. User can install or uninstall various software on the Smartphone, not use feature function on a phone. Thus, the conventional security threats that existed in the PC also exists in the Smartphone. The one of typical threats is malware.

The malware in Smartphone is more threatening than in the PC. Smartphone is used privately, so if Smartphone is infected with malicious code, the destructive power is unimaginable. It reveals Individual secrets, and causes turmoil in the mobile payment, and financial market. In particular phone is vulnerable to malware, because it is always turned on. So Smartphone anti-virus security solution is required in this situation.

In this paper, we develop effectively evaluation items for Smartphone antivirus solution, based on international standard ISO / IEC 9126 (functionality, usability, portability, and efficiency), configure the test environment, and tested a commercial product.

Manuscript received September 17, 2011; revised September 30, 2011; accepted October 8, 2011.

Suk-jo Shin is with the Department of Computer Engineering, Paichai University, Daejeon, Korea (Email: sukssj@pcu.ac.kr)

Sun-Joo Kim is with the Department of Computer Engineering, Paichai University, Daejeon, Korea (Email: uneedme@paran.com)

In-June Jo is with the Department of Computer Engineering, Paichai University, Daejeon, Korea (Email: injune@pcu.ac.kr)

II. SMARTPHONE INTRODUCTION

Smartphone is an intelligent phone with computing power, with PDA functions, Internet browsing function, e-mail, e-books, and remote control functions. It also has convenient user interface using touch-screen, and recognition of handwriting.

Internet browsing, e-mailing, on-line banking, making document, and using multimedia service are possible using Smartphone. Like PC, user can download from app store, and install various applications.

Smartphone can perform many functions, but it is not secure like PC.

As Smartphone users are increasing, they want more service instead of speech quality and SMS service. Smartphone is distinct from the existing mobile phones, because user can select thousand of application from app store.

TABLE I
UNITS FOR MAGNETIC PROPERTIES

OS	iOS	Android	Windows mobile	Blackberry OS	Symbian	Bada
Company	Apple	Google	Microsoft	RIM	Nokia	Samsung
Smartphone	iPhone	Nexus/Galaxy S	Omnia	Bold9000	Nokia 5800 Xpress Music	Wave
Multitasking	○	○	○	○	○	○
Advantage	User Friendly	Openness	Compatible with Windows	Messaging Speed	No 1 Market Share Compatible with Windows	Various Service
Application Store	app Store	Android Market	Windows Mark etplace	Blackberry Application Center	Ovi Store	Samsung Apps
Openness	X	○	△	X	○	×

III. SECURITY THREATS AND ATTACK METHODS

Smartphone's performance reached the level of the PC, and various traditional security threats that existed on the PC also exists in Smartphone. The typical security threats of Smartphone and failure categories by malicious code are the follows.

A. Security threats of Smartphone

There are various types and purpose of security threats of Smartphone. We categorize those into 6 classes: wireless network attack, unfair billing, virus/worms, prevent intrusion (break-in) attacks, DOS attacks, lost or stolen.

Wireless network attack is eavesdropping on phone calls or profiling or tracing usage records on wireless network.

Unfair billing attacks is possible wherever the internet is connected, and is a cross-service attacks, which are SMS / MMS bulk sending, and attack on the vulnerability of service.

Virus/Worm attack is malfunction attack like an information disclosure of personal data, stealing data on your phone, or sending spam.

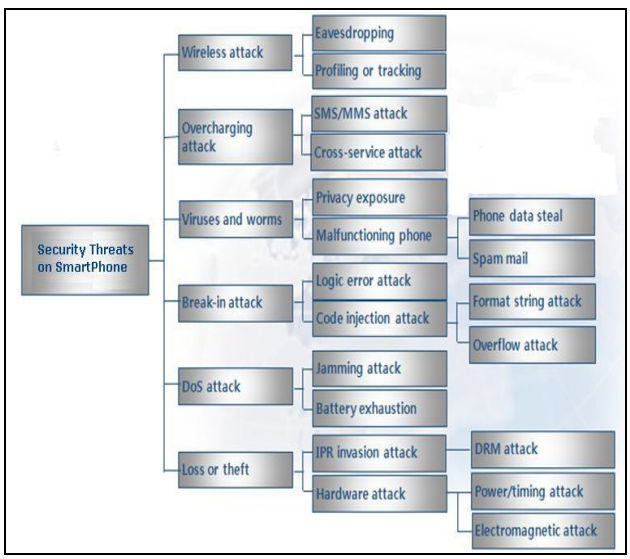


Fig. 1. Attacks on Smartphone

The break-in attack causes the logic error of phone, injects the object code in the phone, and is an overflow attack.

