IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 3 Issue 3 March, 2015

Defending Network Identification for Browsers against web spoofing Attack Technique

Anil Tamrakar, M.Phil(CS)
Research scholar, Dr. C.V. Raman University Bilaspur,kota (C.G.) India, atamrakar21@gmail.com

Dr.K.N Singh, Asst. Professor,
Dr. C.V. Raman University Bilaspur (C.G.), Kota India, knnsingh.ggv@gmail.com

Suraj Prasad keshri, Asst. Professor,
Dr. C.V.Raman University, Kargi road, Bilaspur, Kota (C.G.) India, suraj.softtech11@gmail.com

ABSTRECT: *- The use of standard web securities measure (SSL/TLS), user enter sensitive information such as password into scams website. The scams site cause sub-spatial damage to individual and corporation. In this works, we analyses these attack, then find the often exploit usability failure of browser. We developed and describe Trust Bar, a browsers extension for improve secured identification indicator. User can assigned a name or logo to a secured site, presents by Trust Bar then the browser presents that secured sites otherwise Trust Bar presents to certified sites owner name, and the name or logo of the Certificate Authority (CA) who's identified the owner. Some of this idea is already adopted by browsers, following our work. We describe usability experiment which measured and proved the effectiveness of Trust Bar improved securities and identification indicator. We derive general secure-us abilities principle from our experiment and experience with Trust Bar.*

KEYWORDS: - Cryptanalytic Attack , Security, Internet, SSL/TLS, Phishing Attack.

1. INTRODUCTION

The web is the medium for an increasing amount of business and other sensitive transaction, assume for online banking and brokerage. Virtually all browser and server deployed the SSL and TLS protocol to address concern about securities. The current used of SSL and TLS by browser, still allow web spoofing. There is an alarming increased in the amount of real life web spoofing attack, usually used normal technique. The user of spoofed website, example. Impersonating as financial institution by sends her spoofing emails message that link into the spoofed websites this is often called a phishing attack. The goal of the attacker is often to obtain user ID, passwords and PIN and other personal and financial information's e.g. for identity theft. A study about two million users gave such information to spoofed web site. For example of phishing e-mail message seen the AntiPhishing Working Group phishing archive.Spoofed attack mostly using the phishing technique are significant threat to We investigates spoofed and phishing attack trying to protect naïve as well as expert user. We considered 3(Three) main approached to sites identification indicator Standard-classical indicators: the indicator available in typically current browser consisting mainly of the location (address-URL) bar and of indicator of the activation of SSL/TLS the protocol name https rather than http. Certificate-derived identification indicator. Presenting an identifier (name- logo) for the sites. In current browser the identification is not always done by an entity trusted by the user then we should also identify the entities responsible for includes also a name and logo for the Certificate Authority (CA), responsible for identifying the site. User-customized identifiers allowing user to choose a name and logo for a securely identified site and later presenting this name/logo to identify this (SSL and TLS protected) sites. We implemented the last two approaches in a browsers extension called Trust Bar. We also conducted usability experiment to measure and compared the effective-ness of the three approaches to sites identification indicator. The results confirm the vulnerability of the standard indicator available in current browser and significant improvement in detection of spoofed site when using both of Trust Bar's improved identification indicator especially the user-customized identifier.

2. Web Site Spoofing

The initially designed to Internet and Web protocol assume environment where server, client and router cooperates and follow the standard protocol accepts for unintentional error. The amount and sensitivity of usage increased, concerns about securities fraud and attack. The client and even host connections and addresses, and

use them to launch different attack on the network itself (router and network service like DNS) and on other host and client. The "proliferation" of commercial domain name registrar allowed automated low cost registrations in most top level domain, it is currently very easy for attacker to acquire essential any un allocate domain name and places there malicious host and client. We call this the unallocated domain adversary an adversary who is able to issue and receive messages using many addresses in any domain name excluding the finite list of already allocated domain name. This is probably the most basic and common type of adversary. The SSL or TLS protocols which as we explained in the following subsections securely authenticate website page even in the presence of intercepting adversaries message to and from all domains. Even without SSL and TLS the HTTP protocols securely authenticate web page against domain but receive only message sent to un-allocates domain. However, the securities by SSL and TLS are only with respect to the address (URL's) and securities mechanism (HTTP's, using SSL and TLS, or `plain` HTTP) requester to the applications (usual browsers). The phishing attacks the application specify its request the URL's of the spoofed sites. Namely web spoofing attack focus on the gap between the intention and expectation of the users and the address and securities mechanism specified by the browser to the transport layer.

