TreasurePhone: Context-Sensitive User Data Protection on Mobile Phones

Julian Seifert[1], Alexander De Luca[2], Bettina Conradi[2], and Heinrich Hussmann[2]

[1] Bauhaus-University Weimar, Bauhausstr. 11, D-99423 Weimar, Germany
julian.seifert@uni-weimar.de
[2] University of Munich, Amalienstr. 19, D-80333 Munich, Germany
{firstname.lastname}@ifi.lmu.de

Abstract. Due to increased input and output capabilities, mobile phones hold many different kinds of (mostly private) data. The need for finer grained profiles and integrated data security on mobile phones has already been documented extensively (e.g. [1]). However, there are no appropriate concepts and implementations yet to handle and limit access to data on mobile phones. TreasurePhone has been designed to address this specific problem. It protects the users' mobile phone data based on their current context. Privacy protection is realized by *spheres*, which represent the users' context-specific need for privacy. That is, users can define which data and services are accessible in which sphere. TreasurePhone exploits context information to support authentication and automatic activation of spheres by *locations* and *actions*. We conducted a user study with 20 participants to gain insights on how well users accept such a concept. One of the main goals was to find out whether such privacy features are appreciated by the users even though they make interaction slower and might hinder fast access to specific data. Additionally, we showed that integration of context information significantly increases ease-of-use of the system.

1 Introduction

Modern mobile phones support the creation and storage of many kinds of data ranging from contacts and e-mail to photos and text documents. At the same time, the amount of stored data is growing enormously which increases the need for securing the privacy of this data [2]. For instance, the integration of mobile phones into enterprise environments for mobile handling of e-mail, contacts and other data is enjoying increasing popularity. However, mobile phones still use a simple privacy/security model that only distinguishes between *locked* and *unlocked* [1].

Users have different contexts in their life such as family and work each with a corresponding need for privacy [3]. This makes privacy management of the data stored on their mobile phones practically impossible. That is, a user who has a single mobile phone for her working context as well as for private use cannot hide data belonging to one context while being in the other one. When working for companies that have high security standards, a user might face additional usage restrictions to avoid exposing business data to third parties by using the business mobile phone for private use as well.

One solution for this challenge would be to use more than one mobile phone. Users might have a mobile phone for their work as well as a personal one. From a usability

P. Floréen, A. Krüger, and M. Spasojevic (Eds.): Pervasive 2010, LNCS 6030, pp. 130–137, 2010.

perspective this solution is not satisfying as there are usually more contexts than only *work* and *personal*. Therefore, users would need to use one mobile phone for each context they have.

We argue that privacy protection should be an essential part of the mobile device's operating system and should be addressed during the design of mobile systems. In this paper, we present TreasurePhone which supports context-sensitive protection of the user's data by allowing the user to define so called *spheres*. TreasurePhone uses *locations* for automatic activation of spheres and supports interaction with the user's environment to activate appropriate spheres on the go. TreasurePhone enables users to secure their data in each context in a sophisticated way using one mobile phone. Hence, TreasurePhone reduces the risk of unwillingly disclosing sensitive and private data.

2 Related Work

Work related to TreasurePhone can be generally classified into three categories: conceptual work about data privacy for mobile devices, authentication mechanisms for cell phones, and context-dependent adaptive mobile devices.

Stajano addresses privacy issues that arise from sharing (willingly or unintended) a personal digital assistant (PDA) with others [4]. He describes a system for PDAs which is based on the observation that some data and applications could be used by anybody who gets access to the PDA. However, other applications and data should be accessible only by the legitimate owner of the device. Accessing these *private areas* or "hats" would require authentication and thus secures the privacy of the user. In their work, Karlson et al. conducted interviews to find out basic requirements of data privacy on mobile phones. Their results suggest to use *usage profiles* that correspond to different contexts of the user [1]. These would allow sharing the mobile phone to others without risking disclose of private data. They showed that users would appreciate a security model for mobile phones that is based on usage profiles enabling privacy management. However, the concept of usage profiles was not implemented. Nevertheless, this work, suggesting a role based access model, strongly influenced the design of TreasurePhone.

