Peripheral Privacy Notifications for Wireless Networks

Braden Kowitz
Carnegie Mellon University, HCII
5000 Forbes Ave.
Pittsburgh, PA
kowitz@cmu.edu

Lorrie Cranor
Carnegie Mellon University, ISRI
5000 Forbes Ave.
Pittsburg, PA
lorrie@cs.cmu.edu

ABSTRACT

This study aims to develop techniques for allowing users to form more accurate expectations of privacy. We have developed a peripheral display for notifying users when their computer leaks information into the public space. A two-week trial with eleven participants was conducted to measure the effects of the display.

1. MOTIVATION

1.1 Wireless Networks

Wireless networks are built on top of small radio transmitters and receivers. Because of this, messages sent over wireless networks are easily overheard by others computers nearby. In fact, a recent survey indicated that 21% of home users could access their neighbor's WiFi network from their own homes [4]. In the absence of encryption, private web searches, emails, and instant messages may all be at risk to public exposure.

1.2 Cryptography

At first glance, leaked information may appear to be a simple cryptography issue. But, in practice, the problem is much more intricate. For average users it can be difficult to accurately judge the level of security employed during common messaging tasks.

As an example, consider desktop email applications. For a user to understand the level of privacy she should expect on a wireless network, she must dig deep into the connection settings to see if SSL is enabled. Even if this process is understood, switching to a different medium, such as a web based email client, completely changes the process for determining the security level of the communication channel. Beyond the individual application, encryption on the wireless network itself may also change the level of security. Even within the relatively simple task of reading email, small details of how the task is performed can drastically change one's expected level of privacy.

In addition to all this, users may not have a meaningful choice between applications that offer encryption. However, even if strong cryptography were universally employed, there may still be a fundamental privacy problem at hand.

1.3 Privacy Preferences

In our networked world, computers are constantly broadcasting out information about us. For example, most web browsers send out the previous page visited with each new page request. Some users may not mind this policy, while others regard it as an invasion of their privacy.

Indeed, users report many reasons why they are concerned about privacy on the Internet. Even within identified groupings, individuals regard certain types of personal information as more or less private than others [2]. Because of this, it is difficult to specify what personal information should be presented about a user in differing contexts. Worse, since privacy is not an active consideration in most social situations, computer interfaces should not interrupt users with privacy prompts for each new context [1]. This is perhaps one reason why user information is often automatically disclosed instead of prompting the user for an appropriate action.

1.4 Goals

The aim of this project is to better inform users when personal information is being "leaked" into the public space. In some cases an unintended disclosure is made because an application does not support encryption. Other times, a disclosure may happen because a software program assumes privacy settings for a user. Many applications make these assumptions because providing a notification would be too intrusive to the task at hand. This project aims to deliver such notifications in a non-intrusive way. In some cases, the user may not care about a disclosure. In other situations, sensitive communication may need to be switched to a different medium, such as a telephone call or face to face meeting.

2. PERIPHERAL DISPLAY DESIGN

This project aims to present notifications to users when they may be inadvertently “leaking” information into the public sphere. We view these privacy notifications as peripheral information, which is not central to a user’s task, but can help a user to learn more, do a better job, or keep track of less important tasks [3].

2.1 Large Format

We have constructed a peripheral display to deliver targeted privacy notifications. The display is projected onto a large section of a wall in a public area. We have chosen this setup for a number of reasons. With a projected display, the privacy notifications become integrated into the environment, much like the wireless network itself. Another benefit is that using a projected display does not involve installing software on users’ computers.

Finally, there is some evidence that users may be better able to peripherally monitor large format displays. Given the same visual angle and size of retinal image, subjects have been found more likely to glance over and read words on a wall-sized display than a personal monitor. The intuition is that people regard walls as public spaces. If this is so, then there should be less social stigma attached to viewing information displayed on a wall [5].

2.2 Balancing Notification and Privacy

In order to generate privacy notifications, we capture traffic traveling on unencrypted wireless networks. A naive implementation of a notification display would be to show every captured message on the public display. For instance, one could display every instant message chat or web search along with the name of the sender. Each user would definitely identify the message as their own. But at the same time, displaying the entire message and sender would clearly create a privacy risk to the user.

