International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.139-146
http://dx.doi.org/10.14257/ijsia.2015.9.1.15

A Simple Security Architecture for Mobile Office

Seungcheon Kim[1] and Hoon Jin[2,**]

[1]*Dept. of information Communication Engineering, Hansung University, South Korea*
[2]*Dept. of Computer Engineering, Sungkyunkwan University, South Korea*
[1]*kimsc@hansung.ac.kr*, [2]*bioagent@skku.edu*

Abstract

The Mobile Offices services based on Bring Your Own Device (BYOD) are getting more popular as the use of smart phone grows rapidly. As the free wireless services are being spread, malicious codes can be spread easily. Therefore, how we will provide security in an environment of free wireless has become an issue. This paper suggests security architecture for the better mobile office security and presents required procedures and the analysis of the expected security enhancement.

Keywords: *Mixed data type; BYOD, Security Architecture*

1. Introduction

The smart phone users are increasing at a high speed. A lot of government bodies and private companies are trying to utilize personal smart phones as for a business purpose. Therefore BYOD (Bring Your Own Device) becomes a new business culture of smart-work [1]. The Mobile office supports real-time communication and fast decision making process by connecting mobile devices to internal MIS systems. However, malicious codes have increased with smart phones diffusion. In 2013, about 1 million sorts of malicious codes are expected in android applications [2]. Basically BYOD is exposed to security vulnerabilities, because it uses personal owned private devices which usually company cannot control. If some devices are infected with malicious codes, internal MIS system may be contagious as well. Google-Play [3] doesn't adopt pre-verification systems, security vulnerabilities may exist. Therefore only safe applications, which are proved by trusted organizations, have to be allowed to install in BYOD devices. This paper proposes WLSA (White-List based Security Architecture) which can enhance the overall security level. The trusted authority organizations offer their application lists which are verified and a government office or neutral organization makes and maintains a WL. The remainder of this paper is organized as follows: Chapter 2 surveys the related research works and activities regarding WL systems; Chapter 3 proposes the WLSA scheme and procedure; Chapter 4 presents the analysis and expected advantages; and, finally, the paper concludes with a summary and suggestions for future work.

