A Context-Sensitive Security Model for Privacy Protection on Mobile Phones

Julian Seifert
Bauhaus-Universität Weimar
Bauhausstr. 11
99423 Weimar, Germany
seifert8@uni-weimar.de

Alexander De Luca
University of Munich
Amalienstr. 17
80333 Munich, Germany
alexander.de.luca@ifi.lmu.de

Bettina Conradi
University of Munich
Amalienstr. 17
80333 Munich, Germany
bettina.conradi@ifi.lmu.de

ABSTRACT

In this paper we present a context-sensitive security model for privacy protection on mobile phones. We describe the system TreasurePhone which implements this security model. The Privacy Protection is realized by spheres, which represent the user's context specific need for privacy. That is, users can create any number of spheres and define which services and data are accessible in each sphere. TreasurePhone integrates context information for supporting authentication and activation of spheres by locations and actions. A basic hierarchy is used for determining which location should be activated based on the associated sensor value.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous

General Terms

Human Factors, Security, Management

Keywords

Privacy, Data Security, Mobile Phone

1. INTRODUCTION

Modern mobile phones allow the user to create manifold types of data such as contacts, photos, emails and text documents. Further, the amount of possible storage of these devices is increasing enormously which extends the need for privacy protection [6]. For instance, the integration of mobile phones into enterprise environments for mobile managing of email, contacts, calendars and other data is enjoying increasing popularity. As a result, a growing amount of sensitive data is exposed to the risk of being disclosed to unauthorized people who might get access to the mobile phone. Nevertheless, the existing *binary* security models distinguish between the statuses *locked* and *unlocked*, where after a defined period of inactivity the locked status is activated automatically. This security model requires the user to authenticate for each interaction in case the phone activated the locked status.

Users have clearly distinct contexts in their life such as family and work, each with a corresponding need for privacy [3]. Yet, the existing binary security model does not support privacy management for distinct contexts for data stored on mobile phones. Therefore, in some areas, as it is the case with companies with high security standards, company mobile phones have to be used in the work context. Consequently, users have to use different mobile phones for each context that corresponds to a certain need for privacy. This approach is clearly impractical.

In this paper we present a context-based security model for mobile phones that supports protection of the user's privacy and data. The TreasurePhone system, which is a first implementation of this security model, implements the protection through *spheres*. A sphere represents a context-specific configuration of data protection, based on the user's specific need for privacy. TreasurePhone integrates context information and applies these to *actions* and *locations* to activate corresponding spheres automatically. This model enables the user to secure her data in each context in a sophisticated way using a single mobile phone while keeping the effort minimized through the automated adaptation. Hence, TreasurePhone reduces the risk to disclose sensitive data.

TreasurePhone is based on findings of various existing work. The concept of using multiple profiles for protecting privacy in different contexts was already proposed by Karlson [3]. This work, which is focusing on data privacy and mobile phones, is suggesting *usage profiles* that correspond to the different contexts of the user. Each profile would allow only access to a defined subset of data, which is not considered as sensitive in the respective context. For instance, this would allow to borrow the mobile phone to others without taking the risk of disclosing private data. The concept of TreasurePhone is also related to *Sensay* [4], a system that adapts its behaviour context-based. Sensay processes data captured by several sensors and determines the user's current context based on these results. For instance, the ringer volume is adjusted or the vibration alarm is activated.

The security model that we propose aims to combine the approaches of usage profiles and Sensay, which is not supporting privacy protection. That is, the effort that emerges from using usage profiles shall be minimized by integrating context information for adapting the privacy protection automatically.

2. CONCEPT OF TREASUREPHONE

Privacy cannot be seen as an absolute concept. It is rather a concept about controlling the disclosure and use of personal information dynamically. The dynamic character of

MobileHCI09 September 15 – 18, 2009, Bonn, Germany
ACM 978-1-60558-281-8/09/09 .

privacy is stressed by its context-dependent nature [2]. Furthermore, the user's grasp of what kind of personal data are considered to be private is highly individual [1].

The concept of TreasurePhone is based on the hypothesis that users are willing to protect their data and privacy at all times in an convenient way which requires only little effort. Hence, we propose the concept of spheres. A sphere represents the user's context-specific requirements for privacy of data and services of her mobile phone. That is, the user can define which services such as email, address book, and photo are available in a specific sphere and further which data are accessible. One could imagine a sphere as a filter that lets pass only data and services that are not considered as sensitive in the context of the particular sphere.

