A Framework for Smart Trusted Indicators for Browsers (STIB)

Jude Desti and Hongmei Chi
Department of Computer & Information Sciences, Florida A&M University
Tallahassee, FL 32317
Jude.Desti@gmail.com, chi@cs.fsu.edu

Abstract

Web browsers currently have security indicators which provide security features that notify users of malicious or un-trusted websites. Most of these security indicators are normally synced with some black list data base that has a list with known websites that are known to be malicious. When a user surfs a website that is identified in the black list data base, the security indicators then notify the user with a warning indicating that the current site has been identified as a malicious or un-trusted site and give the user the option to continue or exit the current site. Due to the fact that these black list data base may not possibly contain every malicious site, users may come across a website that they feel that may be a an un-trusted site but have not received a warning message from the security indicator indicating otherwise. In this paper, we propose an extension security indicator called Smart Trusted indicators for Browsers, STIB, which will perform an extensive web activities history check on the current site determining how often that website is viewed or transacted to provide the user with more information about the site and the confidentiality of the legitimacy of the site.

Key words: security indicators, malware, Firefox, IE, browser, vulnerability

1. Introduction

Security is becoming increasingly apparent and more of a major priority in aspects of computer security. In the context of security systems, web browsers are often thought of as the "open door" for information flow through the World Wide Web. This information includes user's personal sensitive credentials and corporate information which allows large amount of everyday business and other sensitive transactions. These mass amounts of activities demand users to provide online credentials needed to carry out these transitions. Knowing that mass amounts of sensitive information are being sent across the web becomes an attraction to malicious users of the web. These malicious users develop different types of web attacks aimed to somehow trick users by posing as a trusted site in effort to gain the users' sensitive data.

Web Spoofing and Phishing attacks are the two highly favored attacks that attacker use against web browsers. Spoofing Attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage [1]. "Webpage Spoofing", also known as Phishing Attack, is another type of spoofing attack. In this attack, a legitimate web page such as a bank's site is reproduced in "look and feel" on another server under control of the attacker. The main intent is to fool the users into thinking that they are connected to a trusted site, for instance to harvest user names and passwords. This attack is sometimes usually used in spam e-mail messages with a link to the attackers' fake website [2]. See Figure 1.

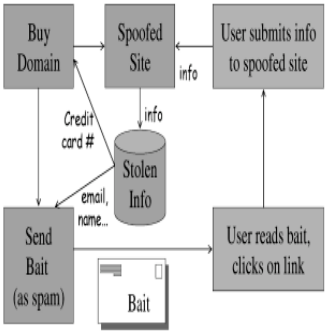
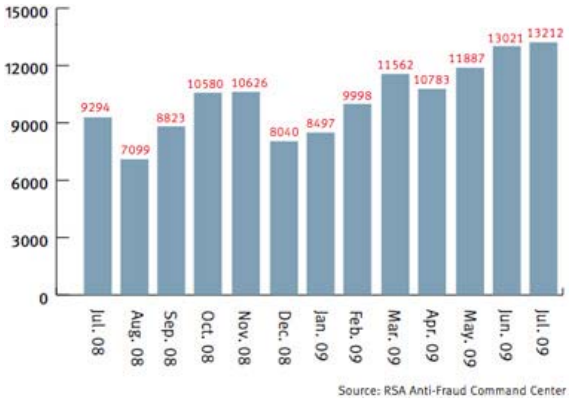


Figure 1: Process of a typical Phishing Spoofing Attack

Unfortunately, users lack knowledge of these malicious activities. Most naïve users are also unaware of security

indicators that are presented by browsers. These indicators intent are to effectively allow users to identify fake or non-trusted sites. Due to users' unawareness of these indicators and malicious activities, they carelessly browse the web and provide their sensitive information to random sites believing that every web site is a trusted website. As these careless web surfing continue to take place, Phishing and Spoofing attacks continue to grow for the compromising of users' credentials and Table 1 shows that trend [3].

