Privacy Requirements Patterns for Mobile Operating Systems

Xiao Xuan*, Ye Wang†, and Shanping Li*
*College of Computer Science and Technology, Zhejiang University, China
†School of Computer Science and Information Engineering, Zhejiang Gongshang University, China
jackyxuan@zju.edu.cn, yewang@zjgsu.edu.cn, shan@zju.edu.cn

***Abstract*—Nowadays mobile devices have rapidly developed. Privacy protection for mobile operating systems has become a hot topic in industry and research, which also brings new challenges. The scenarios in mobile operating systems are different from those in tradition systems. Users of mobile systems face more and more new risks in new scenarios. On the other hand, personal data is growing exponentially every day. It reminds us the importance of privacy protection is also increasing at the same time.**

In this paper, we study the privacy patterns for mobile operating systems. We elicit privacy-related requirements in three ways - knowledge from domain experts, literature review on public documents of existing mature systems and feedback from real users. Based on these requirements, we propose 7 privacy patterns which are presented with the RePa Requirements Pattern Template. All of these patterns were refined by professional business analysts which concrete the result of our work. We believe that our findings can help business analysts with the description for privacy requirements in future mobile operating system development projects.

***Index Terms*—Privacy Requirements Pattern, Privacy Protection, Mobile Operating System**

I. Introduction

Mobile devices have evolved fast these years. People have increasingly relied on smartphone and tablet computer (namely, Pad) in their daily life and work. More and more innovative mobile products are released almost every month, such as smart glasses (e.g. Google glasses), smart watch (e.g. GALAXY Gear and iWatch) and intelligent vehicle systems (e.g. iDrive and G-BOOK) etc. People use mobile devices, and people store their privite information, files and data on mobile devices. Protection for user privacy has become a vital task for modern mobile operating systems.

On the other hand, due to the emerge of new technologies like cloud services, big data and ubiquitous computing, privacy requirements of mobile platforms have been much different from those of traditional systems. For instance, when people use applications employed the APIs of advertisment services, the service providers may collect device location infomation and users' shopping habits for personalized recommendation using data mining techniques. This could be a new risk brought by new technologies and new features of mobile systems.

In this work, we propose 7 privacy requirements patterns for mobile systems based on the result of our empirical study. We interview domain experts and conduct a literature review of public documents of three popular mobile operating systems (i.e. Android, iOS and Windows Phone) to obtain the privacy requirements. Meanwhile, we survey mobile device users on privacy issues by questionnaires. There are in total 107 users (46 Android users, 39 iOS users and 22 Windows Phone users respectively) who provide their useful opinions. Based on aforementioned three sources, we extract initial privacy patterns, which are finally refined by three senior business analysts. The goal of this paper is to present privacy requirements patterns that can be used in mobile operating system development projects to describe privacy requirements.

The rest of this paper is structured as follows. Section 2 provides a brief backgound for privacy patterns and mobile operating systems. In Section 3, the design of the study method is presented. The privacy patterns we proposed are introduced in Section 4. This is followed by the conclusion of this work.

II. Background

A. Privacy Pattern

The concept of software pattern was proposed in 1995 [1]. It is used to document the reusable and repeatable software development knowledge. Many privacy patterns [2][3][4][5][6] were also addressed to prevent the privacy problems from happening.

Besides, some common standards like Common Criteria [7] have been developed by security professionals. These standards represent best practices that report many information security issues which include privacy. Nevertheless, these common standards are too general for privacy assurance in a specific domain, e.g the domain of mobile systems.

B. Mobile Operating Systems

Since the release of the first iPhone in 2007, mobile operating systems have attracted industry's attention and developed rapidly. Nowadays, Google's Android, Apple's iOS and Microsoft's Windows Phone have occupied almost all of the smartphone and tablet markets.

- **Android** is now the most popular mobile operating system in the world. It follows the capability-based privacy model. In Android system, each application must inform the operating system what capabilities it requires. These capabilities are measured in terms of permissions. When

