International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.373-380
http://dx.doi.org/10.14257/ijsia.2015.9.10.34

A Study on Mobile Device Control Model for Critical Data Leakage Prevention in the Enterprise Business Service

Yong-Suk Kang[1], Yoondeok Kim[2], Yongtae Shin[3] and Jong-Bae Kim[4*]

[1,3]Department of IT Policy and Management, Graduate School of Soongsil University, Seoul 156-743, Korea
[2,4]Graduate School of Software, Soongsil University, Seoul, 156-743, Korea*
E-mail: [1]postwin@gmail.com, [2]ghkdldjwls@naver.com, [3]shin@ssu.ac.kr, [4]kjb123@ssu.ac.kr*

Abstract

As information technology environment gets based on mobile, cloud, BYOD, mobile terminal just used for communication in the past is changed to support e-commerce and mobile office using the internet. However, threat of tap and information leak due to terminal loss, theft or infection of malware occurs. Corporations are strengthening access control and security through attaching sticker to a smart phone camera but it looks not enough as fundamental protection measures. In order to maintain high level of security, security control function should be applied and location-based entrants' security policy should be established so that a method to control mobile device can be directly suggested.

Keywords: *BYOD, MDM, Access control, Risk appraisal*

1. Introduction

Mobile terminal just used for communication in the past became an ultra-small terminal to provide business support services to support e-commerce, mobile business to support business while moving, as well as in e-mail using the internet. It is called a smartphone. In addition, enterprises anytime and anywhere is leveraging a system capable of performing the duties of the company by utilizing the mobile terminal and configure the mobile office in order to support them and that business trend is expected to strengthen. However, as use of smart phones and the terminals is expanded, there is high possibility that due to lost and theft of terminal and malware infection, privacy and company secrets can be leaked and actually information leakage happens due to malware infection. As a result, the company has strengthened security through issuing access card utilizing RFID for visiting work site and blocking network connection of terminal not registered and attaching a sticker to a smart phone camera but still the possibility of information leakage in utilizing smart phones lingers [1, 2]. In order to maintain high levels of security and access system, the application of methods that can directly control the mobile device accessing work site by connecting to work system through variety of methods like RFID, Beacon and time standard in link to access system is required and for this purpose we propose mobile access control measures [3].

2. Prevent Information Leakage

Data protection is composed of two axes of preventing invasion and preventing leakage and is defined as a way to protect the system by preventing illegal invasion in traditional

[4*] Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim).

ISSN: 1738-9976 IJSIA

sense. However, now that due to the leakage of various industrial information, damage to corporations increase and customer's information is leaked and then causes financial accidents, preventing information leakage is included in scope of recent information protection. This study includes not only intentional spills but also unintentional mistakes in the scope of information disclosure [4].

As emphasizing the importance of information, cases where the personal and corporate information is leaked using information technologies unlike previous methods increase. Leakage of personal information is a sensitive issue in most organizations that handle and process personal information. Since personal information leakage in Auction, Hanaro Telecom and GS Caltex in 2008, every year the personal information leakage incidents occur and its target is various like mobile communication companies, financial institutions and large internet companies regardless of the nature of the business. In addition, the personal information leakage incident causes the lowering of the corporate reliability, costs incurred in accordance with the class action as well as economic damage [4]. In particular, according to analysis of Korea Internet & Security Agency, 14.5% of companies suffered actual accident, 44.8% of which proved to be not reported to police. This shows significant leakage of personal information occurred considering unrecognized leak of private information. Damage caused by leakage of personal information is more serious than personal information leakage. The result of survey by Symantec and the Ponemon against 1400 employees of 277 corporation worldwide shows that damages due to information leakage increases, an average of $136 per information in 2012, more than 6 dollars up compared to average $130 in 2011. Accident costs due to information leaked by industries also differ. In the industries like health and financial section, where privacy information security is strict, it appears relatively high compared to other industries. As for causes of enterprise information leakage accident, 37% is a crime of malicious purposes, 29% is leakage due to system malfunctions and 35% turned out to be accidental incidents of people.

