EECE 412 Term Project: A Study on SSL Warning Effectiveness

Ildar Muslukhov muslukhovi@gmail.com
Andreas Sotirakopoulos sotirakopoulos@gmail.com
Levi Stoddard levi.stoddard@gmail.com

Abstract—**The Secure Sockets Layer (SSL) protocol employes certificates in order to initiate a secure communication channel between the client PC and a web server. Malicious attackers in order to extract personal-sensitive information from other users may set up environments that aim at luring the users into providing their information thinking that they are using a secure channel of communication. In order for malicious attackers to achieve that, forged certificates must be used in order to initiate a SSL session and trick the user into thinking that he is dealing with a legitimate site. In an effort to fight back such attacks browser developers have created SSL warnings that are presented to the user whenever the server certificate seems to be either misconfigured or not issued by a trusted authority. These warning are designed to give the choice to the user to proceed as there are too many legitimate web sites on the web that have misconfigured certificates. It is observed that users tend to disregard those warnings for various reasons rendering them unable to serve their purpose of protecting the user from malicious phishing attacks. Our term project's goal is to determine the reasons behind users' disregard to SSL warnings as well as to conclude on actions that should be taken, in future SSL warning development, in order to make them more effective in protecting users. In order to achieve this we conducted a user study in a controlled laboratory environment where we studied the reactions and reasonings of users when presented with a SSL warning while trying to access critical and non critical information on line.**

Index Terms—Computer Security, SSL, Warnings

1 Introduction

The Secure Sockets Layer (SSL) protocol was developed to establish secure communication channels between client and server network applications [3]. When establishing a secure connection, public key certificates bind an organization's identity to a public key used for session key establishment. Neglection by an organization to keep certificates current, sign them by a trusted Certificate Authority (CA) or keep them within the organization all lead to warnings during establishment of a secure connection between a web browser and server. Users become habituated to the sight of these warnings as certificate maintenance is frequently disregarded. Due to habituation, users can unknowingly co-operate with threat agents to mount Phishing or Man In the Middle (MITM) attacks by choosing to ignore SSL warnings. Although cryptography is employed for authentication and encryption, the introduction of humans into the loop can nullify any security offered by this protocol.

This project aims to investigate user behavior when presented with browser generated SSL warnings, and the reasons for users to heed (or not) warnings. The project takes the form of a lab study where users are presented with browser warnings amidst completing simple day-to-day tasks. Warnings are triggered in both "high risk", and "low risk" scenarios. User reactions are garnered through instigator observation, and participant feedback in the form of an exit survey.

2 Background Work

Important questions in security related human-computer interaction include *why do people often fail to heed security warning messages?*, *how do they perceive risks involved?*, and *does context matter?* To answer such questions, Cranor proposed a framework for reasoning about the "human in the loop" that gives us a systematic approach to pinpointing possible humans failures in security related tasks [1]. The framework allows us to identify issues in the system before it has been implemented, so we can address them in advance. Egleman et al. showed that users tend to ignore certain types of warnings in phishing attacks, and suggested "active" warnings to deter users from phishing threats [2]. Sunshine et al. showed that users also tend to ignore SSL warnings and discovered that well designed warnings tend to be more effective [4].

3 Experimental Setup

3.1 Tasks

Participants were presented with four tasks:

1) Retrieve the surface area of Greece using either *google.com* or *ask.com*.
2) Retrieve the last two digits of their bank account balance using either *online banking* or *telephone banking*.
3) Locate the book *Freakonomics* on *amazon.com* or *barnesandnoble.com*.
4) Register for an account at either *yahoo.com* or *hotmail.com*, in order to register with *tripadvisor.com*.

