Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study

Robert Biddle, P.C. van Oorschot, Andrew S. Patrick, Jennifer Sobey, Tara Whalen
Carleton University, Ottawa, ON, Canada
SSL Certificates & Cloud Computing

NIST Information Technology Laboratory: “Effectively and Securely Using the Cloud Computing Paradigm” (July 2009)

“All key issues: trust, multi-tenancy, encryption, compliance”

“Security and data privacy concerns are the two critical barriers to adopting cloud computing”

- includes data encryption in transit (e.g., to data storage services) over SSL
Open Letter to Google

Re: “Ensuring adequate security in Google’s cloud based services”

• encryption is not enabled by default for information transmitted by users of Google Mail, Docs, or Calendar

• reasoning: performance issues; choice to enable is left up to users

“If Google believes that encryption and protection from hackers is a choice that should be left up to users, the company must do a better job of informing them of the risks so that they are equipped to make this choice...the sparse information describing encryption options is hidden, and presented in terms that few members of the general public will understand.”
Usable security issues in the cloud

- as highlighted in letter to Google
- data protection is critical in many web-based services
- information about data protection is often hidden or confusing to non-technical users
- similar usability problems arise in the SSL certificates used on the web servers providing these services
Certificate Usability Problems

- failure to consider target user (non-expert)
- entangling identity with confidentiality
- poorly-conveyed certificate information
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...
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.

[Buttons: Proceed anyway, Back to safety]

Help me understand

When you connect to a secure website, the server hosting that site presents your browser with something called a “certificate” to verify its identity. This certificate contains identity information, such as the address of the website, which is verified by a third party that your computer trusts. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are securely communicating with the website you intended, and not a third party (such as an attacker on your network).

In this case, the certificate has not been verified by a third party that your computer trusts. Anyone can create a certificate claiming to be whatever website they choose, which is why it must be verified by a trusted third party. Without that verification, the identity information in the certificate is meaningless. It is therefore not possible to verify that you are communicating with www.vendora.com instead of an attacker who generated his own certificate claiming to be www.vendora.com. You should not proceed past this point.

If, however, you work in an organization that generates its own certificates, and you are trying to connect to an internal website of that organization using such a certificate, you may be able to solve this problem securely. You can import your organization’s root certificate as a “root certificate”, and then certificates issued or verified by your organization will be trusted and you will not see this error next time you try to connect to an internal website. Contact your organization’s help staff for assistance in adding a new root certificate to Windows.
Confusing Wording: Opera 9

Security Issue

Warning  Security  Details

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

Approve  Reject  Help
Entangling Site Identity and Confidentiality

- data sent over SSL channel: https and lock used as indicators
- website identity and channel encryption are often conflated
- studies (e.g., Dhamija et al., 2006) have shown that users associate lock with "being safe"
- what if user is sending encrypted data to unknown or untrusted party?
Complicating the Issue: 
EV Certificates

“Extended Validation” certificates: response to phishing and fraud

- introduced by CA/Browser forum (CAs and browser vendors)
- some requirements for obtaining EV cert (e.g., from Verisign):
  - must be registered entity (not an individual)
  - confirmed physical existence/business presence
  - letter proving requestor is authorized by company to obtain cert
  - at least $1000
Complicating the Issue: EV Certificates

Now there are four grades of certificates for users to keep track of:

- none; self-signed; basic SSL; EV SSL

How can users distinguish and interpret differences in certificate types?

Do EV certificates “downgrade” the other types?
Proposed Certificate Designs

- we reviewed existing certificate designs and their problems
- we created a new set of experimental designs for evaluation
  - tried to make messages clear, short, and informative
    - avoided “secure”; “encryption”; “certification authority”
  - separated identity and confidentiality elements
- added icons for visual identification of elements
Example Design: EV certificate

Identity Confidence: High
This web site claims to be

Standard Bank Ltd.
and this has passed extended confirmation by

Verisign, Inc.

Privacy Protected: Yes
Information sent to and from this web site is protected from eavesdropping.
Identity Confidence: Low
This web site has not provided a name for identity confirmation.

Privacy Protected: No
Information sent to and from this web site is vulnerable to eavesdropping.

Identity Confidence: Low
This web site claims to be
standardbank.com
but this has not been confirmed by any authority

Privacy Protected: Yes
Information sent to and from this web site is protected from eavesdropping.

Identity Confidence: Medium
This web site claims to be
standardbank.com
and this has passed basic confirmation by
Verisign, Inc.

Privacy Protected: Yes
Information sent to and from this web site is protected from eavesdropping.

Identity Confidence: High
This web site claims to be
Standard Bank Ltd.
and this has passed extended confirmation by
Verisign, Inc.

Privacy Protected: Yes
Information sent to and from this web site is protected from eavesdropping.
User Study on Certificates: Overview

We evaluated certificate designs, in order to:

☐ better understand which interface details users comprehend

☐ determine how easily users distinguish identity from encryption

Study with 40 participants

☐ compared proposed design with IE 7 certificates

☐ sample questions: “Who does this web site belong to? Please rate how certain you are on a 1-7 scale.”
Example IE 7 certificate (EV)

VeriSign has identified this site as:

Standard Bank Ltd.
Toronto, Ontario
CA

This connection to the server is encrypted.

