

An Evaluation of New Browser Indicators for Extended Validation Certificates

by

Jennifer Sobey

A thesis submitted to the
Faculty of Graduate Studies and Research
in partial fulfilment of the
requirements for the degree of
Master of Computer Science

Ottawa-Carleton Institute for Computer Science
School of Computer Science
Carleton University
Ottawa, Ontario, Canada

September 2008

©Copyright

Jennifer Sobey, 2008

Abstract

The ability of a user to reliably determine the true identity of a web site is important to online security. However, users often have trouble interpreting browser security cues that are intended to help them with this decision. With the introduction of Extended Validation SSL certificates in Internet Explorer 7.0, web browsers are including new indicators to convey information about different types of certificates.

We carried out a user study which compared a proposed new interface in the Mozilla Firefox 3.0 browser with an alternative interface of our own design to investigate how users react to these new indicators. The unmodified Firefox 3.0 browser interface buttonized an existing region of the browser chrome to the left of the URL bar that produced an identity information box when clicked. Our modified version of this same browser inserted a new *identity confidence* button that conveyed some visual identity information, intended to better draw the user's attention.

Our study included eye tracking data which provided empirical evidence with respect to which parts of the browser interface users tended to look at during the study and which areas went unnoticed. Our results show that, while the new interface features in the unmodified Firefox browser went unnoticed by all users in our study, the modified design was noticed by over half of the participants, and most users show a willingness to adopt these features once made aware of their functionality. However, until users are more educated about these types of identity indicators, Extended Validation SSL certificates may have little effect on online security.

Acknowledgements

Many thanks to Dr. Paul van Oorschot and Dr. Andrew Patrick for their extremely helpful guidance, insight, and feedback on my research. I also thank Dr. Robert Biddle for his many discussions and input regarding the user study and for providing access to the HOTLab's eye-tracking hardware and software for use in the user study.

I thank Johnathan Nightingale at Mozilla for his discussions and technical advice regarding the Firefox 3.0 Beta, as well as Tim Moses at Entrust for his background and insight on Extended Validation SSL certificates. I also thank Rachna Dhamija for her helpful input on web browser standards and user studies.

I would like to thank all of the members of Carleton's Digital Security Group for their feedback on my research, especially Sonia Chiasson and Alain Forget, who helped a great deal with various aspects of the user study. I also thank my thesis examination committee for their valuable feedback and suggestions.

Finally, I would like to thank my family and friends for their support and understanding throughout this process.

Contents

Abstract	ii
Acknowledgements	iii
List of Tables	viii
List of Figures	ix
1 Introduction	1
1.1 Problem Statement	2
1.2 Motivation	3
1.3 Solution Overview	3
1.4 Contributions	4
1.5 Thesis Outline	5
2 Background	6
2.1 Web Browser Security Indicators	6
2.2 Extended Validation Certificates	8
2.3 Consumer Confidence in E-Commerce	9

2.4	Mozilla Firefox 3.0 Beta 1	10
3	Related Work	12
3.1	Phishing Prevention	12
3.1.1	Toolbars	13
3.1.2	Trusted Paths	14
3.1.3	Educating Users	16
3.1.4	Automated Prevention	17
3.2	Web Browser Security Indicators	20
3.2.1	The https Indicator	21
3.2.2	The Lock Icon	21
3.2.3	Extended Validation Indicators	22
3.3	Browser Spoofing	23
3.4	Eye Tracking in User Studies	25
4	User Study Methodology	26
4.1	Design and Implementation	26
4.1.1	Browser Interfaces	27
4.1.1.1	FF3: Firefox 3.0 Beta 1	28
4.1.1.2	FF3mod: Modified Firefox 3.0 Beta 1	28
4.1.1.3	FF2: Firefox 2.0 Control	31
4.1.2	Other Technical Details	31
4.2	Participants	33
4.3	Tasks	34

5	User Study Results	38
5.1	Self-Reported Attention to the Identity	
	Indicators	38
5.2	Objective Measures of Attention to Identity Indicators	41
5.3	Willingness to Transact	42
5.4	Time Spent Gazing at Browser Chrome	52
5.5	Decision Strategies	54
6	Discussion	57
6.1	EV Indicators	57
6.2	Attention to Browser Chrome	59
6.3	Design Implications	60
6.4	Limitations of Study	61
6.5	Current State of EV Support	62
7	Conclusions	65
7.1	Future Work in This Area	65
7.2	Concluding Remarks	66
	Bibliography	68
	Appendix A - Firefox 3.0 Beta 1 Identity Information Boxes	76
	Appendix B - Web Site Screenshots	77
	Appendix C - User Study Documents	83

Appendix D - Source Code Changes to Firefox 3.0 Beta 1	100
Appendix E - Willingness to Transact Data	105

List of Tables

4.1	Participant Demographics	35
5.1	Number and percentage of participants who noticed each identity indicator.	39
5.2	Number and percentage of participants who preferred each browser.	41
5.3	Interface means and standard deviations of willingness to transact ratings	44
5.4	Differences in means of willingness to transact ratings between interfaces	45
5.5	State means and standard deviations of willingness to transact ratings	47
5.6	Differences in mean willingness to transact ratings between states	47
5.7	State means and standard deviations of willingness to transact ratings of gazers vs. non-gazers	48
5.8	Differences in mean willingness to transact between states for gazers	48
5.9	Percentage of participants who reported using various factors in their decision making during the study and in general.	55

List of Figures

2.1	Internet Explorer 7.0's green URL bar for Extended Validation SSL certificates.	9
4.1	Identity indicators used in FF3 (Firefox 3 Beta 1) and FF3mod (Modified Firefox 3 Beta 1).	27
4.2	The <i>identity confidence</i> button in its three different states.	29
5.1	A screenshot of the eye tracker replay function. The large circle near the <i>identity confidence</i> indicator shows the participant's fixation on that region.	42
5.2	Boxplot of participants' mean <i>willingness to transact</i> ratings based on SSL state, grouped by gazer or non-gazer.	50
5.3	Notched boxplot of participants' mean <i>willingness to transact</i> ratings based on SSL state, grouped by gazer or non-gazer.	50
5.4	Boxplot of participants' mean <i>willingness to transact</i> ratings based on Browser and SSL state, grouped by gazer or non-gazer.	51
5.5	Notched boxplot of participants' mean <i>willingness to transact</i> ratings based on Browser and SSL state, grouped by gazer or non-gazer.	51

5.6	Plot of the frequency distribution of time spent gazing at chrome for all participants.	53
5.7	Plot of the frequency distribution of time spent gazing at chrome for gazers and non-gazers.	54

Chapter 1

Introduction

The ability of a user to reliably determine the true identity of a web site is important to online security. With the prevalence of phishing attacks, in which users are lured to fraudulent web sites, it is becoming increasingly important to provide users with effective tools to properly identify the true identity of a site. Secure Sockets Layer(SSL) is a protocol commonly used in validating the identity of a website and enabling the transmission of private information over the Internet. It makes use of cryptographic keys to encrypt the data being transmitted and to provide a signature used in identification. Browser SSL certificates are electronic documents that enable encryption on secure web sites, and also contain information about the certificate holder. The use of these certificates (and the related well-known SSL lock icon) has traditionally been one way of providing identity information to the user, but studies have shown that many users have difficulty interpreting certificates or may not even be aware that they exist [7, 8]. For further explanation of the SSL protocol, see the Background section in Chapter 2.

With the introduction of Extended Validation (EV) SSL certificates [3], web browser software vendors are facing the design challenge of integrating support for these new certificates into their interfaces in a way that will be accepted and understood by users. Microsoft's Internet Explorer 7.0 was the first to introduce new interface features for Extended Validation which included a green background in the URL bar [14]. However, a preliminary study showed that these new visual cues did not make a notable difference in user behaviour [22]. Other leading web browser vendors are currently working on plans to integrate support for Extended Validation in future releases [3]. Additional background on EV SSL certificates is provided in Chapter 2.

1.1 Problem Statement

After discussions with Mozilla developers [37], it was decided to study the identity indicator being introduced in Mozilla's Firefox 3.0 browser. This interface included a small clickable area to the left of the web site's address that produced a pop-up box displaying information about the site certificate. The information displayed in the pop-up box indicated whether the site has an EV SSL certificate, a traditional SSL certificate, or no certificate. The open question to evaluate was whether this interface would be effective in conveying identity information to the user and whether improvements could be made to make the indicator more effective.

1.2 Motivation

In March, 2008, the Anti-Phishing Working Group [1] released their Phishing Activity Trends report for the month of December, 2007 indicating that, while the total number of phishing attacks reported in December decreased by approximately 2300 from the previous month (from 28,074 to 25,683), there had been an increase from 23,630 to 25,328 in the total number of unique phishing web sites. They also reported an increase in phishing attacks targeting non-traditional sites such as automotive associations. As more web sites become potential targets for such attacks, it becomes increasingly important to provide web site owners with some form of protection.

Extended Validation SSL certificates are intended to provide organizations with a means of better identifying themselves to their users. The concept of Extended Validation is still relatively new, but is gaining more exposure as many large companies have already invested in purchasing these new certificates. As of April, 2008, Verisign reported the existence of over 3,500 domains live with Verisign EV SSL certificates [47]. Despite the growing popularity of these new certificates, there has been little scientific study of how users will react to the additional identity information provided in web browsers and whether or not this information is being effectively conveyed.

1.3 Solution Overview

This thesis evaluates two different versions of the Firefox identity indicator – the version introduced in the Beta 1 release of Firefox 3.0 (circa January, 2008) and a modified version of this indicator we designed, intended to better draw the user’s

attention [45]. In a lab study, users interacted with both interfaces by performing tasks that required visiting an e-commerce web site and searching for several items they might purchase. Results were gathered by observation, questionnaire data, and by the use of an eye tracking device.

1.4 Contributions

The evaluation that was carried out resulted in several important contributions and findings with respect to new identity indicators for Extended Validation SSL certificates.

Main research contributions include:

- The design of a new identity indicator for the Firefox browser that could potentially be used to display information about web site certificate information. While the study found that the indicators in the unmodified Firefox beta went unnoticed by all users, our design improved upon this by drawing the attention of more than half of the study participants.
- The user study described in this thesis, to our knowledge, provides the first formal evaluation of the new identity indicators to be introduced in Firefox 3.0, aside from any user testing done by Mozilla. We are not aware of any published results from Mozilla.

Other work contributions include:

- A thorough review of related literature on web browser security, including phishing, browser spoofing, and the use of eye tracking to evaluate user interfaces.

- Eye-tracking data provided empirical evidence with respect to the amount of time users spend gazing at web browser chrome in comparison to gazing at web page content. We found that the majority of the participants' time was spent gazing at content, and that some participants spent as little as 1% of their time gazing at chrome. The eye-tracking data was also used to cross-validate several aspects of the study, such as user-reported events. This does not appear to be a common practice in usable security studies to date, except by Whalen and Inkpen [49].

1.5 Thesis Outline

The remainder of the thesis is organized as follows. *Chapter 2* provides a brief background on existing security indicators in web browsers, Extended Validation SSL certificates, and the Mozilla Firefox 3.0 Beta 1 browser used in the study. *Chapter 3* summarizes related work in the area of web browser security, including phishing, browser spoofing, and the use of eye tracking to evaluate user interfaces. *Chapter 4* describes the user study methodology, including the design and implementation involved, information regarding the participants, and the tasks they were asked to perform. *Chapter 5* presents the results obtained from the study with regard to user attention to identity indicators, their interpretations of these indicators, and other factors used in decision making about trustworthy web sites. *Chapter 6* provides a further discussion of these results, the potential limitations of the study, and the changes in Extended Validation support since the study was conducted. *Chapter 7* contains concluding remarks and suggestions for future work in this area.

Chapter 2

Background

2.1 Web Browser Security Indicators

The most common use of the *Secure Sockets Layer (SSL) protocol* is server-side authentication, in which the server obtains a key pair and an SSL certificate from a trusted third-party. When a secure connection is required between a user's web browser and the web server of the site they are visiting, the browser requests and evaluates the server's certificate, and if acceptable (based on the configuration of the browser), the SSL connection is established. This enables the encryption of information flowing between the browser and the web server to protect against eavesdropping. During this SSL session, the browser must also convey information in the user interface to indicate a secure connection [15, 56].

All of the major web browsers make use of two different indicators for SSL sessions – the character string *https* before the web site's domain name in the URL address bar, and a lock icon somewhere in the browser chrome (the frame of the browser

that includes menus, toolbars, scroll bars, and status bars). In Internet Explorer 7.0, Firefox 2.0, and Opera 9.27, this lock icon is located within the address bar, to the right of the web site's URL [31, 33, 40]. In Apple Safari 3.1.1, the lock is in the top right corner beside the minimize button [2], while in KDE Konqueror 2.5.8, it appears in the toolbar above the URL bar [23]. Clicking on the lock icon will provide a pop-up information box containing certificate information for the web site, in order to help users form an opinion about whether or not they are transacting with the correct entity.

One of SSL's major weaknesses is the ease with which a traditional SSL certificate can be obtained. Certification Authorities such as Verisign [48] and Entrust [12] charge upwards of \$100 and conduct some degree of cross-checking to ensure that the person requesting such a certificate has the authority to do so for a given domain. However, there do exist companies that will issue an SSL certificate for a much lower cost and for which the only requirement to obtain the certificate is to have the ability to reply from an email address on the domain in question. Alternatively, with open source software such as OpenSSL [39], users are able to create their own self-signed certificates which will still invoke the *https* and lock icon indicators but may produce warnings in certain web browsers. Since it is not difficult for attackers to obtain traditional SSL certificates for their malicious web sites, the identity-based features of these certificates are not necessarily sufficient means with which to instill trust in a web site.

2.2 Extended Validation Certificates

The guidelines for Extended Validation (EV) SSL certificates were established by the CA/Browser Forum [3], a voluntary organization consisting of Certification Authorities (CAs) and Internet browser software vendors. These certificates build on the existing technology of the SSL certificate format but involve a more strictly defined and more demanding certificate issuance process. They were introduced with two primary purposes in mind: (1) to provide users with greater confidence regarding the identity of the organization that controls the web site they are visiting; and (2) to facilitate the exchange of encryption keys between the web site and the user's web browser in the same way as done in traditional SSL certificates.

A rigorous authentication process conducted by the EV Certification Authority is intended to allow visitors to a web site having one of these EV SSL certificates to have greater confidence in the site's identity. This vetting process is designed to ensure that EV SSL certificates are only issued to private organizations, government entities, or business entities that have a physical location and business presence and that are not listed on any government prohibited list or denial list, among other criteria. The certificates themselves have five required fields: organization name, domain name, jurisdiction of incorporation, registration number, and address of place of business. One benefit of collecting all of this information may be to make it more difficult to mount phishing attacks using SSL certificates; companies can more reliably identify themselves to users of their web sites, and presumably law enforcement can more easily contact certificate holders in cases of reported phishing attacks [3, 12, 48]. Whether these certificates truly provide any defense against phishing remains an open question,

relying on several factors including a suitable user interface for conveying trustworthy information to users.

In order to support EV SSL certificates, browser developers must make modifications to both the user interface as well as the backend portion of the browser that deals with certificate validation and managing root certificates. As of May 2008, Microsoft's Internet Explorer 7.0 is the only browser to offer support for the EV SSL certificate in production software. When a user visits a web site having an EV certificate, the background of the browser's URL bar turns green and information regarding the web site owner and the issuing CA is displayed beside the padlock icon to the right of the address (see Figure 2.1) [30]. If a user single-clicks on this area of the URL bar, an information box is displayed to provide the user with additional certificate information. Mozilla Corporation, KDE, and Opera Software ASA are also members of the CA/Browser Forum and intend to provide EV certificate support in future releases of their software [3, 23, 32, 40].

2.3 Consumer Confidence in E-Commerce

While one of the secondary purposes of EV SSL certificates is to help prevent phishing attacks from occurring, the main purpose of an EV SSL certificate is to instill

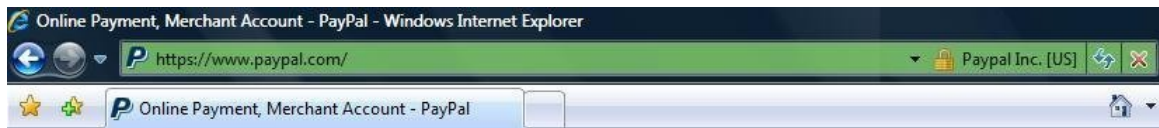


Figure 2.1: Internet Explorer 7.0's green URL bar for Extended Validation SSL certificates.

confidence in users concerning the identity of a web site [3]. A recent study by Accenture [6] determined that many online banking users are aware that they play a role in their own online security, but they often do not practice the necessary security precautions and hold their financial institutions responsible in the event of a security breach. They also found that many users felt they would leave their institution for another if such a breach occurred. This highlights the importance of banks and other e-commerce web sites gaining the confidence of their users. Verisign [48] asserts that the visual display for EV SSL certificates in web browsers will build user trust in e-commerce web sites and increase consumer confidence.

2.4 Mozilla Firefox 3.0 Beta 1

At the time of implementation of our user study (circa January, 2008), the current test version of Mozilla's next generation Firefox browser was Firefox 3.0 Beta 1. With the introduction of EV SSL certificates, Mozilla Developers [37] were looking to find better ways of separating security and identity information. They felt that the lock icon incorrectly conveyed a metaphor for security, when in fact, the certificate information provided by clicking on the lock icon was more related to identity information. For this reason, they removed the lock icon from the URL address bar but left it in the bottom right of the status bar for users who have grown accustomed to using it. The intention at the time was to potentially phase out the use of the lock icon gradually. To replace the lock in the URL bar, they modified the area of the chrome

in which the web site's favicon¹ appears, if one exists, so that this region acted as a button. In cases where a favicon does not exist, a default icon that looks like a piece of paper with the corner of the page turned down is displayed here. Clicking on the favicon or surrounding region brought up a pop-up information box containing identity information about the web site, based on SSL certificate information. Since this new identity indicator did not provide warnings for potentially harmful web sites, a phishing filter was also built into the browser that prevented users from proceeding to web sites that were found on known black lists [34, 37].

