Browser Interfaces and EV-SSL Certificates: Confusion, Inconsistencies and HCI Challenges[⋆]

Jennifer Sobey[1], P.C. van Oorschot[1], and Andrew S. Patrick[2]

[1] School of Computer Science, Carleton University, Ottawa, Canada
[2] Institute for Information Technology, National Research Council, Ottawa, Canada
{jsobey,paulv}@scs.carleton.ca,Andrew.Patrick@nrc-cnrc.gc.ca

Abstract. The introduction of Extended Validation (EV) SSL certificates has caused web browser manufacturers to take a new look at how they design their interfaces for conveying certificate information. In turn, we take a thorough look at the choices they have made. Our observation is that the changes being made significantly increase the confusion surrounding SSL certificates rather than increasing trust. We perform a systematic walkthrough involving dialogues and interfaces related to site identity, certificates, and SSL encryption; raise questions concerning the inconsistencies in their implementations; and highlight the confusion between identity and confidentiality. Prior to carrying out a full user study, we aim to define the problem clearly and to explore some possible alternatives. We suggest some improvements in terms of both mental models and interface design and emphasize the importance of consistency across browsers for appropriate user interaction with these certificate interfaces.

Key words: Usable security, extended validation, SSL certificates, browser security interfaces

1 Introduction

In 1995, the traditional SSL certificate was first used as a way to provide encryption of private data being exchanged with a website and to provide some assurance as to that site's identity [30]. Now, fourteen years later, the loss of confidence in the standard SSL certificate has lead to the introduction of a new Extended Validation (EV) SSL certificate [12] that aims to restore that trust. Indeed, with growing use of the Internet for sensitive transactions such as online banking, it is increasingly important to provide a reliable way of distinguishing a legitimate bank web site from a fraudulent site.

The addition of new EV-SSL certificates adds a layer of complexity to the already difficult design issue of conveying certificate information to the average user. The rather drastic modifications to the interface design of web browsers, which have not only added the new EV-SSL certificates but also changed browser handling of regular SSL and self-signed certificates, as highlighted herein, will in our view, significantly increase user confusion surrounding SSL certificates rather than improve on the current situation. While the present paper focuses on interface issues, other trustworthiness issues related

[⋆] Version: January 13, 2009. This note is a technical report on work-in-progress.

to SSL certificates have arisen in the past [18] and continue to appear, such as the recent flaw in a Comodo re-seller's process whereby they apparently had not done proper verification [23] and the ability to forge SSL certificates by finding collisions in MD5 hashing [19] which is surprisingly still in use. Even if these types of flaws relating to the certificates themselves ceased to appear, the interface problems discussed herein remain.

In this paper we perform a systematic walkthrough involving dialogues and interfaces related to site identity, certificates, and SSL encryption. As a result we: (1) raise concerns about the current state of SSL certificate interfaces in web browsers (including IE, Firefox, Opera and Chrome), by highlighting the inconsistencies between browsers, changes made due to the introduction of EV-SSL certificates, and the failure to distinguish between site identity and confidentiality; (2) suggest possibilities for improvement, both in terms of users' mental models and in the actual design of the browser certificate interface; and (3) make a call to arms for unification and standards for SSL certificate interfaces in browsers.

The remainder of this paper is structured as follows. *Section 2* provides some background on SSL certificates and usable security. *Section 3* explores problems that lead to confusion with SSL certificate cues in web browser interfaces. *Section 4* further explores the inconsistencies in current web browser interfaces. *Section 5* considers improvements that could be made in these interfaces. *Section 6* contains concluding remarks and open questions for future work. *Appendix A* contains figures illustrating the interface features for SSL certificates in the browsers being studied.

2 Background and Related Work

2.1 SSL Certificates and EV-SSL Certificates

Secure Sockets Layer (SSL) [26] is a protocol commonly used in validating the identity of a website (certificates contain information about the certificate subject [26, 34]) and enabling the confidential transmission of information between browser and server over the Internet. It uses cryptographic keys to encrypt the data being transmitted and to provide a signature used in identification. In this paper, we are interested in SSL server certificates and unilateral authentication of the site; we do not explore client certificates or the mutual authentication capabilities of SSL.

Traditionally, two cues implemented in web browsers have conveyed SSL certificate information: (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). While the *https* indicator is simply an indication that encryption is being used, the lock icon provides additional information (when clicked) about the identity of the site providing that encryption.

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. They build on the existing technology of the SSL certificate but involve a more strictly defined issuance process. They originally had two primary purposes: (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 done with traditional SSL server certificates.

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 and that are not 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. The need for this new type of certificate arose from the fact that some CAs were issuing standard SSL certificates without properly verifying certificate information and for fees as little as $30 (or even free 30-day trial certificates, attracting short-duration phishing sites), making it easier for attackers to obtain "legitimate" SSL certificates for fraudulent sites.

2.2 Users and Security

Whitten and Tygar [32] discussed the *unmotivated user property*: security is a secondary goal for most users, who are primarily focused on tasks such as logging into a site or 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 [6, 7, 27, 31]. One study by Schechter et al. [27] 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 [7, 31] but its absence also often goes unnoticed [6], and even when used as a security cue by users, many do not fully understand its meaning [5–7]. The majority of users who do rely on this security indicator remain unaware of its identity feature [6, 7, 31] and do not reliably understand the concept of certificates at all [5, 6].

Jackson et al. [12] performed the first known evaluation of EV-SSL certificate support, on Internet Explorer 7.0. 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. [29] 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.

3 Problems With Interfaces for EV-SSL and Other Certificate Types

3.1 Failure to Identify the Target User

When designing a user interface, such as for displaying or conveying SSL certificate information, it is critical to consider the target user of the interface; this is a well known human-computer interaction (HCI) principle. It is unclear if developers of each of the browser manufacturers have thought through who the target users are for their new SSL certificate interfaces (any such target has yet to be communicated, to our knowledge), 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, for our evaluation in this paper we consider the target user to be the stereotypical online banking customer. This user is able to perform basic tasks such as reading and sending email, and browsing web sites, but does not necessarily have technical understanding or formal training in this area. Since they are performing transactions related to banking, we assume the user has a general understanding of the need to keep personal information "safe" but has no a priori reason to understand the technical implications of a "certificate"; in fact, underlying details and their implications are unclear even to many advanced users. Therein lies the challenge of presenting certificate information in a way that is reliable and easily understood.

3.2 Failure to Distinguish Identity from Confidentiality

With the introduction of EV-SSL certificates, in addition to original certification authority (CA) signed certificates and self-signed certificates, there are now three categories of SSL certificates. With respect to SSL certificates enabling private information to be sent and received securely (i.e., over an encrypted channel), all three types are essentially equal; that is, each can provide the same level of encryption. Traditionally, the *https* indicator and lock icon have indicated this functionality to the user, and several studies [5, 6, 31] have shown that users do associate the concept of the lock (if and when noticed) with being "safe"; this may or may not be a good mental model for this encryption-related functionality, as an encrypted channel to someone you do not trust is not necessarily "good". Indeed, there is also the identity portion of the certificate, for which we believe that users do not currently have any mental model, based on our previous observations of user behavior [29]. This has been a recurring problem with security interfaces in general; either users have no real mental model or, as Smith [28] points out, the user's mental model does not match the system's functionality.

