Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study

Robert Biddle
robert_biddle@carleton.ca

P.C. van Oorschot
paulv@scs.carleton.ca

Andrew S. Patrick
andrew@andrewpatrick.ca

Jennifer Sobey
jsobey@connect.carleton.ca

Tara Whalen*
tjwhalen@gmail.com

School of Computer Science
Carleton University
Ottawa, Ontario, Canada

ABSTRACT

There has been a loss of confidence in the security provided by SSL certificates and browser interfaces in the face of various attacks. As one response, basic SSL server certificates are being demoted to second-class status in conjunction with the introduction of Extended Validation (EV) SSL certificates. Unfortunately, EV SSL certificates may complicate the already difficult design challenge of effectively conveying certificate information to the average user. This study explores the interfaces related to SSL certificates in the most widely deployed browser (Internet Explorer 7), proposes an alternative set of interface dialogs, and compares their effectiveness through a user study involving 40 participants. The alternative interface was found to offer statistically significant improvements in confidence, ease of finding information, and ease of understanding. Such results from a modest re-design effort suggest considerable room for improvement in the user interfaces of browsers today. This work motivates further study of whether EV SSL certificates offer a robust foundation for improving Internet trust, or a further compromise to usable security for ordinary users.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Authentication*; H.4.3 [**Information Systems Applications**]: Communication Applications—*Information Browsers*

General Terms

Security, Human Factors, Design, Experimentation

*Corresponding author. This paper updates a July 2009 technical report[19].

CCSW'09, November 13, 2009, Chicago, Illinois, USA.

Keywords

usability and security, SSL certificates, extended validation, web site identity, user study, browser user interfaces

1. INTRODUCTION

SSL certificates were introduced in 1995 to secure the transfer of information between a client browser and web server. Now, almost fifteen years later, there has been considerable loss of confidence in the level of security provided by the combination of SSL certificates and browser interfaces in the face of various attacks ranging from phishing [3] and fraudulent websites, to malware of various forms. As one response involving a joint effort by browser vendors and service providers who sell SSL certificates, basic SSL server certificates are being demoted to second-class status in conjunction with the promotion [1] of Extended Validation (EV) SSL certificates [6] as the vehicle that can restore trust.

Unfortunately, EV SSL certificates complicate the already difficult design challenge of effectively conveying certificate information to the average user. Their introduction has triggered substantial modifications to the certificate user interfaces in web browsers such as Internet Explorer 7 (IE 7), both in new interfaces supporting EV SSL certificates, and in changes to old interfaces associated with basic and self-signed SSL certificates. These collective changes seem to significantly increase confusion surrounding SSL certificates, negatively impacting usability and security. Moreover, despite a broad diversity of emerging interfaces across the major browsers to support EV SSL [18], there is a void of literature exploring how user interface design in browsers affects usability and security, and how SSL-related design choices are being made and evaluated by browser developers.

As an early step in addressing this gap, the current study explores the interfaces related to SSL certificates in the most widely deployed [12] browser (IE 7), proposes an alternative set of interface dialogs based on guidelines, and compares their effectiveness through a laboratory user study involving 40 participants (45% non-students). The study examines the information dialogs related to the conditions of no certificate, self-signed certificates, basic SSL certificates, and EV SSL certificates, and how these convey to users information related to site identity and encryption. The goals of the study, and of introducing the alternative interfaces, are to

better understand which interface details users comprehend, whether differences between SSL certificates types are clear, and how easily users differentiate site identity information from channel protection (encryption) information.

Supporting users in determining whether to transact with a web site has become more important than ever before, in the face of flagging confidence in SSL. Among our contributions are results that raise an alarm about the changes in browser user interfaces that have been made to accommodate EV SSL, and suggest the need to re-think the design of these interfaces. The problem is much more complex than simply including EV certificates in the current framework of browser dialogs. Indeed, this study found that current IE 7 interfaces provide what may be viewed as misleading information on some critical security issues. Alternative interfaces, motivated by usability issues identified in existing interfaces, are shown to offer a marked improvement in several aspects, despite not matching the graphic quality and familiarity of IE 7. The current study raises important questions regarding the evolution and ongoing utility of self-signed certificates, the real value of EV SSL certificates, and whether SSL, the foundation for e-commerce on the web, is too complicated to be used in a reliable manner by ordinary users.

The remainder of this paper is organized as follows. Section 2 provides background and related work. Section 3 discusses perceived problems with user interface dialogs in current browsers, and presents an alternative design, including a set of proposed dialog boxes. The alternative design is then compared to corresponding interface elements of IE 7 in a user study, as described in Section 4. Results are presented in Section 5, further discussion in Section 6, and concluding remarks in Section 7.

2. BACKGROUND AND RELATED WORK

SSL and EV SSL Certificates. SSL is the the Secure Sockets Layer protocol [14]. It provides assurance about the identity of a website – certificates contain information about the certificate subject [14, 23] – and enables confidential transmission of information between browser and server over the Internet. SSL uses cryptographic keys both to encrypt transmitted data, and to authenticate the communicating entities through a digital signature. The current study focuses on server certificates and unilateral authentication; it does not explore client certificates or SSL's mutual authentication capabilities.

The traditional cues implemented in web browsers to convey SSL certificate information have been: (1) the *https* indicator in front of the site's URL, and (2) the display of a lock icon somewhere in the browser chrome (the frame of the browser that includes menus, toolbars, scroll bars, and status bars). The *https* indicator simply indicates that encryption is being used, while the lock icon provides additional information (when clicked) about the identity of the web site. This study examines the design and presentation of this additional information.

EV SSL certificates were established by the CA/Browser Forum [1], an organization consisting of Certification Authorities (CAs) and Internet browser software vendors. EV SSL certificates build on the existing technology of SSL certificates but involve a more strictly controlled issuance process. The developers of EV SSL certificates originally had two main goals: (1) to provide users with greater confidence regarding the identity of the organization that controls the site visited; and (2) to facilitate the exchange of encryption keys between the site and the user's web browser, as is done with traditional SSL server certificates.

Basic certificates (also referred to as standard or "domain-validated" [24] certificates) describe cases where the certificate authority has attempted to confirm that the applicant controls the domain for which the certificate will be issued. (There is no standardized procedure for conducting this confirmation; one heuristic used is the ability to respond to email messages sent to a domain email address.) Therefore, it is now recognized that these certificates should only be relied upon at most for domain-related information, and not information about a specific organization.

In contrast, extended validation SSL certificates were developed to provide organizational information of known quality and to display this information to the user. The prescribed EV SSL issuance process is designed to ensure that the only parties which can obtain such a certificate are private organizations, government entities, or business entities having a physical location (business presence) in the real world, excluding those listed on any government prohibited list or denial list. EV SSL certificates have five required fields: organization name, domain name, jurisdiction of incorporation, registration number, and address of place of business. Thus, a user may be able to view, for example, the address of a specific company using an EV certificate (as registered with the CA), whereas this information would be unknown under a domain-validated certificate. The apparent justification for this new type of certificate was in part because some CAs were issuing basic SSL certificates without properly verifying certificate information, and for fees as low as $30 (or even offering free 30-day trial certificates, attracting short-duration phishing sites), making it easier for attackers to obtain "legitimate" SSL certificates for fraudulent sites.