Denial of service attacks sends jamming signals or continuous service request to consume your phone battery.

Finally, if a user lost his phone due to neglect and threat of theft, there are attacks on data stored on a smart intellectual property, and attacks on authentication token through the electronic signatures analysis of time required to verify, and electronic magnetic attacks measuring the electromagnetic signal.

B. Types of Smartphone Malware

1) Failure causing malware

Failure causing malware makes Smartphone impossible to use, and modifies and deletes system file to interfere with normal operation, and deletes personal information.

The notorious malicious code was Skulls on Symbian OS which was discovered in 2004, changed all the menu icons with skull and blocked all function except call. There were Locknut which disabled some of the key button, and Gavno which disabled sending and receiving [4].

2) Battery consuming malware

This type of malware is malicious code causing battery consumes faster. Even though the battery production technology is fast, the phone consumes battery fast when using peripherals (Wi-Fi, Bluetooth, multimedia services, etc.).

The notorious malicious code was Cabir which scaned Bluetooth devices continuously.

3) Unfair billing malware

This type of malware is malicious code causing financial loss by endless trial to make a phone call or send SMS/MMS

The notorious malicious code was RedBrowser on J2ME platform which sent SMS to unspecified persons, and Kiazha which changed Smartphone screen with a warming message of asking money and deleted all stored text messages.

4) Information stealing malware

This type of malware is malicious code stealing user information, and changing the security settings of Smartphone and Smartphone serial number, OS, installed applications. The notorious malicious code were InfoJack, Flexispy, PBStealer which transferred the record of call and text messages to a server.

5) Cross platform malware

This type of malware is malicious code infecting PC through Smartphone. The notorious malicious code was Cardtrap.A which copying a worm to Smartphone memory card, so when the memory card was install on PC, it infected PC to delete data, and degrade performance.

IV. ISO/IEC 9126

A. ISO/IEC 9126

This standard on the SW quality characteristics and guidelines defines 6 quality characteristics, and 27 quality sub characteristics to measure software quality on user's perspective.

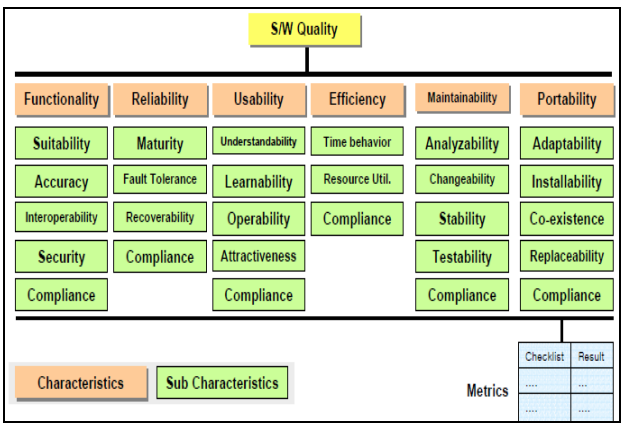


Fig. 2. Software product qualities

1) Functionality

The characteristics of the software product to provide functions which meet stated and implied needs when the software is used under specified conditions, interoperate with other system, prevent loss of important data, and evaluate the accessibility of programs and data.

2) Reliability

The characteristics of the software product to maintain a specified level of performance when used under specified conditions.

3) Efficiency

The characteristics of the software product to of resources used, under stated conditions. For example, the reaction time or resources to perform functions such as utilization is evaluated.

4) Maintainability

The characteristics of the software product to be modified. Modifications may include corrections, improvements or adaptation of the software to changes in environment, and in requirements and functional specifications.

5) Portability

The characteristics of the software product to be transferred from one environment to another. For example, the possibility of change, install/uninstall, and the compatibility with previous version are evaluated.

