Quantifying the Value of SSL Certification with Web Reputation Metrics

Jani Suomalainen
VTT Technical Research Centre of Finland
Espoo, Finland
Jani.Suomalainen@vtt.fi

Abstract— **Protection in the Internet and World Wide Web is based on the Socket Secure Layer (SSL) protocol and certification authorities, who verify the identities of servers with SSL certificates. Trust in the Web is based on users' perception of sites' trustworthiness and privacy as well as knowledge of servers' monitored behavior. Community-based reputation systems enable users to share their views on servers' trustworthiness. In this paper, we provide a large-scale empirical analysis on the correlation of SSL certification and community-based reputation evaluations. By using publicly available global certificate and reputation databases, we study how availability of SSL support and properties of certificates correlates to users' perception of trust, dependability, and privacy. The paper proposes a metric for revealing the benefits that service providers gain from SSL certification in general, from authority selection, and from extended validation. The proposed reputation metric could provide a mean to quantify the users' valuation of security measures. Hence, it can be utilized when selecting and designing new web security mechanisms.**

Keywords-Web security; Web reputation; Web of Trust; SSL; HTTPS; certification; correlation analysis

I. INTRODUCTION

Authentication and confidentiality of communication in the World Wide Web (WWW) is based on HTTPS (Hypertext Transfer Protocol Secure) [1] and SSL (Secure Socket Layer) [2] protocols as well as X509 public key certificates [3, 4]. The authentication model is scalable and capable of preventing most masquerading attacks when used properly. The model has, however, been criticized due to large amount of equally trusted certification authorities (CAs) and loose certification processes, which make acquiring of phishing certificates possible for attackers. Extended validation [5] certificates and additional visual trust indicators in browsers have been proposed as a more secure certification alternative. However, there have not been large scale studies on the benefits that the service providers gain from SSL certification in general and from extended validation.

Trust in WWW is based on users' perception on the trustworthiness of web sites as well as on reputation of services and service providers. To ease users to decide whether to trust a site or not, reputation services, e.g., Web of Trust (WOT) [6], have emerged. These services enable browsers to show visual warning or block access when the user tries to access a web site with poor reputation. The reputation is a measure determined by monitoring the behavior and content of servers. It can be based on automated analysis or on ratings shared by users.

Servers' support for SSL correlates with servers' security related reputation. SSL makes phishing and other masquerading attacks as well as confidentiality breaches harder. Therefore, it should increase reputation of servers when considering trustworthiness and privacy. The correlation and the causal relation between reputation and SSL are not straightforward or direct. In addition to SSL, other factors affect to the users perception of trust. A service provider that invests to security may also invest other factors increasing the reputation. Nevertheless, the correlation can be used as a one metric when evaluating the usefulness of SSL certification.

This paper contributes by providing a large-scale empirical analysis on the correlation of SSL certification and crowd-based reputation evaluations. Existing work studying effectiveness of SSL certification and warnings in browsers has concentrated on experiments with restricted amount of participants. In this study, we analyze real world data in much larger scale. In our study, the data comes from real deployments and thus cannot be distorted due to laboratory arrangements. The study has two implications. Firstly, we measure the benefits that reputations of web services gain from SSL certification and extended validation as well as from the selection of more reputable certification authorities. Secondly, we introduce a metric that can be used when analyzing impacts and visibility of web security solutions.

The paper is organized as follows. Section II presents related work and motivates our research. In Section III, we describe what data was collected for the analysis. Section IV presents results of statistical analysis on the correlation of SSL certificates and reputation ratings. A discussion on the results and their potential exploitation is provided in Section V. Section VI concludes and summarizes the paper.

II. BACKGROUND AND RELATED WORK

A. SSL Certification

Authentication of web servers is based on X.509 certificates, which have been granted to servers by a trusted CA. In typical browsers (including Mozilla Firefox, Internet Explorer, Google Chrome etc.) the amount of accepted root certificates is large. The acceptance criteria depend on the trustworthiness of CA but also on business and politics. If one of these CAs has been compromised and certifies bogus servers, the end-users web transactions are in jeopardy. Browser's security identifiers will not warn on bogus servers certified by trusted CA even if it would have been a different CA that actually had signed the victim service. Attacks demonstrating the weaknesses of CAs have already been reported, including the recent DigiNotar and Comodo incidents [7, 8].

