Supporting Mobile Privacy and Security through Sensor-Based Context Detection

Julian Seifert
Bauhaus-University Weimar
Bauhausstr. 11
D-99423 Weimar, Germany
julian.seifert@uni-weimar.de

ABSTRACT

This position paper addresses challenges of data privacy and security support for mobile phones. We describe the system TreasurePhone [5] which implements a context-sensitive security model. Data privacy and security is realized by *spheres*, which represent the user's context specific need for privacy. That is, users can create 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. Finally, we propose different approaches for advancing the concepts of TreasurePhone and context based privacy protection on mobile devices.

Keywords

Privacy, Security, Mobile Phone, Context, Sensors

1. A CONTEXT-SENSITIVE SECURITY MODEL

Today, mobile phones allow the user to create and manage many kinds of data. That is, besides contacts and calendars now e-mail, photos and other files are possible. Further, with the Internet becoming accessible through mobile phones, all kinds of services are available. At the same time, the amount of data stored on mobile phones is growing dramatically. This trend is likely to continue and shorten the gap between mobile phones and other computers. These emerging capabilities increase the need for appropriate protection of data privacy and security as well as access to services [8]. Nevertheless, mobile devices and in particular mobile phones use a simple security model that distinguishes only between *locked* and *unlocked* [1]. That is, after a certain period of inactivity the device switches to locked mode. For unlocking authentication (e.g., by PIN) is required, which is often perceived as burden and the reason for users to resign to use this security model.

Research on human interaction showed that users act in distinct social contexts such as work and private. Each of these contexts is associated with a particular need for privacy and security [2]. Hence, binary security models do not reflect the user's need for context-depended privacy protection. One concept for approaching this challenge is *profile*-based privacy and security [7, 1]. Each profile corresponds to certain context and restricts the access to certain information. The challenge of this approach is the concept for the profiles being activated (e.g., manual selection with previous authentication).

This position paper proposes an approach for extending TreasurePhone's [5] sensor-based and context-aware adaptation of profiles which implement data privacy protection for reducing the effort for the user. This concept is potentially suitable for general mobile devices.

The concept of TreasurePhone is based on finding of various exiting work. Stajano describes profile-based data protection [7]. This work addresses privacy issues of sharing (willingly or unintended) a personal digital assistant (PDA). This concept is based on the observation that some data and applications could be used by anybody who gets access to the PDA. Yet, other applications and data should be accessible only by the legitimate user. Accessing these private areas or *hats* would require authentication and thus secures the privacy of the user. A similar concept was also presented by Karlson et al. [1]. They suggest *usage profiles* for mobile phones that correspond to the different contexts of the user. Each profile allows access to a certain user defined set of data which is not considered as sensitive in the respective context. One option for decreasing the usage effort that is caused by profile-based security models is to ease authentication for activating profiles. For instance, the system SecurePhone is designed to enable multi-modal biometric authentication [4]. It allows the user to authenticate by face and voice recognition. An alternative option is context-aware profile activation without user intervention. For instance, with SenSay a context-aware mobile phone is introduced that adapts its behavior (e.g., alarm volume) based on the current context which is measured by sensors (e.g., sound and light) [6]. Yet, SenSay does not support privacy and security.

2. CONCEPT OF TREASURE PHONE

The system TreasurePhone aims for supporting data privacy and security protection. It is a prototypical implementation of an operating system for mobile phones which implements the profile concept through providing *spheres*. Initially, the system provides a few preconfigured spheres (*Private, Work, Closed*) along with the *admin sphere*, which allows creating and editing spheres and editing data access rights. The user can create any number of spheres that correspond to different contexts.

By using spheres, the user can specify which data and files are visible at a time. Protected data are hidden and thereby not accessible. Furthermore, spheres allow to specify which services are available. For instance, access to the camera can be restricted. Thereby, no images can be taken and furthermore no previously taken images are accessible at all.

In case the user wants to activate another sphere since

context has changed, the user needs to identify herself by PIN. Then the sphere to activate can be selected from a list of available spheres.

In order to decrease the perceived burden of activating different spheres, TreasurePhone supports the following three concepts: *locations*, *actions*, and *token based authentication*.

The concept of locations allows the user to activate spheres quickly without authentication. When TreasurePhone detects a location by means of an NFC reader, the activation of a corresponding sphere is triggered. For example, a user arrives at her workplace and activates the *work*-sphere by touching the name plate next to the door with the mobile phone. The NFC tag integrated in the name plate is detected and the corresponding sphere is activated (e.g., certain work related data are accessible now without authentication).