V. EVALUATION ON SMARTPHONE ANTI-VIRUS SOLUTION

A. Anti-Virus Solution's Introduction

There are several security solutions to deal with various security threats: F-Secure ANTI-THEFT FOR MOBILE, KASPERSKY Mobile Security, AhnLab AhnLab V3 Mobile, Hauri's ViRobot Mobile, NSHC Droid-x. <Table 2> describes the domestic security solutions.

TABLE II
DOMESTIC SECURITY SOLUTIONS

Product	Description
AhnLab V3 Mobile 	- Real-time detection and blocking malicious code - Improved diagnosis speed using patented search a specific code that speeds diagnosis - Alerts an application that uses personal information excessively and delete - Real-time monitoring files, and processes - Inspection SD memory card, and built-in memory (UMS) - Config diagnosis and treatment options - Scheduled inspection - Deleting information about the detected malware - Updates the engine using 3G, Wi-Fi, and Bluetooth network - Updates the engine using PC-sync - Updates the engine automatically and manually
ViRobot Mobile 	- Protect malware, and virus - Protect application based on behavior, and inspection hazard environment - Pattern update - Block SMS using phone number and keyword - Block using White list/Black list - Block incoming/outgoing call - Access control on Wi-Fi AP(Access Point) - Monitoring and protection on 3G data network traffic - Remote lock / delete - Locking SIM when changed - Encrypt file and directory - Browsing files in SD memory card - Authentication when executing the program

Droid-x 	- Scan and remove viruses, and malware - Real-time protection from virus and malware - O/S vulnerability analysis - Inspect and delete a SMS include malicious code - Detail inspect hacked phone - Anti-phishing, check illegal APP

B. Consideration

Note that when evaluating, we should make sure that S/W is developed for functionality, performance, and security. These characteristics are related to the reliability of its products. A Smartphone anti-virus solution is running on Smartphones, not like software running on PC. In particular, when running Smartphone anti-virus solution, main features like call or SMS / MMS functions should not affect. Thus, main features of Smartphone, and anti-virus solution must be evaluated at the same time.

C. Evaluation Items

As shown in section 5A, there are differences in functionality depending on the manufacturer. Thus, evaluation time and evaluation methods should be different.

Derived evaluation items using ISO / IEC 9126 for Smartphone anti-virus solution are the follows:

Functionality:
1. Real-time scan malicious code
2. Automatic scan and detection when SD memory card is connected
3. Inspection application based on behavior
4. Inspect blocking phone number and SMS
5. Inspect blocking unauthorized e-mail and file transfer when wireless internet is connected
6. Monitoring connection using 3G network and Wi-Fi network
7. Monitoring data communication
8. Update virus patterns automatically/manually

Reliability
1. Even if an error occurs in the anti-virus solutions should be driven normally, and perform without conflicting with other applications should be evaluated.

Usability:
1. Report
   Inspection result.
   Incoming/Outgoing record of blocked phone number list.
   Communication history of applications.
   Update history.
2. Statistic data
   Data communication statistics for a given period.
   Spam blocking statistics for a given period.
3. Alarm
   Alert when detect malicious code.
   Alert when data communication increases rapidly.
   Alert when blocking spam.
4. Configuration
   Configure scanning and curing method for malicious code.
   Configure update period.
   Configure network(3G, Wi-Fi), etc.

Portability:
1. Solution install/uninstall.
2. After installing solution, the operation of other applications (web browsers, e-mail transmission, Internet banking, document editing, etc.).
3. Internet information search, e-mail transmission, Internet banking, make document using Smartphone.
4. Call and SMS/MMS, when scanning malicious cod.

Efficiency:
1. CPU utilization and memory usage when scanning malicious code.
2. Time to scan malicious code.
3. Detection rate of malicious code.
4. False detection rate of malicious code.

VI. TEST ENVIRONMENT AND RESULT

According to the evaluation items derived in Section 5.3, we tested two products on Samsung mobile phone: AhnLab V3 Mobile, Hauri ViRobot Mobile.