While the focus of this research is on interface issues, independent security issues related to SSL certificates have arisen in the past and will no doubt continue to appear. These include legitimate sites that do not employ SSL but nonetheless request sensitive information, certificates issued in error [10], and the recent flaw in a Comodo re-seller's process whereby proper verification was apparently not done [13]. Recent technically-sophisticated SSL attacks include the ability to forge SSL certificates by finding collisions in MD5 hashing [11] (which, surprisingly, is still in use), the null prefix attack [8], and the SSL rebinding attack [24]. However, even if these specific weaknesses were addressed, the interface problems discussed herein would remain.

Users and Security. Whitten and Tygar [22] discussed the *unmotivated user property*: security is a secondary goal for most users, who are primarily focused on tasks such as performing a banking transaction. Many users will miss subtle security indicators, and are not motivated to read manuals to learn their functionality. Conversely, security indicators that are too obtrusive risk that the user will ignore security altogether, either because they become annoyed or grow too accustomed to the indicator.

Several studies have shown that the traditional cues used to provide certificate information often go unnoticed [3, 4, 15, 21]. One study by Schechter et al. [15] 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 in the absence of this indicator. The lock icon is the security indicator most often noticed [4, 21] but its absence also often goes unnoticed [3] and, even when used as a security cue by users, many do not fully understand its meaning [2, 3, 4]. The majority of users who do rely on this security indicator remain unaware of its identity feature [3, 4, 21] and do not reliably understand the concept of certificates at all [2, 3].

Jackson et al. [6] performed the first known evaluation of EV SSL certificate support in Internet Explorer 7. They explored 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 sites, and reported that no one in the untrained group even noticed the new features. In a more recent study involving the Firefox 3.0 Beta 1 interface for EV SSL certificates, Sobey et al. [17] found that the subtle identity indicators in the browser chrome went completely unnoticed by participants, and even a modified indicator designed to be more prominent went unnoticed by half the participants. Of those who did notice the new indicator, a few participants conveyed some understanding of its intended use, but most apparently did not attempt to interpret its meaning. Both studies underline the challenge of introducing new security indicators into existing web browser interfaces in a manner that is obvious and intuitive for the average user.

In other research on SSL certificate warning dialogues, which is related to our work though independent, Sunshine et al. [20], investigated interface dialogue choices for conveying certificate information to users. Their study did not involve EV certificate issues, but rather focused on the appropriate presentation of errors and warning messages (such as domain mismatches).

3. SSL-RELATED USER INTERFACE ISSUES IN CURRENT BROWSERS

There are a number of usability issues associated with SSL-related user interfaces in current browsers, including IE 7. We discuss them in this section to motivate the design of an alternative interface.

3.1 Failure to Consider the Target User

When designing a user interface, it is important to consider the target user. It is unclear whether developers of each of the browsers have thought through who the target users are for their new interfaces that convey information related to SSL certificates, or whether those users have sufficient information or background to take appropriate actions. Since the most common use of SSL certificates is to facilitate online transactions such as banking or shopping, we assume the target user is an average computer user able to perform basic tasks (e.g., reading and sending email, browsing web sites) but someone who has no technical understanding of computers and no formal training in using them securely. We assume the user has a general understanding of the need to keep personal information (e.g., related to banking transactions) "safe" but has no a priori understanding of the technical implications of a "certificate". In fact, underlying details and their implications are unclear even to advanced users. This results in a challenge if, as is currently the case, a design choice is made to present technical certificate information to users.

3.2 Separating Identity and Confidentiality

The addition of EV SSL certificates to self-signed and (CA-signed, basic) SSL certificates results in three categories of SSL certificates (aside from the no-certificate condition). All three are essentially equal with respect to enabling private information to be sent and received securely through an encrypted channel — each can provide the same level of encryption. Traditionally, the *https* indicator and lock icon have indicated this functionality (SSL encryption on) to the user, and several studies [2, 3, 21] have shown that users associate the concept of the lock (if and when noticed) with being "safe". It is unclear whether "encryption means safe" is a sound mental model, as an encrypted channel to an unknown or untrusted party is not always "safe"; nonetheless, browsers typically render a lock icon whenever SSL encryption is underway, independent of site identification information related to certificates. It is likely that this and other aspects of current browser interfaces contribute to users conflating their confidence in site identity and encryption. The current user study and alternative interface proposal explore this. We note that a recurring problem with security interfaces has been that either users have no real mental model or that it does not match the system's functionality [16].

3.3 Conveying Certificate Information

In terms of the wording used to convey certificate information, major problems with current browser interfaces include: (1) messages which use technical terms not easily understood by typical users; (2) messages which are overly long, in an attempt to better explain the information being presented to users; and (3) wording which is misleading or not entirely correct. We now discuss these issues.

Unfamiliar Technical Terms. Ordinary users do not always understand technical terms. As an example, IE 7's dialog for sites that use certificates includes the wording "this connection to the server is encrypted". Arguably, the target user may not have a good understanding of encryption or even of what a server is. Another example of the use of technical terms is Firefox 3.0's self-signed certificate error message: "The certificate is not trusted because it is self signed. (Error code: sec_error_ca_cert_invalid)." This message, which implies that a user should understand the concept of signing a certificate, is likely incomprehensible to most users. In addition to these examples, many of the dialogs for providing additional certificate information specify the issuer and class of certificate, as well as the security protocol used for encryption. These levels of detail are probably only understood by highly technical users and should perhaps be hidden at a deeper level in the dialog boxes.

Lengthy Messages. In contrast to using highly technical terms to convey certificate information, the Opera 9.60 and Google Chrome (Beta) browsers, in particular, make an effort to explain the concepts to users more thoroughly [18], but this unfortunately results in fairly lengthy dialogs. Chrome Beta, for example, presents the user with a lengthy dialog upon visiting a site with a self-signed certificate that explains the concept of a certificate and why the particular site they are attempting to visit may not be trustworthy. While some of the wording is fairly easy to understand, experience suggests few users will take the time to

read lengthy messages. Furthermore, users seeing long messages frequently become conditioned to simply dismiss the warning [7].

Misleading or Confusing Wording. A common problem across browser interfaces is the existence of misleading or confusing wording in dialogs to the user. One particular aspect is messages relating to the "security" of the site. For sites using self-signed certificates, Opera displays a message stating "This page may not be secure." Interpretation of this message depends on the meaning of "secure." As mentioned earlier, self-signed certificates are capable of providing the same level of encryption as the other types of certificates; they differ only in terms of site identity. So quite possibly, the site is in fact providing confidentiality (which some would equate with being secure). The message displayed by Chrome for sites having EV SSL certificates includes the wording "it can be guaranteed that you are actually connected to..." *Guaranteed* almost certainly is the wrong word here. Are all known and future attacks impossible, will attackers never find a way to spoof an EV certificate [24], and will CAs never issue certificates in error (despite past experience otherwise [10, 11, 13])? Who is the guarantor if something goes wrong?

