A LITERATURE SURVEY ON ANTI-PHISHING BROWSER EXTENSIONS

Oinam Bhopen Singh[1] and Dr. Hitesh Tahbildar[2]

[1] PhD Scholar, School of Engineering and Technology, University of Science and Technology, Meghalaya Ri-Bhoi, Meghalaya-793101, India.
[2] Computer Science Department, H.O.D, Assam Engineering Institute, Guwahati, India

ABSTRACT

Phishing is the fraudulent acquisition of personal information like username, password, credit card information, etc. by tricking an individual into believing that the attacker is a trustworthy entity. It is affecting all the major sector of industry day by day with lots of misuse of user's credentials. So in today online environment we need to protect the data from phishing and safeguard our information, which can be done through anti-phishing tools. Currently there are many freely available anti-phishing browser extensions tools that warns user when they are browsing a suspected phishing site. In this paper we did a literature survey of some of the commonly and popularly used anti-phishing browser extensions by reviewing the existing anti-phishing techniques along with their merits and demerits.

KEYWORDS

Browser extension, Anti-Phishing, Blacklist, Whitelist, Heuristics, etc.

1. INTRODUCTION

With the development of Internet and World Wide Web, our world has become a global village allowing us to interact, educate, buy and sell goods and services at the mere click of the mouse. But along with this we have seen an increase in illegal activities, like phishing, hacking, etc., so cyber crime is now recognized as a major international problem, and phishing specially has become a serious issue for all organization dealing with online e-commerce.[1] Over the last decade phishing attacks have grown considerably on the World Wide Web.

Phishing is a criminal mechanism employing both social engineering element and technical element to steal consumers' personal identity data and financial account credentials. Social engineering element use spoofed e-mails pretending to be from legitimate business organizations and agencies, designed to lead user to fake websites that trick recipients into divulging someone's personal information like usernames and passwords. Technical element involves setting up of websites pretending to be legitimate websites of banks, financial institution, etc., by corrupting local navigational infrastructures to misdirect users to fake websites.[2] It also plants crime ware onto PCs to steal user's personal information directly, by setting up systems to intercept users online account names and passwords.

As reported in the June 2014 phishing trend report of Anti-Phishing Working Group(APWG), the number of phishing websites leaped by 10.7% over the 4th quarter of 2013 and the number of unique phishing websites stands at 125,215.[2] The most targeted industry sector for phishing continues to be the payment service. Every year hundreds of million dollars are lost for entering personal information into Fake web sites by unsuspecting users. To respond to this threats, software vendors and companies with a vested interest in preventing phishing attacks have

DOI:10.5121/ijcses.2015.6402

released a varieties of anti-phishing toolbars.[3] In this paper we have done literature survey on anti-phishing browser extensions. The merits and demerits of each browser extensions along with methods used are listed. Finally, we compare the different browser extension using the criteria of technique used, cost, user friendliness and security algorithm.

We also use some terms like blacklist, white list, heuristic-based, etc in this paper. A blacklist is list which contains URLs of known phishing sites. It is an access control technique that allows access to anything outside the list. If a requested URL is found on a blacklist, the anti-phishing browser extension tool generates a warning indicating the URL to be a phishing site. A white list is a list of websites that are approved and legitimate based on all familiar login user interfaces of websites for a user. Whenever a user tries to login to a particular website, the information of the website will be compared with the one stored in the white list; if the site is not present in a white list, user will be warned for a possible attack. A heuristic-based anti-phishing technique is used to analyse the contents of the webpage to estimate whether a page has some phishing heuristics characteristics. Some common heuristic properties or characteristics are checking the host name, checking the age of the domain name, checking the page rank of the domain and checking against previously seen images. Based on these heuristics characteristics a risk rating percentage is calculated and compared with a small threshold value. If the risk rating percentage is more than the threshold values the website is assumed a phishing page.

2. OVERVIEW OF ANTI-PHISHING BROWSER EXTENSIONS

There are varieties of anti-phishing browser extension available today using different techniques/methods like black list, white list, heuristic or user ratings to identify a fraudulent web site. A few of them are studied below showing the technique used along with their merits and demerits.

2.1. ANTIPHISH

AntiPhish [4] is a browser extension or plug-in tool that keeps track of a user's sensitive information like password and prevents this information from being passed to a website that is not considered safe. The checking is done by the application instead of the users (who are considered as lay man without any experience. Automated form-filler applications have inspired the development of AntiPhish. Most browsers such as the Internet Explorer or Mozilla have integrated common functionality that allows form contents to online banking website to be stored and automatically inserted if the user desires which is protected by a master password. When AntiPhish is installed, a new master password is requested by the browser as soon as the user enters inputs into a form for the first time. The sensitive information is capture and store by the AntiPhish menu after the password is entered. The encryption of the sensitive information is done by the master password before it is stored. The algorithm that is used for encryption and decryption is symmetric DES algorithm. In this implementation of AntiPhish, the user has to tell the browser extension which piece of information available in the page is important and need to be protected from phishing attacks. The AntiPhish menu scan the page once the user enters sensitive information like password. It captures and stores this information as well as a mapping of where its information belongs to.