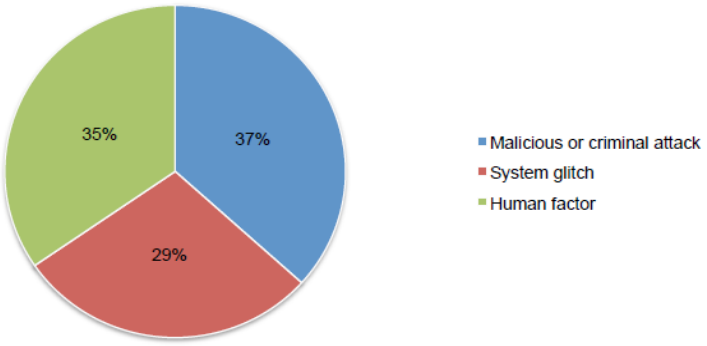

Figure 1. Ratio of Causes for Information Leak Accidents

In addition, the factors that affect this information leaks is the following 7 kinds.

Table 4. Factors Which Affect Information Leak Accident

No.	Factor
1	Presence of management manual for violation incidents of corporations
2	Positive attitude of corporations toward information security
3	CISO responsibility for corporate information security

4	Management mistakes of third parties (vendors, outsourcers, partners, etc.)
5	Prompt recognition and response to data breach harm
6	Loss of mobile devices, PC and media in which information is stored
7	Has recovery experts been hired specifically for data breach accidents and its recovery?

Disclosure of privacy and state secrets, business secrets may degrade the reliability of the organization and at the same time causes fatal damage to corresponding organization and so active action is required. However, as various terminals like BYOD (Beyond Your Own Device) etc. emerges and they are used in work, there are limits in preventing everything by existing access control system and so proactive measures to overcome them should be provided.

3. Facility and Access Security

The original purpose of the facility and access security is security control to protect it from outside attack but now it is focused on protecting the trade secrets of intangible assets that are directly related to the survival of businesses. Access control systems is to protect internal personnel, prevent intrusion, protect internal important facilities and various information by restricting the access of entrants to offices, laboratories, general business, airport and military unit as well as important places of building and vulnerable parts. Most of these access control systems have cards checked when accessing using RF card in which unique ID number is stored, based on RFID and bio-recognition technology and controls access by storing the unique ID in a terminal that registers biometric information in case of using bio-recognition technology such as fingerprint recognition, facial recognition and iris recognition. The basic configuration of the physical access security system is that main processing unit such as access control controller (ACU: Access Control Unit) is used and contact input device such as RF reader or biometric device is used as input device. Reader input section transmits the unique ID number and limits the access through checking ID registration, access per gate and access time available based on the unique ID number of entrant. However, access control systems are simple systems which identify card of entrant and biometric information through a reader device to check its access history and it paths it can't access and in case entrant and access pattern for each path is changed due to fixed access level provided, it might not be identified and so it has vulnerability that it can't cope with access situations for access restricted areas. Also it can't identify relevance of access path since fixed access authority is used even if a person uses different path to get access to a specific area. In case of a mobile terminal owned by entrant, if function control is not conducted, information can be leaked through a camera and voice recording in security restricted areas and so steps for that is necessary. In order to improve this, LBS (Location Based Service) should be essentially used so that access control can be strengthened [5, 6]. Positioning systems can use GPS in case of outdoors and use methods like WLAN, Bluetooth, UWB [7] in case of indoors so that location of mobile terminal can be identified and security control function can be applied.

