Model Driven Architecture for Mobile Device Services

Regin Joy Conejar\textsuperscript{1} and Haeng-Kon Kim\textsuperscript{1}

\textsuperscript{1}School of Information Technology, Catholic University of Daegu, Korea
*rejin@cu.ac.kr, hangkon@cu.ac.kr

Abstract. Although remarkable improvements in the growth of business applications for mobile devices have been made in recent years, the development in this area is still not as mature as it is for desktop computers. The development of services that can be fully functional in mobile environments and operable on a variety of devices is an important and complex task for the research community. This paper presents a mobile-driven architecture for mobile device services, provides mobile developers with an in-depth view of mobile device services. It includes mobile email and mobile instant messaging, mobile security and management. A critical aspect of developing future services for mobile devices will be ensuring that the services provide a sufficient performance.

Keywords: Mobile Device Services, Mobile information services, Model Driven Architecture, Mobile Applications

1. Introduction

Over the past decades, billions of people have hooked themselves up to the thing called the Internet via computer, and more recently over smart devices and mobile devices such as smart phones. This communication revolution is now extending to objects as well as people. Nowadays mobile devices, such as mobile phones, personal digital assistants (PDA) or smart phones, are ubiquitous and accompany theirs users almost every time and everywhere. Their capability of connecting to local area networks via Bluetooth or Wireless LAN potentially enables new types of mobiles device services. They are mostly employed only for communication or personal information management purposes.

Mobile devices, such as smartphones, mobile internet devices and web-enabled media players, are becoming widespread. These devices possess limited resources, which motivates resource optimizations. Mobile devices are hawking the marketplace over their stationary counterparts. Thus, mobile users requirement are rapidly increasing in terms of running more complex services on these mobile devices [9]. The Model Driven Architecture (MDA) paradigm is combined with the graphical modeling tool and the graphical models that are then used to generate mobile device services, to intersect the development of platform-specific clients from the implementation of the mobile device service functionality; producing a fully functional device-aware Mobile Service.
This research proposes a model-driven architecture (MDA) specifically to the development of mobile device services. MDA would greatly help in easing the development process of mobile device services development for mobile platforms since it would address the problem of redundancy of tasks in developing a service that would run on several platforms. By having a high-level model that would describe the services and having this model is transformed to mobile device services for different mobile platforms.

2 Related Works

Mobile devices are becoming the most indispensable computing and communicating device a person needs. With the advent of smart phones, the mobile phone has become as powerful as any ordinary desktop computer in terms of the services it can offer and its communication power [6]. People are now using their mobile phones not just for calling and sending messages but also for browsing the Internet, playing games, listening to music, taking pictures and videos just to name a few of the mobile device services. In response to the rising demand for better mobile device services, companies have developed various types of mobile device services that would suit different people with different mobile needs.

One problem about this though is that, developing any type of mobile device services, is quite difficult. It still takes a large amount of skill and familiarity with how the framework is used before a person can create a decent amount of mobile device services and the workflow specification for a simple application. Other things that makes developing services for mobile devices more difficult as compared to desktop applications are factors such as device limitations (e.g. screen size, computing power, power consumption) [7], different operating systems for mobile devices, different data representation and additional device capabilities (e.g. Bluetooth, Wifi, GPS, Camera enabled) which are not standard to all devices and therefore should be considered when developing a uniform device services that can be run on different mobile devices.

3. MDA for Mobile Device Services

3.1 Mobile instant messaging (IM)

Mobile instant messaging (IM) is the ability to engage in an IM conversation from a mobile device. Note that there is a difference between SMS aka “text messaging” and mobile IM. Text messaging is a network operator-provided service, whereas mobile IM integrates with enterprise IM systems and possibly with popular consumer services such as AOL, Yahoo Messenger, Google Talk and other means of IM. This a messaging service that aims to transpose the Internet desktop messaging such as Skype, Window Live Messenger, Yahoo Messenger or MSN experience to the usage scenario of being connected via a mobile devices or cellular devices (see Figure 1).
3.2 Mobile Email

Access to mobile email is evolving from being an a mainstream enterprise application. Mobile bodies are driving this transition by demanding that IT provide them access to email while they are out of the office or on the go. In some cases, mobile bodies find ways of working around IT by using consumer email services to perform business email. This ensures that mobile email is secure and manageable. Features such as remote data wipe, password protection and data encryption are critical. In addition, data roaming charges are unpredictable and potentially very costly. Most enterprises use email for communication and collaboration on their desktop and laptop devices. However, email usage on mobile devices (e.g., mobile phones) is not nearly as widespread.