Table 1: Phishing attacks within the past 12-month



This all proves to imply that there is indeed an extreme need of effort towards developing better indicator tools or extending the current existing functionalities for the security indicators that will more effectively allow user to identify fake websites.

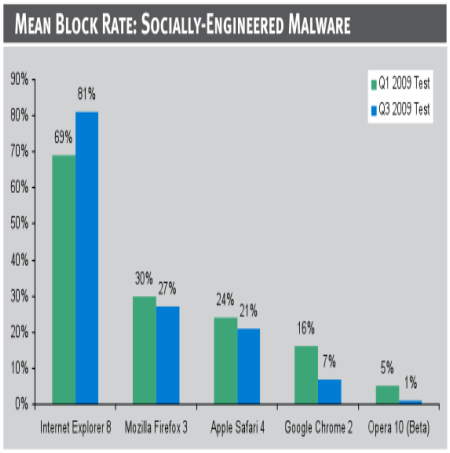
In chapter two, we will discuss and explore the security indicators that our most popular web browsers use. In chapter three, we will then showcase some of the related efforts and researches that are aimed toward providing better web browser indicators that will allow users to better recognize and distinguish the difference between a trusted website from an un-trusted website. Chapter 4 and 5 will then elaborate on our approach and method to recognizing trusted websites and provide our implementation scheme to those approaches. We will then conclude with chapter 6 with why our approach will be a more superior method in being able to notify user whether or not they're surfing through trusted websites.

2. VULNERABILITY of BROWSERS

In this section, we explore and identify several different web browsers and how their security indicators handle web browser attacks such as Web Phishing and Spoofing attacks. We will diagnose and explore the different methods taken by the security indicators to identify trusted or malicious sites for each browser. We will see that modern web browsers offer additional layers of protection against web-based threats.

Web browser protection contains two main functional components: In-the-cloud reputation-based system and internal browser request reputation information. However, not all of the browsers take same approach to browser protection. In-the-cloud reputation-based system searches the internet for malicious websites and categorizes them according to content. This is sometimes done automatically, manually, or sometime a combination of both. Internal browser request reputation information resides on the web browser and the information that it request from the in-the-cloud system about specified URLs. When results from the request about a URL listing reports as a malicious site, redirection to warning messages or pages is executed.

Table2 Increasing rates for socially-engineered Malware



2.1 INTERNET EXPLORER (IE)

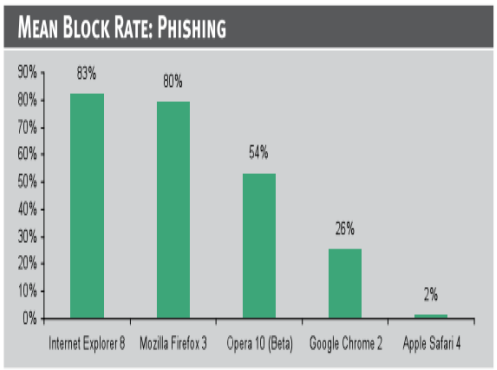
Internet Explorer is a free web browser from Microsoft and is also one of the most popular internet browsers today. Microsoft claims that IE is the fastest and safest browser for web users. The Q3 2009 Socially Engineered Malware and Phishing Test Report Summary generated by NSS Labs [4] reported that IE is and continues to be the best protected browser against Socially-Engineered Malware, web page links that directly leads to a download delivering malicious payloads, and Phishing attacks. Results from the report showed that IE had a block rate of 81% for Socially-Engineered Malware while other browsers declined from

previous test results. See Table 2. Results for Phishing attacks showed that IE had a block rate of 83%. See Table 3.

The Socially-Engineered Malware result were based upon experientially validated evidence gathered during 12 of 24x7 testing, performed every 4 hours, over 70 test runs, each one adding fresh new malware URLs. Internet Explorer improved 12% from previous test taken, evidence of ongoing concerted efforts made in the SmartScreen technology [4].