2.1.1 TECHNIQUE USED

Automated form-filler, master password and symmetric DES algorithm are some of the technique used in AntiPhish

2.1.2 MERITS

AntiPhish can easily mitigate phishing attacks if the user is viewing a pure HTML web page. It helps in controlling the flow of sensitive information. AntiPhish generates warnings whenever user tries to transmit sensitive information of a user to a web site that is considered unsafe.

2.1.3 DEMERITS

AntiPhish required manual interaction to specify the information (only password) on a web site that is considered sensitive. It also generates false alarms if web server addresses or URLs are used instead of domains.

2.1.4 COST

It can be downloaded freely as a Mozilla Firefox plug-in.

2.2. DOMANTIPHISH

DOMAntiPhish [5] leverages the original idea of AntiPhish. This is also a browser extension which use layout similarity based approached. Every time a user successfully logs into a new web site after DOMAntiPhish is installed the browser automatically store the hash of the entered password, using SHA-1, along with the DOM-Tree representation of the web site. And whenever the password is reused, a similarity check is done instead of raising an alert. A phishing attempt is assumed if the current page is similar to the one on which the information has been entered originally and if the pages are different it is assumed that the piece of information is legitimately reused.

2.2.1 TECHNIQUE USED

Layout similarity approached is used by comparing DOM-Tree representation.

2.2.2 MERITS

User's interaction is not required; the browser automatically stores the hash of the entered password. Whenever a password is reused it does not immediately sound an alert, but a similarity check is done.

2.2.3 DEMERITS

Spoofed web page can be created by combining images that looks visually similar to a legitimate web page. The DOM of the spoofed web page could be different and detection would be evaded.

2.2.4 COST

The prototype is implementable.

2.3 DYNAMIC SECURITY SKIN

Dynamic Security Skin [6] is a browser extension for Mozilla Firefox, allowing a user to verify a remote web server easily and hard for an attacker to spoof. First, the browser extension provides the user with a trusted password window where the users enter usernames and passwords and the browser display security information. A photographic image is required to be recognized for establishing a secure path between the user and this window. The second technique provides a user to differentiate between a fake website and a secure or authenticated website. Here, for each transaction and user the remote server generates an abstract image that is unique. This image is used to create a skin, customizing the appearance of the server's web page. The browser computes the image that is received from the server and display it in the user's trusted window. Now the user can visually verify that the images match to authenticate the content from the server.

2.3.1 TECHNIQUE USED

A verifier-based protocol known as Secure Remote Password Protocol (SRP), is used for mutual authentication of the user and the server. And the skin is generated by Server-generated random Images.

2.3.2 MERITS

The user need to recognize and remember only one image and one low entropy password, to authenticate himself/herself, while interacting with the server any number of time. Authenticating content from a server require user to perform only one visual matching operation to compare two images.

2.3.3 DEMERITS

Some demerits can be leak of the verifier, leak of the images, spoofing the trusted window and spoofing the visual hashes.

2.3.4 COST

It can be freely downloaded.

2.4 EBAY'S ACCOUNTGUARD TOOLBAR

The eBay's AccountGuard [7] toolbar is a browser extension provided to its customers for keeping track of auction sites. AccountGuard monitors the web pages visited by users and give a warning in the form of colour tab. The colour tab is usually grey, but if the user is on an eBay or PayPal site it will turn green and red if the site is known to be a spoof by eBay.

2.4.1 TECHNIQUE USED

It is based on a combination of heuristics and blacklists.

2.4.2 MERITS

One merit of eBay toolbar is it allows users to submit suspected spoof site to eBay which will be added in the blacklist after verification.

2.4.3 DEMERITS

Some demerits of this browser toolbar are that it is applicable only to eBay and PayPal websites. Denial of service attacks is possible.

2.4.4 COST

The eBay toolbar runs with internet explorer and is available free to user.

2.5 GOLDPHISH

GoldPhish [8] is a browser extension tool that use content based anti-phishing approached and uses Google as its search engine. This mechanism gives higher ranks to well established web sites. The basis for content based anti-phishing approach is that phishing pages are not active for long period of time and therefore acquiring low rank while searching. Three major steps are used in the design approach. The first step is to capture an image of the current website in the user's web browser. In the second step, for converting the captured image into computer readable text, the technique of optical character recognition is used. In the third step, the converted text is entered into a search engine to retrieve results and analyses the page rank.