978-1-4799-6327-0/14/$31.00 © 2014 IEEE

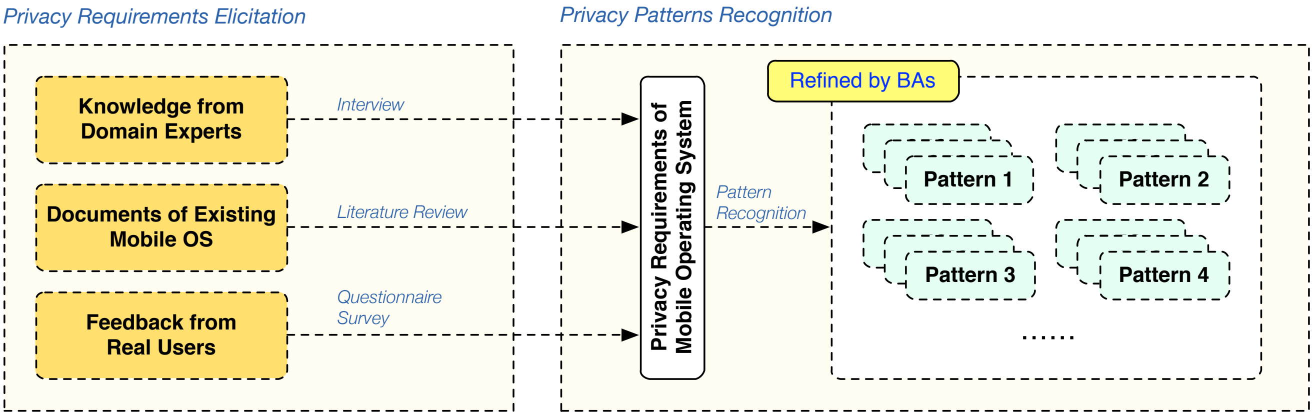
Privacy Requirements Elicitation
Privacy Patterns Recognition
Knowledge from Domain Experts
Documents of Existing Mobile OS
Feedback from Real Users
Interview
Literature Review
Questionnaire Survey
Privacy Requirements of Mobile Operating System
Pattern Recognition
Refined by BAs
Pattern 1
Pattern 2
Pattern 3
Pattern 4
......

Fig. 1. The Method Overview of Our Approach

an application is installed on a mobile device, a list of all the permissions that the application requires access is shown to the user, and the user is able to decide whether to continue with the installation process or not.

- **iOS** is a closed source operating system introduced by Apple. It adopts a different privacy model from Android. When a user installs an iOS application, she will be never notified what permissions the application requests until the time when the application is running and it needs to access certain user resources (e.g. contacts and photos) or device functions (e.g. Bluetooth and location service). Besides, iOS provides a host of privacy settings. The user can withdraw and regrant any permission any time which is convenient for privacy management.
- **Windows Phone** is a smartphone operating system developed by Microsoft. Similar to Android, permission requests are mandatory for each Windows Phone application that is about to be installed. However, Windows Phone does not offer a specific setting panel for privacy management like what iOS does.

III. Method Overview

As shown in Fig. 1, our approach consists of two phases. In the first phase, we elicit the privacy requirements for mobile operating systems. Since we do not have the requirement documents for any of mobile systems, we rely on the knowledge from domain experts. Further, we perform a systematic literature review on the public documents (e.g. developer guideline, best practice, product description and offical policy statement) of Android, iOS and Windows Phone which are related to privacy issues. In order to concrete our work, we ramdonly survey 107 users of Android, iOS and Windows Phone devices with questionnaires about privacy requirements on mobile operating systems. According to the feedback from these users, we modify the requirements that we have identified.

The second phase is privacy patterns recognition. In this phase, we formulate the initial privacy patterns using *RePa Requirements Pattern Template* [8]. To improve the accuracy of representation, we let three senior business analysts to help refine the initial patterns. All of these business analysts have dedicated to software requirement analysis for more than eight years.

With our approach, we recognize 7 privacy patterns for mobile operating systems in the end. All of these patterns are detailed in Section 4.

IV. Privacy Patterns

We identify 7 privacy requirements patterns for mobile operating systems presented in Table I - VII. These patterns are established for all RE-activities on mobile operating systems from seven privacy related aspects. In most cases, these patterns are not completely independent of each other. For example, the Pattern 7 *Mobile Communication Secrecy* is correlated to the Pattern 5 *Privacy Protection over Mobile*

TABLE I
Privacy Pattern 1: Authorized use of sensors or portals

Name: Authorized use of sensors or portals		
Context	*RE Activity*	All
	Pattern Type	Product
	Stakerholders	Requirements Engineers, Developers, Application Providers, Users
Problem	To prevent unauthorized use of sensors or portals.	
Forces	The access to the device's sensors or portals must be strictly controlled. A side-effect is that the user may decline a permission request by accident or due to the misunderstanding of the access purpose, which will cause some application funcitions disabled.	
Solution	The system shall demand the application to explicitly ask for permission from the user to access the sensors and portals. The system shall also provide a host of settings to manage these permissions.	
Application and Example	An application must explicitly request the permission for use of microphone.	

