Bridging physical and virtual privacy mechanisms during mixed-presence collaboration: implications for inconspicuous privacy.

Mohamad Salimian
Dalhousie University
Halifax, Nova Scotia,
Canada B3H 4R2
srizi@cs.dal.ca

Derek Reilly
Dalhousie University
Halifax, Nova Scotia,
reilly@cs.dal.ca

Stephen Brooks
Dalhousie University
Halifax, Nova Scotia
sbrooks@cs.dal.ca

Bonnie MaKay
Dalhousie University
Halifax, Nova Scotia
bmackay@cs.dal.ca

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

Abstract

Providing usable privacy mechanisms should be a key design concern for collaborative technologies like shared displays and telepresence systems, especially when these technologies are intended for use in public spaces. However, differences in culture, experience and background knowledge make concrete approaches problematic. We argue that in order to achieve robust privacy-sensitive designs in mixed presence collaborative systems we need to consider both inconspicuous and conspicuous privacy actions, and moreover support actions that lie on a continuum between obvious and unseen. We illustrate this through the design of three physical privacy mechanisms that permit document sharing between collocated and remote collaborators. We explore each mechanism in a public "mixed reality cafeteria" setting.

Author Keywords

Privacy; inconspicuous styles; security

ACM Classification Keywords

Design; human factors; security

Introduction

Mixed presence collaborative environments are becoming popular in different domains such as healthcare, education and office work. Mixed presence systems can choose from or mix a range of technologies, including virtual worlds [1], video conferencing, and desktop sharing software.

During collaboration between remote and co-located collaborators many privacy events can happen, such as sharing documents (or a part of a document) with all or just a subgroup of participants, having visual or audible chat with other participants or having different levels of privacy relative to other collaborators in a larger group [2]. Being aware of ongoing events in a collaboration space helps participants and groups to manage their privacy in an effective way.

Privacy and security has to be managed simultaneously in two channels in a mixed presence spaces: collocated space (physical) and remote (virtual). Each channel requires appropriate privacy and awareness mechanisms.

People have well-established practices for negotiating privacy during collocated collaboration. However, these practices break down when collaborating over distances: for example, by not being able to determine easily when people are paying attention, and not being able to hide, show and share documents as is done with paper.

Our research is exploring potential designs to support privacy in heterogeneous, document-centric, mixed presence collaboration. Collaborative cross-reality involves the design of linked physical and virtual environments with the goal of supporting collaboration that fluidly combines and alternates between synchronous and asynchronous, collocated and remote modalities. In particular, we want to determine how people "naturally" manage security and privacy while performing some tasks both in the digital and real world. To better understand how to design for these situations, we plan to observe how individuals participate in activities that may require them either to reveal artifacts to or hide them from both co-located individuals as well as those remotely located. People utilize their prior experiences and the strategies and practices already developed through these prior experiences to make sense of encounters with IT artifacts [4]. Therefore, we want to explore how prior experiences with collocated collaboration influence how people choose to share documents with collaborators in mixed presence contexts. Often solutions do not build on prior experience: instead they focus on establishing secure procedures that users should follow, specifying proper security policies, and providing end-user assistance with these procedures or specifications [3][5]. We are exploring how physical patterns of security-related behavior might transfer to mixed presence collaboration (in particular, how users can manage their own privacy around a table whose contents are mapped onto a virtual table in a virtual world). Through this we hope to identify new research directions and design ideas pertaining to user-centric IT security.

Using inappropriate privacy mechanisms can confuse users and produce conflicts and undesirable results. As an extreme example, putting a curtain around your table in a café will simply attract attention from strangers. Expectations surrounding privacy are socially negotiated: varied cultural backgrounds yield differing expectations about personal space and privacy management, as do different contexts. Inconspicuous privacy management provides an opportunity to avoid conflicts and confusion between collaborators. However, sometimes a privacy action needs to be communicated to collaborators, as when revealing a card in a card game, for example. Physical privacy actions can involve both conspicuous and inconspicuous elements: to continue with the card game example, holding cards close to one's chest is conspicuous, while slightly adjusting their orientation to allow a friend to see them may be inconspicuous.