2.5.1 TECHNIQUE USED

It is based on content based anti-phishing approached.

2.5.2 MERITS

False positive are not resulted and provides zero day phishing.

2.5.3 DEMERITS

Some demerits of GoldPhish are it delays the rendering of a webpage. Google's PageRank algorithm and Google's search service are vulnerable to attacks.

2.6 ITRUSTPAGE

The iTrustPage [9] is a browser extension tool that does not rely on automation to detect phishing. It relies on user input to check the legitimacy of a web site and prevents from entering any data into suspicious web form.

The browser extension intercepts the user input and prompts the user for search terms that describe the Web page the user intend to visit. With these search terms, iTrustPage performs a Google search and validates the web form only if it appears among the top search results. If the suspicious web form does not appear in the top search results, iTrustPage presents visual previews of those pages that do appear in the top search result, and asks the user whether any of them visually match the current form. If a match is found, the current form is likely to be a phishing attack.

2.6.1 TECHNIQUE USED

It is based on spam filters and blacklists.

2.6.2 MERITS

Some merits of iTrustPage are that it is effective and easy to use. False negatives and false positive associated with automatic phishing detection is avoided.

2.6.3 DEMERITS

Spam filters are not perfect. Phishing pages must be discovered and quickly added to blacklists. It is believe that blacklists and spam filters will have only a temporary and marginal effect on the prevalence of phishing attacks.

2.6.4 COST

iTrustPage is a downloadable extension to Firefox free for users.

2.7 LINKGUARD

LinkGuard [10] is a tool that use character based anti-phishing approach. The technique used by LinkGuard for detecting phishing sites is to extract the DNS names from the visual and actual link and then compares them. If these names are not the same, then it is phishing of category 1. Possibly phishing attack of category 2 directly use dotted decimal IP address in actual DNS. If the actual link or the visual link is encoded then possible phishing attack of category 3 and 4, hence first the link is decode and then analysed. When there is no destination information in the visual link then the hyperlink is analysed. During analysis DNS name is searched in blacklist and whitelist, if it is present in whitelist then it is sure that the link is genuine and if link is present in blacklist then it is sure that link is phished one. If the search result is not found in either white list or blacklist, LinkGuard conducts pattern matching to detect phishing pages.

2.7.1 TECHNIQUE USED

It is based on character based antiphishing technique, blacklists, whitelists and pattern matching.

2.7.2 MERITS

It detects known as well as unknown attacks. Experiments proof that LinkGuard, can detect up to 96% unknown phishing attacks in real-time. False positive or false negatives are not there for phishing attacks of category 1. LinkGuard handles categories 3 and 4 correctly.

2.7.3 DEMERITS

Phishing attack of category 2 may result in false positives, as use of dotted decimal IP addresses is desirable in some special circumstances instead of domain names.

2.8 MICROSOFT SMARTSCREEN FILTER

Microsoft SmartScreen Filter [11] is a plug-in tool design for Internet Explorer 9 (IE9) users. The approach used for identify a page is phishing or legitimate is through blacklist and heuristics method. When a user visits a page, the contents of the page are compared against heuristic characteristics. A yellow shield will appear to warn the user if the page fails to pass the heuristic test, and will advice the user not to enter any important data. However, if no suspicious properties are found, the tool will check its URL against a blacklist. A red shield will appear if a match is found in the blacklist and inform the user about it. It is then up to the users whether they want to proceed or cancel the page. Users can also report to Microsoft about new fraudulent URLs using SmartScreen reporting feature. SmartScreen blacklist verifies URLs before adding them to the blacklist.

2.8.1 TECHNIQUE USED

SmartScreen uses blacklist and heuristic analysis.

2.8.2 MERITS

SmartScreen provides additional security in a network as it allows the administrator to set up a group policy which restricts users from ignoring warning shown by SmartScreen Filter. It also provides protection against downloadable malicious files like key-loggers.

2.8.3 DEMERITS

Blacklist needs to be updated regularly and users will be vulnerable to newly created phishing websites.

2.8.4 COST

It can be downloaded as toolbar for Internet Explorer 9.

