Economic Incentives in the HTTPS Authentication Process

Rémy Degenne
Advisor: Heiko Niedermayer
Seminar Future Internet SS2013
Chair for Network Architectures and Services
Department of Informatics, Technische Universität München
Email: remy.degenne@tum.de

ABSTRACT

In this paper, the authentication system of the HTTPS protocol is considered from an economical perspective. The use of SSL certificates to authenticate web servers has a number of known technical flaws but is widely used. The different actors of the HTTPS authentication system are identified and the study of their roles and incentives for security shows the lack of a clear reason to progress towards a more secure system.

Keywords

HTTPS, Certificate, SSL, Incentives, CA, Security

1. INTRODUCTION

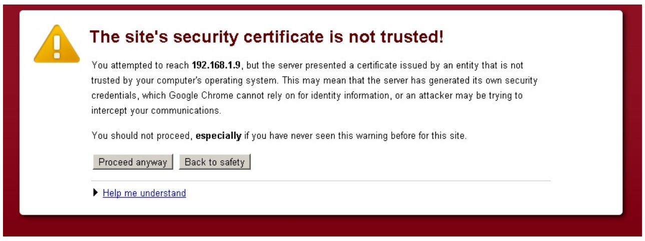
Many websites ask the user for sensitive data like a login and password, that could be used for other purposes, or credit card informations. To send these informations safely, the transmission must be encrypted and the user must be sure of the identity of the organization managing the server. A safe authentication process is essential to establish trust between the user and the organization. This is usually done by using the HTTPS protocol in which Certification Authorities are used to confirm the identity of the server. This system was the victim of multiple successful attacks and is widely criticized. Here we will describe this authentication process and analyze the possible reasons leading the different actors of the process to increase the security.

2. HTTPS AUTHENTICATION PROCESS AND THE USE OF CERTIFICATES

2.1 HTTPS

HTTPS is designed to be a secured version of the HTTP protocol and is widely used to protect sensitive data, like payment information during an online transaction. It is in fact the HTTP protocol stacked on top of a SSL or TLS layer (Secure Sockets Layer / Transport Layer Security) and has the security of these underlying protocols.

One aspect of the SSL/TLS protection system is an identification of the server. When somebody reaches a domain using HTTPS, the server must confirm its identity by providing a valid certificate prior to any data exchange between the client and the server. If it fails to provide valid credentials, the browser will show a warning, informing the user that the identity of the server could not be verified and that she should not proceed as seen in Figure 1.



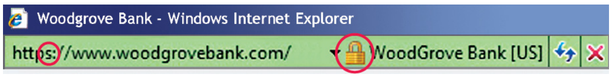
The site's security certificate is not trusted!

You attempted to reach **192.168.1.9**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

Figure 1: Google Chrome warning - untrusted certificate

The major web browsers include visual clues to tell a user that a website is using HTTPS, like coloring of the address bar or the use of a lock icon. The purpose is to help the user know that the web site is really the one it claims to be and that any exchanged data will be encrypted.



Woodgrove Bank - Windows Internet Explorer
https://www.woodgrovebank.com/
WoodGrove Bank [US]

Figure 2: Internet Explorer HTTPS visual clues

2.2 The SSL certificates

The purpose of a SSL certificate is to be sure of the identity of one server. The certification system is centralized and rely on a group of trusted actors that will in turn sell certificates to servers that they trust [12].

Certificates are created by Certification Authorities (CA). Each CA issues a root certificate to identify itself. The Internet browser stores a list of such certificates corresponding to every CA it trusts that allows it to verify the identity of these authorities.

To be identified by a browser using the SSL certification system, a web server must acquire a certificate from one of the trusted Certification Authorities. The link between a server and a root CA must not be direct : a CA can give (or more likely sell) a certificate to an agent that will itself create other certificates and distribute them. A browser will consider that a certificate is valid if it is possible to follow the trust chain back to a known trusted CA.

