High-Level Design for a Secure Mobile Device Management System

Keunwoo Rhee[1,⋆], Sun-Ki Eun[1], Mi-Ri Joo[1],
Jihoon Jeong[1], and Dongho Won[2]

[1] The Attached Institute of ETRI,
P.O. Box 1, Yuseong, Daejeon, 305-600, Korea
{kwrhee,eunsunki,mrjoo,jihoon}@ensec.re.kr
http://www.etri.re.kr
[2] College of Information and Communication Engineering,
Sungkyunkwan University,
2066, Seobu-ro, Jangan-gu, Suwon, Gyeonggi-do, 440-746, Korea
dhwon@security.re.kr
http://www.skku.edu

Abstract. Corporate security is threatened by Bring-Your-Own-Device trend. As mobile devices that provide high computing and wireless communication capabilities are increasingly being used in business, leakage of personal information and confidential data stored in a mobile device increases and bypass routes to corporate internal network are created by the mobile devices. A mobile device management system is a security solution to cope with these problems. This paper proposes platform-independent mobile device management system with using the Common Criteria for Information Technology Security Evaluation. As a result, the proposed design improves the security of the mobile device management system and guarantees high usability.

Keywords: mobile device management system, high-level design, Security Target, Common Criteria.

1 Introduction

ISO/IEC 15408 - The Common Criteria for Information Technology Security Evaluation (CC) is widely accepted as a framework in which computer users can specify their security functionalities and assurance requirements, developers can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims [1]. Especially, The Security Target (ST) of the CC, an implementation-dependent statement of security needs for a specific identified Target Of Evaluation (TOE) [2], can be a basis for development method since it entails a systematic way of conforming security requirements. Therefore, in

⋆ Corresponding author.

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 348–356, 2013.
© Springer-Verlag Berlin Heidelberg 2013

this paper we specify the proposed Mobile Device Management (MDM) system based on the structure of the ST.

The structure of this paper reflects the overall structure of the ST. The remainder of this section, we give an overview of an MDM system. Section 2 summarizes security objectives and Security Functional Requirements (SFRs) to design a secure MDM system. Section 3 shows core modules and describe their functionalities. Section 4 presents the relationship between SFRs and the proposed system. Finally, Section 5 shows the significance and applicability of this paper.

1.1 Mobile Device Management Systems

An MDM system comprehensively manages mobile devices by monitoring their status and controlling their functions remotely using wireless communication technology such as cellular network or Wi-Fi, as well as managing the required business resources.

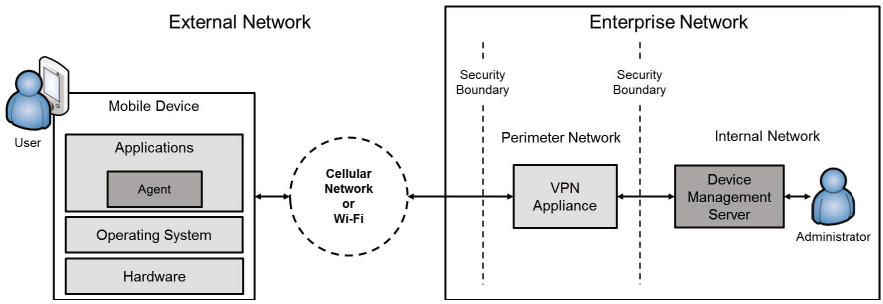

Fig. 1. The Operational Environment of an MDM System. The proposed MDM system is composed of an agent and a device management server. The security boundary includes firewall, IPS, web application firewall and so on.

The proposed MDM System consists of two main components, as shown in Fig. 1. We assume that an administrator connects to the DM server and manages the system via web browser:

An agent collects mobile device status data and sends them to the device management server [3]. It also applies policies received from the device management server to the mobile device and transmits the result back to the device management server [3]. The agent is installed on the mobile device as an application [3].

A Device Management (DM) server manages the data of registered mobile devices and users. In addition, it distributes the MDM policies and applications [3].

In the operational environment, a VPN appliance also plays a key role although it is not a component of the proposed MDM system. The VPN appliance authenticates incoming connection requests and securely relays the traffic between the agents and the DM server. Instead of a VPN, we can use validated cryptographic module [4] and communication protocol (e.g. IPSec, SSH, TLS, TLS/HTTPS) to establish a secure channel

In this system, data flows between the components are as follows.

Enrollment and Configuration (Administrator → DM server). The mobile device data and user data of the organization are registered in the DM system and the policy to be applied to each mobile device is configured [5].

Authentication (Agent → DM server). When an agent is run after installation, certain mobile device data (e.g. IMIE, IP/MAC address, phone number, etc.) are sent to the DM server to verify whether they match the data registered in the system [5].