Large scale studies on how the certificates are used has been performed by Eckersley et al. [9], who scanned public Internet for certificates and reported several vulnerabilities. Vratonjic et al. [10] analyzed certificates with the million most popular web sites and reported that most HTTPS servers do not use certificates properly. Typical problems are domain mismatch, certificate expiration and untrusted (self-signed) certificates.

Dhamija et al. [11] studied users ability to distinguish real web sites from spoofed sites using SSL warnings. They found that 23% of participants did not check browser's passive security indicators at all when evaluating the trustworthiness of the site. Sunshine et al. [12] performed a survey and a laboratory test to examine users' reactions to different active SSL warnings. They noted that users' behaviour depends on the actual message as well as on the service type. Tests revealed that more than the half of the hundred participants ignored the warnings of the main stream browsers and proceeded to the web sites anyhow. A bit more moderate results were gained by Egelman et al. [13] who found that 21% of sixty study participants ignored active warnings and fell to phishing attacks. When the security indicators and warnings are ignored, the credibility of a web site depends on various other factors. These factors were studied by Fogg et al. [14]. Their study, made with 1400 participants, reveals that real-world feel, ease of use and expertise are the most important categories affecting to credibility.

SSL certificates are assigned to service providers through diverse certification processes. Typically, it is enough that the requester has an access to email, which has been registered for the domain name holder. This makes acquirement of phishing certificates possible for attackers. Some certification authorities may have more trustworthy processes in use but the large amount of equally trusted authorities means that end-users do not have practical means to separate real and trustworthy certifications from bogus certification received from a compromised or careless authority.

Extended Validation Certificates [5] and additional visual trust indicators in browsers have been proposed as a more secure certification alternative. EV certificates are given for servers, which have gone through stricter authentication processes. Browsers identify servers with EV certificates as more trusted by displaying additional trust indicators, notably green address bar. See Figure 1 and Figure 2 for examples of address bar in Mozilla Firefox 8 and Internet Explorer 8 looks when browser connects to services with either unsecure HTTP, (ignored) invalid certificate on HTTPS server, valid regular certificate on HTTPS server, or EV certificate on HTTPS server. EV trust indicators have been supported for a couple of years in the main stream browsers including Microsoft Internet Explorer (since version 7, released October 2006), Mozilla Firefox (version 3, June 2008), Opera (version 9.5, June 2008), Google Chrome (September 2008) and Safari (version 3.2, November 2008).

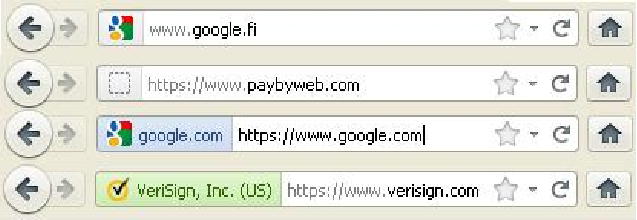

Figure 1. Security indicators in address bar of Mozilla Firefox 8 (from top to bottom: unsecured HTTP, ignored certificate error, regular certificate, extended validation certificate)

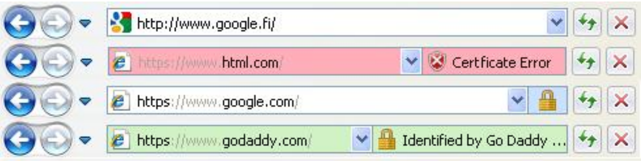

Figure 2. Security indicators in address bar of Internet Explorer 8

The question whether the extended validation increase the security and trustworthiness has been considered by few researchers. Sobey et al. [15] studied whether users notice the additional trust indicators by tracking eye movements of 28 untrained test participants who were making online shopping decisions. They concluded that the validation indicators in Mozilla Firefox 3's address bar went unnoticed for all participants and proposed, as an alternative, more visible and obtrusive trust indicators. Similar results were gained by Jackson et al. [16] studied whether extended validation would help users to detect phishing attacks more easily with a test group of 27 participants and whether security trained users, who had read a help file, are capable to use these indicators. They noted that the trained users did not outperform the untrained users as extended validation did not help users to detect control attacks.

