VIRTUAL BROWSER PLUS

An advance technique against phishing attacks

Ambarish Kumar Gupta
Information Technology
G.C.E.T.
Greater Noida, India
ambarishgupta89@gmail.com

Anuj Singh
Information Technology
G.C.E.T.
Greater Noida, India
anujdiesel@gmail.com

Anoop Rai
Information Technology
G.C.E.T.
Greater Noida, India
Anooprai7@gmail.com

Manish Singh
Information Technology
G.C.E.T.
Greater Noida, India
manish6232@gmail.com

***Abstract*—Phishing problem has grown in the last decades, becoming the most common web threat today. More than hundreds of anti-phishing mechanisms ranging from security toolbars to web browser add-ons concentrate on how to inform the user whether the website is fake or not. All such approaches are preventive by nature. Phishers continually target the weakest link in the security chain, namely, consumers in their attacks. Various usability study and survey have demonstrated neither server-side security indicators nor clients-side toolbars and warnings are successful in preventing the vulnerable users from being deceived. In this paper, we proposed a different approach, 'Virtual Browser Plus'-to counter phishing attacks. Instead of identifying the fake ones, Virtual Browser will allow access only to the genuine sites users will be given on-demand browsing service over the internet, where they can remotely connect to a secure server and use pre-configured browsers to securely connect to any websites of their choice.**

***Index Terms*—Phishing, Anti-phishing, Virtual Browser (VB), Internet security.**

1. INTRODUCTION

The term phishing is derived from fishing, in which the fish catcher puts a bait to catch fishes. In same manner today's modern cyber world, phishing attacks combine technology and social engineering to gain access to restricted information of a user. The most common phishing attacks today send mass e-mail or instant message asking the victim to visit a fake website to disclose personal credentials. Although phishing is a simple social engineering attack, it has proven to be surprisingly effective. Hence, the number of phishing scams is continuing to grow, and the costs of the resulting damage are increasing. Researchers across the globe as well as the IT industry experts have identified the urgent need for anti-phishing solutions.

1.1 DEFINITION

Website phishing is a variation on the word 'fishing' (James 2005). The concept is that bait is thrown out with the hope that the user will grab it just like the fish. The commonly used bait is either an email or an instant messaging site, which will take the user to hostile phishing websites, mostly to an exact replica of institutional website. This fake website will have similar look & feel of the original one. This page will be asking for the sensitive information like user name, password, credit card details, etc. When the victim (user.) enters the information, the data is sent to the publisher who thereby uses the same for his personal gain. Phishing has become the most common channel for thieves to acquire personal information to aid them in identity theft(Brody et al,2007;and Anderson et al,2008). According to anti phishing working group (APWG, 2010a) define phishing activities as a form of online identity theft that employs both social engineering and technical subterfuge to steal customers personal identity data and financial account credentials. Phishing incidents are handled by the Indian computer emergency response team (CERT-IN) in India.

Year	2006	2007	2008	2009	2010	2011	2012
Incidents	339	392	604	374	508	486	578

Table1: year-wise summary of phishing incidents handled by CERT-IN.

1.2 PHISHING ATTACKS

The phishing problem has evolved significantly over the past years. The present economic crisis and unemployment are an added argument for the great increase in the number of phishing attempts, cheating internet users. Though there are many techniques for phishing like code based key logger, DNS poison, search engine phishing etc. most phishing attacks trick users into submitting their personal information using a web form. Even though using web form to submit sensitive information on genuine sites, it has few problems which make this attack effective and hard to prevent.

First, the look and feel of a website and its forms are easy to copy and spoof. Second, web browsers fail to effectively visually differentiate Secure Socket Layer (SSL) connection from a non-SSL one.

1.3 SOLUTIONS AND REQUIREMENTS

To counter the phishing attack, software vendors and companies around the globe have released a variety of anti-phishing tools. Many of them can be found on download.com.

In this paper, we are aiming to develop a novel technique to deter the growing phishing attacks. Instead of detecting the site is legitimate or not, we propose a client-side virtual Browser which will restrict the users to log in to a secured server using SSL protocol hosted on an IP address instead of

ISBN: 9788175157538

Domain Name after the successful log in to our virtual browser the user will be allowed to access a domain specific pre-configured virtual web browser which will allow the user to access a particular web site only through a safe mode. The user will be given the option to add or remove new web sites on this virtual browser, but only after complete security check, the user will be given a new browser tab inside the main browser to access the additional site.

2. *Abbreviations and Acronyms*

CAPTCHA	Computer and Human Apart
CERT	Computer Emergency Response Team
DNS	Domain Name Server
E-Mail	Electronic mail
GPL	General Public License
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
PIN	Personal Identification Number
OS	Operating System
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Recourse Locator
VB	Virtual Browser

3. *Related Work*

The growth rate of phishing attacks has spurred calls for solutions. A number has been proposed ranging from quick fix changes to more substantial redesign. In this section we provide an overview of the anti-phishing proposals. A comprehensive survey done by APWG on phishing countermeasures can be found on their website.