One of the more controversial wordings is in Firefox 3.0 messages that distinguish basic from EV SSL certificates. The identity indicator pop-up box says "you are connected to (insert domain name) which is run by (insert organization)" for sites with basic SSL or EV SSL certificates. However, the organization information is only filled in completely on sites with EV SSL certificates; for basic SSL certificates, this field is populated with "(unknown)". To illustrate the problem, we visited the web sites of two large banks – Wells Fargo in the United States and the Royal Bank of Canada. On the former, the Firefox identity indicator message reads "You are connected to wellsfargo.com which is run by (unknown)". Similarly for the latter, the message displayed is: "You are connected to rbc.com which is run by (unknown)." Considering sensitive banking transactions, one would hope that this would make online banking customers very suspicious of the legitimate banking web site – but of course, only if they are reading the message, and if they are not, then the messaging framework has also failed. This signals the need for reworking these design choices.

3.4 Guidelines for an Alternative Proposal

Given the certificate architecture and related functionality in today's Internet, an improved design for SSL information displays would offer a clear separation between identity and confidentiality indicators, since these are in fact separate concepts. By providing one (ideally simple and concise) set of messages relating to confidence in a site's identity and another relating to confidentiality protection, users may be able to form a better understanding and determine appropriate levels of confidence in both the site identity (authenticity) and the confidentiality of information sent to or received from it. SSL information displays should also avoid ambiguous terms like "secure" because these terms only cause users to draw vague conclusions about the "security" of a site without separating the implications of confidence in identity and confidentiality. Using the term "secure" also fails to take into account other issues such as malware on legitimate sites or on end-user machines themselves.

In terms of confidentiality, the only important distinction is between sites that do not use SSL certificates and sites that do use any of the three types of SSL certificate. For sites that do not use SSL, a simple message is appropriate, such as *"Information sent to and from this web site is vulnerable to eavesdropping."* A mental model involving the user interacting with a site is preferable to one involving a server or the actual organization hosting the site. Indicating that the communication may not be private might suffice to convince a user not to exchange any sensitive information with the site. Conversely, for sites that do have certificates for SSL encryption, a corresponding message is appropriate, such as *"Information sent to and from this web site is protected from eavesdropping."* While not all SSL connections are necessarily trustworthy (i.e., not all are with a known and trusted second party), the encryption does provide privacy from outside parties; separate messaging about identity helps guide how much trust a user should place in that private connection.

A particularly tricky issue is the wording choice for interfaces related to self-signed certificates, given the threat of *man-in-the-middle* (MITM) attacks. In a MITM scenario, transmitted information is confidential on each "hop" of an end-to-end trip, but the trip is through an untrusted intermediate point at which information may be decrypted and re-encrypted. We do not consider the vulnerability at such a proxy point to be *eavesdropping* per se, as the encryption along each hop works perfectly as intended; rather, the proxy point is masquerading as a legitimate host. We view this as a failure in identity, rather than in confidentiality. As such, for self-signed certificates, we suggest that the certificate interface show that the level of confidence in the site's identity is low,[1] but also state that the information is nonetheless protected from eavesdropping. Although this combination of factors may seem contradictory, it exactly expresses the complexity of the situation: private communication to an unconfirmed party.

For identity-related messages, terms such as "recognized authority" and "certification authority" are too technical and easily misunderstood by ordinary users. For sites with no certificate, a simple message is called for, such as *"This web site has not supplied a name for identity confirmation"*. For self-signed certificates, the alternative message changes only slightly to *"This web site claims to be (identity) but this has not been confirmed by any authority"*.

For CA-signed basic certificates, the proposed message is *"This web site claims to be (identity) and this has passed basic confirmation by (authority)"*, where (authority) is the name of the certificate issuer. For EV SSL certificates the proposal is to use the phrase "extended confirmation", e.g., *"This web site claims to be (identity) and this has passed extended confirmation by (authority)"*. The objective is to keep these messages as simple as possible for the ordinary user, while allowing advanced users to access further certificate information details, such as issuing authorities and encryption protocols, using a similar drill-down functionality as is currently implemented in web browsers.

None of the alternative messages employ the ambiguous term *secure*, nor the term *certificate* (nor mention of any level of certificate). There is no more reason to require a browser user to understand levels of certificates than to re-

[1]For self-signed certificates, the site identity is unconfirmed from the browser's viewpoint; site identity verification in this case relies on means beyond the browser itself.

quire that an automobile driver know how many pistons are in their car engine.

3.5 Alternative Design and Evaluation

Using the above guidelines, an alternative set of designs for certificate dialog boxes was designed, as shown in Figure 1. These dialog boxes would appear when users click on a lock icon or similar security indicator in a web browser. The dialog box is divided into two parts, one for identity and one for confidentiality, and each of these two concepts is visually delineated by its own icon. These icons were chosen to denote these two basic concepts, rather than the specific *states* of identity and confidentiality. Thus, they remain constant for all types of certificate. The "identity" icon consists of a silhouette of a person with a question mark superimposed over it, to suggest the concept of "seeking identity." The "confidentiality" icon consists of a pair of people, one of whom is transmitting a secret by whispering; this is intended to suggest the concept of "transmitting private data."

The icons were accompanied by the text messages described in the previous section. The identity information was labelled "identity confidence," to indicate that there is an assessment of the identity information being made. The confidentiality information was labelled "privacy protection," to communicate the idea of confidentiality through simple, clear language. The title bar of each dialog box contains two additional pieces of information: the level of identity confidence (with a three-state identity indicator [17]), and the URL of the site.

Once the initial dialog box designs were completed, the designs were evaluated in a laboratory study that compared them with the dialogs found in IE 7. Participants in the study were asked to read the dialogs, describe what these dialogs meant to them, and rate the interfaces on a variety of dimensions including ease of finding information, ease of understanding information, and preferences for one design over another. The goals of the study were to evaluate which interface elements users understand better, to explore if differences between types of SSL certificates are clear, and to examine if users can differentiate between site identity information and channel protection (encryption) information.

4. METHOD

4.1 Participants

Participants were recruited within a university campus, using posters and email lists. Participants were required to have experience with web browsing, and normal color vision (to avoid problems with red and green elements of the IE certificate designs). Recruitment notices stated that this was a usability study for web browser security. Eligible participants could be students, faculty, or staff.

Forty participants took part in the study (13 male, 27 female). Participants ranged in age from 18–59; 63% were less than 30 years old. Twenty-two participants (55%) were full-time students, and the remaining 45% were university staff, primarily in administration. Seventy percent of participants used the web more than 10 hour per week; for web browsers, 78% used IE weekly, and 68% used Firefox weekly. When self-rating their current computer skills on a 7-point scale, where "1" represented poor and "7" represented excellent, the mean rating was 5.5. Seventy-eight percent of participants used online banking, and on a 1-7 scale of concern about the security of personal information online, where "1" represented "not at all concerned" and "7" represented "very concerned," the mean rating was 5.6.

