ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Hardware Based Prevention of Phishing Attack

Amit Solanki
M.Tech. Scholar, Dept. of Computer Science & Engg.
Swami Keshvanand Institute of Technology
Jaipur, India
amit.solanki48@gmail.com

S.R.Dogiwal
Reader, Scholar, Dept. of Computer Science & Engg.
Swami Keshvanand Institute of Technology
Jaipur, India
dogiwal@gmail.com

Jitendra Sharma
M.Tech. Scholar, Dept. of Computer Science & Engg.
Swami Keshvanand Institute of Technology
Jaipur, India
jitendra0511@gmail.com

Abstract: Phishing is a widespread problem that is impacting both business and consumers.phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication [1]. This paper explains the method used for phishing prevention using Hardware based Login technique to prevent phishing and with the help of this technique user can prevent form phishing easily using the hardware locking system.

Keywords: Phishing, Phishing statistics, Phishing Techniques, Hardware based Login.

I. INTRODUCTION

Phishing is the activity of fraudulently presenting oneself online as a legitimate enterprise in order to trick consumers into giving up personal financial information that will be used for identity theft. Phishing is most commonly perpetrated through the mass distribution of e-mail messages directing users to a web site, but other venues are utilized as well[3].

A phishing scam is one in which victims are tricked into providing personal information such as account numbers, passwords and credit card details to what they believe to be a legitimate company or organization. In order to carry out this trick, the scammers often create a "look-a-like" webpage that is designed to resemble the target company's official website. Typically[1], emails are used as "bait" in order to get the potential victim to visit the bogus website. The emails use various devious ruses to trick readers into clicking on the included links, thereby opening the bogus website. Information submitted on these bogus websites is harvested by the scammers and may then be used to steal funds from the user's accounts and/or steal the victim's identity.

A. Spam Classification:

Through the use of classification techniques, we can identify specific spam groups. In some cases the identification can include a specific individual; in other cases, groups of e-mails can be positively linked to the same unspecified group[5]. Forensic tools and techniques can allow the identification of group attributes, such as nationality, left- or right-handedness, operating system preferences, and operational habits.

B. Spam Organization:

There are two key items for identifying individual spammers or specific spam groups: the bulk mailing tool and the spammer's operational habits. People who send spam generally send millions of e-mails at a time. To maintain the high volume of e-mail generation, spammers use bulk-mailing tools. These tools generate unique e-mail headers and e-mail attributes that can be used to distinguish e-mail generated by different mailing tools. Although some bulk-mailing tools do permit randomized header values, field ordering, and the like, the set of items.

That can be randomized and the random value set are still limited to specific data subsets. More important than the mailing tool is the fact that spammers are people, and people act consistently (until they need to change).They will use the same tools, the same systems, and the same feature subsets in the same order every time they do their work. Simplifying the identification process, most spammers appear to be cheap. Although there are commercial bulk-mailing tools, most are very expensive[7]. Spammers would rather create their own tools or pay someone to create a cheaper tool for them. Custom tools may have a limited distribution, but different users will use the tools differently. Based on the results of this minimal organization, we can identify specific attributes of this spammer:

a. The hash buster is nearly always connected to the subject.

b. The file sizes are roughly the same number of lines (between 50 and 140 lines—short compared to most spam messages).

c. Every one of the forged e-mail addresses claims to come from yahoo.com.

C. Classification Techniques:

After we identify and profile individual spam groups, we can discern their intended purpose. To date, there are eight specific top-level spam classifications, including these four:

a. ***Unsolicited commercial e-mail (UCE)****:*-This type is generated by true company trying to contact existing or potential customers. True UCE is extremely rare, accounting for less than one-tenth of 1 percent of all spam. (If all UCE were to vanish today, nobody would notice.)

b. ***Nonresponsive commercial e-mail (NCE)****:*-NCE is sent by a true company that continues to contact a user after being told to stop. The key differences between UCE and NCE are (1) the user initiated contact and (2) the user later opted out from future communication. Even though the user opted out, the NCE mailer will continue to contact the user. NCE is only a problem to people who subscribe to many services[2], purchase items online, or initiate contact with the NCE Company.

c. ***List makers*** these are spam groups that make money by harvesting email addresses and then use the list for profit, such as selling the list to other spammers or marketing agencies.

d. ***Scams*** Scams constitute the majority of spam. The goal of the scam is to acquire valuable assets through misrepresentation.