¹A favicon, which is also known as web site icon or page icon, is an image designated by the web site designer to be associated with that particular web site. It is typically displayed to the left of the URL bar, beside the web site's address.

Chapter 3

Related Work

3.1 Phishing Prevention

A phishing attack is an attack in which users are fooled into disclosing personal information such as credit card numbers or passwords by means of a fraudulent email or web site. Typically, an email is sent to the user that is intended to direct them to a fraudulent web site; this is often done with the use of a link to the page in the email itself. Often the fraudulent web site will appear very similar, if not almost identical, to a site the user is familiar with and therefore tricks the user into thinking it is safe to provide the sensitive information the site is soliciting.

This type of attack takes advantage of human interpretation of security information, rather than exploiting system vulnerabilities, and relies on the fact that users will often mistake these fraudulent emails or web sites for legitimate ones based on cues that can easily be spoofed [44]. The prevalence of phishing attacks emphasizes the important of designing security cues that are reliably understood and correctly

interpreted by users but that are not easily imitated by attackers.

3.1.1 Toolbars

There have been many proposals for phishing prevention tools that place toolbars in the browser to help users detect attacks. Wu et al. [53] divided existing toolbars into three types, based on the information they provide to the users. The first type, neutral information toolbars, display information such as domain name, host country, and registration date. SpoofStick [5] and Netcraft Toolbar [36] are examples of such a toolbar, and rely on the user to interpret this information correctly in order to make judgments about the web sites they are visiting. The second type of toolbar is the SSL-verification type, in which web sites that use SSL are differentiated from those that do not, and is intended to make users suspicious when non-SSL sites ask for sensitive information. Trustbar [21] is one such example that extracts information from the web site's certificate and displays the web site hostname and CA, with logos if available. For non-SSL web sites, general warnings are displayed. The third type of toolbar allows the system to make decisions about potential phishing attacks and is seen in tools such as SpoofGuard [4]. This toolbar employs a traffic light metaphor in which an indicator changes from green to yellow to red, depending on the web site the user visits. It may be easier for a user to interpret this type of signal but requires trust in the tool itself.

Wu et al. [53] conducted a study to test these three types of toolbars and concluded that all types fail to protect users from more sophisticated attacks, mainly because users do not reliably pay attention to the toolbar indicators or do not interpret them

correctly. In order to address this issue, they developed the Web Wallet [54] which places a sidebar into the web browser beside the page content, and is intended to be a trusted area for entry of sensitive information. If the tool determines that the web site may not be legitimate, it probes the user for their intended web site and displays a list of sites from which they must choose. One main goal was to incorporate the tool into the user's work flow so that it cannot go unnoticed, but there were several remaining weaknesses. The tool still relied on the user to make a decision about the web site they intended to visit; this could lead the user to an incorrect web site. There were also several attacks that succeeded against users in their study, including a spoof of the web wallet itself that successfully convinced users they were behaving securely by using the fake wallet.

3.1.2 Trusted Paths

Many anti-phishing solutions are centered around the concept of providing users with some trusted component that users can identify as being legitimate and that is very difficult for attackers to spoof. Dhamija and Tygar [7] proposed Dynamic Security Skins, which makes use of individualized photographic images that are displayed to the user by the web server when entering sensitive information. The user is able to verify that the correct image is being displayed and, because the image is unique to the individual, it is much more difficult for an attacker to display the correct image when trying to collect information in an untrusted form. However, they acknowledge that attacks on this scheme are still possible, as users may not reliably use the trusted password window or may not correctly identify their personal image. No formal

user testing was done on this system, as the implementation of the proposal was incomplete.

Ye et al. [56] introduced a synchronized random dynamic (SRD) boundary proposal in which borders are placed around web sites that contain colors based on security information. All browser windows are synchronized to have the same border color that changes at random time intervals, and a trusted reference window is intended to allow the user to identify the correct color at a given time. Attacks on this scheme are more difficult because the attacker cannot reliably predict the color that should appear on a window's border at any given time. Their user study claimed that trusted windows were correctly identified 80% of the time and untrusted windows were correctly identified 87%, which shows promise for these types of techniques.

Parno et al. [41] proposed making use of a trusted device to perform mutual authentication with a server, rather than relying on the user interface of web browsers to provide the security. In their proposal, a trusted device such as a cell phone or Personal Digital Assistant (PDA) acts as a second authenticator in addition to the user's password and also authenticates the server in the process. Because the device communicates directly with the web server, the user does not need to rely on security cues in the web browser to determine if the session is secure. While this eliminates the possibility of being fooled by browser spoofing attacks, it introduces other vulnerabilities such as theft of the trusted device or malware on the device that could lead to the system being compromised. A similar approach building on this work was proposed by Mannan et al. [27], but also aims to defend against session hijacking attacks.

3.1.3 Educating Users

Because many phishing prevention strategies rely on users to recognize potential threats, there are recurring proposals related to various ways to educate users. Kumaraguru et al. [25] designed an embedded training email system which periodically sent fake phishing emails to its users. If the user clicked on the link in the email, the system would display a warning designed to educate them about the dangers of phishing. These warnings could be in the form of typical security warnings, text and graphic warnings, or comic strips, depending on the group to which the participant was assigned. The results of their study showed that the comic strip approach was the most effective technique since users tend to dismiss windows with a lot of text, and this approach helped to prevent 70% of the users in this group to fall for the final phishing attack in the study.

Sheng et al. [44] created an online game in order to educate users about ways to avoid phishing attacks. Throughout a 15 minute session, users are taught how to identify phishing URLs, where to look for security cues in web browsers, and how to use search engines to locate legitimate web sites. Participants in their study were divided into three groups in order to compare people who used the game against people who were trained using existing materials and a tutorial. They found that users of their game performed notably better overall in correctly identifying web sites. However, these users were more likely to fall for attacks in which the address bar was spoofed, since the game emphasizes parsing the URL but not looking to other cues.

Both studies showed that these types of educational tools may be effective in

helping users gain knowledge about phishing. However, as Göring [18] points out, a general rule in Human-Computer Interaction seems to be that user education is not always the solution. This is especially true in computer security since behaving securely is not the user's primary task. Even if designers can convince users to be educated on a new security feature, which seems like a difficult task in itself when so many such features exist, another challenge lies in convincing them to behave as educated users.

3.1.4 Automated Prevention

Many studies [8, 9, 22, 53] have found that users are likely to fall for some phishing attacks no matter how much education they receive. This supports the idea that automated tools to detect phishing without user intervention may be more effective. Liu et al. [26] propose a solution that makes use of visual characteristics of web sites to identify potential phishing sites. Their solution consists of two phases. In the first phase, incoming and outgoing messages are monitored on mail servers to detect keywords and suspicious URLs that may indicate phishing. In the second phase, their system compares the potential phishing web page against the legitimate page for visual similarities. The system analyzes the overall layout of the page spacing, the colors, fonts, and content. It also divides the pages into blocks and compares blocks for similarity between the two pages. If the system finds that the pages are notably similar, based on a set threshold value, it will report a phishing attack. Their experiments showed that, by setting the correct parameters, the system can successfully detect most phishing attacks. But this also comes at the expense of

causing more false positives in which legitimate web sites are classified as phishing web sites. Since all attack warnings are handled by human administrators, this increases the work involved in managing the system. They must also ensure that attackers cannot compromise their system so that users can reliably trust that it is working properly.

Zhang et al. [57] developed a phishing detection approach called CANTINA that is based on analysis of a web page's content. They based this approach on the assumptions that attackers often copy the layout and information from legitimate sites and that phishing sites often contain terms that are common on a given page but relatively rare on the web as a whole. The system uses a TF-IDF score¹ calculation for each term found on a web page and generates a signature for the page by taking the five highest scoring terms. These terms are then fed into a search engine such as Google and, if the domain name matches the highest search result, the page is considered to be legitimate. Otherwise it is considered to be a phishing site. In addition to this comparison, the system also takes into account such things as the age of the domain, known images on the page, suspicious URLs or links, and forms on the page. During testing, they were able to successfully detect 94-97% of phishing sites, but there is a trade off between false positives and detection rates. They also acknowledge that the system could be subverted by attacking the TF-IDF algorithm, influencing Google page ranks, or launching denial of service (DoS) attacks on Google.

¹TF-IDF, which stands for term frequency-inverse document frequency, is a score often used in data mining and is a statistical measure for evaluating the importance of a word in a given document in a collection of documents. The score grows proportionally to the number of times the word appears in the document, but is also offset by the frequency with which it occurs in the collection.

Systems such as these may be valuable for phishing prevention since they do not rely on user interaction; however, these systems need to function correctly and reliably in order for users to trust their performance.

Ronda et al. [42] argue that completely automating anti-phishing tools may not be the answer and propose the design of a tool that integrates automation with user input. They claim that automated systems may cause too many false positives, are more easily subverted by attackers, and do not as easily support multiple languages. Their tool focuses on web pages that request information in an HTML form and, upon identification of such a page, will guide users to making the right decision about that web page. Its automated functionality maintains a whitelist of well-established and trusted domains, as well as a history of web pages that have been trusted by the user in the past. However, when the user attempts to enter information into a form on a page that has not automatically been classified as “trusted,” the tool will interrupt the user and ask them to describe the form they intend to fill out. The user’s description is then used as a query to Google, and the top 10 search results are compared to the user’s current web page. If that page is found in these results, it is considered to be “trusted.” Otherwise, the tool presents a preview of the top 3 search results and asks the user if any are similar to the page they originally visited. If so, the original site is deemed to be a phishing site and the user is redirected to the legitimate web site. Because of the small number of web sites containing forms that users tend to visit, they claim their tool is not too disruptive, and a user study showed that the tool was easy to use and the whitelist was effective. Whether it actually prevented phishing attacks remains an open question, since measuring this would have required compromising user privacy. But the authors believe that there

were indications of phishing prevention based on the observation of redirections from original pages to Google search results in some cases.

3.2 Web Browser Security Indicators

One of the main challenges in the design of web browser security cues is the *unmotivated user property* noted by Whitten and Tygar [50]. Security is a secondary goal for most users; they are primarily focused on tasks such as checking email or browsing a web site. If security indicators are too subtle, many users will not be motivated to search for them or read manuals to learn their functionality. Conversely, if the user finds the security indicator too obtrusive there is a risk that the user will ignore security altogether, either because they become annoyed or they grow too accustomed to the indicator.

A lack of attention to security cues can result in users falling victim to phishing attacks. Dhamija, Tygar and Hearst [8] investigated why these attacks can be so effective and identified a number of factors that contributed to their success. Three groups of factors dealt directly with browser security indicators: (1) lack of knowledge of security and security indicators; (2) lack of attention to security indicators; and (3) lack of attention to the *absence* of security indicators. Even when these cues are actively being used, many users cannot reliably distinguish between a legitimate indicator and an attacker's image of one. Images of a lock icon or security logo placed in the content of a web page are often considered by users to be equally as trustworthy, since many users may make no distinction between the page content and the chrome of a web browser [7].

3.2.1 The *https* Indicator

As mentioned, one indication of a secure connection to a web site is the placement of the string *https* in front of the address in the browser's URL bar. Several studies have shown that many users do not notice the presence or absence of the *https* indicator in a web site's address [8, 9, 43, 49]. One study by Schechter et al. [43] involved removing the *https* indicator and having users login to a banking web site. All 63 participants proceeded to enter their password and complete the task, despite the absence of the indicator.

3.2.2 The Lock Icon

In several studies, the lock icon is found to be the security indicator most often noticed [9, 49] but its absence often goes unnoticed [8]. Even when this indicator is used as a security cue by users, many do not fully understand its meaning [7, 8, 9]. Whalen and Inkpen [49] noted that while the lock metaphor alone may be a more powerful indicator of a secure connection than *https*, the icon is not being used to its full potential if there is no interaction with it. In most browsers, the lock not only signifies a secure connection, but clicking on the lock icon results in the display of identity information based on the web site's certificate. The majority of users who do rely on this security indicator are not even aware of this identity feature [8, 9, 49] and do not reliably understand the concept of certificates at all [7, 8].

The challenge of properly presenting indicators such as the lock icon in the chrome is worsened in small devices like smart phones and personal digital assistants (PDAs). Niu et al. [38] evaluated browsers used on these devices and identified a number of

problems, particularly with respect to the URL bar and browser chrome. The URL address bars are often truncated because of the smaller viewing area and, while the lock icon is small enough to be displayed in this area, the functionality of being able to click on it and view certificate information is not always present. It is also conceivable that users may have a more difficult time noticing security indicators because so much other information must also be fit onto the small screen. With the growing popularity of these devices, it is essential that browsers used on smaller screens are designed to be effective and intuitive.

3.2.3 Extended Validation Indicators

Jackson et al. [22] performed an evaluation of the current EV certificate support in Internet Explorer 7.0 with respect to picture-in-picture phishing attacks, in which attackers make use of images, within the content of a web page, that mimic a browser window. They found that the new security indicators had no significant effect on the users' ability to identify legitimate and fraudulent web sites, and reported that no one in the untrained group even noticed the new features. Although the primary intent of Extended Validation is to identify a web site and not to prevent phishing attacks, the study also showed that the new features had no major impact on user behaviour in any way. The authors do suggest that Extended Validation could become more useful in the future as users gain more awareness.

3.3 Browser Spoofing

When discussing the use of visual indicators to convey security and identity information, it is also necessary to consider how these indicators may be exploited by attackers. Already in 1996, Felton et al. [13] describe a spoofing attack in which they were able to rewrite all of the URLs on a web page in order to direct users to an attacker site. They noted that their attack would be even more successful by overwriting the location and status bars using simple javascript so that the SSL indicators would appear as expected to the user. Ye et al. [55, 56] took this one step further by implementing an attack that removed the location and status bars provided by the browser and replaced them with their own. This attack was also implemented on browsers much more recent than those available in the original 1996 study. Since they had complete control over these new bars, they were able to spoof the traditional security indicators and even control the pop-up windows that displayed certificate information or security warnings.

Internet Explorer 7.0 has taken steps to help prevent these types of spoofing attacks. Prior to version 7.0, the browser URL location bar, status bar, and other menu items could be hidden or disabled using standard application programming interface (API) calls. While the status bar can still be hidden, all windows (including pop-up windows) are required to display the location bar at the top. The developers of this browser have also placed all of the relevant security and identity indicators in the location bar, such as the lock icon and the green background for EV SSL certificates [31]. This makes it significantly more difficult for an attacker to overwrite the indicators in the location bar; they can no longer simply disable the default

location bar using an API call and create their own. Restrictions such as this would be useful in all web browsers to decrease the likelihood of spoofed security indicators.

One attack that is no more difficult in this new IE 7.0 feature is the picture-in-picture attack. Because of the similarity between the image and a legitimate browser window, the user can be fooled into thinking the site has simply opened a new window in front of the original [8]. Jackson et al. [22] acknowledge that without major changes to browser interface design, the only ways for users to identify these types of attacks are to notice which window has focus (two windows should not be in focus at once) or to try dragging or maximizing the window, and even these strategies are not fool-proof.

Grier et al. [19] proposed a new web browser design, called the OP web browser, that aims to improve overall browser security. The browser is divided into five subsystems, including a browser kernel, a user interface (UI) component, a storage component, a network component, and a web page subsystem. These components are isolated from each other, with all communication being managed by the kernel. The UI component does not render any web page content directly, as this is handled by the web page subsystem. This allows for stronger guarantees that the UI will not be unexpectedly affected by any potentially malicious web page content. Their evaluation of the browser also proved that the address bar cannot be spoofed, even when the web page subsystem is compromised. This is an important property for web browsers, especially when additional security and identity information is placed in this region of the browser chrome.

3.4 Eye Tracking in User Studies

Whalen and Inkpen [49] built upon the previous research on web browser security cues by incorporating eye tracking data into their evaluation. By tracking the user's gaze and fixation on the screen during the study tasks, they were able to obtain empirical results to cross-check what was reported by users with their actual behavior. There was very little variation between the visual cues that users reported using during the tasks and the data obtained from the eye tracker, but the tracking was also useful in identifying events that may otherwise have gone unreported, such as users looking for a padlock in the wrong location.

Another study by Kumar et al. [24] involved an eye tracker to implement a gaze-based password system that made use of the orientation of users' pupils to create passwords and authenticate to the system. The eye tracking data had a margin of error of 1° which resulted in some degree of inaccuracy, but despite this the error rates in their gazed-based password system were similar to those of passwords entered on a keyboard. These results support the use of eye tracking devices to reliably gather data on user gaze.

Henderson [20] discusses important evidence linking user gaze fixation with attention. He states that a user's eye movements are a behavioral sign of attention across the scene presented to them. In particular, the duration of gaze fixations tends to be a good indicator of a user's visual attention. The longer the user gazes at a particular region of a scene, the more likely that region has caught their attention. These findings also support the use of eye tracking devices in order to determine which areas of the screen are drawing user attention.

Chapter 4

User Study Methodology

4.1 Design and Implementation

The purpose of the user study carried out in this thesis was to explore user reactions to a new identity indicator introduced in Mozilla Firefox 3.0 Beta 1 and to determine whether or not this indicator could be improved upon with a design of our own. The indicator we evaluated in the Firefox 3.0 Beta 1 is a small buttonized portion of the chrome to the left of the URL bar that contains the web site favicon, or the default icon in cases where web sites do not use their own favicon. We designed an indicator that would be displayed in the same location of the browser chrome, but that was larger than the original Mozilla proposal and that displayed information about the web site's identity on the button. Both indicators (the unmodified Firefox 3.0 Beta 1 indicator and our modified indicator) would trigger a pop-up information box that provided identity information for the web site based on the site's certificate if a user clicked on the button (see Appendix A).