SmartSrceen® Filter is the technology that Internet Explorer uses that focuses on preventing phishing and malware attacks. As a reputation-based feature, SmartScreen blocks new threats from existing malicious sites that traditional anti-virus or anti-malware signatures does not block. This mechanism is able to block in the navigation experience and in the file download experience depending on the situation. With this type of control, SmartScreen is able to block entirely malicious sites, portions of sites or just a single malicious download on sites like social networking or file-sharing sites. The known malicious sites and malware downloads are sourced by Microsoft Internal and 3rd party data base. The data base also includes sites with Extended Validation Certificates which attest to the identity of legitimate business. When such sites are requested, the background of the URLs is highlighted in green indicating a secure and/or trusted website and increases the appearance of legitimacy to the user.

Table 3 Increasing rates for Phishing



2.2 MOZILLA FIREFOX

Firefox is another real popular web browser from Mozilla. Firefox is an open-source browser that is free, small and fast. It's based on Mozilla code and is one of the most standard-compliant browsers available on Microsoft Windows (Window 98 – Vista), Mac OS X, and Linux [5]. The Q3 2009 Socially Engineered Malware and Phishing Test Report Summary generated that Firefox caught 27% of the threats issued to the browsers. Far fewer then the Internet Explorer, Firefox came in second place on blocking malicious sites and downloading malicious payloads. Unlike IE, Firefox enables built-in Phishing and Malware Protection by default. Once users enter an address in the URL, that address is checked against a blacklist that Firefox downloads periodically. If sited on the blacklist, Firefox displays a popup which warns the user that the visited site is suspected to be a fraudulent site and provides the user the option to leave the site or to ignore the warning. See Figure 2.

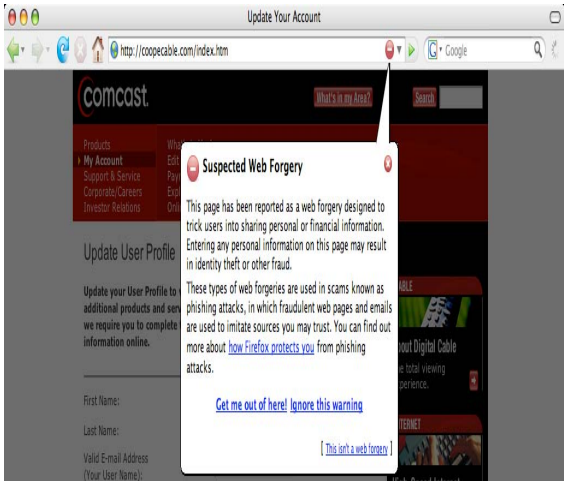


Figure 2: Snippet of Firefox indicatory warning of a malicious site identified from the blacklist data base

Like several other web browsers, Firefox also utilize the Google SafeBrowsing API. Google SafeBrowsing for Firefox is an extension that alerts the user if a web page that that is being visited appears to be asking for the user's personal or financial information under false pretences. This tool combines advance algorithms with reports about misleading pages from a number of sources and warns the user if they have encountered a page that is trying to trick them into disclosing personal credentials. For Firefox, this is an optional feature that sends the URL information to Google to determine the likelihood of being scammed.

2.3 SAFARI

Safari is a web browser developed by Apple in 2003 for the Mac OS X v10.4. Safari is the first official "out-of-beta" version created as the default web browser for the Mac System. As many of Apple's products, Safari is renowned for its sleek design and ease of use. Apple's goal for Safari is usability, speed, standard compliance, and integration with OS X [5]. In aspects of Security, Safari does not hold up a strong edge in security matters. The Q3 2009 Socially Engineered Malware and Phishing Test Report Summary generated that Safari caught 21% of the live threats [4]. Unfortunately, Safari fell third for the Social-Engineer Malware test and fell dead last to all the web browsers (IE, Firefox, Chrome, & Opera) tested for the Phishing test. When a suspicious phishing site or sites with harbor malware is identified by safari, it sometimes gives one warning pop-up message about the suspected nature of the site and sometimes prevents the site from loading. In aspects of SSL Certified sites, Safari is also weaker than its competitors in identifying digital certificates traffic. Safari does warn of invalid digital certificates, but it isn't nearly as superior as the other top browsers. Unlike other browsers who alter the entire web page with red or multicolored warnings, Safari, once again, only warns the user once with a small pop-message indicative of the suspicion of the site. Safari fails to point out Extended Validation Certificates and sometimes never highlight the domain name making it more difficult to tell a malicious site from a trusted/secure site.

