FaceProfiles: Inconspicuous, Private and Secure Mobile Device Sharing

Alina Hang
Media Informatics Group
University of Munich (LMU)
alina.hang@ifi.lmu.de

Emanuel von Zezschwitz
Media Informatics Group
University of Munich (LMU)
emanuel.von.zezschwitz@ifi.lmu.de

Alexander De Luca
Media Informatics Group
University of Munich (LMU)
alexander.de.luca@ifi.lmu.de

Heinrich Hussmann
Media Informatics Group
University of Munich (LMU)
hussmann@ifi.lmu.de

CHI 2014 Workshop on Inconspicuous Interaction, April 26, 2014, Toronto, ON, Canada.

Abstract
Mobile device sharing can lead to socially awkward situations – for example when sensitive information is (un)intentionally revealed (e.g. photos). Therefore, we propose a concept called FaceProfiles that enables owners of mobile devices to share their device in a spontaneous, privacy-aware and secure manner. The concept combines two existing approaches (i.e. face recognition and rights management) to design an inconspicuous way to adapt the user interface when sharing the device, circumventing social implications like actively showing mistrust to others.

Author Keywords
Mobile devices, security, privacy, device sharing.

ACM Classification Keywords
H.5.2. Information interfaces and presentation: User Interfaces – User interface management systems (UIMS).

Introduction
Mobile devices have evolved from plain communication devices to small personal computers [1] that store numerous of sensitive data (e.g. photos, videos or contact details). In order to protect this data, users can set up a variety of authentication mechanisms like PINs or (graphical) passwords.

However, current lock screen mechanisms follow all-or-nothing approaches, which lead to privacy issues when users share their device with others like for communication purposes (e.g. a friend who needs to make a call) or content presentation (e.g. photos that are shown to a friend). Once the device is unlocked and in the hands of the borrower, the owner of the device has only limited control. They have to fear unintentional revelation or manipulation of their personal data [3, 4].

The concerns that users have during device sharing strongly depend on the trust level they have to the borrower [2]. Therefore, Liu et al. [5] proposed a system called xShare that allows device owners to create profiles with different right policies. Each time the device is shared, the user has to select one of the previously defined profiles. However, this approach can lead to social implications (i.e. the borrower sees how the profile is switched) and thus, endangers the trust between device owner and borrower. Concepts for mobile device sharing need to be less obtrusive and should be hidden from the device borrower.

Our previous research [3] has shown that mobile device sharing is short, spontaneous and can be initiated by the device owner or borrower. In general, users like to be in full control of what is being shared or hidden, meaning that users want a flexible solution that enables them to define rights on different levels: While some applications can be shared as a whole, other applications should be restricted to certain functionalities (e.g. read-only operations).

Concept

We propose a concept called FaceProfiles that enables users to share their device in a spontaneous, privacy-aware and secure manner. It combines existing approaches (i.e. face recognition and rights management) for an inconspicuous interaction between device owner and borrower.

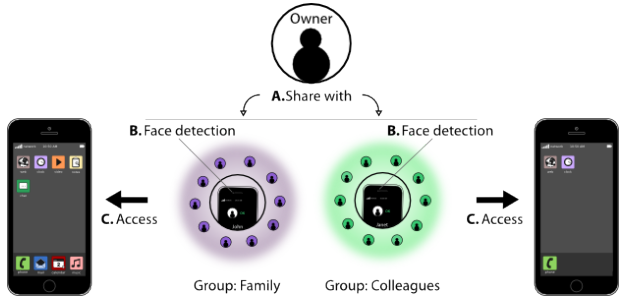

Figure 1: FaceProfiles concept. The device owner has the intention to share the smartphone (A). Borrowers are recognized by face detection (B) and the user interface is adapted accordingly (C).

The basic idea is that the device implicitly adapts to new sharing partners and restricts access to data and applications (either as a whole or partially). Thus, sensitive information and operations are hidden from the borrower in a seamless manner to prevent socially uncomfortable situations.

Our concept consists of three components. First, contacts are organized in groups (e.g. family or friends). Second, each group is granted different permissions in order to restrict access accordingly. Permissions can be managed on application as well as functionality level. Third, the previously information is combined with face recognition (using the device's front camera) to adapt the user interface accordingly when sharing the device.

Sharing Procedure
The general sharing procedure is depicted in figure 1. Whenever the owner shares the device (A), the new user is recognized by face detection (B). Depending on the group(s) the borrower is assigned to, the access rights for this user are calculated and the user interface is seamlessly adapted accordingly (C). Sharing the device with a person that is not in the contact list requires special treatment like a default profile with limited usage rights.