4.1.1 Browser Interfaces

To evaluate the new identity indicators, participants were exposed to all three possible states of the indicator in both browsers studied (see Figure 4.1). The indicator in each browser had three possible states: (1) *identity unknown*, for web sites without SSL certificates or with self-signed SSL certificates; (2) *location verified*, for web sites with traditional SSL certificates; and (3) *identity verified*, for web sites with EV SSL certificates.¹ Because Mozilla had not yet implemented the functionality required to identify EV SSL certificates at the time of the study implementation, the desired effect of state in the identity indicator was achieved by building three separate versions for each of the two browsers – one for each state of the indicator.

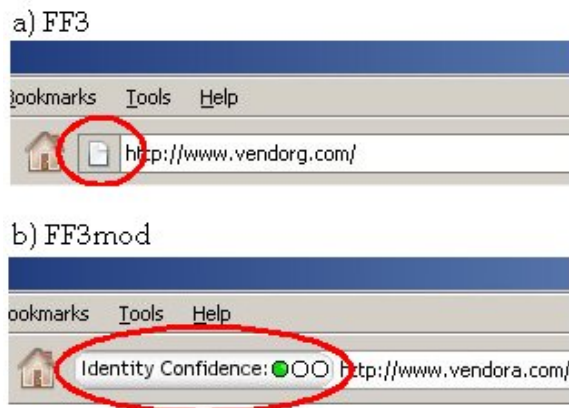


Figure 4.1: Identity indicators used in FF3 (Firefox 3 Beta 1) and FF3mod (Modified Firefox 3 Beta 1).

¹The italicized names here are those assigned by Mozilla developers as identifiers for the three different SSL states. These names are not intended to explore, or tenure opinion, on the “true” level of security resulting from the use of the different types of certificates.

4.1.1.1 FF3: Firefox 3.0 Beta 1

The first browser used in the study was the Firefox 3.0 Beta 1 as proposed by Mozilla.² This browser interface is referred to as FF3 hereafter. The identity indicator in this browser interface is located to the left of the URL bar, where a web site's favicon appears if one exists. This 20 x 20 pixel region of the browser chrome was made clickable by Mozilla developers; single-clicking on this region of the chrome would reveal a pop-up information box containing the identity information for the web site. In this interface, this information box was the only distinguishing feature between the three states of the indicator (see Appendix A). Therefore, we built one version of this interface that always displayed the *identity unknown*(non-SSL) information box when the indicator was clicked, a second version always displayed the *location verified*(SSL) information box, and a third version always displayed the *identity verified*(EV-SSL) information box.

4.1.1.2 FF3mod: Modified Firefox 3.0 Beta 1

We hypothesized that the buttonized 20 x 20 pixel region in FF3 might be too subtle and go unnoticed by most users. Because of this, we designed a second interface by modifying the publicly available Beta source code. Complete code changes are found in Appendix D. This interface is referred to as FF3mod and is simply a modified version of the FF3 browser that uses a different identity indicator. Rather than buttonizing an existing feature in the browser chrome, the identity indicator in FF3mod replaced the portion of the chrome where the FF3 identity indicator was displayed

²This was the current beta version in January, 2008 when the study was being implemented.

with a 144 x 20 pixel *identity confidence* button. This new identity indicator was designed with the same functionality as the unmodified indicator in FF3; clicking on the *identity confidence* button would reveal the same pop-up information box containing the web site's identity information.

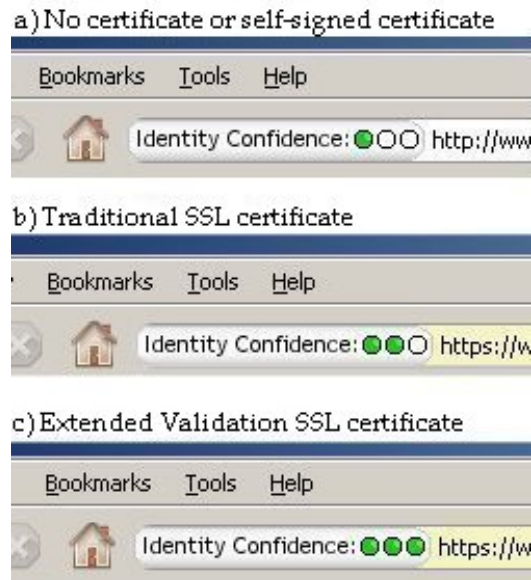


Figure 4.2: The *identity confidence* button in its three different states.

The *identity confidence* indicator was designed as a white button containing the words “Identity Confidence:” followed by a meter that consisted of three green lights (see Figure 4.2). For the *identity unknown* state used for web sites with no SSL certificate or self-signed SSL certificates, only one of the three lights would appear lit. For the *location verified* state used for web sites with SSL certificates, two of the three lights would appear lit, and for the *identity verified* state used for web sites with EV SSL certificates, all three lights would appear lit. As was done with FF3, we built

three different versions of this interface. One version always displayed the *identity unknown*(non-SSL) indicator and corresponding information box if it was clicked (see Appendix A), a second version always displayed the *location verified*(SSL) indicator and corresponding information box, and a third version always displayed the *identity verified*(EV-SSL) indicator and corresponding information box.

Several design considerations were taken into account during the design and implementation of this *identity confidence* button. The white background colour of the button was chosen to provide a contrast against the dark grey browser chrome that surrounded it. This was intended to catch the user’s attention. The size of the button was chosen mainly based on the amount of information we wished to clearly display on the button; this larger size might also attribute to better drawing user attention, at the expense of previous chrome “real estate”. The button was rounded on the left and right edges and contained shading around the perimeter in an attempt to emphasize the appearance of a clickable button.

Since one of the initial concerns was whether users would realize these new identity indicators were clickable, a major design decision was the implementation of the *identity confidence* meter on the button, using the three green lights. This was intended to provide basic identity information to the users who chose not to click on the indicator (or were unaware that it was clickable). While other browser security indicators have used a traffic light metaphor in the past [4, 11, 16], the use of three different colours in these types of indicators can create accessibility problems for colourblind users. If a user has trouble distinguishing between the green, yellow and red elements of an indicator then they may not be able to reliably distinguish the state of the indicator. Another reason to avoid this metaphor was the implications those colours may have

on the three different states of the identity indicator. The natural inclination would have been to assign red to the *identity unknown* state, yellow to the *location verified* state and green to the *identity verified* state. However, many legitimate websites will be classified as *identity unknown* simply because they do not make use of secure connections; a red indicator may falsely convey the idea that all such web sites are not to be trusted, and owners of such web sites might then reasonably be opposed to, or offended by, the use of such a browser design feature. Similarly, the colour yellow is often associated with warnings and may also falsely imply that all web sites with traditional SSL certificates should be considered untrustworthy. The use of three green lights was intended to provide a meter for web site identity – the more lights that are lit up, the more confident a user can be in the identity of the site.

4.1.1.3 FF2: Firefox 2.0 Control

A third browser was also included in the study as a control condition, giving a total of seven different interfaces. This browser consisted of the unmodified Firefox 2.0 browser (FF2) in circulation at the time of the study (circa January, 2008), containing no support for EV SSL certificates. Thus the user interface for this third browser in the study contained the traditional lock and *https* indicators but no additional identity indicators.

4.1.2 Other Technical Details

Live web sites were not used in the study for several reasons. One main reason was, as previously mentioned, the EV functionality had not yet been fully implemented in Firefox 3.0 at the time of the study. In addition to this, not many web sites had

purchased and implemented the new EV SSL certificates. Consistency across the study was also a consideration in this decision since each participant was to view the exact same web sites. Since the study was run over the course of two months, live web sites could potentially change during that time and introduce inconsistencies in what was viewed by each participant.

Because seven different interfaces would be shown to the participants during the study, seven different web sites were also created. Appendix B contains screenshots from these web sites. The sites were based on a very simply design for an e-commerce web site selling computers, peripherals and accessories. All seven web sites were very similar in order to reduce biases introduced by the appearance of the web site. However, the illusion of visiting seven different web sites was created for the user by changing the vendor name, the logo, and by interchanging the order of product categories. This was intended to reduce the possibility that participants would dismiss the security cues if they believed they were interacting with the same web site for each task.

To provide the same experience as visiting live web sites, the sites used in the study were hosted locally on a Windows XP Professional machine using Apache 2.2.8. Since the domain name and organization that is displayed in the pop-up information boxes of the new indicators is pulled from SSL certificates, a self-signed certificate containing this information was created for each web site. It is important to note that the certificates were only used for these two pieces of information; the actual SSL identity state (*identity unknown* – non-SSL, *location verified* – SSL, and *identity verified* – EV-SSL) that was shown to the user was always determined by the state that was hard-coded into each of the seven interfaces.

A Tobii 1750 eye tracker [46] set to a resolution of 1024 x 768 pixels at 96 dpi was used to capture and store data about each participant’s gaze and fixation throughout the study. The stored data allows playback of a recording of eye location on the screen and also captures the x and y co-ordinates of each eye’s location at intervals of 20 milliseconds. This device was located at the bottom of the monitor used by each participant for web browsing and captured eye movement as long as the user stayed within the range of the device. A second monitor was set up for the experimenter (the author of this thesis) and displayed a real-time view of the eye tracking functionality. This allowed the experimenter to note any times where the participant’s gaze focused on the identity indicators and also provided a way to monitor that the eye tracker was functioning properly throughout the study. A calibration done at the beginning of the tasks ensured that the eye tracker device was configured correctly; if the participant moved or the eye tracker was no longer capturing the gaze, this calibration would be performed again.

4.2 Participants

Complete demographic information for the participants in the study is presented in Table 4.1. A total of 28 participants took part in the user study. They were recruited through the use of an online campus recruiting system as well as posters displayed on campus. Sixteen were male and twelve were female, with ages ranging from 18 to 29. Twenty-four participants were undergraduate students and had a variety of majors and years of university education. Two participants were Computer Science and Engineering students who had high technical knowledge of computer security. With the

exception of one other participant, the remaining users had relatively little computer security knowledge. Despite this, 21 out of 28 participants rated their concern for using their credit cards online as 8 or higher on a Likert scale from 1 (low) to 10 (high). All participants had made a purchase online in the past; 50% of participants reported making online purchases at least once per month. All participants browsed the Internet at least 5-10 hours per week, and consequently were very familiar with the use of a web browser. Microsoft's Internet Explorer was the web browser customarily used by 15 of the participants, 8 used Mozilla Firefox, 4 used Apple's Safari, and one participant reported using Netscape.

4.3 Tasks

Each participant in the study was asked to complete a 60 minute lab session. The participants were randomly assigned to one of two groups, with each group having the same distribution of gender, age, and education. Before proceeding to the tasks, participants in Group 1 were informed that the study's purpose was "to evaluate different web browsers and web sites that could be used for Internet shopping". This was not intended to deceive the participants in any way, but to ensure that there was no specific focus on security so that they would not be influenced to act any differently than they normally would. Participants in Group 2 were provided with the same purpose statement but were also told that "we are interested in such things as visual appearance, item pricing, amount of contact details, trust in the site's authenticity, and ease of use". The purpose of the additional information was to evaluate whether the subtle reference to trust in the site's authenticity would influence the participant

	Group 1	Group 2
Gender		
Male	8	8
Female	6	6
Education		
Completed College	1	0
Undergraduate (In Progress)	11	13
Masters (In Progress)	1	1
PhD (In Progress)	1	0
Program of Study		
Computer Science/Engineering	1	1
Arts/Sciences/Other	13	13
Age Group		
18-22	8	10
23-29	6	4
Browser Used Most Often		
Internet Explorer	8	7
Firefox	3	5
Safari	3	1
Netscape	0	1
Hours Per Week Browsing Web		
5 to 10	1	5
10 to 20	11	0
20+	2	9
Frequency of Online Purchases		
Rarely	7	2
Several per year	2	4
Once per month	4	4
Several per month	1	4

Table 4.1: Participant Demographics

to focus more on the identity indicators. All other aspects of the study were identical for both groups.

After the introduction, the participant performed a sequence of seven tasks. Each task involved the following steps:

1. Read a brief description of three items to be located on a web site.
2. Double-click on a desktop icon corresponding to the task number to open one of the web sites within one of the seven browser interfaces.
3. Locate the three requested items on the web site and record the price of each on a sheet provided.
4. Answer a series of two questions: (1) on a 10-point Likert-scale, “How willing would you be to make purchases on this web site with your own credit card?” and (2) “What factors did you use in making your decision?”

The order of presentation of the browser interfaces, web sites and tasks were counterbalanced using spatially balanced 7x7 Latin squares [17] to avoid bias created by the order in which the independent variables are presented. Once all seven tasks were completed, a follow-up interview was conducted in which participants were asked for their opinions regarding the web browsers used in the study. Each of the seven interfaces were reopened and the identity indicator in each version was pointed out and explained to the participant. Because the interfaces had been counterbalanced, half of the participants received the explanation of the FF3 identity indicator first, while the other half received the explanation of the FF3mod identity indicator first. For each indicator, the participant was asked whether or not they recalled seeing

that indicator while performing the tasks, and if so, how many times they recalled seeing it. After viewing examples of both new identity indicators, the participants were asked which they would prefer to use at home if given the choice. Finally at the end of the lab session, each participant filled out a questionnaire used to collect demographic information. All documentation used in the user study can be found in Appendix C.

Chapter 5

User Study Results

Each participant completed all 7 tasks, giving a total of 196 tasks from which to draw data. The results were analyzed based on both qualitative data (observation of the participant's behavior during the study, post-task questionnaires and interviews at the end of the session) and quantitative data (gathered by the eye tracker, participant observation and the post-task questionnaire).

5.1 Self-Reported Attention to the Identity

Indicators

User attention to identity indicators was determined by observing participants during the study and by reviewing their responses to the follow-up interview. The results showed that the identity indicator introduced in the FF3 web browser went unnoticed by all of the participants in our study; no one reported noticing it in the post-task questionnaires or follow-up interviews, nor was anyone observed fixating on the

	Group 1		Group 2		Total	
	Number	Percent	Number	Percent	Number	Percent
FF3 Indicator	0	0%	0	0%	0	0%
FF3mod Indicator	6	43%	9	64%	15	54%

Table 5.1: Number and percentage of participants who noticed each identity indicator.

indicator while that browser was being used. Because this indicator went unnoticed, no one attempted to click on the indicator and therefore no one saw the pop-up information box that distinguished between the three certificate levels.

Table 5.1 shows the number and percentage of participants who reported noticing identity indicators. Of the 14 participants in Group 1 (those given minimal instructions), 6 reported noticing the FF3mod *identity confidence* indicator when they were asked during the post-task interview if they noticed it during the tasks. This same indicator was reported to be noticed by 9 participants in Group 2 (the group given enhanced instructions). Of these 15 participants who reported noticing the FF3mod *identity confidence* indicator, 7 reported seeing it on at least two different interfaces. Five participants were unsure of how many times they had seen this indicator, while the other 3 said they only noticed it once near the end of their tasks as they became more observant of the browser features.

All 7 participants who reported noticing the FF3mod *identity confidence* indicator at least twice while performing their tasks also reported noticing the different states of the indicator. Three of these participants displayed immediate understanding of this indicator and actively used it when making decisions about their willingness to transact with the web sites. When asked in the post-task questions why they assigned

the higher ratings to the web sites using SSL, these three users reported looking to the FF3mod *identity confidence* and assuming that the number of green lights implied trust in the web site. The participants who did not use the indicator in their decision-making dismissed it, stating reasons such as “I don’t understand what it means” or “I just assumed all of the web sites were the same”. None of these participants made any attempt to interact with (click on) the *identity confidence* button and therefore did not see the pop-up information box at any point.

During the follow-up interview, participants were explicitly shown the two different browsers (FF3 and FF3mod) and the identity indicators that were evaluated in the study and were asked which they would prefer to use at home if given the option. The FF3mod browser with the *identity confidence* button was chosen by 22 of the 28 participants (78%), as is shown in Table 5.2. When asked why they would choose this option, participants gave reasons such as the indicator being more eye-catching and easier to notice, and the fact that it provides some identity information without having to click on the button. Most felt the unmodified FF3 version was too subtle. The 4 participants who preferred FF3 stated that they liked the fact that it took up less space in the chrome but commented that they would need to somehow be made aware that it existed. One participant had no preference for either indicator, and one other clearly stated they preferred the traditional lock icon to either of these identity indicators.

Interface Preference	Number	Percent
FF3mod	22	78%
FF3	4	14%
No Preference	1	4%
Neither	1	4%

Table 5.2: Number and percentage of participants who preferred each browser.

5.2 Objective Measures of Attention to Identity Indicators

The results obtained with respect to participants' self-reported attention to identity indicators were verified with the eye tracker data. The eye tracker allowed for replay of each session in order to visually analyze times at which the user may have looked at the indicators. The replay screen portrays a moving blue dot that signifies the user's gaze; the larger the dot becomes, the longer the user has fixated on that region of the screen (see Figure 5.1). Data files that recorded the x and y co-ordinates of the gaze at intervals of 20 milliseconds were also analyzed to determine times at which the participant's gaze was fixated on the indicator's co-ordinates.

The eye tracker data confirmed that the 15 participants who reported noticing the FF3mod *identity confidence* indicator throughout the tasks did in fact fixate on the co-ordinates where the button was displayed for an average of 1.1 seconds at a time. Data from the participants who did not report noticing the *identity confidence* indicator showed that if their gaze did fall on the co-ordinates of interest, it was only for approximately 0.25 seconds at most.

In addition to the identity indicators being studied, 7 participants also reported



Figure 5.1: A screenshot of the eye tracker replay function. The large circle near the *identity confidence* indicator shows the participant's fixation on that region.

using the traditional indicators (the lock icon or *https*) to help make decisions about identity and trust. The eye tracker data confirmed that these users did in fact fixate their gaze on the appropriate co-ordinates throughout the seven tasks. There were also 4 participants who did not report using the traditional indicators in their decision-making but whose gaze fixated on their co-ordinates for an average of one second during most tasks.