With *SenSay* Siewiorek et al. present a mobile phone that adapts its behavior in a context-based way [5]. This system processes data captured by several sensors and determines the user's current context based on the results. SenSay adapts the ringer volume, vibration and alerts to the current context. It can further provide remote callers with the ability to communicate the importance of their call which optimizes the availability of the user. Another contribution with its focus on context-based adaptation is presented by Krishnamurthy et al. [6]. Instead of using various sensors to determine the current context of a user, this system makes use of near field communication (NFC). With NFC, the context can be determined on a fine grained base. This system as well as SenSay manage to determine the context of the user, but use a different approach. Both systems do not focus on privacy issues or data security.

TreasurePhone provides a first implementation of a usage profile based system for mobile devices as suggested by Stajano and Karlson et al. The prototype applies findings presented by Krishnamurthy and Siewiorek and combines them to provide an advanced security model.

3 TreasurePhone

Threat model. In this work, we model two main threats against which the described system is resistant:

The first threat consists in unwillingly disclosing private or unappropriate data to the "wrong" people. Mobile phones are often borrowed to friends and other people, mostly to help them by providing a possibility to make phone calls, browse the Internet, etc. While interacting with the phone, the borrower might accidentally gain access to data that the owner of the mobile phone might want to keep private (e.g. when browsing the photos on the mobile device). Using TreasurePhone, a special sphere could be used that grants access to the call application only to avoid such problems.

The second threat are attackers that willingly try to steal information (e.g. important business data) from a user. By disabling (and encrypting[1]) data of other contexts, TreasurePhone limits those kind of attacks. For instance, business data can only be stolen while the device is set to the business sphere.

Concept. Privacy cannot be seen as a fixed state. It rather means dynamically controlling the disclosure and use of personal information [7]. The dynamic character of privacy is stressed by its context-depended nature [3]. Furthermore, the user's grasp of what kind of personal data is considered as private is highly individual [8]. In the field of sociology and psychology, the concept of *faces* exists that was proposed by Goffman [9]. According to Goffman, people use different faces depending on their current context; a face defines what information a person reveals to a specific audience.

The concept of TreasurePhone is based on the hypothesis that users are willing to protect and manage the privacy of their private data stored on their mobile phones. Based on Goffman's faces we propose the concept of *spheres* that allow users to protect their data privacy. A sphere represents the user's privacy requirements for data on her mobile phone in a specific context. That is, the user can define which applications such as e-mail clients, address books, photo viewers etc. are available in a specific sphere and furthermore, what exact data is accessible and which is not. One can imagine a sphere as a filter that lets pass only data that are not private in this sphere. This way, users could create spheres for their home, family and friends as well as work context – each providing only as much access to data as desired. The spheres concept includes one special sphere that allows exclusive administrative actions such as creating, editing or deleting spheres as well as deleting or changing access rights of data. This sphere is called *Admin Sphere* (*AS*) and requires the user to authenticate before accessing it. Usually this sphere will only be active when the user wants to perform administrative work. All other spheres do not allow deleting data or editing access rights of data. Besides the *AS*, TreasurePhone contains three spheres by default: *Home*, *Work* and *Closed*, which serve as examples of typical configurations that are not bound to certain contexts but can be applied in various matching situations. While *Home* provides access to all services, *Closed* denies access to all of them. This set of default spheres was compiled based on the results of a small study with five participants who used diaries to collect the contexts for which they would use spheres.

[1] Please note that this feature has not been implemented in the prototype.

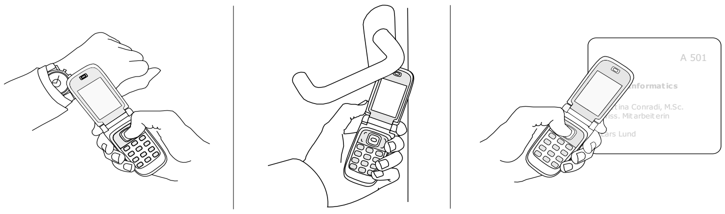


Fig. 1. a) Authentication using a personal token that is integrated into a wristband. b) Controlling a lock using actions. c) Reading a location that is based on an NFC tag integrated in a nameplate.