3. Server Authentication with SSL/TLS

The Secure Socket Layer (SSL) protocol mainly to protect sensitive traffic such as credit card number sending by consumers to web server. Transport Layer Securities (TLS) is the name of an IETF's standard designed to provide SSL function most browser enables We use from here on, the name SSL, but refer also to TLS. We focus on SSL's core functionalities and basic operation. Simplified a bit SSL operations is divided into two phases a hand-shake phases and a data transferred phases. We illustrate this in Figure for connection between a client and an imaginary bank site (http://www.bank.com). During the hand-shake phases the browser confirm that the servers has a domain names certificate singe by a trusted Certificate Authority (CA) authority it to use the domain names www.bank.com contain in the specify website address (URL's).Next browsers choose a random keys k and send to the servers Let EncrytPKserver (k), i.e. the key k encrypted using the public key PKserver. The browser also send MACk(message), i.e. Message Authentication Codes used key k compute over the previous message. This proved to the server that an adversary did not tamper with the message to and from the client. The server returns MACk(message) this prove to the browser that servers was able to decrypt EncrytPKserver(k) and therefore owns PKserver. This concludes the hand-shake phase. The data transferred phase used the established share secret key to authenticate and then encrypt request and response. Again simplified the browser compute

Client's

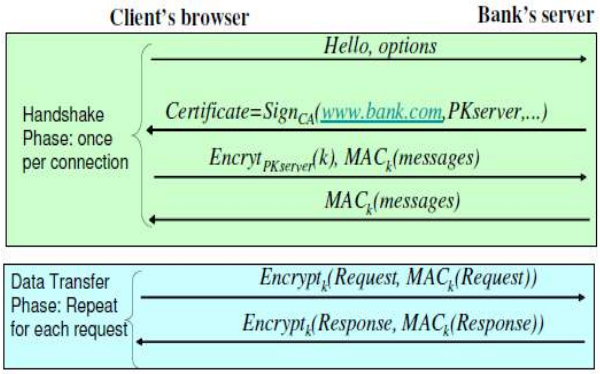


Fig 1: Simplified SSL and TLS Operations

3.1 Servers (domain names) authentications:- SSL confirm that the servers has the private keys which can decrypted message encrypts to client uses public key PKserver. The applications uses SSL e.g. the browses should confirmed that this public keys belong to the "right server". The particular current browser validate that the certificate is valid sign by a trusted certificate authority and contain the domain name of the site (www.bank.com in this example).

3. 2. Confidential and authentications of the traffic between client and servers to uses encrypted and message authentications (MAC's) using the shared secret "master key" established during hand-shake phases. Unfortunately most website page are not protected by SSL. This includes most corporate and government web page and other sensitive website page. The reason of performance the SSL protocols while fairly optimized still consume sub-spatial resource at both servers and clients, includes at least four flows at the beginning of every connection state in the server and computationally-intensive public key cryptographic operation at the beginning of many connection.

4. Website Spoofed and Phishing Attacks

4.1 Tricks to user into requested the spoofed web site in step 1a or into used http rather than https i.e. not protect the requests and responses using SSL.

4.2 Returns an in corrected IP's address for the website servers in step 2b. This can be done by exploiting one

of the known weaknesses of the DNS protocol or many DNS server. A typical example is DNS cache poisoning ("pushing" false domain-to-IP mapping to the cache of DNS server).

4.3 captured the requests in step 3a (sent to the right IP's address) and return a responded in step 3b from the spoofing website.

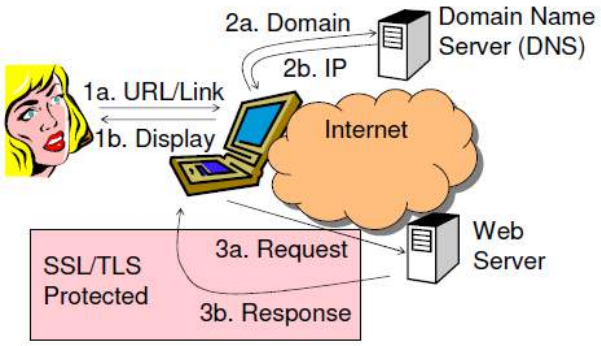


Fig 2: HTTP requested/responses with SSL protection

5. Secure Vs Insecure Site Indication

The Exist browser indicated that a website is SSL-protected by a small SSL status icon usually in the status area at the bottom of the page see Figure 3. This indication is not very visible and off-guard users may not notice its absence when accessed a sensitive website. The most real-life spoofed attack are on website without SSL and TLS protections even in case where the attacker uses domain name which do not appear related to any known trademarks. A website can requesting that the browsers avoid displayed the status area (Generally by using the "window. open" JavaScript's module), making the lack of SSL even harder to notice . To prevent these threat Trust Bar detect that a website is not SSL protects it display a highly visible warning message (see Fig:3 (a), (b)) or icon. We recommend that corporate or other serious website avoid these warning messages by protecting all of their webpage and certainly all of their web form preferably presented the corporate logo in Trust Bar. By protecting all of their page such sites will make it quite likely that their users will quickly notice the warning messages in the trusted browsers area, the user receive a spoofed versions of a web page of such website. This ensures that all the organization web page will present the logo and credentials of the site (and organization) in Trust Bar used and re-enforcing the brand of the organization. A possible concern is that users may be irritated by the Trust Bar warning, which would appear on most web page (since most are unprotected).