5.3 Willingness to Transact

There was a wide range of answers to the Likert-scale question, “How willing would you be to make purchases on this web site with your own credit card?” where a rating of 1 was low, and 10 was high. Nine participants assigned the same rating

across all 7 browser interfaces, basing their decisions solely on visual appearance and professionalism (which was kept relatively constant across all 7 web sites). The raw data for this measurement is included in Appendix E.

Two types of statistical tests were performed on this data in order to determine which independent variables played a role in any differences between the willingness ratings.

- Analysis of Variance (ANOVA): a statistical method used to make simultaneous comparisons between two or more means. It compares the variance between conditions with the variance within conditions to test for significant relations between variables. The result of this test is expressed as a value resulting from Fisher's F test – a ratio of the variance between the means across treatments to the variance between the groups. The p value shown after this result is the probability that this effect is due to chance [28].
- Tukey Honestly Significant Difference (HSD) Test: a post-hoc statistical method of multiple comparisons that test for a significant difference between a pair of means based on rankings from smallest to largest. This test is conducted after significant differences are discovered in an ANOVA [28].

The first analysis of our data was a two-way ANOVA with condition (7 interfaces) and instructions (2 groups) as the factors. Table 5.3 presents the means and standard deviations for this analysis. The 7 interfaces consisted of FF3 and FF3mod in all three SSL states, as well as the FF2 control. The groups here refer to Group 1 – minimal instructions and Group 2 – enhanced instructions. We adopted a significance criteria of $\alpha < .05$ for all analysis of the study data. There was a significant main effect of

condition ($F(6,156) = 4.09, p < .001$), meaning that there were significant differences in ratings assigned across the 7 interfaces. There was no significant difference in ratings between the two groups ($F(1,26) = .52, p < .48$). There was also no interaction between the interface condition and the groups.

	Group 1		Group 2		Overall	
Interface	Mean	SD	Mean	SD	Mean	SD
FF2	4.93	2.87	5.36	2.56	5.14	2.68
FF3 non-SSL	3.86	2.32	4.93	2.70	4.39	2.53
FF3 SSL	4.64	2.82	5.43	2.62	5.04	2.70
FF3 EV-SSL	4.93	2.56	5.71	2.53	5.32	2.53
FF3mod non-SSL	3.71	2.59	4.57	2.71	4.14	2.64
FF3mod SSL	5.07	2.27	5.29	2.49	5.18	2.34
FF3mod EV-SSL	5.57	2.95	5.79	2.49	5.68	2.68

Table 5.3: Interface means and standard deviations of willingness to transact ratings

Post hoc tests were conducted to determine where the significant pairwise differences were among the means using a Tukey HSD test. There was a significant difference in the means between the FF3 non-SSL interface and the FF3mod EV-SSL interface, as well as between the FF3mod non-SSL interface and both the FF3 EV-SSL and FF3mod EV-SSL interfaces, as seen in Table 5.4. There were no significant differences between non-SSL and SSL interfaces or SSL and EV-SSL interfaces. Since the ratings for the FF2 control interface were not significantly different from any other interface, we chose to remove this condition from further analysis.

A second analysis was performed using a 2-way ANOVA to compare the two browser conditions with the three different states of each browser. Table 5.5 gives

	FF2	FF3 non-SSL	FF3 SSL	FF3 EV-SSL	FF3mod non-SSL	FF3mod SSL	FF3mod EV-SSL
FF2	–						
FF3 non-SSL	NS	–					
FF3 SSL	NS	NS	–				
FF3 EV-SSL	NS	NS	NS	–			
FF3mod non-SSL	NS	NS	NS	*	–		
FF3mod SSL	NS	NS	NS	NS	NS	–	
FF3mod EV-SSL	NS	*	NS	NS	*	NS	–

Table 5.4: Differences in means of willingness to transact ratings between interfaces. Note: NS=non-significant difference between the means, *=significance using Tukey HSD with alpha = 0.05

the means and standard deviations for each SSL state and browser. There was no interaction found between the factors of browser and state, meaning that there was no change in the simple main effect of one variable (eg: SSL state) over levels of the second variable (eg: browser). There was no significant difference between the browsers ($F(1,27) = 0.40, p < .53$). There was however a significant main effect of SSL state ($F(2,54) = 6.03, p < .005$). These results were followed up with a Tukey HSD test and the significant difference was found to be between the non-SSL and EV-SSL states, as seen in Table 5.6. There were no significant differences between non-SSL and SSL states, nor between SSL and EV-SSL states.

With the help of the eye tracking data, we classified participants as “gazers” or “non-gazers.” Participants who were considered to be gazers looked at either the traditional security indicators (lock icon, *https*), the FF3mod *identity confidence* indicators, or both, during each task for at least 0.5 seconds. There were 11 participants classified as gazers in the study. All other participants were classified as non-gazers, regardless of what they reported looking at during the study. By making this distinction, we identified that participants who look at SSL indicators (either traditional lock and *https* or the new identity indicators) de-value non-SSL connections and assign higher ratings to web sites with SSL or EV SSL certificates; but in the study, less than 40% of participants were gazers.

To verify the difference in ratings assigned to non-SSL and SSL connections, we performed further analysis on the data, looking at the gaze factor. The means and standard deviations for each SSL state among gazers and non-gazers are shown in Table 5.7. By performing a two-way ANOVA comparing state and browser among non-gazers, as expected, there was no significant difference in ratings across SSL state

	FF3		FF3mod		Overall	
State	Mean	SD	Mean	SD	Mean	SD
non-SSL	4.39	2.53	4.14	2.64	4.27	2.56
SSL	5.04	2.70	5.18	2.34	5.11	2.51
EV-SSL	5.32	2.53	5.68	2.68	5.50	2.59

Table 5.5: State means and standard deviations of willingness to transact ratings

	non-SSL	SSL	EV-SSL
non-SSL	–		
SSL	NS	–	
EV-SSL	*	NS	–

Table 5.6: Differences in mean willingness to transact ratings between states. Note: NS=non-significant difference between the means, *=significance using Tukey HSD with alpha = 0.05

($F(2,32) = 1.61, p < .22$). However, there was a very significant main effect of SSL state among the gazers ($F(2,20) = 6.32, p < .008$). A Tukey HSD test was used to discover the differences in the various SSL states among gazers; there was a significant increase in mean ratings from non-SSL(3.41) to SSL(5.50) interfaces, as well as from non-SSL(3.41) to EV SSL(5.95) interfaces, as can be seen in Table 5.8. The increase from SSL to EV SSL interfaces was not significant.

A basic boxplot (Figure 5.2) and a notched boxplot (Figure 5.3) were plotted to obtain a visual representation of the data. The line that extends from each box (sometimes referred to as the “whiskers”) shows the upper and lower extreme values in the data being analyzed. The top hinge of the box denotes the upper quartile (the 75th percentile), while the bottom hinge of the box denotes the lower quartile

	Gazers		Non-Gazers	
State	Mean	SD	Mean	SD
non-SSL	3.41	2.70	4.64	2.42
SSL	5.50	2.54	4.94	2.54
EV-SSL	5.95	3.03	4.82	2.51

Table 5.7: State means and standard deviations of willingness to transact ratings of gazers vs. non-gazers

(the 25th percentile), implying that 50% of the scores fall within the box. The thick line across the box indicates the median score. In the notched boxplot, the notch provides a measure of the 95% confidence interval around the median. The implication is that for two medians to be significantly different from each other, their notches must not overlap [29]. In Figure 5.3 for example, we can see that the notches for non-SSL interfaces and SSL interfaces among gazers overlap, as well as those for SSL interfaces and EV-SSL interfaces. However, the differences can be seen between non-SSL interfaces and EV-SSL interfaces.

	non-SSL	SSL	EV-SSL
non-SSL	–		
SSL	*	–	
EV-SSL	*	NS	–

Table 5.8: Differences in mean willingness to transact between states for gazers. Note: NS=non-significant difference between the means, *=significance using Tukey HSD with alpha = 0.05

When the 95% confidence interval falls outside of the hinges of the box, protruding notches are plotted to indicate that the notch falls higher or lower than can be plotted

on the box [29]. This can be seen in Figure 5.3 at the bottom of the boxes for the gazers. This means that in this data, the 95% confidence interval of the median falls lower than the 25th percentile, indicating low confidence due to a large amount of variation within these groups. This could be explained in part by the fact that some participants deemed the web sites to be very professional and assigned extremely high ratings, while others deemed the sites to be unprofessional and assigned low ratings. By observing these types of behaviour during the study, we determined that running more participants would be unlikely to decrease the variation in the data.

To give an overall view of the data obtained from the study, boxplots were also plotted to show all 7 interfaces (Figures 5.4 and 5.5). As can be seen in Figure 5.4, many of the medians fall on the upper or lower hinge of the box. To get a better picture of these boxes, Figure 5.5 shows the notched boxplots where there is evidence of low confidence intervals for these medians.

One interesting comparison to note in Figure 5.4 is the appearance of a higher median for the FF3 SSL interface than for the FF3 EV SSL interface. We hypothesize that this may be caused by one of several factors. On a few occasions, participants reported not seeing a lock icon in a given interface despite the fact that one existed; this sometimes led to a lower rating for that interface. When asked after each task what they were using in their decision-making, some gazers reported judging the web site's appearance in addition to the traditional and/or new indicators which led to some variation in assigned ratings. The notches on these boxes in Figure 5.5, however, do illustrate that there is no statistically significant difference between the medians for these two interfaces.

In addition to analyzing these ratings with respect to gazers vs. non-gazers, the

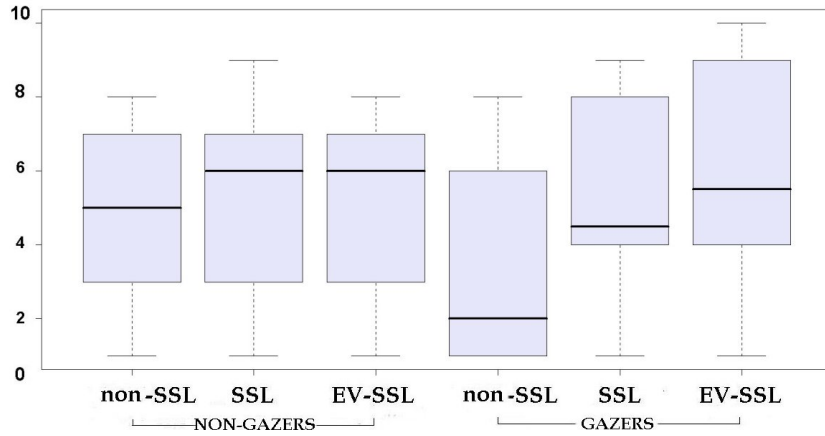


Figure 5.2: Boxplot of participants' mean *willingness to transact* ratings based on SSL state, grouped by gazer or non-gazer.

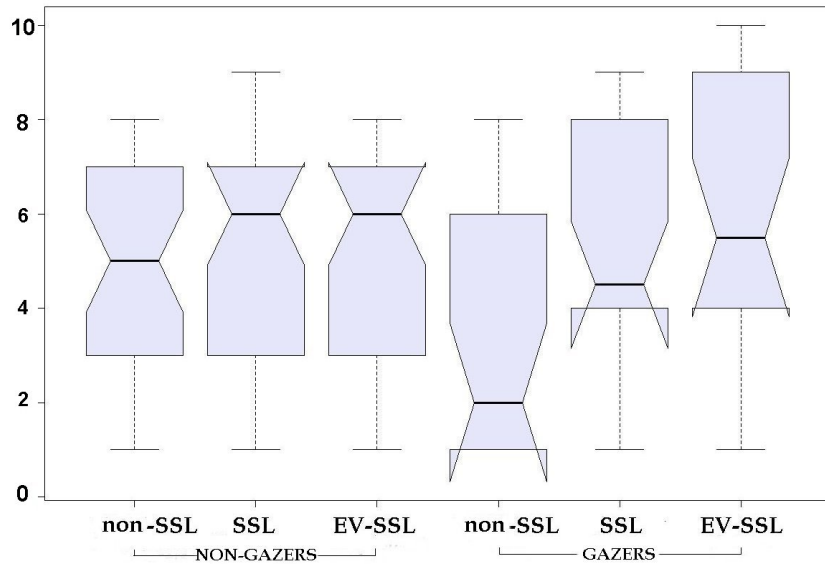


Figure 5.3: Notched boxplot of participants' mean *willingness to transact* ratings based on SSL state, grouped by gazer or non-gazer.

three users who reported using the FF3mod *identity confidence* indicator in their decision-making were compared with other gazers who did not. Participants who used the FF3mod *identity confidence* indicator in their decision-making assigned a

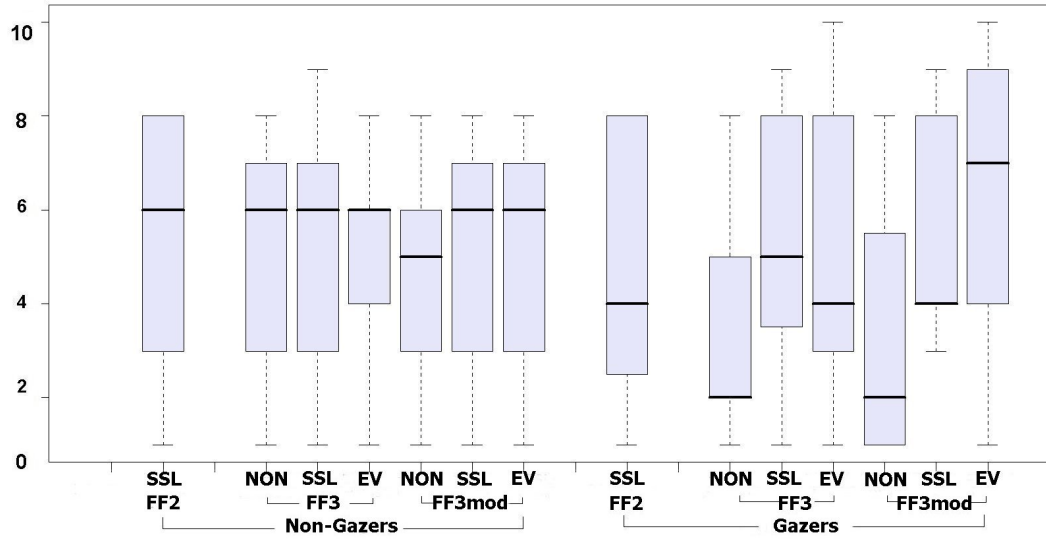


Figure 5.4: Boxplot of participants' mean *willingness to transact* ratings based on Browser and SSL state, grouped by gazer or non-gazer.

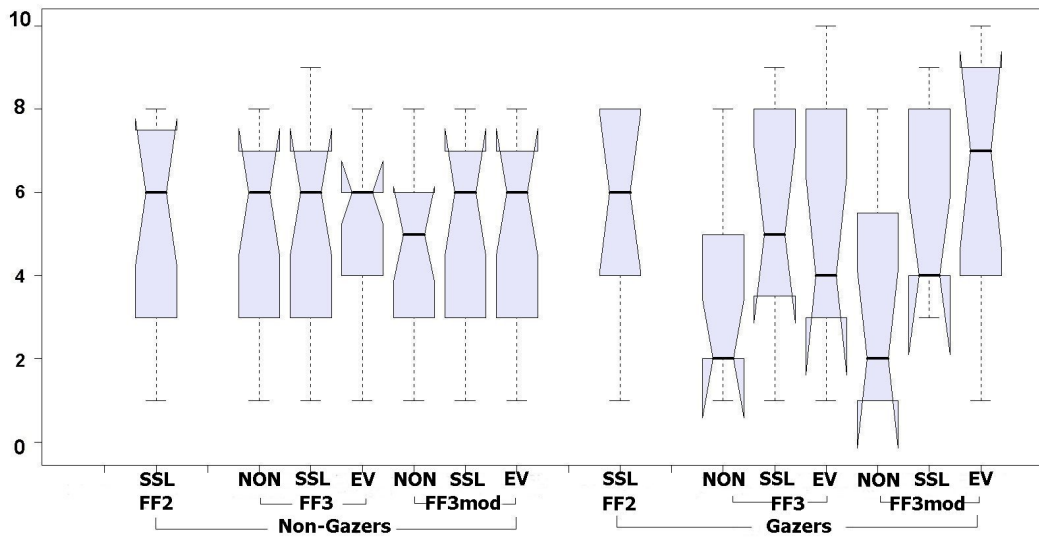


Figure 5.5: Notched boxplot of participants' mean *willingness to transact* ratings based on Browser and SSL state, grouped by gazer or non-gazer.

mean rating of 8.33 to the EV SSL interfaces, 6.50 to interfaces with SSL, and 3.83 to interfaces with non-SSL connections. Although these differences appear large, the small number of participants who made use of this new indicator in their decision-making prevented a meaningful statistical comparison.

5.4 Time Spent Gazing at Browser Chrome

One of the more interesting findings in the eye tracking data was how long users spent gazing at the content of the web pages as opposed to gazing at the browser chrome. For each participant, we compared the amount of time the participant's gaze data contained co-ordinates within the browser chrome during the study tasks with the amount of time the participant's gaze data contained co-ordinates in the page content. On average, the 11 participants who were classified as gazers spent about 9.5% of time gazing at any part of the browser chrome. The remaining 17 participants who did not gaze at indicators spent only 4.3% of their time focusing on browser chrome as opposed to content (some spent as little as 1%).