Instruction (DM server → Agent). The DM server sends each agent the mobile device control policy, and commands such as 'remote wipe, according to the mobile device status data and the individual user [5].

Control and Report (Agent → DM server). The agent controls the functions of the mobile device according to the mobile device control policy or command. And then it reports the results to the DM server [5].

2 Security Objectives and Security Functional Requirements

At first, SFRs should be defined to design a secure system. The SFRs have been already defined in Rhee's researches [5,6]. Rhee's researches are based on the structure of the Protection Profile (PP) [2] to define SFRs. Thus, the security problems are identified by analyzing threats, organizational security policies, and assumptions and then the security objectives are provided as high-level solutions to the identified security problems.

The proposed system cannot directly comply some of the SFRs defined in the Rhee's researches since the proposed system is a part of the system as defined in Rhee's researches. However, some other components such as a VPN appliance in the operational environment satisfy the SFRs which cannot directly be complied. This can be permitted if the components in the operational environment are certified and integrated with the proposed system. For example, Mobiledesk VPN v1.0 (KECS-NISS-0356-2011) [7] is a CC certified product.

The full description of the security objectives and SFRs can be found in [5,6].

3 System Design and Security Functions

In this section, we design the system architecture. Since the proposed system consists of an agent and a DM server, we describe their logical modules and data flow between them.

3.1 Agent

An agent is composed of six logical modules. They are application management, audit and report, communication, device control, policy management, and security management. Fig. 2 describes the architecture of an agent.

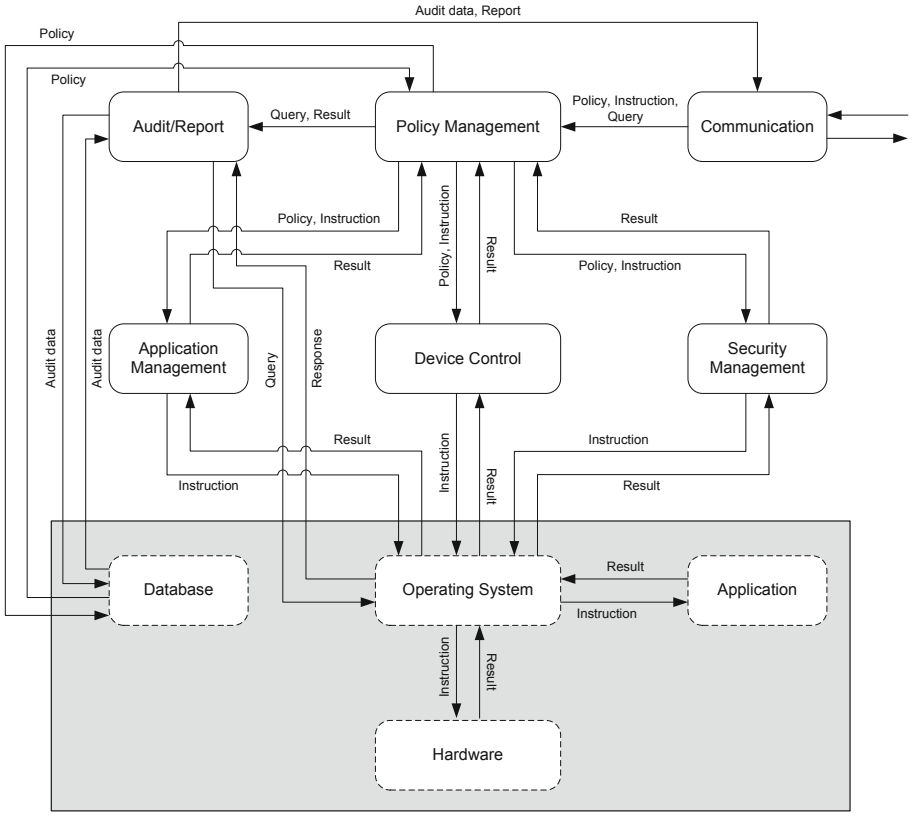

Fig. 2. The Architecture of an Agent. Actually, the applications and hardware modules are controlled by the operating system. For instance, the operating system controls the camera module of the mobile device according to the instruction from the device control module.

The application management module controls installation and execution of applications, updates applications, prevents uninstallation of enterprise applications, and removes unauthorized applications.

The audit and report module collects information of a mobile device and result of the instruction. And then it sends the audit data and the report to the communication module. When the communication module loses connection to the server, it stores the audit data in the database or as a file until the connection module reconnects to ensure that audit data are generated and stored in the DM server-side database.

