Towards Privacy-Aware Mobile Device Sharing

Emanuel von Zezschwitz
University of Munich
Media Informatics Group
Amalienstr. 17, 80333 Munich, Germany
emanuel.von.zezschwitz@ifi.lmu.de

Alina Hang
University of Munich
Media Informatics Group
Amalienstr. 17, 80333 Munich, Germany
alina.hang@ifi.lmu.de

ABSTRACT

Modern smartphones are loaded with sensible data. At the same time, there are situations, in which a user must share or wants to share the device with others. Since common authentication methods still follow a single-sign-on approach, new privacy issues arise. We argue that sharing cannot always be avoided and thus should be supported by refined authentication systems. Our assumption is based on the findings of a focus group that we conducted to get insights about sharing practices, privacy threats and need for protection.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation (e.g. HCI)**]: User Interfaces - User interface management systems (UIMS).

General Terms

Design, Human Factors, Security.

Keywords

Mobile device, sharing, security, privacy.

1. INTRODUCTION

Today's smartphones are multimedia devices whose features go beyond writing text messages and making phone calls. The diversity of available services and applications implicates that a modern mobile device provides access to various types of sensitive data. At the same time, due to the additional (online) services, current devices are more often shared than older mobile phones. In contrast to the users' sharing behaviour, authentication methods used to secure data access did not change and do still follow all-or-nothing approaches [2].

Based on the findings of Karlson et al. [2], we assume that mobile device sharing cannot always be avoided and that people are concerned about their data. Consequently, they want to share only specific functionalities of their smartphones (e.g. messaging), while the rest should remain hidden. We argue that such all-or-nothing approaches are outdated and need to be refined by new authentication concepts. Only few work has been done on privacy issues related to mobile device sharing. Consolvo et al. [1] examined location disclosure and discovered that the amount of private information people are willing to share is based on their social relationships. In 2006, Stajano [4] elaborated on a theoretical concept, which supports secure device sharing. Three years later, Liu et al. [3] implemented the first concept, called xShare, which enables users to hide private data by explicitly setting preconfigured profiles.

We conducted a focus group to get up-to-date insights into mobile device sharing with current smartphones. The results indicate that the subject is of high relevance and new authentication and sharing mechanisms need to be implemented to reduce the users' concerns.

2. FOCUS GROUP

Although, we are aware of the fact that focus groups do not target at getting a representative sample and there are limitations especially on generalizability, we chose to conduct a focus group to get first insights on the topic in a short time frame.

Our main goal was to find out: *a*) how people share their devices, *b*) with whom and why and *c*) which privacy and security concerns they have while sharing.

2.1 Design and Conduction

We recruited seven participants for the focus group, five were male. The average age was 23 (22 to 27). Following the conventions of focus groups, the group was chosen not to be too heterogeneous. Overall the discussion lasted 70 minutes, free drinks and food were provided. The session was recorded on video and lead by a moderator. In addition, two minute writers were present.

2.2 Results

The focus group revealed that there are three main concerns: (a) The fear of losing sensitive data, (b) the fear of data manipulation and (c) the fear of misuse.

While (a) is privacy related, (b) and (c) are security issues. Privacy concerns (e.g. "someone could read my emails") were mentioned most often. Data manipulation issues can be unintended and often remain unnoticed by the device owner (e.g. changing system settings). Misuse is any deliberate attack, which does not necessarily change stored data (e.g. posting inappropriate status updates using an active Facebook account).

Device sharing is not always intended by the device owner and thus can be unauthorized. In one case, an unattended device was used to take photos. In a second case, a person

Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)
June 18, 2012, Newcastle, UK

was allowed to view some pictures but read the owner's private messages instead. In addition, the focus group revealed that people have privacy concerns even when sharing the device with trusted friends. Mainly due to push notifications, which are triggered in shared scenarios. Another concern is based on the fact that friends could access sensitive data by mistake (e.g. while browsing photos).

According to our participants, most critical applications were photo galleries, messaging apps, social media and web browsers. Our participants were especially concerned about the fact, that apps using online accounts (e.g. Facebook) usually remain active after the user once logged in (even after rebooting) and thus grant access to everyone using the device without repeating the authentication process.

