The Development of Mobile Device Management Framework on Android Platform for Devices Security and Applications

Kurnia Anggriani
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
kurnia.anggriani@students.itb.ac.id

Rinaldi Munir
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
rinaldi@informatika.org

Yusep Rosmansyah
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
yusep@stei.itb.ac.id

Abstract- The increasing number of mobile device usage and the policies of bring your own devices (BYOD) cause the diversity of data stored on mobile devices, not only personal data but also corporate data. Based on that fact, the number of threats are also increase. There are mobile malware and physical threats, such as loss of mobile devices and threats from user behavior. Therefore, the research conducted to develop a mobile device management framework, a tools to monitor, control and protect mobile devices. Qualitative method is used, domain analysis, the framework design and a framework prototype. The results of the study are the functional requirements of mobile device management, and a prototype framework of mobile device management on the Android platform. Functional requirements of mobile device management is 21 features obtained from the comparison of 3 mobile device management software wherein the features possessed by at least 2 software. Mobile device management framework consists of a server and a client. The server consists of a mobile device management, policies, networks and applications. Clients consist of seeing the policy and send a message to the server. Protoype has implemented 12 of the 21 features. The framework of mobile device management is developed on the Android platform. The results of the research are the functional requirements of mobile device management and a prototype framework of mobile device management on the Android platform. Testing of the framework is using black box testing, the benefits of framework testing and expert judgement. Mobile device management framework can be developed on other platforms such as iOS and Windows Phone.

Keywords: framework, mobile device management, Android.

I. INTRODUCTION

Bring your own device (BYOD) policy cause the increasing number of mobile device usage, not only for personal but also enterprise use [1]. Based on a survey on mobile device security, the increasing use of mobile devices as same as the increasing of the threats [2]. The threats are not only malware, but also physical threats such as loss of mobile device and user behavior [3]. Mobile device management is a tool used to monitor, control and protect the mobile devices [4]. Mobile device management consist of security devices, applications, networks and data [5]. Framework is a semi complete application used to develop applications in a certain domain [6].

II. RESEARCH QUESTIONS

The research questions of this study is:

1. How to identify the requirements of mobile device management?
2. What is the requirements of mobile device management?
3. How to develop mobile device management framework on Android platform?
4. How to test the mobile device management framework?

III. METHOD

The research starts with problem identification to formulate research questions on the development of mobile device management framework. The literature review from previous research, books, journals and scientific articles, and websites related to the development of the framework and the concept of a framework for mobile device management. Domain analysis was performed to determine the requirements the framework on the Android platform. Domain analysis is done by exploring mobile device management software on the Android platform that already exist. The design of mobile device management framework is done after the architectural design. Prototype application made by a predetermined design. Prototype application was conducted to test the mobile device management framework. Making conclusions and suggestions based on the research that has been done.

The method of this research is as below:

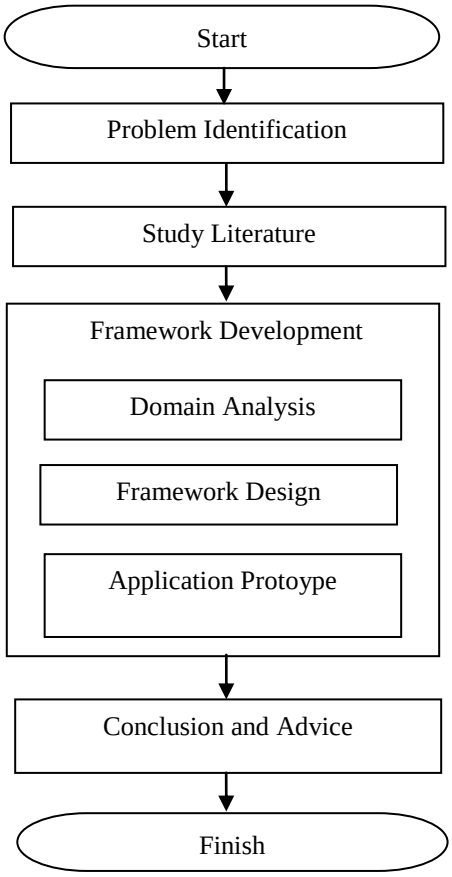

Figure 1. The Research Method

IV. STUDY LITERATURE

1) Framework

Framework is defined as a semi-complete application that can be reused and modified to produce specific applications [7]. Framework is an application that can be modified and customized by the developer [6].

Framework have a physical representation in terms of classes, methods and objects. The main benefits of the framework instead of reuse of implementation but the reuse of the structure. From the standpoint of architectural abstraction, reuse framework provides functions on three levels of analysis, design and implementation as shown in Figure 2.