3 RELATED WORK

3.1 Visual Security Indicators

Jennifer Sobey with the Ottawa-Carleton Institute for Computer Science, School of Computer Science, Carleton University, has been involved with research in aspect of SSL/TLS Certification of web sites [6]. They introduced the Extended Validation (EV) SSL certificates for Internet Explorer 7.0, web browsers which included new indicators to convey information about different types of certificates. The Extended Validation SSL certificate indicator is a more noticeable indicator that draws users' attention. A snippet of the indicator is shown in Figure 3. The indicator they evaluated and extended upon was on the Firefox 3.0 Beta 1 version which already had a small buttonized portion of the browser chrome (where all the menus and toolbars on the browser window are located) to the left of the URL bar that contains a web sites' icon. Sobey designed the EV indicator which would be displayed in the same location but was larger and displayed information about the websites' identity on the button. The indicator would trigger a pop-up information box that provided identity information for the web site based on the sites' certificate.

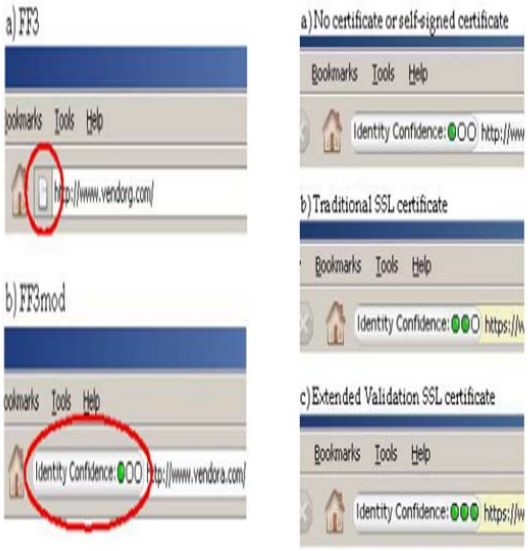


Figure 3: (left) Identity indicator used in Firefox 3 Beta 1 and modified Firefox 3 Beta 1. (right) The *identity confidence* button in its three different states

3.2 Graphical Security Indicators

Amir Herzberg and Ahmad Jbara [2] with Bar Ilan University has been involved in research dealing with web security measures in aspects of users entering sensitive credentials into fake websites. They have introduced and contributed a security and identification indicator called, the TrustBar, a browser extension. This extension allows users to assign a name or logo to identify SSL/TLS-protected sites. The goal of the Trustbar is to present a highly visible, graphical interface, establishing securely the identity of a web site. The Trustbar was implemented as an extension for the open-source Mozilla TM and Firefox TM browsers. Trustbar allow the site and the certificate authority to be identified by the logo of the website. A snippet of the indicator is shown in Figure 4. It controls a significant area, located at the top of every browser window that is large enough to contain highly visible logos and other

graphical icons for credentials. This approach prevents many security indicators spoofing attacks as described by Li and Yongdong [1], where a spoof site opens windows to hide browser indicators like padlocks and location area and to overwrite them with misleading indicators.

Figure 4: Screen-Shots of secure sites with logo in TrustBar

3.3 Dynamic Security Skins

Rachna Dhamija and J.D. Tygar [7] from the University of California, Berkeley have proposed Dynamic Security Skins, a scheme that allows a remote web server to prove the websites' identity in simplified way for users to verify . First, the browser extension provides a trusted window in the dedicated to username and password entry. A photographic image is used to create a trusted connection between the user and the window to prevent spoofed windows and texted entry fields. The second part of the scheme allows the remote server to generate unique abstract image for each user and each transaction. This image creates a "skin" that automatically customizes the browser window for identified authenticated web pages. A snippet of the indicator is shown in Figure 5. This proposal simply allows the user to visually identify a trusted site with a "skin" image that appears on the boarder of the browser window.