There are different types of certificates corresponding to different visual clues in the web browsers. To deliver a Domain Validation (DV) certificate, a CA usually checks that the

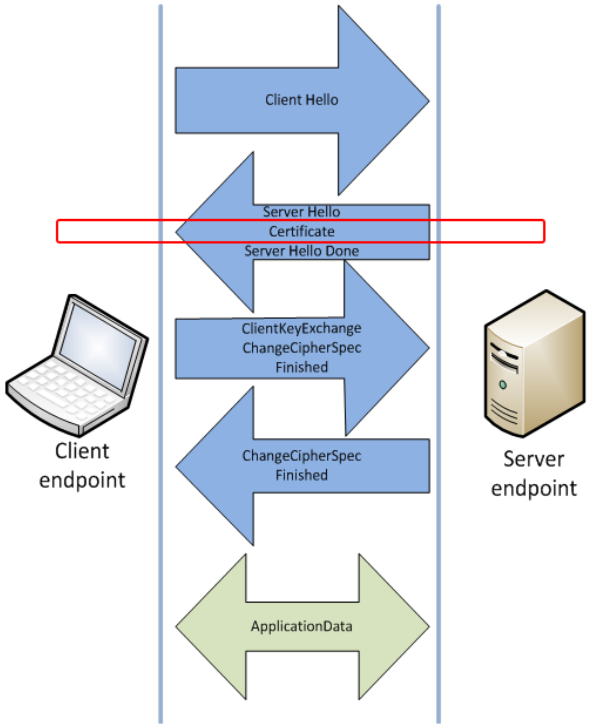


Figure 3: HTTPS Handshake

person owns the validated domain. An Organization Certificate (OV) can be issued after verifying the identity of the organization and will display additional information in the Internet browsers about the organization. There are also Extended Validation (EV) certificates that are designed to have e reinforced security. To obtain one of these an organization must usually have contact with the CA by letter, by phone or face to face and provide proof of its identity, right to use the domain and additional information concerning the organization.

The possible cases of a wrong authentication process are the following :

1. The certificate provided is expired.

2. The certificate can not be verified. it can be self-signed or created by a CA that is not trusted by the browser.

3. The certificate was made for a domain name that does not match the name of the issuer.

4. The certificate is not valid.

The browsers show different warnings for these errors to inform the user about the nature of the problem.

3. THE CERTIFICATION AUTHORITIES AND THE CERTIFICATE MARKET

The actors of the authentication process are the Certification Authorities, the browsers, the organizations or individuals who manage the servers and the users. The Certification Authorities sell certificates to the owners of the servers who buy them to give the user a proof of the identity of the server and thus to allow the user to trust any transaction with this server.

The browser has an important role in the certificate validation because it decides which Certification Authorities can be trusted in its validation process. This makes the organizations managing the major browsers important actors in the definition of the certificate attribution procedures.

The user has contacts with the servers through the browser and expects to be able to use the services provided safely. the user does not have direct contact with the Certification Authorities.

There exists many Certification Authorities trusted by the major internet browsers, in many countries. Microsoft trusts 333 root Certification Authorities [1] and more than a thousand Certification Authorities with the secondary authorities. Few big Certification Authorities that have a huge part of the market. Symantec, Comodo and Godaddy together have more than 75% of the market share.

The certificates sold by the majors Certification Authorities have the same practical value, as these Certification Authorities are trusted by all common browsers. A valid certificate from one trusted CA allows authentication as well as one from an other trusted CA. As presented in [5], a situation with identical products like this one should lead to a competition based on the price of the product. this is not the case and the prices vary greatly between the different Certification Authorities and a few Certification Authorities sells the majority of the certificates on the market. The market shows little signs of a price competition as the Certification Authorities with higher market shares also have high prices.

The Certification Authorities sell the same product but offer different services with the certificates, like support to help for the deployment of the certificates and HTTPS or additional security audit.

4. TECHNICAL FLAWS

The SSL certificate authentication presents a number of known flaws and successful attacks on Certification Authorities did occur.

