World Journal of Science and Technology 2012, 2(3):30-33
ISSN: 2231 – 2587
Available Online: www.worldjournalofscience.com

Proceedings of *"National Conference on Emerging Trends in Computer Technology (NCETCT-2012)"*
Held at R.C.Patel Institute of Technology, Shirpur, Dist. Dhule, Maharashtra,India.
April 21, 2012

Design of a plug in for a browser against phishing and spoofing attacks

Akanksha Upadhyaya

Department Of Computer Engineering, Lakshmi Narain College Of Technology, Indore, India

Abstract

Recent years have seen a rapid increase in the size of web users. In the same way scam web sites (fraud web sites) and hackers are also increased. Users enter sensitive information such as passwords, their personal and professional information into scam web sites. Such scam sites cause substantial damages to individuals and corporations. In this proposed work, I analyze these attacks, and try to find out how they exploit usability failures of browsers. I n this paper development and description of a security method by which a browser extension improves, using secure identification indicator, is described. A survey on presently available anti phishing toolbars against phishing attacks will be performed. Users can assign a name/logo to a secure site, presented by a tool bar when the browser presents that secure site; otherwise, the Tool bar presents the certified site's owner name, and the name/logo of the Certificate Authority (CA) who identified the owner.In this paper description and development of a usability experiment, which measure, and prove the effectiveness, of security and identification indicators will be done. Trying to derive general secure-usability principles from my experiments and will investigate spoofing and phishing attacks and countermeasures, trying to protect naïve as well as expert users and also perform the survey on the available toolbars in the market.

Keywords: Certificate Authority (CA), SSL/TLS

INTRODUCTION

The web is the medium for an increasing amount of business and other sensitive transactions, for example for online banking and brokerage. Virtually all browsers and servers deploy the SSL/TLS (secure socket layer/transport layer security) protocols to address concerns about security. However, the current usage of SSL/TLS by browsers still allows web spoofing, i.e. misleading users by impersonation or misrepresentation of identity or of credentials. Indeed, there is an alarming increase in the amount of real-life web-spoofing attacks, usually using simple techniques. Often, the swindlers(cheaters) lure the user to the spoofed web site, e.g. impersonating as financial institution, by sending her spoofed e-mail messages that link into the spoofed web-sites; this is often called a phishing attack. The goal of the attackers is often to obtain user-ID's, passwords/PINs and other personal and financial information, and abuse it e.g. for identity theft.There are three main approaches to site identification indicators.

Standard/classical indicators: The indicators available in typical current browsers, consisting mainly of the location (address/ URL) bar, and of indicators of the activation of SSL/TLS (a padlock and the use of the protocol name https rather than http).

Certificate-derived identification indicator: If, as in current browsers, the identification is not always done by an entity trusted by the user (directly or by delegation), then we should also identify the entity responsible for the identification. Namely, in this case the identification indicator includes also a name or logo for the Certificate Authority (CA), responsible for identifying the site.

User-customized identifiers: Allowing users to choose a name or logo for a securely identified site, and later presenting this name/logo to identify this (SSL/TLS protected) site.

Mainly the proposed work concentrates on the attacks named as phishing and spoofing, which are described below :

PHISHING

Phishing is the process by which someone obtains private information through deceptive or illicit means in order to falsely assume another persons identity.

There are many variations on this scheme, its possible to phish for another information in addition to username and password such as credit card number, bank account number, social security number etc. phishing presents direct risk through the use of stolen credentials and indirect risk to institution that conduct business on line through erosion of customer confidence.The process of phishing can be explained by the following figure.1[7].It shows the simplified

*Corresponding Author

Akanksha Upadhyaya
Department Of Computer Engineering, Lakshmi Narain College Of Technology, Indore, India

Tel: +91-8871690768
Email: upadhyayaakanksha@yahoo.com

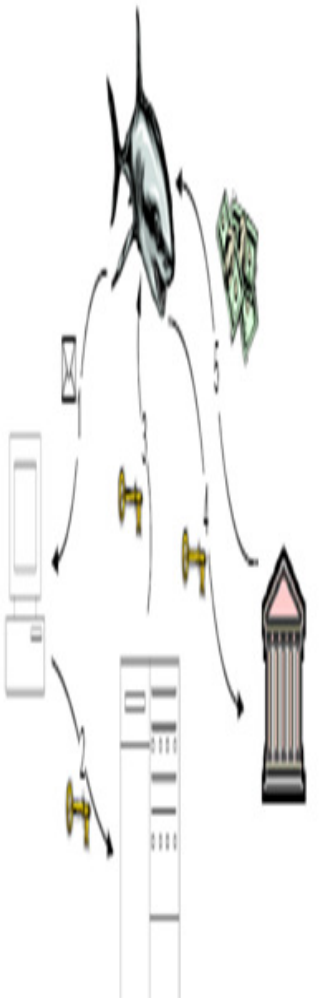

Fig 1. flow of phishing attack in major 5 step

SPOOFING

Spoofing is the creation of TCP/IP packets using somebody else's IP address. Routers use the

1. A deceptive message is sent from the Phishers to the user.
2. A user provides confidential information to a Phishing server (normally after some interaction with the server).
3. The Phishers obtains the confidential information from the server.
4. The confidential information is used to impersonate the user.
5. The Phishers obtains illicit monetary gain.

