Protecting the Privacy of Displayed Information

Peter Tarasewich, Jun Gong, Richard Conlan
HCI Laboratory, College of Computer & Information Science, Northeastern University
360 Huntington Avenue, 202 WVH, Boston, MA 02115

{tarase, gjoliver, kaige} @ccs.neu.edu

ABSTRACT

Current technologies allow users to access information in virtually any public setting. This creates situations where sensitive information, both organizational and personal in nature, can be seen and captured by nearby people and technology. Therefore, methods are necessary to ensure the privacy and security of information displayed in public spaces. The authors have developed Web browser privacy blinders, which hide sensitive information from view while leaving other information unobscured. Research to date on this topic is reviewed, along with current and future work

1. INTRODUCTION

Maintaining privacy in the mobile environment remains difficult because the context of a device or application can change rapidly and without notice. This is in sharp contrast to a fixed environment, like an office, where people can consistently control the way that information is handled to minimize the chance of divulging sensitive information to unauthorized parties. In an office, computer screens can be pointed towards a user such that other people cannot easily read them [1]. People are not intentionally careless when it comes to protecting information in public places, but normal human behavior makes it easy for unsafe conditions to exist. For example, laptop computers are often used whenever and wherever needed or desired (e.g., in a airplane). In this situation, the user can become more focused on the task at hand rather than the fact that information might be overseen or recorded by someone close by. While current technology makes it easy to access information anywhere and anytime, it does not concurrently provide adequate protection of that information. Effective solutions to privacy protection problems must not only be technically sound, but usable and understandable from a social perspective. Mobile users need interaction methods that work well with multiple and varied tasks, and in environments that can change rapidly and potentially be hostile. If this is not accomplished, users must accept tradeoffs between the pervasive availability of information and the potential loss of privacy and security [1].

While privacy is often maintained through methods (e.g., encryption) that keep data from being read by unauthorized parties, this research looks at the relatively unexplored but equally important problem of maintaining the privacy of displayed information. Our overall goal is to create technically sound but practical methods of maintaining privacy of sensitive information that is displayed in public and mobile environments. Any solution must be resilient enough to work in any context (i.e., location and task independent), and ultimately adapt to changing contexts.

2. BACKGROUND

Privacy is valued and expected by most people to varying degrees. Usually an individual expects reasonable access to personal information while restricting strangers' access to this same information. Privacy requirements will also vary based on the type of information, and on the preferences of the information's owner (e.g., individual or organization) [e.g., 2].

Several hardware-based solutions have been explored to solve the problem of maintaining information privacy on mobile displays. Privacy covers have been developed for laptop screens that provide a clear view of the screen's contents to the user but obscure the view to anyone looking at the screen from an angle. Contents of screens can also be blurred, readable only through devices such as special eyeglasses. While potentially valuable in protecting the privacy of information, these techniques may have potential drawbacks in terms of 1) additional cost; 2) additional weight, bulk, and power consumption; 3) increased complexity; and 4) distortion or degradation of the displayed information, which could affect performance.

Our ongoing research concerns the development and testing of *privacy blinders* and related techniques. Privacy blinders [4] mimic the use of yellow sticky-notes to cover parts of a larger document so that they are not viewable by others. Blinders can be used to provide a mixed display in which sensitive information is hidden (covered) but information not considered private is displayed normally. If the user decides to view the sensitive information, they can temporarily remove the blinder. For example, blinders on a tablet PC or PDA might be removed by touching them with a stylus. When the stylus is removed from the screen, the blinders reappear. It is also possible to create blinders that can only be removed with a certain gesture, thereby creating a level of security along with information privacy.

Furthermore, privacy blinders can automatically respond to a predefined organizational and/or personal "privacy policy," which specifies what types of information are covered under different circumstances. An organizational policy might be dictated by the company a person works for, while a personal policy is customized to a user's own comfort level and privacy requirements. This method can also account for user context changes; if a person moves to a less public space, they might turn off the blinder feature and view all information without obstruction. Context might also be taken into account automatically by the system. For example, a change in location from a private office to a public meeting room might modify privacy settings by design. This flexibility allows adaptation to the changing environment of the mobile device user.

3. BLINDERS TO HIDE INFORMATION

To date we have completed two pilot studies with privacy blinders. The first study [4] tested the basic concept of the blinders in terms of usability and effectiveness. We used a limited-function Mozilla Web browser prototype in a controlled laboratory study with each subject searching three "canned" banking Web sites for specific information. Privacy blinders were

displayed based on special HTML tags next to information that was defined to be sensitive in nature. The blinders were set to a predefined size, and appeared centered directly over sensitive information. The user could reveal information protected by a blinder in one of two predetermined ways. For one, the blinder disappeared when the stylus was moved over it. The blinder reappeared when the stylus moved away. In the second, the privacy blinder disappeared for a total of 10 seconds when a special stylus gesture was made, then reappeared.