II. PHISHING STATISTICS

Phishing in general took on a more organized direction. Phishers have refined their attacks, both in e-mail and malware, and have begun to target specific secondary and tertiary targets[6]. We highlight the perspective of statistics and the evolutionary development of phishing:

a. Phishers are refining their e-mail techniques. Their e-mails are much more effective than regular spam. A single mass mailing of 100,000 emails may have a receive rate as high as 10 percent and collect as much as 1 percent in victims.

b. Phishers of 2005, mainly Romanians, build their own PHP bulk-mailing tools so they can move more efficiently off the Internet. This allows them to use hacked or stolen dedicated servers to offload their mass mailing rather than client-end bulk-mailing software.

c. Phishers have found a use for every account they acquire: from money laundering to theft, shuffling, and identity theft.

d. Phishers are refining their key-logging malware. Rather than collecting data from all Web sites, they are now looking for data from specific URLs.

e. Phishers are becoming more technically savvy. Besides using known and 0-day exploits to configure the systems used for phishing, they also use weaknesses in the telephone infrastructure, such as Caller ID (CID) spoofing, to protect themselves from the mules that they contact and to perform money-laundering activities.

Phishers are taking advantage of Cross-Site Scripting (XSS) vulnerabilities, URL redirection opportunities, and any browser-specific exploits that enable them to employ attacks that allow them to gain user information. Cross-Site Scripting is done by inserting a script into an URL or a form that is later executed in the client browser.

III. PHISHING TECHNIQUES

In this section we are discussing about phishing techniques that fraudsters are using to capture members' personal and financial information:

A. Scam: Social Networks:

Members should be wary of clicking any links in emails or accessing social networking sites for holiday themes such as Halloween upon us[4]. Holiday scams contain links that redirect members to an indirect site registered by the fraudster.

a. ***Prevention:*** Members should close their browsers if they see a link to download or install an application.

B. Scam: Call Forwarding:

Fraudster is call forwarding your members' landline or cell phone number to another telephone. In most cases, it's a prepaid cell phone.

a. ***Prevention:*** Members should place a password on their telephone numbers to prevent them from being call forwarded.

C. Scam: Text Messaging:

Fraudster sends a text message (smishing) and your members respond to the request.

a. ***Prevention:*** Credit unions should advise members to be alert when text messages appear on their cell phone, smart phone or PDA device. If the text message requests personal or financial information, members should contact the credit union immediately and not respond to the text message. If a smishing attack occurs, proactively communicate to members via statement stuffers, website alerts and voice message alerts.

D. Scam: System Intrusions:

Fraudsters are focused on phishing your members to provide account numbers, passwords and user names to get into the home banking system[7]. The industry has shown an uptick in system intrusions through unauthorized ACH and/or wire requests.

a. ***Prevention:*** Credit unions should implement multifactor authentication to prevent fraudsters from gaining access to systems.

Members should monitor their transaction activity daily to help identify any unauthorized activity. They should watch for unauthorized ACH or wire transfers.

E. Scam: Voice Vishing:

This scam attempts to trick members into providing personal and financial information over the phone. Most vishing scams begin with an email or text message asking your member to call a toll-free number[2]. When members call the number, they are led through a series of voice prompted menus that ask for key financial information such as a card or member account and the PIN.

a. ***Prevention:*** Members should not call the telephone number. Rather, they should report this to the credit union and telecommunications carrier immediately. This number needs to be shut down to help prevent others from responding to the attack.

F. Scam: Spoofing Caller ID:

Members receive a call from either a live person or a recorded message with a spoofed caller ID[9]. The caller ID may list a legitimate looking telephone number. Fraudsters have spoofed caller ID systems or assign any area code to a phone number so it appears to be an 800 number or a local number.

a. ***Prevention:*** Members should never provide any personal or financial information to the caller. Always hang up and contact the credit union to report this activity. Your credit union will not request personal or financial information from you via a telephone call.

IV. ANTI PHISHING

Phishing will stop if the majority of users are educated and know how to handle computers. There are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing[8].

A. Legal Responses:

On January 26, 2004, the U.S. Federal Trade Commission filed the first lawsuit against a suspected phisher. The defendant, a Californian teenager, allegedly created a webpage designed to look like the America Online website, and used it to steal credit card information. Other countries have followed this lead by tracing and arresting phishers. A phishing kingpin, Valdir Paulo de Almeida, was arrested in Brazil for leading one of the largest phishing crime rings, which in two years stole between US$18 million and US$37 million. UK authorities jailed two men in June 2005 for their role in a phishing scam, in a case connected to the U.S. Secret Service Operation Firewall, which targeted notorious "carder" websites. In 2006 eight people were arrested by Japanese police on suspicion of phishing fraud by creating bogus Yahoo Japan Web sites, netting themselves 100 million yen ($870,000 USD). The arrests continued in 2006 with the FBI Operation Card keeper detaining a gang of sixteen in the U.S. and Europe.