During completion of these tasks, participants believed we were investigating the ease of accessing information online. Tasks *1* and *3* exist for the sole purpose of enforcing this belief. Participants were presented with SSL warnings during tasks *2* and *4*. To deter participants from completing tasks under the circumstance where they are uncomfortable but intent on "pleasing" the investigators, we allowed two possible paths for competing each task; One insecure path, the other secure. Warnings are only displayed on the insecure path of each task. Participants were instructed to first try the primary source of information (insecure path), and then try the secondary source (secure path) if unsuccessful with the first.

In each of tasks *2* and *4*, the observer took note as to whether the participant heeded or did not heed to the SSL warning presented. These tasks were presented in the order *2* followed by *4* for half the participants, and *4* followed by *2* for the remaining. The re-ordering was arranged to prevent a bias due to warning exposure in one scenario before the other.

3.2 HTTPS Proxy

As discussed above, study participants are presented with SSL warnings at pre-chosed times during completion of the assigned tasks. To present these warnings we implemented a custom HTTPS proxy server which enabled us to present selected warnings for sites of selected domain names. Each participant's web browser was configured to establish HTTPS connections through this proxy, allowing us complete control over the displayed warnings.

3.2.1 Warning Selection

Upon execution, the proxy receives *blacklist* and *warning configuration* files. The blacklist file contains a list of domain names for which warnings should be generated. The warning configuration file contains the identifier of the warning which should be presented. Three warnings are possible, and are described further in the *Implementation* subsection. The participant is not hindered when attempting to access HTTPS enabled sites outside the blacklist.

3.2.2 Implementation

The need to trigger SSL warnings through use of a proxy is not common, therefore we implemented custom software to satisfy this requirement.

We selected [5] as a starting point for our proxy server. The proxy is written in Java and of a small code size, which simplifies the modification and development process. Previously this proxy only altered the signing CA of a server's X.509 certificate; Our work augmented this functionality with the ability to generate connection establishment warnings.

Figure 1 illustrates the operation of the proxy server. Connection proxying occurs in three stages. In stage 1

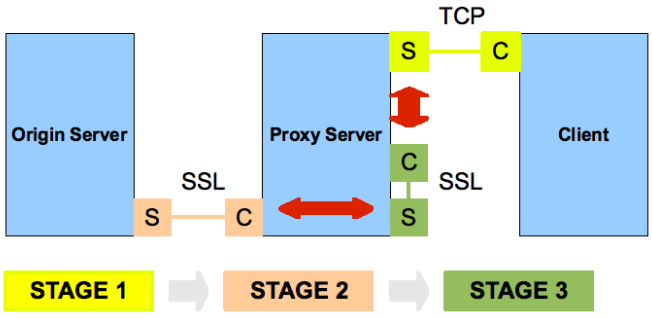


Fig. 1. HTTPS proxy server.

the proxy intercepts the client's request for a remote resource. In stage 2, the proxy establishes an SSL connection to the origin server holding the remote resource, and obtains it's X.509 certificate. In stage 3, the proxy alters the origin certificate, re-signs the certificate with it's own private key, and listens for an SSL connection using the forged certificate. The proxy then connects to it's own SSL server socket, and pipes data between this socket and the requesting client. Warnings displayed to the client are generated in stage 3, and are a result of the forged certificate presented by the proxy server.

The following subsections describe the algorithm we used to trigger each SSL warning. Note that in all cases, the participants browser has one of the proxys certicates added to its list of trusted CAs, referred to as the proxys trusted certicate.

Certificate Expired

1) Decrypt server certificate from origin server using CA's public key.
2) Replace the "Not Valid After" field, with a value in the past.
3) Sign the server certificate with the proxy's trusted certificate, and use this server certificate in connection establishment with the client.

Unknown CA

1) Decrypt server certificate from origin server using CA's public key.
2) Sign the server certificate with the proxy's non-trusted certificate (not in the client's list of trusted CA's), and use the newly signed server certificate in connection establishment with the client.

Domain Mismatch

1) Follow the same procedure as *Certificate Expired*, but replace the "Common Name" field (issued to) rather than the "Not Valid After" field.