In order to protect the data, the user chooses the appropriate sphere depending on the current context. However, to prevent any person other than the legitimate owner from accessing private data, the activation of other spheres requires the user to authenticate to the system if the current sphere is not the *AS*. Fast and secure methods for authentication that do not require manual entry of a PIN minimize the effort for the user [4]. The TreasurePhone prototype supports authentication using a personal token that contains an NFC tag (see Figure 1a). It has to be noted here, that the benefit of the personal token comes with a security flaw. If an attacker can steal both, the token and the mobile device, full access to the device will be granted. To minimize the effort of spheres even further, context-dependent activation of spheres by *location* is supported by the system. A location in TreasurePhone is a configuration that is associated with a sensor value such as GPS coordinates, a Wi-Fi network identifier, a Bluetooth identifier or an RFID tag (see Figure 1c). Whenever a location is recognized, the corresponding sphere is activated. Besides locations, TreasurePhone supports interaction with the user's environment by *actions*. An example could be a Metro Network (like the Tokyo Metro system) that supports the use of NFC-enabled mobile phones to handle payment. When a user leaves the metro network at his work place, touching the gate mechanism with the phone would activate the *Work* sphere. Entering the metro network at his work location on the other hand could switch back to the *Closed* sphere.

Example Scenario. Using TreasurePhone implies initial effort for configuring the system. However, this is not mandatory because of the set of default spheres that are available. The configuration effort consists of creating individual spheres according to the user's needs and contexts in addition to the default spheres. For example, Bob could create a new sphere named *Friends*, which he intends to use while he is with friends, for instance at home or in a pub. He configures this sphere to allow access to messages, the address book and the photo service. Now Bob can start to create and manage data. After a while the configuration of Bob's TreasurePhone looks like the illustration in Figure 2. In the spheres *Home*, *Friends* and *Work* some contacts and other documents are visible. The spheres *Friends* and *Home* overlap and both allow access to the data in the intersection. The *Admin Sphere* encloses all data and Bob can access all data while this sphere is active.

When Bob turns on his mobile phone the *AS* is initially activated. After checking if there are new messages and having a look at today's appointments at work, Bob activates the *Home* sphere. Thereby personal data like photos, messages and contacts

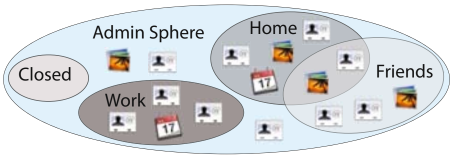


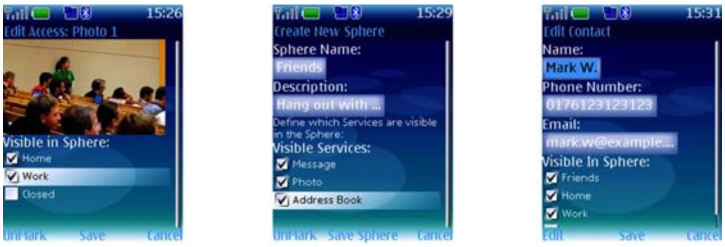
Fig. 2. The sphere model: The *Admin Sphere* allows access to all data; other spheres limit access and might overlap

are accessible, however, all business related data are hidden now. When Bob leaves his apartment he locks the RFID based lock of the door using his TreasurePhone, which is also usable as a key (See Figure 1b). This requires the configuration of corresponding *actions* for the lock. Bob configured the action *Locking Door* to activate the *Closed* sphere when finished. By using this action Bob does not have to think of changing the sphere. As Bob arrives at his office, his mobile phone detects the Bluetooth identifier of his desktop computer, which is associated with the location *My Office*. The sphere *Work* gets activated automatically. Now Bob has access to his calendars, documents, messages and all other data that is work-related. However, photos of his family and friends are now hidden.

Prototype Implementation. The TreasurePhone prototype is written in Java ME and implements the fundamental concepts: spheres, locations, actions and services as well as an abstraction for data. A sphere management subsystem controls which sphere is activated and what data and services are accessible. Activation is based on context information such as sensor data that correspond to locations and actions. The implementation also contains interfaces for applications which allows access management of applications that are registered as services.

The TreasurePhone prototype provides basic functionalities of standard mobile phones such as call, SMS, address book, camera, and a photo viewer. The user interface changes or grants access depending on whether the AS or another sphere is activated (see Figure 3). Editing access rights for data is only available while the *AS* is activated.

The default assignment of data access rights follows the basic rule: data is accessible in the sphere in which it was created. For instance, if the sphere *Home* is activated while


15:26
Edit Access: Photo 1
Visible in Sphere:
☑ Home
☑ Work
□ Closed

15:29
Create New Sphere
Sphere Name:
Friends
Description:
Hang out with ...
Define which Services are visible in the Sphere:
Visible Services:
☑ Message
☑ Photo
☑ Address Book

15:31
Edit Contact
Name:
Mark W.
Phone Number:
0176123123123
Email:
mark.w@example...
Visible In Sphere:
☑ Friends
☑ Home
☑ Work

Fig. 3. Screens of TreasurePhone (*AS* activated): *a)* Editing access rights for a photo. *b)* Creating a new sphere named “Friends”. *c)* Editing contact details.

the user makes a photo, this picture is accessible by default in this sphere. In case of the *AS* being activated, the image would not be accessible in any of the normal spheres.