A self-signed certificate can be created by anyone who takes the time to obtain a program such as OpenSSL [24]. With a few simple command lines, an SSL certificate can be created and installed on any web server. The certificate creator has complete control over the content of the certificate fields, including the organization name and issuer; thus anyone could create a self-signed certificate that claimed to be for Wells Fargo and issued by Verisign, Inc. Accordingly, users should place little or no confidence in the identity specified in a self-signed certificate (unless they have received the certificate or fingerprint thereof from a party they trust, e.g., PGP-style). We liken this to the identity confidence associated with a business card received in postal mail, or letterhead in such a mail item; it may look professional, but anyone with an inexpensive printer can create one asserting arbitrary information.

A CA-signed certificate was originally intended to provide greater confidence in a site's identity, because of its creation (endorsement) by a trusted third party which is relied upon for confirming the correctness of (some of) the information provided by the party requesting the certificate. This currently remains the most common type of certificate used by banks and e-commerce web sites. Unfortunately, many different certification authorities issue these certificates, with varying levels of due diligence in terms of verifying identity; and today's browsers can neither distinguish among these, nor meaningfully convey differences to common users. The well-known CAs such as Verisign charge up to $400 USD and require extensive contact information and registered domain names, whereas certificates can be obtained from smaller companies such as GoDaddy.com for as little as $29.99 USD and require much less information from the requesting individual. Because of the variety and availability of these certificates, we liken their identity features to a library card. Some libraries will give cards out freely to anyone who wishes to obtain one, while other libraries (such as a University library perhaps) may have special requirements for obtaining a card. Librarians manually verifying the cards in large cities (in cases where cards are required to enter the library) are not able to distinguish, on the spot, cards whose names do not match the individuals holding them.

Finally, EV-SSL certificates are intended to provide the greatest confidence in a site's identity. According to the CA/Browser Forum [3] guidelines, these are only issued to business entities, government entities, or private organizations who are registered in their jurisdictions and have a verifiable physical business presence. They currently cost $500-$1500 USD and all CAs issuing such certificates are supposed to follow strict guidelines for verifying the organization's identity. We liken the identity features of this type of certificate to an individual's passport – a government-issued document that requires background checking before it is issued.

3.3 Other Problems

We identify two other problems related to how emerging browser interfaces handle EV-SSL certificates and their relatives: (a) disrupting users' previous experience (with previous browser versions) of how server certificates are handled, including essentially downgrading ordinary SSL certificates and treating self-signed certificates now as if they were all fraudulent, at first cut; and (b) tremendous inconsistencies in the interfaces across different browsers. We discuss relevant details of both of these in Section 4.

4 Problems Due to Changes and Inconsistency Across Browsers

With the introduction of EV-SSL certificates, most of the major web browsers have drastically changed the interfaces for displaying certificate information to the user, in several cases including changing the implications of the original certificates (self-signed and CA-signed). These changes have also increased the level of inconsistency across the various browsers, with each web browser providing different visual cues and messages about SSL certificates. These inconsistencies suggest to us that browser vendors are struggling to find the proper interface design for providing SSL certificate information and this indicates a major problem in this area.

In the following sections, we explore the four conditions (no certificate, self-signed, CA-signed, and EV-SSL), and the corresponding SSL interfaces for Internet Explorer 7.0.6, Firefox 3.0.3, Opera 9.60 and Google Chrome (Beta) [10, 17, 21, 25]; we have deferred consideration of other major web browsers since KDE Konqueror [13] has not yet implemented support for EV-SSL certificates and we expect their current interfaces will change significantly once this is done, while the recent changes made to Apple Safari 3.2 [2] were extremely minimal and the few user dialogues that do exist in this browser are similar to those found in other browsers we consider.

4.1 Sites with no SSL certificate

When visiting a webpage that does not use SSL, most web browsers will not produce any type of indicator to signify the lack of SSL certificate. While often fine, since many non-SSL sites are only used to display non-sensitive information and do not request sensitive user information, in some cases the user is asked to input the latter. Though many legitimate web sites request passwords on a non-SSL web page, users should be cautioned against supplying sensitive information in these cases. However, it is difficult to accomplish this education until the interfaces are usable and easily understood. The lack of the *https* indicator and lock icon is the de facto cue to indicate that a page may not use encryption. However, this violates a general HCI principle – that users do not generally tend to notice the *absence* of an indicator. To add to the confusion, web pages can be constructed which are not protected by SSL in the normal sense, thus having no visible chrome lock icon, but which nonetheless (request and) secure passwords, through appropriate browser frame technology not visible to the end-user.

With the changes to the SSL certificate interface in Firefox 3.0, a new identity indicator has been introduced to provide a level of confidence in a site's identity [21] (see also [29]). This indicator is a small button located immediately to the left of the URL bar and its background color will change depending on the certificate type for the site – blue for CA-signed certificates and green for EV-SSL certificates. For sites with no SSL certificate, this indicator has a grey background and clicking on it will produce a pop-up box indicating that the site's identity is unknown (see Appendix A, Figure 11). We note that Firefox is the only current browser to provide an indicator that is always visible regardless of SSL condition.

4.2 Sites with self-signed SSL certificates

Among the more disruptive recent changes to the SSL interface in most web browsers has been the cues for, and handling of, self-signed certificates. Given the goal of the new EV-SSL certificates to provide higher confidence in a site's identity, one might argue that self-signed certificates fall at the opposite end of the spectrum in that they provide little to no guarantee in a site's identity. This indeed seems to be the reasoning behind the changes browsers have made in this regard, but severely disrupts users' previous experiences in going to such sites, which they might have external reasons for trusting and may have been previously visiting without disruption (thus intending to rely on SSL's encryption functionality, but not its identification functionality). All four browsers studied here implement a mechanism for interrupting and at least temporarily blocking the user before they can reach a site using a self-signed certificate; the severity of warnings varies largely across the browsers.

After entering the URL for a site using a self-signed certificate, Opera presents a pop-up dialogue advising the user that the site may not be secure and prompting to accept or reject the loading of the page. The user need only click the "approve" button to proceed to the site. The other three browsers load a substitute page whose content is a warning message indicating the site may not be secure. Google Chrome presents two buttons: "proceed anyway" and "back to safety". Internet Explorer presents two links: "Click here to close this page" and "Continue to this website (not recommended)". Firefox makes it the most difficult to continue by only displaying a warning with a link labeled "or you can add an exception..." which leads to a rather involved four-step process of temporarily or permanently accepting the self-signed certificate. It is not clear how common users will interpret the word "exception." Appendix A provides details of these warning messages and the steps involved in proceeding to a site (see Figures 5, 7-9).