3.3 Virtual Machine Environment

Participants completed all tasks in a virtual machine (VM) environment. Microsoft's *Virtual PC* virtualization software was used to meet this requirement. One VM hosted the proxy server, and another hosted the desktop environment where participants completed tasks. Both VMs executed on the same physical laptop, with the

client machine in full-screen mode (participant is unaware they are working within a virtual machine). We selected Windows XP Professional (SP3) as the operating system for both machines because most participants have exposure to this operating system. Also, we have many different client VM's with a different web browser installed on each; Prior to beginning the lab experiment, users are asked which browser they use (Internet Explorer, Firefox or Chrome), and we supply a VM with only this browser installed.

Our reasons for administering the study on virtual machines are two-fold:

1) VMs can be reset after each participant interview, ensuring that each participant performs the assigned tasks in an identical environment.
2) Clients are entering confidential information on their bank's web site (and possibly during email registration). The use of VMs ensures that participants do not gain access to one another's personal information as a result of information caching.

3.4 Exit Survey

Participants are required to complete an exit survey hosted on *www.surveymonkey.com*. The survey gathers participant demographic information, technical background, and justification for their actions during the task phase. After completion of the exit survey, the study's purpose is revealed to each participant through an oral debriefing.

4 Results

Due to time constraints and difficulties in finding participants, our current sample size consists of ten participants. As a result, all conclusions drawn here are preliminary.

4.1 Dummy Tasks

All users completed the dummy tasks successfully, and without use of the secondary information source.

4.2 Bank Task

Most participants, although they claimed during the exit survey that they had never seen the warning on their banks web site, ignored it and proceeded (Figure 2). The two participants that did heed reported they were unaware of the option to overcome the warning.

The most common reason users gave for ignoring the warning was that they have seen it before in so many places, and nothing bad happened to their information. This is evident from Figure 3 where users are asked whether they felt that there was some risk involved in accessing the web site and most of our participants either answered NO or Not Sure.

Another reason common among users was that they trust their bank's web site. An interesting finding was

Fig. 2. Seen the warning previously on the bank web site.

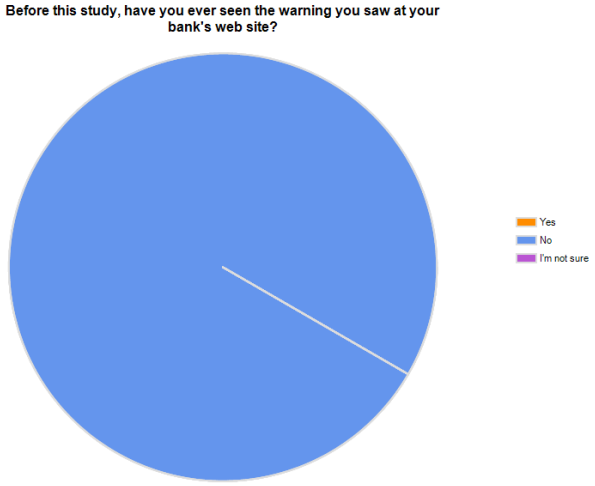
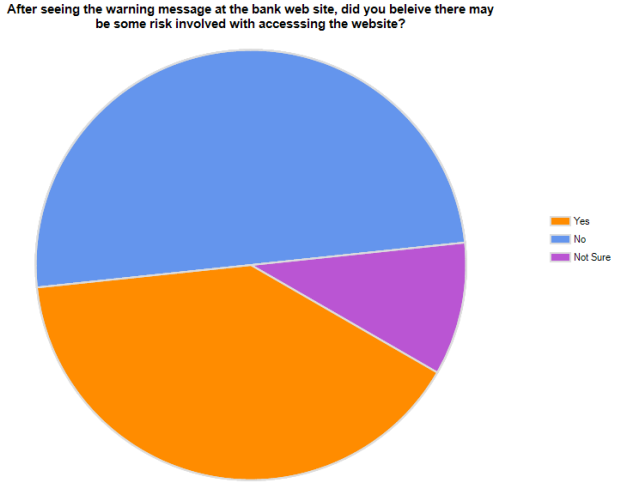


Fig. 3. Risk involved in accessing the bank web site.



that one user found to difficult to operate the phone banking system and after retrying the online banking system, added the exception. This situation illustrates that users aim for convenience while searching for information, and prefer the path of least resistance as opposed to the path of most security.