Steps 3 and 5 are of interest primarily to law enforcement personnel to identify and prosecute Phishers. The discussion of technology countermeasures will center on ways to disrupt steps 1, 2 and 4, as well as related technologies outside the information flow proper.

DAMAGE CAUSED BY PHISHING:-

The damage caused by Phishing ranges from denial of access to e-mail to substantial financial loss. This style of identity theft is becoming more popular, because of the readiness with which unsuspecting people often divulge personal information to Phishers, including credit card numbers, social security numbers, and mothers' maiden names. There are also fears that identity thieves can add such information to the knowledge they gain simply by accessing public records. Once this information is acquired, the Phishers may use a person's details to create fake accounts in a victim's name. They can then ruin the victims' credit, or even deny the victims access to their own accounts. they require technical sophistication, and are sensitive to changes in browsers, operating systems and their configurations. Several of these works also propose solutions, "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. That address is only used by the destination machine when it responds back to the source. A common misconception is that "IP spoofing" can be used to hide your IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth. This is generally not true. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection. However, IP spoofing is an integral part of many network attacks that do not need to see responses (blind spoofing).

PAPER ORGANIZATION

This theory is organized as follows.

SECTION-1: The introduction to the paper is given in Chapter 1. This section describes the objectives, motivation and justification.

SECTION-2: In Chapter 2 reviews numerous existing and emerging technologies that are related to the work presented in this thesis.

SECTION-3/4: In the next section, 3 and 4 will give the implementation of the solution and the suggested approach of solving it.

SECTION-5: In section 5 draws conclusions from the work described in previous chapters and discusses possibilities for future development. Finally, in the last section i.e. Appendix, we have provided the annotated bibliography. This section is an exhaustive list of the journals and research papers referred to during the preparation of the thesis.

LITERATURE REVIEW

Felten et al. first identified the web-spoofing threat in [2]. In this work, as well as follow-up works [1, 3, 4, 6, 2] done prior to the first publication of the current manuscript [4], the focus was on attacks and countermeasures for knowledgeable and wary users. Specifically, the users were expected to correctly and carefully check indications such as the URL (location) of the web site and the security lock (SSL/TLS) indicator. These works showed clever web spoofing attacks, using scripts, Java applets or other `features' and bugs of common browsers, to fool even naive and expert users. These attacks are not easy to deploy, as by disabling (important) browser functionalities, or using enhancements to the browser indicators to make it hard or impossible for the attacker to display spoofed versions of important browser indicators [2, 1]. However, as noted by [3], these proposals rely on users' noticing and

understanding their `signals`, which are (even) more elaborate than the existing location bar and SSL indicator. Therefore, these proposals are unlikely to be of significant value for most (naïve, inattentive) users. In fact, practical web-spoofing attacks deployed so far, rarely if ever use advanced technical means; at the most, they use basic scripts and browser vulnerabilities, e.g. to present fake location bar [2]. Essentially all of the many reported attacks left significant clues for the expert, naive user, such as the lack of use of SSL/TLS (indicated by an open padlock icon, or by the lack of a padlock icon), and/or the use of a URL from a domain not owned by the victim web site. Such attacks are therefore mostly oblivious to the use of countermeasures such as proposed in [3] Still, these simple attacks are very effective [4]. In contrast to the above mentioned (and previous) works, my goal is specifically to provide reasonable, if not complete, protection even for the naïve user and general user. increase in the amount of real-life web-spoofing attacks, usually using simple techniques. Often, the swindlers lure the user to the spoofed web site, e.g. impersonating as financial institution, by sending her spoofed e-mail messages that link into the spoofed web-sites; this is often called a phishing attack. The goal of the attackers is often to obtain user-ID's, passwords/PINs and other personal and financial information, and abuse it e.g. for identity theft. Therefore, the significant improvement in detection of spoofed sites is required. Also in [8] Lorrie carnor, Serge Egelmen, Jason hang described the working procedure of ten popular toolbars available in market. overview of given toolbars is as follows: (fig 3)*Cloud mark ant phishing toolbar* relies on user ratings. when visiting a site, users have the option of reporting the site as good or bad. The toolbar will display the colored icon for each site visited. Next is the *EarthLink toolbar*(fig 4*)*, it appears to rely on a combination of heuristics or ratings, and manual verification. Little information is presented on the earth link website; however, we used the toolbar and observed how it functions. The toolbar allow user to report suspected phishing site, after verification and adding to the black list. The *calling id toolbar*(fig 2) boasts its use of 54 different verification tests in order to determine the legitimacy of a given site.