Some researchers have addressed the problems of weak certification by proposing means to determine certificates' trustworthiness and to **limit certificate issuers' authorities**. Marlinspike presented [17] a solution called Converge for turning off all untrusted CAs in a browser. The idea includes a trust management scheme, where other users' views and consensus on particular CAs can be queried from notaries. Another solution called CertLock, presented by Soghoian and Stamm [18], tries to detect suspicious CA changes in certificates. They focus particularly on CA's country of origin and in the prevention of governmental attacks. CertLock uses browsers history information on certificates and warns end-users if CA's country of origin has been changed. In Perspectives [19], presented by Wendlandt et al., a trusted party collects issuer identity information frequently from TLS servers. The browser plugin may then query whether the issuer has been changed and warn end-user accordingly. A related certificate transparency proposal was made by Laurie and Langley [20]. They proposed that end-users would accept only those certificates, which are available from trusted and public source. The approach would prevent long-life attacks, as service providers could to monitor this public source and suppress fake certificates, claiming their domain names.

B. *Web Reputation*

SSL certification provides mechanisms for checking that web servers belong to the legitimate entities. However, it does not address whether the server acts inappropriate and expected manner and thus whether the site can be trusted. Untrustworthy web sites can be avoided by using blacklists, containing sites with bad reputation, and whitelists, containing sites with good reputation. Black- and whitelisting can be based either on automated techniques, where server's content is checked against malware fingerprints, or manual techniques, where users evaluate sites' trustworthiness. Human based evaluation is extensive only when a large number of people, a community or a crowd, are participating.

One of the crowd based reputation information providers is WOT. WOT is a company, which collects information from the open community of volunteers. These volunteers evaluate the web sites they visit by using browser add-ons, which are available for Firefox, IE, Chrome, Safari, and Opera. The WOT company was founded July 2006. In November 2011 they reported that their database contains ratings from over 33 million servers.

The strength of WOT is in the detail of information. Evaluation is based on collecting users' subjective ratings, which vary from very poor (numeric values 0-19), poor (20-39), unsatisfactory (40-59) and good (60-79) to excellent (80-100). Ratings are given to four different categories:

1. Trustworthiness – whether the site is safe to use and free of malware and phishing attacks
2. Vendor dependability – whether the commercial actor (e.g., a web shop) behind the server can be trusted and provides good shopping experience
3. Privacy – whether the server is trusted to protect users information appropriately and does not collect private information for vague purposes
4. Child safety – whether the server contains material such as adult content, violence or hateful language, not suitable for the children

In addition to the ratings, WOT provides confidence information for each rating. Confidence is presented by using six different categories and numeric value from 0 to 100. A rating is more credible when large amount of contributors have given similar ratings and when these contributors itself have high individual confidence rating. Individual confidence ratings grow among time when users contribute. WOT does not reveal how the confidence ratings and reputation ratings are exactly calculated to make misuse harder.

Reputation systems are vulnerable for manipulating attacks as discussed by Moore et al. [21] who analyzed a phishing focused service called PhishTank [22]. They noted that the service is dominated by most active users and there is a risk of manipulation by small number of people. The accuracy, completeness and vulnerabilities of the WOT metrics have been analyzed by Chia et al. [23]. They found that WOT was more comprehensive than the compared automated services (Google's Safe Browsing, McAfee's SiteAdvisor and Norton's Safe Web) in detecting malicious domains. They also argued that WOT may be resistant against manipulation attacks due to advanced statistical analysis on the contributors' behavior but that it is still vulnerable for determined malicious gamers. However, as manipulation is likely to affect only restricted amount of servers, it is not likely to distort our large scale statistical studies.

Accuracy of crowd-based reputation systems and black lists has been enhanced by combining results from various heterogeneous sources. For instance, WOT utilizes blacklisting information from PhishTank. Use of quantitative web traffic information was proposed by Sharifi et al. [24], who automated information collection from various web services, including traffic ranking and search engine hits, and analyzed how well this information supports scam detection.

III. Combining SSL Certificate, Web Reputation and Web Rank Data

We collected, combined, and analyzed data from three different repositories as illustrated in Figure 3. First we received SSL certificate database collected in SSL observatory project of Electronic Frontier Foundation (EFF). Secondly, information on web server's popularity was received in form of a list of top million servers produced by Alexa. Then, for the all valid certificates and for all top servers, we requested Web reputation ratings from WOT.