To build a notification display that preserves privacy, we limit the amount of information displayed to a single word. This means that for each message received, only one word is selected to be displayed. Upon receiving a chat message or web search, the computer splits up the message into a set of words. Words that are not in an English dictionary are removed from the list. Some proper nouns and profane words are also removed from the list. Then, the longest of the remaining words (if any) is chosen for display. The sender of the message is not shown on the display.

This technique provides privacy to the user. To most observers, words will appear on the screen as if by random. But if a particular user has just sent a message, she may notice a recently used word on the display. Eliminating the sender, receiver, and conversational context will hopefully preserve good characteristics of the information, such as recognition by the user, while preventing unwanted disclosure.

We take two additional steps to help the user identify the word as their own. First, a word appears on the screen immediately after a message is sent. So if a user performs a web search, a word from that search may be displayed even before the results are returned. This creates an effect of temporal causality. The second technique is to display words with a style and color unique to each user. This does not identify the source of a message. But, users should be able to better identify words that originated from their computer when presented in a consistent manner.

We believe that this display provides utility to the user while mitigating possible privacy risks. By paying attention to these notifications, users may be able to generalize and deduce which common tasks “leak” information onto the local network. Our current prototype display produces notifications for outgoing AOL Instant Messenger chats and web searches with Google, Yahoo, and AOL.

3. EXPERIMENTAL TRIAL

3.1 Protocol

We tested the peripheral display described above with a small group of participants who work in a shared space. Eleven out of approximately 24 people in the space volunteered to take part in the study. We found from an initial survey that nearly all participants were frequent users of web browsers, chat clients, and wireless networks. Six of the subjects used AOL Instant messenger, the IM protocol detected by the display.

The display was installed in the participant’s workplace for a period of two weeks and captured network messages only from users who volunteered for the study. During the first week, the display did not present privacy notifications: every time a word would normally be shown, a random word was selected instead and displayed a few minutes later. The purpose of this procedure is to adjust users to the presence of the display without actually providing privacy notifications. During the second week, the display began to show privacy notifications as described in the previous section.

Surveys were administered before the display was installed, at the end of the first week, and after the display was removed. All surveys measured users comfort level with "discussing private matters" over a number of locations and communication medium. In addition, the display recorded the time and date for each leaked messages.

3.2 Results

We were unable to detect any significant change in participant's comfort level in discussing private matters over wireless networks, instant messages, or searching the web for private information. We expected to see a small drop in network usage if people felt less private on the network, but we did not see any significant drop in instant message or web search usage.

We did, however, receive some interesting comments on the open-ended portions of the surveys. Three of the eleven participants correctly indicated that the words were coming from instant messages or web searches. In addition, several participants noted a change in their expectations of privacy:

- *“I DID become much more self conscious of what I was writing when chatting with friends even though I didn't feel I was chatting about anything private.”*
- *“[Instant Messaging] felt less private. It wasn't that anyone could get any context from the words, but it did make me feel less ‘secretive’. ”*

4. NEXT STEPS

Due to the feedback on the surveys, we would like to pursue this technique further. In the future, it may be possible to test the peripheral display with a large number of users in a public space. To measure results more accurately, we would like to present users with tools, such as VPNs, to help secure their messages. The proportion of users adopting such security tools may be a good indicator that the display affects users' expectations of privacy.

5. ACKNOWLEDGEMENTS

Special thanks to Lorrie Cranor for her extensive guidance in developing this work and the related experimental trial. Also, thanks to Rob Reeder, Dawn Dowling, Charles Bartel, Mary Ann Blair, and all of the MHCI students who helped with this project.

6. REFERENCES

[1] Cranor, Lorrie and Mark Ackerman. “Privacy Critics: UI Components to Safeguard Users’ Privacy”. *Conf. Human Factors in Computing Systems* CHI’99 2 (1999): 258-259.

[2] Cranor, Lorrie, Joseph Reagle, and Mark S. Ackerman. *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*. 14 Apr. 1999. AT&T Labs-Research. 23 Sept. 2004.

[3] Maglio, Paul, and Christopher Campbell. “Tradeoffs in Displaying Peripheral Information”. *Proceedings of ACM CHI 2000 Human Factors in Computing Systems*. (2000): 241-248.

[4] Metz, Cade. "The Trouble With Wireless" *PC Magazine* 19 Apr. 2004.

[5] Tan, Desney, and Mary Czerwinski. “Information voyeurism: social impact of physically large displays on information privacy”. *Extended abstracts on Human factors in computing systems.* (2003): 748-749