We performed a one-way ANOVA on the data, this time testing for significant differences in the amount of time spent gazing at browser chrome between gazers and non-gazers rather than in willingness to transact ratings. There was a significant main effect of gaze ($F(2,20) = 15.04, p < .0006$). Figure 5.6 illustrates the distribution of the time spent gazing at browser chrome across all participants, while Figure 5.7 shows the difference in distribution between gazers and non-gazers. The plot of the non-gazers illustrates that, aside from one outlying participant, all non-gazers spent less than 7% of their time (less than 40 seconds) gazing at chrome. However, in the

plot of the gazers' data we can see that the distribution of time is less uniform, with the majority of participants spending between 5% and 15% of their time gazing at chrome.

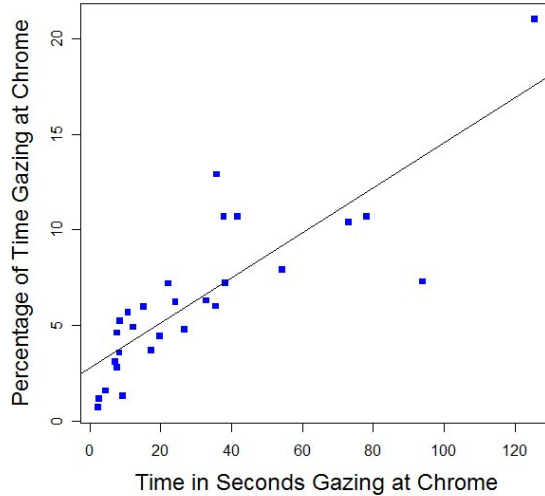
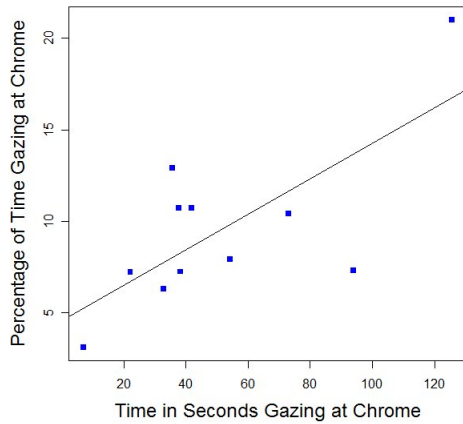
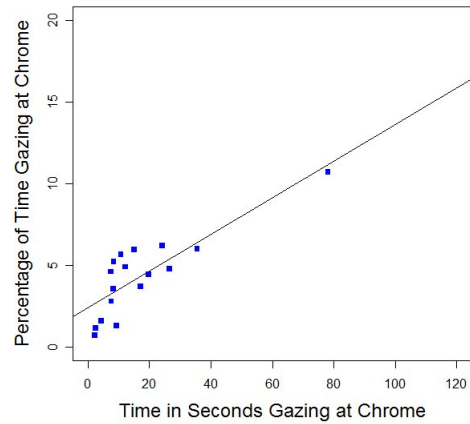


Figure 5.6: Plot of the frequency distribution of time spent gazing at chrome for all participants.

While other studies have found that many users are unable to distinguish between web page content and chrome, this study suggests they do distinguish between the two and spend the majority of their time gazing at the parts of the screen that display content rather than chrome. This finding was also supported by the participants' comments during the follow-up interview. When the identity indicators were pointed out to participants, many made comments such as "I didn't even think to look up there" or "I was only focusing on the web page itself."



(a) Gazers



(b) Non-gazers

Figure 5.7: Plot of the frequency distribution of time spent gazing at chrome for gazers and non-gazers.

5.5 Decision Strategies

After each task, participants were asked what factors they used in making decisions about whether or not to trust the web site. Twenty (71%) of the participants in the study reported the visual appearance and professionalism of the web site as a factor in their decision-making. Seven (25%) of the participants reported looking for the traditional lock icon and/or *https* indicators, and three (11%) participants reported using the new FF3mod *identity confidence* button to make decisions. Three other participants reported looking to the content of the web page for security information and logos.

In the participant information questionnaire at the end of the study, participants were also asked to identify the factors they typically use in real world situations to determine whether or not to trust a web site. A complete list of decision making

Factor	Used in Study Tasks	Used in General
Company Reputation	–	64%
Appearance and Professionalism	71%	39%
Lock Icon and/or <i>https</i>	25%	32%
Security Information in Content	11%	25%
Peer Recommendations	–	25%
Contact Information	14%	21%
Payment Methods Available	7%	11%
FF3mod <i>identity indicator</i>	11%	–
Site Regularly Updated	–	4%
Number of Pop-Ups	–	4%
Listed with Better Business Bureau	–	4%

Table 5.9: Percentage of participants who reported using various factors in their decision making during the study and in general. Dashes are used to indicate decision strategies that were not available in the study or do not apply in general.

factors reported by participants is given in Table 5.9. The factor that was most commonly reported by participants was the company’s reputation, which was mentioned by 18 participants (64%). Eleven participants (39%) mentioned basing decisions on the appearance and professionalism of the site, nine (32%) reported using the traditional lock icon and/or *https* indicators, seven (25%) reported looking for security information in the content of a web page, and seven (25%) reported basing decisions on recommendations from friends or peers. Other factors included the amount of contact information, the payment methods used by the web site, whether or not the site is regularly updated, the number of pop-ups generated by the site, and whether or not the company is listed with the Better Business Bureau.

Chapter 6

Discussion

6.1 EV Indicators

The results showed that the identity indicator used in the unmodified FF3 browser did not influence decision-making for the participants in the study in terms of user trust in a web site. These new identity indicators were ineffective because none of the participants even noticed their existence. Had they known that this clickable area existed beside the browser's URL bar, they would have been able to distinguish between the three SSL states by clicking on that area and seeing the pop-up information box. Since this functionality was not discovered, the indicators were of no value to the user. The differences in ratings based on state for this browser can only be explained by the use of the traditional lock icon and *https* indicators.

While almost half of the participants also failed to notice the new FF3mod *identity confidence* indicator, it is important to note that 15 participants did take notice of this indicator. It was even more promising that 3 participants made use of it in their

decision-making and reported an understanding of its meaning during the post-task questions. This supports the idea that some users may be able to reliably make use of such indicators to evaluate web site identity. The 12 others who reported noticing the *identity confidence* indicator did not report using it in decision-making, possibly because they did not fully understand its purpose. Many participants reported noticing the indicator late in the study after most of the tasks were completed; this suggests that as users are given more exposure to the new indicators, they may be more likely to take notice of them.

It is also interesting to note that, in general, participants classified as gazers assigned lower ratings to non-SSL interfaces and higher ratings to both SSL and EV SSL interfaces, but there was no statistically significant difference in ratings given to SSL vs. EV SSL interfaces in either browser. Even among the three participants who reported using the FF3mod *identity confidence* indicator in their decision-making, only one participant gave notably different ratings to the FF3mod SSL (rated a 4) and the FF3mod EV SSL (rated a 10) interfaces. The other two participants also used the traditional lock icon or *https* to aid in their decisions and thus assigned high levels of trust to all SSL interfaces. Since nothing was done in the study to educate participants on the differences between SSL and EV SSL, and as far as we know they had no background knowledge in the area, it is not surprising that ratings given to these interfaces did not differ greatly. If the goal of EV SSL certificates is to give users a higher level of confidence in a web site's identity than traditional SSL certificates, it is possible that users will need to be better educated on the different levels of identity indicators.

6.2 Attention to Browser Chrome

Previous studies have indicated that most users appear unable to distinguish between web page content and browser chrome [7]. Comments from the participants such as “I didn’t look up there, I only looked at the web page itself” lead us to believe that perhaps they do distinguish between the two but do not refer to the term *chrome*. With the use of eye tracking data, our study showed that participants spent very little time looking at any parts of the browser chrome. This presents an important challenge when it comes to incorporating security cues into web browsers; any content provider can trivially modify the content of a web site to include security information. This problem is amplified by the fact that many users actually look for security information in the page content of a web site. During the study, several users mentioned they had looked for security logos within the web site’s page content or looked for statements on the payment pages regarding the security of their credit card information. These types of security cues could be easily incorporated into an attacker’s web site and many users would evidently be fooled by this technique.

While elements of the browser chrome can also be spoofed [13, 55, 56], doing so is more work for the attacker. It becomes even more difficult (but still not impossible) when browsers such as Internet Explorer 7.0 and the proposed OP browser [19] place restrictions on which parts of the window can be hidden. However, in order to provide identity indicators that can best aid users in identifying web sites, designers apparently need to place these identity cues in the chrome. Two main open questions remain: (1) how can users be persuaded that the elements of the chrome are worth looking at; and (2) how can it be ensured that users can distinguish a legitimate

indicator from a spoofed indicator?

6.3 Design Implications

The fact that most users tend to ignore the browser chrome suggests that designers need to somehow find a way to draw visual attention to any security cues provided by the browser. This was the intention of the FF3mod *identity confidence* indicator by making it larger than the original FF3 indicator and using a color contrast to the browser chrome surrounding it. However, this was still not enough to get almost half of the study participants to take notice of it. Better techniques for drawing user attention to important security indicators might be needed, especially if these indicators are meant to be intuitive for the user. (Of course, parties responsible for other buttons in the chrome likely feel similarly about the importance of their buttons unrelated to security.) However, this is also dangerous advice if attackers can counter this by finding ways of spoofing these parts of the chrome. The design of these indicators should be done in a way that makes it much more difficult for attackers to replicate. Mozilla developers [37] attempted to do this by having the identity indicator’s pop-up window overlap slightly with the location bar (see Appendix A), but this is unlikely to be noticed by most users.

Another important design issue to note was the “clickable” feature of both the FF3 and FF3mod indicators. Not one participant in the study clicked on any of the indicators, even those who did notice and use the FF3mod *identity confidence* indicator. The FF3mod indicator was designed to have rounded edges and shading in an attempt to make it appear button-like, however this failed to cause users to click

on this button. Perhaps more shading or a different shape would have been more effective. It is also possible that including action words, such as “click here” might have had more of an effect, but it seems unreasonable for every clickable button to be so annotated.

6.4 Limitations of Study

One of the major limitations of the study was the fact that it was conducted in a laboratory setting rather than in the field. This may have led to participants acting differently than they normally would in their own environments. Some participants may have felt more secure than during their normal web browsing because it was a university setting, while others may have paid more attention to security because of the more formal setting. The eye tracker may have also influenced participants to behave differently since they were aware that their eye movements were being recorded. However, the eye tracker provided valuable data for analysis and this was the main reason for the use of a laboratory setting; it would not be realistic to expect participants to install eye trackers in their home environments for the purposes of the study.

Having users visit 7 web sites, each displayed in a different browser interface may have also contributed to creating an unrealistic experience. In a normal web browsing, each web site they visit will not likely cause the identity indicator to alternate in state so frequently. Part of the reasoning for users noticing the FF3mod *identity indicator* in the study might possibly be due to the fact that the region of the chrome where it was located changed between each interface they were shown.

The fact that the tasks involved recording prices rather than following through with financial transactions may have also influenced participants to be less concerned with security. This effect was balanced by asking them questions after each task regarding their willingness to transact with the web site; these questions were intended to draw their attention to security issues. This may explain why several users noticed the identity indicators later in the study, as they became increasingly aware of security.

Another potential limitation of the study was participants' lack of familiarity with the various components of the study. Twenty of the 28 participants did not use Mozilla Firefox as their usual web browser. The novelty of an unfamiliar browser may have distracted participants because not only were the identity indicators new to them, but so was the overall look and feel of the browser window. The concept of EV SSL certificates is also relatively new, and some users do not fully understand SSL itself, so it is likely many users were not even aware that they should be looking for cues relating to the certificate types. As users gain more knowledge of EV SSL certificates, they may become more likely to use the types of identity indicators used in this study to make decisions about online security.

6.5 Current State of EV Support

As of May 2008, Internet Explorer 7.0 is the only browser to provide full EV support in production software. In all other browsers, web sites with EV SSL certificates currently behave in the same way as web sites with traditional SSL certificates. Users can however view the certificate details to determine whether or not the certificate is SSL or EV SSL, should they be aware that this feature is available to them. Both

Opera [40] and Mozilla [32] plan to include EV support in future releases of their browsers; this support is currently included in beta versions under development.

The World Wide Web Consortium (W3C) [51], an international consortium in which members work together to develop standards for the Web, is currently looking to develop standards for identity indicators in the UI of the web browser as part of an existing project. A working draft of a technical report on this project recommends that identity information regarding a web site *should* be presented to the user through the primary user interface (part of the chrome available to the user without initiating any action) and *must* at least be presented in a secondary user interface (only viewed when initiated by some user action). This report also recommends that all information provided in these identity indicators must be taken from validated certificates and not from unauthenticated sources [52]. The original intent of the CA/Browser Forum [3] was to standardize the indicators for EV certificates across all web browsers, however each browser vendor is currently implementing EV support differently.

While Mozilla Firefox 3.0 Beta 1 was the latest version available at the time of study implementation, the current version of this browser in May 2008 is Release Candidate 1 [35], a publicly available preview. In this version, the EV indicators have changed somewhat from what was presented in the Beta 1 release. The indicator is located in the same region of the chrome, to the left of the URL bar where the site's favicon is shown. This region is still buttonized and clickable to produce the identity information pop-up box. However, there are now visible changes to this region of the chrome if the web site has a traditional SSL or EV SSL certificate. For traditional SSL, the background of the favicon button is colored blue. For EV SSL, the background changes to green and the buttonized region is expanded to include the organization

name and country code. The biggest change in this new version is the handling of self-signed certificates; when a user navigates to a secure web site using a self-signed certificate, they are presented with a warning message that does not allow them to continue unless they create an exception for that particular site [10, 35].

While these changes may be an improvement over the original Firefox 3.0 Beta 1 used in this study, the findings of the study are apparently still very relevant to this newer Firefox version. Comments on a recent blog entry about the new identity indicator [10] indicate that many users will not be aware the button is clickable; the graphics techniques used to buttonize this region of the chrome have not changed greatly from what was done in Beta 1. There exists also the issue of accessibility in regard to the button background colours; colourblind users may not be able to distinguish the different states of the button. This was the reasoning behind our FF3mod *identity indicator* making use of one colour and conveying the difference in states by some other means. Finally, including the Organization name on the button for sites with EV certificates does cause the button to use a larger area of the chrome; however, if this does succeed in drawing user attention, the absence of this larger button on sites without EV certificates may not necessarily be noticed.

Chapter 7

Conclusions

While the introduction of Extended Validation SSL certificates was intended to help users make informed decisions regarding the identity and authenticity of a web site, the study carried out in this thesis shows that there are still many obstacles to overcome before this is realized. The challenge lies in the fact that many users do not currently have a good understanding of existing security cues in web browsers. It therefore appears difficult to incorporate new indicators into the browser chrome that will prove to be intuitive and effective.

7.1 Future Work in This Area

A natural extension of the study would be to evaluate user reactions to the indicators as a function of users being given increasingly more information before the study tasks. This could either be done by including more security implications in the introductory instructions, or by providing user education on EV SSL certificates before the study tasks. The hope would be to have more participants notice the identity indicators so

as to better evaluate their understanding and interpretations of the various states and their preferences for each indicator. A future field study would also be interesting to measure behavior over time as users become more aware of the EV SSL features to see whether these indicators would continue to aid them in their decision-making or whether they would eventually be dismissed.

One feature of the indicator that could not be studied was the information in the pop-up box triggered by clicking on the indicator (none of the participants attempted to interact with the indicators), and users' interpretation of the information presented by these boxes. Another natural aspect to study is the effect of the particular wording of this pop-up box as well as its behavior in the browser. Having the browser display a message pointing out the new features of this box might successfully draw the user's attention to the identity indicator. Another option might be to display the information box the first n times a user visits a given web site. These techniques would be intended to draw the user's attention to the dynamic functionality of the identity indicators, which was never discovered in our study.

7.2 Concluding Remarks

This thesis carried out the first known evaluation of the new identity indicators in the proposed Firefox 3.0 web browser, other than Mozilla's own user testing for which no user study has been published to our knowledge. In this study, the unmodified Firefox 3.0 Beta 1 browser cues failed to effectively convey the identity information, at least in the absence of additional user training or awareness. By introducing a modified design of the Firefox 3.0 Beta 1 browser, the number of users who reported noticing

an identity indicator increased to 15 of 28 (over 50% of the study participants) and three users showed immediate understanding of the indicator. However, to have users take notice of this new *identity confidence* button, more valuable space was used in the browser chrome.

Another contribution was the use of eye-tracking to cross-validate many aspects of the study, as well as providing empirical evidence with respect to the small amount of time users spend gazing at browser chrome. In general, participants in this study spent no more than 10% of their browsing time gazing at any region of the chrome, and often as little as 1% of their time. Regardless of the size of an identity indicator, many users tend to look to the content of the web site for security information rather than the browser chrome. This presents a challenge for browser interface designers who wish to provide to the user intuitive identity cues that will not go unnoticed. They need to ask how they can persuade users that the elements in the chrome are worth their attention, and how they can ensure that users will be able to distinguish legitimate indicators from spoofing attacks.

The study also showed that users who pay attention to indicators such as lock icons, *https*, and/or the new identity indicators show a tendency to value web sites that use SSL and de-value sites that do not employ SSL certificates. However, the fact that there were no statistically significant differences in willingness to transact with web sites having SSL vs. EV SSL certificates implies that the main goal of EV SSL certificates may be difficult to reach. Until users are aware that identity indicators exist in the browsers and are able to effectively interpret their meaning, it is possible that Extended Validation SSL certificates will have little effect on confidence in a web site and online security in general.