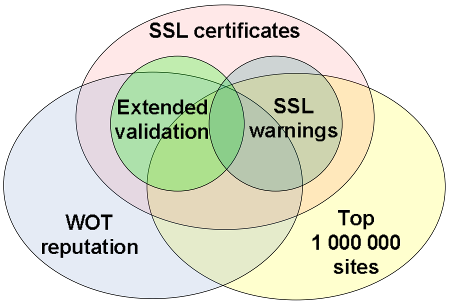

Figure 3. Composition of analysis data

SSL certificates available in the public Internet have been collected in EFF's SSL observatory project [9, 25]. The database contains almost 4 million certificates, including both 'regular' certificates as well as extended validation certificates. We used certificates, which were collected December 2010 and classified as valid by EFF. For the analysis we resolved and selected those HTTPS servers, which had complete domain name (certificates with wild cards in domain names were ignored), were active and fully working in November 2011. Services were classified as active if the request (to the root directory of the SSL (443) port) resulted a reply larger than 1kB. This limit filtered most servers were HTTPS port is used only for redirection to HTTP port or for some other limited purpose.

List of top million servers, collected by Alexa [26], was used to get domain names of servers, which are really used and frequently visited. This enables comparison between HTTP only servers and servers with HTTPS support. For each server in the list, we collected HTTPS status information indicating whether the HTTPS port was open and whether the connection succeeded without warnings.

WOT reputation metrics were collected for all HTTPS sites as well as for HTTP only sites among top million servers in order to enable comparisons. The confidence limit does not affect substantially to counted averages but it filters out some suspicious ratings. In our analysis, described later, we used only those ratings with reasonable confidence value (12 or higher). Data was collected and analyzed with Linux shell and Perl scripts. SSL status queries and certificate verifications were done on a client based on OpenSSL. Certificates of contacted servers were verified against root certificate list used by Mozilla. MySQL was used as database software. For EFF dataset we found 201,099 active and reputed HTTPS servers and for Alexa dataset we found reputation information for 132,533 HTTP only servers, for 68,961 HTTPS servers, and for 34,985 broken HTTPS servers (showing security warnings when connected).

IV. Correlation between Web Reputation and HTTPS Support

A. Does the HTTPS Support Increase Reputation?

The effect of HTTPS support to reputation rankings was studied by calculating average and distribution of reputation values from the Alexa dataset, which contained information from top million servers. The results for trustworthiness and privacy reputation are given in Table 1 and Table 2, respectively. For both metrics the rating for errorless HTTPS support gives around six additional points. Similarly, the amount of poor and very poor rates drops from around 9% to 4% when HTTPS was supported. Additionally we studied how the security warnings, such as domain mismatch or self-signed certificate, affects the ratings. We noted that HTTPS increases trustworthiness only when used correctly. However, even misused SSL based cryptography increases privacy ratings with one point.

Table 1. Trustworthiness reputation of servers with and without SSL support and with broken SSL support showing Warnings

Server type / count	Avg	Distribution (%)				
		Ex.	G	***Uns.***	Poor	***VP***
HTTPS / 13,497	84,7	84,5	9,5	1,8	1,0	3,1
Broken HTTPS / 9,483	78,7	73,1	13,4	4,1	2,5	7,0
HTTP only / 41,250	78,6	72,1	13,8	5,0	2,5	6,5

Table 2. Privacy reputation of servers with and without SSL support and with broken SSL support showing Warnings

Server type / count	Avg	Distribution (%)				
		Ex.	G	***Uns.***	Poor	***VP***
HTTPS / 13,001	84,9	86,0	8,1	2,0	1,1	2,8
Broken HTTPS / 8,776	80,0	73,7	13,1	4,9	2,4	5,8
HTTP only / 37,197	78,9	73,4	13,0	6,6	2,8	6,2

The servers in HTTPS category may have also the HTTP port open. Hence, we cannot say whether the user evaluations were done in the HTTPS secured connection or not. From the larger EFF dataset, we found servers that had only HTTPS port active. For 431 servers the average trust value was 86,6 (when the average value for all HTTPS servers in ‘EFF dataset’ was 85,8). The privacy ratings for 371 servers were 87,9 (and 87,1 for all). This small sample indicates that reputation of servers supporting only HTTPS would be even larger.

We studied also how trustworthiness and privacy reputations correlate with the popularity of server. Sliding averages presented in Figure 4 illustrate that the better ranking Alexa increases trustworthiness and privacy value. The difference of reputation between secured and unsecured is visible despite the popularity, though the difference is smaller with more popular servers.