4. Security Threat and Vulnerability of Mobile Terminal

4.1 Threat of Portability of Mobile Terminal

The number of accidents like theft and loss caused by portable convenience of a mobile terminal is said to reach the monthly average of about 20 million units in 2010. This causes threats such as leakage of personal information and confidential information of countries and companies, providing infiltration route bypassing the main system and its resulting system is destroyed due to a lost or a stolen terminal. In recent years, smart network system where business of the company or organization is performed and the information is processed through the mobile terminal is being built and users save file, memory, calendar, video, pictures, and business file in mobile terminals and store it in the cloud via an App. Portable convenience and mobile work support can increase work efficiency because of instant access to work anytime and anywhere but lost or stolen issue in proportion to its portability also increases.

4.2 Threat of Contents of Mobile Terminal

The app installed on the mobile terminal is downloaded through various Internet markets and used by its installation. However, when you install the App through unusual illegal market or install untested App even through normal market, you are exposed to various security threats. In particular, in this case, because a malicious third party can increase the communication cost by sending an e-mail or text message to an unspecified number of mobile terminals by adjusting or even leak a specific user's sensitive personal information, leak of information, denial of service, SPAM, and illegal use, etc. can occur [8].

4.3 Threat of Openness of Mobile Environment

The mobile terminal has a higher performance and functionality than the common feature phone and its multimedia processing ability is also excellent. However, as the performance of the latest feature phone is improved, the characteristic that distinguishes the feature phone and a mobile terminal comes from their openness. Openness of the mobile terminal provides Wi-Fi and an external interface along with the traditional functions of the phone call. In addition, it is introducing the API (Application Programming Interface) using an SDK (Software Development Kit) for use in the development and construction of the system resources of an app. In terms of security, however, external interface extends the attack path of malicious code and internal interface makes it easy for malware to construct hidden mobile app for malicious developer or user. In addition, since there is variety of penetrating paths for attacking such as 3G, 4G, LTE, WiFi and Bluetooth in the mobile environment, it is difficult to control security threat which exists in each network. This openness will also provide a route of infection of malicious code.

4.4 Vulnerability of Low Performance of Mobile Terminal

The mobile terminal may have more various constraints than a typical computer environment. Biggest weakness is the limited battery capacity. In order to detect malicious threats such as Viruses, worms, Trojans, lots of effort is needed to apply security mechanism to detect and prevent them but it has difficulty due to structural performance issues in the mobile terminal. Recently mobile terminals equipped with high-capacity battery increases, But many apps show up as much as that. So applying security software like in a PC environment meets many challenges. Thus, the mobile terminal has environmental difficulty in detecting malware and conducting real-time monitoring and preventing leakage of confidential and personal information.

5. Model for Security Control Policy of Mobile Terminal

5.1 Strengthen Security Function Control of Mobile Terminal

Owner of a mobile terminal is not an enterprise but an individual in mobile security and so concern about the user's complaint is very serious. As a mobile work environment get common, In particular, the subject who uses mobile terminal is an individual even if it is the incorporate terminal device in a mobile office. This means, that no matter who is the owner of the mobile terminal, he or she can't help but feel inconvenience and anxiety as security is applied to terminal of individuals and so minimizing dissatisfaction and effective installation and operation should be done. The security control functions of the mobile terminal are composed of a remote control, password control and device control. Prerequisite to reflect a consistent security policy with minimal inconvenience of members is the following three. First, security control should be applied in order to use the company's business app. Second, the security control should be minimized in usual days. Third, when the mobile security controls have been removed, business apps in company should be banned to use. In addition, In order to prevent the core information within the enterprise from leaking outside through a camera, voice recorder, USB, etc., they should be strictly controlled. In order to apply it, a mobile security control should be carried out when their mobile terminal came into the house while those functions should be turned off automatically when it is outside the company.

5.2 Recognition of a Mobile Terminal Using A Positioning Service

Control of the mobile terminal import and export starts from the point when passing through access control system and the security policy can be reflected in accordance with movement path of a mobile terminal. In particular, it is possible for a large production facilities or military base to take advantage of the base station of Telecommunications Company and the WiFi AP and take advantage of the indoor positioning telecommunications company based on Beacon when you enter the room. Beacon is a technical mean and devices that can transmit and receive data each other by recognizing the position of a mobile terminal as a type of wireless sensor where short-range position recognition is applied. If you have the beacon device installed indoors in a specific place and a mobile terminal equipped with Bluetooth 4.0 technology approaches it, various kinds of information and service can be provided using a local area of communication technique while mobile terminals are mutually recognized.

