ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (244-248), Month: April - June 2015, Available at: www.researchpublish.com

A System to Detect and Prevent Phishing

[1]Saritha L.R, [2]Vinayak Pillai, [3]Deepak Reddy, [4]Dinesh Reddy

Dept. of IT, SIES-GST, Mumbai, India

Abstract: **Anti-phishing refers to the method employed in order to detect and prevent phishing attacks. Anti-phishing protects users from phishing. A lot of work has been done on anti-phishing devising various anti-phishing techniques. Some techniques works on emails, some works on attributes of web sites and some on URL of the websites. Many of these techniques focus on enabling clients to recognize & filter various types of phishing attacks. In general anti-phishing techniques can be classified into following four categories.**

Keywords: **Anti Phishing, Cyber Security, Data Stealing Security, Phishing, Securing Data.**

I. INTRODUCTION

Phishing:

Phishing is to illegally carry out fraudulent financial transactions on behalf of users using a forged email that contains a URL pointing to a fake web site masquerading as an online bank or a government entity. A phisher may lure a victim into giving his/her Social Security Number, full name, & address, which can then be used to apply for a credit card on the victim.

Anti-phishing:

Anti-phishing refers to the method employed in order to detect and prevent phishing attacks. Anti-phishing protects users from phishing. Anti-phishing techniques. Some techniques works on emails, some some works on attributes of web sites and some on URL of the websites.

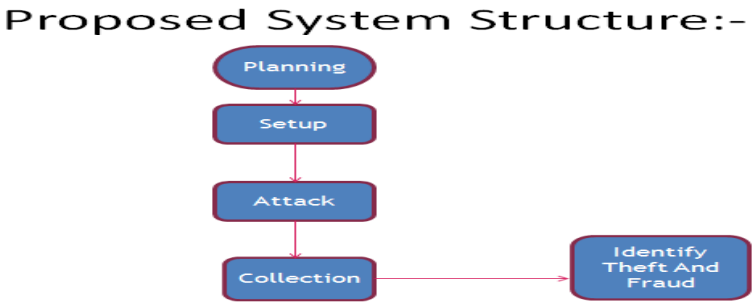
Many organizations are concentrating on phishing monitoring and research. Below are several famous organizations in the anti-phishing field. Anti-phishing Work Group: a group where you can report the phishing and get lots of information about phishing. They have an official website for collected phishing events and work together with many group companies [12]. CNCERT/CC is a functional organization under Internet Emergency Response Coordination Office of Ministry of Information Industry of China, who is responsible for the coordination of activities among all Computer Emergency Response Teams within China concerning incidents in national public networks. It provides computer network security services and technology support in the handling of security incidents for national public networks, important national application systems and key organizations, involving detection, prediction, response and prevention.

It collects, verifies, accumulates and publishes authoritative information on the Internet security issues. It is also responsible for the exchange of information, coordination of action with International Security Organizations [13]. IRIS-CERT is Red IRIS' security service, and is aimed to the early detection of security incidents affecting Red IRIS centers, as well as the coordination of incident handling with them. Proactive measures are in constant development, involving timely warning of potential problems, technical advice, training and related services.

The Messaging Anti-Abuse Working Group (MAAWG) is a global organization focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages [15]. Many anti-virus software companies are also taking some efforts in the phishing research. If we find some suspicious incidents, they are also the places where we can report it.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (244-248), Month: April - June 2015, Available at: www.researchpublish.com

II. SYSTEM ARCHITECTURE



It collects, verifies, accumulates and publishes authoritative information on the Internet security issues. It is also responsible for the exchange of information, coordination of action with International Security Organizations [13]. IRIS-CERT is Red IRIS' security service, and is aimed to the early detection of security incidents affecting Red IRIS centers, as well as the coordination of incident handling with them. Proactive measures are in constant development, involving timely warning of potential problems, technical advice, training and related services.

The Messaging Anti-Abuse Working Group (MAAWG) is a global organization focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages [15]. Many anti-virus software companies are also taking some efforts in the phishing research. If we find some suspicious incidents, they are also the places where we can report it.

III. NEED FOR PROJECT

Phishing is a particularly devious form of Internet scam. Customers of banks and financial institutions are often prime targets for “phishers” who trick them into divulging sensitive personal information such as their credit- or debit-card account numbers and personal identification numbers (PINs), by making bogus offers using spoof e-mails and fake Web sites. The technique is also used to steal identities.

1. Phishing, and other spam-related attacks, do not exploit technical vulnerabilities. They leverage a technological medium to exploit human weaknesses.

2. The difference is significant – and game changing. While technical weaknesses can often be addressed with technical solutions, curbing phishing and related scams mandates addressing the underlying human problem at their cores — an issue has nothing to do with the digital age.