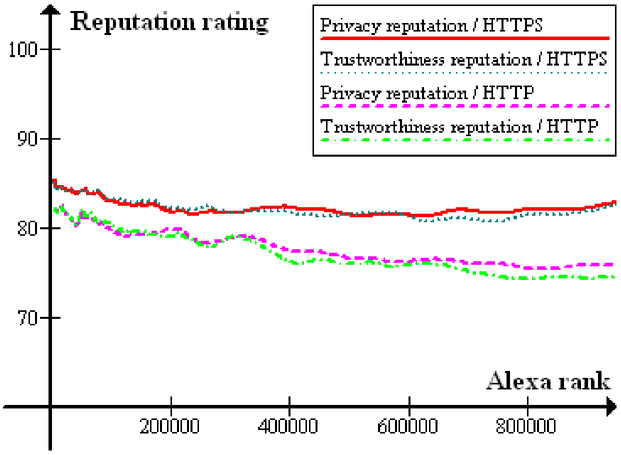

Figure 4. Dependency between reputations and popularity

B. Differences between CAs

There are clear differences between the reputation of servers certified by different CAs. The following table presents results of CAs, which all had more than thousand valid certificates used by active and trustworthiness ranking with reliability at least 12 points servers within ‘EFF dataset’. The results show a difference of over 10 points between the averages of the best and the worse CAs. The difference is even significant when looking at the ratio of poor and very poor sites: increase from close zero to 7,4%. Different CA brands provided by one company have not been combined in the table. For example, Comodo is also the provider of The Usertrust Network and Terena certificates, Symantec is the owner of Verisign and Thawte.

TABLE 3. TRUSTWORTHINESS REPUTATION OF SERVERS CERTIFIED BY DIFFERENT CAS

CA / certificate count	Avg	Distribution (%)				
		Ex.	G	*Uns.*	Poor	*VP*
Cybertrust / 1061	89,3	96,6	3,0	0,2	0,0	0,2
Verisign / 9993	88,7	92,1	6,0	0,8	0,4	0,7
Terena / 1410	88,6	95,7	4,3	0,0	0,0	0,0
Entrust / 1747	88,1	92,8	4,6	1,4	1,0	0,2
Thawte / 5506	85,9	85,3	10,7	1,6	1,0	1,3
Usertrust N. / 1994	83,9	77,4	18,7	1,0	1,0	2,0
Equifax / 4828	82,0	74,0	19,0	1,9	1,3	3,8
Comodo / 1557	81,9	75,8	16,2	2,1	0,7	5,3
GoDaddy / 2973	79,0	67,5	22,7	2,5	1,8	5,6
Total / 39482	*85,8*	*84,6*	*11,6*	*1,2*	*0,8*	*1,8*

C. The Value of Extended Validation Certificates

Extended validation provides only small or no increase of reputation at all. Table 4 compares trustworthiness and privacy values of EV certificates to non-EV certificates within the EFF dataset. Trustworthiness average is 0,7% higher and privacy value is 0,5% smaller.

TABLE 4. TRUSTWORTHINESS AND PRIVACY REPUTATION OF SERVERS WITH REGULAR OR EXTENDED VALIDATION CERTIFICATES

Certificates / count	Avg	Distribution (%)				
		Ex.	G	*Uns.*	Poor	*VP*
Trustworthiness						
Regular / 36297	85,7	84,5	11,7	1,2	0,7	1,9
EV / 3185	86,4	85,8	9,9	1,8	1,2	1,3
Privacy						
Regular / 32166	87,1	88,2	7,3	1,5	0,7	2,3
EV / 2839	86,6	87,1	7,6	2,3	1,2	1,7

Table 5 describes CA specific trustworthiness ratings for CAs with more than 100 EV certificates. When comparing to CA specific numbers to generic CA results in Table 3, there is a small increase of reputation all CAs except for the largest EV provider. For Verisign the EV rate is 0,7% smaller than the rate for all Verisign certificates.