4.3 Sites with CA-signed SSL certificates

Web sites with certificates signed by trusted CAs are generally considered to provide greater identity confidence than self-signed certificates, but less than the new EV-SSL certificates. Different browsers' interfaces have taken this into account in different ways. As was traditionally the case, the *https* indicator and lock icon are still displayed in each of the four browsers we examined. However, each browser also implements additional cues for these sites.

In Google Chrome, upon encountering a valid CA-signed SSL certificate, the background of the URL bar is colored yellow and the *https* text is colored green. In Opera, the domain name is included to the right of the lock icon and the background of this area is colored yellow. Firefox colors the background of its new identity indicator blue and clicking on this indicator will provide more information about the site's identity; for a CA-signed certificate, it states "You are connected to (domain name) which is run by (unknown)" where (domain name) is taken from the Common Name field of the certificate, and (unknown) is taken from the Organization Name field but only filled in properly for sites with EV-SSL certificates. In each browser, clicking on the lock icon presents a pop-up box containing further certificate information. The lock icon and pop-up are in fact the only interface features for CA-signed SSL certificates in Internet Explorer. See Appendix A (Figures 10-13) for images of the interfaces and appropriate pop-up boxes.

4.4 Sites with EV-SSL certificates

One element that currently remains constant across the four browsers' interfaces with respect to EV-SSL certificates is the use of the color green. However, the location and use of this color varies greatly between the four browsers studied here. In Google Chrome, the interface is barely distinguishable from the interface for a traditional SSL certificate, except for the addition of the organization name and country code displayed in green text to the right of the lock icon; the pop-up box that results from clicking on the lock is also nearly identical to that for traditional SSL certificates, except that the words "Extended Validation" appear in the description of the certificate. In Opera, the area that was colored yellow for CA-signed certificates is colored green and includes the organization name and country code rather than the site's domain. The message displayed in the pop-up box when the lock icon is clicked also gives a more detailed message about the identity of the site being "correct". In Internet Explorer, the entire background of the URL bar is colored green in this certificate condition. The information displayed in the area to the right of the lock icon alternates periodically between the organization name/country code, and the CA who issued the certificate. Firefox's identity indicator turns green in this certificate condition and expands to include the organization name and country code; clicking on this button produces the same pop-up as seen for CA-signed certificates, but now fills in the organization name in the "run by" field. Figures 1-4 in Appendix A show the URL bar indicators in each browser, while Figures 10-13 show the associated pop-up dialogues.

Summary Comments Table 1 summarizes the certificate interface features of each web browser; Appendix A shows images of the various interfaces. After examining the security-related interface features of all four browsers, we did not find that any one browser was necessarily better or worse than another in all regards. The main benefit we found in Firefox 3.0 was the constant (though sometimes subtle) presence of an identity indicator regardless of the type of SSL certificate being used, if any. Arguably, its biggest drawback is its treatment of sites using self-signed certificates, which causes users to navigate numerous screens with technically-phrased security messages. Internet Explorer 7.0 has a slightly more obvious indicator for EV-SSL certificates than the other browsers (turning the entire URL background green) and required fewer steps than Firefox to enable visiting a site with a self-signed certificate, although some may argue that this makes it dangerously easy to bypass the warning message in the case of a fraudulent site. We found that both Opera and Chrome use wording that might be more easily understood by the target user; however, their security dialogues are rather long and history suggests that users may consequently skip reading the content of the warnings. We expect that by taking a closer look at these strengths and weaknesses, it would be possible to improve these interfaces, and to address consistency, we strongly encourage interface standards for more effectively displaying certificate information. The W3C Web Security Context Working Group [33] has outlined guidelines and requirements for presenting security information to users; however, these guidelines are currently flexible enough to allow for the inconsistencies we have found in our evaluation.

5 Further Discussion and Steps Toward Improvement

5.1 Strawman Mental Model for Identity Confidence

In section 3.2, we gave analogies for the different types of certificates. It is not clear what current mental model users have for these, if there is a dominant one at all [29]. We suggest the previously-mentioned progression of letterhead/library cards/passports

No SSL Certificate	
IE 7.0	No indicators
Firefox 3.0	Grey background on identity indicator. “This web site does not supply identity information. Your connection to this website is not encrypted.”
Opera 9.6	No indicators
Chrome Beta	No indicators
Self-Signed SSL Certificate	
IE 7.0	Interruption: “There is a problem with this website’s security certificate.” Clicking on a link will continue to the site.
Firefox 3.0	Grey background with warning icon on identity indicator. Interruption:“Secure connection failed.” User must go through a 5-step process to accept the certificate before continuing to the site.
Opera 9.6	Interruption: “This page may not be secure.” Clicking on the “approve” button will continue to the site.
Chrome Beta	Interruption: “The site’s security certificate is not trusted!” Clicking on “proceed anyway” will continue to the site.
CA-Signed SSL Certificate	
IE 7.0	“(Issuer) has identified this site as (domain name)” “This connection to the server is encrypted.”
Firefox 3.0	Blue background on identity indicator. “You are connected to (domain name) which is run by (unknown).” “Your connection to this web site is encrypted to prevent eavesdropping.”
Opera 9.6	Yellow background on identity indicator. “The connection to (domain name) is secure”
Chrome Beta	Yellow background on URL bar. “The identity of this web site has been verified by (issuer)” “Your connection to (domain) is encrypted with XXX-bit encryption”
EV-SSL Certificate	
IE 7.0	Green background on URL bar. “(Issuer) has identified this web site as: (Organization name and address)” “This connection to the server is encrypted.”
Firefox 3.0	Green background on identity indicator. “You are connected to (domain name) which is run by (organization name and address).” “Your connection to this web site is encrypted to prevent eavesdropping.”
Opera 9.6	Green background on identity indicator. “The connection to (domain name) is secure...it can be guaranteed you are connected to (domain name)...”
Chrome Beta	Green text in URL bar. “The identity of (Organization name and address) has been verified by (issuer)” “Your connection to (domain) is encrypted with XXX-bit encryption”

Table 1. Summary of the SSL indicators and dialogs for identity and confidentiality.

as a strawman proposal for a user's mental model of the identity features of self-signed, CA-signed and EV-SSL certificates, based on concepts that most users are familiar with. They imply the same information about an individual's identity as browsers are trying to convey about a site. A certificate is an endorsement of *name* only and not of character. In other words, even with an EV-SSL certificate, we are being assured that the site owner has been verified but not necessarily that the owner is trustworthy. The same applies to the various forms of ID for individuals; while a passport is a fairly reliable document used for identification purposes, it does not necessarily imply anything about a person's character, although a border agent may have additional information linked to a particular passport number. It is also possible that passports (and EV-SSL certificates) are issued in error, and that the systems that verify them fail in their verification.