4.2 Materials

The user study was a within-subjects experiment that compared two different certificate designs: the alternative certificate designs ("alt"), along with the certificates from Internet Explorer 7 ("IE"). Graphical images of the certificate interface windows used in IE 7 and the ones proposed in the alternative design were prepared. This resulted in seven images in total: four for the alternative design, and three for IE 7 (see Figure 1). The domain of online banking was chosen for the experiment because such a high-risk financial environment demands that identity information be accurate, and that encryption be active. In this context, the certificate information is critical to determining the safety of an online transaction. The study did not use a real bank, to avoid any experimental confounds involving, for example, assessments of trustworthiness for that specific bank based on personal history or its reputation. Instead, we chose an imaginary bank name—"Standard Bank Ltd." of Toronto — and created images of certificate information displays for standardbank.com, as shown in Figure 1.

The experiment was counterbalanced so that half of the participants were shown the three IE certificate displays before the four alternative designs; the other half saw the four alternative designs before the IE images. Within each condition, the order of the certificate displays (e.g., self-signed, basic, EV) was randomized. Participants were assigned to one of these conditions depending on the order in which they signed up for the study.

For each certificate information display, participants were asked a set of questions which they would answer while looking at the images. Questions were similar for both sets of designs; minor variants were added to take into account the differences in the overall design (e.g., the alternative design has two icons but IE has only one). The wording of the questions was designed to avoid allowing participants to simply parrot the words shown in the dialog boxes in their responses. For example, to determine participants' understanding of the information about confidentiality, the words "eavesdropping" and "encrypted" were avoided in the questionnaire itself. Instead, we asked, "Is data sent to this web site safe from interception in transit?"

4.3 Procedure

The entire experiment took place in an office, using a laptop computer to display images to the participant. After informed consent was obtained, participants were shown an example of a basic certificate, using screenshots of the Opera browser, to familiarize them with the general idea of how web site security information could be displayed in a browser window. (We did not introduce the term "certificate" during this introduction.) The participants were then shown a series of images: the first set of certificate designs (either alternative or IE), followed by the second set, for a total of seven images. For each image, participants were asked a set of questions verbally by an experimenter, who sat next to the participant throughout the experiment. A sheet containing the questions was provided to the participants for reference. The questions asked about a number of aspects of the displays, including the ease of finding and under-

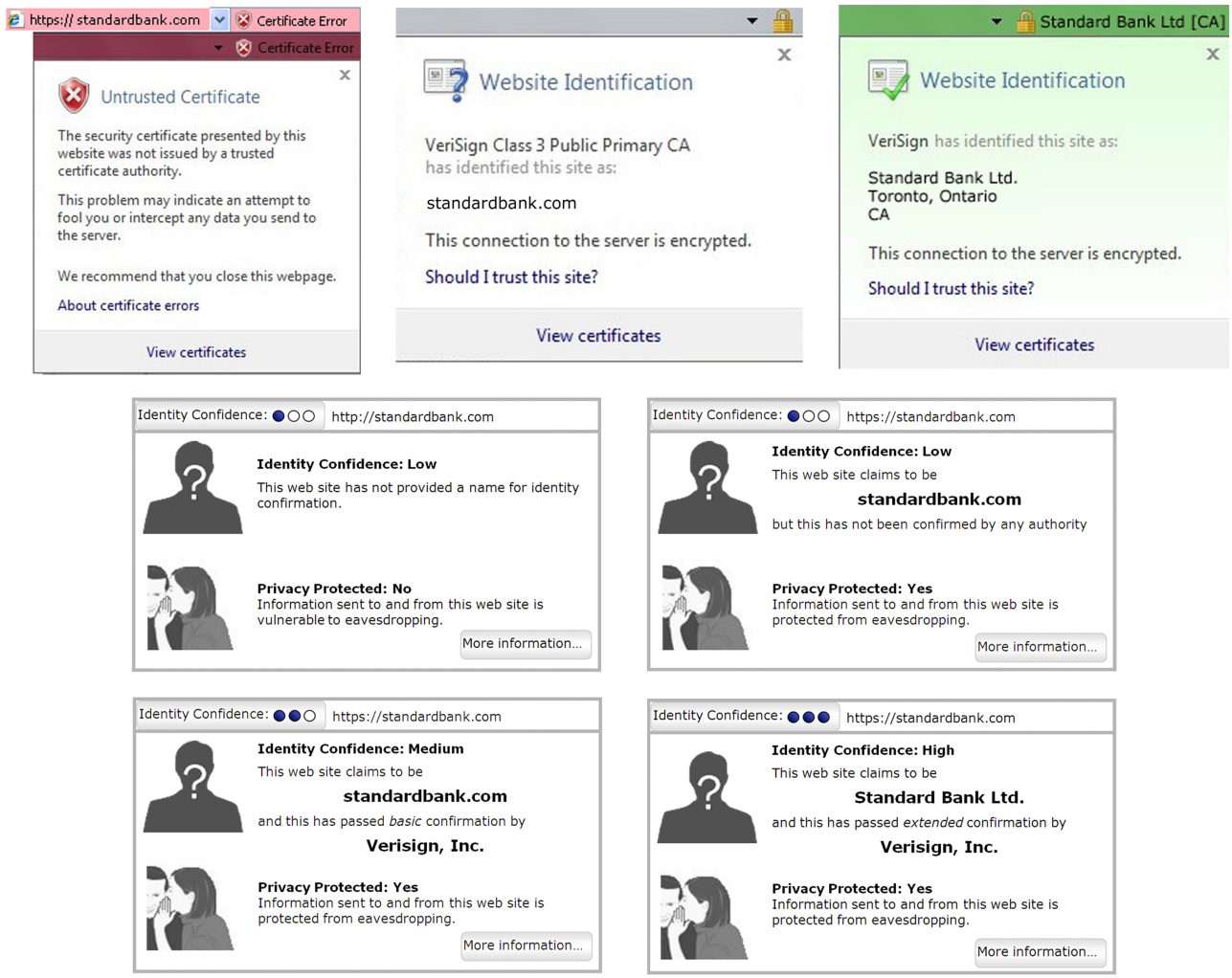

Figure 1: SSL information dialogs for IE 7 (top row) and the alternative design (bottom two rows). The IE 7 dialogs, left to right, are for the certificate conditions: self-signed, basic (ordinary SSL certificate), EV (extended validation certificate). The alternative dialogs are for the certificate cases: no certificate (middle row left), self-signed (middle row right), basic certificate (bottom row left), EV certificate (bottom row right).

standing information about identity and confidentiality, and opinions about any icons used. The experimenter recorded responses through hand-written notes, supplemented by an audio-recording of the experiment session. After all seven images were viewed, a final set of questions was posed which allowed free form responses as well as comparisons between the two designs. To conclude, basic demographic information was collected on a paper-based questionnaire. The entire session took approximately one hour.