User Authentication
Face recognition for user authentication can take place at different stages of device sharing. It can be applied continuously (that is, during all times of the interaction) or it can be connected to the standard unlock approach as known from current smartphones like the swipe gesture on Android devices and iPhones. Whenever a user (owner or borrower) unlocks the device (e.g. using a swipe gesture), face detection is initiated. This approach has the advantage that collisions, like several users interacting with the device, can be avoided. Additionally, since face detection only takes place at a dedicated time slot, the battery life is not affected excessively, which is crucial for mobile devices.

Combining the identification mechanism with the unlock procedure, copes well with social implications, since the interface stays invisible until an unlock has been performed. Once it is visible, the interface has already been adapted. If the change is small (e.g. only two apps missing), the change blindness effect helps to make the adaptation difficult to notice.

It should be noted that the technical aspects of face recognition are not in the focus of this work. We assume the existence of a well-working face recognition mechanism. The data (i.e. photos) that is needed for face recognition can be retrieved from various sources on the mobile device. For example from pictures that the user has assigned to contacts or from social networks like Facebook. Instead of face recognition, novel devices might feature fingerprint readers, which could also be used to implicitly authenticate the user.

Group and Contact Management
Mobile devices offer users the possibility to organize their contacts in different groups. Our concept exploits this possibility to grant permissions on a group-level. For example, while contacts in group *A* have the permissions to read and write emails with a given application, contacts in group *B* have read-only access.

One of our previous studies [3] has shown that there are some groups that most users have in common when organizing their contacts. These include family, friends and colleagues. At the same time, groups can be very distinct between different users. Thus, offering a predefined set of groups seems important to support fast generation and sorting, but also a flexible organization of groups should be possible, e.g. allowing user defined groups or putting contacts into multiple groups.

In order to reduce the burden of group organization, existing groups can be retrieved from other sources like social networks.

Rights Management
The use of groups is advantageous, since it facilitates the process of granting of rights. Permission can be given on an application or functionality level. For

example, group A has the right to use application B. However, at some point, users might want to have more detailed control of what group A is granted to do, e.g. the group can use application B, but only functionality C without the functionality D.

Moreover, there are instances in which a user belongs to a group but should not get the same rights for a specific app based on e.g. trust issues. Thus, the rights management mode has to support such special cases. That is, while rights assignment on group level is fast, detailed user rights have to be supported as well.

Discussion, Conclusion and Future Work

FaceProfiles empowers users to share only specific parts of their mobile devices and adapts implicitly to new sharing scenarios. It is based on sharing preferences of the users and is flexible in assigning new rights to new users (by exploiting groups) and new applications. We are aware that predefined groups might lead to a "lazy user" who relies solely on them. This is something that needs to be studied. Even the best privacy concept can only succeed if the trade-off between configuration effort and benefit is acceptable.

The main goal of this concept is to create an inconspicuous approach for mobile device sharing to circumvent socially awkward situations. However, there are further challenges when combining existing approaches that have to be addressed.

Though face recognition technologies are advancing, they still lack in terms of accuracy. Thus, how can the proposed concept handle false positives/negatives? While the latter can be addressed by allowing users to define a guest account which is used as fallback solution, the former occurrence has impacts on the user's privacy (i.e. information is revealed that the sharing partner is not supposed to see).

Users are implicitly authenticated by their face (which is also sensitive information), without actually knowing about the authentication procedure. How comfortable are users with this kind of authentication? How much information does the system have to provide to the user about this? And if further information is provided, how does this affect the inconspicuous nature of the proposed concept?

We believe that the workshop will be a great opportunity to discuss these questions.

Acknowledgement

This work was funded by a Google Research Award.

References

[1] Böhmer, M., Hecht, B., Schöning, J., Krüger, A., Bauer, G. Falling asleep with Angry Birds, Facebook and Kindle: a large scale study on mobile application usage. In Proc. Mobile HCI 2011.

[2] Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., Powledge, P. Location disclosure to social relations: why, when, & what people want to share. In Proc. CHI 2005.

[3] Hang, A., von Zezschwitz, E., De Luca, A. Too much Information! User Attitudes towards Smartphone Sharing. In Proc. NordiCHI 2012.

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

Liu, Y., Rahmati, A., Huang, Y., Jang, H., Zhong, L., Zhang, Y., Zhang, S. xShare: supporting impromptu sharing of mobile phones. In Proc. MobiSys 2009.