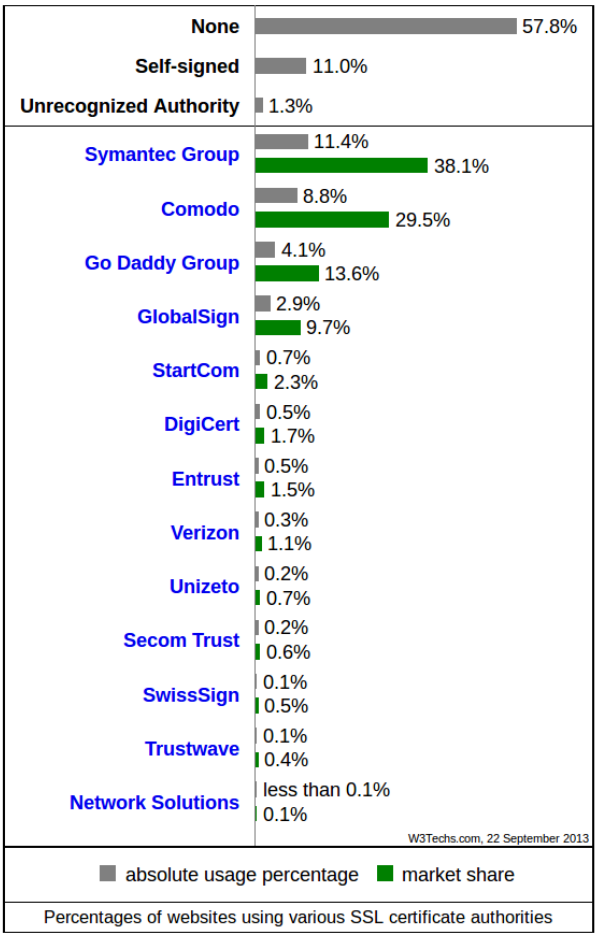
4.1 A Difficult Deployment

A first problem limiting the use of HTTPS is the impossibility to embed objects that do not support HTTPS in a page. A page using HTTPS wanting to include such an object will trigger a security warning, asking the user if he wants to obtain only the HTTPS content. Many web sites rely on such components, like advertisement banners. This leads to a number of web sites not supporting HTTPS. Some web sites can also want to use HTTPS and become unexpectedly faced with such embedded content that only supports HTTP. A user would face a warning but could need to ignore it to use the web site properly and would lose any security benefits from HTTPS.

4.2 A Weakest-Link Problem

The biggest problem in the certification system is the possibility for any CA to give a certificate for any domain name.

doi: 10.2313/NET-2014-03-1_06



W3Techs.com, 22 September 2013

Percentages of websites using various SSL certificate authorities

Figure 4: The SSL Certification Market

For example google.com already has a certificate but any CA can issue a different certificate for it that will also be considered valid by the browsers, regardless of the owner of the certificate. A compromised CA, for example a secondary CA that was successfully bought by a malicious agent, can issue certificates for any name to anybody and the certificate will be considered valid. This means that a successful attack on the weakest CA compromises the entire system. The browsers trust more than a thousand Certification Authorities in more than 40 countries.

A successful attack on a CA, DigiNotar, occurred in 2011. Hundreds of false certificates were issued for domain names including the ones of Google, Yahoo! and Mozilla. Man-in-the-middle attacks using the fraudulent certificates were reported in Iran. When this was revealed, DigiNotar was removed from the trusted Certification Authorities lists in the major browsers and went bankrupt. Others successful attacks occurred also on companies having a big market share like Comodo [6]. The certificates issued were revoked and this CA is still trusted by the browsers.

There are widely accepted Certification Authorities in many countries and most of these countries own a CA or have the power to demand false certificates to use them as they want. The certificate system technically allows any of these governments to transgress the security rules.

4.3 Warnings only

An other problem with the certificate system is in the nature of the response to a invalid certificate. The browsers only display a warning that will be ignored by 20% of the users for untrusted certificates errors such as certificates with a wrong name, according to [2]. This means that an attacker wanting to impersonate a known web site will succeed in those cases without needing any real certificate.

4.4 Certificate revocation

When a certificate is misused, it has to be revoked. There are two existing revocation processes : Certificate Revocation Lists (CRL) and the Online Certificate Status Protocol (OCSP).

A CRL is a list maintained by a CA and downloaded regularly by a browser to be checked locally. As the CRL can become a big file the clients employ a caching strategy, meaning that the list is not always up to date [3]. An other reason for this list to be outdated is the rate at which the CA updates the list. An other problem is that browsers tend to ignore parts of these lists to avoid preventing access to popular websites.