2.9 NETCRAFT

Netcraft [12] is an anti-phishing browser extension which displays information about the site, including the domain's registration dates, hosting country, and popularity among other toolbar users. Since phishing sites are hosted for a short period of time compared to the legitimate sites they imitate, so the above information are helpful in detecting phishing sites. The Netcraft web site explains that the toolbar "traps suspicious URLs containing characters which have no common purpose other than to deceive", "enforce display of browser navigation controls in all windows, to defend against popup windows which attempt to hide navigational controls". Netcraft have a anti-phishing community who are giant neighbourhood watch group, empowering the most expert and alert members to defend everyone within the community against attacks. Once the first recipients of a phishing mail have reported the target URL, it is blocked for community members as they subsequently access the URL.

2.9.1 TECHNIQUE USED

It uses several methods to determine the legitimacy of given web site. Some of them are sniffing technique, blacklist, as well as heuristic methods and also depend on user's ratings.

2.9.2 MERITS

Netcraft have several merits. Some of them are it allows phishing site feed, hosting phishing alerts, SSL CA phishing alerts, phishing site takedown, map of current phishing attacks.

2.9.3 DEMERITS

Users can override the warning displayed by Netcraft. And some of the critical information like site rank, primary language, netblock owner, IP address, operating system, web server, and when the server was last changed provided by Netcraft are very useful to potential attackers.

2.9.4 COST

Netcraft anti-phishing toolbar can be downloaded free and runs on Firefox 1.0 and on Microsoft Internet Explorer.

2.10 PASSPET

Passpet [13] appears as a toolbar button next to a text field in the browser toolbar. The text and image on the toolbar button are the name and icon of Passpet's persona. It improves the security and convenience of website logins through a combination of several previously used techniques. The user is asked to input a master address in the form username@hostname, where hostname identifies a Passpet server. A set of animal icons with a random name is chosen automatically which forms Passpet's persona for interacting with the user. Then the user chooses a master secret. When the browser starts, the user has to click the Passpet's persona to wake up the persona which was initially sleeping and enters the master secret. The user clicks the Passpet button to fill in a password. The password is filled in on the website when the Passpet text field flashes.

2.10.1 TECHNIQUE USED

It uses a combination of several techniques like password hashing, petnames, password strengthening, and UI customization.

2.10.2 MERITS

Passpet allows the user to change passwords for individual sites and improves the convenience of logging in to websites. It also allows the user to log in from more than one computer and have to memorize only one secret.

2.10.3 DEMERITS

Some of the demerits of Passpet are attacks on DNS ("pharming attacks") can hijack connections to non-SSL sites and steal their site password. Like all password-hashing systems, Passpet is vulnerable to an offline dictionary attack against

2.10.4 COST

Passpet tool can be downloaded as a Firefox extension.

2.11 PHISHNET

PhishNet [14] is an anti-phishing browser extension which improves the efficiency and resilience of blacklists. It comprises of two major components- URL prediction component and an approximate URL matching component. The first component works in an offline fashion, which generates systematically new URLs by examining current blacklists and by employing various heuristics. It also checks whether the new URLs generated are indeed malicious or not with the help of content matching techniques and DNS queries in an automated fashion. The second component performs an approximate match of a new URL with the existing blacklist by using novel data structures to perform approximate matches with an incoming URL based on hash maps and regular expressions to catch semantic and syntactic variations.

2.11.1 TECHNIQUE USED

It uses technique like blacklists, heuristics and approximate matching algorithm.

2.11.2 MERITS

New sources of maliciousness can be discovered in and around the original blacklist entries and also add them to the blacklist, significantly increasing its resilience to evasion. It can deviate from the exact URL match of a blacklist to an approximate URL match.

2.11.3 DEMERITS

PhishNet suffers from low false positives and exhaustively identifying new heuristics and evaluating their efficiency is a problem.

2.11.4 COST

Only the beta version is released.

2.12 PHISHPROOF

PhishProof [15] is an anti-phishing browser extension tool designed to help Firefox users distinguish between legitimate and phishing websites. PhishProof is easy to use because the users are notified immediately via an alert message when the system evaluates a website as a phishing website. PhishProof can run on any system having Firefox (version 12 and later). After the PhishProof toolbar is installed on Firefox, a toolbar appears on the main browser window. The toolbar has two states, idle and active. When a browser or a new tab is opened, no page is loaded in the browser window, the PhishProof toolbar is in idle state, which contains a menu button with PhishProof logo. The PhishProof toolbar become active when a page is loaded in the browser window. PhishProof's active state has four components: PhishProof menu button, Risk rating bar, since label and country label. PhishProof's menu button contains menu items that redirect users to the PhishProof website. The risk rating bar shows the risk rating percentage for current page calculated by the PhishProof toolbar. The toolbar uses red colour to show risk percentage, whereas green colour is used to display rest of the bar. The risk rating bar also displays the value of risk rating percentage calculated. The "since label" displays the registration date of current page in the browser window. This is used to compute age of the website. The "country label" displays country initials and the flag of country hosting webpage in the browser window.