4.3 Account Registration Task

Here participant's actions were analogous to those on their bank's web site. Most ignored the warnings on the grounds of having seen them before - except for those who again did not realize how to add a security exception. This time however more people claimed that they have seen the warning before in this web site (Figure 4). We believe this not to be true but to be related with the notion among population that the Yahoo web site is less secure than a bank web site. This notion reflects also on the results of Figure 5 where users more claim that they felt there was some risk involved in accessing the Yahoo web site.

Fig. 4. Seen the warning previously on the Yahoo web site.

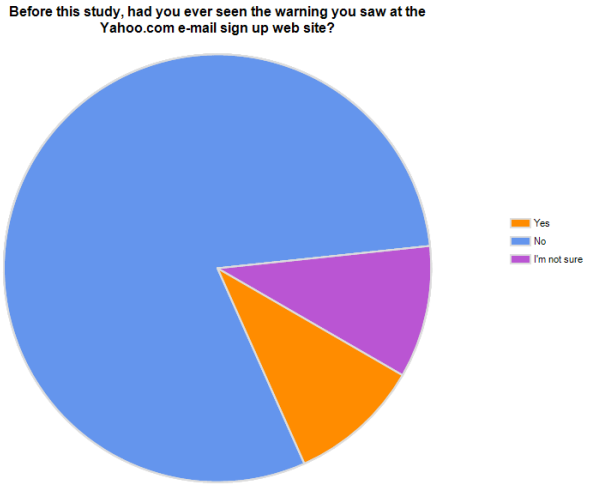
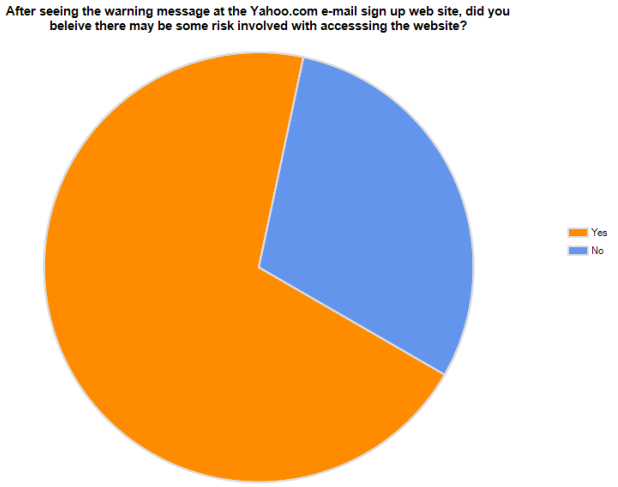


Fig. 5. Risk involved in accessing the Yahoo web site.



An interesting finding is that one subject ignored the bank warning but chose to heed to the Yahoo warning on the grounds that he has more confidence in his bank than in Yahoo. Again the most common reason for ignoring the warning is habituation.

4.4 Participant Demographics and Technical Experience

Our participants were all in the age range of 19-29 years with an equal number of male and female participants. All of them were of college or higher education level. Having a small sample we did not observe any correlation between gender, age or level of education and decisions about heeding or ignoring the warning. When our users where asked in a Liktert scale from 1 to 5 to self asses their computer expertise they reported an average of 3.3 which we consider quite high. However when they were asked technical details such as *what is a Main in the Middle (MITM) attack?* or *what is an SSL certificate?* almost none could answer correctly. Based on these findings, we believe that user self-assessment of technical skills is not always optimal. We kept this scale, as it was used in the previous study we are extending, and they used it heavily to draw conclusions upon participant behavior.