B. Technical Responses:

Anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem[3].

a. Helping to Identify Legitimate Websites:

Most websites targeted for phishing are secure websites, meaning that SSL with strong cryptography is used for server authentication, where the website's URL is used as identifier. In theory it should be possible for the SSL authentication to be used to confirm the site to the user, and this was SSL v2's design requirement and the meta of secure browsing [3]. But in practice, this is easy to trick. The superficial flaw is that the browser's security user interface (UI) is insufficient to deal with today's strong threats. There are three parts to secure authentication using TLS and certificates: indicating that the connection is in authenticated mode, indicating which site the user is connected to, and indicating which authority says it is this site. All three are necessary for authentication, and need to be confirmed by/to the user[8].

b. Click-thru Syndrome:

However, warnings to poorly configured sites continued, and were not down-graded. If a certificate had an error (mismatched domain name, expiry), then the browser would commonly launch a popup to warn the user. As the reason was generally misconfiguration, the users learned to bypass the warnings, and now users are accustomed to treat all warnings with the same disdain, resulting in Click-thru syndrome[3]. For example, Firefox 3 has a 4-click process for adding an exception, but it has been ignored by an experienced user in a real case of MITM. Even today, as the vast majority of warnings will be for misconfigurations not real MITMs, it is hard to see how click-thru syndrome will ever be avoided.

C. Social Responses:

One strategy for combating phishing is to train people to recognize phishing attempts, and to deal with them. Education can be effective, especially where training provides direct feedback[3]. One newer phishing tactic, which uses phishing e-mails targeted at a specific company, known as spear phishing, has been harnessed to train individuals at various locations, including United States Military Academy at West Point, NY. In a June 2004 experiment with spear phishing, 80% of 500 West Point cadets who were sent a fake e-mail were tricked into revealing personal information.

V. HARDWARE BASED LOGIN

In order to access account, user has to provide following information:

a) Personal Identification Number (User ID)
b) Password
c) USB Lock (USB Device Provided by the Bank)

Each user has its own unique USB Device for each account. There are Following Steps in this technique:-

Step 1:

User required to connecting form web page of online banking and Plug-in USB device to the system which is provided by the respective Bank for Login and input the personal identification number ID, password.

Step 2:

After that Plugging, User inputs User_Id and Password. Then the computer will verify the client's information accompanied with USB device in Offline Mode.USB Device contains information related to user in Encrypted way. In verification process we use Encryption and Decryption algorithm for enhancing security. After that Successful verification of Offline process this information communicates with host computer of the bank for verification and authentication. In case of failure User will not be able to access the account.

Step 3:

In this process all information goes to host computer in encrypted way and at the host end, it verifies from the database and allow accessing the account and user can further proceed for Online Transactions. In this process USB Device is connected with the Client Computer, in the absence of this USB Device, User can't access the Account.

VI. CONCLUSION

Phishing is an issue of increasing importance since everyone can be targeted and since the techniques used by phishers are more and more sophisticated. Moreover, the damage done can be enormous and the phishers are hard to catch. Therefore, without being an expert of information techniques, it is possible to implement some simple measures in the everyday life to strengthen protection when we are online. Learning to be suspect and getting the reflex of checking the truth of the information you might receive is important [4]. Changing passwords often and being able to recognize signs of spoofed e-mails or website is also necessary. In order to improve the security on E-commerce transaction, application of information techniques and restriction from law would block the illegitimate transaction from happening. Users need to change him own habit to attend to personal information so as to make the online transaction more secure.

We believe that Hardware based Login is not only useful for preventing phishing attacks, but also can shield users from malicious or unsolicited links in Web pages and Instant messages. Our future work includes further extending the Hardware based login approach.

VII. REFERENCES

[1]. ONGUARD ONLINE. Phishing quickfacts, 2008.

[2]. DHAMIJA, R., AND TYGAR, J. D. The battle against phishing: Dynamic Security Skins. In SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security (New York, NY, USA, 2005), ACM Press, pp. 77–88.

[3]. ANTI-PHISHING WORKING GROUP. Anti-phishing Best Practices Recommendations for Registrars. Report, 2008.

[4]. Ian Fette, Norman Sadeh, and Anthony Tomasic. Learning to detect phishing emails. In ACM International conference onWorldWideWeb (WWW), 2007.

[5]. Tyler Moore and Richard Clayton. An Empirical Analysis of the Current State of Phishing Attack and Defence. InWorkshop on the Economics of Information Security, 2007.

[6]. Cyber Crime and Doing Time. (2011). the epsilon phishing model. Retrieved 12 Mar, 2011.

[7]. NETCRAFT INC. Netcraft anti-phishing toolbar. visited jan 1, 2009.

[8]. "APWG - Phishing activity trends: Report for December 2007," http://www.antiphishing.org/reports/apwg report dec 2007.pdf, 2007.

[9]. Steve Sheng, Bryant Magnien, Ponnurangam Kumaragu-ru,Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge, "Anti-Phishing Phil: The Design and Evalu-ation of a Game That Teaches People Not to Fall for Phish," In Proceedings of the Second Symposium on Usable Privacy and Security (SOPUS□11 Pittsburgh, Pennsylvania, July 20 - 22, 2011), ACM Press, New York.