With the Online Certificate Status Protocol, the client sends a request to the CA to know if a certificate is valid. This implies that a client must contact the CA each time that it contacts a web site and causes a latency in the HTTPS handshake. The same type of cache problem on the side of the CA as with CRLs is possible, as the CA must also update its lists. A browser will not prevent a user to reach a site if the CA cannot be contacted, because this connection can be impossible for example in the case of a user contacting a payment portal for a public internet access who is prevented to reach any other site until the payment is done. Finally, OCSP allows the CA to gain information on all web sites with certificates that the user visits and this is a Privacy problem.

5. ACTORS AND THEIR SECURITY INCENTIVES

There are four types of actors in the certificate authentication system : certification authorities, browser vendors, server owners and users. All these actors have few incentives to increase the security of the certificate authentication system as it is.

5.1 Certification Authorities

It is difficult to know the details of the security of the Certification Authorities. DigiNotar was audited after the successful attacks it suffered and it appears that they did not use an antivirus software and had weak root passwords among other problems.

The security procedures to verify the identity of the certificate buyers are almost non-existent for Domain Validation certificates and depend greatly on the CA for Organization Validation certificates. The Extended Validation certificates are subject to strict rules defined in concert with the major browser vendors.

Liability could be a security incentive for the Certification Authorities but the Certification Authorities place all responsibility on their clients (the servers), who denies this responsibility in their user's terms of agreement. Thus the companies that make the certificates are not responsible of their failure. The reputation loss could be a significant cost in this case but the successful attacks on VeriSign and Comodo did not lead to a ban of their certificates and the big Certification Authorities are considered 'too-big-to-fail' and thus have a weaker incentive.

5.2 Browsers

The organization behind an internet browser has two main purposes that dictates their policy regarding the authentication security. They have to make sure that the user can access as much web sites as possible and that the user does it safely. These two goals can conflict and a browser can have a lower security policy in order to increase its usability.

Some web sites do not support HTTPS and the ones supporting it are not all safe. According to SSL Pulse [8], only 24.6% of the 168,000 most visited web sites can be considered secure, and only 823 support HTTP Strict Transport Security, a protocol that restricts data exchange to HTTPS only. A browser cannot offer only access to sites well protected without preventing the use of a huge part of the web. The warning procedure in case of an authentication problem is also designed to allow the user to enjoy web services in an environment where the HTTPS protocol is not perfectly applied.

The attacks on Comodo and DigiNotar are a good example of an adaptation of the security policy according to usability requirements. DigiNotar was a minor actor of the certificate market and the browsers removed their certificates from the trusted Certification Authorities lists as a result of the security breach. In the case of Comodo, holder of 12% of the market share according to [1], the browsers did not remove the CA from the trusted Certification Authorities lists but made an effort to remove only compromised certificates. [1] argues that this is a too-big-to-fail case : one browser can not remove all Comodo certificates without preventing its users to access a large part of the major web sites.

The browser organizations are also agents with the power to negotiate security features with the Certification Authorities. They are the ones who decide if a CA is trusted or not and as such can influence the certificate deliverance procedures. The CA/Browser Forum for example regroups many Certification Authorities and browser software vendors and aims to define the Extended Validation certificate standard [15]. As noticed before, it is difficult for a browser to ban an important CA and thus this power of decision of the browser providers is limited.

Browsers vendors have an incentive to provide a good level of security to the user because it is part of the service quality of this browser but this is strongly mitigated by usability concerns and leads to browsers having a fail tolerant policy.

5.3 Organizations owning servers

The organizations managing servers are the clients of the Certification Authorities and buy certificates to make the user trust their service. Only 35% of the top 1000 web sites have a SSL certificate and 6.8% have an Extended Validation certificate. A server owner uses a certificate in most cases to protect payment and login data transfers.

