Managing Privacy During Ad Hoc Collaboration

Kirstie Hawkey

Faculty of Computer Science, Dalhousie University

hawkey@cs.dal.ca

Abstract

This research introduces the concept of privacy issues related to the incidental viewing of traces of previous activity during ad hoc co-located collaboration. Web browsers are the representative application, as several of their convenience features record traces of previously visited web visites. We introduce a 4-tier privacy gradient to allow individuals to classify privacy levels associated with their actual web browsing. Before being able to develop a privacy management solution, the nature of web browsing activity with respect to privacy concerns must be examined. This research begins that exploratory process.

1 Introduction

Privacy issues arise when private information is incidentally viewed on a computer display during ad hoc co-located collaboration. While this collaboration may be conducted around a group workstation intended solely for group work, more often individuals gather around a computer that is being used for personal as well as group business. When a work device is used at least partially for personal use, there can be an expectation by the user of a certain amount of privacy [5]. As computers are used, transactions are logged creating traces of the user's actions [3]. These traces of activity may reveal aspects of computer use that the user prefers to remain private. However, it is not always clear to a computer user exactly which 'private' artifacts are being created and stored and which can subsequently be viewed by others during normal computer usage [5]. Ordinarily, normative privacy [2] is achieved for computer displays by physically locating the display so that others cannot view it or relying on the social norms that preclude others from openly staring at information on a display within someone's 'personal zone' [4]. However, normative privacy is impossible during collaboration around a display, as we are inviting others to look at an area of the display and the display becomes a part of the collaboration. In this research, web browsers are used as the representative application. Web browsers are often used during collaboration to find information or share previously found sites and are typically used for information gathering and entertainment of a more personal nature. Web browsers offer 'convenience features' (histories, favorites, auto completion of URLs, etc.) that record past interactions for future reference. Currently, users must choose to either turn these features off or periodically clear the stored information if they want to maintain privacy either through the web browser tools or with commercial privacy software.

2 Survey of Web Browser Privacy Issues

We are conducting an on-line survey of 270 individuals exploring the privacy dimensions that arise during face-to-face collaboration or when computers are communally used. Participants are being recruited from business, the university community, and the public. Participants are grouped according to their primary setting of web browsing activity (home, school, work) and the type of computer used (laptop, single user computer, shared computer). We want to learn if there may be different levels of privacy desired depending on the user and how the context (their relationship to the viewer and the level of control the viewer has) of subsequent viewing of private information impacts privacy concerns. We will examine the influence of device mobility on privacy concerns and the actual settings in use for browser convenience features.

3   Privacy Gradient Diary Study

Lau et al. [1] state that privacy interfaces should make it easy to create, inspect, modify and monitor privacy policies and that the policies should be applied proactively to objects as they are encountered. We conducted a diary study to explore the issue of privacy gradients and whether or not we can capitalize upon patterns of actual web browsing to allow users to easily and effectively manage the privacy of web browsing artifacts. Obviously, privacy is a very complex issue with both privacy concerns and willingness to maintain a privacy management scheme varying on an individual basis. However, our hypothesis is that people may be willing to organize their information across a small number of privacy levels or gradients. We examined a 4-tier privacy gradient scheme (*public, semi-public, private, don't save*) to see if that level of granularity was appropriate and how people chose to categorize information across these gradients. We also explored normal web browsing activities to see if patterns exist that would make organization within privacy gradients easier. For example, do people use different browser windows for activities of different privacy types? Do they tend to have sequences of one type of activity or another? We recruited 20 participants from the general university community. Participants had to use a laptop for the majority of their browsing activity and periodically be in situations whereby others could view the traces of their previous browsing. Over the course of a week, we logged the actual sites visited by users, along with a time stamp and which browser window displayed the page. Daily, the user was presented with this information in an electronic diary application and asked to indicate how they would classify the privacy level of each web page if others were to view the history of this activity later using the privacy gradients:

- *public* (don't care who views the site)
- *semi-public* (may be private in some contexts of viewing)
- *private* (very few or possibly no one else should ever see)
- *don't save* (no need for anybody, including the user, to see it again).

After classification, the viewing history was sanitized so that only the time stamp, browser window, and privacy level was sent to the researchers. In addition, the users completed pre and post study questionnaires to tease out some additional information and see if the initial classifications changed after a week of consciously thinking about the privacy levels they were associating with the various web sites encountered

4   Results and Future Work

The privacy gradient diary study was completed this summer and the privacy survey is underway. Analysis of results to date will be presented at DCSI '04. These results will help guide the development of a privacy management system for ad hoc co-located collaboration.

References

[1] Lau, T., Etzioni, O., and Weld, D. S. (1999). Privacy Interfaces for Information Management. Communications of the ACM, 42(10): 89-94.

[2] Moor, J. H. (1997). Towards a Theory of Privacy in the Information Age. ACM SIGCAS Computers and Society, 27(3): 27-32.

[3] Palen, L. and Dourish, P. (2003). Unpacking "Privacy" for a Networked World. In Proceedings of CHI 2003, Ft. Lauderdale, FL. 129-136.

[4] Tan, D. S. and Czerwinski, M. (2003). Information Voyeurism: Social Impact of Physically Large Displays on Information Privacy. In Proceedings of CHI 2003, Ft. Lauderdale, FL. 748-749.

[5] Weisband, S. P. and Reinig, B. A. (1995). Managing User Perceptions of Email Privacy. Communications of the ACM, 38(12): 40-47.