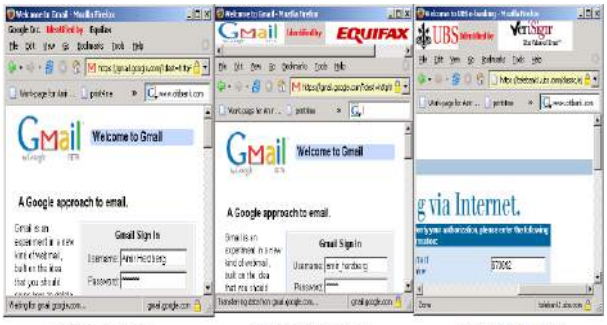
6. Identification of Web Sites and Certification Authority

6.1 Certificate derived identifications:- Name are taken from the "organization name" field of the existing X.509 SSL certificate. Such name is presenting together with the text "Identified by" the names or logos of the Certificate Authorities (CA) which identify this website. The site may provides the logos in an appropriates (public key attributes) certificates extensions. This may be the same as the certificate used for the SSL connection or another certificates (e.g. identified by a <META> tag in the pages). The logos may be sign by entity that focused on validating logo e.g. national and international trademark agencies or by a certificates authority trusted by the user.

6.2 Users customized identifications: The users can identify logos for a site, e.g. by "right-click" on an image of the logos (which usually appear on the same pages). User can also select a text site identifier (a `petname'), presented by Trust Bar to identified the site. Whenever open a page with the same public key, Trust Bar automatic present this logos or petname for the site.

(a) Chase (b) Amazon (c) Passport (d) eBay (e) PayPal

Fig 3: Unprotected Login to Important Sites.



(a) Gmail (text) (b) Gmail (logos) (b) UBS (logos)

Fig 4: Secure sites with logo in Trust Bar

7. User certified Logos Identifications ("Web Trust Bar")

Trust Bar generate upon installation a private signatures key which it used later on to signed logos certificate linking public key and logo if the users specify the used of the logos for the public key. These "user certificate" can be store in a file accessible via the web network so that other instances of Trust Bar belonging to the same users and to other trusted him can automatic used the logo. Trust Bar allow user to specified the location of one's or more repository from which it download logos certificate .Trust Bar allow the users to inputs or approved logos certificate validations key, e.g. of the same user on another machine. These allow a user to certify a logos in one machine (e.g. office) and used to automatically in other machine (e.g. house or cell phone). The users can also inputs or approved logos certificate validations key of logos certifications authority or of other user her trust.

8. Experiments:-

Specifically, our experiments compared fake web site rate for the three web attack approached:

8.1 standard browsers securities identifications indicator:-The locations or URL and SSL-TLS indicator. website identifications indicator are available in typically browser and including the address Bar and the SSL-TLS indicator (The status bar and at the ends of the address bar protocols name "https" in the address bar yellow background). See Fig 5. Certificate derived indicator of organizations and identify-authorities (CA). Identifications of SSL-TLS protected website by displaying of the names and logos of the organizations and the names and logos of the certificate authorities as in Fig 6. This is default identifications of SSL-TLS protected page, user the Trust Bar extension (version 0.4) running in the Firefox browsers. (Version 1.5.0.4). User Customize identifications indicator. Identifications of website by display a users select logos and name for the website (Fig 7). The idea of names assigned was introduces independent by PetName.

Fig 5: Classical browser security and location indicators. These indicators include address bar, status bar. They all considered vulnerable so attackers forge them to build malicious sites.