Cloud Service and Pattern 6 *Financial Information Protection*, because the cloud service and the financial application both require secure transport techniques which are reported in the Pattern 7. In the following paragraphs, we elaborate these 7 patterns respectively.

Table I shows the privacy pattern about authorized use of the device's sensors and portals. Modern mobile device is armed with many kinds of sensors and input devices, including fingerprint scanner, position indicator, Bluetooth, camera and microphone etc. For privacy consideration, the system should always forbid the application to manipulate these hardwares without user permissions.

TABLE II
PRIVACY PATTERN 2: AVOIDANCE OF PRIVACY LEAKAGE IN USER BEHAVIOR INFORMATION COLLECTION

Name: Avoidance of Privacy Leakage in User Behavior Information Collection		
Context	*RE Activity*	All
	Pattern Type	Product
	Stakerholders	Requirements Engineers, Developers, Information Collectors, Users
Problem	To prevent privacy leakage as conducting user behavior information collection.	
Forces	The constraint for the collection process should be set up and always followed. The scope of collectable information should be restricted. A side-effect is that the user may worry overmuch about privacy reveal during user behaviors collection.	
Solution	The system shall notice user specifically and distinctly what kinds of user information is needed for behavior analysis. The most sensitive user information (e.g. password) shall be strictly prohibited to touch and collect.	
Application and Example	A request, with detailed explanation, will be shown to user for permission of user behavior collection.	

The pattern introduced in Table II focuses on avoidance of privacy leakage in user behavior information collection. On account of the great development of data analysis and mining technology, user behavior analysis has been widely used for many kinds of business and IT purpose. The user behavior information can be used for advertisements, user experience improving and service recommendations. However, in mobile systems, user behavior information usually contains more privacy-sensitive data, so that the system must discipline the collection process and limit the scope of collectable information. Collection without user permission should be forbidden, and the excessive authorization should be avoided.

As shown in Table III, the pattern is about protection for the user's personal mobile data including messages, contacts, calendar, photos and location information etc. Besides, the device identification such as IMEI, ICCID and the usage of cellular network are also deemed as privacy-sensitive data. As we mentioned in Section 2, Andiord, iOS and Windows Phone have employed specific privacy mechanism to this scenario. It is that the application must obtain the permission from the user, before it first accesses to the corresponding data.

TABLE III
PRIVACY PATTERN 3: GUARD FOR PERSONAL MOBILE DATA

Name: Guard for Personal Mobile Data		
Context	*RE Activity*	All
	Pattern Type	Product
	Stakerholders	Requirements Engineers, Developers, Application Providers, Users
Problem	To carefully protect the user files, personal data and credentials.	
Forces	The access to the user's files/data/credentials must be strictly controlled. A side-effect is that the user may decline a permission request by accident which causes some funcitions of the application disabled.	
Solution	The system shall provide warnings to the user when an application intend to access user files, data and credentials. If and only if the user has granted the permission, the application can touch the corresponding resources. The user can withdraw or regrant any permissions in somewhere of the system later.	
Application and Example	An application must explicitly request the permission for access to the user's Short Messaging Service.	

The pattern 4 refers to protect the data privacy over mobile cloud services. Usually, the user would like use cloud services more frequently in the mobile operating system, which is caused by two main reasons: first, the mobile device has smaller storage; second, the mobile system updates more frequently. This fact explains the importance of this pattern. As shown in Table IV, this pattern reports the system shall always perform data encrytion before uploading the data to cloud servers and use secure tokens for authentication. Meanwhile, the user must be noticed with the content of the cloud-based

TABLE IV
PRIVACY PATTERN 4: PRIVACY PROTECTION OVER MOBILE CLOUD SERVICES

Name: Privacy Protection over Mobile Cloud Services		
Context	*RE Activity*	All
	Pattern Type	Product
	Stakerholders	Requirements Engineers, Developers, Cloud Service Providers, Users
Problem	To protect privacy over mobile cloud services	
Forces	There is a tradeoff between automated backup and customized setting, as well as between data recoverability and user privacy.	
Solution	The system shall ensure confidentiality of data backup. The data encryption must be performed before the data sending over the Internet. Secure tokens shall be used for authentication. The user should be awared what data will be backed up to the cloud. The user also can stop the backup function, and delete unwanted data from cloud with her device any time.	
Application and Example	The system uses 256-bit AES encryption to transmit the user's data to cloud servers.	