TreasurePhone provides one special sphere, the *Admin Sphere* (*AS*). This sphere is the administration mode. To activate this sphere the user has to authenticate, which prevents unauthorized persons from accessing its administrational functionalities. Depending on the device capabilities, manifold ways for authentication can be used [5]. Switching from one sphere to another requires the user first to authenticate, which activates the *AS*. Then the user can choose the sphere she wants to activate from a list.

2.1 Actions and Locations

In order to minimize the effort of activating spheres, TreasurePhone incorporates the concepts of *actions* and *locations*, which are based on the integration of context information. An action can be any kind of interaction with the environment such as controlling an electronic lock or buying tickets using NFC technology. The user defines which action is associated with the activation of a certain sphere. Locations are a specific form of actions: Sensor values that identify an abstract or concrete location are detected, which triggers the activation of a corresponding sphere. For instance, when a user arrives at her office, the Bluetooth ID of her desktop computer is detected. This ID is linked to a location *Office* and thus the *Office Sphere* is activated. The

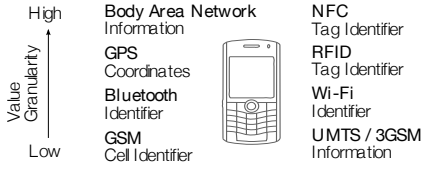

Figure 1: Sources of context information.

location concept is not constrained to certain sensor values but rather supports any sensor values that the device is able to provide. This means, a location could be associated as well with an NFC tag identifier as with certain GPS coordinates but also Wi-Fi identifiers, GSM cell information etc. (See Figure 1). Due to the considerable differences in range of the sensors the granularity differs as well. Therefore, the location concept of TreasurePhone incorporates a hierarchy of sensor values and corresponding actions. The finer the granularity of the associated sensor values, the higher the priority of the location.

Imagine an office building in which Wi-Fi is available. The user Alice associated this network with the location *At work*. Further, the Bluetooth IDs of the desktop computers in the office and in the meeting room correspond to locations that activate the spheres *My Office* and *Meeting Room*. As soon as Alice enters the building the sphere *Work* is activated because the location *At work* was detected. Later, when she goes to the meeting room, her mobile phone detects the Bluetooth ID of the desktop computer in this room. Her mobile phone activates the sphere *In Meeting* because the Bluetooth sensor value has a shorter range and therefore a higher priority.

2.2 User Study

We conducted a user study with twelve male and eight female participant in the age between 23 to 32 years. The goal was to find out the users' rating of the sphere-based security model. Thereto, the participants completed a series of usage tasks two times in randomized order. The tasks covered all system specific actions such as creating, editing, and activating spheres, as well as managing access to certain data. In one series, they had to use a prototype of TreasurePhone that integrates context information captured by the mobile phones NFC sensor. In the other series, a prototype was used that does not support context information integration. Afterwards, the participants filled out a questionnaire.

In average, the participants rated (Scale 1-5) the security model's capabilities to protect privacy with 4.2 (M=4.0, SD=.89) and the usefulness of context-specific spheres for privacy protection with 4.6 (M=5.0, SD=.50). 19 of the participants stated that they would prefer the system with support of actions and locations through the integration of context information.

3. CONCLUSIONS

In this work, we presented a context-sensitive security model and a prototypical implementation, TreasurePhone. With spheres, the user can easily protect her privacy which costs little effort due to the integration of context information for automatic adaptation of the current sphere.

As a next step, this system is to be integrated in a mobile phone operating system. This will allow further investigation concerning usability, the user's acceptance of the system and most important whether TreasurePhone will actually provide a higher level of privacy protection in practice than existing security models.

4. REFERENCES

[1] A. De Luca and H. Hußmann. Threat Awareness - Social Impacts of Privacy Aware Ubiquitous Computing. In *INTER 2007*, June 2007.

[2] X. Jiang, J. I. Hong, and J. A. L. Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. In *Ubicomp 2002*, 2002.

[3] A. K. Karlson, A. B. Brush, and S. Schechter. Can I Borrow Your Phone? Understanding Concerns When Sharing Mobile Phones. In *CHI 2009*, April 2009.

[4] D. Siewiorek, A. Smailagic, J. Furukawa, A. Krause, N. Moraveji, K. Reiger, J. Shaffer, and F. L. Wong. Sensay: a context-aware mobile phone. In *ISWC*, 2003.

[5] F. Stajano. One user, many hats; and, sometimes, no hat - towards a secure yet usable pda. In *12th Int. Security Protocols Workshop*. Springer-Verlag, 2004.

[6] F. Stajano. Will your digital butlers betray you? In *WPES 2004*. ACM, 2004.