** Corresponding author is Prof. Hoon JIN

ISSN: 1738-9976 IJSIA

2. Related Work

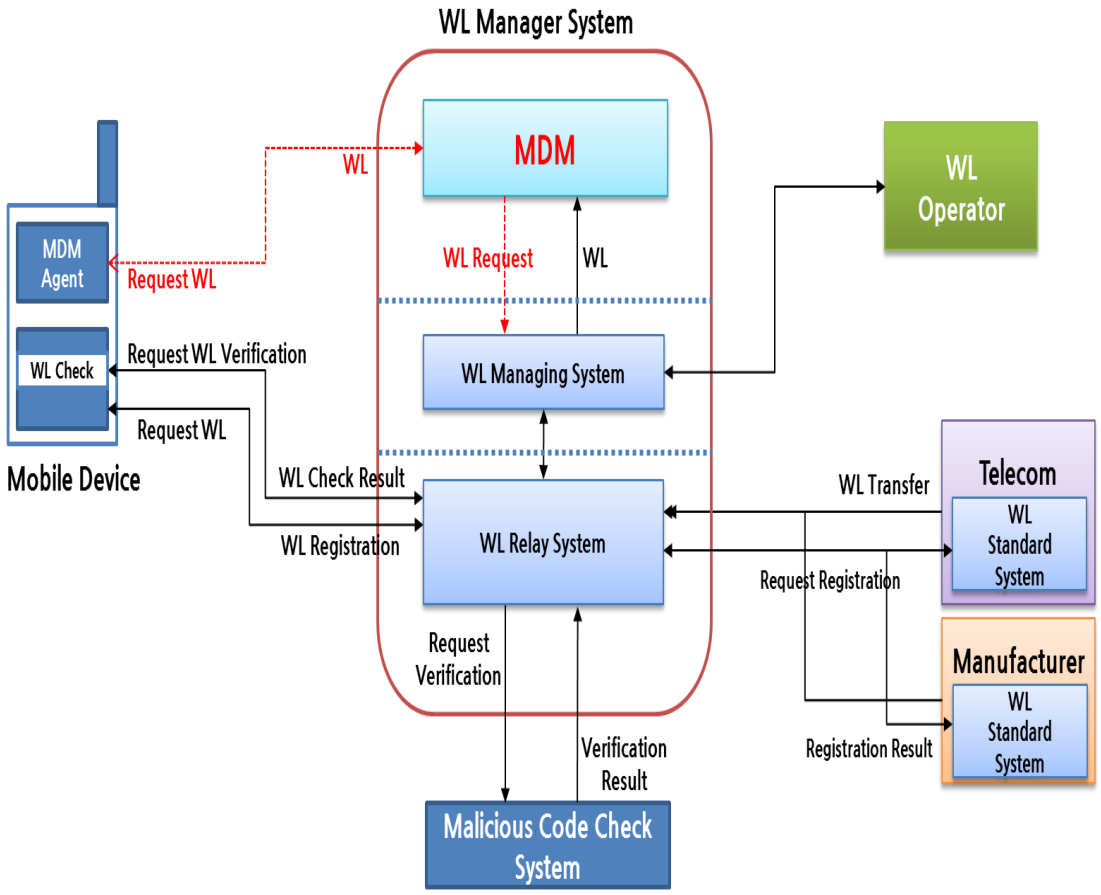

Figure 1. WLSA Diagram

A WL is defined as the trusted and safe applications list for smart phones. The WL is made by trusted or authorized organizations or companies, such as telecom companies, major smart phone manufacturers, government bodies and etc. On the other hands, there is a black-list which can identify malicious codes by containing applications list. Usually vaccine programs utilize blacklist based systems. WL based methods of blocking malicious codes were suggested by analyzing security threats [4-5]. A WL DB is an essential information container for enhancing security strength and user's convenience. Furthermore with previous research works, more detailed architecture regarding building and managing the WL is required.

3. Proposed Architecture

In order to make and manage a WL, the participation of trusted organizations is necessary. A basic WL component diagram is suggested as Figure 1. Trusted organizations, such as telecom companies or smart phone manufacturers, provide their own WL to the WL manager who operates main WL systems. The WL manager sends the list to the malicious verification system in order to recheck them. MDM (Mobile Device Management) systems utilize the WL for allowing or blocking application running on smart phones. Usually MDM agent software on mobile devices and MDM servers exchange WL information frequently in order to maintain update status. A MDM agent program checks the application on the smart phone when a user runs mobile office software. If MDM agent software finds applications which are absent from WL, then the

MDM agent take over the root authority from OS and stops mobile office applications as well as sends the application information to the WL manager system in order to check the safety.

The MDM agent which is installed in BYOD devices can reduce the range of application download as well as utilization. Therefore WL manager has to expand WL-DB to the enough range of application usages. Usually app markets of trusted organizations verify applications before upload on markets, therefore these markets are safer than usual android markets which are most frequently used. Figure 2 shows the information exchange procedures between WL providers and the manager. These procedures must be operated with very safe way.