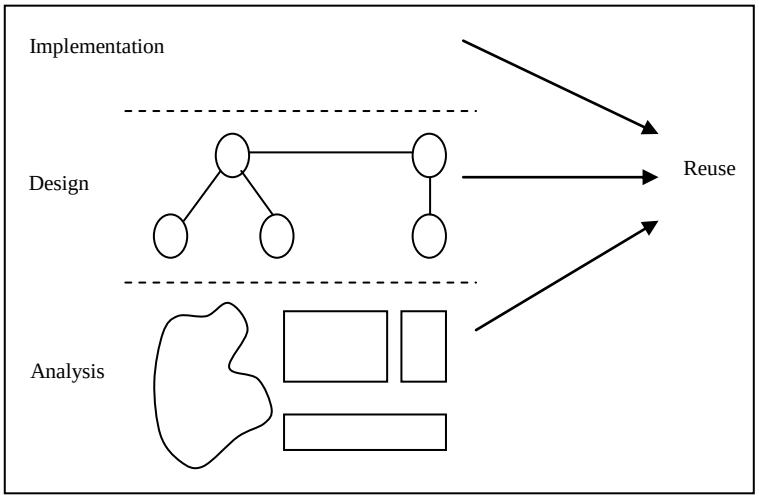

Figure 2. Reusable of Framework

The main benefits of the framework for developer is [6]:

1. Modularity

Framework improving modularity by encapsulating method implementations are easy to change, into a stable interface. The modularity of the framework can help improve the quality of software by means of localizing the impact of design changes and implementation.

2. Reusability

Given stable interface framework improves reusability by means of defining generic components that can be reused to create new applications.

3. Extensibility

Framework increases the expansion by providing explicit hook methods, thus enabling an application to extend implementation of interface provided application framework. The expansion of this framework is important to ensure an adjustment to the services and features of the new application.

4. Inversion of Control

Runtime of the architecture framework is characterized by the inversion of control. This architecture enables the adjustment steps with the application process object event handler is invoked through a request mechanism framework.

2) Threat and Weakness of Mobile Devices

The mobile device must support the security objectives. The main purpose of the base security for mobile devices is as follows:

1. Confidentiality, ensure that the data stored on the mobile device can not be accessed by unauthorized parties.
2. Integrity, detecting changes intentional or unintentional on the stored data.
3. Availability, ensure that users can access resources using mobile devices when needed.

To achieve these objectives, the mobile device must be secured from a variety of threats and weaknesses. Here are the threats and weaknesses of mobile devices [8]:

1. Lack of control over physical security.
2. Use of mobile devices are not reliable.
3. Use of untrusted network.
4. Use of untrusted applications.
5. Interaction with other systems.
6. Use of untrusted content.
7. Use of location services.

3) Mobile Device Management

Mobile device management is a set of mobility management and security tools. Mobile device management can be developed with location-based configuration or as a hosted service [4]. Mobile device management is not just a set of data that is stored on the mobile device but also the hardware such as the camera and the USB port on the mobile device [5]. Mobile device management refers to the frameworks or solutions that control, monitor and regulate the use of mobile devices in the enterprise or service provider [9].

V. ANALYSIS AND DESIGN

1) Domain Analysis

Domain analysis is conducted by exploring mobile device management software, they are Aegis Safer, Blackberry Enterprise 10 and MaaS360 [10, 11, 12]. The mobile device management software can be implemented on the Android, iOS and Blackberry. The next step is features comparison. The results of the comparison is functional requirements of mobile device management framework. Functional requirements is supported by at least two software. Table 1 is a functional requirements of mobile device management framework .

TABLE 1 FUNCTIONAL REQUIREMENTS OF MOBILE DEVICE MANAGEMENT FRAMEWORK

No	Functional Requirements
1	MDM Admin register the mobile device to mobile device management software
2	MDM Admin authenticate the device
3	MDM Admin manage the camera usage (disable / enable) .
4	MDM Admin manage the microphone usage (disable / enable) .
5	MDM Admin manage SD cards usage such as SD card replacement .
6	MDM Admin manage SIM card usage such replacement SIM
7	MDM Admin manage outgoing calls (disable / enable)
8	MDM Admin lock the device's screen remotely
9	Admin MDM reset the device
10	MDM Admin manage the use of GPS
11	MDM Admin manage the use of WiFi
12	MDM Admin manage the use of Bluetooth
13	MDM Admin manage the use of tethering
14	MDM Admin create an application blacklist
15	MDM Admin send information to the client application blacklist
16	MDM Admin create a whitelist of applications
17	MDM Admin send information to the client application whitelist
18	MDM admin create appropriate policies with the organization
19	MDM Admin set the policies
20	Users notice the policy that applies on the device
21	Users send messages to the server

2) Framework Design

Framework design consists of functionality modelling, framework architecture, class identification, class design and hot spot identification.

1. Functionalities Modeling

Functionalities modeling is illustrated through use case diagrams. Use cases diagram provide an overview of specific application functions that can be created using the framework.