Bibliography

- [1] Anti-Phishing Working Group. Phishing activity trends report, Dec. 2007.
http://www.antiphishing.org/reports/apwg_report_dec_2007.pdf. [Accessed: May 27, 2008].
- [2] Apple. Safari. <http://www.apple.com/safari/>. [Accessed: May 21, 2008].
- [3] CA/Browser Forum. Guidelines for the issuance and management of extended validation certificates.
http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf. [Accessed: May 27, 2008].
- [4] N. Chou, R. Ledesma, Y. Teraguchi, and J. C. Mitchell. Client-side defense against web-based identity theft. In *11th Annual Network and Distributed System Security Symposium (NDSS '04)*, February 2004.
- [5] CoreStreet Ltd. Spooftick. <http://www.spooftick.com/>. [Accessed: May 27, 2008].
- [6] P. Damiano. Consumers have great expectations for online security.
http://www.banktech.com/aml/showArticle.jhtml?articleID=207800150&cid=RSSfeed_BankTech_News. [Accessed: May 25, 2008].

- [7] R. Dhamija and J. Tygar. The battle against phishing: Dynamic security skins. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '05)*, 2005.
- [8] R. Dhamija, J. Tygar, and M. Hearst. Why phishing works. In *Human Factors in Computing Systems (CHI 2006)*, April 22-27, 2006.
- [9] J. S. Downs, M. Holbrook, and L. Cranor. Decision strategies and susceptibility to phishing. In *Proceedings of the 2006 Symposium on Usable Privacy and Security*, July 2006.
- [10] dria.org Personal Webblog. Firefox 3: Site identification button. <http://www.dria.org/wordpress/archives/2008/05/06/635/>. [Accessed: May 25, 2008].
- [11] Earthlink Inc. Earthlink tool. <http://www.earthlink.net/software/free/tool>. [Accessed: May 27, 2008].
- [12] Entrust. Extended validation SSL certificates. <http://www.entrust.com/ev/index.htm>. [Accessed: April 7, 2008].
- [13] E. Felton, D. Balfanz, D. Dean, and D. Wallach. Web spoofing: An internet con game. In *Proceedings of the 20th National Information Systems Security Conference*, 1996.
- [14] R. Franco. Better website identification and extended validation certificates in IE7 and other browsers.

- <http://blogs.msdn.com/ie/archive/2005/11/21/495507.aspx>. [Accessed: April 7, 2008].
- [15] S. Garfinkel. *Web Security, Privacy and Commerce*. O'Reilly, Mahwah, N.J., 2002.
- [16] Geotrust Inc. Trustwatch toolbar. <http://toolbar.trustwatch.com>. [Accessed: May 27, 2008].
- [17] C. Gomes, M. Sellmann, C. Van Es, and H. Van Es. Computational methods for the generation of spatially balanced Latin squares. <http://www.cs.cornell.edu/gomes/SBLS.htm>. [Accessed: January 10, 2008].
- [18] S. Gorling. The myth of user education. In *16th Virus Bulletin International Conference*, 2006.
- [19] C. Grier, S. Tang, and S. T. King. Secure web browsing with the OP web browser. In *2008 IEEE Symposium on Security and Privacy*, May 18-21, 2008.
- [20] J. M. Henderson. Human gaze control during real-world scene perception. *Trends in Cognitive Sciences*, 7(11):498–504, November 2003.
- [21] A. Herzberg and A. Jbara. Security and identification indicators for browsers against spoofing and phishing attacks. <http://eprint.iacr.org/2004/155.pdf>. [Accessed: May 25, 2008].
- [22] C. Jackson, D. R. Simon, D. S. Tan, and A. Barth. An evaluation of extended validation and picture-in-picture phishing attacks. In *Proceedings of Usable Security (USEC '07)*, 2007.

- [23] K Desktop Environment. <http://www.kde.org>. [Accessed: April 7, 2008].
- [24] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Gaze-based password entry. In *Proceedings of the 2007 Symposium on Usable Privacy and Security*, 2007.
- [25] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge. Protecting people from phishing: The design and evaluation of an embedded training email system. In *Proceedings of the 2007 Computer Human Interaction (CHI 2007)*, 2007.
- [26] W. Liu, X. Deng, G. Huang, and A. Y. Fu. An antiphishing strategy based on visual similarity assessment. In *IEEE Internet Computing*, March/April 2006.
- [27] M. Mannan and P. C. van Oorschot. Using a personal device to strengthen password authentication from an untrusted computer. In *Financial Cryptography and Data Security (FC '07)*, Feb.12-15, 2007.
- [28] S. E. Maxwell and H. D. Delaney. *Designing experiments and analyzing data: A model comparison perspective (2nd ed.)*. Lawrence Erlbaum Associates, Mahwah, N.J., 2004.
- [29] R. McGill, J. W. Tukey, and W. A. Larsen. Variations of box plots. *The American Statistician*, 32(1):12–16, February 1978.
- [30] Microsoft. Extended validation SSL certificates.
<http://www.microsoft.com/windows/products/winfamily/ie/ev/default.aspx>.
[Accessed: April 7, 2008].

- [31] Microsoft. Internet Explorer 7.0 features.
<http://www.microsoft.com/windows/products/winfamily/ie/features.mspx>.
[Accessed: April 7, 2008].
- [32] Mozilla. EV-Certs for Firefox.
<http://mozillalinks.org/wp/2007/05/ev-certs-for-firefox/>. [Accessed: April 7, 2008].
- [33] Mozilla. Firefox web browser. <http://www.mozilla.com/en-US/firefox/>.
[Accessed: April 7, 2008].
- [34] Mozilla. Mozilla Firefox 3.0 beta 1 release notes.
<http://www.mozilla.com/en-US/firefox/3.0b1/releasenotes/secure/>. [Accessed: May 25, 2008].
- [35] Mozilla. Mozilla Firefox 3.0 release candidate 1 release notes.
<http://www.mozilla.com/en-US/firefox/3.0rc1/releasenotes/>. [Accessed: May 25, 2008].
- [36] Netcraft Ltd. Netcraft anti-phishing tollbar. <http://toolbar.netcraft.com/>.
[Accessed: April 7, 2008].
- [37] J. Nightingale. Personal Communication, September 19, 2007.
- [38] Y. Niu, F. Hsu, and H. Chen. iPhish: Phishing vulnerabilities on consumer electronics. In *Usability, Psychology and Security UPSEC '08*, April 14, 2008.
- [39] OpenSSL. <http://www.openssl.org/>. [Accessed: July '13, 2008].
- [40] Opera Software. <http://www.opera.com>. [Accessed: April 7, 2008].

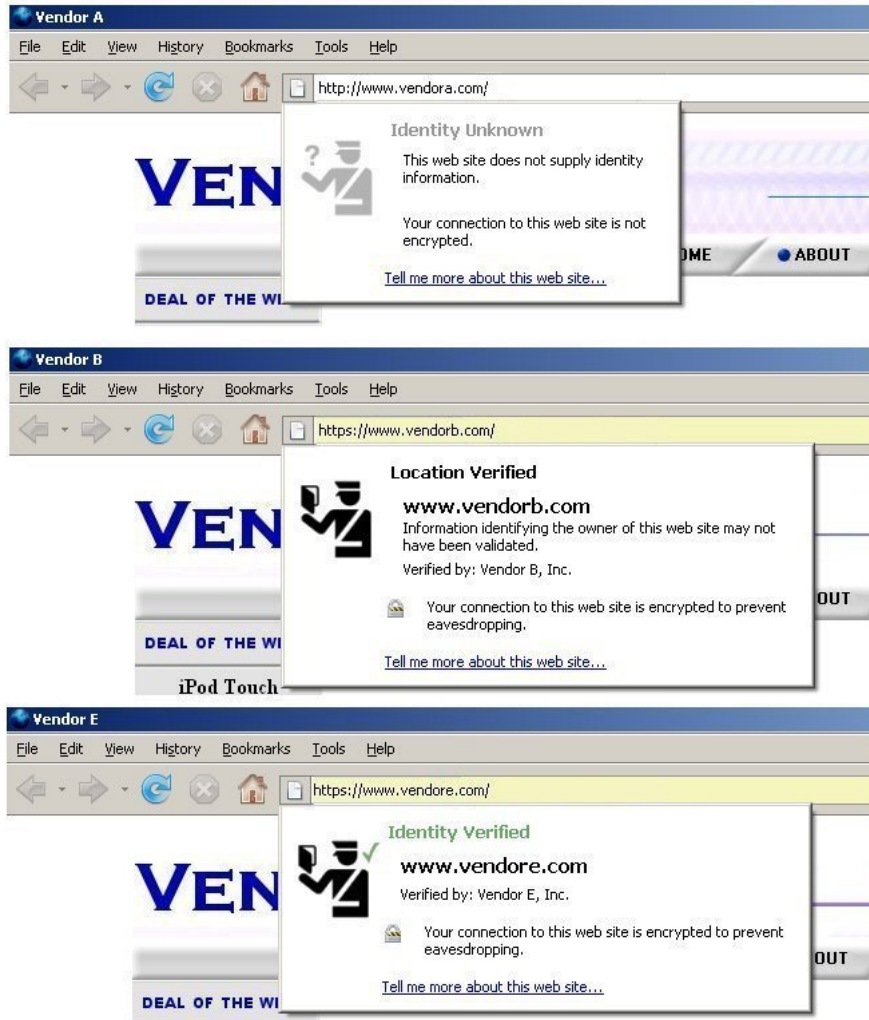
- [41] B. Parno, C. Kuo, and A. Perrig. Phoolproof phishing prevention. In *Proceedings of Financial Cryptography and Data Security (FC '06)*, 2006.
- [42] T. Ronda, S. Saroiu, and A. Wolman. iTrustPage: A user-assisted anti-phishing tool. In *Proceedings of the ACM European Conference on Computer Systems (EuroSys)*, April 2008.
- [43] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The emperor's new security indicators. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, May 2007.
- [44] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge. Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 2007 Symposium on Usable Privacy and Security*, 2007.
- [45] J. Sobey, R. Biddle, P. C. van Oorshot, and A. S. Patrick. Exploring user reactions to browser cues for extended validation certificates. Tech. Rep. School of Computer Science, Carleton University, TR08-10, June 2008.
- [46] Tobii Technology AB. <http://www.tobii.com>. [Accessed: January 10, 2008].
- [47] Verisign. Extended validation customers. <http://www.verisign.com/ssl/ssl-information-center/extended-validation-ssl/index.html>. [Accessed: April 7, 2008].

- [48] Verisign. Extended validation SSL certificates FAQ.
<http://www.verisign.com/ssl/ssl-information-center/faq/extended-validation-ssl-certificates.html>. [Accessed: April 7, 2008].
- [49] T. Whalen and K. Inkpen. Gathering evidence: Use of visual security cues in web browsing. In *Proceedings of Graphics Interface 2005*, pages 137–145, May 2005.
- [50] A. Whitten and J. D. Tygar. Why Johnny can’t encrypt: A usability case study of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, August 1999.
- [51] World Wide Web Consortium. <http://www.w3.org/>. [Accessed: May 25, 2008].
- [52] World Wide Web Consortium. Web security context: Experience, indicators, and trust (working draft 3 April 2008).
<http://www.w3.org/TR/wsc-xit/indicators>. [Accessed: May 25, 2008].
- [53] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Human Factors In Computing Systems (CHI 2006)*, 2006.
- [54] M. Wu, R. C. Miller, and G. Little. Web wallet: Preventing phishing attacks by revealing user intentions. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '06)*, 2006.
- [55] E. Z. Ye, Y. Yuan, and S. Smith. Web spoofing revisited: SSL and beyond. Tech. Rep. Department of Computer Science, Dartmouth College, TR2002-417.

- [56] Z. Ye, S. Smith, and D. Anthony. Trusted paths for browsers. *ACM Transactions on Information and System Security*, pages 153–186, May 2005.
- [57] Y. Zhang, J. Hong, and L. Cranor. CANTINA: a content-based approach to detecting phishing web sites. In *Proceedings of the 14th Annual Network and Distributed Systems Security Symposium (NDSS)*, 2007.

APPENDIX A

Firefox 3 Beta 1 Identity Information Pop-Up Boxes



This figure shows the text boxes corresponding to the different states of Firefox 3.0 Beta 1. The information pop-up box appears when users click on the identity indicator. The box on the top is for web sites with self-signed certificates or no certificate, the middle box is for web sites with traditional SSL certificates, and the bottom box is for web sites with an EV SSL certificate.

APPENDIX B

Web Site Screenshots

The image below is a screenshot of a sample web site used in the study. All 7 websites were intended to be similar in quality; therefore, we used the same web site and simply changed the vendor's name, the logo in the top right corner, the order of the products displayed on the home page, and the featured products along the left of the page. (Two additional home pages are displayed on the following page for comparison.)



Vendor A

File Edit View History Bookmarks Tools Help


Identity Confidence: <https://www.vendora.com/> Google

VENDOR A

HOME ABOUT CONTACT LINKS

DEAL OF THE WEEK WELCOME

G4 Dual 1.0 PM



Price: \$449

BEST SELLER

G4 Dual 1.25 PM



Price: \$799

APPLE DESKTOPS

PARTS AND ACCESSORIES

APPLE NOTEBOOKS

PERIPHERALS

IPODS

© 2007 Vendor A DESKTOPS | NOTEBOOKS | PERIPHERALS | ACCESSORIES | IPODS designed by TMLAT

Done www.vendora.com

Vendor E

File Edit View History Bookmarks Tools Help

Identity Confidence: <https://www.vendore.com/> Google

VENDOR E

HOME ABOUT CONTACT LINKS

DEAL OF THE WEEK WELCOME

iPod Classic



Price: \$349

BEST SELLER

G4 Dual 1.25 PM



Price: \$799

PERIPHERALS

IPODS

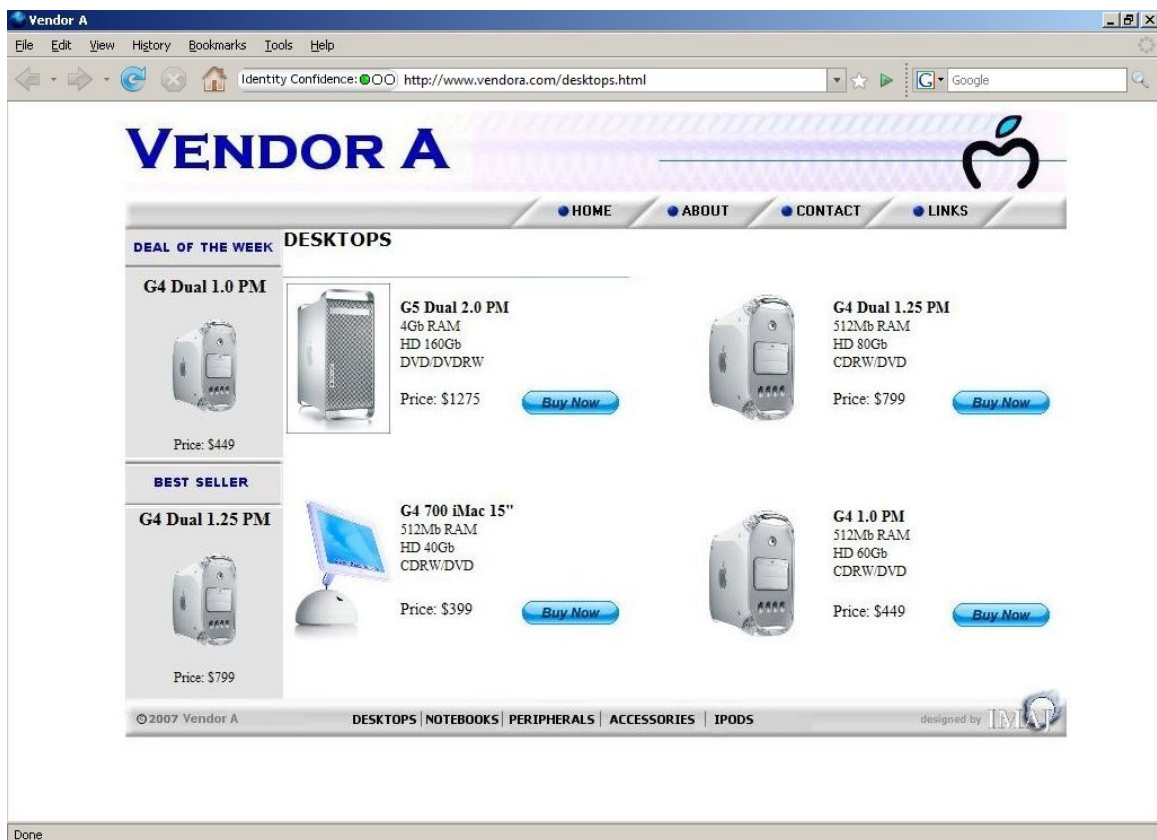
ACCESSORIES

APPLE NOTEBOOKS

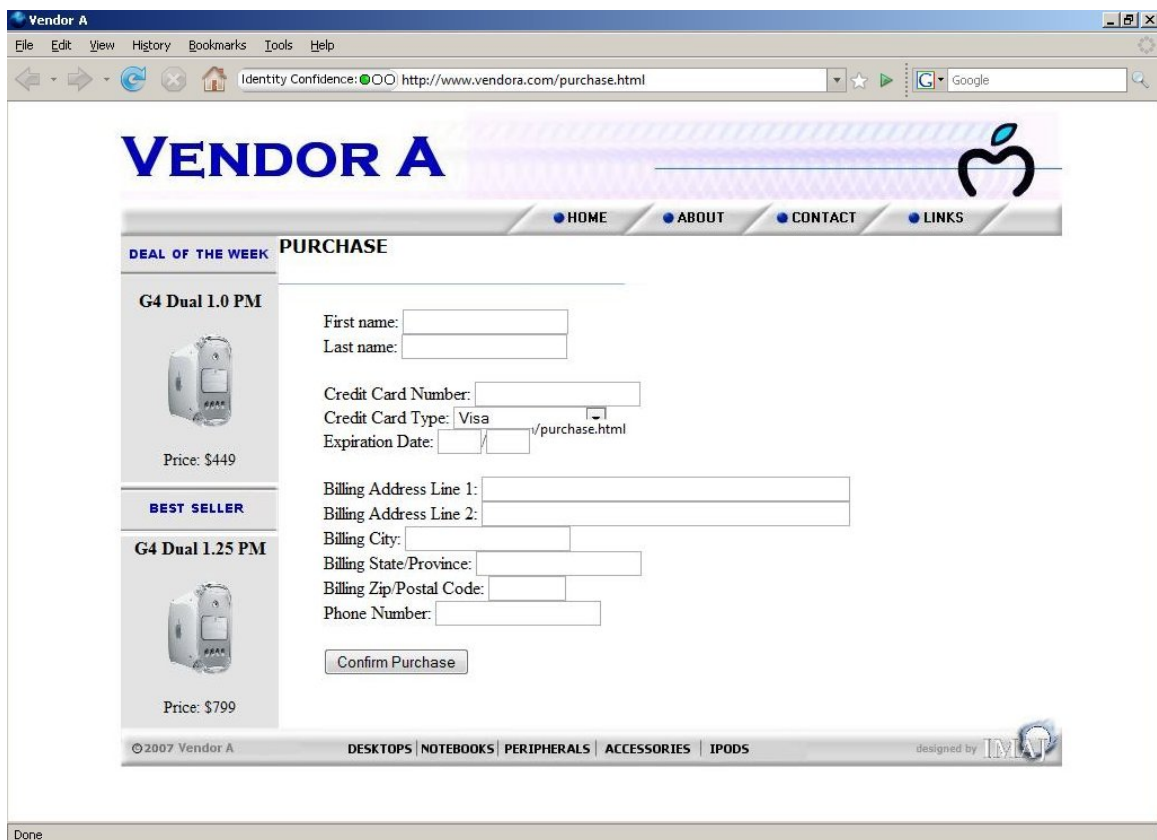
APPLE DESKTOPS

© 2007 Vendor E PERIPHERALS | NOTEBOOKS | IPODS | DESKTOPS | ACCESSORIES designed by TMLAT