We chose the Nokia 6131 NFC mobile phone as platform for the first prototype, which comes with a built-in NFC reader. The prototype allows the user to authenticate via a personal token, which contains an NFC tag or by entering a PIN. NFC is also used for locations. The physical correspondence of a location in TreasurePhone is an NFC tag attached to an object (see Figure 1 *c*).

4 User Study

We conducted a preliminary evaluation of TreasurePhone to study two basic questions. First, will users accept the increased complexity of handling the mobile device required by the privacy features? Second, will the use of automatic sphere switching by context (locations and actions) have a positive effect on the usability of the system? We randomly recruited 20 volunteers; 8 female and 12 male. Participants were undergraduate and PhD students with a technical background and aged between 23 and 32 years. They indicated they had all used mobile phones for at least six years. Half of the subjects use profiles (like silent, vibrate etc.) of their mobile phone on a daily basis; the others only occasionally or not at all. 19 of the subjects use PIN authentication when they turn on their mobile phone while only 3 use PIN authentication after each period of inactivity. During the study we first explained the system and then a training phase with the prototype was conducted by the participants. For training, each feature of the system was explained to them and tested with a small task. Next, practical tasks were carried out. Finally the users filled out a questionnaire regarding the system. Answers were given on a five point Likert scale (1=worst, 5=best). Overall the procedure took around 40 minutes, up to one hour.

The practical tasks started with a system configuration, in which users had to create and configure a sphere. This was followed by a series of five tasks in randomized order, which covered all actions that are specific for the concepts of TreasurePhone (see figure 4). For instance, participants created a contact in the address book and set the access rights for this contact to ’visible in sphere x’. Other tasks required the participant to activate different spheres in order to hide or get access to data. These five tasks were repeated two times in randomized order. One time participants used a prototype that did not integrate context information and a second time they used a system that supported context information integration. That is, one time the participants could make use of token based authentication (a wristband with an integrated NFC transponder), locations, and actions and the other time they could not. The context free prototype used an assigned PIN to activate the *Admin Sphere* and to switch between spheres.

Results of the study show that on average, users consider the system easy to understand (Avg=4.4, Mdn=4, SD=.5). They appreciate the support given by integrated context and 19 out of 20 participants stated that they would prefer using a system that implements locations, actions, and token based authentication. Users rated the general system’s capabilities to secure privacy as 4.2 (Mdn=4,SD=.8) and the usefulness of spheres for privacy protection as 4.6 (Mdn=5,SD=.5). However, users estimated their willingness to store more sensitive data on their mobile phone, if this was running TreasurePhone, with 3.2 (Mdn=3,SD=1.1). Nevertheless, users stated that on average (4.1)

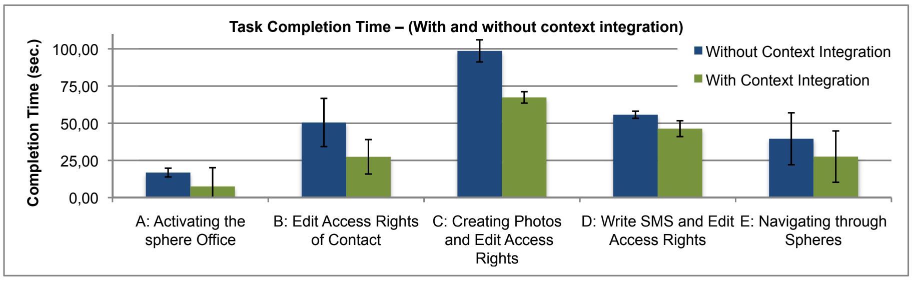


Fig. 4. Task completion times of the practical tasks with and without context information integration (error bars display the standard deviation)

they would feel more secure when sharing their TreasurePhone secured mobile phone with others (Mdn=5,SD=1).

