Shining Chrome: Using Web Browser Personas to Enhance SSL Certificate Visualization

Max-Emanuel Maurer, Alexander De Luca, Tobias Stockinger
University of Munich
Media Informatics Group
Amalienstr. 17
80333 München, Germany
{max.maurer, alexander.de.luca}@ifi.lmu.de, stockinger@cip.ifi.lmu.de

Abstract. Average users lack the technical expertise to understand SSL certificates and security is not their primary goal. Thus, it is very hard to create a notable impact on user behavior using SSL-status indicators. However, with the introduction of web browser Personas (simple skins) as a possibility to change the browser's chrome, it becomes possible to provide a large status indicator without wasting screen real estate. In this work, we present an evaluation of Personas to represent the current SSL status combined with newly designed SSL warning messages, both in the lab and in the field. Results suggest that the concepts positively influenced security awareness.

Keywords: SSL certificates, Security Awareness, Security

1 Introduction

Communicating security issues to Internet users is a challenging task. One part of the problem space is how to visualize encryption state. A properly encrypted connection is an important security factor, even though it does not implicitly guarantee that the user is safe. In the past years the visualization in browsers has changed: The overlooked padlock icon has vanished and indicators in and around the URL bar have been introduced. The understanding of certificates has also become more complex with the introduction of Extended Validation certificates. With this kind of certificate, not only the match of encryption key and domain is verified but also certain company specific properties are validated [3]. This means that current indicators have to be adapted to display the difference between the two certificate types.

In this paper, we present SSLPersonas, which visualizes the current SSL status of the browser by changing the browser's chrome. Additionally, we propose a new type of warning pages that block website access for insecure SSL statuses. Both ideas were implemented as a plugin for Mozilla Firefox and evaluated in a lab study as well as using questionnaire results from 169 real users of the plugin that had used the plugin for up to six months.

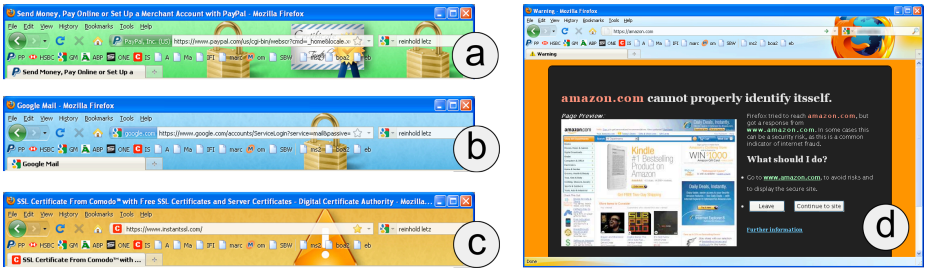

Fig. 1. Proposed Personas for **a)** Extended Validation certificate **b)** Standard SSL certificate **c)** Warning (partially unencrypted content); **d)** Browser with a standard Persona displaying the changed warning page for a non-matching URL.

Visualizing certificate details has been recently covered by Biddle et al. [2]. They evaluated a new kind of interface for those details based on guidelines making it easier to understand the certificate related information and in that way improved the accuracy of security decisions.

A big problem of web security is that it is not the users' primary goal [11]. Together with the phenomenon of change blindness [6] this results in passive indicators not being noticed. As an alternative the users can be actively interrupted during their browsing task by showing them a dialog box and forcing them to decide on an option [4]. Unfortunately users tend to get quickly habituated and dismiss those messages without paying further attention [1].

2 SSLPersonas

Modern web browsers allow for completely changing the browser's chrome. Based on this, we came up with the idea of using this space for the visualization of the SSL certificate status. The expression “Persona” is used throughout this work as a reference to a special kind of browser skin, not changing the whole UI but only the window background. Personas therefore enable framing the current web page occluding a relatively big portion of the browser without wasting space for other UI elements in contrast to other security plugins or toolbars. By separating the browser chrome and the content, it is extremely hard for attackers to modify or mimic a Persona. The browser in figure 1d is using a standard Persona.