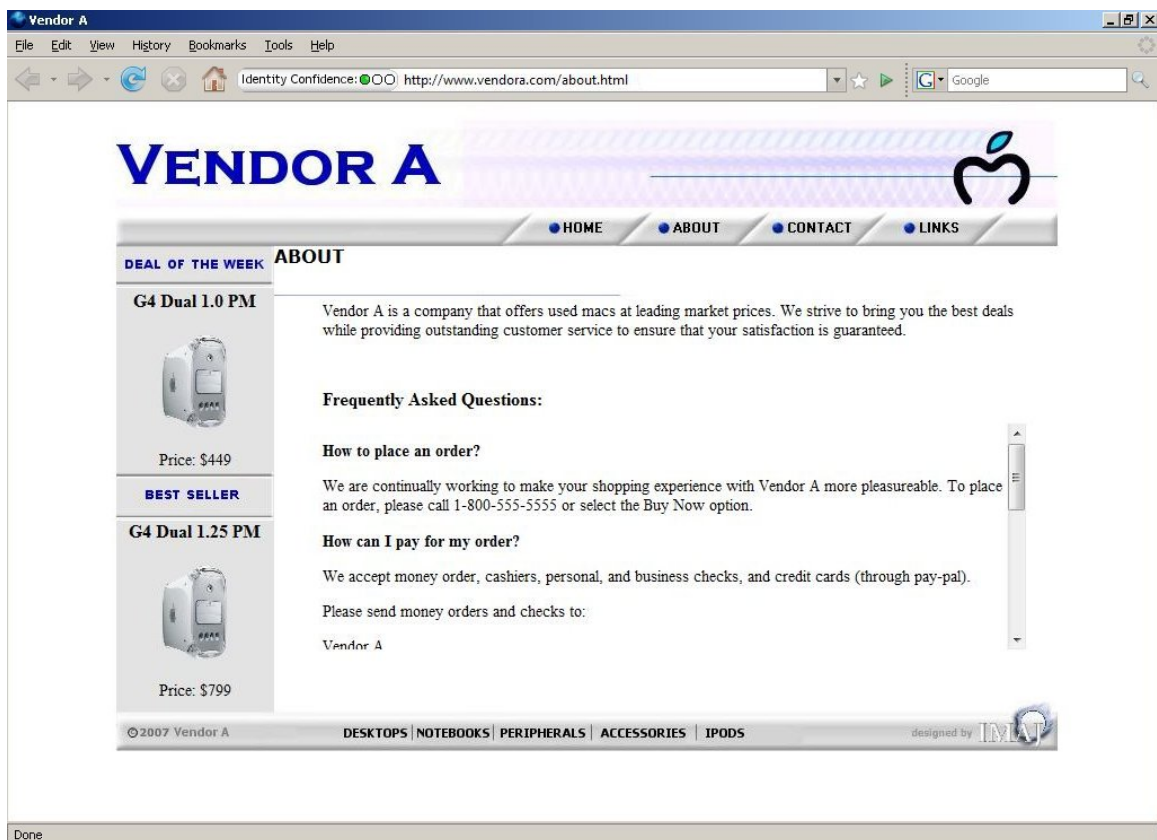
Done www.vendore.com



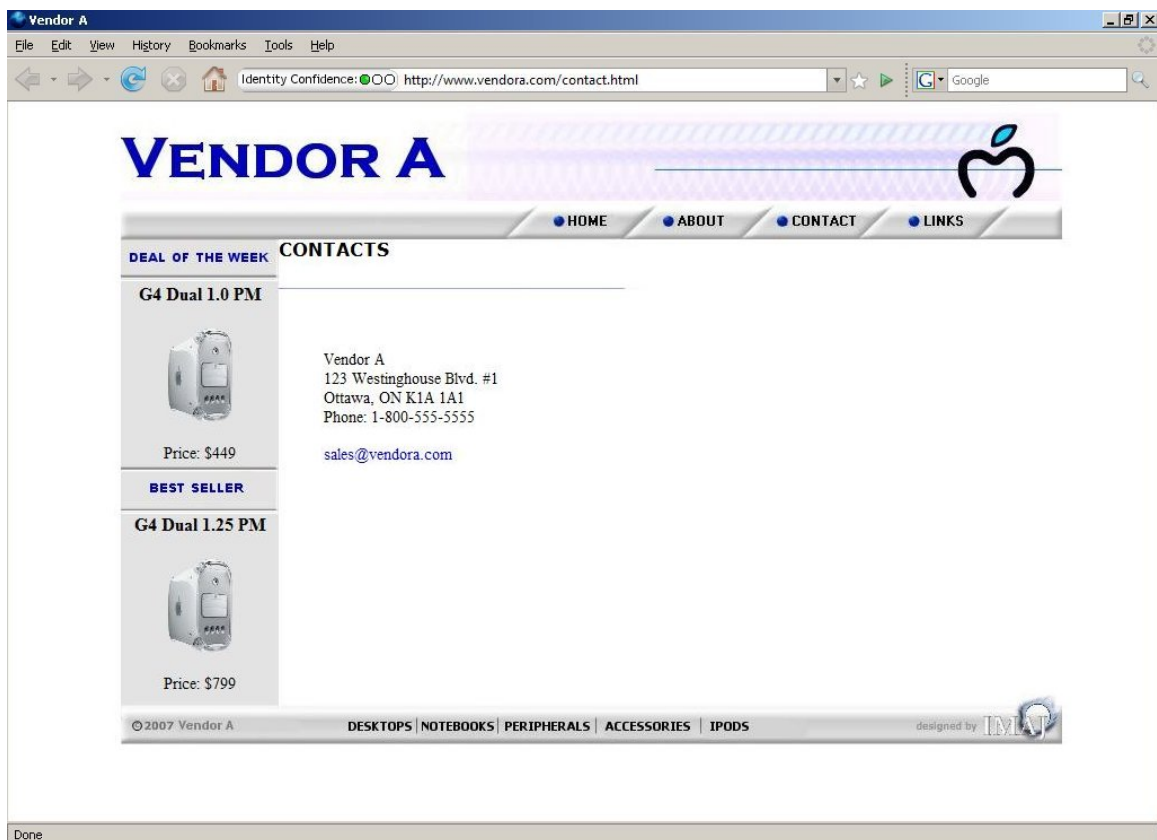
Sample page displaying available products in the “desktops” category. These were the pages participants viewed most during the study as they searched for product pricing.



Purchase page that would appear if any participant clicked on the “buy now” buttons. Proceeding with a purchase was not part of the study tasks; this page was simply included for completeness of the web site should any participant choose to click the buttons.



The “About Us” page that provided information about the vendor. Viewing this page was not a natural part of the study tasks, but many participants navigated to this page as they were asked about their “willingness to transact.”



The “Contact Us” page that provided contact information for the vendor. Again, this was not seen during any part of the study tasks but was often viewed by participants as they made decisions about “willingness to transact.”

APPENDIX C

User Study Documents

Informed Consent Document
Usability Test Instructions
Usability Test Tasks
Post-Task Questions
Post-Task Interview
Participant Demographics Document

Informed Consent

Thank you very much for agreeing to participate in this research. The purpose of an informed consent is to ensure that you understand the purpose of the study and the nature of your involvement. This informed consent must give enough information for you to decide whether or not you want to participate in the study. Contact information is provided below.

Concerns about the research topic or methods:

- Jennifer Sobey, principal researcher, 613-520-2600 X 4340,
jsobey@connect.carleton.ca
- Dr. Robert Biddle - 613-520-2600 X 6317, robert_biddle@carleton.ca
- Dr. Paul Van Oorschot - 613-520-2600 X 4356, paulv@scs.carleton.ca
- Dr. Andrew Patrick - 613-277-9211, andrew@andrewpatrick.ca

Concerns about the ethics of this study:

- Dr. Avi Parush, chair of Carleton University Ethics Committee for
Psychological Research, 613-520-2600 X 6026, avi_parush@carleton.ca
- Dr. Anne Bowker, Departmental Chair of Psychology at Carleton University,
613-520-2600 X 2648, psychchair@carleton.ca

Research Purpose: The purpose of this study is to investigate some new web browsers and websites for use in Internet shopping. We want to evaluate their usability and effectiveness for web browsing.

Task Requirements: During this study, we will ask you to visit six (6) different websites and perform a series of tasks relating to online shopping. We will encourage you to think aloud as you perform these tasks. When the tasks are completed, we will conduct a short interview to gather information about your opinions about the sites you have seen.

Duration and locale: The study will take approximately one hour. It will be conducted in the HOT Lab located in room 214 SSRB.

Ethics Approval: This research has been reviewed and approved by the Carleton University Ethics Committee for Psychological Research.

Potential risk/discomfort: There are no potential physical or psychological risks.

Right to withdraw: You have the right to withdraw at any time or ask me to restrict my research activity without any consequences to you. *Anonymity/Confidentiality:* All data that is collected will be held completely confidential. The data will only be made available to those people involved with this testing. Data will be coded for identification purposes.

Eye Tracking: The computer used during this study is equipped with an eye tracking device that records eye movements across the screen.

I am aware that the reason for informed consent is to make sure that I understand why the study is being done and what my rights are. My signature below indicates that I have read the above information and that I agree to take part in this study.

Signature (participant): _____

Signature (researcher): _____

Date: _____

Usability Test Instructions

This usability test is designed to test new browsers and websites for Internet shopping. Please keep in mind that you are not being tested; I am testing the effectiveness of the software. I will be asking you to complete a series of tasks and would like you to think aloud while you try to complete them. Don't worry if you can't find the correct answers every time. If you become frustrated with a task, just let us know and you can simply move on to the next. The session will take about an hour.

The first step in this study will involve visiting seven (7) different links in order to complete the seven (7) tasks on your worksheet. Once you have completed the tasks, I will conduct a short interview with you to gather your opinions about the websites you visited. (*Group 2 only*: I am interested in such things as visual appearance, item pricing, amount of contact details, trust in the site's authenticity, and ease of use.)

Do you have any questions?

Usability Test Tasks

Task #1:

- Imagine you are in need of a new laptop computer. You have researched different models and settled on a MacBook that has everything you want.
- While making this purchase, you also decide to buy a mouse for the laptop and an iPod.
- Double-click on “task #1” on the screen to visit a website that sells these 3 products. Locate each item and record the prices in the spaces below.

1. \$_____MacBook Pro Intel Core Duo 1.83GHz 15” Notebook (512Mb RAM, HD 80Gb, DVD-R)
2. \$_____Apple Pro Mouse
3. \$_____iPod Nano

Task #2:

- Imagine your home computer has just died and you decide to purchase a new desktop instead of repairing it.
- You also decide to replace your keyboard with a new wireless version and also want an iPod.
- Double-click on “task #2” on the screen to visit a website that sells these 3 products. Locate each item and record the prices in the spaces below.

1. \$_____G4 Dual 1.25 PM Desktop (512Mb RAM, HD 80Gb,
CDRW/DVD)

2. \$_____Wireless Bluetooth Pro Keyboard

3. \$_____iPod Shuffle

Task #3:

- Imagine you have been asked to purchase a new laptop for work, and can add any accessories you like.
 - You decide to buy a mouse for the laptop and an iPod.
 - Double-click on “task #3” on the screen to visit a website that sells these 3 products. Locate each item and record the prices in the spaces below.
1. \$_____G4 1.0 PowerBook 17” Notebook (512Mb RAM, HD 80Gb, DVDRW)
 2. \$_____Apple Mighty Mouse
 3. \$_____iPod Classic

Task #4:

- Imagine you are buying your first computer and you also need a monitor to go with it. (Note that monitors can sometimes be referred to as peripherals).
 - You also decide you want to buy an iPod at the same time.
 - Double-click on “task #4” on the screen to visit a website that sells these 3 products. Locate each item and record the prices in the spaces below.
1. \$_____G5 Dual 2.0 PM Desktop (4 Gb RAM, HD 160Gb,
DVD/DVDRW)
 2. \$_____17LCD Studio Display
 3. \$_____iPod Touch

Task #5:

- Imagine that you are buying a new laptop, but the model you want doesn't have enough memory for the games you wish to play.
- You decide to buy an extra memory card to go with it, as well as an iPod Shuffle.
- Double-click on "task #5" on the screen to visit a website that sells these 3 products. Locate each item and record the prices in the spaces below.

1. \$_____G4 1.67 PowerBook 15" Notebook (512Mb RAM, HD 80Gb, DVDRW)
2. \$_____1 GB PC2700 (Extra memory card)
3. \$_____iPod Shuffle

Task #6:

- Imagine you have decided to upgrade your home computer and know which new model you want to buy.
- You also decided to buy a new wireless mouse for it and a new iPod.
- Double-click on “task #6” on the screen to visit a website that sells these 3 products. Locate each item and record the prices in the spaces below.

1. \$_____G4 700 iMac 15” Desktop (512Mb RAM, HD 40Gb,
CDRW/DVD)

2. \$_____Wireless Bluetooth Pro Mouse

3. \$_____iPod Touch

Task #7:

- Imagine you need a new laptop computer but dislike typing on the small keyboards.
 - You decide to buy an external keyboard to plug into it and an iPod as well.
 - Double-click on “task #7” on the screen to visit a website that sells these 3 products. Locate each item and record the prices in the spaces below.
1. \$_____MacBook Pro Intel Core Duo 2.16GHz 17” Notebook (1Gb RAM, HD 120 Gb, DVD-R)
 2. \$_____Apple Pro Keyboard
 3. \$_____iPod Nano

Post Test Questions

Two questions were asked after each of the seven tasks:

1. On a scale of 1 to 10, where '1' means "definitely not willing" and '10' means "definitely willing," how willing would you be to make purchases on this website with your own credit card?
2. What factors did you use to make your decision about how willing you would be to make purchases on this website?

Participants were asked to circle the answer for question #1 on a sheet provided to them and responded orally to question #2.

Post Task Interview

The following questions were asked orally of participants once all seven tasks were completed:

1. How did the browsers used today compare to the browser you use at home?
2. Did these browsers provide you with less information, more information, or about the same amount of information as the browser you use at home?
3. Did you notice any differences between the browsers used in the study today?
(If so, what was different?)
4. Did you notice the presence of this identity indicator and pop-up information box? (FF3 indicator shown to the participant). If yes, on how many of the websites do you recall having this indicator shown? Did you notice any changes in this indicator when you visited different websites?
5. Did you notice the presence of this identity indicator and pop-up information box? (FF3mod indicator shown to the participant). If yes, on how many of the websites do you recall having this indicator shown? Did you notice any changes in this indicator when you visited different websites?
6. If you were asked to use one of these browsers for your everyday web browsing and online shopping, which would you prefer to use? Why?

The order of questions 4 and 5 were chosen randomly so that half of the participants were shown the FF3 indicator first and the other half were shown the FF3mod indicator first.

Participant Demographics Document

The information provided on this form will be kept completely confidential. **Please do not put your name anywhere on this form.**

1. **Age:** ____ years old

2. **Gender:** Male Female

3. **What is your current level of education?**

High School

College/technical school

Undergraduate degree

Master's degree

PhD degree

4. **Please indicate whether or not your current education level has been completed:**

In Progress/Incomplete

Completed

If currently a student:

5. **What year of your program are you in?** (Please enter the number, eg: 3rd)

6. **Which category best describes your current program?**

Computer Science & Engineering

Arts & Social Sciences

Natural Sciences (Eg: Chemistry, Biology, etc.)

Business & Public Affairs

Other, please specify: _____

7. How many hours per week do you typically spend using the Internet?

less than 1 hour

1-5 hours

5-10 hours

10-20 hours

more than 20 hours

8. Which web browser do you use most often?

 Internet Explorer

 Mozilla Firefox

 Apple Safari

 Opera

 KDE Konqueror

Other - specify: _____

9. How often do you make purchases online?

Never

Rarely

Several times per year

About once a month

Several times per month

About once a week

Several times per week

Every day

10. On a scale from 1 to 10, where '1' means "not at all concerned" and '10' means "extremely concerned," how concerned are you about the security of your information/credit card number when making purchases online? *(Please circle the appropriate number)*

(Not at all Concerned) 1 2 3 4 5 6 7 8 9 10 (Very Concerned)

11. How do you typically decide if a website is secure enough to enter your credit card information?

12a. Prior to today, have you heard of the term "certificate" in reference to website security?