In mixed reality configurations, we want to map privacy actions across linked physical and virtual spaces. This challenges one's ability to achieve conspicuous and inconspicuous privacy actions, due to incongruities in the experience of local and remote players. For example, physical cards may be tracked, and their horizontal orientation mapped to their visibility in a linked virtual world. If this mapping is discrete (i.e. either visible or not visible), then inconspicuous privacy may be compromised, as the actor needs to be wary of card orientation threshold lest they unintentionally reveal their cards. A discrete mapping also gives remote players an impoverished view of the other players–leaving only conspicuous privacy actions visible—they would be unable to observe how players sort their cards, for example. If the mapping is continuous, for example by positioning cards in the virtual 3-D space according to their orientation in physical space, players at the physical game table might not know what remote players can and cannot see, again making it difficult to have control over how conspicuous or inconspicuous their actions are. With a continuous mapping remote players may be at an advantage, given a real-time 3-D view of how cards are held at the physical table, while being able to control exactly when their own cards become visible.

Card Game Prototype and Study Design

To learn how people might manage their own privacy around a tabletop whose contents are mapped onto a virtual table in a virtual world, we implemented a document sharing prototype and a card game that can be played by people seated at the table alongside remote participants who use virtual world clients. This is achieved using a combination of physical objects (in this case playing cards, paper documents, and physical blinds to hide personal workspaces) and virtual counterparts, combined using the TwinSpace mixed reality framework [6].

We want to observe the conspicuous and inconspicuous behavior of individuals in terms of how they share and hide their cards and documents (or parts of documents) both to the group around them and to those remotely. The implementation allows participants to manage their own security and privacy and negotiate it with the other participants. A participant can show one of his cards or documents to a collocated participant by showing it physically or to a remote participant by placing it face down on a dedicated region of the table. For instance if a participant is amused by how fortunate she is to end up with an ace, she can show the ace to selected participants in order to share her amusement and still not ruin the game. Again, we see here a difference in how conspicuous the private action may be, due to technological differences when sharing with a remote vs. local collaborator. A more continuous mapping could permit a local player to physically tilt her ace toward where a remote player is virtually located, but this requires a clear awareness of spatial correspondence and of the virtual locations of remote players, and faith that virtual player locations wholly determine what they can and cannot see. An alternative approach is to give each local player their own sharing region physically shielded from other local players using a blind. While this permits more discrete sharing, it invites the curiosity and suspicions of the other local players whenever the player's hand is brought behind the blind. During the document sharing activity, each participant will be given a fake credit card statement, and will be asked to share specific bill payments. We want to observe how participants share their documents or a portion with others. Again, this is a conspicuous action but the way users hold the documents can contain inconspicuous privacy actions, for example holding the statement so that credit card numbers cannot be read. This level of granularity in document sharing is hard to capture and translate into a virtual representation. Our technical approach is to take a snapshot/scan of the visible region of a document, and creating a rendition of that visible region as a unique virtual document. We anticipate that this side-effect of creating a virtual copy may be off-putting when sharing sensitive information.

Conclusion

We argue that during synchronous collaboration privacy should be managed dynamically by collaborators, often involving both inconspicuous and conspicuous forms (and sometimes both forms simultaneously). Our study gives us an opportunity to study and explore ways that people manage privacy and security in virtual and physical space simultaneously. Participants can use some conspicuous and inconspicuous mechanisms to protect their privacy, however technological limits impact the ability to achieve inconspicuous privacy actions (in particular) when communicating with remote collaborators. We hope to learn more about the suitability of different real-virtual mappings for managing privacy-sensitive mixed-presence collaboration.

References

[1] A. Petrakou, "Interacting through avatars: Virtual worlds as a context for online education," *Comput. Educ.*, vol. 54, no. 4, pp. 1020–1027, May 2010.

[2] J. Lang, "Privacy, Territoriality and Personal Space – Proxemic Thoery," in in *Creating Architectural Theory: The role of the behavioral sciences in design*, New York, 1987, pp. 145–156.

[3] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, 2012, pp. 1–16.

[4] J. McCarthy and P. Wright, "Technology as Experience," Oct. 2007.

[5] J. Goecks, W. K. Edwards, and E. D. Mynatt, "Challenges in supporting end-user privacy and security management with social navigation," in *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, 2009, p. 1.

[6] D. F. Reilly, H. Rouzati, A. Wu, J. Y. Hwang, J. Brudvik, and W. K. Edwards, "TwinSpace: an infrastructure for cross-reality team spaces," in *Proceedings of the 23nd annual ACM symposium on User interface software and technology - UIST '10*, 2010, pp. 119 – 128.