3.4 Other Works

Bryan Parno, Cynthia Kuo, and Adrian Perrig [8,10] from Carnegie Mellon University; involved in proposing using a trusted device to perform mutual authentication that eliminates reliance on perfect user behavior, thwarts Man-in-the-Middle attacks after setup, and protects a user's account even in the presence of key loggers and most forms of spyware. The goals of this tool are to prevent attacker from modifying, and viewing the users account. These goals are with the assumption that users can be trusted to correctly identify sites at which they wish to establish accounts with. This assumption is made due to the fact that phishing attacks generally target users with existing accounts. The trusted device takes from of a cell phone, PDA, or even smart phones. Users cannot readily disclose the authenticator on the cell phone to a third party, and servers will refuse to act on instructions received from someone claiming to be a particular user without presenting the proper authenticator. Assuming that there is a secure connection between the cell phone and the browser, the trusted device tool provides an additional authenticator, such that the Man-in-the-Middle attacker must compromise the device and obtain the users password to access the users' account. This approach simply reduces the reliance of users protecting their selves against phishing attacks and will provide a mechanism based on cryptographic operations on a trusted mobile device.

Figure 5: The browser displays the visual hash as a border around the authenticated website

4: PROPOSED WORKS

Privacy indicators attempt to turn privacy policy information into intuitive icons. Unfortunately, current indicator designs are not very effective for a variety of reasons. To date, there have been few studies on optimal indicator designs [11]. Many privacy indicators ignore the web activities information in client's sides.

In this research paper, we propose an extension to the current web browser security indicators that will provide users with more information about a certain site. Users sometimes come across sites that they may feel distrustful about due to maybe not being familiar with the site, the site not having an SSL/TLS Certification or maybe just the appearance of the site. Due to security indicators not being able include every malicious website in their black list data base, sites that may be distrustful to the user may not be distrustful to the security indicators which will not strike a warning message to the user. In this case, we propose the "STIB" indicator button which will provide the user with history and statistics information on how often the site is viewed and transacted upon providing the user with more in dept information about the site which will lead to the confidentiality of the legitimacy of the site.

The "STIB" is an extended security indicator that further determines the legitimacy of a web site through a history check of the site. The history check would be scanned upon how many times a site has been view by users over a specified period of time on the internet and upon the amount of times the current active machine have view the site. Note that the STIB does not notify the users of malicious site such as spoofing and phishing sites. It is simply extends history information on the viewing activities for the website. Determining the statistics on how often a certain website is view by users will allow the STIB to provide the user with more in dept information to guide the user into making a "smarter" choice on whether or not the site should be viewed. The STIB will also perform similarity checks on URLs against sites that are normally viewed on the current machine on a daily basis. This feature will allow the user to notice that there might have been a mistype of the URL and allow the user to view similar website that has been viewed before. For example, a user may check "www.cnn.com" on a daily basis. If the user mistype the URL with "www.cmn.com", a website that has never been viewed before by the machine and is not recognized in the blacklist data base, then the STIB will provide warning message with the similarity and history information of the websites allowing the user to make a "smarter" choice on whether or not they should continue to view the website.

To show and prove that our Smart Trusted Indicator for Browsers will provide history information of URLs, we will take the following approach:

1) Research and determine the different ways to discover the number of views a URL receives.

2) Create the policies that we will use to categorize the viewing result numbers for the URLs to either being "Below Normal Viewing", "Average Normal Viewing" or "Above Normal Viewing". These results will result from and categorized to both the current machine being used and the internet. (This approach will allow the user to have a better understanding of resulting viewing numbers mean for a certain URL)

3) Create the policies to identify common or similar URLs used by the machine by analyzing history of URLs visited.

4) Implement these policies to a browser indicator button located in a visible and recognizable location on the browser window.