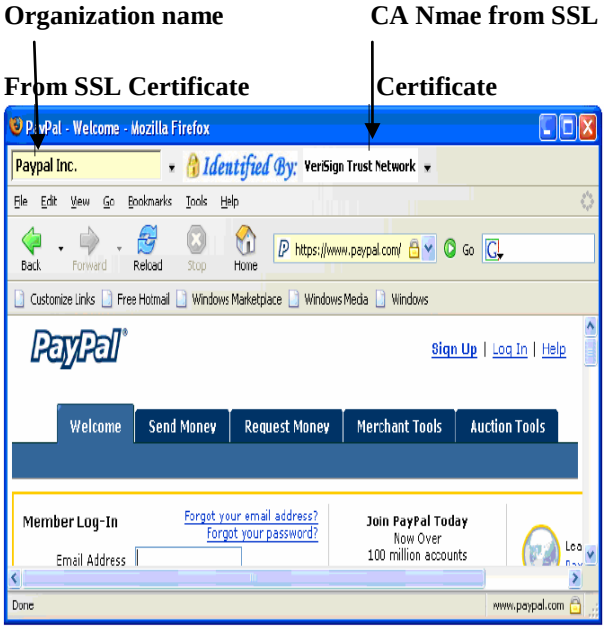


Fig 6: Site identifications by "Paypal Inc" identify by "VeriSign" using Trust bar.

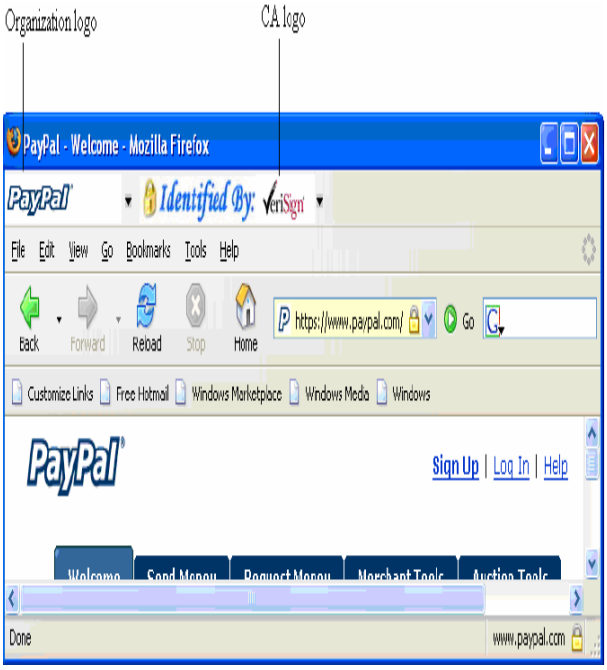


Fig 7: Site identification by "Paypal logos" identify by "VeriSign logos" using Trust bar. The logos of VeriSign presented automatically as VeriSign is widespread well-known CA. Nevertheless user may replace its logo with his/her own

9. Conclusions:-

Website phished and spoofed attacks are infect increasing common. In paper we described browsers with protocols extension that we design implements and tests that will help detect website spoofed attack. The idea is to enhance browser with a mandatory's improve securities identifications indicators. The indicator would be users' customizable, using information's from the certificates by default. Our experiment confirm that improve indicator can significantly improve the detection rate and throughout of user. Notice that while our experiment shown a conclusive advantages and impact of the improve indicator we are not sufficient to actually estimated the expect real life detection rate. Such measurement required a much and more extensive longer terms experiment. Another issue, which we did not test sufficient is the impacts of used graphically indicator (Example:-logo) vs. text indicator. In our experiment it is hard to compared between the two because user were limits in time and motivates to achieve many click, so they preferred to minimally customize the system. We believe that our result and experience justify the addition of improved indicators to new browsers indeed early release of version 7 of the Internet Explorer (IE) browser include a certificate derived indicator which is very similar to what we proposed and implement in Trust Bar. The IEv7 indicators identified the CA and restrict the "certificate derived indicator.

REFERENCES :-

[1] Anti-Phishing Working Group, Phishing Archive, http://www.antiphis.org/phish/archive.

[2] Anti-Phish Work Groups, Phish Attacks Trend Report - March 2009, published April 2009.

[3] Anti-Phishing Working Group, Phishing Activity Trends Report - May 2006.

[4] Virus tries to con PayPal users, BBC News.

[5] Client side catched for TLSS. by B. Donah, Hovavs Shacham,. In proceedings of the Internet Society's 2002 Symposium on Network and Distributed System Security (NDSS), 2008.

[6] Tyler Close, Petname Tool: Enabling web site recognition using the existing SSL infrastructure, presented in W3C Workshop on Transparency and Usability of Web Authentication, March 2006, New York City.

[7] Neil Chou, Robert Ledesma, Yuka Terguchi and John C. Mitchell, Client-Side defense against webbased identity theft, NDSS, Feb. 2006.

[8] The Coordinated Spam Reduction Initiative, Microsoft corporation, February 2006.

[9] Citibank™ corp., Learn About or Report Fraudulent http://www.citibank.com/domain/spoof/report_abuse.htm, April 2009.

[10] Rachna Dhamija. The battle against phishing: Dynamic security skins.

[11] Rachna Dhamija, J.Doug Tygar, and Marti Hearst. Why Phishing Works. Proceedings of the Conference .