2.12.1 TECHNIQUE USED

PhishProof use a combination of blacklist and heuristic methods.

2.12.2 MERITS

Some of the merits of PhishProof are it does not require users input. If phishing is detected alert message is immediately notified to the user. Users can also report spoofed site to PhishProof website. It can identify website with short life time. PhishProof use three level of protection

2.12.3 DEMERITS

PhishProof cannot protect from malware. It is not included in a tab browser.

2.12.4 COST

PhishProof can be downloaded a Firefox toolbar.

2.13 PWDHASH

PwdHash [16] is an anti-phishing browser extension that produces different password for each website, defending against password phishing and other attacks by improving web password security. It applies a combination of the plaintext password entered by the user with a cryptographic hash function. Basically, the password hashing method is extremely simple; instead of sending the user's cleartext password, a hash value *hash (pwd, dom)* derived from the user's password, *pwd,* and the site domain name, *dom* is sent to a remote site. The *dom* is referred as the salt. A Pseudo Random Function keyed by the password is used to implement the *hash*. The resulting hash password is normally handled at the server as the hash output is tailored to meet the server password requirement. This deters from stealing password as the password received at a phishing website is not useful at any other websites. So for the same reason passwords gathered by cracking into a low security website are not useful anywhere, thus protecting financial institutions from sites with not enough security. When implementing PwdHash prototype as an extension of Mozilla Firefox it add a lock icon to the password fields to indicate when protection is enabled, rather than a new toolbar with a password "traffic light".

2.13.1 TECHNIQUE USED

The main technique used in PwdHash is cryptographic hash function.

2.13.2 MERITS

Different passwords are produced for each site which deters password stealing as these passwords is not useful at any other domain.

2.13.3 DEMERITS

User passwords cannot be protected from keyloggers, spyware and other software that is installed on the local machine. It does not defend against phishing attacks that use general web cache poisoning attacks and HTTP response splitting.

2.13.4 COST

We can download from PwdHash website the source code and the extension of PwdHash:
http://crypto.stanford.edu/PwdHash

2.14 SPOOFGUARD

SpoofGuard [17] is a browser helper object or plug-in of Internet Explorer. It uses domain name, image, link and URL check to evaluate that a given webpage is part of a spoof attack. SpoofGuard uses three additional files stored in the user profile directory; one is the host names of email site such as Hotmail or Yahoo! Mail used in the referring page check. The other two files are the file of hashed image history and the file of hashed password history.

SpoofGuard monitors the Internet activity of a user and compute a spoof index. If the index exceeds a level selected by the user then it warns the user. This index is translated into a traffic light: green for low index, indicating the page is probably safe; yellow for index in the middle; and red for spoof index above a threshold, indicating the page is probably hostile.

2.14.1 TECHNIQUE USED

SpoofGuard use several heuristics methods and also use PwdHash for password hash function.

2.14.2 MERITS

SpoofGuard image check and outgoing password check are important strengths, since together these checks stop outgoing data. There is no performance degradation as a result of SpoofGuard.

2.14.3 DEMERITS

There are occasionally spurious yellow lights while browsing. It triggers a false post warning when we use a legitimate site for the first time and enters user name and password.

2.14.4 COST

SpoofGuard can be downloaded as a plug-in of Internet Explorer free for public uses.

2.15 SPOOFSTICK

SpoofStick [18] is a simple browser extension that helps users detects spoofed (fake) websites. Since the most relevant domain information is displayed prominently it is easier to spot a spoofed website. For example if a user is visiting Microsoft, the toolbar will display “You are on Microsoft.com”. If the user is at a spoofed website, the toolbar might instead display “You are on

11.19.32.4”. If rogue website has a domain name which is semantically or syntactically similar to a legitimate site then SpoofStick extension can help users to detect an attack.

2.15.1 TECHNIQUE USED

URL check. Converts IP Address to DNS Address.

2.15.2 MERITS

Users are allowed to customize the appearance of the toolbar so the general purpose graphics property is address by SpoofStick.

2.15.3 DEMERITS

Clever use of frames can fool SpoofStick when different sites are opened in multiple frames in the browser window. The website is not in English.

2.15.4 COST

SpoofStick can be downloaded as a toolbar for Internet Explorer and Firefox free for public uses.

2.16 TRUSTBAR

TrustBar [19] is a browser extension with improve secure identification indicators. The secure site presented by TrustBar can be assigned a name/logo by the user; otherwise, the Certificate Authority (CA) name/logo is presented by TrustBar to identify the owner. The goal of TrustBar is establishing securely the identity of the web site by presenting highly visible and graphical interface. This browser extension runs on open-source Mozilla and Firefox browser. TrustBar controls a significant area large enough to contain highly visible logos and other graphical icons for credentials at the top of every browser window. It must appear in every window of the browser, protected or unprotected, including windows used for helper applications and applets.

