Security Requirements of a Mobile Device Management System

Keunwoo Rhee[1], Woongryul Jeon[1] and Dongho Won[1]

[1]*Sungkyunkwan University*
2066, Seobu-ro, Jangan-gu, Suwon, Gyeonggi-do 440-746, Korea
{Kwrhee, wrjeon, dhwon}@security.re.kr

Abstract

Many enterprises are adopting Mobile Device Management systems to monitor the status and control the functionalities of smart phones and tablet PCs in order to solve the security problems of confidential enterprise data being leaked whenever a device is misused or lost. However, no criteria have been established as yet to evaluate whether such Mobile Device Management systems correctly provide the basic security functions needed by enterprises and whether such functions have been securely developed. Therefore, this paper proposes security requirements of a Mobile Device Management system by modeling a threat and applying a security requirement engineering methodology based on Common Criteria.

Keywords: *Mobile Device Management System, smart phone, tablet PC, Common Criteria, security requirement*

1. Introduction

The number of cases of confidential business information leakage via mobile devices has continued to rise. As such, enterprises are considering the adoption of a Mobile Device Management (MDM) system to manage not only the data stored in their employees' mobile devices but also hardware such as the cameras and USB ports of mobile devices [1, 2]. However, no criteria have yet been established to evaluate whether such MDM systems fully provide the basic security functions needed by enterprises and whether such functions have been securely and reliably developed.

Therefore, this paper proposes the first security requirements of an MDM system. The proposed security requirements contain the basic criteria with which to evaluate the essential security functions required by business organizations and to determine whether these security functions are correctly implemented. Consumers can refer to it to clearly present requirement of an MDM system for purchase. Developers can use the security requirements to improve the security and reliability of their products and evaluators of MDM systems can use it as a reference in their evaluation work.

This paper is organized as follows: Section 2 analyzes the architecture and operation of the MDM system. Section 3 identifies threats. Section 4 proposes security requirements of an MDM system which applies a methodology based on CC V3.1. And lastly, Section 5 presents the conclusion.

2. Mobile Device Management System

The MDM system comprehensively manages mobile devices by monitoring their status and controlling their functions remotely using wireless communication technology such as Over-

the-Air (OTA) or Wi-Fi, as well as managing the required business resources. Figure 1 shows the MDM system architecture and operation [3, 4, 5, 6, 7].

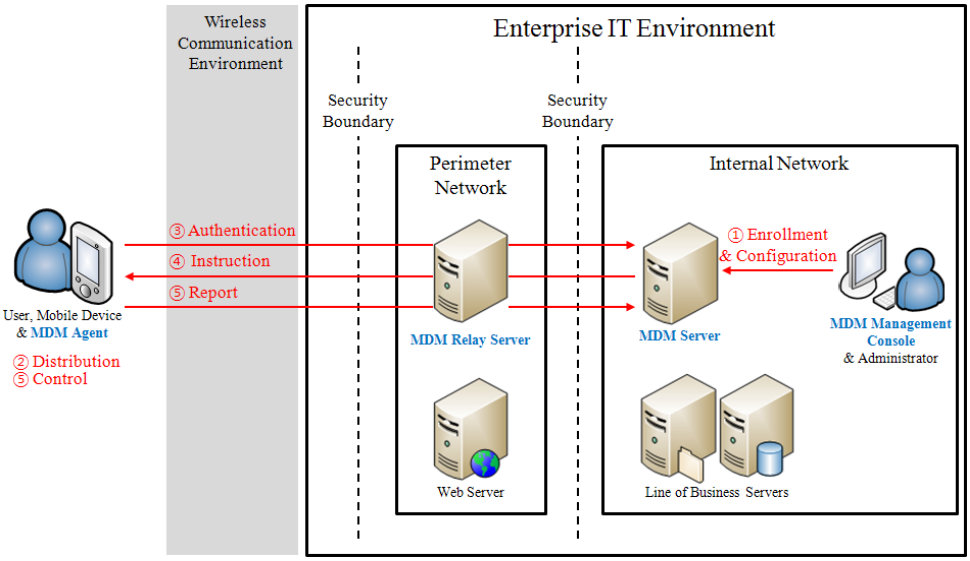

Figure 1. Mobile Device Management System

Operation among the above four components is executed in five steps, of which Step 4 and Step 5 are repeated regularly and as needed [3, 4, 5, 6, 7].

Step 1. Enrollment/Configuration: The mobile device data and user data of the organization are registered in the MDM system and the policy to be applied to each mobile device is configured.

Step 2. Distribution: The MDM agent is distributed and installed in the users' mobile devices. The MDM agent can be distributed through the application store/market or in-house.

Step 3. Authentication: When an MDM agent is run after installation, the mobile device data (IMEI, IP/MAC address, phone number, etc.) are sent to the MDM server to verify whether they match the data registered in the system.