3. Deceptive actors impersonating legitimate parties have been conning people since the dawn of civilization.

4. In fact, a primary reason why phishing continues to be an effective method of attack – even after a decade of anti-phishing efforts – is precisely because anti-phishing technologies are often designed to combat phishing by implementing technical “solutions” rather than addressing the human source of the problem. Technical countermeasures can be circumvented, and if a human target is not otherwise shielded, problems occur. Software that attempts to block or erase phishing emails before a user reads them, for example, does nothing if a user is directed to a rogue website via a text message, and may, at times, even aggravate the problem by lowering a person’s guard when a cleverly constructed email does reach the user; the recipient thinks that illegitimate emails are blocked, and, therefore, grants unwarranted trust to messages that he or she does receive.

IV. OBJECTIVE

The objective really depends on what trade-off between efficiency/productivity and security you're willing to make. While most researchers agree on the importance of preventing phishing attacks; few have precisely defined the goals of a technique to effectively combat them. Below, we enumerate these goals, arranged in decreasing order of protection and generality:

1. Ensure that the user’s data only goes to the recipient that the user thinks it is going to.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (244-248), Month: April - June 2015, Available at: www.researchpublish.com

2. Prevent the user's data from reaching an untrustworthy recipient.

3. Prevent an attacker from abusing the user's data.

4. Prevent an attacker from modifying the user's account.

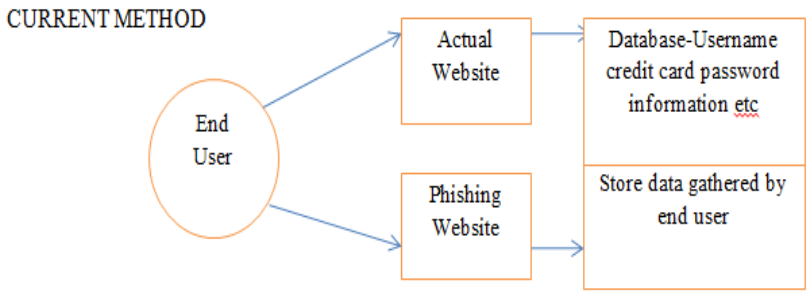
Prevent an attacker from viewing the data associated with user's accountStopping general phishing (the mass mail, badly written, generic kind) is'nt impossible, and can be achieved without too much sacrifice, through proper employee training. Highly targeted, professional grade phishing though, is incredibly hard to stop, as it may appear to be from (or be from) legitimate email accounts, be well written and highly relevant to the person receiving it. I would say stopping this kind of attack is near impossible for any organization that relies on interaction with the outside world.There have been some examples of these attacks recently (against people who most likely do have employee training)

- http://www.canberratimes.com.au/it-pro/security-it/hackers-breach-reserve-bank-20130311-2fv8i.html
- http://www.h-online.com/security/news/item/Highly-specialised-MiniDuke-malware-targets-decision-makers-1813304.html

Of course training employees to exhibit "proper" behaviour requires the proper internal organization to support it. There's not much point in telling employees not to do something that will actually be required of them (for example clicking links to change their user details, etc).

V. METHODOLOGY

The process used to collect information and data for the purpose of making business decisions. The methodology may include publication research, interviews, surveys and other research techniques, and could include both present and historical information.



The figure shows the current scenario. When user accesses his information online by logging into his bank account or secure mail account, the person enters information like username, password, and credit card information etc. on the login page. But this information can be captured by attackers using various phishing techniques. (For instance Phishing website can collect the login information the user enters and redirect him to the original site.)

PROPOSED METHODOLOGY

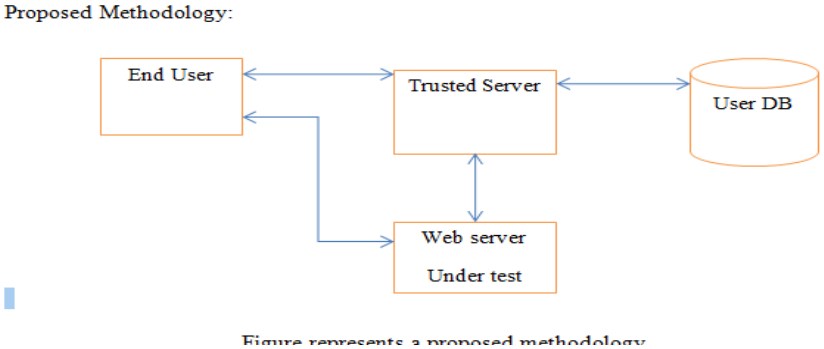
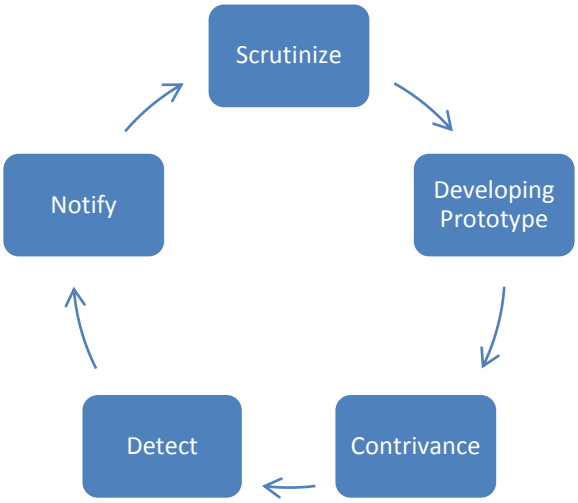