Differences in location-based services and technologies, such as using existing NFC and GPS is that NFC can be used in a way of one to one contact within 10m but, Beacon has a long distance availability up to a maximum radius of 50 ~ 70m and data can be delivered to multiple users even if users only go through the installation location. In the case of GPS position signal in terms of location recognition, error of tens of meters from the present location of the mobile terminal, and when it is in an indoor location, confirmation of location is not possible. However, Beacon can be installed and utilized indoor and outdoor while a precise position can be detected up to about 5 cm. Location-based indoor location system is made up of a wireless signal sensing device, RM generation algorithm for the positioning, the positioning algorithm, and expressing system. Wireless signal sensing unit performs sensing technology, such as radio frequency, infrared, ultrasound, and sensing technology is sensing time, angle, frequency and signal strength.

5.3 Apply Role-Based Access Control Model

For effective access control of facilities and use of mobile terminal, role-based hierarchical access and use control should be implemented by applying a role-based

access control model based on classification of the access areas. Permission of access and mobile terminal control should be assigned in connection with degree of protection and security level of the entrant as well as the role, the title and the position of the entrant.

5.4 Apply Mobile Terminal Security Policy Based on Risk Appraisal

Starting from the time point passing through an access control system, control for mobile terminal should reflect security policy according to the movement path of the mobile terminal. At this time, the important thing is that control policies should be based on risk assessment and for that, Whitelist-based mobile terminal function should be allowed, Blacklist-based function should be blocked and policy should be established and reflected in three perspectives of policy of above actions.

6. Embody Security Control of Mobile Terminal

In order to prevent the company's core information from being revealed through a camera, a voice recorder and a USB, role-based access control and risk assessment- based mobile terminal security control policy should be applied. In order to do this, first the security control functions of the mobile terminal should be embodied. In order to use the company's work app as security policy for mobile terminals, above granular security controls should be applied and security controls for terminal should be minimized. In case mobile security controls have been removed, company's work app should not be used and access to protected areas of the company should not be allowed. In order to apply it, first access should be controlled through RFID-based SpeedGate and security access control for mobile terminal should be activated simultaneously at the same time access starts. Second, for the employee registered on Whitelist, security control function like camera should be activated in protected area after Beacon awareness and actions should be taken so that some functions can be used according to security policy in case of moving out of protected area. Third, it should be configured so that if any user registered on Blacklist like a new visitor comes, the Beacon Blacklist should be recognized, installation of MDM Agent should be induced and subsequently he should be allowed to pass SpeedGate. Fourth, security control functions of the mobile terminal should be activated during work hours.

The mobile terminal security control system implemented in this study was suggested in order to manage various security control functions and blocking various threats through interworking between the server and the client system and it was configured this way so that such policy can be reflected to client for control. In this case the server may check and determine the various conditions from the client and coordinate to process the service. It is operated through the interface of the control system, which is configured in this process. In mobile terminal security control system, its organization and policy can be centrally managed on single screen and convenient operating environment is provided through interlocking with the organization's HR DB. It provides the convenience of policy management created by integration of organization management screen and policy management screen and provides the function that makes application of the policy by the organization and applied organizations by policy to be checked. And it provides fine-grained control methodology (Allow / detection / blocking / exception) for the use of role-based security zoning controls and risk assessment-based security controls of functional mobile devices. If any person registered on the Whitelist / Blacklist for security control policies enters workplace carrying mobile terminal, I / O control policy defined in advance by the administrator is implemented so that immediate security is secured. By fundamentally blocking data transmission channel such as Wifi, Bluetooth and tethering pursuant to security policy defined in advance in the workplace, policy has been implemented so that attempt to leak information is prevented in advance. Leakage of important information should be prevented by banning fundamentally saving information

in memory in a smart device and external SD card through USB cable in the workplace. In case you lose your mobile devices in which MDM is installed, locating a lost device with function to locate the lost device and additional action (data deletion, factory reset, etc.) may prevent important information from being leaked. By enabling status of MDM Agent's installation, implementation and operation to be controlled in batch, releasing MDM from terminal manager using API of manufacturer on malicious purpose or by mistake is fundamentally banned. Additionally by registering and controlling all log records generated from registered mobile terminal, support of preparation and audit for post failure becomes possible.