One approach is using Dynamic Security Skins(DSS), which allow a remote based server to proves its identity in a way that is easy for human user to verify and hard for an attacker to spoof. If user interface elements are customized in a way that is recognizable to the user but very difficult to predict by others, attackers cannot mimic those aspects that are unknown to them. It assigns each user a random photographic image that will always appear in the password window. An image which will be very personal to the user. The user should easily be able to recognize the personal image and should only enter his password when this image is displayed.

The second approach is using Completely Automated Public Turning Test to tell computer and Human apart (CAPTCHA) kind of challenge –response test which can create hurdle for bots (League, 2009). The base of CAPTCHA is to use hard artificial intelligence (AI) to distinguish human and bot apart which was originally involved from visual authentication and identification.

The third approach is an intelligence system (Somanetal, 2008) which will detect the phishing attacks by finding the original page corresponding to the suspect page and subsequently do the structural matching of both the pages to uncover any distortion present

These different are all preventive by nature and its proved all are not successful in their aim since:

- Phishers can convincingly imitate the appearance of legitimate websites.
- Users tend to ignore security indicators of warnings.
- Users do not necessarily interpret security cues appropriately.

However, these approaches cannot completely foil phishing attacks and will take a long time to be effective on a global scale.

4. *Virtual Browser*

After a careful study of existing anti-phishing tools and available countermeasures and approaches, we came to the conclusion that phishing is a social engineering attack and that our approach to counter that will not the same, and we cannot have a solution that will be user-dependent. Our solution has to be purely technology-oriented, which will be difficult to breach and replicate. In that part we shall proceed on to a new method, which will not underestimate any previously suggested actions and works by any means.

4.1 Design Principles

The VB is designed keeping in mind that human user are the weakest link in the security chain. The VB is method where the user's intention is obvious; hence nothing is left for the user to decide. In the VB, the user not only surf the internet but also do transactions with preselected financial institutions, and check or download e-mail on a secured platform. The user will have the option to add or delete a website from the browser. The user will provide two different platform one where user are restricted to preselected site/domain and another one where user are open to surf for any site/domain.

4.2 Design Assumption

We assume that an end user will agree to use VB keeping the following in mind:

- It is the security that matters not the speed.
- VB is not meant for regular Internet browsing.
- VB will be available after successful installation.
- During installation/configuration, the user will provide the name of the institutions/sites which he intends to visit on VB.
- The user will not share the authentication password/steps for the VB with a third person by any means.

4.3 Technology

Our proposed design is platform independent model; one can use open source (General public License or GPL) or a proprietary solution for the same. We prescribe software set

ISBN: 9788175157538

for the model; one need to have the following to offer the service to the end user.

- Adequate memory space and processor's speed.
- Firewall support for the application.
- Database supports to create a white list of domain name as maintain the user data and log.
- Built-in encryption support (SSL and TLS).

4.4 How it works

We give the step-by-step guide for the usage of VB; we have taken the best available practices as on the date to make it a layered authentication system as well as the whitelist, blacklist method to create our own database of sites.

4.4.1 Installation Process

- VB will be installed as usual application software.
- User configures the domain name list as per his interest.
- The user will provide the authentication password.

4.4.2 Authorization to Virtual Browser

- The user will run VB application.
- VB will authenticate the user on the basis of user name and password.
  There will not be any password field to enter the password. The user will use a dynamic virtual key board to punch the password.
- The user may have to OK the photograph from many random photographs that is popped-up.

4.4.3 Inside Virtual Browser

- VB will be a single frame-based browser window, something like the pop-up window for regular advertisements.
- Home window for VB will have tabs depending upon the site opt opted for during configuration of domain name list.
- VB will have a back-to-home link and a session log out link.
- The user will have two option one for secure platform for which only preselected sites/domain are available and other for open surf beside those preselected sites/domain.
- For e-mail account, any external hyperlink within the domain will not work in secure platform rather of that it will work in open platform hence no chance to be deceived.
- For financial sites, it will allow browsing within the domain based on the hyperlink available for the site. It will not allow the user to steer away to any other domain or any other IP-based site in secure platform.
- VB will maintain a time-based session to check on idle time, over a stipulated time the session will automatically logoff, and will delete all session's related information from browser.

4.5 Advantages

All other available anti-phishing solutions give active or passive warning to the user regarding the status of the domain, but VB will only allow sites as opt-in model. So the option of ignoring the message and continuing with browsing in same platform is not applicable in this case.

Various web proxies also provide secure access to sites which user can visit through them. But in our case we have full control on the same.