Figure represents a proposed methodology

Figure represents a proposed methodology

When user registers with the server, server generates pair of unique keys for the user. From that pair one key for the user is saved on the user database of the trusted server and another key is propagated to the user.When the user logs into the system through the web server1, user selects a random image which is available on his/her machine (Every time when user logs into the system he/she can select any image available onto the system).This image is divided into two shares such that one share is kept with the user and other share is encrypted and sent to the web server. Web server1 sends this encrypted share along with its details to the trusted server. Trusted server provides decrypted version of this share if and only if server1 was registered with trusted server. The decrypted share is sent back to the client. At the client side decryptography is performed to obtain the original image by stacking together the shares. If the original image obtained is as is, the website is genuine/secure website and not a phishing website.

VI. SOFTWARE DEVELOPMENT LIFECYCLE



VII. WORKING OF THE SYSTEM

The various modules which we intend to include in our system are as follows:

1. Login , Password :

This module creates a login Id and Password as per user demand and admin if required.

2. Change Password:

This module helps user to change password and assign a new password according to their needs whenever necessary.

3. Inspect:

This aspect actually executes the algorithm and finds out if the website is an authentic one or not.

4. Black List:

This list stores all the malicious links.

VIII. FUTURE SCOPE

Our future work includes further extending the Link Guard algorithm, so that it can handle Cross Site Scripting (CSS) attacks. Cross-site scripting (CSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Vulnerabilities of this kind have been exploited to craft powerful phishing attacks and browser exploits. Cross-site scripting was originally referred to as CSS, although this usage has been largely discontinued due to the confusion with cascading style sheets.

IX. CONCLUSION

Phishing has becoming a serious network security problem, causing financial loss of billions of dollars to both consumers and e-commerce companies. And perhaps more fundamentally, phishing has made e-commerce distrusted and less attractive to normal consumers. In this paper, we have studied the characteristics of the hyperlinks that were embedded in phishing e-mails. We then designed an anti-phishing algorithm, Link Guard, based on the derived characteristics. Since Phishing Guard is characteristic based, it can not only detect known attacks, but also is effective to the unknown ones.

We have implemented Link Guard for Windows XP. Our experiment showed that Link Guard is light-weighted and can detect up to 96% unknown phishing attacks in real-time. We believe that Link Guard is not only useful for detecting 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 Link Guard algorithm, so that it can handle CSS (cross site scripting) attacks.

REFERENCES

[1] M. Naor and A.Shamir; “Visual cryptography,” in Proc. EUROCRYPT, 1994, pp. 1– 12.6.

[2] Thiyagarajan, P.; Aghila, G.; Venkatesan, V.P.; "Anti-Phishing Technique using Automated Challenge ResponseMethod"', in Proceedings of IEEE- International Conference on Communications and Computational Intelligence,1999.2.

[3] D. Jin, M. S. Kanakanahalli and W-Q Yan; .Visual Cryptography for Print and Scan ,IEEETransactions, ISCAS-2004, pp. 572-575.

[4] B. Borchert, .Segment Based Visual Cryptography,. WSI Press, Germany, 2007.7.

[5] Ishtiaq, S.; Nourian, A.; Maheswaran, M.;" CASTLE: A social framework for collaborative antiphishingdatabases", in Proceedings of IEEE- 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2009.3

[6] Liang Xiaoying.; Sun Bin.; Wen Qiaoyan.; "A DNS based Anti-Phishing Approach," in Proceedings of IEEE-Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.5.

[7] Mintu Philip;Divya James;” A Novel Anti phishing Framework based on Visual Cryptography” in International Journal of Distributed and Parallel Systems, Vol. 3, No.1 January 2012.4.

[8] Mather Aburrous, M.A. Hossain, Keshav Dahal, Fadi Thabtah “Prediction phishing websites using classification mining techniques with experimental case studies” in proceedings of Seventh International Conference on Information

[9] Juan Chen, Chuanxiong Guo-“Online Detection and Prevention of Phishing Attacks (Invited Paper)”in proceedings of Communicational and networking in china.