5. RESULTS

5.1 Data Presentation and Analysis

The results to be shown make use of box plots and non-parametric inferential analyses. In notched box plots [9], the box area shows the second and third quartiles (25 to 75 percentiles) and the horizontal line shows the median. The "whiskers" in the plots show the range of values that fall within a distance from a box edge that is 1.5 times the size of the box. Any data points outside that distance are considered outliers, and these are shown as circles. The notched areas of the box represent the confidence interval of the median estimate. If the confidence interval reaches one of the quartile boundaries, the notches fold back on themselves. If the notched areas in two plots *clearly* do not overlap, the medians are most likely significantly different at a 95% confidence level. If the notches do overlap, there may or may not be significant differences. Although the box plots provide a useful visual summary of the data, appropriate statistical tests are required to make any conclusions, and these were always performed. Due to the ordinal nature of the rating scales and the finding that the data distributions were often markedly skewed, the non-parametric Kruskal-Wallis test of medians was used. A significance criterion of $p<.05$ was adopted for all analyses.

5.2 Finding and Understanding Certificate Information

Participants were asked to indicate, using 7-point scales ranging from "not at all easy" to "extremely easy", how easy it was to both *find* and *understand* two pieces of the certificate information: the web site ownership, and whether or not the data was safe from interception in transit. Figure 2 shows the ease of finding ownership information. Here the alternative design resulted in two statistically significant improvements: for both self-signed ($\chi^2(1) = 9.08$) and basic ($\chi^2(1) = 4.45$) certificates, the web site ownership information was easier to find. Figure 3 shows the ratings for ease of understanding the ownership information. There were no statistically significant differences found between the two design types for this question.

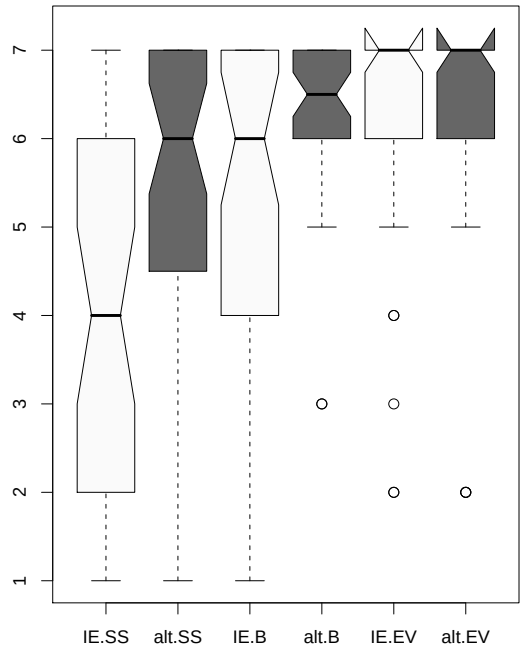

Figure 2: Ease of finding ownership information. Interfaces: IE (Internet Explorer), alt (alternative). Certificate types: SS (self-signed), B (basic), EV (Extended Validation).

Figure 4 shows the ratings data for ease of finding information about safety of data in transit. The alternative design resulted in two statistically significant improvements: for both basic ($\chi^2(1) = 11.23$) and EV ($\chi^2(1) = 13.34$) certificates, the data safety information was easier to find. Figure 5 shows the ease of understanding the information about the safety of data in transit. The alternative design again resulted in two statistically significant improvements: for both basic ($\chi^2(1) = 4.81$) and EV ($\chi^2(1) = 12.05$) certificates, the data safety information was easier to understand. So, in many cases, participants found that the alternative design made it easier to find information about site ownership, and to find and understand information about the safety of data in transit.

This study confirmed that technical language can be an impediment to users' understanding, e.g., several participants mentioned that they did not understand the word "encrypted", which is used in IE 7. To illustrate, one participant commented that "*[IE 7 is] a little bit more confusing…it tells me that it's encrypted but I don't really know exactly what 'encrypted' means*," and another said, "*I don't know if my information is safe, because I don't know what 'encrypted' means.*"

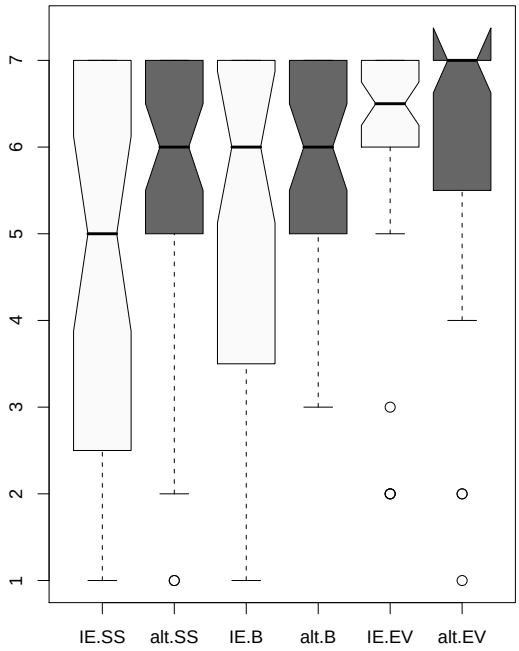

Figure 3: Ease of understanding ownership information.

5.3 Confidence in Ownership and Data Safety

Participants were asked to answer two questions about their level of certainty in the certificate information using 7-point scales ranging from "not at all certain" to "extremely certain". In terms of certainty about site ownership, there were no statistically significant differences found between the two design types. However, for the safety of the data in transit (see Figure 6), the alternative design resulted in two statistically significant improvements: for both self-signed ($\chi^2(1) = 24.14$) and basic ($\chi^2(1) = 5.06$) certificates, participants were more certain. (Note that for both of these certificate conditions, encryption is enabled, thus the data was indeed protected in transit.)

5.4 Accuracy of Security Decisions

In order to assess whether users could make correct security decisions based on the information supplied in the browser messages, participants were asked, "Is data sent to this web site safe from interception in transit?" In cases where an SSL connection was depicted, our interpretation was that the correct answer was "yes", regardless of the type of certificate.

The results indicate that participants often were not able to make correct judgements about data protection, especially when viewing the IE interface dialogs. For self-signed certificates, 26 out of 40 participants viewing the alternative dialog correctly replied "yes", while only 2 out of 40 were correct when using the IE dialog ($\chi^2(1) = 29.07$). For

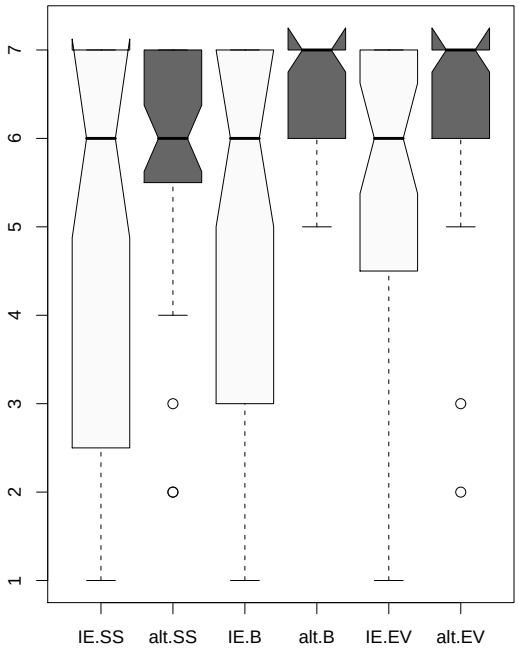

Figure 4: Ease of finding data safety information.