2.16.1 TECHNIQUE USED

TrustBar is based on certificate-derived identification indicator and user-customized identifiers.

2.16.2 MERITS

TrustBar identifies, by default, both site and the certificate authority which identifies the site. A ‘Hey’ security indicator can be click to report a site that is suspected to be fraud.

2.16.3 DEMERITS

It is not able to compare the impact of using graphical indicator and textual indicators. Unauthorized transaction can be created by viruses and other malicious software due to operating system vulnerabilities.

2.16.4 COST

It can be downloaded as Mozilla Firefox toolbar.

2.17 TRUSTWATCH

TrustWatch [20] is a domain verification toolbar and search site developed by GeoTrust. It help consumers to verify the identity and check security standards by displaying information of web sites that are conducting e-business or requesting confidential information. It is implemented using Internet Explorer which contains an optional pop-up blocker. Suspicious sites can also be reported through the link provided by TrustWatch. These names will examined and shared with other organizations that monitor fraudulent activity. The TrustWatch toolbar instantly display several key factors that should be used to evaluate the trustworthiness of a web site that is requesting confidential information. TrustWatch display a green, yellow or red light for web site verification rating. A green light is displayed to user when a website is safe for exchange of user's sensitive data because the site has been verified by a recognized Certificate Authority (such as GeoTrust or VeriSign) and has a valid SSL certificate installed. A red warning light or a yellow light will appear if a website is not verified or fraudulent.

2.17.1 TECHNIQUE USED

TrustWatch use blacklist method.

2.17.2 MERITS

Easy to use free tool. Toolbar provide optional pop-up blocker with link to report suspicious sites. It also provides personal security ID to prevent toolbar spoofing.

2.17.3 DEMERITS

Until the newly developed phished URL get entered into the black listed database there is high chance of users falling prey into it.

2.17.4 COST

TrustWatch is free and available for download from www.trustwatch.com.

2.18 VIRTUAL BROWSER EXTENSION (VBEX)

Virtual browser extension [1] is a web browser plug-in, which checks for the authoritative NS and verifies the same for a requested website. VBEx comes with individual whitelist for the user depending upon the sites selected or registered with Virtual Browser. Registered user can download the plug-in multiple times in different computers depending upon their requirement. VBEx searches for the authoritative name server responsible for the domain and queries for the IP address for the domain, thus it prevents any kind of misuse of DNS entries on the host files of the local computer or on the local DNS server. In addition, it also maintains a white list of websites that engage in online financial transactions for which the default protocol should be HTTPS, failing which it will prevent the web browser from loading the requested website.

2.18.1 TECHNIQUE USED

Virtual browser extension uses a hybrid method which is the combination of restriction lists or Blacklist (including manual reporting, link analysis, honey pots, and web crawlers), heuristic and visual similarity based.

2.18.2 MERITS

The default protocol is HTTPS, failing which it prevents the web browser to load the requested web site. If the site is not present in white list; the user will be warned for a possible attack and a block page is displayed.

2.18.3 DEMERITS

VBEx cannot protect users against key-loggers and screen-grabbers and client-side scripting attack.

2.18.4 COST

The virtual browser extension can be downloaded as a Firefox plug-in after user authentication.

2.19 WEB OF TRUST

Web of Trust [21] is a toolbar powered by the ratings of websites by users who have rated millions of websites based on their experiences. Each user's rating behaviour is tracked by the system before deciding how much it trusts the user to keep the ratings more reliable. WOT simply shows web site reputations as traffic lights (colour coded symbols) next to search results: red indicates potential danger, yellow warns you to be cautious and green indicates that the website is trusted. A gray symbol with a question mark means not enough ratings to calculate from.

2.19.1 TECHNIQUE USED

The technique used by WOT for collecting ratings and reviews from users is based on a unique crowdsourcing approach.

2.19.2 MERITS

Website reputation as traffic lights is shown next to search results. And by clicking on the traffic light icon will give information about a website's reputation and other user's opinions.

2.19.3 DEMERITS

A single rating from a single person can mark a site as unsafe, even if there is no useful information about that rating.

2.19.4 COST

WOT can be downloaded as a Firefox add-on.

3. DISCUSSION AND COMPARISON

The main benefit of this paper is to learn different anti-phishing browser extensions along with their different criteria and one can decide the appropriate browser extension that will be useful for their work. So some of the security algorithms used are discussed below and the comparisons of the various anti-phishing browser extension are shown in the table.