[The information of a mobile device]

- assigned IP address
- SIM state
- version of the operating system
- installed application name/version/permission
- Bluetooth status
- Wi-Fi status
- GPS status
- phone number
- IMEI
- hardware resource
- data roaming setting
- device type

The communication module provides connections to the DM server. For efficiency, the agents and the DM server cannot make connections all the time. Therefore, when the push message arrived, it connects to the DM server and downloads policy and data.

The device control module controls the hardware devices and the functions provided by the platform.

[The hardware devices and the functions provided by the platform]

- USB portable storage, USB debugging, USB tethering
- Wi-Fi, Wi-Fi Direct, Wi-Fi hotspot
- Bluetooth, Bluetooth tethering
- File/data transfer via NFC and vendor provided protocols
- Synchronization via vendor provided applications
- Camera
- GPS
- Microphone
- External memory such as a SD card.
- Screen capture
- Screen lock
- Data reset or wipe

The policy management module manages configurations related to the application management, device control, and security management. It sends the policies or instructions to the application management module, device control module, and security management module. In addition, it verifies the integrity of the policy to prevent unauthorized modification.

The security management module sets authentication policy such as password, pin, and so on. In addition, it detects the modification of the platform and protects itself from the unauthorized deletion or stop.

3.2 Device Management Server

A DM server is composed of five logical modules. They are application management, audit and report, communication, identification and authentication, and policy management. Fig. 3 describes the architecture of a DM server.

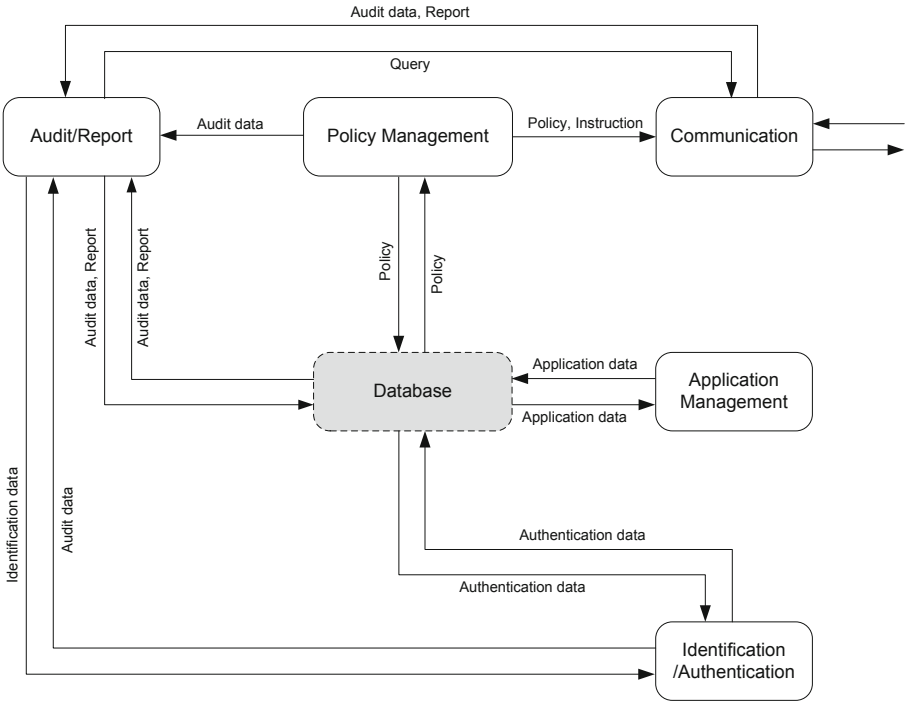

Fig. 3. The Architecture of a DM Server. Each module of the DM server provides user interface for administrator's management.

The application management module manages the list of permitted applications (whitelist) or the list of unpermitted applications (blacklist) with the hash values or digital signatures of applications.

The audit and report module manages audit data from the agents and administrative events (e.g. administrators login, policy change, etc.). In addition, it provides methods to search a specific audit event, a registered user or a mobile device.

[**Audit events**]

- Administrator's login
- Failure of login attempts (with the number of attempt)
- Session locking or termination
- Duplicate login attempts (with the ID)
- Registration of a user
- Modification of the information of an administrator, a registered user, and a mobile device
- Modification of the security policy
- Transfer a security policy or an instruction to the agents, response from the agents
- Violation of the security policy
- Start and stop of the audit and report module

The communication module provides connections to the agents. When the DM server transmits a new policy or instruction to the agent, the communication module sends push message to the agent first. In addition, it manages the session with the administrator and the agents.