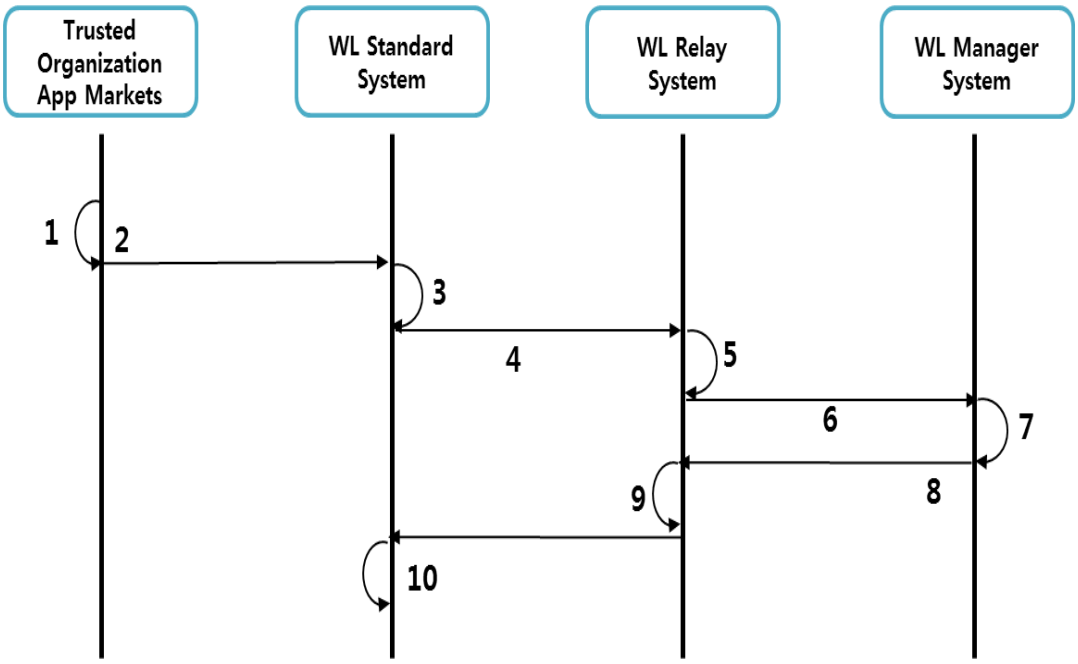

Figure 2. WL Transaction Procedures

1. Trusted organizations make WL message information, such as application name, maker information, hash information and *etc*., by extracting data from mobile applications from their app markets.
2. Trusted organizations transfer the message information to the WL standard sys-tem.
3. WL standard system performs electronic signatures and encrypts WL message in-formation.
4. WL standard system connects WL relay system and transfers the encrypted mes-sage.
5. WL relay system connects to the WL manager system.
6. WL relay system is ready to transfer the message to the WL manager system.
7. WL manager system decrypts the transferred message and verifies electronic sig-natures as well as hash data. WL manager system inserts received WL to the WL data base.
8. WL manager system notifies the result of the transaction to the WL relay system.
9. WL relay system registers the transaction history and closes the connection.
10. WL relay system transfers the transaction result to the WL standard system and finishes the procedures.

4. Analysis

Mobile Applications are categorized into three parts as Figure 3, ① White-List, ② Grey-List and ③ Black-List. Applications in white-list are considered safe, whereas applications in blacklist are unsafe. Applications in grey-list are not identified whether they are safe or unsafe. Therefore reducing the range of grey-list is very important for enhancing safety as well as the convenience of users.

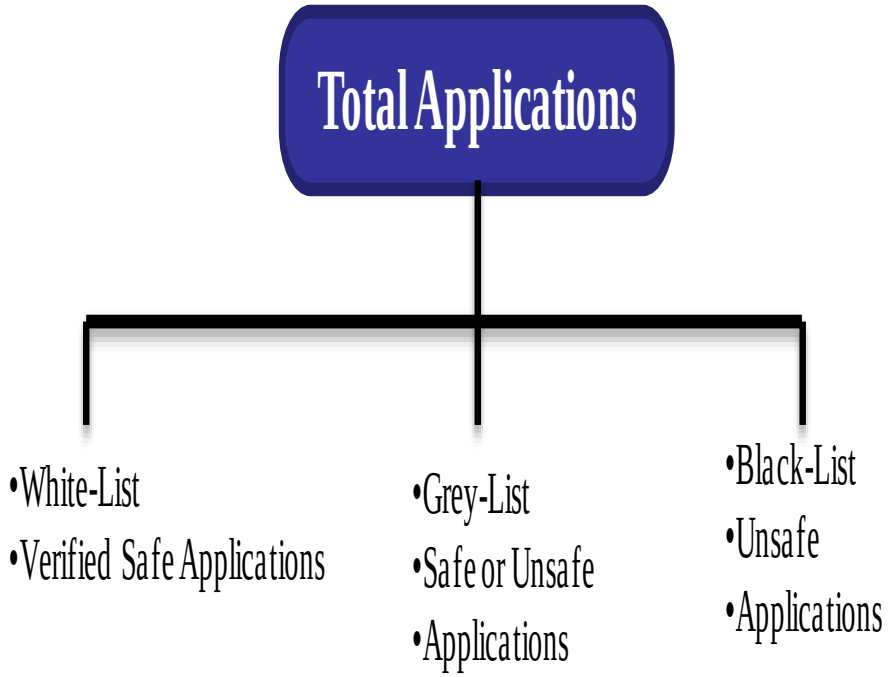

Figure 3. Application Category According to Safety

The total applications of Figure 3 can be presented as Eq. (1).