3.1 SYMMETRIC DES ALGORITHM

DES is a symmetric block cipher, operating on 64-bit blocks using a 56-bit key. DES encrypts data in blocks of 64 bits.[22] The input to the algorithm is a 64-bit block of plaintext and the output from the algorithm is a 64-bit block of ciphertext after 16 rounds of operations. The key length is 56 bits by stripping off the 8 parity bits, ignoring every eight bit from the given 64-bit key. The basic building block of DES is a suitable combination of permutation and substitution on the plaintext block (16 times).

3.2 SECURE HASH ALGORITHM(SHA-1)

When a message of any length of less than 264 bits is input, the SHA-1 produces a 160-bit output called a message digest (or a hash code). The message digest can then be input to the Digital Signature Algorithm, which generates or verifies the signature for the message. Signing the message rather than the message often improves the efficiency of the process because the message digest is usually much smaller than the message.[22] The SHA-1 is secure because it is computationally impossible to find a message which corresponds to a given message digest or to find two different messages which produce the same message digest.

Table 1: Comparisons of different Anti-Phishing Browser Extensions.

Sl.No	Anti-Phishing Browser extensions	Technique used	Security Algorithm	User friendliness	Cost
1	AntiPhish	• Automatic form filler • Master password	Symmetric DES algorithm	User interaction required	Can download free.
2	DOMAntiPhish	• Based on layout similarity of WebPages	Secure Hash Algoritm-1	Automatic	Prototype only
3	Dynamic Security Skin	• Secure Remote Password Protocol • Server generated random Image	Hash function	Visual Matching is required	Can download free.
4	eBay's AccountGuard	• Combination of heuristics and blacklists	-	User color tab on toolbar	Available free to user
5	GoldPhish	• Using Image for Content based anti-phishing approached	Google's PageRank Algorithm	Easy to use	Conference paper
6	iTrustPage	• Based on spam filters . • Use blacklists. • Uses whitelist	PageRank Algorithm	User input is required	Can download free.
7	LinkGuard	• Uses character based anti-phishing technique, • Uses blacklists, • Uses	LinkGuard Algorithm	Easy to use	Conference paper

		whitelists • Uses pattern matching.			
8	Microsoft SmartScreen Filter	• Uses blacklist • Heuristic analysis.	-	User friendly displays color shield	Can download free.
9	Netcraft	• Uses sniffing technique • Blacklist, • Heuristic methods • User's ratings.	Secure Hash Algorithm	Very user friendly	Available free to user
10	Passpet	• Master password • Password strengthening, • UI customization.	Password Hashing Algorithm	Just click the icon	Can be download free.
11	PhishNet	• Blacklists • Heuristics	Approximate matching algorithm.	Easy to use	Only beta version
12	PhishProof	• Blacklist • Whitelist • Heuristic	Symmetric key Algorithm for SSL	Does not require user input	Can be download free
13	PwdHash	• Cryptographic hash function.	Cryptographic Hash Algorithm	Easy to use	Available free to user
14	SpoofGuard	• Uses Heuristics methods • Use PwdHash for password hash function.	Password Hashing Algorithm	Easily identifiable color icon is used	Available free to user
15	SpoofStick	• URL Check	--	Very user friendly	Available free to download

16	TrustBar	• Uses certificate-derived identification indicator • User-customized identifiers.	Encryption Algorithm	User friendly	Can download for free.
17	TrustWatch	• Use blacklist method	Cryptographic Algorithms	User friendly	Can download for free.
18	Virtual Browser Extension	• Uses hybrid method which is the combination of restriction lists, heuristic and visual similarity based.	Cryptographic Algorithms	Very user friendly	Free
19	Web of Trust	• A unique crowdsourcing approach that collects ratings and reviews from users.	-	Traffic light is used	Can download for free.

4. CONCLUSIONS

From the toolbars examined in these studies, we have found that most of them use methods like blacklist, whitelist, heuristics, and automated form-filler using master password, layout similarity, users rating or a combination of these methods. Most of these browser extensions toolbars give warning using color indicator or prevent them from loading if found in the blacklist. So there is a need to frequently update the blacklist in order to successfully prevent users from being deceived. And except for few toolbars most of them have not upgraded their browser extension which ultimately will be of no use. So, there is need for much more effective technique and also a need to educate the users about the risk and awareness of phishing.

REFERENCES

[1] Purkait S, “Preventing Phishing Attacks with Virtual Browser Extension”, The IUP Journal of Information Technology, Vol. IX, No. 3, pp. 7-30, September 2013.