4.5 Security Decision Factors

Table 1 illustrates the results of participants responding to rate the effectiveness of various warning elements on a Liktert scale (ranging from 0 to 6).

Factors	Average Rating
Text of the warning	2.90
Colors of the warning	2.30
Choices the warning presented	2.10
Destination URL	3.00
Look and feel of destination site	3.70
Other factors	3.75

TABLE 1
Factors influencing participant's decision.

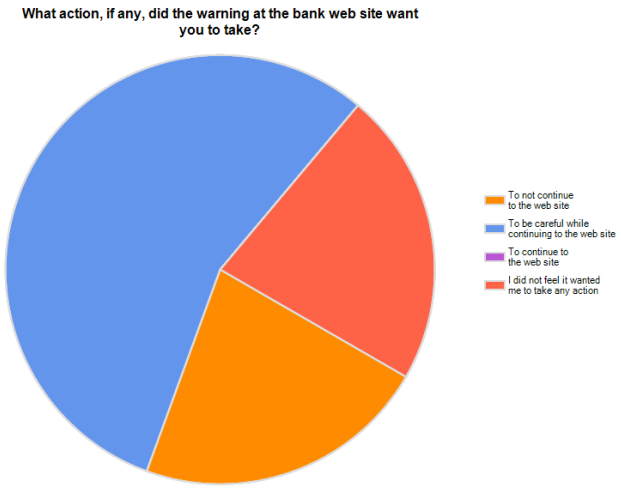
The most common factor, encompassed under "Other factors" was the response that they were so used to seeing the warning that they decided to ignore it.

When asked to pick the most important factor from the list in the table above, users chose the destination URL as the one of most importance by 44.4%.

5 Conclusion

We would like to note that users generally read the text of the warning thoroughly, yet still cannot understand what the warning wants them to do (Figure 6) or the reason for which they have been presented a warning. They are unable to determine if the warning indicates a legitimate security threat to their information. Most participants believed that the warning was a result of the browser, or the legitimate organization's web site - not with the secure connection establishment.

Fig. 6. Action the warning wanted users to perform.



This clearly demonstrated that warnings not only fail to clearly describe the source of the problem, but users lacking in security education are unable to understand even relatively simple explanations as presented in most recent conclusions.

Finally habituation remains the number one cause of ignoring security warnings. Little can be done to address this issue as long as there are so many legitimate sites with miss-configured or self-signed certificates (it is estimated that 20% of the 1000 most visited websites have certificate issues). That said we believe that making it more difficult for the average user to add an exception (the path that Firefox 3/3.5 has taken) will protect users from making harmful decisions out of habit. Also we feel that by paying more attention to the look and text of the warning messages, users will start to realize the dangers of ignoring them and will become educated in necessary security precautions.

REFERENCES

[1] L. F. Cranor. A framework for reasoning about the human in the loop. In Proceedings of the 1st Conference on Usability, Psychology, and Security, pages 115, Berkeley, CA, USA, 2008. USENIX Association.

[2] S. Egelman, L. F. Cranor, and J. Hong. Youve been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceeding of the SIGCHI Conference on Human Factors in Computing Systems, pages 10651074, New York, NY, USA, 2008. ACM.ropean Symposium on Research in Computer Security, pages 411427, 2008.

[3] T. Dierks, C. Allen, "The TLS Protocol: Version 1.0," January 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2246.txt [Accessed: Dec. 6, 2009].

[4] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L.F. Cranor. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In Proc. of the 18th Usenix Briefings, Las Vegas, USA, July (2009).

[5] S. Inguva, D. Boneh, I. Baker, "SSL Man in the Middle Proxy," April. 12, 2007. [Online]. Available: http://crypto.stanford.edu/ssl-mitm. [Accessed: Oct. 28, 2009].