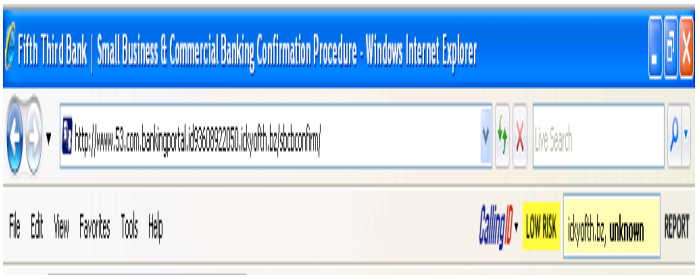

Fig 2. The CallingID Toolbar indicating a low-risk site.

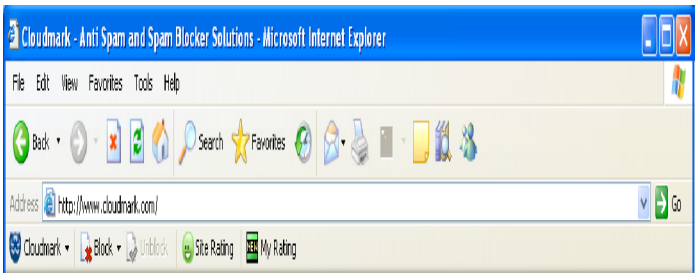

Fig 3. The Cloudmark Anti-Fraud Toolbar indicating a legitimate site

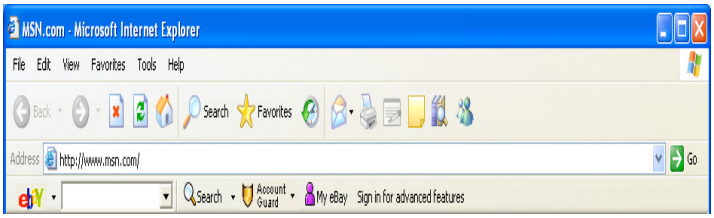

Fig 5. The eBay Toolbar at a site not owned by eBay that is not known to be a phishing site.

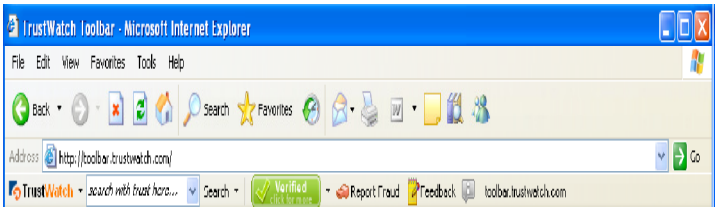

Fig 6. The GeoTrust TrustWatch Toolbar at a verified site.

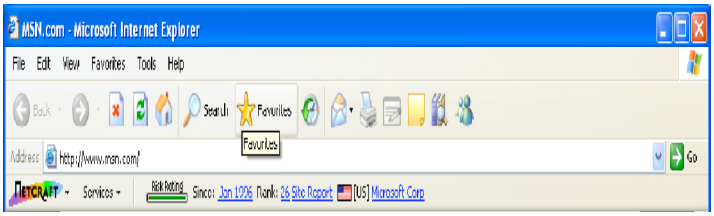

Fig 7. The Netcraft Anti-Phishing Toolbar at a legitimate web site.

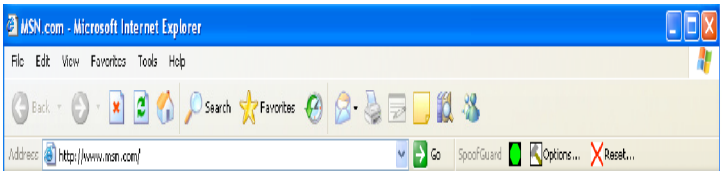

Fig 8. SpoofGuard at a legitimate web site.

Table 1. Comparison of working of toolbars

toolbar	Falsely identified as phishing	unsure
netcraft	0(0%)	0%
spoofguard	218(42%)	256(50%)
Geo trust	0 (0%)	256(50%)
E bay	0%	0%
Earthlink	5(1%)	493(96%)
Cloudmark	5(1%)	493(96%)
Caller id	10(2%)	177(34%)

The *e bay toolbar*(fig5),uses a combination of heuristics and blacklist. The account guard indicator has three modes: green ,red, grey.The icon is displayed with a green background when the user visits a site known to be operated by eBay. The icon is displayed with a red background shows the phishing site. Gray is used for unpredicted site. The geo trust trust watch toolbar, shown in fig 6 ,label site as green(verified as trusted.).Yellow(not verified), or red(verified as fraudulent).*Net craft anti phishing toolbar*, shown in fig 7, uses several methods to determine the legitimacy of a given website. It explains that the toolbar "traps suspicious URLs containing characters which have no common purpose other than to deceive."The spoof guard shown in fig 8, is an anti phishing toolbar developed at phishing toolbar against phishing attacks and make a

comparative study on it. Compare the working of my toolbars against other toolbars.