The identification and authentication module authenticates and identifies administrator, user. In order to authenticate and identify them, it provides enrollment methods. Actually, this module authenticates and identifies users by information of their mobile devices.

The policy management module provides methods to configure the policy related to application management, device control, and security management.

4 Rationale

Table 1 indicates which components provide the SFR's functionality. Each SFRs claimed in Rhee's researches trace back to at least one components. In Table 1, FCS_CKM.1$\tilde{4}$, FCS_COP.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1, FPT_ITC.1, and FTP_ITC.1 are satisfied by the VPN. In addition, FPT_STM.1 is provided by the operating system. The operating system gets the trusted time from an NTP server, a base station, or a GPS satellite.

Table 1. The completeness of SFRs. Some functionality to satisfy the SFRs claimed in PP is provided by the operational environment. The letter indicates where the functionality to satisfy the SFRs is provided. 'A' means that the agent provides the functionality. 'S' means that the DM server provides the functionality. The letter 'E' means that the IT environment provides the functionality.

SFRs	Components	SFRs	Components
FAU_ARP.1	A, S	FDP_SDI.2	A
FAU_GEN.1	A, S	FDP_UCT.1	A, S
FAU_GEN.2	S	FDP_UIT.1	A, S
FAU_SAA.1	S	FDP_ERA_EXT.1	A
FAU_SAR.1	S	FIA_AFL.1	A, S
FAU_SAR.2	S	FIA_ATD.1	A
FAU_SAR.3	S	FIA_SOS.1	A, S
FAU_STG.1	S	FIA_UAU.2	A, S
FAU_STG.3	S	FIA_UAU.4	S
FAU_STG.4	S	FIA_UAU.7	A, S
FCS_CKM.1	E	FIA_UID.2	S
FCS_CKM.2	E	FMT_MOF.1	S
FCS_CKM.3	E	FMT_MSA.1	S
FCS_CKM.4	E	FMT_MSA.2	S
FCS_COP.1	E	FMT_MSA.3	S
FDP_ACC.1	A	FMT_SMF.1	S
FDP_ACF.1	A, S	FMT_SMR.1	S
FDP_APP_EXT.1	A	FPT_ITC.1	E
FDP_ETC.1	A, S	FPT_ITT.1	A, S
FDP_IFC.1	A, S, E	FPT_ITT.2	A, S
FDP_IFF.1	A, S, E	FPT_STM.1	E
FDP_ITC.1	A, S, E	FTA_CTL_EXT.1	A
FDP_LOC_EXT.1	A	FTA_MCS.1	S
FDP_MDC_EXT.1	A	FTA_SSL.1	A, S
FDP_RIP.1	A	FTA_SSL.2	A, S
FDP_SDC_EXT.1	A	FTA_SSL.3	S
FDP_SDI.1	A	FTP_ITC.1	E

5 Conclusion

In this paper, we use the structure of the ST to design a secure MDM system. Our approach is similar to the researches by Pedersen et al., 2006 [8] and Vetterling et al., 2002 [9]. It is very useful way to assure the security functionality. However, the TOE and the version of the CC are different. Besides, we focus on the more detailed modules and their relationship. The framework of the proposed platform-independent design may guarantee high usability.

References

1. Lee, K.: A Study on the Design of Secure Multi Function Printer conforming to the Korea Evaluation and Certification Scheme. Ph. D. Dissertation, Sungkyunkwan University, Suwon (2011)

2. CCMB: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 4 (2012)
3. Rhee, K., Won, D., Jang, S.W., Chae, S., Park, S.: Threat Modeling of a Mobile Device Management System for Secure Smart Work. Electron. Commer. Res. (to be appeared)
4. Module Validation List, Computer Security Resource Center, National Institute of Standard and Technology, http://csrc.nist.gov/groups/STM/cmvp/validation.html
5. Rhee, K., Jeon, W., Won, D.: Security Requirements of a Mobile Device Management System. International Journal of Security and Its Applications 6, 353–358 (2012)
6. Rhee, K.: A Study on the Security Evaluation of a Mobile Device Management System. Ph. D. Dissertation, Sungkyunkwan University, Suwon (2012)
7. Mobiledesk, Samsung SDS, http://www.sdsems.co.kr/WebContent/product/vpn.jsp
8. Pedersen, A., Hedegaard, A., Sharp, R.: Designing a Secure Point-of-Sale System. In: 4th IEEE International Workshop on Information Assurance, pp. 51–65. IEEE Computer Society Press, Washington, DC (2006)
9. Vetterling, M., Wimmel, G., Wisspeintner, A.: Secure Systems Development based on the Common Criteria: The PalME Project. SIGSOFT Softw. Eng. Notes 27, 129–138 (2002)