Should I trust this site?

View certificates
Self-signed

Untrusted Certificate

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

This problem may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

View certificates

Basic

Website Identification

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

standardbank.com

This connection to the server is encrypted.

Should I trust this site?

View certificates
User Study: Method

- recruited on university campus (email lists, posters)
- participants needed to be experienced with web browsing, have normal color vision
- faculty, staff and students all eligible
- 40 participants: 13 male, 27 female, aged 18-59
- 55% were students; 45% were staff (primarily in administration)
- 78% used online banking (study used a simulated online bank scenario)
User Study: Materials

- within-subjects design with two different sets of certificates: alternative design and Internet Explorer 7
- showed designs for four certificate types: no certificate; self-signed; basic; EV
- IE has no design for “no certificate”: showed seven images in all
- counterbalanced: half the participants saw IE first, half saw alternative
- randomized order of certificate type (e.g., self-signed, EV...) shown
- participants answered questions while viewing images
Finding and Understanding Certificate Information

- on 7-point scales, indicate how easy it was to find and to understand
  - web site ownership information (who owns this web site?)
  - whether or not data was safe from interception in transit
- improvements shown for alternative design (statistically significant):
  - ownership information rated as easier to find for both self-signed and basic certificates
  - information about data safety in transit rated as easier to find for basic and EV certs
  - information about data safety in transit rated as easier to understand for basic and EV certs
Technical terminology

- technical language shown to be an impediment to understanding

- protection of data in transit

“I don’t know if my information is safe, because I don’t know what ‘encrypted’ means.”
Confidence in Ownership and Data Safety

☐ on 7-point scales, indicate how certain you are about
  • web site ownership information (who owns this web site?)
  • whether or not data was safe from interception in transit

☐ improvements shown for alternative design (statistically significant):

☐ for safety of data in transit: for self-signed and basic certs, participants were more certain about the safety information
Accuracy of Security Assessment

☐ asked participants “Is data sent to this web site safe from interception in transit?” [avoided using the word “encrypted”]
☐ our interpretation: encryption means “safe in transit”

☐ for self-signed:
  ☐ 26/40 participants viewing alternative design said “yes” [correct]
  ☐ 2/40 participants viewing IE design said “yes”

☐ for EV:
  ☐ 38/40 participants viewing alternative design said “yes” [correct]
  ☐ 29/40 participants viewing IE design said “yes”
Willingness to Enter Bank Information

- on 7-point scale, indicate how likely you are to enter your bank account number and password, if this was your bank

- for self-signed: likelier to enter information in alternative design

- however, likelihood still very low: 1.10 for IE, 1.80 for alternative, where 1 = “not at all likely”
Opinions about Icons

- Participants rated the icons in each design: how well they matched the text that they accompanied.
- Note that alternative icons remained static throughout: text changed.
- Two cases where alternative design rated lower than IE.
EV cert: for alternative design, the identity icon (head w/question mark) rating was poorest for EV: thought to be incongruous with high identity confidence
self-signed: alternative privacy icon rated lower than IE icon: IE icon rated high, because self-signed message is very negative (warning)
Interface Preferences

- two sets of designs (alternative, IE): overall, which design was
  - easier to understand
  - gave more confidence in web site ownership
  - gave more confidence in safety of data in transit
  - which design was preferred overall

- alternative design chosen in the first three aspects but not the fourth
  - likely: aesthetic grounds (colour); familiarity with Windows/IE design
modest re-design led to improvements in user understanding, ease of finding information

better refinement of overall visual design could lead to improvements

but: overall, are we working with a flawed basic model?

requires more than simple adjustments
Self-Signed & Safety of Data in Transit

- question: is data safe in transit in the case of self-signed certificates?
- if interpreted in end-to-end scenario – safe from eavesdropping – then yes, this is true
- however, could be interpreted as safe at the endpoint as well (“is the other party trustworthy?”)—but this is not fulfilled by encryption
- majority of people thought IE self-signed message indicated that data was not safe in transit
- “This may indicate an attempt to...intercept any data you send to the server” : choice of wording suggests insecurity in transit
Self-signed Certificates

- participants were confused by the self-signed case in alternative design: how can there be private transmission to an untrusted party? These concepts seen as incongruous

- IE’s self-signed message is highly negative, acting as a warning: is there little room for legitimate use of this cert?

- options such as Wendlandt et al.’s Perspectives (2008) could be helpful here: “trust on first use” systems

- network of notaries for checking site’s public key; keeps record of key over time (i.e., has key changed recently -- is it reliable?)
EV Certificates

- if self-signed certificates are downgraded, what about basic (domain-validated) certificates?
- seen as inferior to EV certs?
- Firefox 3 states web site is “run by (unknown)” for basic certificate, which looks like a warning
- where does this leave small business owners, individuals?
Conclusions

- purpose of study was to gain insights into users’ comprehension of SSL certs

- study demonstrated that simple changes led to significant differences in perception and understanding

- lack of consistency across browsers can lead to confusing user experience (especially with many grades of certificate)

- rather than incremental design improvements, radical changes to the SSL framework may be necessary for real progress
Questions?

Contact: tjwhalen@gmail.com