Step 4. Instruction: The MDM server sends to an MDM agent the mobile device control policy and commands like "remote wipe" according to the mobile device status data and user.

Step 5. Control/Report: The MDM agent controls the functions of the mobile device according to the mobile device control policy/command and reports the results to the MDM server.

3. Threats

Threats must be clearly identified in order to accurately deduce the security requirements. Since a threat consists of an attack performed by a threat agent on an asset, it is important to correctly identify attacks [8].

To analyze the attacks that a threat agent can perform, we studied the currently known vulnerabilities of mobile devices [9, 10, 11]. The attacks stated in the PP of a system similar to the proposed MDM system were reused [12, 13]. Table 1 shows the identified threats of the MDM system.

Table 1. Threats

Threat	Description
T1.Disclosure	Threat agent can leak the confidential data saved in the MDM system or the operational environment of the MDM system as well as data transferred between the components of the MDM system.
T2.Software	Threat agent can modify the operating system or application of the operating environment of the MDM system.
T3.Bypass	Threat agent can bypass the security functions of the MDM system to incapacitate the security features of the MDM system.
T4.Data(1)	Threat agent can change the data saved in the MDM system in an unauthorized way.
T5.Data(2)	Threat agent can change the data transferred by the MDM system in an unauthorized way.
T6.Traffic	Threat agent can capture and analyze the data transferred by the MDM system and leak the confidential information.
T7.Spoof	Threat agent can access the MDM system via consecutive authentication attempts or reuse the authentication data to impersonate the authenticated user/administrator.
T8.Malware	Threat agent can infect the MDM system with malware and execute the malware.
T9.DoS	Threat agent can inhibit normal operation of the MDM system.
T10.Leakage	Threat agent can extract confidential data from the data remaining in the MDM system and the operating environment of the MDM system.
T11.Record	Threat agent can exhaust the storage capacity of both the MDM system and the operating environment of the MDM system so that security-related events and data essential to the MDM system's functionality will not be recorded.
T12.Disaster	Threat agent can stop the operation of the MDM system in the event of an unforeseen natural disaster such as an earthquake, fire or flood.
T13.New	Threat agent can attack an MDM system using a new unknown vulnerability.

4. Proposed Security Objectives and Security Requirements

4.1. Security Objectives

This section deduces security objectives which correspond to the identified threats. The security objectives provide high-level solutions to the identified threats.

Table 2. Security Objectives

Security Objective	Description
OE1.Location	The MDM server, relay server and management console of the MDM system components should be located in a physically safe location and protected by the network security system.
OE2.Admin.	An administrator of an MDM system should not have any malicious intent, and must be properly trained.
OE3.OS	Any service that is not needed is removed and any vulnerability is corrected to assure the reliability and security of the operating system of MDM server/relay server/management console.

Table 2. (*Continued*)

Security Objective	Description
O1.Audit	The MDM system should correctly record and safely maintain the security events to track responsibility for the security-related activities.
O2.Mechanism	The MDM system should provide a security mechanism (encryption algorithm, password, etc.) that conforms to the OSPs.
O3.Update	The MDM system should provide an update function for removing newly discovered vulnerabilities and improving performance.
O4.Data	The MDM system should protect the saved data from unauthorized exposure, alteration and removal.
O5.Channel	The MDM system should provide a secure communication channel to ensure reliable data transfer between the MDM system's components.
O6.Enrollment	The MDM system should provide a function for registering mobile devices and their users.
O7.Distribution	The MDM system should provide the means to distribute the MDM agent only through the method and path designated by the organization.
O8.IA	The MDM system should authenticate and clearly identify the user and the mobile device's activity before executing it.
O9.Authentication	The MDM system should provide a follow-up function in cases of authentication and identification failure.
O10.Access	The MDM system should enable only the authorized administrators to change the security configuration of the mobile device and should restrict general users from changing it.
O11.Status	The MDM system should provide the mobile device status data to the administrators and MDM server.
O12.Configuration	The MDM system should be able to apply the security configuration to mobile devices.
O13.Restriction	The MDM system should deliver a recognizable alert to the user /administrator when a user/administrator violates the OSPs when activating the MDM system operation, and restrict the use of the mobile device and MDM system.
O14.Deletion	The MDM system should assure that user data or functional data are not left over in the task domain used by the functions when it is terminated.
O15.Install	The MDM system should provide a function for installing only the authorized software in the mobile device, and should not enable the installation or removal of unauthorized software.
O16.Execution	The MDM system should provide a function for executing only the authorized processes in the mobile device, and should not install or remove any unauthorized processes.
O17.Anti-Malware	The MDM system should provide a means of coping with malware that infiltrates the MDM system or that already exists in it.
O18.Detection	The MDM system should provide a means of detecting and coping with illegal changes of the MDM system and the operational environment of the MDM system.
O19.Protection	The MDM system should prevent the termination or removal of the MDM agent by an unauthorized entity or user other than the administrator.

