

UNDERGRADUATE THESIS PROJECT PRE-PROPOSAL
School of Engineering and Applied Science
University of Virginia

Developing a More Meaningful Privacy
Interface Using the Mozilla Web Browser

Submitted by

Jennifer Kahng

Computer Science

TCC 401

Section 4 (11 am)

September 25, 2000

TCC Advisor: Rosanne Welker

Technical Advisor: David Evans

On my honor as a University student, on this assignment I have neither given nor received unauthorized aid as defined by the Honor Guidelines for Papers in TCC Courses.

Signed _____

Developing a More Meaningful Privacy Interface Using the Mozilla Web Browser

Background Information

Since its introduction, the World Wide Web has rapidly expanded into a global community spanning much of the Internet. Today users, also known as "surfers," can search for information, communicate with people and purchase just about anything through the Web. User specific information is required and this is where users are at the most risk. Web browsers have configurable security and privacy capabilities to help make web surfing more secure, however these features often go unused. Files called "cookies" store where surfers go and, if they filled out forms containing personal information, that information is also stored.[2] Controls such as ActiveX, Java, JavaScript and CGI also have the potential to compromise a surfer's privacy. Although those controls were created to help web sites cater to users, they can also be used maliciously to send information from surfer to server without the knowledge of the surfer. Vulnerabilities in the controls themselves can also be exploited, resulting in file theft or information gathering that the surfer did not authorize.[1]

The two most prolific web browsers, Netscape Navigator and Microsoft Internet Explorer, have the capability of disabling or notifying the surfer of a cookie or ActiveX control, but have sparse or confusing explanations for why they may be security hazards. Other security settings are presented in a similar manner.

Internet Explorer uses the words "Low," "Medium-low," "Medium" and "High" as different levels of browser security. Text such as "Appropriate for most Internet sites"

accompanies the level names. There is also the option of creating a custom level of security, where the user can delve into the specifics of whether or not to allow cookies or ActiveX controls or other scripts, but without any detail of those components. Netscape Navigator has two areas for security settings. The most obvious is the "Preferences" screen, where users can tell Netscape what they do and do not want to see. The extent of the "Preferences" security settings covers cookies and JavaScript. The "Security Info" menu contains more features, but again, lacks detail. Both of these web browsers install with preset security settings deemed reasonable enough for the average user. For the most part, users trust the companies who make their web browsers and believe that the default settings are adequate for their needs.

Research Objective

The lack of detail for security and privacy settings in web browsers often confuses and frustrates users. Generic messages pop up when the surfer visits a web site with secure content, or when the surfer visits between secure and non-secure web sites. The warnings all look the same and eventually, the surfer stops reading them, automatically pressing the "Ok" button and even disabling all future messages, regardless of if the threat to their privacy is real. The mechanisms to keep user information private may be correct, but it means nothing if the user does not know how to configure the settings properly. What if there were ways to inform the user, in understandable terms, why their web activities were unsafe and what they could do to keep their personal information private? By researching why current web browser privacy settings are not effective, I will design an interface which controls the Mozilla browser's privacy features, offering more meaningful descriptions and options for users.

Methods

There are several preliminary steps need to finish before any design and implementation can begin. First and foremost is research into why current privacy features are so ineffective. One way to accomplish this may be to observe a group of people web browsing, particularly to sites which would generate security warnings, and then afterwards, ask them why they behaved the way they did. It would be best to do this type of experiment in a controlled environment where the surfer is unaware of why they are being studied. This information should be evaluated to determine alternative presentation methods. Another window message would not be logical, as users tend to dismiss them without thought.

Another step is determining what others tried doing to get around the issue of unusable user interfaces. Studies of current security software interfaces reveal that while the user may really want to use the software, its poor design prevents them from using it effectively. In many cases, because users believe they have configured the software correctly, they actually end up doing more harm than good because of a misunderstanding of the functionality.[3] Other sources for similar topics include the IEEE Security and Privacy Conferences as well as the ACM's Special Interest Group on Computers and Society, both of which cover the topic of privacy on the Internet. The ACM's Special Interest Group on Computer-Human Interaction conference proceedings and other published papers will also be helpful in designing an interface that will actually be useful. Additionally, since Mozilla itself is an open project, the development web site and associated newsgroups provide ample sources of information and contacts for various aspects of the browser.

After I develop a design, it should be implemented and tested. The Mozilla web browser is an ideal candidate for implementation, as its source code is freely available. Mozilla is written in C++, a language I have spent the last three years learning and using, so I am comfortable and competent with the syntax and methods. I also started a correspondence with personnel at Netscape who are working on the security aspects of Mozilla. They may be able to help me implement my design and they are very interested since the interface is a problem they are aware of and are eager to try and solve. Testing will also be difficult since it relies, again, on users and how they react. It would at least be nice to know if they noticed a difference in what was presented.

Throughout the duration of my thesis project, I will correspond with Rosanne Welker in the TCC department for help and guidance. She may be able to offer suggestions for my project if I get stuck or act as a sounding board if I have multiple avenues that I could pursue. I will also work with David Evans, an Assistant Professor in the Computer Science Department. He is teaching a course on Security and Privacy on the Internet this semester that I am taking. Information gleaned from that course as well as Professor Evans' own insight and knowledge should also help my thesis project.

Impact Statement

The resources I have available should enable me to develop a design and implement an improved privacy interface in the Mozilla web browser. Once completed, the application will help users protect themselves better while using the Web. Presenting the user with meaningful information with regard to their web activities serves two purposes. Not only are they protecting

their personal information from malicious parties, but they are also gaining more knowledge with what goes on when they browse. The more surfers understand the environment they are in, the more likely they are to take action when someone or something tries to harm them.

Works Cited

1. Fisch, Eric A., and Gregory B. White. Secure Computers and Networks: Analysis, Design, and Implementation. New York: CRC Press. 2000.
2. Oppliger, Rolf. Security Technologies for the World Wide Web. Boston: Artech House. 2000
3. Whitten, Alma, and J. D. Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." Proceedings of the 8th USENIX Security Symposium, August 1999. 12 Sept. 2000. <<http://www.cs.cmu.edu/~alma/johnny.pdf>>