7. Conclusion

Currently mobile device management industry is evolving rapidly from the MDM market to MAM market and has started to be used as infrastructure for factory automation and production automation. In this process, study on MDM and MAM technology is not yet enough since people will pay more attention to importance of the security issue. Vulnerability of mobile terminal has already been confirmed and so we try to study on method to support factory automation and production automation based on BYOD through research on the key technologies such as preventing forgery of application and message security in terms of interoperability according to the characteristics of mobile terminal.

References

[1] Lionel M. Ni, Yunhao Liu, Yiu Cho Lau, Abhishek P. Patil, LANDMARC: Indoor Location Sensing Using Active RFID, Wireless Networks, (2004), Volume 10, Issue 6 , pp 701-710
[2] Dong-Hui Yu, Sung-Hyun Weon, Propagation Delay Modeling and Implementation of DGPS beacon signal over the Spherical Earth, Journal of information and communication convergence engineering, 5(4) (2007), 295-299 (5 pages)
[3] Jung-Tae Kim, Analyses of RFID System Using Lighted Weight Algorithm, Journal of information and communication convergence engineering, 7(1) (2009), 19-23 (5 pages)
[4] HONG, YOUNG-RAN, Design and Implementation of a Framework for Risk Management of Data Loss, Department of Industrial and Information systems engineering Graduate School of Soongsil University (2013)
[5] Mu-Hsing Kuo, Liang-Chu Chen, Chien-Wen Liang, Building and evaluating a location-based service recommendation system with a preference adjustment mechanism, Expert Systems with Applications, (2009), Volume 36, Issue 2, Part 2, pp. 3543–3554
[6] Jun Wook Lee, Ok Hyun Paek, Keun Ho Ryu, Temporal moving pattern mining for location-based service, Journal of Systems and Software, (2004), Volume 73, Issue 3, pp. 481–490
[7] Lei Zhu, Sheng Sun, Menzel W., Ultra-wideband (UWB) bandpass filters using multiple-mode resonator, Microwave and Wireless Components Letters, IEEE, (2005), Volume 15, Issue 11
[8] Debevec E. M., Gates R. B., Masuda M., Pella J., Reynolds J., Seeb L. W., SPAM (version 3.2): Statistics Program for Analyzing Mixtures, Journal of Heredity, (2000), Vol. 91 No. 6 pp. 509-510

Authors

Yong-Suk Kang, he received his bachelor`s degree in Public Administration from Kwandong University in Korea in 1995. He worked in the IT field as an Information Security Architect over 20 years. Now he is the Vice President of SK infosec Co., LTD. since 2010.

Yoondeok Kim, he received his bachelor's degree of Computer Science in Korea Polytechnic University, Siheung(2014). He is currently taking his master's degree in Software Engineering in Graduate School of Soongsil University in Seoul. His current research interests include Ontology and Machine Learning.

Yong-Tae Shin, he is a Ph.D. professor in the School of Computer Science and Engineering at Soongsil University, Seoul, Korea. His research interests focus on Multicast, IoT, Information Security, Content Security, Mobile Internet, and Next Generation Internet.

Jong-Bae Kim, he received his bachelor's degree (1995) and master’s degree (2002) in Business Administration at University of Seoul, Seoul, doctor’s degree in Computer Science at Soongsil University, Seoul (2006). Now he is a professor in the Graduate School of Software, Soongsil University in Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.