4.2. Security Functional Requirements

Security Functional Requirements (SFRs) are the set of security functions required to achieve the security objectives. In general, a developer can select the SFRs to achieve the security objectives from CC document [14].

Table 3 shows all SFRs include refined or extended requirements.

Table 3. Security Functional Requirements

Class	Component
Security Audit	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.3 FAU_STG.4
Anti-Virus	FAV_INT_EXT.1
Cryptographic Support	FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1
User Data Protection	FDP_ACC.1, FDP_ACF.1, FDP_APP_EXT.1, FDP_IFC.1, FDP_IFF.1, FDP_MDC_EXT.1, FDP_RIP.1, FDP_SDC_EXT.1, FDP_SDI.1, FDP_SDI.2, FDP_UCT.1, FDP_UIT.1, FDP_WIP_EXT.1
Identification and Authentication	FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2
Security Management	FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1
Protection of the TSF	FPT_ITC.1, FPT_ITT.1, FPT_ITT.2, FPT_STM.1
MDM System Access	FTA_MCS.1, FTA_SSL1, FTA_SSL.3,
Trusted path/cannels	FTP_ITC.1, FTP_TUD_EXT.1

5. Conclusion

This paper proposes security requirements which can be used as a request for a proposal to procure an MDM system, a guideline for developers to develop a secure MDM system, and criteria with which evaluators can evaluate the completeness of a developed system. Thus, the MDM system was analyzed, a threat was modeled, and CC based security requirements were deduced.

Acknowledgements

"This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program" (NIPA-2012-H0301-12-3007) supervised by the NIPA (National IT Industry Promotion Agency).

Corresponding author: Dongho Won.

References

[1] Sybase, Inc., Why Managing Mobility Matters **(2010)**.

[2] Cisco Systems, Inc., Global IT Survey Highlights Enthusiasm over Tablets in the Enterprise, Shows Customization, Collaboration and Virtualization as Key Features **(2012)**.

[3] Apple, Inc., iPhone in Business Mobile Device Management **(2010)**.

[4] Sybase, Inc., Afaria: A Technical Overview **(2011)**.

[5] Microsoft Corporation, System Center Mobile Device Manager 2008 Security Target Version 1.2 **(2009)**.

[6] R. Layland, J. Wexler, A. Datoo, A. George, O. Rege, J. Marshall, J. Herrema and B. Duckering, "The 2011 Mobile Device Management Challenge – Defusing Mobile Anarchy in the Enterprise", Network World and Robin Layland present **(2011)**.

[7] T. Henderson, "How mobile device management works", IT WORLD **(2011)**.

[8] CCMB, Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model. Version 3.1, Revision 3, Final, CCMB-2009-07-001 **(2009)**.

[9] C. Guo, H. J. Wang and W. Zhu, "Smart-Phone Attacks and Defenses, Proceedings of ACM SIGCOMM HotNets", **(2004)** November 15-16; San Diego, USA**.**

[10] G. Hogben and M. Dekker, "Smartphone: Information security risks, opportunities and recommendations for users", European Network and Information Security Agency **(2010)**.

[11] W. Jeon, J. Kim, Y. Lee and D. Won, "A Practical Analysis of Smartphone Security", Proceedings of HCII 2011, LNCS, vol 6771, pp.311-320, Springer, Heidelberg, **(2011)** July 9-14; Orlando, USA**.**

[12] National Institute of Standards and Technology, System Protection Profile-Industrial Control Systems Version 1.0 **(2004)**.

[13] H. Lee and D. Won, Protection Profile for Data Leakage Protection System. Proceedings of FGIT 2011, LNCS, vol 7105, pp.316-326, Springer, Heidelberg, **(2011)** December 8-10; Jeju, Korea.

[14] CCMB: Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components. Version 3.1, Revision 3, Final, CCMB-2009-07-002 **(2009)**.

Authors

Keunwoo Rhee received B.S. degree in Information and Communication Engineering and M. S. degree in Computer Engineering from Sungkyunkwan University in 2004 and 2006, respectively. He joined The Attached Institute of ETRI in 2008, and is currently a member of engineering staff of The Attached Institute of ETRI. His interests are cryptography, information security, information assurance, and security evaluation.

Woongryul Jeon received B.S. and M.S. degrees in Computer Engineering from Sungkyunkwan University in 2006 and 2008, respectively. During 2006-2008, he worked in Information Security Group (ISG). He is currently Ph.D. course student of the College of Information and Communication Engineering. His interests are cryptography, information security and information assurance.

Dongho Won received M.S. and Ph.D. degrees in Electronic Engineering from Sungkyunkwan University in 1978 and 1988, respectively. After working at ETRI from 1978 to 1980, he joined Sungkyunkwan University in 1982, and is currently a Professor of the College of Information and Communication Engineering. His interests are cryptology and information security.