$$T_{APP} = N_{WL} + N_{GL} + N_{BL} \quad (1)$$

- T_{APP} : *Total number of mobile applications*
- N_{WL} : *Number of White-List applications*
- N_{GL} : *Number of Grey-List applications*
- N_{BL} : *Number of Black-List applications*

When a mobile user downloads applications from app-markets, the probability of infection by malicious codes is suggested as Eq. (2). First, if all applications in white-list are safe, then the probability of infection can be zero. Second, if applications in black-list are unsafe, then the probability of infection is 100%. Third, if applications in grey-list are not sure, then the probability of infection can be changed according to the app markets.

$$P_{MAL\_Down} = (N_{GL} * P_{MAL} + N_{BL}*100\%)/T_{APP} \quad (2)$$

- P_{MAL_Down} : *Probability of downloading malicious apps*
- P_{MAL} : *Probability of infection in Grey-List apps*

Most applications in black-list can be blocked by mobile vaccine programs, therefore N_{BL}* can be omitted as Eq. (3).

$$P_{MAL\_Down} = (N_{GL} * P_{MAL})/T_{APP} \quad (3)$$

We analyzed the probability of infection by download applications in grey-list. We assumed that the total applications (T_{APP}) in markets are 500,000 and the domain of grey-list (N_{GL}) may be 10%, 20% and 30% respectively. We supposed that the probability of malicious code infection (P_{MAL}) can be varied from 0.1% ~ 10%. Table 1 is parameters and values for the analysis.

Table 1. Analysis Parameters and Values

Analysis Parameters	Values
T_{APP}	500,000
P_{MAL}	0.1% ~ 10%
N_{GL}	T_{APP} * 10% or 20% or 30%

The result of the analysis is presented as Figure 4 and Table 2. In this analysis, we can have the range of possible infection from 5 to 15,000. It means that companies or organizations which use BYOD based mobile office services can prevent possible infection from malicious codes. As the domain of grey-list increases, the possibility of infection and inconvenience of users also become higher. Eventually it is highly desirable that all applications have to be categorized into white-list or black-list, but it is very hard because of the quantity and complexity of whole mobile application codes.

Table 2. Analysis Parameters and Values

T_{APP}	Possible Blocking Malicious Code by WL
T_{APP} 10%	5 (P_{MAL} 0.1%) ~ 5,000 (P_{MAL} 10%)
T_{APP} 20%	10 (P_{MAL} 0.1%) ~ 10,000 (P_{MAL} 10%)
T_{APP} 30%	15 (P_{MAL} 0.1%) ~ 15,000 (P_{MAL} 10%)