TABLE III
TESTED PRODUCTS

Product	AhnLab V3 Mobile	ViRobot Mobile
Test equipment	Samsung Galaxy (SHW-M110S)	Motorola MOTO GLAM (XT800W)
Build version	Android 2.2	Android 2.1

As shown in Table IV, there is more than three times in a specific point. it is affected by the scanning method and the number of signature. The scanning time isn't a critical factor, but more accurate malware detection is more important.

TABLE IV
TESTED RESULT

Quality Characteristic	Evaluation item	AhnLab V3 Mobile	ViRobot Mobile
Fuctionality	Real-time scan malicious code	O	O
	Automatic scan and detection when SD memory card is connected	O	X
	Inspection application based on behavior	O	O
	Inspect blocking phone number and SMS	-	O
	Inspect blocking unauthorized e-mail and file transfer when wireless internet is connected	-	-
	Monitoring connection using 3G network and Wi-Fi network	-	-
	Monitoring data communication	-	O
	Update virus patterns automatically /manually	-	O
Reliability	After Antivirus solution process is forcibly terminated, and make sure that the program will restart normally	O	O
Usability	Report	O	-
	Statistic data	-	O
	Alert when detect malicious code	-	-
	Alert when data communication increases rapidly	-	O
	Alert when blocking spam	-	-
	Configuration	O	O
	Configure scanning and curing method for malicious code	O	O
	Configure update period	-	O
	Configure network(3G, Wi-Fi), etc.	-	O
Portability	Solution install/uninstall	O	O
	After installing solution, the operation of other applications (web browsers, e-mail transmission, Internet banking, document editing, etc.)	O	O
	Internet information search, e-mail transmission, Internet banking, make document using Smartphone	O	O
	Call and SMS/MMS, when scanning malicious code	O	O
Efficiency	CPU utilization and memory usage when scanning malicious code	-	-
	Time to scan malicious code	23"09	7"7
	Detection rate of malicious code	-	-
	False detection rate of malicious code	-	-

All evaluation items can not be applicable, because each phone has different features. Scanning time is also different because of number and size of files.

VII. CONCLUSIONS

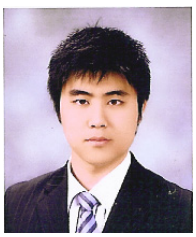
In this study, we derived evaluation items for Smartphones anti-virus solutions, and tested two product according to evaluation items. As a result, evaluation items cover all feature in two products.

However, without technical support for test equipment, the memory usage and CPU utilization, and false malware detection rates could not be evaluated. In this study we evaluated two products, and more products should be evaluated. An additional research on verifying false malware detection rate is needed

Evaluation items derived in this study can be used for the future introduction of smart anti-virus solution.

REFERENCES

[1] KCC, “Statistics for domestic Smartphone”, 2011.03.25.
[2] TTA, “Dictionary for information and communication”
[3] Dataworld, “INFORMATION SECURITY ALL GUIDE v.5", 2010. 02. 17.
[4] Kiyoung Kim, DongHo Kang, “Smartphone security technology on open mobile environment”, KIISC Vol 19 No. 5, 2009. 10.
[5] http://www.hauri.co.kr
[6] http://www.kaspersky.co.kr/sdk_anti-virus_mobile
[7] http://www.ahnlab.comhttp://www.ahnlab.com



Suk-Jo Shin received the B.S. and M.S. degrees in computer engineering from Paichai University, Daejeon, Korea, in 2008 and 2010.
He is currently pursuing a doctorate in computer engineering at Paichai University.

Sun-Joo Kim received the B.S. and M.S. degrees in computer engineering from Paichai University, Daejeon, Korea, in 1999 and 2001.
He is currently an research engineer in the S/W Quality Evaluation center at the Telecommunications Technology Association.
His current research interests include security testing and Common Criteria.

Chun-Yan Jiang received the B.S. degrees in computer engineering from Paichai University, Daejeon, China, in 2009.
She is study for a master's degree in computer engineering at Paichai University.

In-June Jo received the B.S. and M.S. degrees in computer engineering from ChonNam University, Gwangju, Korea, in 1982 and 1985, respectively, and the Ph. D. degree in computer engineering from Ajou University, Suwon, Korea in 1998. He is currently a professor in the computer engineering at Paichai University. His current research interests include security of mobile and network