2. Framework Architecture

Framework architecture consists of a server and a client. From the server side consists of mobile device management, application management and policies management. The client side consists of notice the policy and send a message to the server. Figure 3 represents the architecture of mobile device management framework.

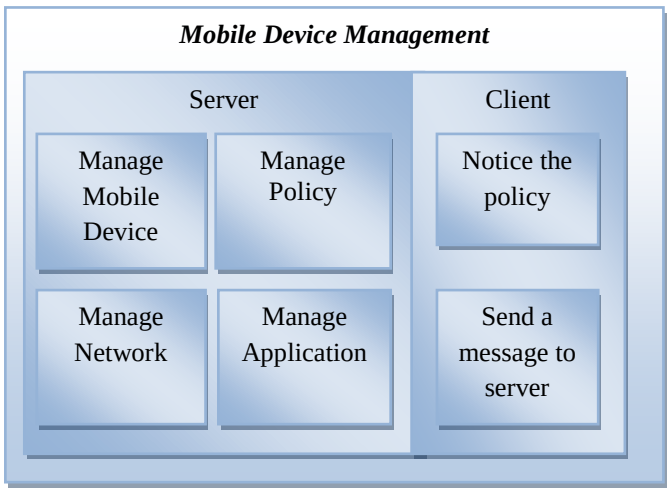

Figure 3 Architecture Mobile Device Management Framework

3. Class Identification

Class identification is conducted after the domain analysis. Classes on the mobile device management framework are Device, Applications, Policy, Camera, Bluetooth, GPS, WiFi, Microphone, SD card, SIM card, Tethering, Calls and User.

4. Hot spots Identification

Hot spots are part of a framework which can be modified according to the needs of application developers. Exploration of the application's feature on the same domain used to decide which function is need to change. Hot spot card is needed to identify the requirements changing.

Registration of the device's hot spot has various implementations where developers can choose to use all or some of the attributes for device registration.

Create the policy's hot spot has various implementation where developer can control the policy acccording to the needs of mobile device management.

Manage application's hot spot has various implementation where developers can choose how to manage applications, Blacklist or Whitelist.

VI. IMPLEMENTATION AND EVALUATION

Framework mobile device management is implement as a application prototype. The prototype is develop using Java programming and Eclipse Galileo as integrated development environment. The prototype is develop for Android platform.

The implementation in this research has several limitations:

1. All function in the prototype is control by user, not mobile device management admin.
2. Implement class device: device registration, authentication devices, remote screen lock and reset the device, class camera, wifi, bluetooth, GPS, calls, tethering and microphone, class manages an application, consists of making a whitelist and blacklist applications.

Figure 4 is interface of mobile device management.

Figure 4 Interface of Management Device

VII. CONCLUSION

The conclusion of this research is:

1. Mobile device management framework has developed and implemented as a application prototype.
2. The requirements of mobile device management is conducted by domain analysis which exploring the features of three software of mobile device management then do a comparison feature.
3. Framework of mobile device management on the Android platform was developed with determine the method and pemission and API provided by Android according to the requirements of mobile device management.
4. Framework of mobile device management is tested by building a protype then do black box testing. Testing framework is also done with the benefit of the framework is the fulfillment of the modularity, reusability, extensibility and inversion of control. Expert judgment is made to declare that the research has achieved its objectives.

VIII. PREFERENCE

[1] Miller, Keith dkk. (2012). "BYOD: Security and Privacy Considerations". IEEE.

[2] Polla, M dkk. (2013) "A Survey on Security for Mobile Devices". IEEE Communications Survey&Tutorials. Hal.446-471.

[3] Mohan, Felix. (2013) "Realizing the Mobile Enterprise : Balancing the Risks and Rewards of Consumer Devices". Report Based on Discussions with the Security for Business Innovation Council.

[4] Tatte, G and Bamnote, D. (2013). "Mobile Device Management: A Functional Overview". International Journal of Computer Science and Applications. Hal.319-323

[5] Rhee, K dkk. (2012). Security Requirements of a Mobile Device Management System. International Journal of Security and Its Applications. Hal.353-358.

[6] Fayad, M dkk. (1999). *Building Application Frameworks: Object Oriented Foundations of Framework Design*. New York: Willey.

[7] R.E, F dan Johnson, B. (1988). *Design Reusable Classes. Journal of Object Programming*. MA: Addison Wesley

[8] NIST. (2013). "Guidelines for Managing and Securing Mobile Devices in the Enterprise".

[9] Bergman, N dkk. (2013). *Hacking Exposed: Mobile Security and Solutions*. New York: McGraw Hill.

[10] MarkAny. [*Online*]. Available: www.markany.com. Downloaded 18 Januari 2014.

[11] Blackberry Enterprise 10. [*Online*]. Available: http://us.blackberry.com/business/software/bes-10.html. Downloaded 18 Januari 2014.

[12] MaaS360. [*Online*]. Available: http://www.maas360.com/. Downloaded 18 Januari 2014.