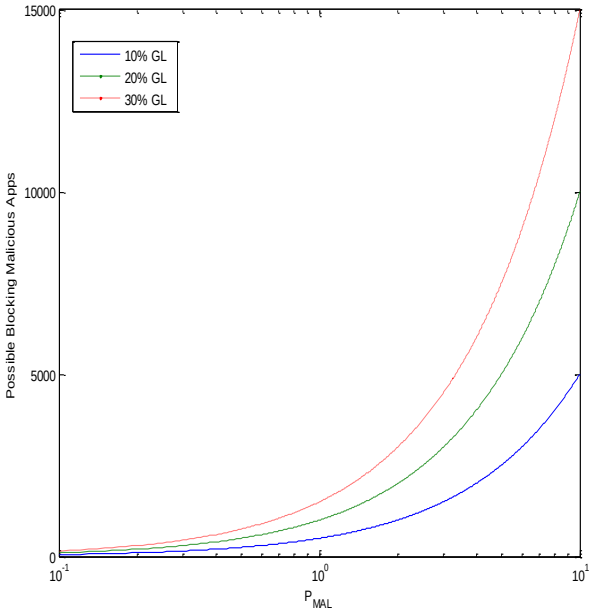

Figure 4. Number of Possible Malicious Apps According to P_{MAL}

5. Conclusion

The security architecture is very important for the safe mobile office environment using BYOD. However, there are considerable malicious codes in application markets because of post verification systems. Internal MIS systems can be exposed to various malicious codes via BYOD mobile devices. In order to reduce the possibility of infection, an application download policy from only safe application list is required. In this paper, we proposed WLSA (White-List based Security Architecture) for BYOD users as well as presented the analysis of possible expectations by using WLSA. WLSA can be a very complicated and large scale system, therefore WLSA should be driven only by government or major companies. If a white-list covers only small domain of whole applications, then it will cause user's inconvenience. On the other hand, if a white-list covers most domain except black-list, it can be utilized by most government officers, company staffs as well as citizen for public services. As a result, white-list can enhance the safety level and reduce the anxiety of infection.

Acknowledgement

This research was financially supported by Hansung University.

References

[1] K. W. Miller, J. Voas and G. F. Hurlburt, "BYOD: Security and Privacy Considerations", IT Professional, vol. 14, no. 5, (**2012**) September-October, pp. 53-55.
[2] S. Shankar, "As BYOD caches on, IT sector gets ready for 1M malicious apps", mydigitalfc.com, (**2012**) December 25.
[3] http://play.google.com
[4] K. Lee, R. S. Tolentino, G.-C. Park and Y.-T. Kim, "A Study on Architecture of Malicious Code Blocking Scheme with White List in Smartphone Environment", FGCN 2010, Part I, CCIS 119, pp. 155-163 Springer, Heidelberg, (**2010**).
[5] J. D. Stueckle, "Android Protectoin System: A Signed Code Security Mech-anism for Smartphone Applications", Air force institute of technology, Thesis, (**2011**) March.
[6] K. Y. Kim and D. H. Kang, "Smart Phone Security Technology in Opened Mobile Environment", Korea Institute of Information Security & Cryptology, vol. 19, no. 5, (**2009**).

Authors

Seungcheon Kim, He has received the B.S., M.S. and Ph.D. degrees in Electronic Engineering Department of Yonsei University, Seoul, Korea, in 1994, 1996 and 1999, respectively. He is currently with the Department of Information and Communication Engineering, Hansung University, Seoul, Korea, where he is responsible for teaching and research in wireless data communication networks, and ubiquitous sensor networks. He has worked as a post doctorial research fellow in the School of Electrical and Information Engineering in the University of Sydney, Australia, from 2000 to 2001, where he conducted research about 4G Mobile Wireless Communications. He's also worked as a senior research engineer in the Home Network Group of Digital TV Laboratory and the Digital Tech. Group of DA Laboratory, LG Electronics Inc., from 2001 to 2003, where he designed the Home Network Protocol and developed several Home Networking Devices. He has served as a director of Industrial cooperation research center in Hansung University. He was a visiting scholar in the department of computer science in the University of Oregon, United States, from 2009 to 2010. His

research interests include the traffic managements in Wireless and mobile communication networks, architectures of 4G Wireless Networks and the design of Home Networking Protocol and Ubiquitous Network Architecture.

Hoon Jin, He is a research professor at College of Information & Communication Engineering in Sungkyunkwan University. He learned and studied Artificial Intelligence, in detail, data mining, bioinformatics, agent system, semantic web. He received the Ph.D. degree in Department of Computer Science of Kyonggi University, Suwon, Korea, in 2007. After graduation, He worked at Korea Research Institute of Bioscience and Biotechnology (KRIBB) in Daedeok Science Town of Daejeon, Korea during 3 years as a post-doctoral researcher. Then He worked as a senior researcher at Creative Design Institute aiming for studying the product service systems design in 2010. Recently he has worked as a research professor/senior researcher, at Yonsei Institute of Convergence Technology, Yonsei University for 3 years. His main research interests are in fields of data mining, bioinformatics, ontology, semantic web technologies and now actively researches about biomedical text mining.