3.2.1 Mobile Email MDA

The enterprise data center architecture is the most common mobile devices model driven architecture (see Figure 2). The enterprise deploys the email servers in their own data center along with a mobility server.
The mobility server provides functions to secure and make reliable connection with the mobile device. Mobile device provisioning, policy administration and monitoring. Synchronization of Email and remote device wipe and access control. The advantage of this architecture is that the enterprise retains control over the servers and the end-to-end data flow. The enterprise can lock down the application servers and mobility server in their data center and thereby control the storage/journaling/retrieval of confidential information contained in the email messages. In addition, many enterprises will lock down the mobile device using device encryption, access control mechanisms, and remote wipe capabilities. Lastly, the enterprise can achieve fault tolerance by deploying redundant servers in backup data centers.

3.3 Mobile Device Security and Management Services

Mobile Security has become increasingly important in mobile services. It is of particular concern as it relates to the security of personal information now stored on smartphones or mobile devices. More and more users and businesses use mobile devices and smartphones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, mobile devices and smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company and organization. All mobile device and smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones...
that can come from means of communication like SMS, MMS, wifi networks, and GSM. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users.

Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

3.3.1 Mobile Device Threats

The use of mobile devices leaks the enterprise to security threats such as:

- **Device loss or theft** - With mobile devices becoming fancier, more popular, and more expensive, they are increasingly liable to theft. Even then, many thieves are more interested in accessing your wireless service and potentially, stealing your identity.
- **Data leakage** - Any sensitive data stored on a mobile device can be easily transferred to other storage devices and computers (see Figure 3).

![Fig. 3. Data Leakage](image)

Data leakage is incremental movement of information from areas of high trust office and business location with little or no protection. It makes theft a little easier every day. Figure 3 shows how data leakage of data from secure locations. One of the many problems of data leakage is the taking of information from applications and placing it into spreadsheets, PDF files, word documents and other distributable formats.
Unauthorized wireless usage - Wireless security policy violations can expose the enterprise to system attacks (e.g., connection to a wireless ad hoc network can lead to man-in-the-middle attacks).

3.3.2 Mobile Device Services Management

Business, organizations and enterprises should ensure that their mobile device network management system enables the administrator to perform functions such as disable the device and restore the device to factory defaults (including the ability to delete all files and flush caches), Change the password and delete locally stored password history, Control system software upgrades, Control application installation and removal, Control use of SMS and MMS messaging, control multimedia capabilities such as cameras and microphones, Control data transfer between the mobile device and servers and other management security features to avoid data leakage and data access by unauthorized individuals.

4 Conclusion

The competencies of mobile devices services have increased significantly over the last several years and with platforms, such as Apple’s iPhone and Google’s Android, will no reservation to endure its expansion in the future generation. This Model Driven Architecture for Mobile Device Services has ushered in a new era of applications and has presented developers with a wealth of new opportunities. Unfortunately, with these new opportunities have come new challenges that developers must overcome to make the most of these cutting-edge platforms. Developing mobile device services for platforms such as Android require extensive testing as mobile email and mobile instant messaging, mobile security and management can greatly influence performance and it is impossible to completely profile a configuration because ultimate mobile device services depends on user interaction, network traffic and other applications on the device.

References

1 Mobile information services, University of Miami Leonard M. Miller School of Medicine, http://it.med.miami.edu/x291.xml.
2 Florence T. Balagtas-Fernandez, “Model-Driven Development of Mobile Applications”.
3 J. Dunkel and R. Bruns, “Model Driven Architecture for Mobile Applications”
4 Chris Thompson, Jules White, Brian Dougherty, Hamilton Turner, Scott Campbell, Krzysztof Zienkiewicz, and Douglas C. Schmidt, “Model-Driven Architectures for Optimizing Mobile Application Performance”.