Most browsers already use colors in the URL bar to make people aware of the current SSL state. We combine this approach by using specially designed Personas that are displayed in the browser while visiting a website that uses an SSL certificate. The Personas use a similar color scheme as the Firefox browser itself and are additionally enhanced with some imagery to make their meaning more clear. A green Persona (see figure 1a) showing two padlock icons and a certificate icon is shown for Extended Validation certificates. For standard SSL certificates a blue Persona with only one padlock icon is shown (see figure 1b). For web pages being SSL secured but transmitting some information over unencrypted channels, a yellow warning Persona is used (see figure 1c).

Browsing SSL secured sites can additionally lead to blocking browser pages as

recommended by the W3C [9]. In the case that a certificate has not been verified by a certificate authority – e.g. a self signed certificate – a warning message blocks access to this site. Another problem can occur when a certificate is used for a domain it was not issued for. We redesigned the upcoming warning messages by firstly modifying text and appearance and secondly by adding a preview image of the blocked site (see figure 1d) (without really loading the site).

3 Lab Study

3.1 Methodology and Participants

The concept was examined in a lab study by measuring if SSLPersonas is able to change the opinion of a user towards a specific website. We used a between subjects design with 24 participants. Twelve used a standard version of Mozilla Firefox, the other half had the plugin installed. The participants had to browse 14 different websites in seven categories. After each website, they had to report their personal assessment about security and trustworthiness of the website. We provided no explanations how the plugin worked or what the purpose of the study was until all assessments were made.

The 14 websites covered seven different cases. For each case, a well known and a hardly known web page was used – measured by their Alexa rating[1] for Germany, the country has been conducted in. The websites were shown to the participants in random order. The seven different cases consisted of the three different Persona states – Extended Validation (1), standard validation (2), mixed content (3) – and two kinds of non-SSL-secured sites – genuine (4) and phishing ones (5) – and finally two different types of warnings – mismatched domain (6) and unknown issuer (7).

After viewing each website, participants had to answer a set of questions. For all Persona related websites, people were asked four questions: First they should tell whether they knew a website beforehand or not. This was used to check if our assignment for well-known and unknown websites did hold. After that, they had to rank the trustworthiness of the site on a five point Likert scale ranging from -2 (“this website seems suspicious”) to +2 (“this website seems trustworthy”). Another question concerned whether people would log in on the respective website -2 (“I definitely would not log in on this site”) to +2 (“I would log in without concerns”). The fourth question asked whether security assessment was possible: -2 (“I cannot see whether this site is secure”) to +2 (“There are enough indicators that this site is secure/insecure”). People should also name those indicators. Finally, we asked questions to determine how people would have reacted to the warning pages (cases 6 and 7).

The 24 participants – mostly students – were randomly assigned to one of the two groups. The 12 participants of the control group were in average 27 years old (ranging from 14 to 45; two thirds male). They used the Internet for 4.2 hours (SD 2.6) in average each day. All of them used the Internet for shopping and communicating;

[1] alexa.com computes a website ranking in a worldwide and country-based manner.

Table 1. Likert medians and means for the unknown websites of the different groups.

	SSL						No SSL			
	Extended Validation (1)		Standard SSL (2)		Partially not encrypted (3)		Genuine (4)		Phishing (5)	
Trustworthiness										
Median	1,5	1	1	0	-1	0	0	0	-1	-1
Mean	* 1,50	0,83	* 0,67	0,58	* 0,50	0,17	* 0,33	0,17	* 0,58	-0,5
SD	0,52	0,94	0,89	1,00	1,24	1,11	0,89	0,72	1,56	1,68
Would login										
Median	1	1	-0,5	-0,5	-1	0	0	-0,5	-1,5	-2
Mean	* 0,92	0,33	* -0,5	-0,6	* -0,5	-0,2	-0,4	* -0,5	-0,8	* -0,8
SD	1,16	1,23	1,38	1,44	1,38	0,94	1	1,17	1,4	1,53
Can determine security										
Median	1	0	-0,5	-1	0	-1	-1	-0,5	-1,5	1
Mean	* 0,58	-0,1	* -0,1	-0,7	* 0	-0,7	* -0,9	-0,7	-0,8	* 0,42
SD	1,51	1,08	1,24	1,44	1,21	1,23	1,08	1,3	1,47	1,38

Secure Insecure * Plugin better * Plugin worse Plugin group Control group

nine of them for online banking. Looking at the plugin group, demographics are nearly equal: 58 percent male; average age of 23 years (range 14 to 30); using the Internet for 3.3 hours (SD 1.9) per day. Ten people use the Internet for shopping, twelve for communication and eleven for online banking.