As every certificate has the same use regardless of the CA that issued it, a great number of server owners buy cheap Domain Validation certificates [5] that allow them to use the HTTPS protocol but do not give the user any information on the identity of the owner of the certificate. Many companies also buy valid certificates but use them wrong for costs reasons : a company can for example have a valid certificate for a domain and use it also for subdomains. this is one of the factors explaining the great number of domain mismatches in valid certificates (see figure 5) [5]. The difficulty and the cost of maintaining a correct deployment of the certificates is an other factor.

The CA with higher costs are also big actors of the market, especially for Extended Validation certificates. [1] explains this fact by the support sold with the certificate, by a reputation factor, by the pressure on the buyer from his hierarchy resulting in the choice of a leader of the market perceived as safer and by the perception that these leaders are too big to see their certificates invalidated. This last reason is the result of a preference for a maintained usability in case of a failure of the certificate system over the avoidance of a security risk.

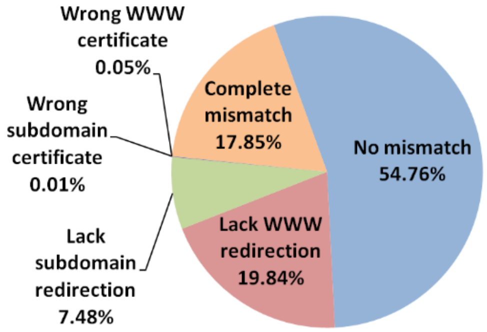


Figure 5: Domain mismatch among trusted unique certificates with valid signatures

The companies using certificates want to send trust messages to the users but weight their security efforts with their costs. An organization that does not choose to use an Extended Validation certificate has no interest in doing more than what is requested to have the user navigate their site without security warnings.

[4] shows that the EV certificates does not increase significantly the trust of the user. A consequence is that a company gains all possible trust benefits by using a Domain Validation certificate, that does not even provide information on the identity of the owner.

5.4 Users

Studies like [2] suggest that a large part of the users ignore the SSL errors. At least 20% of the users would ignore a warning that the name in the certificate and the name of the domain do not match. This percentage is larger with the other types of errors. The type of certificate seems to have few effect on the trust a user places on a web site [4]. Certificates designed to convey more trust like Extended Validation certificates do not increase the perceived trustworthiness of a server. In a study presented in [18], 48% of the participating users stated that nothing bad was happening when confronted to a certification error.

The environment of the user is also misleading. Some web sites use 'trust seals' provided by the Certification Authorities that are shown in the content of a page and should help the user to know that the site is secured [20]. These seals are a content of the page and thus do not provide any real security information. They are misleading for this reason and for their effect on the confusion between browser chrome and page content present in many users, who do not know where a valid security visual clue can be shown [19]. An other caracteristic of the web environment is the irregularity of the appearance of HTTPS clues. Some websites use HTTPS only for a sign-in page and use HTTP everywhere else. Thus, it is usual to visit a page without HTTPS or to see the HTTPS indicators disappear between two pages. The actual situation is one in which the users know only little about security and the practical use of HTTPS make it hard to make good use of the security visual clues.

The user lacks information to control the authentication process. As the browsers accepts certificates silently when they are valid, only a minority of users caring much for security will try to know which CA signed a certificate. A user does not know in general which CA he should trust and will not detect a suspicious CA.

The user who cares much about the security places himself in the same situation as described for a browser : the number of sites he can access is really small and he loses much in terms of usability.

According to [9], a user ignoring certificate warnings gains from this. The user who try to avoid malicious sites will make some effort in the process and try to adapt to the warnings and this is a cost.

The potential gain is to avoid a man-in-the-middle attack, but if the user only adapts to the warnings it is likely that he has a dangerous usage of the sites anyway. For example, accessing the site without typing https:// in the url often means that the user accesses the HTTP site and is then redirected to the HTTPS site. In this case, the attack can occur before the HTTPS site is reached. Worse, as almost none of the phishing sites published on PhishTank use certificates [9] [14], almost every warning is a false positive. Sites using certificates are nearly 100% honest. Ignoring the security warnings completely can be a winning decision in this context. The 'stupid' user is in fact acting as a rational agent.