TABLE 5. TRUSTWORTHINESS REPUTATION OF SERVERS EV CERTIFIED BY PARTICULAR CAS

CA / certificates	Avg	Distribution (%)				
		Ex.	*G*	*Uns.*	*Poor*	*VP*
Cybertrust / 255	89,9	100	0	0	0	0
Verisign/ 1688	88,0	91,0	5,3	1,9	3,5	0,9
Thawte/ 183	86,2	85,2	8,7	3,3	33,9	0,0
Comodo / 226	83,2	81,0	11,5	0,9	6,6	4,9
Globalsign/ 366	83,1	70,2	25,7	1,9	2,2	1,1

V. DISCUSSION

A. The Value of SSL and the Limitations of the Metric

Our intuition was that the support for HTTPS affects to reputation in two manners: Visibility of security indicators may increase it and security warning indicators and dialogs as well as published security problems will decrease the reputation. However, service providers who are willing to invest more on HTTPS are typically also willing to invest on other factors increasing reputation. The reputation is not a result of HTTPS support. Instead, they are both results of security efforts. However, even though the correlation does not imply causality, it indicates possible causes. Future research is needed to understand, in more detail, what is the value of SSL certification and what is the value of other factors contributing to reputation.

The results show that there is a clear correlation between HTTPS support and Web reputation. The reputation average of valid SSL certificates was significantly higher than the average of servers with broken certificates. Hence, it seems to pay off to have a working HTTPS support.

The difference of reputation average between the best CA and the worst CAs was significant. Certification authorities are not typically selected from the security perspective, instead price, compatibility with browsers and easiness are likely to be more important factors. Hence, the correlation may not be used to indicate of weak certification procedures but it can be used to characterize attackers' probable selections.

The difference between regular and extended validation certificates was insignificant. Since EV certificates are more expensive it would be likely that these service providers would had invested also in other factors contributing sites trustworthiness. For that reason we expected the trustworthiness ratings for EV certificates to be higher. Detected correlation seems to indicate that the additional trust indicators in browsers (Figure 1 and Figure 2) are undetected by the users. This result confirms the previous small scale end-users studies that trust indicators are ignored. Hence, according to these results we could ask why to pay an extra for extended validation.

We did not analyze differences between applications and business sectors. It may be likely that HTTPS and extended validation are typically used in more critical services, such as banks, and that WOT contributors valuate these services differently or more carefully. In the future, it should be studied how the application field affects to the reputation.

Reputation systems may utilize information on the SSL certification. Currently, WOT collects information on newly discovered phishing attacks from PhishTank and adjust reputations accordingly. Similarly, knowledge that a server has a valid certificate may increase trustworthiness and privacy reputation values of the domain name.

B. How to Utilize the Reputation Metrics?

Reputation metrics provide us a mean to quantify users' perception of security. These metrics provide researchers a better understanding on the effectiveness and impact of security mechanisms. Hence, the metrics can be valuable when developing new useful security solutions. Also, the information on the correlation can be used by decision makers, when analyzing which security mechanisms are needed and provide enough benefits to justify the investments.

Metrics may be used also to enhance applications for existing web security solutions. Specially, they are usable in notary based CA selection approaches. For instance, in Convergence [17], the browser trusts only those SSL certificates which have been certified by CAs, which are accepted by particular notaries. However, it may be difficult for notaries to know which CAs to trust. Reputation gives notaries a tool, formal metric, which can be used when evaluating CAs' trustworthiness. This would act as an incentive for CAs to verify services more thoroughly, as root certificates with bad trustworthiness averages could be considered as untrusted in some browsers.

VI. Conclusions and Future Work

In this paper, we studied the correlation between web reputation metrics (particularly WOT trustworthiness and privacy values) and SSL certification. Web reputation metrics provide researchers a statistical mean to quantify users' perception of trust and privacy and, hence, impact and effectiveness of security solutions. The results of our-large scale HTTPS/SSL correlation analysis reinforce the doubts on the inefficiency of the extended validation in SSL certification. They also reveal the differences between servers certified by different authorities.

In the future, more studies and analysis is needed to fully understand the causal relation between security mechanisms and end-user's perception of security. We need to study differences between particular web service categories and within selected services in order to understand all the contributing factors.

References

[1] E. Rescorla. HTTP Over TLS. IETF Specification. 2000. http://www.ietf.org/rfc/rfc2818.txt.

[2] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol. Version 1.1. IETF Specification. 2006. http://www.ietf.org/rfc/4346.txt.

[3] International Telecommunication Union. ITU-T Recommendation X.509. 2008. http://www.itu.int/rec/T-REC-X.509-200811-I/en.