While there is a clear distinction in identity confidence between a self-signed certificate (no identity confidence) and an EV-SSL certificate (highest level of identity confidence), the identity implications of a traditional CA-signed certificate are not entirely clear. CAs who issue such certificates are generally expected to be trusted third parties who verify the owner's identity, but we have seen that a full SSL certificate can be obtained for as little as $29.99 (possibly with a stolen credit card), with the only verification at the time of the certificate request being the ability to reply from a valid e-mail address; the latter of course is much easier with recent DNS attacks (see Kaminsky [14]). What is even more alarming is the availability of free trial SSL certificates for testing purposes that can be obtained for periods of 15-90 days. Many of these trial certificates are issued using an automated validation process in which the entity requesting the certificate need only reply from a valid e-mail address on the domain [4, 11]. These certificates can also be obtained for IP addresses and, since they still invoke browser cues such as the lock icon, users could be easily fooled if they do not pay attention to URLs. According to a recent report from the Anti-Phishing Working Group [1], ninety days is much longer than the lifespan of most phishing web sites, so a free trial certificate would serve such purposes well. This raises the question of whether or not a traditional SSL certificate can provide any greater confidence in a site's identity than a self-signed certificate.

5.2 Exploring Wording for Conveying Certificate Information

While examining the various interfaces used to display certificate information, none of the four web browsers met all of the requirements of our idea of the target user. We found three major problem areas in terms of the wording used to convey certificate information: (1) some messages used technical terms not easily understood by the typical user, (2) some messages were quite long in an attempt to better explain the information being presented to the user, and (3) some of the wording was misleading or not entirely correct. We examine these problems further below.

Technical Wording As an example, Internet Explorer's dialogue for sites that use certificates includes the wording "this connection to the server is encrypted" to convey the concept of confidentiality. Arguably, the target user we are considering 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's self-signed certificate error message: "The certificate is not trusted because it is self signed. (Error code: sec_error_ca_cert_invalid)." Not only does this message imply that a user should know what the concept of signing a certificate means, but it also includes an error message that means absolutely nothing to the typical user. In addition to these two specific examples, many of the dialogues 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 presumably only understood by highly technical users and should perhaps be hidden at a deeper level in the dialogue boxes.

Lengthy Messages In contrast to using highly technical terms to convey certificate information, we noticed that Opera and Chrome in particular made an effort to explain the concepts to users more thoroughly; this unfortunately resulted in fairly lengthy dialogues. Chrome Beta, for example, presents the user with a lengthy dialogue 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 their wording seems fairly easy to understand, past experience suggests few users will take the time to read such a lengthy message. Furthermore, users seeing such a long message frequently become conditioned to simply dismiss the warning (see Kumaraguru et al. [15]).

Misleading or Confusing Wording Possibly the most common problem we observed across the various interfaces was the existence of misleading or confusing wording in the dialogues to the user. One particular such aspect was messages relating to the "security" of the site. For sites using self-signed certificates, Opera displayed a message indicating "This page may not be secure." User interpretation of this message depends on the meaning of the term "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 it could be very possible that the page is in fact secure (here meaning, reliably providing confidentiality). The message displayed by Chrome for a site having an EV-SSL certificate includes the wording "it can be guaranteed that you are actually connected to..." "Guaranteed" is surely too strong a word to use in this case; it implies that all known and future attacks are impossible, and that attackers will never find a way to spoof an EV certificate, and that CAs will not make any errors in issuing certificates (despite past experience otherwise [18, 19, 23]). We are aware of no such proofs or convincing arguments to date.

One of the potentially more controversial wordings is in the Firefox messages that distinguish standard SSL certificates from EV certificates. The identity indicator pop-up box says "you are connected to (insert domain name) which is run by (insert organization name)" for sites with standard SSL or EV-SSL certificates. However, the organization name is only filled in properly on sites with EV-SSL certificates; for standard SSL certificates, this field is populated with (unknown). To illustrate the problem with this, we visited two well known banking web sites – Wells Fargo in the United States and Royal Bank of Canada. On the Wells Fargo web site, the Firefox identity indicator message reads "You are connected to wellsfargo.com which is run by (unknown)"; a similar message is displayed on the Royal Bank web site: "You are connected to rbc.com which is run by (unknown)." Considering sensitive banking transactions, it stands to reason that this should 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 illustrates the need for reworking these design choices.

5.3 Suggestions for Improvement

In this section, we offer suggestions and alternatives to current dialogues as a starting point for improvement, and solicit feedback.

Our first suggestion is a call to arms for consistency across the various web browsers. It is true that many users typically only make use of one web browser; however, there are instances in which users will encounter unfamiliar browsers such as at their work place, at a public Internet terminal, or at a friend's house. These users cannot be expected to understand cues presented about certificates when each browser does this differently. In the interest of ensuring consistency, we also recommend the use of consistent indicator(s) for identity and confidentiality, to be displayed for all sites – even those with no SSL certificate. Sobey et al. [29] evaluated one such indicator that could be used for this purpose.

We next suggest making a clear separation between identity and confidentiality indicators, since these are in fact two orthogonal 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 with the site in question, we expect that users would be able to form a better mental model and appropriate levels of confidence they should have in the site identity (authenticity), and the confidentiality of information sent to or received from it. We also strongly suggest avoiding ambiguous terms like "secure" in these messages; these terms can only cause users to draw vague conclusions about the "safety" of the site without separating the implications of confidence in identity and confidentiality, let alone failing to take into account other issues such as malware on legitimate sites or on end-user machines themselves.

In terms of confidentiality, the only distinction we presently see is between sites that do not use SSL certificates and sites who do use any of the three types of SSL certificate. For sites which do not use SSL, we suggest wording such as *"Information sent to and from this web site is not private (i.e., is publicly visible)."* We feel that a mental model involving the idea of the user interacting with a site is preferable to one involving a server or even the actual organization hosting the site. Indicating that the information 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, we suggest the wording *"Information sent to and from this web site is private (i.e., is not publicly visible)."* While not all SSL connections are necessarily trustworthy (i.e., with a second party that is known and trusted), the encryption does provide privacy from third parties; adding separate messaging about identity is necessary to explain how much trust a user should place in that private connection.

For identity-related messages, we believe that wording such as "recognized authority" or "certification authority" are too vague and easily misunderstood by many users. We expect that more users are familiar with the concept of a third party and that this is a better way of describing the relationship with a certification authority. Also, third party is more neutral and therefore accurate (it may be a trusted or untrusted party), whereas "recognized authority" and "certification authority" suggest, possibly incorrectly at times (e.g., for free, trial certificates with uncorroborated subject names), trustworthiness. For sites with no certificate, we therefore suggest a simple message such as *"This web site has not supplied a name (identity) that has been verified by any third party"*. For self-signed certificates, the message would change only slightly to *"This web site has supplied a name (identity) but that name has not been verified by any third party."* For CA-signed certificates we suggest *"This web site has supplied a name (identity) that has been verified by a third party,"* and EV-SSL certificates might extend this message to include the name of the issuer as is often being done in current interfaces. For example, *"This web site has supplied a name (identity) that has been verified by Verisign, Inc."* Our objective with these messages is to keep them as simple as possible for the target user, while allowing more advanced users to access full details of the certificate information, such as issuing authorities and encryption protocols, using similar drill-down functionality as currently implemented in web browsers.