Table 1: Security incentives for the HTTPS actors

Actor	Security incentives
User	Protect his data
Server	Send a trust message
Browser	Provide good service to the user
Certificate Authority	Reputation loss in case of fail

Table 2: Factors limitating the increase of security

Actor	Limitations
User	Limited control, effort cost
Server	Costs of additional security
Browser	Usability in conflict with security
Certificate Authority	Small consequences of a fail

6. TECHNICAL SOLUTIONS AND ECONOMIC INCENTIVES

Technical and regulatory approaches are currently studied to avoid the problems of the current HTTPS system. A regulation is a possible tool that the users can use collectively to influence the other actors of the process, something that they cannot do individually.

6.1 Technical improvements

Here are presented three improvements currently in use or proposed. These are small changes and they do not address the weakest-link problem of the certificate system.

Google Chrome use a mechanism named Public Key Pinning to authenticate the most visited web sites. This is a whitelist system where the browser stores the keys corresponding to the major servers and the certificates of these servers must correspond to the known keys. It allows the extension of the usability of these sites in the case of a corrupted CA but is only possible for a few web sites. A variant of this certificate pinning is a mechanism in which a server can tell a browser to remenber a given certificate for a given amount of time and that the certificate will not change in this time period. During later connections, the browser can verify that the certificate did not change. Indeed a change of certificate is likely to be the sign of a fraudulous certificate because a server typically change its certificate once in a year.

in [3] a Short-Lived certificate is proposed to make the revocation of certificates easier and avoid certificate revocation lists : a certificate becomes obsolete after a few days and is then invalid if it is not renewed. The expired certificates must be strictly refused for this method to increase the effectiveness of the revocation process.

A strong form of HTTPS was proposed in 2012 to allow the administrator of a web site to set the server as 'HTTPS only'. This is named HSTS for HTTP Strict Transport Security [23]. In this case, the server can only be accessed through HTTPS and any certification problem ends the connection instead of only raising a warning. The client browser remembers that the site should only be accessed by HTTPS and will also raise an error if it tries to use HTTP. This is a good way of making sure that any connection to the server will benefit from the HTTPS security but has a number of drawbacks. The first one is the cost of this system for the server organization. As we saw earlier, many web sites have an implementation of the certicication system that is not perfect, and many warnings are raised due to benign mistakes, like a certificate valid for a domain name but not for a specific subdomain. In the case of HSTS, an imperfect implementation leads to a unusable web site. A second problem is contained in the principle of HSTS: if for some reason the certificate is not valid, even if the web site administrator is not responsible for the failure, the site will not be accessible. This can be a wanted feature to maintain strict security but can hurt the usability.

A complementary approach to reinforce the security of HTTPS is to improve the quality of the information given to the user. In the current system, the security is user-centered [17], meaning that the user has to make the decision to pass through a warning or not. To be efficient, this system needs a clever user. The improvement of the security can be a consequence of the improvement of the visual information provided to the user, as studied in [19].

6.2 The European Regulation

As most of the major Certificate Authorities are under the jurisdiction of the European Union, an EU law can affect the certification system and could be the incentive that is needed to increase the security. The EU Commission proposed in June 2012 such a regulation. The texts is targeted at the Certificate Authorities and does not affect the browsers or the web sites. It places the liability on the CAs for any damage caused by a security problem related to the issued certificates. In [1], it is noted that a small company like DigiNotar could not have survived this liability in many cases as it could be the cause of damage to companies as big as Google : a liability spread along the HTTPS chain depending on the causes of the problem could be a better approach.

The EU proposes to control the security levels of the Certification Authorities and to force them to report incidents and their effects. indeed VeriSign did not reveal the breaches in their security before it was discovered by Reuters two years later. on the other side, the EU proposal does not address the issue of the HTTPS implementation in the websites. The enforcement of the security controls is left to the member states.

This regulation proposal aims to control a number of Certification Authorities in the EU to impact the HTTPS system globally but this does not solve the principal design problem of the CA system. As the fall of any CA in the world means the failure of the entire HTTPS trust mechanism, a local regulation without the removal of this technical issue may fail to address the core of the problem.