TABLE V
PRIVACY PATTERN 5: AUTHENTICATION OF MOBILE USERS

Name: Authentication of Mobile Users		
Context	*RE Activity*	All
	Pattern Type	Product
	Stakerholders	Requirements Engineers, Developers, Users
Problem	To prevent unauthenticated person to steal or tamper user data and files.	
Forces	There is a tradeoff between usability and security.	
Solution	The system shall provide authentication for the device, folders, applications and privacy-sensitive data. The encryption algorithm of password shall be strong. The length requirment shall be set appropriately.	
Application and Example	The user can set a screen lock password.	

backup, and is able to remove unwanted data from cloud servers any time through her mobile device.

See Table V, authentication of mobile users is defined that the unauthenticated access to the mobile device, folders, applications or privacy-sensitive is fobidden. Many cases show that the mobile device is easy to be touched, or even stolen by malicious people. The authentication mechanism (e.g digital password, graphical password and biometric) can well solve this problem.

TABLE VI
PRIVACY PATTERN 6: FINANCIAL INFORMATION PROTECTION

Name: Financial Information Protection		
Context	*RE Activity*	All
	Pattern Type	Product
	Stakerholders	Requirements Engineers, Developers, Application Providers
Problem	To ensure that the user's financial information will never be revealed.	
Forces	The user's financial information must be protected in a more secure way.	
Solution	The system shall strictly prevent any application to store the user's financial information permanently in local. The application cannot transmit user financial information to any invalid or unauthenticated parties. The credentials and data must be transmited in a secure way.	
Application and Example	It will be always failed that an e-bank application tries to keep a user's account password locally.	

New technologis, such as 4G telecommunications and Near Field Communication, let mobile payment become easier and more popular. In recent years, the mobile e-business and e-banking applications emerge in endlessly. The pattern shown in Table VI provides a solution to protect the user's financial information.

Table VII shows the privacy pattern about the communication secrecy of mobile systems. Communication in public channel is dangerous. Hackers may perform man-in-the-middle attack to intercept data and files. Hence, the system should always block the privacy-sensitive data transmitting through an insecure way.

TABLE VII
PRIVACY PATTERN 7: MOBILE COMMUNICATION SECRECY

Name: Mobile Communication Secrecy		
Context	*RE Activity*	All
	Pattern Type	Product
	Stakerholders	Requirements Engineers, Developers, Application Providers
Problem	To perform secure communication with other participants.	
Forces	The communication between the device and servers must be protected with secure tansport techniques. Using secure transport techniques will raise the application's development cost.	
Solution	The system shall request the application transmit privacy-sensitive data with secure channel forcibly.	
Application and Example	A Instant Messaging application cannot send messages without using SSL protocol.	

V. CONCLUSION

In this paper, we study on the privacy requirements patterns for mobile operating systems. Our method consists of two phases - privacy requirements elicitation and privacy patterns recognition. We use the knowledge from domain experts, the information from public documents and the result of user survey to indentify privacy requirments of mobile systems. Based on these requirements, we propose 7 privacy patterns and format them with RePa requirements pattern template.

ACKNOWLEDGMENT

This research is sponsored in part by NSFC Program (No. 61103032) and National Key Technology R&D Program of the Ministry of Science and Technology of China (No. 2012BAH13F04).

REFERENCES

[1] J. Vlissides, R. Helm, R. Johnson, and E. Gamma, "Design patterns: Elements of reusable object-oriented software," *Reading: Addison-Wesley*, vol. 49, p. 120, 1995.

[2] S. Romanosky, A. Acquisti, J. Hong, L. F. Cranor, and B. Friedman, "Privacy patterns for online interactions," in *Proceedings of the 2006 conference on Pattern languages of programs*. ACM, 2006, p. 12.

[3] R. Slavin, H. Shen, and J. Niu, "Characterizations and boundaries of security requirements patterns," in *Proceedings of the 2nd Int. Workshop on Requirement Pattern (RePa)*. IEEE, 2012, pp. 48–53.

[4] M. Hafiz, "A pattern language for developing privacy enhancing technologies," *Software: Practice and Experience*, vol. 43, pp. 769–787, 2013.

[5] E. Fernandez-Buglioni, *Security patterns in practice: designing secure architectures using software patterns*. John Wiley & Sons, 2013.

[6] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, *Security Patterns: Integrating security and systems engineering*. John Wiley & Sons, 2013.

[7] Common criteria for information technology security evaluation. http://www.commoncriteriaportal.org/cc/.

[8] L. Chung, B. Paech, L. Zhao, L. Liu, and S. Supakkul, "Repa requirements pattern template v1. 0.1," in *Proceedings of the 2nd Int. Workshop on Requirement Pattern (RePa), Chicago, USA*, 2012.