Hypotheses: We formulated four hypotheses: **H1**: Using Personas for positive SSL statuses – like an SSL certificate being present – will increase the trustworthiness of a web page. **H2**: Using a Persona to warn users about a web page transmitting some data over unencrypted channels will reduce the trustworthiness. **H3**: The absence of the Persona on non-encrypted websites will reduce their trustworthiness. **H4**: The redesigned SSL warning pages will enable more users to choose the correct/secure option.

3.2 Results

The classification of known and unknown sites worked well for cases 1, 2 and 5. The websites for case 3 and 4 were known by hardly any participant. In contrast, the classification of unknown sites matched very well. Thus, the following results will mostly be taken from the unknown websites. For the well-known websites, we found a tendency of them being rated nearly equally to the unknown sites whilst the plugin seemed to have more influence on people using unknown sites.

Comparing the five cases, the SSLPersona-enhanced browser outperformed the standard one. The medians and means of the participants' answers ranging from -2 to +2 can be found in table 1. In case of correctly SSL-secured sites (case 1 and 2), people in the plugin group rated trustworthiness, the willingness to log in and the ability to determine security higher. These values support H1.

For the partially encrypted page using the warning Persona (case 3), we expected to get lower ratings for trust and log in willingness. The ability to determine security should still be higher. Again all those assumptions hold when looking at the median values. This supports H2.

In case of the non-SSL sites and the phishing sites, both groups saw a standard any

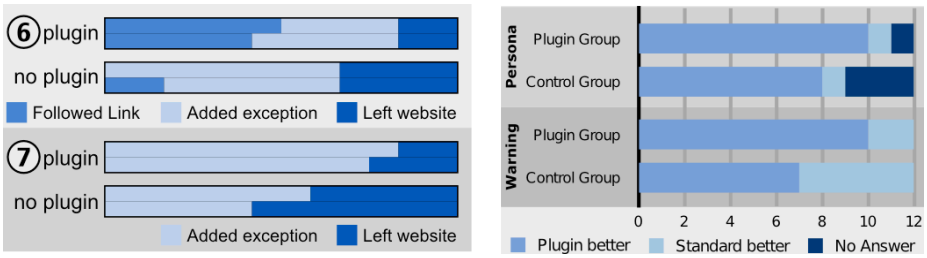

Fig. 2. Left: Warning message decisions for cases 6 and 7. Upper half of each bar represents well-known websites, the lower half hardly known websites. **Right:** When showing participants pictures of the standard or plugin enhanced version, people from both groups preferred the enhanced version.

Persona. For H3, we expected the results of the plugin group to drop due to a missing positive feedback. This did not happen. The study duration was much too short for people to get used to the plugin and expecting the green Persona to show up. Furthermore, the order of the visited websites was randomized for each participant.

Looking at the warning page for a non-matching URL (case 6), participants had three options to choose from: Leaving the site, visiting the link the certificate was intended for and adding an exception and continuing to the site. The best option in such a case would be to visit the URL the certificate was originally issued for. This was done by zero (known) and two (unknown) participants for the control group in contrast to six (known) and five (unknown) using the plugin (see figure 2 left).

When confronted with an untrusted issuer certificate (case 7), the only option was to leave the site or set up an exception. Since our websites both were genuine but used self signed certificates, setting up an exception was okay in this case. Again plugin users used the exception more often (see figure 2). Comparing the correct answers with a repeated-measures ANOVA – within-subject factors: "known" and "warning type" – the results for the between subjects variable "group" are highly significant ($F_{1,22}$=16, p=0.001) which confirms H4.

After rating the websites, the participants were debriefed and shown some side-by-side images of a browser with and without the plugin. Overall, 75% of the participants preferred the plugin version. The same holds for the comparison of the warnings. 71% preferred the plugin warnings (see figure 2 right).