Because this is a laboratory experiment, our results should be handled with care. However, they suggest user acceptance of the security features, and a preference for the context integration. Users did not mind increased complexity (and even did not consider it that complex). Also they agreed that their data would be more secure on such a phone. One user confirmed this by stating "I wouldn't need to be concerned about my data so much when I want to share my mobile phone with a friend or when I just leave it at some place". One user was especially happy that this system would provide her the possibility to limit the access to specific applications as well: "I like that I can even define access policies for facilities such as camera and address book". The results are already quite encouraging, even more since none of the participants was in a business that requires carrying around sensitive data on a mobile device. We expect business users to be even more concerned about their data privacy.

A detailed analysis of task completion times shows that, not surprisingly, tasks were completed significantly faster with the prototype that uses context information for task switching (see Figure 4). The data was analyzed using paired-samples t-tests. For each task the prototype using NFC was faster than the PIN version. The results for task A ($t(18)=7.26$, $p<.001$), B ($t(16)=4.15$, $p<.003$), C ($t(15)=5.91$, $p<.001$) and D ($t(18)= 3.85$, $p<.003$) were highly significant while the difference in task E was significant ($t(17)=2.89$, $p<.05$). The positive results for the context version are supported by the users' opinion. One user explicitly stated "it makes changing the profiles fast and easy".

5 Conclusions and Future Work

In this work, we presented TreasurePhone, an approach toward a mobile phone operating system which supports context dependent data privacy for users based on spheres. Supporting locations and actions for changing spheres makes adapting to the users' current context easier. The results of the user study show that integrating context and fast authentication makes the system significantly faster in use and is favored by the users over a system that requires manual authentication and manual sphere switching.

While our study suggests that users are interested in the security and privacy provided by TreasurePhone, future studies of long term use would be valuable to determine whether users prefer using spheres to existing “binary” security models in day to day use of their phones. Steps toward answering this question include implementing an advanced prototype, whereas spheres are integrated at the operating system level in order to meet the requirements for a longterm study. Additionally, we would like to implement support of further sensors for interaction with locations such as GPS or Bluetooth identifiers and thus extend TreasurePhone’s context sensitivity. A very interesting aspect with respect to the sensors is which of them are actually suitable for context switching from a usability’s point of view. That is, which of them can be used and understood by the users.

Acknowledgments

We would like to thank the reviewers and especially A.J. Brush for their fruitful comments that greatly helped to improve this paper.

References

1. Karlson, A.K., Brush, A.J.B., Schechter, S.: Can I Borrow Your Phone?: Understanding Concerns when Sharing Mobile Phones. In: CHI 2009: Proceedings of the 27th international conference on Human factors in computing systems (2009)
2. Stajano, F.: Will Your Digital Butlers Betray You? In: WPES 2004: Proceedings of the 2004 ACM workshop on Privacy in the electronic society. ACM, New York (2004)
3. Lehikoinen, J.T., Lehikoinen, J., Huuskonen, P.: Understanding privacy regulation in ubicomp interactions. Personal Ubiquitous Comput. 12(8), 543–553 (2008)
4. Stajano, F.: One user, many hats; and, sometimes, no hat - towards a secure yet usable pda. In: 12th Int. Security Protocols Workshop. Springer, Heidelberg (2004)
5. Siewiorek, D., Smailagic, A., Furukawa, J., Krause, A., Moraveji, N., Reiger, K., Shaffer, J., Wong, F.L.: SenSay: A Context-Aware Mobile Phone. In: ISWC 2003: Proceedings of the 7th IEEE International Symposium on Wearable Computers, Washington, DC, USA. IEEE Computer Society, Los Alamitos (2003)
6. Krishnamurthy, S., Chakraborty, D., Jindal, S., Mittal, S.: Context-Based Adaptation of Mobile Phones Using Near-Field Communication. In: Annual International Conference on Mobile and Ubiquitous Systems, pp. 1–10 (2006)
7. Jiang, X., Hong, J.I., Landay, J.A.: Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing. In: Borriello, G., Holmquist, L.E. (eds.) UbiComp 2002. LNCS, vol. 2498, p. 176. Springer, Heidelberg (2002)
8. De Luca, A., Hußmann, H.: Threat Awareness - Social Impacts of Privacy Aware Ubiquitous Computing. In: INTER: A European Cultural Studies Conference in Sweden (INTER 2007), Norrköping, Sweden, June 2007, pp. 1650–3686 (2007)
9. Goffman, E.: The Presentation of Self in Everyday Life. Doubleday Anchor Books, New York (1959)