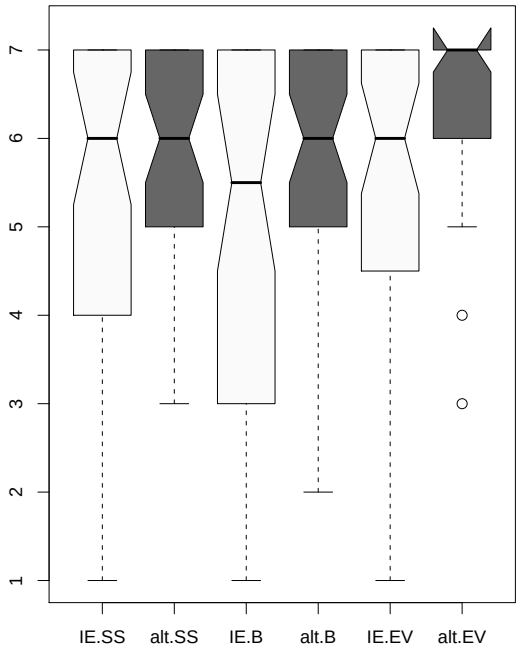

Figure 5: Ease of understanding data safety information.

basic certificates, 34 out of 40 participants viewing the alternative dialog correctly replied "yes", while 26 out of 40 were correct when using the IE dialog. (This difference was not statistically significant.) For EV certificates, 38 out of 40 participants viewing the alternative dialog correctly replied "yes", while only 29 out of 40 were correct when using the IE dialog ($\chi^2(1) = 5.88$). These results indicate that the alternative dialog was better able to support correct decisions about the confidentiality of data.

Participants were also asked to express their willingness (on a 7-point scale from "not at all willing" to "extremely willing") to enter private banking information: "On the basis of this information, how willing would you be to enter your bank account number and password if your bank's web site displayed this message?" The results are shown in Figure 7. For the case of self-signed certificates, participants were more willing to enter banking information ($\chi^2(1) = 8.50$) in the alternative design than for IE; here participants' willingness was quite low in both designs, with medians of 1.10 (IE) and 1.80 (alternative design). There were no significant differences for the other certificate types.

5.5 Opinions About Icons

The icons used in both designs were rated by participants to determine how accurately the icons matched the text that they accompanied (using 7-point scales ranging from "not all all accurate" to "extremely accurate"). IE's design had only one icon per certificate, hence participants were asked about "the icon in the top left corner." The alternative design had separate icons for identity confidence and privacy protection, so participants provided ratings for the top (identity confidence) and bottom (privacy protection) icons. For the analysis, the ratings for the IE icon were compared with the ratings for the two individual icons in the alternative design and the results are shown in Figures 8 and 9.

For the alternative design, the accuracy rating of the (top) identity confidence icon decreased as the certificate strength increased ($\chi^2(2) = 14.55$), such that the EV certificate resulted in the lowest rating. It is clear that participants felt that the icon did not match the information in the text for the basic and EV certificates. Also, the accuracy rating of the (bottom) privacy protection icon in the alternative design remained fairly constant across all certificate types. (Recall that these icons do not change depending on the certificate type: only the *text* changes.)

When comparing the icons used in the alternative design with the IE icons, there were two cases where the alternative design icons were rated lower than those in IE. In the EV certificate condition, the alternative design's identity icon (see Figure 8) was rated lower than the IE icon ($\chi^2(1) = 12.45$). This result is likely due to the low rating of the identity confidence icon for this specific condition, because participants may have judged the question mark (and its association with "questionable") as incongruous with the rating of "high identity confidence." (Note that although there appear to be non-overlapping notches in Figure 8 (self-signed) and in Figure 9 (basic), these results were not found to be statistically significant using the Kruskal-Wallis test.)

Also, in the self-signed certificate condition, the alternative design's privacy icon (see Figure 9) was rated lower than the IE icon ($\chi^2(1) = 8.04$). This finding suggests that participants preferred the IE self-signed icon (an "X" on a red shield) over the whispering icon used in the alternative design because it was a better match to the dialog's accompanying text information (independent of whether both the IE icon and the text may mislead users into believing that encryption is not operational in this condition).

5.6 Interface Preferences

At the end of the session, participants compared the two designs and rated their preferences on four aspects: which

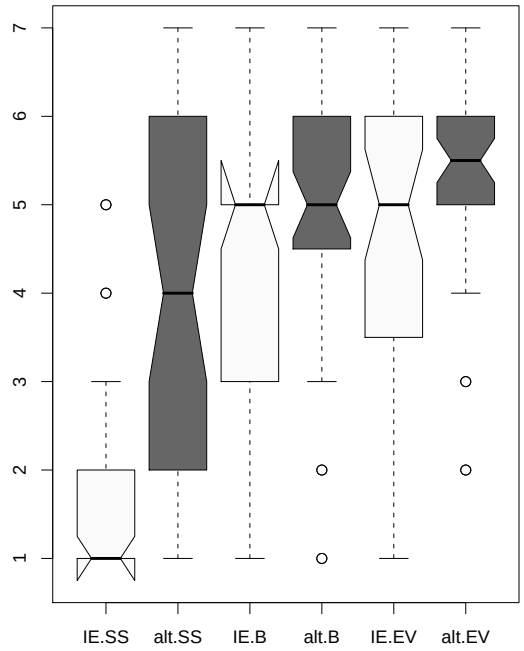

Figure 6: Certainty of data safety information.

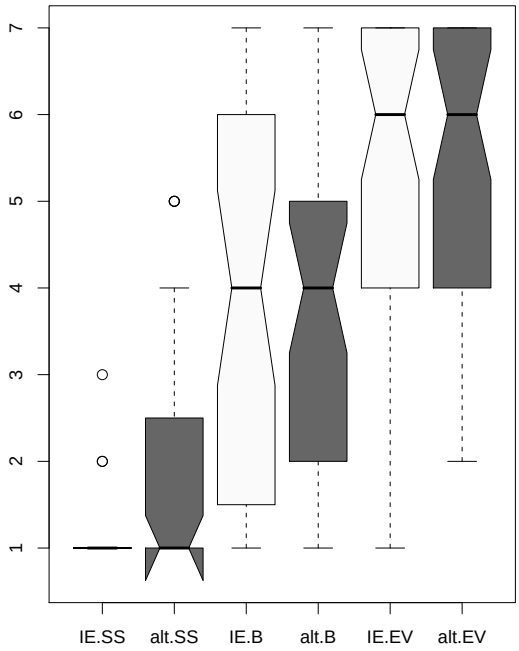

Figure 7: Willingness to enter banking information.

design was easier to understand; which design gave more confidence in the web site ownership; which design gave more confidence in data safety;[2] and which design was preferred overall. Each question used a two-ended seven-point scale, such as the following (where "set 1" was the first design that was viewed in the experiment):

Please use the scale below to indicate which set of message windows were easier to understand:
Set 1 much easier 3–2–1–0(same)–1–2–3 Set 2 much easier

We collected the ratings for each design regardless of the order of presentation and then compared the totals. The results (shown in Table 1) reveal that the alternative design was preferred for most aspects (although not significantly so). However, the design used in IE was slightly preferred in "overall" ratings. Participant comments suggest this is likely due to two main factors. First, IE's design was preferred on aesthetic grounds; we heard several comments about its good use of color and the refined look of its icons. For example, one participant commented that "*I liked the colours of the second set. Green means go, red means stop, grey means ok*," and another stated that "*I felt that with the icons, [IE 7 set] was more professional*." The alternative design, on the other hand, primarily used black and white, and the icons were somewhat simplistic.