We emphasize that none of our suggested messages involves any use of the word "certificate" (nor any level of certificate) – we see no more reason for a browser user to understand levels of certificates than for an automobile driver to require knowledge of how many pistons are in their car. Also, we avoid the ambiguous word "secure."

6 Conclusion and Future Work

We have explored a number of open issues with respect to SSL certificates and the interfaces used to display this information to the user. We have also proposed some possible analogies and message wordings related to the various types of certificates that may help users to form better mental models, in the sense that they lead to less confusion and increase the chances of appropriate user responses to cues and messaging related to SSL certificates. While the CA/Browser Forum outlines specific goals of EV-SSL certificates, other parties may have competing objectives. For example, one viewpoint put forth by others is that the purpose of EV-SSL certificates is to increase the completion rate in on-line 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 easier to use than competing browsers, which might suggest minimizing dialogues or interventions which block web sites. The possibility of such competing objectives does not simplify the design problem of the community as a whole.

Our aim here was to define the problem clearly, to explore some possible alternatives, and to gain a consensus on what the real problem is prior to carrying out a full user study. As mentioned in the paper, there are currently inherent problems in the SSL certificate infrastructure itself, such as legitimate non-SSL sites that request sensitive information or certificates that are issued in error, but even if these problems were solved we are still left with the fundamental interface problems. We are currently testing prototypes informally and plan to follow with a full usability test when these prototypes appear suitable; this would complement our earlier user study [29]. However, even if we were to establish a good metaphor for the four different certificate conditions, it remains unclear at present if this could be implemented into browsers in a way easily understood by the common user while not easily mimicked by attackers. Regardless, we strongly suggest that browser designers work together on common standards for interface cues and messaging related to SSL certificates that will both promote and/or support an effective mental model and ensure that site identity and confidentiality protection levels are being conveyed effectively. We should also keep in mind that by following a path seeking to incrementally improve the current situation (e.g., by altering the wording in dialogue boxes, and searching for better metaphors to support effective mental models), we may inch toward a design which is a local optimum far from what might otherwise be possible in alternate frameworks. If a significantly more effective interface is not found or possible, then it may be necessary to consider redesigning the hierarchy and framework of SSL certificates from scratch.

Acknowledgments. 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. Funding from NSERC ISSNet is also acknowledged.

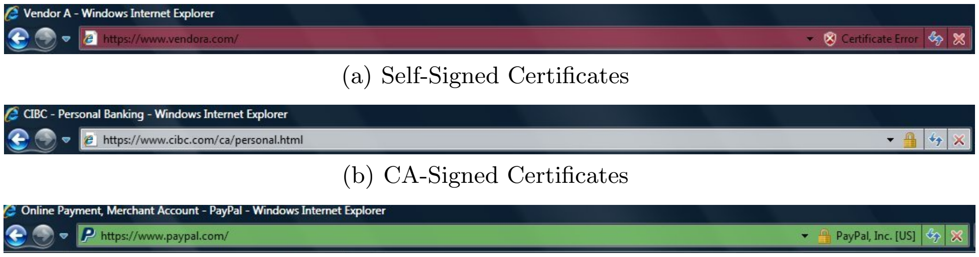
References

1. Anti-Phishing Working Group. Phishing Activity Trends: Report for the Month of January 2008. http://www.antiphishing.org/reports/apwg_report_jan_2008.pdf
2. Apple Inc. Apple - Safari, http://www.apple.com/safari/
3. CA/Browser Forum, http://www.cabforum.org/
4. Comodo. Free SSL Certificate Trial, http://www.instantssl.com/ssl-certificate-products/free-ssl-certificate.html/
5. Dhamija, R., Tygar, J.: The Battle Against Phishing: Dynamic Security Skins. In: Proceedings of the Symposium on Usable Privacy and Security (2005)
6. Dhamija, R., Tygar, J., Hearst, M.: Why Phishing Works. In: Human Factors in Computing Systems (CHI 2006), April 22-27 (2006)
7. 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).
8. Franco, R. Better Website Identification and Extended Validation Certificates in IE7 and Other Browsers, http://blogs.msdn.com/ie/archive/2005/11/21/495507.aspx
9. GoDaddy.com. SSL Certificates, http://www.godaddy.com/gdshop/ssl/ssl.asp?ci=8979
10. Google. Google Chrome Beta, http://www.google.com/chrome
11. ipsCA. Free SSL Certificates, http://certs.ipsca.com/Srvc/free_ssl.asp
12. Jackson, C., Simon, D.R., Tan, D.S., Barth, A.: An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks. In: Proc. of Usable Security (2007)
13. K Desktop Environment. Konqueror, http://www.konqueror.org/features/browser.php
14. Kaminsky, D. Black Ops 2008: Its The End Of The Cache As We Know It. Black Hat Briefings USA, August 6-7 (2008)
15. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J., and Nunge, E.: Protecting People From Phishing: The Design and Evaluation of an Embedded Training Email System. In Proceedings of the 2007 Computer Human Interaction (2007)
16. Microsoft: Extended Validation SSL Certificates, http://www.microsoft.com/windows/products/winfamily/ie/ev/default.mspx

17. Microsoft: Internet Explorer 7.0 Features, http://www.microsoft.com/windows/products/winfamily/ie/features.mspx
18. Microsoft: Microsoft Security Bulletin MS01-017 (March 22, 2001; updated March 28, 2001), Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard, http://www.microsoft.com/technet/security/bulletin/ms01-017.mspx
19. Molnar, D., Stevens, M., Lenstra, A., de Weger, B., Sotirov, A., Appelbaum, J., Osvik, D. A.: MD5 Considered Harmful Today: Creating a Rogue CA Certificate. 25th Chaos Communication Congress, Berlin, Germany, December 30 (2008)
20. Mozilla: EV-Certs for Firefox, http://mozillalinks.org/wp/2007/05/ev-certs-for-firefox/
21. Mozilla. Mozilla Firefox 3.0, http://www.mozilla.com/en-US/firefox/
22. Nightingale, J.: Personal Communication, September 19th (2007)
23. Nigg, E. Untrusted Certificates. Personal blog, December 23, 2008, https://blog.startcom.org/?p=145
24. OpenSSL. OpenSSL: The Open Source toolkit for SSL/TLS, http://www.openssl.org/
25. Opera Software, http://www.opera.com
26. Rescorla, E.: SSL and TLS: Designing and Building Secure Systems, Addison-Wesley, ISBN 0-201-61598-3 (2001)
27. Schechter, S.E., Dhamija, R., Ozment, A., Fischer, I.: The Emperor's New Security Indicators. In Proc. of the 2007 IEEE Symposium on Security and Privacy, May (2007)
28. Smith, S.W.: Humans in the Loop: Human-Computer Interaction and Security. IEEE Security and Privacy. 1 (3): 75–79. May/June (2003)
29. Sobey, J., Biddle, R., van Oorschot, P.C., Patrick, A.S.: Exploring User Reactions to New Browser Cues for Extended Validation Certificates. In Proc. of the European Symposium on Research in Computer Security (ESORICS), October (2008)
30. Thawte: Extended Validation SSL Certificates – solving a trust problem https://www.thawte.com/ssl-digital-certificates/free-guides-whitepapers/pdf/ev_whitepaper.pdf
31. Whalen, T. and Inkpen, K.: Gathering Evidence: Use of Visual Security Cues in Web Browsing. In: Proc. of Graphics Interface 2005, pp. 137–145, May (2005)
32. Whitten, A., Tygar, J.D.: Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium, August (1999)
33. World Wide Web Consortium. Web Security Context: User Interface Guidelines (working draft 24 July 2008). http://www.w3.org/TR/2008/WD-wsc-ui-20080724/
34. Z. Ye, S. Smith, and D. Anthony. Trusted paths for browsers. ACM Transactions on Information and System Security, pages 153-186, May (2005).