[2] APWG, “Phishing Activities Trend Reports 1st quarter 2014. Accessed on 19th July 2014. http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf

[3] Lorrie Cranor, Serge Egelman, Jason Hong, and Yue Zhang, “Phinding Phish: An Evaluation of Anti-Phishing Toolbars” Carnegie Mellon University.

[4] Kirda E and Kruegal C, "Protecting Users Against Phishing Attacks with AntiPhish", Proceedings of the 29th Annual International conference on Computer software and Applications, COMPSAC 2005, pp. 517-524, Edenburgh, Scotland, 2005.

[5] Angelo P.E. Rosiello, Engin Kirda, Christoper Kruegel and Fabrizio Ferrandi, "A Layout-Similarity-Based Approach for Detecting Phishing Pages", Secure Systems Lab, Technical University Vienna.

[6] Rachna Dhamija and J.D. Tygar, "The battle against phishing: Dynamic Security Skins". Proceedings of 2005 ACM Symposium on Usable Security and Privacy, pp 77-88,bACM Press, July 2005.

[7] eBay Toolbar and Account Guard, Accessed 20th July 2014. http://pages.ebay.in/help/account/toolbar-account-guard.html.

[8] Metthew Dunlop, Stephen Groat, and David Shelly "GoldPhish: Using Images for Content-Based Phishing Analysis", in proceedings of Internet monitoring and protection, 5th International conference, Barcelona, pp 123-128, 2010.

[9] Ronda T, Saroiu S and Wolman A, "iTrustPage: A User-Assisted Anti-Phishing Tool", Proceedings of the 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems, pp.261-272, 2008.

[10] Juan Chen, Chuanxiong Guo, "Online Detection and Prevention of Phishing Attacks" in proceedings of Communicational and Networking in China, 1st International conference, Beijing, pp1-7, 2007.

[11] Microsoft SmartScreen Filter. Accessed 20th July 2014. http://windows.microsoft.com/en-in/internet-explorer/products/ie-9/features/smartscreen-filter.

[12] Netcraft extension accessed 18th July, 2014. http://toolbar.netcraft.com

[13] Ka-Ping Yee, Kragen Sitaker, "Passpet: Convenient Password Management and Phishing Protection". Symposium on Usable Privacy and security, July 12 – 14, 2006, Pittsburgh, USA.

[14] Pawan Prakash, Manish Kumar, Ramana Rao Kompella, Minaxi Gupta, "PhishNet: Predictive Blacklisting to Detect Phishing Attacks", Purdue University, Indiana University.

[15] Taimoor Zahid, "An Anti-Phishing tool: Phishproof", A dissertation submitted to the University of Manchester for the degree of Master of Science in the faculty of Engineering and Physical science, 2012.

[16] Ross B, Jackson C, Miyaki N *el al.* "Stronger Password Authentication Using Browser Extensions". Proceedings of USENIX Security Symposium, pp. 17-32, 2005.

[17] Chou N, Ledesma R, Teraguchi Y and Mitchell J C, Client –side Defense against web-based identity theft. Proceedings of 11th annual Network and Distributed System Security Symposium, California, USA, 2004.

[18] Spoofstick: A great tool to know you are on a fake web site, accessed 18th July, 2014. http://www.scambusters.org/spoofstick.html

[19] Herzberg A and Jbara A, "Security and Identification Indicators for Browsers Against Spoofing and Phishing Attacks", ACM *Transactions on Internet Technology*, Vol. 8, No. 4, Article 16, pp.1-36, 2008.

[20] TrustWatch accessed 18th July,2014. https://www.trustico.co.in/material/DS_TrustWatch.pdf

[21] Web of Trust add-on. Accessed on 17th August 2014. https://mywot.com/en/aboutus.

[22] Man Young Rhee, "Internet security, Cryptographic principles, algorithm and protocol" Wiley publication pp 57-73, 2003.

Authors

O Bhopen Singh Received his B.Sc. in 1994 from Panjab University Chandigarh and MCA degree from Manipur University, Imphal in 2001. Presently he is doing Ph.D and his current research interest is authentication and securing e-government websites from phishing and web spoofing. He is currently working as Sr. Lecturer at ICFAI University, Nagaland, INDIA.

Dr.H.Tahbildar Received his B.E. degree in Computer Science and Engineering from Jorhat Engineering College, Dibrugarh University in 1993 and M. Tech degree in Computer and Information Technology from Indian Institute of Technology, Kharagpur in 2000. He received his Ph.D in Computer Science and Application in 2012 from Gauhati University and his current research interests are Automated Software Test data generation of procedural and Object oriented programming, Program Analysis, E-Governance, E-Govermance Security. He is working as HOD, Computer Engineering Department, Assam Engineering Institute, Guwahati, INDIA.