An action can be any kind of interaction with the environment such as controlling an electronic lock or buying tickets using NFC technology. Again, the user defines which sphere activation is associated with certain actions.

In cases the user wishes to activate the admin sphere or to switch to another sphere and no action and location are available, the user needs authenticate herself. In addition to manual authentication by PIN, TreasurePhone supports token based authentication whereas an NFC tag integrated into a wristband serves as token. We found that users prefer this way of authentication over manually typing in a PIN.

3. EXTENDING EXPLICIT INTERACTION

Whitten and Tygar point out that security is rarely a primary goal of the user [9]. Therefore, systems that aim for supporting privacy and security protection depend heavily on the user being aware of the potential risks and that users act according to them. However, in all situations the user is not aware of the risk, it is likely that the user is not willing to take the additional effort caused by security mechanisms. Therefore, the user should be further supported by automized activation of spheres.

Recent mobile phones allow collecting rich information about the user's current context by means of sensors such as global positioning system (GPS) sensor, an NFC readers, Bluetooth, and Wi-Fi. For taking advantage of those data and for being able to conduct field studies, the concepts of TreasurePhone need to be implemented on the operating system level (e.g., using Android).

Collected context data could be used for rule-based activation of profiles by extending the location concept of TreasurePhone to more supported sensors. For example the Bluetooth ID of a desktop computer in the user's office is likely to be an appropriate parameter for activating a corresponding sphere.

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.

However, this approach depends on the user who is required to take effort to configure the system. Therefore, even though it extends the capabilities of TreasurePhone, the potential of this approach is debatable. On the one hand, the question needs to be investigated, to what extent users are willing to invest effort for configuring locations and respectively actions. On the other hand, the question which sensors are appropriate as basis for locations and potentially for actions needs clarification.

Alternatively, sensor data can be used for building probabilistic models for automatically classifying to which context the mobile phone should adapt by activating the most appropriate sphere. Raento et al. showed with ContextPhone that using mobile phones equipped with sensors complex aspects such as user availability can be modeled [3]. Nevertheless, it is unknown to what extend sensor data are practical for modeling the user's particular need for privacy and security protection.

Using probabilistic models based on machine learning suffer from this amount of uncertainty. That is, for a particular amount of situations the model would classify the current contexts incorrectly. Therefore, the question arises to what extend a system which deals with uncertainty is capable to support privacy and security protection and how far classification errors can be controlled.

4. REFERENCES

[1] A. K. Karlson, A. J. B. Brush, and S. Schechter. Can I Borrow Your Phone?: Understanding Concerns when Sharing Mobile Phones. In *CHI '09*, 2009.

[2] J. Lehikoinen, J. Lehikoinen, and P. Huuskonen. Understanding Privacy Regulation in Ubicomp Interactions. *Personal and Ubiquitous Computing*, 12(8), 2008.

[3] M. Raento, A. Oulasvirta, R. Petit, and H. Toivonen. ContextPhone: A Prototyping Platform for Context-Aware Mobile Applications. *IEEE Pervasive Computing*, 4(2):51–59, 2005.

[4] R. Ricci, G. Chollet, M. Crispino, S. Jassim, J. Koreman, A. Morris, M. Olivar-Dimas, S. García-Salicetti, and P. Soria-Rodríguez. The "SecurePhone" a Mobile Phone with Biometric Authentication and E-signature Support for Dealing Secure Transactions on the fly. In *SPIE 2006*, 2006.

[5] J. Seifert, A. De Luca, B. Conradi, and H. Hussmann. TreasurePhone: Context-Sensitive User Data Protection on Mobile Phones. In *Pervasive 2010*, Helsinki, Finland, 17–20 May 2010. (to appear).

[6] 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 '03*. IEEE Computer Society, 2003.

[7] F. Stajano. One User, Many Hats; and, Sometimes, no Hat - Towards a Secure yet Usable PDA. In *12th Int. Sec. Protocols WS*. Springer, 2004.

[8] F. Stajano. Will Your Digital Butlers Betray You? In *WPES '04*. ACM, 2004.

[9] A. Whitten and J. D. Tygar. Why Johnny can't Encrypt: A Usability Evaluation of PGP 5.0. In *8th USENIX Security Symposium*, 1999.