APPENDIX A
SSL Certificate Interfaces in Major Web Browsers

The following figures portray the interface cues for SSL certificates in current web browsers. In Section 4, we provide a comparison of these interface features and explore relevant problems users may face when encountering these cues.

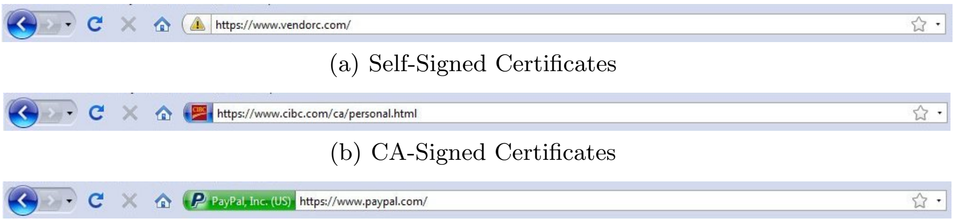

Vendor A - Windows Internet Explorer
https://www.vendora.com/
Certificate Error
CIBC - Personal Banking - Windows Internet Explorer
https://www.cibc.com/ca/personal.html
Online Payment, Merchant Account - PayPal - Windows Internet Explorer
https://www.paypal.com/
PayPal, Inc. [US]

(a) Self-Signed Certificates

(b) CA-Signed Certificates

(c) EV-SSL Certificates

Fig. 1. Microsoft IE 7.0 URL bars in the three certificate states

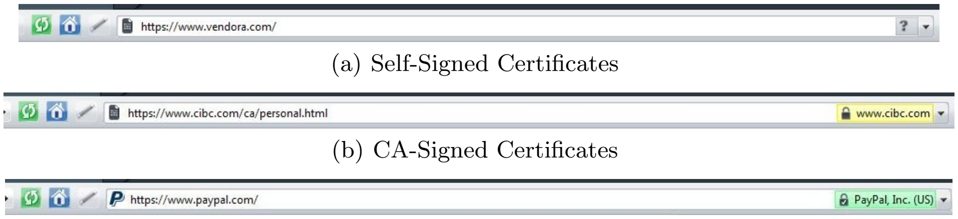


(a) Self-Signed Certificates

(b) CA-Signed Certificates

(c) EV-SSL Certificates

Fig. 2. Mozilla Firefox 3.0 URL bars in the three certificate states

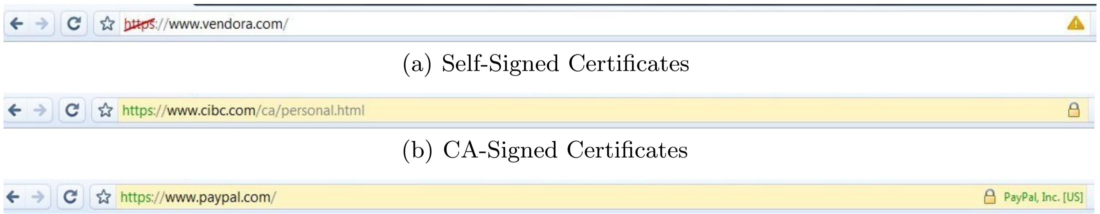


(a) Self-Signed Certificates

(b) CA-Signed Certificates

(c) EV-SSL Certificates

Fig. 3. Opera 9.6 URL bars in the three certificate states

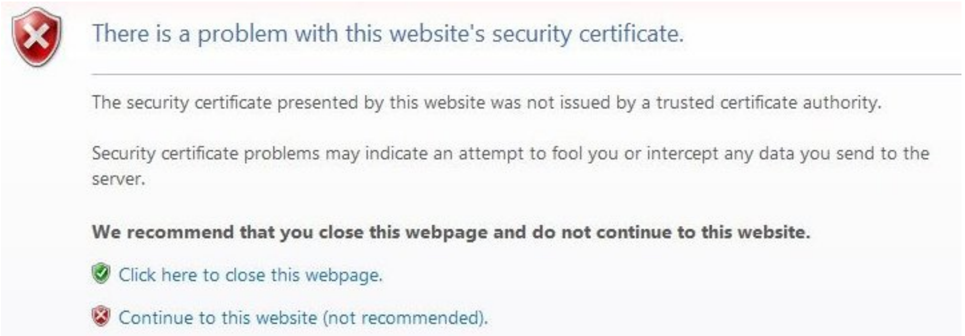

~~https~~://www.vendora.com/
https://www.cibc.com/ca/personal.html
https://www.paypal.com/
PayPal, Inc. [US]

(a) Self-Signed Certificates

(b) CA-Signed Certificates

(c) EV-SSL Certificates

Fig. 4. Google Chrome URL bars in the three certificate states



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

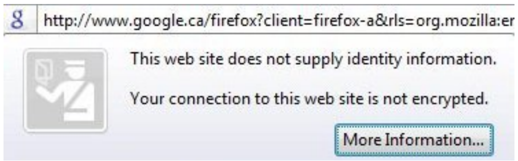
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

Fig. 5. Interruption encountered when visiting a website with a self-signed certificate in IE 7.0