[4] R. Housley, W. Ford, W. Polk, and D. Solo. Internet X.509 Public Key Infrastructure, Certificate and CRL Profile. IETF Standard. 1999. http://www.ietf.org/rfc/rfc2459.txt.

[5] CA/Browser Forum. Guidelines For The Issuance And Management Of Extended Validation Certificates. Version 1.3. 2010. http://www.cabforum.org/Guidelines_v1_3.pdf.

[6] Web of Trust . WWW site. Available: http://www.mywot.com/. [Accessed March 3rd 2012].

[7] G. Keizer . Hackers may have stolen over 200 SSL certificates. Computerworld. 2011. http://www.computerworld.com/s/article/9219663/Hackers_may_have_stolen_over_200_SSL_certificates. [Accessed March 3rd 2012].

[8] Mills, E. Comodo: Web attack broader than initially thought. CNET, 2011. Available: http://news.cnet.com/8301-27080_3-20048831-245.html;. [Accessed March 3rd 2012].

[9] P. Eckersley and J. Bums. An Observatory for the SSLiverse. Presentation at DEFCON 18. 2010.

[10] N. Vratonjic, J. Freudiger, V. Bindschaedler, and J. Hubaux. The Inconvenient Truth about Web Certificates. The Workshop on Economics of Information Security (WEIS). Fairfax, Virginia, USA, 2011.

[11] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. Proceedings of the SIGCHI conference on Human Factors in computing systems. Montreal, Quebec, Canada, 2006. CHI '06, pp. 581-590.

[12] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: an empirical study of SSL warning effectiveness. Proceedings of the 18th conference on USENIX security symposium. Montreal, Canada, 2009. SSYM'09, pp. 399-416.

[13] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems. Florence, Italy, 2008. CHI '08, pp. 1065-1074.

[14] B.J. Fogg, et al. What makes Web sites credible?: a report on a large quantitative study. Proceedings of the SIGCHI conference on Human factors in computing systems. Seattle, Washington, United States, 2001. CHI '01, pp. 61-68.

[15] J. Sobey, R. Biddle, P. C. Oorschot, and A. S. Patrick. Exploring User Reactions to New Browser Cues for Extended Validation Certificates. Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security. Malaga, Spain, 2008. ESORICS '08, pp. 411-427.

[16] C. Jackson, D. R. Simon, D. S. Tan, and A. Barth. An evaluation of extended validation and picture-in-picture phishing attacks. Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security. Scarborough, Trinidad and Tobago, 2007. FC'07/USEC'07, pp. 281-293.

[17] M. Marlinspike. SSL and the future of authenticity. Presentation at BlackHat USA . 2011. http://www.youtube.com/watch?v=Z7Wl2FW2TcA. [Accessed March 3rd 2012].

[18] C. Soghoian and S. Stamm. Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL. 3rd Hot Topics in Privacy Enhancing Technologies, 2010. HotPETs 2010, pp. 50-61.

[19] D. Wendlandt, D. G. Andersen, and A. Perrig. Perspectives: improving SSH-style host authentication with multi-path probing. USENIX 2008 Annual Technical Conference. Boston, Massachusetts, 2008. ATC'08, pp. 321-334.

[20] B. Laurie and A. Langley. Certificate Authority Transparency and Auditability, 2011. http://www.links.org/files/CertificateAuthorityTransparencyandAuditability.pdf.

[21] T. Moore and R. Clayton. Evaluating the Wisdom of Crowds in Assessing Phishing Websites. Proceedings of the Financial Cryptography and Data Security, 2008. FC'08, pp. 16-30.

[22] PhishTank. Web site. Available: http://www.phishtank.com/. [Accessed March 3rd 2012].

[23] P.H. Chia and S. J. Knapskog. Re-Evaluating the Wisdom of Crowds in Assessing Web Security. Proceedings of the Financial Cryptography and Data Security. 2011.

[24] M. Sharifi, E. Fink, and J. G. Carbonell. Detection of Internet scam using logistic regression. Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics. 2011. Pp. 2168-2172.

[25] Electronic Frontier Foundation. The EFF SSL Observatory. Available: https://www.eff.org/observatory. [Accessed March 3rd 2012].

[26] Alexa. Top 1,000,000 sites. 2011. Available: http://s3.amazonaws.com/alexa-static/top-1m.csv.zip. [Accessed November 28th 2011].