4 Field Study

Based on the lab study, the plugin was improved (e.g. UI bugs fixed) and published on August 20, 2010 through the Firefox addon webpage. It quickly gathered public interest and was installed several thousand times. Different blogs and podcasts related to security covered the plugin and reported about the concept [5, 8]. By March 2011, the plugin was downloaded more than 15,000 times. It has around 2,300 active users. 86% use Windows, 8% Unix and 6% Mac OS. 45% percent are US English users, 32% are German, 5% British followed by smaller amounts of French, Spanish, Italian, Brazilian and Russian users.

4.1 Methodology and Participants

Having a real-world user base with a broad spectrum of nationalities provides a good baseline for evaluating experiences with the plugin and its concept. Thus, we created an online questionnaire and a plugin update to invite them to take part in the research. No further incentives were provided.

The questionnaire consisted of three sets of questions. Firstly, a small set of nine questions from the IBM "Post-Study System Usability Questionnaire" [7] was used with 5-point instead of 7-point Likert scales. The second set contained eleven questions about plugin usage and security knowledge. Finally, we collected demographics of the participants.

The survey was available in English and German. Incoming participants were diverted according to their browser language. The survey was also available through several external links – like the plugin's web page.

After deploying an update, Firefox automatically recommends it to the users. Therefore, most of the users quickly updated (approx. 1,700) in the two weeks period the questionnaire was available. From those users, 169 (approx. 10%) completed the questionnaire. 88% of them used the English version 12% the German version. The average age of the participants was 41 years (range: 9 to 70). Only 16 participants (9.5%) were female. Please note that there was no way to check whether the demographic data was valid.

4.2 Results

Analyzing the responses, we found that a large number of respondents has to be categorized as sophisticated users. In average, participants spend 30 hours (SD 23.1) per week on the Internet, 12% more than 60 hours. Rating their computer skills, only 2% stated to be "inexperienced", 21% had "average" skills, 48% had "advanced" and 28% "expert" skills. 9% of the participants stated they had been victim to a phishing attack before, but only one attack successfully fooled the victim.

We had no technical means to find out how long people had installed the plugin before and added a respective question. 15% stated having used the plugin less than one month, 40% 1-2 months, 30% 3-5 months and 15% more than five months. Comparing the groups of new and old users, no major changes in answers can be found except for the stated experience level. Whilst 69% of the long-term users stated either to be advanced or expert Internet users, those users made up only 48% of the group of new users. Probably early adopters were rather experts whilst more and more inexperienced users discovered the plugin lately. The high number of expert users can be explained with the effort of finding an extra security plugin which is usually not taken by novice users due to the secondary goal property of security [10].

In the questionnaire, we showed pictures of Firefox's standard SSL indicator – a green bar in front of the URL indicating an Extended Validation certification. We asked them whether they had noticed it before. 82% confirmed this. We asked those users to explain what it meant: 11% gave a correct explanation (mentioning the concept of Extended Validation) and 57% mentioned at least security. From the 82% of people that stated they had noticed the bar, 50% said they had already clicked on

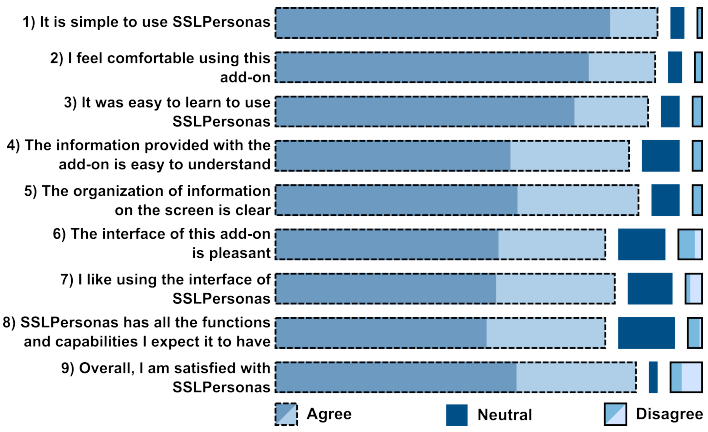

Fig. 3. The distribution of Likert answers throughout the nine questions extracted from the IBM Post-Study System Usability Questionnaire.

this field at least once and half of those were able to correctly describe the contents of this field. "Do you know the difference between the blue and green Persona." resulted in 62% saying they knew it but again only 21% gave a correct answer. Another 21% of the respondents thought it had to do something with the "strength of encryption" and some people thought the blue Persona would indicate that some contents of the website are not encrypted. This means that although users estimated themselves to be security experts the detailed answers were mostly incorrect.

