Toward Web Browsers that Make or Break Trust

Hazim Almuhimedi
School of Computer Science
Carnegie Mellon University
hazim@cmu.edu

Amit Bhan
Heinz School of Public Policy and Management
Carnegie Mellon University
abhan@andrew.cmu.edu

Dhruv Mohindra
Heinz School of Public Policy and Management
Carnegie Mellon University
dmohindr@andrew.cmu.edu

Joshua S. Sunshine
School of Computer Science
Carnegie Mellon University
josh.sunshine@cs.cmu.edu

1. INTRODUCTION

The Internet as we know it today depends on secure communication—electronic commerce relies on the private transmission of payment information, social networking sites and configurable portals on the secret exchange of login credentials, etc. Certificates and encryption are the fundamental building blocks of the Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols used to protect transmitted data.

Modern browsers handle the majority of the workload necessary to communicate securely over the web: encryption of outgoing data, decryption of incoming data, validation of certificates, storage of certificates, maintenance of trusted certificate authority list, etc. However, browsers rely on users to perform (at least) two tasks to support secure communication: recognize encrypted websites and respond to invalid certificates. Studies have confirmed that these tasks are unusable—users do not notice or do not understand encryption identification mechanisms in browsers [1, 2] and connect to websites with invalid certificates just as they connect to websites with valid certificates [3].

Browser designers have recognized this fundamental flaw in their design and both major browsers have implemented substantial changes to their certificate management interfaces in their upcoming releases—Firefox 3 and Internet Explorer 8. In this paper, we describe the two-pronged experimental evaluation of the relevant features of Firefox 3. The first prong is a 270 user online survey which asked users to evaluate a screenshot of a website displayed using Firefox 2 or 3 and identify if the website was encrypted. The second prong is a 10 user lab study which compared the reaction of users to invalid certificates from both familiar and unfamiliar websites in Firefox 2 and 3.

2. CERTIFICATE MANAGEMENT

An encrypted website is identified in Firefox 2 in three ways: 1) The URL begins with https. 2) The address bar is yellow instead of white. 3) There is a lock icon on the right side of the address bar and in the status bar. Firefox 3 adds a favicon popup to this list – a small window that appears when the user clicks on the favicon displaying the certificate authority, domain name, lock icon, and the message "Your connection to this website is encrypted to prevent eavesdropping." In addition, the lock icon does not appear on the address bar (and therefore does not appear at all if the status bar is disabled). Firefox recognizes extended validation, by adding a green rectangle displaying the name of the corporation responsible for the website to the address bar.

When a user visits a website with an invalid certificate in Firefox 2 a dialog appears, titled "Unable to identify <domain name> as a trusted site." Users are presented with three options are including the default, "Accept this certificate temporarily for this session." Finally, the dialog contains two buttons, "OK" and "Cancel." We believe that the vast majority of users click "OK," accepting the default, without further thought although we have not verified this assumption empirically. Firefox 3, instead presents users with a full page error message containing only one actionable item, a link titled "Or you can add an exception..." Once the user clicks on this link a box opens up in the same window presenting the user with two buttons: "Get me out of here!" or "Add Exception..." Clicking "Add Exception..." will open another dialog box. The user then clicks two more buttons to add the exception – "Get Certificate" and "Confirm Security Exception." Adding a certificate in Firefox 3 requires at least 4, not particular simple, user actions as compared to one simple action in Firefox 2.

3. ENCRYPTION NOTIFICATION SURVEY

We evaluated the encryption notification mechanisms with an online survey completed by 270 participants. Each user saw two randomly selected images in a random order: one of a small bank, Sanford Institution for Savings, and one of Google, Ask, or Wikipedia. Eight screenshots of Sanford were used: (a) Firefox 2, Encrypted (b) Firefox 2, Unencrypted (c) Firefox 3, Encrypted (d) Firefox 3, Unencrypted (e) Firefox 3, Encrypted with Favicon Popup (f) Firefox 3, Encrypted without Extended Validation (g) Firefox 3, Encrypted with Favicon Popup off the Browser Chrome (h) Firefox 2, Unencrypted with Favicon Popup off Browser Chrome. Users were asked two questions about each image. The first, a yes/no question, asked "Does the webpage displayed in the image to the left use encryption?" Screenshots b, d, and h are unencrypted so the correct answer is 'No.' The second, a free response question, asked "How do you know?"

The most interesting results are contained in the answers to the encryption question for all Sanford screenshots. Image (c), which represents the Sanford website as it displays

by default in Firefox 3, confuses more users than Image (a) which is the Firefox 2 equivalent (Firefox 3 58% Correct vs. Firefox 2 71% Correct). The Sanford websites pays GoDaddy for extended validation and Image (c) reflects that fact. Users are not used to extended validation yet so one might think that the difference just discussed represents extended validations newness. However, Image (f), displays the Sandford website as if it did not have extended validation but the situation hardly improves.