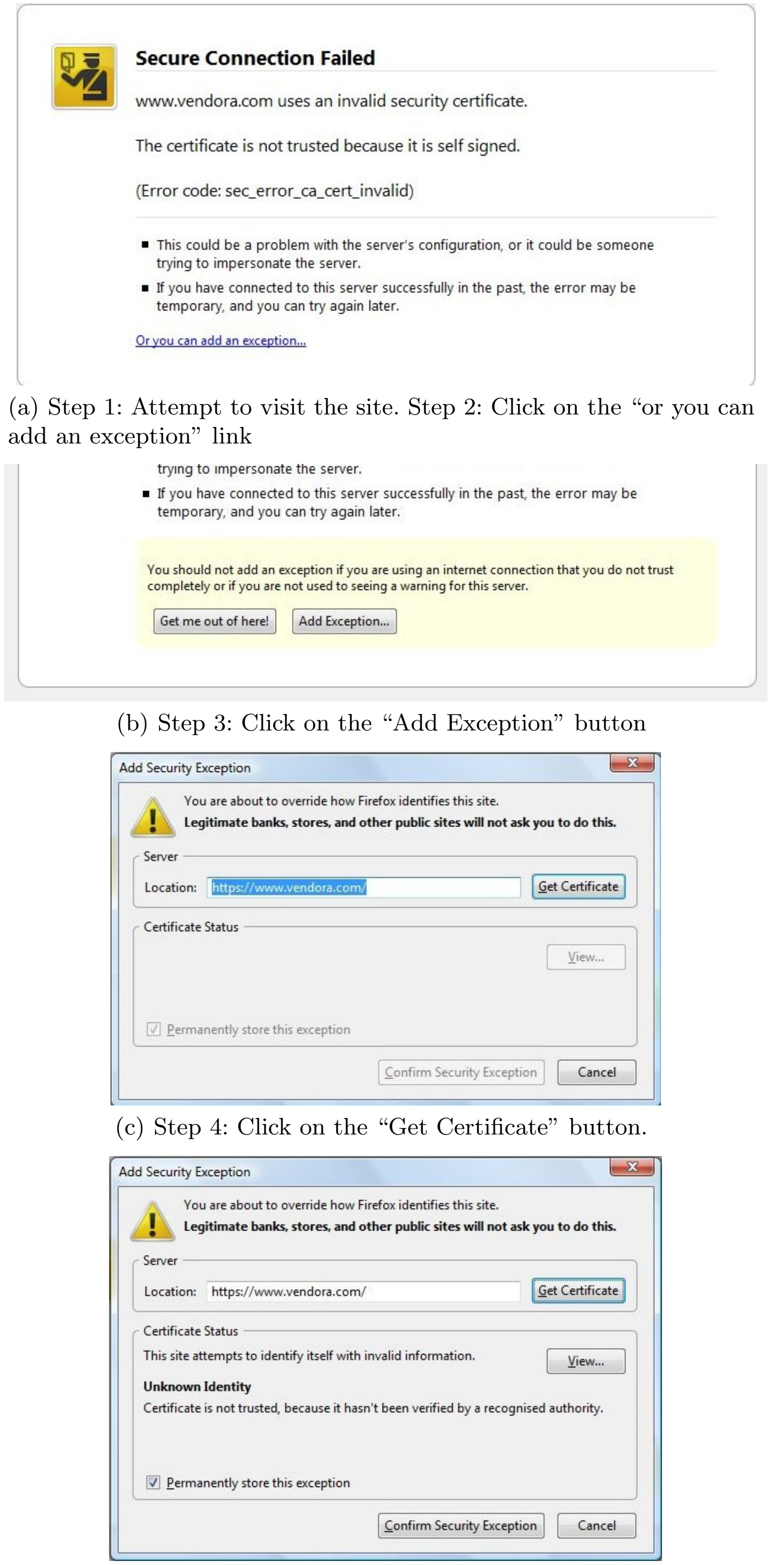


http://www.google.ca/firefox?client=firefox-a&rls=org.mozilla:er

This web site does not supply identity information.

Your connection to this web site is not encrypted.

Fig. 6. Firefox 3.0's identity pop-up box for a site having no SSL certificate



Secure Connection Failed

www.vendora.com uses an invalid security certificate.

The certificate is not trusted because it is self signed.

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception...

(a) Step 1: Attempt to visit the site. Step 2: Click on the "or you can add an exception" link

trying to impersonate the server.

- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

(b) Step 3: Click on the "Add Exception" button

Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://www.vendora.com/

Certificate Status

☑ Permanently store this exception

(c) Step 4: Click on the "Get Certificate" button.

Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://www.vendora.com/

Certificate Status

This site attempts to identify itself with invalid information.

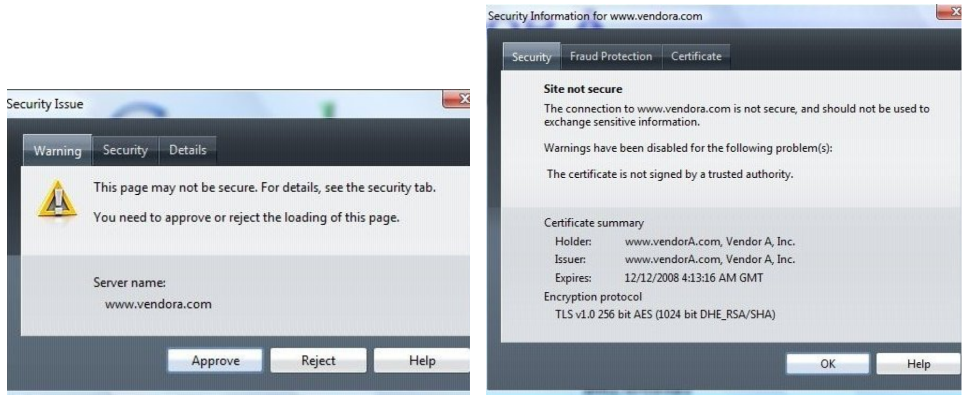
Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognised authority.

☑ Permanently store this exception

(d) Step 5: Click on the "Confirm Security Exception" button.

Fig. 7. Steps involved in visiting a website with a self-signed certificate in Firefox 3.0



Security Issue

This page may not be secure. For details, see the security tab.

You need to approve or reject the loading of this page.

Server name:
www.vendora.com

Security Information for www.vendora.com

Site not secure

The connection to www.vendora.com is not secure, and should not be used to exchange sensitive information.

Warnings have been disabled for the following problem(s):

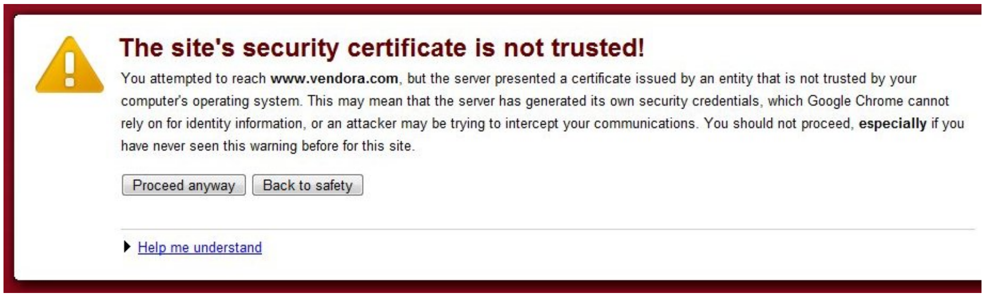
The certificate is not signed by a trusted authority.

Certificate summary
Holder: www.vendorA.com, Vendor A, Inc.
Issuer: www.vendorA.com, Vendor A, Inc.
Expires: 12/12/2008 4:13:16 AM GMT
Encryption protocol
TLS v1.0 256 bit AES (1024 bit DHE_RSA/SHA)

(a) Pop-up upon entering the URL for the site.

(b) Click on the "OK" button to proceed to the page.