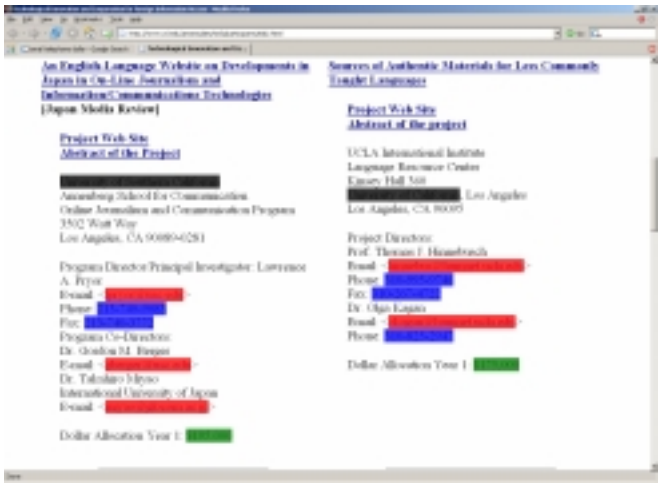

Figure 1. A random webpage with privacy blinders enabled.

In the second study [4], a FireFox Web browser extension with user-configurable privacy settings allowed users to browse personal information from any Web site. Unlike the software from the first study, this extension did not simply look for predefined HTML tags. It preprocessed any Web page, located user-defined sensitive information, placed user-customized blinders on top of the specified content, and presented the resulting "blinded" Web page to the user. Figure 1 shows a random Web page viewed with privacy blinders. Properties of the privacy blinders that could be user-configured included 1) whether to group blinders, 2) to use fixed or variable blinder sizes, and 3) setting the blinder opacity (transparency). Besides these blinder properties, the "privacy policy" could also be customized through an interface shown in Figure 2. Four classes of potentially sensitive content were supported. These were 1) monetary amounts (a number starting with "$" or containing two decimal points); 2) email addresses (abc@xyz.dom); 3) telephone numbers (e.g., xxx-xxx-xxxx); and 4) a user-specified delineated list of words and phrases that they wanted covered. All participants in this study responded positively to using the privacy blinders, and felt that privacy blinders would be useful on a PDA or mobile phone. Additional results of both studies can be found in [4].

4. CONTINUING WORK

While the original intent of the privacy blinders had been to protect sensitive personal and financial information from onlookers, there are many alternative uses that we had not originally envisioned, including parental filters, workplace privacy, highlighting, and color-coding of sensitive terms.

Work continues on examining different sizes and shapes of blinders, alternate ways of placing and removing blinders, and degrees of user customization One idea is rather than completely removing a blinder, it might be set to drop its opacity level, allowing the user to view the information through a translucent panel, but still discouraging onlookers who are at a distance from the screen. When this is done, the software can also be compared directly against hardware-based techniques for screen privacy. One implementation difficulty has been determining what content to cover. Currently the plug-in relies upon a simple matching paradigm to determine what to cover.

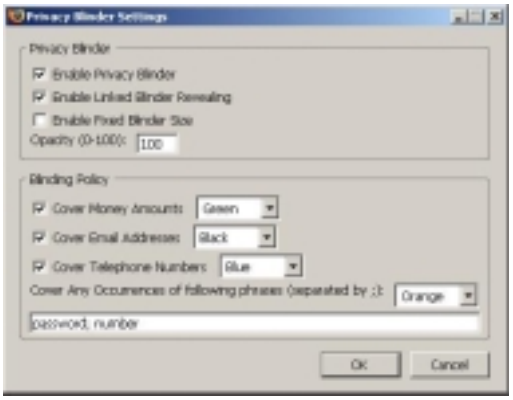

Figure 2. Configuration Dialog Box for Privacy Blinders.

Since our pilot studies, we have also modified the plug-in to cover graphics as well as text, and continue to add to its functionality and ability for user customization. Our long-term goal is to establish an interface that allows the easy definition of a personal "privacy policy" that can be used along with organizational privacy settings as required (see [3] for a good discussion of developing privacy rules).

We are planning to run longitudinal field tests where participants will be given a version of the software to run on their personal devices. The software will automatically track information about the privacy settings and how often blinders appear on various Web sites. The software will prompt the user for feedback after performing tasks with the browser. Versions of the privacy blinder software will also be created to run on PDA's and mobile phones.

Context data (such as location, co-location, and scheduled events) might also be used to automatically ensure that a user is interacting with a mobile system in the safest possible manner, and might increase privacy management effectiveness by shifting the burden of environmental awareness from user to system.

5. REFERENCES

1. Dourish, P., Grinter, R.E., Delgato de la Flor, J., and Joseph, M. Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem. *Personal and Ubiq. Computing*, 8, (2004), 391-401.
2. Hawkey, K. and Inkpen, K. M. Keeping Up Appearances: Understanding the Dimensions of Incidental Information Privacy. *Proc. of CHI 2006*, (2006), 821-830.
3. Karat, C.-M., Karat, J., Brodie, C., and Feng, J. Evaluating Interfaces for Privacy Policy Rule Authoring. *Proc. of CHI 2006*, (2006), 83-92.
4. Tarasewich, P., Gong, J., and Conlan, R. Protecting Private Data in Public, *Adjunct Proc. of CHI 2006*, (2006), 1409-1414.