Users are dramatically better at determining that the Sanford website is encrypted when one shows them the Favicon popup as in Image (e). They correctly decide that the website is encrypted 79% of the time. However, there is a fairly straightforward spoof which takes advantage of the popup. Image (h), which displays a spoofed popup which looks exactly the same as the popup in (e) has by far the most incorrect responses (69%).

When one looks at the responses given to the "How do you know" question, explanations for the above phenomena emerge. 55% of popup-viewing users relied on the popup to determine if the page is encrypted. The popup window explicitly states that website is "encrypted" so it is no surprise that confused users found their answer in the popup. One user, who wrongly indicated that Image (h) was encrypted wrote: "Because the pop up says so...but the url doesn't say https." The popup was even able to override this user's otherwise correct thinking! One can also see an explanation for the comparatively worse performance of Firefox 3 without the popup to Firefox 2. The lock icon was sited by 44 users as an indicator of encryption. However, Firefox 3 does not present a lock icon unless one enables the popup. We suspect that the response to image (f) and (a) would have been identical if the lock icon appeared in the address bar in Firefox 3.

4. LABORATORY STUDY

We recruited 10 Carnegie Mellon subjects for the in-lab user study. The study was divided into two parts—the first involved having the user visit an untrusted and unfamiliar website, canada.com. Users were asked to register for an email address at this site and send an email. The second part was further divided into two subtasks involving a trusted and familiar website, the CMU library catalog (Cameo). The first subtask asked users to look up the ISBN number of Shakespeare's Hamlet in Cameo using Firefox 2. This subtask had two simultaneous purposes—it provided an informal evaluation of the Firefox 2 warning mechanism and it reinforced users' trust of the website. The second subtask asked users to find the ISBN number of a different version of Hamlet, again in Cameo, using Firefox 3. We interviewed users after they had completed both tasks.

For the purpose of gathering timing metrics, the tasks on Firefox 3 were divided into three intervals represented as Interval 1, Interval 2 and Interval 3. Interval 1 begins with the display of the warning and ends when the user clicks "Or you can add an exception..." The second interval is between this link click and the click of "Add Exception..." Interval 3 starts when the user clicks "Add Exception..." and ends when the user actually adds the certificate and clicks "Confirm."

All six Firefox 2 users quickly clicked "OK" when the warning dialog appeared and visited the website. In addition, in Firefox 3, nine out of ten users eventually added an exception and visited the website, but these users were substantially delayed. Two Firefox 3 users even switched to Internet Explorer after a few minutes of frustration and had to be told to switch back to Firefox. The one user who did not add the exception was a trusted user. He said to himself during the process, "I don't know what to do." However, when we interviewed him afterward he said, "I didn't know if the site was safe. I didn't want to do something permanent. Firefox 2 gave me the choice to install the certificate temporarily." He seemed willing to add the exception temporarily for the sake of the study, but unwilling to endanger himself later by permanently adding the exception.

There are also important differences in the results between the users of the trusted and untrusted websites. Users aggregate results were similar in both Intervals 1 and 3. However, the mean time for untrusted users in Interval 2 is 15 times as long as trusted users. We believe this dramatic result can be explained by the button labels. "Get me out of here!" implies danger to the user and users in the untrusted case were worried about the website. Users took more time to decide and even clicked the back and forward buttons repeatedly. In fact, two users in this case even ended up clicking 'Get me out of here...' once before returning and eventually adding the exception. However, users in the trusted case were unworried and quickly clicked "Add Exception."

5. CONCLUSIONS

Before the study began our hypothesis could be summarized as: "The more things change the more they stay the same." In particular we thought that the differences between: familiar and unfamiliar websites, Firefox 2 and Firefox 3, Extended Validation and Normal Certificates, and Favicon Popups and Lock icons would be minimal. We now believe that we were basically correct. However, we discovered many subtleties in this process that together have substantial impact. These have been discussed at length throughout the paper. The proposed changes to Firefox 3 that have been successful are those that take advantage of users existing mental models and do not try to impose new models on users. Extended validation was not successful in our study, because it is a new concept. However, changing the button labels when one reaches a website with an invalid certificate – "Add exception..." and "Get me out of here" instead of "OK" and "Cancel" has been very effective.

6. REFERENCES

[1] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590, New York, NY, USA, 2006. ACM.

[2] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum. Users' conceptions of web security: a comparative study. In *CHI '02: CHI '02 extended abstracts on Human factors in computing systems*, pages 746–747, New York, NY, USA, 2002. ACM.

[3] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The emperor's new security indicators. In *SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 51–65, Washington, DC, USA, 2007. IEEE Computer Society.