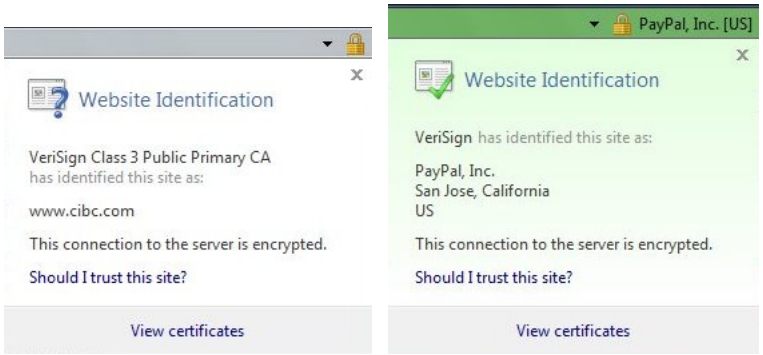
Fig. 8. Dialogs involved in visiting a website with a self-signed certificate in Opera 9.6



The site's security certificate is not trusted!

You attempted to reach **www.vendora.com**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

Fig. 9. Dialog encountered when visiting a website with a self-signed certificate in Chrome Beta



Website Identification

VeriSign Class 3 Public Primary CA
has identified this site as:

www.cibc.com

This connection to the server is encrypted.

Should I trust this site?

View certificates

(a) CA-Signed Certificates

PayPal, Inc. [US]

Website Identification

VeriSign has identified this site as:

PayPal, Inc.
San Jose, California
US

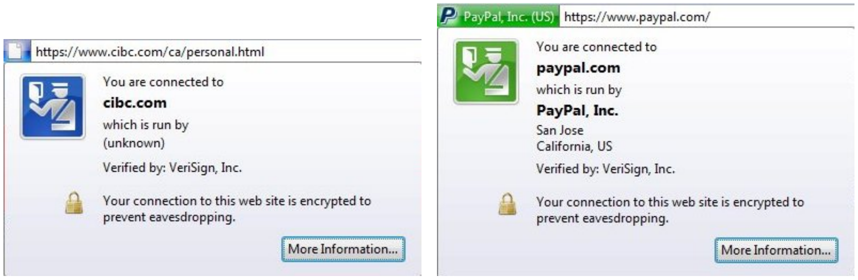
This connection to the server is encrypted.

Should I trust this site?

View certificates

(b) EV-SSL Certificates

Fig. 10. IE 7.0's certificate pop-up box for sites with CA-signed vs. EV-SSL certificates



https://www.cibc.com/ca/personal.html

You are connected to
cibc.com
which is run by
(unknown)

Verified by: VeriSign, Inc.

Your connection to this web site is encrypted to prevent eavesdropping.

More Information...

(a) CA-Signed Certificates

PayPal, Inc. (US) https://www.paypal.com/

You are connected to
paypal.com
which is run by
PayPal, Inc.
San Jose
California, US

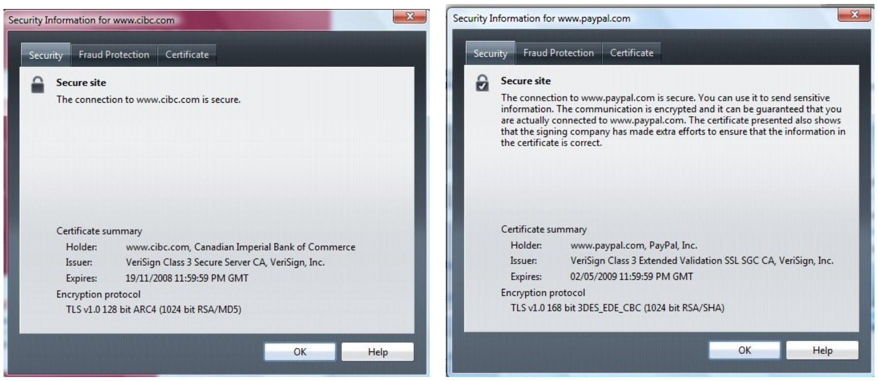
Verified by: VeriSign, Inc.

Your connection to this web site is encrypted to prevent eavesdropping.

More Information...

(b) EV-SSL Certificates

Fig. 11. Firefox 3.0's identity pop-up box for sites with CA-signed vs. EV-SSL certificates



Secure site

The connection to www.cibc.com is secure.

Certificate summary

Holder:	www.cibc.com, Canadian Imperial Bank of Commerce
Issuer:	VeriSign Class 3 Secure Server CA, VeriSign, Inc.
Expires:	19/11/2008 11:59:59 PM GMT

Encryption protocol

TLS v1.0 128 bit ARC4 (1024 bit RSA/MD5)

Secure site

The connection to www.paypal.com is secure. You can use it to send sensitive information. The communication is encrypted and it can be guaranteed that you are actually connected to www.paypal.com. The certificate presented also shows that the signing company has made extra efforts to ensure that the information in the certificate is correct.

Certificate summary

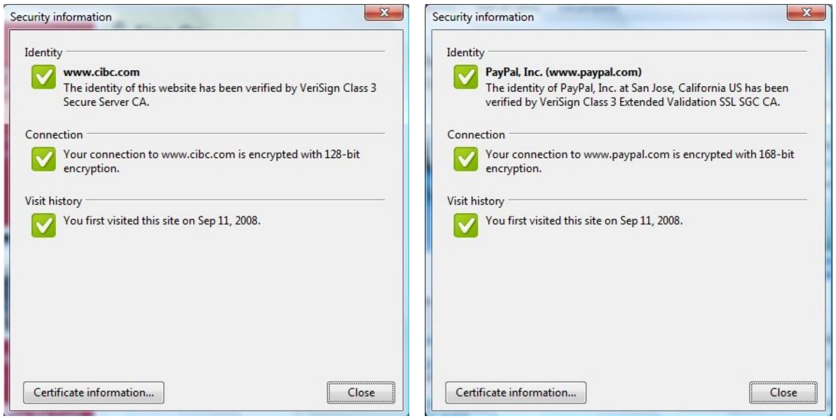
Holder:	www.paypal.com, PayPal, Inc.
Issuer:	VeriSign Class 3 Extended Validation SSL SGC CA, VeriSign, Inc.
Expires:	02/05/2009 11:59:59 PM GMT

Encryption protocol

TLS v1.0 168 bit 3DES_EDE_CBC (1024 bit RSA/SHA)

(a) CA-Signed Certificates (b) EV-SSL Certificates

Fig. 12. Opera 9.6's certificate pop-up box for sites with CA-signed vs. EV-SSL certificates



www.cibc.com

The identity of this website has been verified by VeriSign Class 3 Secure Server CA.

Your connection to www.cibc.com is encrypted with 128-bit encryption.

You first visited this site on Sep 11, 2008.

PayPal, Inc. (www.paypal.com)

The identity of PayPal, Inc. at San Jose, California US has been verified by VeriSign Class 3 Extended Validation SSL SGC CA.

Your connection to www.paypal.com is encrypted with 168-bit encryption.

You first visited this site on Sep 11, 2008.

(a) CA-Signed Certificates (b) EV-SSL Certificates

Fig. 13. Chrome Beta's certificate pop-up box for sites with CA-signed vs. EV-SSL certificates