As we will be using our own secure DNS, theoretically we will be able to stop all the attacks like:

- Deceptive phishing
- Malware-based phishing
- Key logger s and screen loggers
- Session hijackers
- Web Trojans
- Hosts file poisoning
- System recognition attacks
- Data theft
- DNS-based phishing('pharming')
- Content-injection phishing
- Man-in-the-middle phishing
- Search engine phishing

4.6 Some Common Issues

Performance: As VB implemented on the top of a native browser it will consumes more memory space and latency of JavaScript parsing decreases with rise in number of lines.

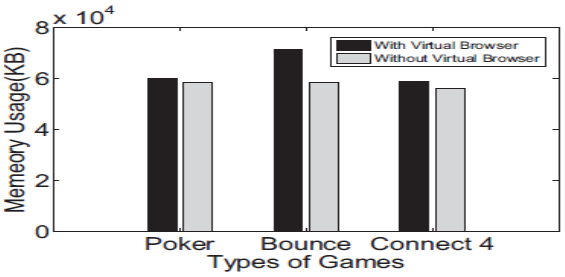

Diagram 1: Comparison of Memory Usage of VB and Native Browser

ISBN: 9788175157538

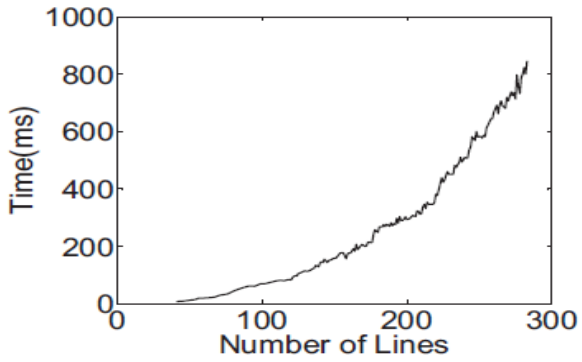

Diagram 2: Latency of JavaScript Parsing

Speed: Since VB is going to occupy more memory hence loading time increases simultaneously that effect negatively to the operational speed of VB and due to self DNS matching time laps.

Security: Although, our design is going to beat the phishing attacks but threats are in a larger domain that we cannot cover it as a whole. So we adopt two methods to ensure security: avoidance and redirection. We use for sandbox all the components inside Virtual Browser by cutting off the inflows and outflows to and from the sandbox. We avoid using some of JavaScript's dangerous functions in the Virtual Browser implementation to achieve isolation. We enable shared objects and communications with security access control. Because we have already built an isolated sandbox, in the second part of the design, we mainly redirect dangerous flows within the third party code back to the sandbox to facilitate communication.

5. Problem Statement

The VB is slow compare to the regular browser, as it checks its own DNS database and matches with the requested website I.P. address before allowing or restricting the website. The end result is user-waiting time is: more in the case of a website opening though the VB.

There is a possibility that the VB DNS list can itself be spoofed. We need to safeguard the same with more security.

After all the measures, there is no way we can make sure that the user will not visit the sites form other browser.

VB will not be of any help against any key logger installed on the computer.

User needs to remember one more username and password for the VB.

6. Proposed Approach

We propose the concepts of browser virtualization in order to overcome all the issues and problem listed above we will make a case study on a preexisting sand box and there approaches to compete all these negative factors, A deep study of documentation of pre-existing VB is needed to refine our design. After that we will modify our design/prototype accordingly and again have to make a careful analysis of the design and try to make it more robust, light-weighted, speedy, secure and more powerful. If all things will go in a right passion we will implement it practically.

Acknowledgment

This research paper is made possible through the help and support from everyone, including: parents, teachers, family, friends, and in essence, all sentient beings.
Especially, please allow me to dedicate my acknowledgment of gratitude toward the following significant advisors and contributors: I would like to thank Mr Javed Mia for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper.
As well as all the other professors who have taught me over the past years of my pursuit of the bachelor degree.

References

1. The IUP Journal of Information Technology, Vol. VIII, No.2,2012, pp. 7-21 Common vulnerabilities and exposures. http://cve.mitre.org

2. Doxygen.: http://www.stack.nl/~dimitri/doxygen/FBJS http://wiki.developers.facebook.com/index.php

3. JavaScript game site. http://javascript.internet.com/games

4. JavaScript reference. https://developer.mozilla.org/en/Core_Javascript_1.5_Reference

5. JavaScript test cases. http://mxr.mozilla.org/mozilla/source/js/tests/ecma

6. Mozilla rejects native code approach of chrome's nacl. http://css.dzone.com/articles

.

7. Microsoft Live Labs. Web Sandbox http://websandbox.livelabs.com/

8. Mozilla. Narcissus JavaScript engine http://mxr.mozilla.org/mozilla/source/js/narcissus/

9. CERT (2012), "Indian Computer Emergency Response Team (CERT-IN)" November 2012,available at http://www.cert-in.org.in/

10. Google.caja: http://code.google.com/p/google-caja/

ISBN: 9788175157538