PROPOSED ARCHITECTURE

The given diagram(fig 9) shows the systems architecture which will be followed during this research, according to system first the information is gathered from the browser's (Firefox and internet Stanford University. This toolbar employs a series of heuristics to identify phishing pages. Table 1 shows the comparison of working of the different toolbar against phishing.

PROBLEM DOMAIN

The current usage of SSL/TLS by browsers, still allows web spoofing, i.e. misleading users by impersonation or misrepresentation of identity or of credentials. Indeed, there is an alarming increase in the amount of real-life web-spoofing attacks, usually using simple techniques. Often, the swindlers lure the user to the spoofed web site, e.g. impersonating as financial institution, by sending her spoofed e-mail messages that link into the spoofed web-sites; this is often called a phishing attack. The goal of the attackers is often to obtain user-ID's, passwords/PINs and other personal and financial information, and abuse it e.g. for identity theft. Therefore, the significant improvement in detection of spoofed sites is required.

SOLUTION DOMAIN

As described in the problem domain, In this paper it is proposed: the solution by the approach of a browser extension i.e. plug in. It also includes usability experiments, to measure and compare the effectiveness of the approach to sites identification indicators, The following work provide the given solutions:

- Provide prevention from the spoofing and phishing done by using URL.
- Allow to open, only the authentic web pages.
- Provides the authenticity rating to the web pages.
- Designs the certificates providing authenticity.
- Maintain the data base according to which authenticity rating will be provided.
- Performing a survey on the available anti.

OBJECTIVE AND EXPECTED OUTCOME

In proposed work I am trying to develop and implement a plug in, a browser extension for improved secure identification indicators. Users can assign a name/logo to a secure site, presented by plug in when the browser presents that secure site; otherwise, Trust Bar presents the certified site's owner name, and the name/logo of the Certificate Authority (CA) who identified the owner. Some of these ideas are already adopted by browsers, following is my work.

- This paper describes usability experiments, which measure, and prove the effectiveness, of plug in improved security and identification indicators. I will try to derive general secure-usability principles from my experiments with plug in. Performing a survey on the available anti phishing toolbar against phishing attacks and explorer) about the web pages then the pruning of the result is performed and if we get some fraudulent result then alarm is generated.

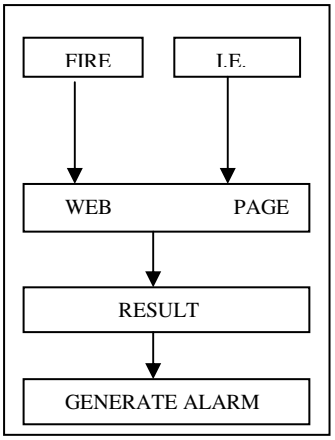

Fig.9: system architecture

CONCLUSION

In this dissertation, I will describe usability experiments, which measure, and prove the effectiveness, of plug in improved security and identification indicators. I will try to derive general secure-usability principles from my experiments with plug in. Performing a survey on the available anti phishing toolbar against phishing attacks and make a comparative study on it.Compare the working of my toolbars against other toolbars.

REFERENCES

[1]. Anti-Phishing Working Group, Phishing Archive, at http://www.antiphishing.org/phishing_archive.html

[2]. Anti-Phishing Working Group, Phishing Attack Trends Report - March 2004, published April 2004, available online at http://www.antiphishing.org/resources.htm

[3]. Anti-Phishing Working Group, Phishing Activity Trends Report - May 2006, available online at http: //www. antiphishing. org/reports/apwg_report_May2006.pdf.

[4]. Virus tries to con PayPal users, BBC News, Wednesday, 19 November, 2003, online at http: //news. bbc.co. uk/2/hi /technology/3281307.stm.

[5]. Citibank™ corp. Learn About or Report Fraudulent E-mails, April 2004, at http:// www. citibank. com/ domain /spoof/ report_abuse.htm.

[6]. Rachna Dhamija, at el, April 2006, "Why Phishing Works." Proceedings of the Conference on Human Factors in Computing Systems (CHI2006), pp. 581-590, Montreal, Quebec, Canada.

[7]. Phishing seminar , at, http://www.google.com

[8]. Lorrie Cranor, et al, November 13, 2006. Phinding phish: an evaluation of anti-phishing toolbar at cylab, Carnegie mellon university, Pittursburg.