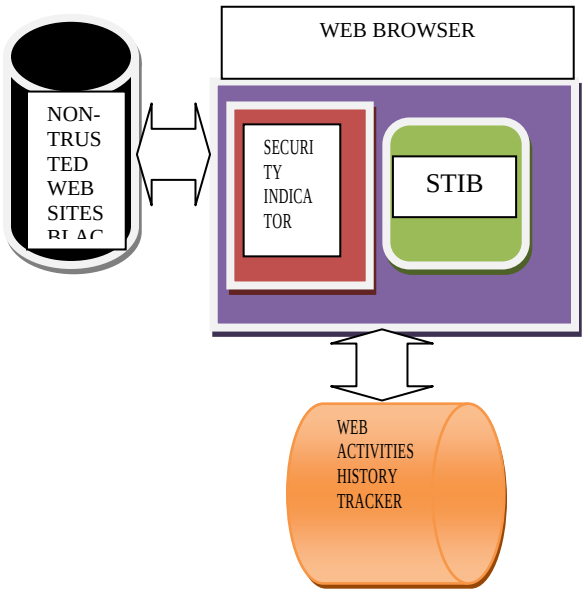


Figure 6; the basic architectural frame work of how our STIB will perform on web browsers:

5 FUTURE WORKS

Future work for this research includes our implementation for the STIB. We also plan to test the effectiveness and the impact of the STIB by performing various experiments. These experiments will include the participation of several users browsing the web and using the STIB when needed. We will observe how useful and how much of an impact the STIB will have on the users to determine the quality of our STIB.

6 CONCLUSIONS

In conclusion, we believe that our approach with the Smart Trusted Indicator for Browsers will be beneficial to users that will need more information about a website for the confidentiality of the site being legitimate. As mention before, most of the current browser security indicators are able to identify malicious sites by comparing the URLs to a blacklist data base system. Due to the fact that these blacklist data base systems will not be able to include every known malicious site, the STIB will extend history information on sites that may not be considered as malicious but may be unfamiliar or distrustful to the user. We hope that this approach will prove to be an extra aide for users to guide them into making smarter viewing choices while browsing the internet.

7 ACKNOWLEDGMENTS

This work has been supported in part by U.S. Department of Education grant P120A080094, and by NSF Minority Institutions Infrastructure grant CNS-0424556

8 REFERENCES

[1] Li, T.Y., & Wu, Y. “Trust on Web Browser: Attack vs. Defense.” *Applied Cryptography and Network Security*, Page 241-253. (2003).

[2] Herzberg , A. & Jbara, A. “Security and identification indicators for browsers against spoofing and phishing attacks.” Published by ACM. (2008).

[3] “Help Net Security: RSA online fraud report highlights phishing and brand attacks.” http://www.net-security.org/secworld.php?id=7963. (2009)

[4] NSS Labs, Security Certified. “Web Browser Security Test Result Summary – Q3”. www.nsslabs.com/browser-security. (2009)

[5] Google, Inc. “Google Safe Browsing for Firefox”. http://www.google.com/tools/firefox/safebrowsing/. (2007)

[6] Roger A. Grimes, InfoWorld. “How Secure Is Safari? ”. http://www.pcworld.com/article/158706/how_secure_is_safari.html. (2009)

[7] Sobey, J. “An Evaluation of New Browser Indicators for Extended Validation Certificates.” Ottawa, Ontario, Canada. .(2008)

[8] Dhamija, R., Tygar, J.D., & Hearst, M. “Why phishing works.” *In Proceedings of the Conference on Human Factors in Computing Systems (CHI).* Montreal, Quebec, Canada. Page 581 – 590. (2006)

[9] Parno, B., Kuo, C., & Perrig, A. “Lecture Notes in Computer Science: Phoolproof Phishing Prevention” *Published by Springer Berlin / Heidelberg.* Page 1-9. (2006).

[10] Egelman, S., Cranor, L. F., and Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceeding of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy, April 05 - 10, 2008). CHI '08. ACM, New York, NY, 1065-1074.

[11] Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. 2009. Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proceedings of the 27th international Conference on Human Factors in Computing Systems*(Boston, MA, USA, April 04 - 09, 2009). CHI '09. ACM, New York, NY, 319-328