Second, IE's design was more familiar to participants, particularly as it evoked the look-and-feel of Microsoft's products (including security products) in general. For instance, one participant commented that "*In comparison to [the alternative design, IE 7] is a lot closer to the kind of popup windows you'd usually see with Windows...it uses more of the language and the icons you associate with desktop Windows security...so it's already kind of familiar*."

[2]This question was added after the first four participants' sessions, thus the total for this is calculated using $n = 36$.

Table 1: Preferences for Each Design Type

aspect	IE	alt.	δ
easier to understand	38	47	+9
more confidence in ownership	32	38	+6
more confidence in data safety (n=36)	30	42	+12
preferred overall	44	39	−5

5.7 Results Summary

The alternative design demonstrated significant improvements over IE in the following areas:

- easier to find web site ownership information
- easier to find and understand data safety information
- increased confidence in data safety (when encryption is present)
- accuracy of security decisions

User preference data also indicates that the alternative design was slightly preferred for ease of understanding and increased confidence, although its unfamiliarity and its lack of aesthetic refinement prevented it from being the overall preferred design among participants.

6. FURTHER DISCUSSION

The alternative interface for displaying SSL information was found to offer statistically significant improvements in confidence, ease of finding information, and ease of understanding. In none of these aspects was the alternative design worse than IE 7. Only in the suitability of the icons was the IE design found to be better than the alternative interface. The improvements made in the alternative interface involved only simple interface changes in wording and text placement. Such results from a modest re-design effort suggests that many of the issues raised in Section 3 can indeed be addressed. Taking this as a first step, it is clear there is considerable room for improvement in the design of

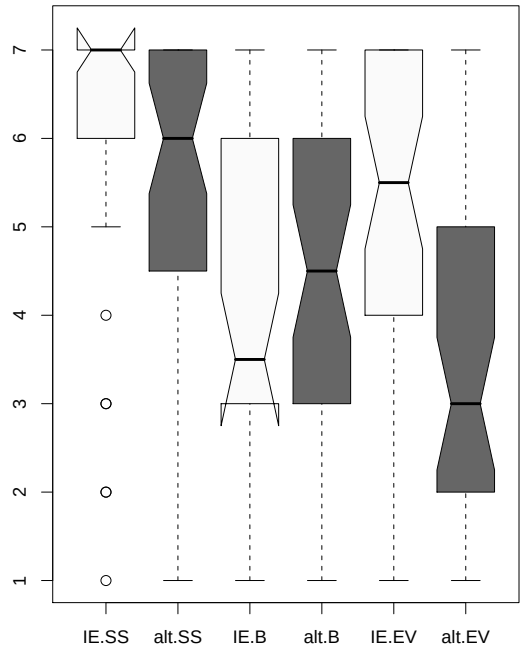

Figure 8: Accuracy of (top) identity icon in alternative design compared with single icon in IE design.

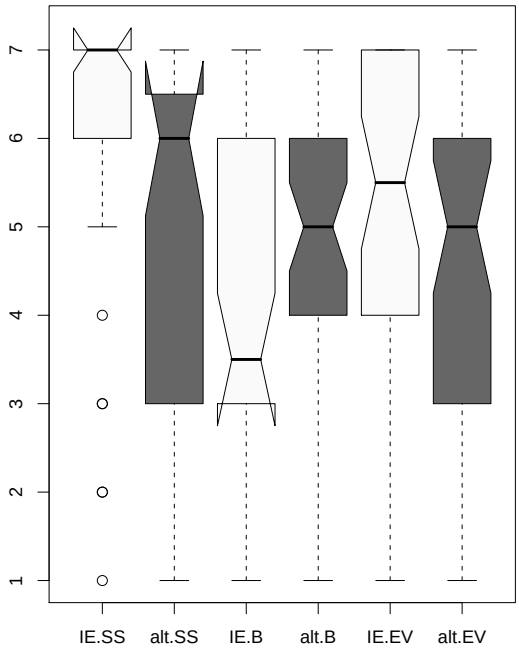

Figure 9: Accuracy of (bottom) privacy icon in alternative design compared with single icon in IE design.

certificate-related dialogs and user interfaces in IE 7, and other browsers.

Some specific details of the alternative design warrant comment. This design avoided use of the term "encryption", which is present in the IE interfaces. Observation of user study participants indicated that those who did not understand this term found the alternative design clearer in ease of understanding of data safety, perhaps explaining the significant difference between the alternative design and IE in the basic and EV conditions. This difference, however, was not significant in the self-signed condition. Our interpretation here, based on comments made by the participants, is that for the IE interface, participants concluded (incorrectly) that data in transit was *not* safe, and as the IE dialog message was so negative, they felt they understood this easily (despite their wrong conclusion).

The alternative design choice of an identity icon with a question mark on the silhouette of a head proved to be a poor choice, particularly in the EV condition (see Figure 8), where participants found that the icon did not match the text well, as discussed in Section 5.5. This suggests that in a future design, a better choice could be made. Overall, the relatively poor aesthetic quality of icons in the alternative design offer further opportunity for improvement, as discussed in Sections 5.6 and 5.7.

It is worth highlighting how poorly the IE 7 interface fared, especially in the self-signed condition, with respect to participants' accuracy on the question of whether data is protected in transit. This demonstrates the success of the alternative design in signaling to users that encryption is on in the self-signed case, and in disentangling confidence in web site identity from encryption. It is worth mentioning that here the message text in the IE 7 interface is, "This may indicate an attempt to ... intercept any data you send to the server." This appears to be an attempt to warn users about possible man-in-the-middle or fake-endpoint attacks, which do not involve interception of data in transit, but rather at the endpoint. This choice of wording may lead to the wrong impression by participants.

The treatment of self-signed certificates in IE 7 effectively implements a decision to downgrade self-signed certificates to untrusted status, relative to IE versions prior to the introduction of EV certificates. This apparent decision requires serious consideration by the security community: *Is down-grading, or the complete elimination of support for self-signed certificates, in the best interests of the Internet community as a whole?* This should be considered in light of the current rules which stipulate that individuals are not eligible to acquire EV SSL certificates, even if they were willing to pay (see Section 2).

The self-signed certificate condition is the case where separating identity confidence from encryption is most relevant: specifically, when web site identity confidence is low, but encryption is operational. There are two main cases to consider here: (1) a user has some out-of-band reason to trust the web site in question (for example, the site's SSL certificate has been imported in a trustworthy manner); and (2) there is no additional outside information. In case (1), the utility of self-signed certificates remains high, whereas in case (2), self-signed certificates expose typical users to security dangers. It would seem strong arguments could be made on both sides as to whether or not continued use of self-signed certificates is advantageous.