Our participants agreed in parents and close friends being the most trustworthy groups. However, the discussion about which data should be shared to those groups was very controversial. Examining sharing preferences according to unknown persons is illustrating the individuality of privacy concerns. While one participant stated she would never share a device with an unknown person, another participant said that she has no privacy concerns at all due to the fact that private data is only critical when shared with closely related people. Consequently, sharing a mobile phone is not only a matter of trust but also influenced by the data-borrower relationship.

Another noticeable finding is that in contrast to close friends who are considered confidential based on their relationship, most participants would share a device with their parents because they "are too unskilled to access private data". However, the trust level does not always depend on the relationship status as even close friends can be untrustworthy and some data may only be critical to specific persons inside a group. Hence, privacy settings have to be configurable on a very detailed individual-related level.

3. IMPLICATIONS

Finally, we gave our participants the chance to come up with own concepts to protect sensitive data while device sharing.

One proposal consisted of a so-called "kiosk mode". A mobile device running this mode would load all applications in their initial state, hiding all personal information. The participants stated that such a mode should be available immediately (e.g. via a dedicated button). However, the participants mentioned this mode would not allow for fine-grained privacy settings as it would not be possible to "show some pictures and hide the rest". In "kiosk mode", all galleries would be empty. Thus, it can be interpreted as an all-or-nothing approach on data level.

This shows that one of the main problems is to find the right granularity of data protection. The results indicate that device sharing is strongly app-related and data-related (e.g. showing a subset of pictures [data] in a gallery [application]) and thus a concept must be configurable on a single file level. Another important aspect is that in most cases, sharing a mobile device is a spontaneous action and thus, privacy settings must adapt as quickly as possible to new sharing partners.

As two participants already experienced unauthorized device usage, a concept should implement white-listing and adjust automatically. The findings illustrate that privacy needs are very subjective. Thus, all security levels from "just me" to "anyone" should be supported.

The authentication mechanism has to be non-obstructive and should not require the user's attention. Therefore an implicit authentication approach like face recognition should be deployed.

Finally, the focus group revealed social implications, as several participants were worried about a friend being offended to see that some of the phone's features are locked. Such trust issues have to be avoided.

4. CONCLUSIONS

The focus group revealed that people are prone to share mobile devices and that privacy concerns are an indispensable part of this action. The results indicate that currently used all-or-nothing security mechanisms are outdated and do not adequately support privacy-aware mobile device sharing.

Based on the findings, we argue that new authentication methods need to be implemented, which are (a) usable and (b) secure and allow spontaneous mobile device sharing in a (c) relationship-aware, (d) transparent and (e) modular manner. In our future work, we plan to examine the different aspects of such a concept in more detail. A prototype shall be realised and evaluated in real life situations to proof its additional value compared to all-or-nothing approaches.

5. ACKNOWLEDGEMENTS

We want to thank Christian Becker for his valuable help with the focus group. This work was partially funded by a Google Research Award.

6. REFERENCES

[1] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, CHI '05, pages 81–90, New York, NY, USA, 2005. ACM.

[2] A. K. Karlson, A. B. Brush, and S. Schechter. Can i borrow your phone?: understanding concerns when sharing mobile phones. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, pages 1647–1650, New York, NY, USA, 2009. ACM.

[3] Y. Liu, A. Rahmati, Y. Huang, H. Jang, L. Zhong, Y. Zhang, and S. Zhang. xshare: supporting impromptu sharing of mobile phones. In *Proceedings of the 7th international conference on Mobile systems, applications, and services*, MobiSys '09, pages 15–28, New York, NY, USA, 2009. ACM.

[4] F. Stajano. One user, many hats; and, sometimes, no hat: Towards a secure yet usable pda. In B. Christianson, B. Crispo, J. Malcolm, and M. Roe, editors, *Security Protocols*, volume 3957 of *Lecture Notes in Computer Science*, pages 51–64. Springer Berlin / Heidelberg, 2006.