Yes No

12b. If yes, what is your understanding of what a certificate is?

12c. How do you know if a website has a certificate?

13a. Prior to today, have you ever heard of the term "phishing"?

Yes No

13b. If yes, what is your understanding of what phishing is?

APPENDIX D

Firefox 3 Beta 1 Source Code Modifications

The following changes were made to the Windows source code files for Firefox 3.0

Beta 1:

Browser\Base\Content\browser.js:

Changed lines 10, 13, and 15 so that all three were set to the appropriate mode for the particular version of the browser. For the interface that was hard coded to always show the non-SSL state, all three lines were set to `IDENTITY_MODE_UNKNOWN`. Similarly, these lines were all set to `IDENTITY_MODE_DOMAIN_VERIFIED` for the SSL state and to `IDENTITY_MODE_IDENTIFIED` for the EV-SSL state.

```
/**
 * Determine the identity of the page being displayed by examining
 * its SSL cert(if available) and, if necessary, update the UI to
 * reflect this. Intended to be called by onSecurityChange
 *
 * @param PRUint32 state
 * @param AUTF8String host
 */
1  checkIdentity : function(state, host) {
2      var currentStatus = gBrowser.securityUI
3          .QueryInterface(Components.interfaces.nsISSLStatus
4              Provider).SSLStatus;
5      this._lastStatus = currentStatus;
6      this._lastHost = host;
7
8      if (state & Components.interfaces.nsIWebProgressListener.
9          STATE_IDENTITY_EV_TOPLEVEL)
10         this.setMode(this.IDENTITY_MODE_IDENTIFIED);
11     else if (state & Components.interfaces.nsIWebProgressListener.
12         STATE_SECURE_HIGH)
13         this.setMode(this.IDENTITY_MODE_DOMAIN_VERIFIED);
14     else
```

```
15     this.setMode(this.IDENTITY_MODE_UNKNOWN);  
16 }
```

Browser\Themes\Winstripe\Browser\jar.mn: Added the line “skin/classic/browser/identitybar.png” so that the appropriate image file for the new *identity confidence* indicator would be included in the build.

Browser\Themes\Winstripe\Browser\browser.css: Changed lines 7, 11 and 15 in the code below to reflect the appropriate color for the title in the identity information drop-down box: grey for the non-SSL interface (#999), black for the SSL interface, and green for the EV-SSL interface (#6A6). For all interfaces, line 20 was changed from 16px to 144px and line 21 was changed from 16px to 20px to reflect the size of the *identity confidence* indicator. Margines set in line 26 were both changed to 0, and line 34 was changed to point to the image file for the *identity confidence* indicator.

```
/* Popup Title */
1 #identity-popup-title {
2     font-size: 120%;
3     font-weight: bold;
4 }
5
6 .verifiedIdentity > #identity-popup-title {
7     color: #6A6;
8 }
9
10 .unknownIdentity > #identity-popup-title {
11     color: #999;
12 }
13
14 .verifiedDomain > #identity-popup-title {
15     color: black;
16 }

/* ::::: page proxy icon ::::: */

17 #page-proxy-deck,
18 #page-proxy-favicon,
```

```
19 #page-proxy-button {
20   width: 16px;
21   height: 16px;
22 }
23
24 #page-proxy-deck {
25   cursor: -moz-grab;
26   margin: 2px 3px;
27 }
28
29 #page-proxy-favicon {
30   list-style-image: none;
31 }
32
33 #page-proxy-button {
34   list-style-image: url("chrome://global/skin/icons/
35   folder-item.png") !important;
36 }
```


Browser\Locales\EN_US\Chrome\Browser\browser.properties: For the non-SSL version of the interface, lines 1-3 and 5-11 were modified to contain the same information as in lines 13-15. Lines 17 and 18 was also changed to contain the same message as line 19 and 20. For the SSL and EV-SSL versions of the interface, lines 17 and 19 both contained the message from line 17. In the SSL version, lines 5-11 and 13-15 were modified to contain the same information as lines 1-3, and similarly for the EV-SSL version, lines 1-3 and 13-15 were modified to contain the same messages as lines 5-11.

```
# Identity information
1 identity.domainverified.title=Identity Verified
2 identity.domainverified.body=This web site is owned by:
3 identity.domainverified.supplemental=
4
5 identity.identified.title=Location Verified
6 identity.identified.body=You are currently visiting:
7 identity.identified.supplemental=Information identifying the owner
8   of this web site may not have been validated.
9 identity.identified.verifier=Verified by: %S
10 identity.identified.state_and_country=%S, %S
11 identity.identified.title_with_country=%S (%S)
12
13 identity.unknown.title=Identity Unknown
14 identity.unknown.body=This web site does not supply identity
15   information.
16
17 identity.encrypted=Your connection to this web site is
18   encrypted to prevent eavesdropping.
19 identity.unencrypted=Your connection to this web site is
20   not encrypted.
```

APPENDIX E

Raw Willingness to Transact Data

Field Descriptions

PART: Participant Number

GROUP: Group Condition (1=limited instruction, 2=enhanced instructions)

BROWSER: Browser (FF2=Firefox 2, FF3=Firefox 3, FF3mod=modified Firefox 3)

STATE: SSL State (NON=non-SSL state, SSL=SSL state, EV=EV-SSL state)

INTERFACE: Interface (Browser and State fields combined)

RATING: Willingness to transact rating assigned to the interface (1-low, 10-high)

GAZER: Classification as gazer or non-gazer (yes=gazer, no=non-gazer)

PART	GROUP	BROWSER	STATE	INTERFACE	RATING	GAZER
P001	1	FF2	SSL	FF2_SSL	4	yes
P001	1	FF3	NON	FF3_NON	3	yes
P001	1	FF3	SSL	FF3_SSL	4	yes
P001	1	FF3	EV	FF3_EV	4	yes
P001	1	FF3M	NON	FF3M_NON	2	yes
P001	1	FF3M	SSL	FF3M_SSL	4	yes
P001	1	FF3M	EV	FF3M_EV	4	yes
P002	1	FF2	SSL	FF2_SSL	2	no
P002	1	FF3	NON	FF3_NON	2	no
P002	1	FF3	SSL	FF3_SSL	2	no
P002	1	FF3	EV	FF3_EV	2	no
P002	1	FF3M	NON	FF3M_NON	2	no
P002	1	FF3M	SSL	FF3M_SSL	2	no
P002	1	FF3M	EV	FF3M_EV	2	no
P003	1	FF2	SSL	FF2_SSL	8	no
P003	1	FF3	NON	FF3_NON	7	no
P003	1	FF3	SSL	FF3_SSL	7	no
P003	1	FF3	EV	FF3_EV	8	no
P003	1	FF3M	NON	FF3M_NON	6	no
P003	1	FF3M	SSL	FF3M_SSL	7	no
P003	1	FF3M	EV	FF3M_EV	8	no
P004	1	FF2	SSL	FF2_SSL	4	yes
P004	1	FF3	NON	FF3_NON	2	yes
P004	1	FF3	SSL	FF3_SSL	5	yes
P004	1	FF3	EV	FF3_EV	1	yes
P004	1	FF3M	NON	FF3M_NON	1	yes
P004	1	FF3M	SSL	FF3M_SSL	3	yes
P004	1	FF3M	EV	FF3M_EV	4	yes
P005	1	FF2	SSL	FF2_SSL	1	yes
P005	1	FF3	NON	FF3_NON	2	yes
P005	1	FF3	SSL	FF3_SSL	1	yes
P005	1	FF3	EV	FF3_EV	3	yes
P005	1	FF3M	NON	FF3M_NON	2	yes
P005	1	FF3M	SSL	FF3M_SSL	4	yes
P005	1	FF3M	EV	FF3M_EV	1	yes
P006	1	FF2	SSL	FF2_SSL	1	yes
P006	1	FF3	NON	FF3_NON	4	yes
P006	1	FF3	SSL	FF3_SSL	1	yes
P006	1	FF3	EV	FF3_EV	3	yes
P006	1	FF3M	NON	FF3M_NON	3	yes
P006	1	FF3M	SSL	FF3M_SSL	4	yes
P006	1	FF3M	EV	FF3M_EV	4	yes
P007	1	FF2	SSL	FF2_SSL	4	yes
P007	1	FF3	NON	FF3_NON	2	yes
P007	1	FF3	SSL	FF3_SSL	3	yes
P007	1	FF3	EV	FF3_EV	3	yes
P007	1	FF3M	NON	FF3M_NON	2	yes
P007	1	FF3M	SSL	FF3M_SSL	4	yes
P007	1	FF3M	EV	FF3M_EV	10	yes

PART	GROUP	BROWSER	STATE	INTERFACE	RATING	GAZER
P008	2	FF2	SSL	FF2_SSL	8	no
P008	2	FF3	NON	FF3_NON	8	no
P008	2	FF3	SSL	FF3_SSL	8	no
P008	2	FF3	EV	FF3_EV	8	no
P008	2	FF3M	NON	FF3M_NON	8	no
P008	2	FF3M	SSL	FF3M_SSL	8	no
P008	2	FF3M	EV	FF3M_EV	8	no
P009	2	FF2	SSL	FF2_SSL	3	no
P009	2	FF3	NON	FF3_NON	3	no
P009	2	FF3	SSL	FF3_SSL	3	no
P009	2	FF3	EV	FF3_EV	3	no
P009	2	FF3M	NON	FF3M_NON	3	no
P009	2	FF3M	SSL	FF3M_SSL	3	no
P009	2	FF3M	EV	FF3M_EV	3	no
P010	2	FF2	SSL	FF2_SSL	7	no
P010	2	FF3	NON	FF3_NON	7	no
P010	2	FF3	SSL	FF3_SSL	7	no
P010	2	FF3	EV	FF3_EV	6	no
P010	2	FF3M	NON	FF3M_NON	4	no
P010	2	FF3M	SSL	FF3M_SSL	6	no
P010	2	FF3M	EV	FF3M_EV	5	no
P011	2	FF2	SSL	FF2_SSL	7	no
P011	2	FF3	NON	FF3_NON	8	no
P011	2	FF3	SSL	FF3_SSL	8	no
P011	2	FF3	EV	FF3_EV	6	no
P011	2	FF3M	NON	FF3M_NON	5	no
P011	2	FF3M	SSL	FF3M_SSL	7	no
P011	2	FF3M	EV	FF3M_EV	7	no
P012	2	FF2	SSL	FF2_SSL	8	yes
P012	2	FF3	NON	FF3_NON	2	yes
P012	2	FF3	SSL	FF3_SSL	8	yes
P012	2	FF3	EV	FF3_EV	10	yes
P012	2	FF3M	NON	FF3M_NON	1	yes
P012	2	FF3M	SSL	FF3M_SSL	8	yes
P012	2	FF3M	EV	FF3M_EV	10	yes
P013	2	FF2	SSL	FF2_SSL	5	no
P013	2	FF3	NON	FF3_NON	5	no
P013	2	FF3	SSL	FF3_SSL	5	no
P013	2	FF3	EV	FF3_EV	5	no
P013	2	FF3M	NON	FF3M_NON	5	no
P013	2	FF3M	SSL	FF3M_SSL	5	no
P013	2	FF3M	EV	FF3M_EV	5	no
P014	2	FF2	SSL	FF2_SSL	1	yes
P014	2	FF3	NON	FF3_NON	1	yes
P014	2	FF3	SSL	FF3_SSL	4	yes
P014	2	FF3	EV	FF3_EV	4	yes
P014	2	FF3M	NON	FF3M_NON	1	yes
P014	2	FF3M	SSL	FF3M_SSL	4	yes
P014	2	FF3M	EV	FF3M_EV	4	yes

PART	GROUP	BROWSER	STATE	INTERFACE	RATING	GAZER
P015	2	FF2	SSL	FF2_SSL	1	no
P015	2	FF3	NON	FF3_NON	1	no
P015	2	FF3	SSL	FF3_SSL	1	no
P015	2	FF3	EV	FF3_EV	1	no
P015	2	FF3M	NON	FF3M_NON	1	no
P015	2	FF3M	SSL	FF3M_SSL	1	no
P015	2	FF3M	EV	FF3M_EV	1	no
P016	1	FF2	SSL	FF2_SSL	8	no
P016	1	FF3	NON	FF3_NON	4	no
P016	1	FF3	SSL	FF3_SSL	4	no
P016	1	FF3	EV	FF3_EV	4	no
P016	1	FF3M	NON	FF3M_NON	4	no
P016	1	FF3M	SSL	FF3M_SSL	2	no
P016	1	FF3M	EV	FF3M_EV	7	no
P017	2	FF2	SSL	FF2_SSL	8	no
P017	2	FF3	NON	FF3_NON	8	no
P017	2	FF3	SSL	FF3_SSL	6	no
P017	2	FF3	EV	FF3_EV	8	no
P017	2	FF3M	NON	FF3M_NON	8	no
P017	2	FF3M	SSL	FF3M_SSL	7	no
P017	2	FF3M	EV	FF3M_EV	7	no
P018	1	FF2	SSL	FF2_SSL	6	no
P018	1	FF3	NON	FF3_NON	6	no
P018	1	FF3	SSL	FF3_SSL	6	no
P018	1	FF3	EV	FF3_EV	6	no
P018	1	FF3M	NON	FF3M_NON	6	no
P018	1	FF3M	SSL	FF3M_SSL	6	no
P018	1	FF3M	EV	FF3M_EV	6	no
P019	2	FF2	SSL	FF2_SSL	3	no
P019	2	FF3	NON	FF3_NON	3	no
P019	2	FF3	SSL	FF3_SSL	3	no
P019	2	FF3	EV	FF3_EV	3	no
P019	2	FF3M	NON	FF3M_NON	3	no
P019	2	FF3M	SSL	FF3M_SSL	3	no
P019	2	FF3M	EV	FF3M_EV	3	no
P020	1	FF2	SSL	FF2_SSL	8	yes
P020	1	FF3	NON	FF3_NON	1	yes
P020	1	FF3	SSL	FF3_SSL	9	yes
P020	1	FF3	EV	FF3_EV	9	yes
P020	1	FF3M	NON	FF3M_NON	1	yes
P020	1	FF3M	SSL	FF3M_SSL	9	yes
P020	1	FF3M	EV	FF3M_EV	9	yes
P021	2	FF2	SSL	FF2_SSL	6	no
P021	2	FF3	NON	FF3_NON	6	no
P021	2	FF3	SSL	FF3_SSL	6	no
P021	2	FF3	EV	FF3_EV	6	no
P021	2	FF3M	NON	FF3M_NON	6	no
P021	2	FF3M	SSL	FF3M_SSL	6	no
P021	2	FF3M	EV	FF3M_EV	6	no

PART	GROUP	BROWSER	STATE	INTERFACE	RATING	GAZER
P022	1	FF2	SSL	FF2_SSL	6	no
P022	1	FF3	NON	FF3_NON	6	no
P022	1	FF3	SSL	FF3_SSL	6	no
P022	1	FF3	EV	FF3_EV	6	no
P022	1	FF3M	NON	FF3M_NON	6	no
P022	1	FF3M	SSL	FF3M_SSL	6	no
P022	1	FF3M	EV	FF3M_EV	6	no
P023	2	FF2	SSL	FF2_SSL	4	no
P023	2	FF3	NON	FF3_NON	3	no
P023	2	FF3	SSL	FF3_SSL	1	no
P023	2	FF3	EV	FF3_EV	4	no
P023	2	FF3M	NON	FF3M_NON	3	no
P023	2	FF3M	SSL	FF3M_SSL	1	no
P023	2	FF3M	EV	FF3M_EV	6	no
P024	1	FF2	SSL	FF2_SSL	1	no
P024	1	FF3	NON	FF3_NON	1	no
P024	1	FF3	SSL	FF3_SSL	1	no
P024	1	FF3	EV	FF3_EV	4	no
P024	1	FF3M	NON	FF3M_NON	1	no
P024	1	FF3M	SSL	FF3M_SSL	4	no
P024	1	FF3M	EV	FF3M_EV	1	no
P025	2	FF2	SSL	FF2_SSL	8	yes
P025	2	FF3	NON	FF3_NON	6	yes
P025	2	FF3	SSL	FF3_SSL	8	yes
P025	2	FF3	EV	FF3_EV	8	yes
P025	2	FF3M	NON	FF3M_NON	8	yes
P025	2	FF3M	SSL	FF3M_SSL	7	yes
P025	2	FF3M	EV	FF3M_EV	7	yes
P026	1	FF2	SSL	FF2_SSL	8	yes
P026	1	FF3	NON	FF3_NON	7	yes
P026	1	FF3	SSL	FF3_SSL	7	yes
P026	1	FF3	EV	FF3_EV	8	yes
P026	1	FF3M	NON	FF3M_NON	8	yes
P026	1	FF3M	SSL	FF3M_SSL	8	yes
P026	1	FF3M	EV	FF3M_EV	8	yes
P027	2	FF2	SSL	FF2_SSL	6	yes
P027	2	FF3	NON	FF3_NON	8	yes
P027	2	FF3	SSL	FF3_SSL	8	yes
P027	2	FF3	EV	FF3_EV	8	yes
P027	2	FF3M	NON	FF3M_NON	8	yes
P027	2	FF3M	SSL	FF3M_SSL	8	yes
P027	2	FF3M	EV	FF3M_EV	9	yes
P028	1	FF2	SSL	FF2_SSL	8	no
P028	1	FF3	NON	FF3_NON	7	no
P028	1	FF3	SSL	FF3_SSL	9	no
P028	1	FF3	EV	FF3_EV	8	no
P028	1	FF3M	NON	FF3M_NON	8	no
P028	1	FF3M	SSL	FF3M_SSL	8	no
P028	1	FF3M	EV	FF3M_EV	8	no