Related to this down-grading issue, one might also interpret recent interface changes as suggesting that continued use of basic certificates may also be threatened. In Firefox 3, as discussed in Section 3.3, the message displayed for basic certificates says that the web site is "run by (unknown)", which appears to be a warning to users and site operators.

If one accepts the launch of EV certificates as acknowledgment that basic SSL certificates can no longer be trusted, one may ask where this leaves individuals, informal organizations and small business entities that presently depend on (inexpensive) basic certificates.

7. CONCLUDING REMARKS

We have explored a number of issues with respect to SSL certificates and the interfaces used to display certificate-related information to users. With the aid of a user study, we have gained insight into users' understanding of current dialogs, and found that fairly simple user interface changes can significantly alter user perceptions and understanding.

While the CA/Browser Forum [1] outlines the goals of EV certificates, other parties may have competing objectives. For example, one viewpoint [5] – which is worrisome from a security perspective – is that the purpose of EV SSL certificates is to increase the completion rate in online transactions (i.e., to decrease "cart abandonments") independent of whether or not this is in users' best interests. Browser developers may also have an agenda of making their browser more widely-adopted than competing browsers, which might suggest minimizing dialogs or interventions that block web sites in order to prevent users from switching browsers. The possibility of such competing objectives complicates the interface design problem.

It is also noteworthy that there is a growing disparity in user experiences across different browsers. With the introduction of new browsers, new versions thereof, and new interfaces within them due to the deployment of EV SSL certificates, users are faced with new and/or changing interfaces and numerous, often technical, messages. This introduces challenges due to unfamiliarity and lack of consistency. What is lacking is a comparable experience across browsers.

The current path of development for browser interfaces that display SSL information is one of incremental design, in an attempt to effectively convey site identity information and confidentiality protection to users. We note with concern that following such an incremental path to improve current interfaces (e.g., by altering the wording and icons in dialog boxes) may result in progress toward a design which is a local optimum, but possibly far from what might otherwise be possible in simpler overall frameworks, e.g., with fewer grades of SSL certificates. We do not rule out the possibility that the path to real progress may involve redesigning the hierarchy and framework of SSL certificates.

Returning to the issue of the target users, the alternative design resulted in some user experience improvements. Beyond this we remain interested in the broader issue of whether it is realistic to expect non-technical people to use browsers with four grades of certificates (none, self-signed, basic, EV SSL), and encourage the research community to debate the question: *Are EV SSL certificates a robust foundation for improving Internet trust, or a band-aid solution which further complicates usable security for ordinary users?*

Acknowledgments. We thank Cormac Herley, Ben Laurie, Tim Moses, and anonymous referees for helpful comments, and our study participants for helping with our research. The first author acknowledges support through the NSERC Discovery Grant program. The second author is Canada Research Chair in Network and Software Security, and is supported in part by an NSERC Discovery Grant/ Discovery Accelerator Supplement, and the Canada Research Chairs Program. Partial funding from NSERC ISSNet is also acknowledged.

8. REFERENCES

[1] CA/Browser Forum. http://www.cabforum.org/

[2] R. Dhamija and J. Tygar. The Battle Against Phishing: Dynamic Security Skins. In *Proc. of the Symp. on Usable Privacy and Security*, (2005).

[3] R. Dhamija, J. Tygar, and M. Hearst. Why Phishing Works. In *CHI Conf. on Human Factors in Computing Systems*, April 22-27 (2006).

[4] J. S. Downs, M. Holbrook, and L.F. Cranor. Decision strategies and susceptibility to phishing. In *Proc. of the Symp. on Usable Privacy and Security*, (2006).

[5] P. Hallam-Baker. Does Anyone Fall for Phishing Scams Anymore? *IT Security Journal.com*, (2008). http://www.itsecurityjournal.com/index.php/Latest/Does-Anyone-Fall-for-Phishing-Scams-Anymore.html

[6] C. Jackson, D.R. Simon, D.S. Tan, and A. Barth. An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks. In *Proc. of Usable Security*, (2007).

[7] 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 *CHI Conf. on Human Factors in Computing Systems*, (2007).

[8] M. Marlinspike. Null Prefix Attacks Against SSL/TLS Certificates. http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf. 29 July (2009).

[9] R. McGill, R.W. Tukey, and W.A. Larsen. Variations of box plots. *The American Statistician*, 32(1):12–16, Feb. (1978).

[10] Microsoft Security Bulletin MS01-017 (Mar.22 2001; updated Mar.28 2001). Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard, http://www.microsoft.com/technet/security/bulletin/ms01-017.mspx

[11] D. Molnar, M. Stevens, A. Lenstra, B. de Weger, A. Sotirov, J. Appelbaum, and D.A. Osvik. MD5 Considered Harmful Today: Creating a Rogue CA Certificate. *25th Chaos Communication Congress*, Berlin, Germany, December 30 (2008).

[12] Net Applications. Global Market Share Statistics, March 2009, http://marketshare.hitslink.com/browser-market-share.aspx?qprid=2 (retrieved April 11, 2009)

[13] E. Nigg. Untrusted Certificates. Personal blog, December 23, 2008, https://blog.startcom.org/?p=145

[14] E. Rescorla. *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley (2001).

[15] S.E. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The Emperor's New Security Indicators. In *Proc. 2007 IEEE Symp. on Security and Privacy*, May (2007).

[16] S.W. Smith. Humans in the Loop: Human-Computer Interaction and Security. *IEEE Security and Privacy*, 1(3):75–79, May/June (2003).

[17] J. Sobey, R. Biddle, P.C. van Oorschot, and A.S. Patrick. Exploring User Reactions to New Browser Cues for Extended Validation Certificates. *Proc. of European Symposium on Research in Computer Security (ESORICS)*, 2008.

[18] J. Sobey, P.C. van Oorschot, A.S. Patrick. Browser Interfaces and EV-SSL Certificates: Confusion, Inconsistencies and HCI Challenges. Technical Report TR-09-02 (January 15, 2009), School of Computer Science, Carleton University, Canada.

[19] J. Sobey, T. Whalen,, R. Biddle, P.C. van Oorschot, and A.S. Patrick. Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study. Carleton University, School of Computer Science, Technical Report TR-09-06 (July 2009).

[20] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L.F. Cranor. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *Proc. of the 18th Usenix Security Symposium*, August (2009).

[21] T. Whalen and K. Inkpen. Gathering Evidence: Use of Visual Security Cues in Web Browsing. In *Proc. of Graphics Interface 2005*, pp. 137–145, May (2005).

[22] A. Whitten and J.D. Tygar. Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0. In *Proc. of the 8th USENIX Security Symposium*, August (1999).

[23] Z. Ye, S. Smith, and D. Anthony. Trusted Paths for Browsers. *ACM Trans. on Information and System Security*, pp. 153–186, May (2005).

[24] M. Zusman and A. Sotirov. Sub-Prime PKI: Attacking Extended Validation SSL. *Black Hat Security Briefings*, Las Vegas, USA, July (2009).