7. CONCLUSION

The HTTPS protocol is the widely used mean of authentication of websites and it suffers from important technical flaws. These technical flaws are combined with a situation in which nobody gains clearly by enforcing strict security. Some Certification Authorities are too big to be in danger when they suffer a security breach, the browsers need to guaranty security but it is in conflict with the usability, the companies owning servers have few means to show their security efforts and as a result few reasons to pay for them and the user, who is the most interested in an increase in security, has almost no information or control over the process. There are some efforts to find technical solutions as well as new regulations for web authentication

8. REFERENCES

[1] Hadi Asghari, Michel J.G. van Eeten, Axel M. Arnbak and Nico A.N.M. van Eijk: *Security Economics in the HTTPS Value Chain*, In Proceeding of the Twelfth Workshop on the Economics of Information Security, 2013

[2] Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. (2009, August): *Crying Wolf: An Empirical Study of SSL Warning Effectiveness.* In USENIX Security Symposium (pp. 399-416)

[3] Topalovic, Emin, Brennan Saeta, Lin-Shung Huang, Collin Jackson, and Dan Boneh: *Towards Short-Lived Certificates*, Web 2.0 Security and Privacy (2012).

[4] Jani Suomalainen: *Quantifying the Value of SSL Certification with Web Reputation Metrics*, ICIMP 2012 : The Seventh International Conference on Internet Monitoring and Protection, 2012

[5] Vratonjic, Nevena, Julien Freudiger, Vincent Bindschaedler, and Jean-Pierre Hubaux: *The inconvenient truth about web certificates* In Economics of Information Security and Privacy III, pp. 79-117. Springer New York, 2013.

[6] *Comodo admits two more registration authorities hacked* `http://www.infosecurity-magazine.com/view/16986/comodo-admits-two-more-registration-authorities-hacked`

[7] *Key Internet operator VeriSign hit by hackers* `http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202`

[8] *SSL Pulse page* `https://www.trustworthyinternet.org/ssl-pulse/`

[9] Herley, Cormac. *So long, and no thanks for the externalities: the rational rejection of security advice by users* In Proceedings of the 2009 workshop on New security paradigms workshop, pp. 133-144. ACM, 2009.

[10] *W3Techs Web technology Surveys* `http://w3techs.com/technologies/overview/ssl_certificat`

[11] FUNG, Adonis PH; CHEUNG, K. W: *SSLock: sustaining the trust on entities brought by SSL* In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010. S. 204-213.

[12] Pradeep Kumar Panwar, Devendra Kumar: *Security through SSL*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012

[13] Adams, Anne, and Martina Angela Sasse: *Users are not the enemy* Communications of the ACM 42, no. 12 (1999): 40-46.

[14] *PhishTank page*`http://www.phishtank.com`

[15] *CA/Browser Forum* `https://www.cabforum.org/forum.html`

[16] Ye, Eileen, Yougu Yuan, Sean Smith: *Web spoofing revisited: SSL and beyond*, 2002.

[17] Zurko, Mary Ellen: *User-centered security: Stepping up to the grand challenge.* In Computer Security Applications Conference, 21st Annual, pp. 14-pp. IEEE, 2005.

[18] Friedman, Batya, David Hurley, Daniel C. Howe, Edward Felten, and Helen Nissenbaum. *Users' conceptions of web security: A comparative study.* In CHI'02 extended abstracts on Human factors in computing systems, pp. 746-747. ACM, 2002.

[19] Whalen, Tara, and Kori M. Inkpen. *Gathering evidence: use of visual security cues in web browsers.* In Proceedings of Graphics Interface 2005, pp. 137-144. Canadian Human-Computer Communications Society, 2005.

[20] Stebila, Douglas. *Reinforcing bad behaviour: the misuse of security indicators on popular websites.* In Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction, pp. 248-251. ACM, 2010.

[21] Boehme, Rainer, and Tyler Moore. *The Iterated Weakest Link–A Model of Adaptive Security Investment.* 2009.

[22] Flinn, Scott, and Joanna Lumsden. *User perceptions of privacy and security on the web.* 2005.

[23] Hodges, Jeff, Collin Jackson, and Adam Barth: *Http strict transport security (hsts).* `http://tools.ietf.org/html/draft-ietf-websec-strict-transport-sec-04` 2012.