The IBM usability questions used a 5-point Likert scale ranging from 1-'strongly agree' to 5-'strongly disagree'. All questions were answered with a Median of 1, which means that the plugin is very helpful to the users. The best mean value was for "It is simple to use SSLPersonas" having 1.2 (SD 0.6). The worst mean value was 1.7 (SD 0.9) for "SSLPersonas has all the functions and capabilities I expect it to have". More details on the nine questions can be found in figure 3.

To our surprise, 38% stated that SSLPersonas changed the way they use the Internet.

5 Limitations, Discussion and Conclusion

As with any lab study, this one also had problems with ecological validity. The field study was supposed to fill this hole. Interestingly, we found that the real users of SSLPersonas largely consist of expert users. Although the concept primarily targets novice users, expert users dominate both, the early adopter and the basic user group while novice users adopt the concept much more slowly. We assume this is due to different factors. For instance, novice users do not know about the security issues and thus do not search for solutions. Therefore, a novice user would not install the plugin by herself. This suggests that especially security enhancements should be delivered with the browser.

Despite the high number of experts, the percentage of people that were able to correctly distinguish between the different kinds of SSL certificates – the green and

the blue Persona – is very low. The number of people misleadingly assuming a stronger encryption is equally high. This puts the whole concept of different types of certificates into question as they seem not to be self-explaining. Our green Persona potentially added up to this fact because it contained two lock icons instead of one in the blue Persona. After the study, we changed that and added an icon of a "green man" as a metaphor for the validated company identity.

Both studies support our hypothesis that SSLPersonas improves security awareness in standard web browsing tasks without occupying extra screen space. In the lab study, we could show that SSLPersonas influences the users' rating of websites towards a better (more secure) behavior. The published plugin was installed by many people of which 169 participated in a survey. The results attest SSLPersonas positive effects on security-aware behavior. Being able to positively influence the users security decisions at no cost in combination with the fact that expert users also rely on the concept shows the value and importance of this work.

We also proposed new layouts for certificate warning pages with the main goal to avoid habituation. They enabled the participants to make significantly more rational decisions when dismissing the warning dialogs.

Personas as a status display for SSL information seem to be able to influence security assessment. In the future other factors could be added to the underlying concept to get a more complete security analysis.

References

1. Amer, T.S., Maris, J.B.: Signal words and signal icons in application control and information technology. Journal of Information Systems 21 (2006)
2. Biddle, R., van Oorschot, P.C., Patrick, A.S., Sobey, J., Whalen, T.: Browser interfaces and extended validation SSL certificates: An empirical study. In: CCSW '09. ACM (2009)
3. CA/Browser Forum: Extended validation ssl certificates. http://cabforum.org
4. Egelman, S., Cranor, L.F., Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: Proc. CHI '08. pp. 1065–1074. ACM, Florence, Italy (2008)
5. Gibson, S., Laporte, L.: Security now episode 277. http://www.grc.com/securitynow.htm Visited 03/27/2011
6. Grimes, J.: On the failure to detect changes in scenes across saccades. Perception 2, 89–110 (1996)
7. Lewis, J.R.: IBM computer usability satisfaction questionnaires: psychometric evaluation and instructions for use. International journal of human computer interaction 7 (1), 57–78 (1995)
8. Morton, B.: SSLPersonas - SSL blog - Entrust insights. http://ssl.entrust.net/blog/?p=321 Visited 03/27/2011
9. Roessler, T., Saldhana, A.: Web security context: User interface guidelines (2009)
10. Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of PGP 5.0. In: Proc. USENIX '99. pp. 169–184 (1999)
11. Wu, M., Miller, R.C., Garfinkel, S.L.: Do security toolbars actually prevent phishing attacks? In: Proc. CHI '06. pp. 601–610. ACM (2006)