International Journal of Information Technology and Management

Vol. VIII, Issue No. XI, February-2015, ISSN 2249-4510

PROTECTION STRATEGY IN E-BANKING- AN END USER APPLICATION

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VIII, Issue No. XI, February-2015, ISSN 2249-4510

Protection strategy in e-Banking- An end User Application

Rekha Mittal

Extension Assistant Professor, Pt. J. L. N. Govt. College, Faridabad

Abstract – With the increase in the online trading activities, there has been a phenomenal increase in the phishing scams which have now started achieving monstrous proportions. Seeking sensitive user data in the form of online banking user_id and passwords or credit card information, which may then be used by 'phishers' for their own personal gain is the primary objective of the phishing e-mails. In this paper we discuss an Anti-Phishing application for the end user which keeps track of the sites with which the user indulges in financial transactions, scans his e-mail account for mails which appear to have come from these institutions and warns him against suspected phishing e-mails, if the same are detected in his mailbox.

Index Keys –Phisher, Privacy, Security, Spam, Anti-phishing

----------♦----------

INTRODUCTION

Committing a crime in complete anonymity, having gained someone else's identity is a dream come true for any criminal. Phishing is a form of online identity theft which employs both social engineering and spyware methods to steal consumers' personal identity data and financial account credentials [1].

Prior to the advent of Internet such efforts on part of criminals were limited to isolated individuals, who were lured into getting their personal information through social engineering. However with the rapid growth of internetworking around the globe and the phenomenal popularity gained by Internet since the early days of 1990's, the going has never been easier for such criminals or 'phishers'. Their strategy is to send out millions of spam mails to potential targets around the globe, masquerading as it came from original institutions such as banks, insurance companies etc. These mails request the recipients to click on the embedded URLs which lead them to fraudulent but apparently official looking phishing websites where the users are made to divulge with their personal information such as passwords, account numbers and such. These are then collected by the phishers from the server side using web tools such as key loggers and used for their personal gains. Since it first occurred in the mid 1990's by attacking America Online, phishing has become a threat to online services provided by financial organizations, ISPs, retailers and governments. On an estimate, almost 5% recipients of phishing e-mails give away their personal information to these phishing sites while they are in operation [2].

A survey conducted by Gartner Inc.(World's leading information technology research and advisory company), found that 3.6 million adults lost money due to phishing attacks during the period from Sep '06 to Aug '07, leading to a huge financial loss assumed to be of the tune of $3.2 billion in US alone [3] compared to $2 billion lost in the year 2006 [4]. This loss is not only due to the financial loss which is borne by the individuals and the financial institutions on account of the fraudulent transactions by the phishers. There are a host of reasons responsible for the success of phishing attacks [5] a few of which are: lack of user's computer knowledge, use of changed URLs, rapid technological advancements in the field of computer science, lack of awareness amongst internet users about elements phishing for their sensitive information etc. In this paper we discuss a desktop based Anti-Phishing application for a naïve user against faked website based phishing attacks. The design of the application is based on the premise that a user is more susceptible to fall victim to a phishing e-mail which appears to have been sent from an institution like a bank, insurance company, investment company or an e-commerce site with which he has an existing relationship rather than from one with which he has no relationship. So if the user receives an e-mail claiming to be from, say Axis bank, but he does not have an account with them, then he is unlikely to forward any sensitive information to the phishing site. The application keeps track of names and URLs of websites with which the user has a relationship, scans the e-mail account of the user for e-mails which apparently have been sent by these institutions, looks for embedded URLs in these messages and generates a phishing

warning for the mails which appear to be phishing e-mails.

The paper is structured as follows: In the next section we talk about various types of phishing attacks. Section 3 describes the design and working of our application along with a live example of how a warning about a phishing e-mail is generated. In Section 4 we discuss the related work. Section 5 talks about the future work followed by Section 6 wherein we conclude our paper.

Types of Phishing Attacks

Two different types of phishing attacks may be distinguished: Malware-based phishing and deceptive phishing [15]. For malware-based phishing malicious software is spread by deceptive emails or by exploiting security holes of the computer software and installed on the user's machine. Then the malware may capture user input, and confidential information may be sent to the phisher. The focus of this paper is deceptive phishing, in which a phisher sends out deceptive emails pretending to come from a reputable institution, e.g., a bank. In general, the phisher urges the user to click a link to a fraudulent site where the user is asked to reveal private information, e.g., passwords. This information is exploited by the phisher, e.g. by withdrawing money from the users bank account. A number of tricks are common in deceptive phishing:

- Social engineering: The invention of plausible stories, scenarios and methodologies to produce a convincing context and in addition the use of personalized information.
- Mimicry: The email and the linked website closely resemble official emails and the official websites of the target. This Includes the use of genuine design elements, trademarks, logos and images.
- Email spoofing: Phishers hide the actual sender's identity and show a faked sender address to the user.
- URL hiding: Phishers attempt to make the URLs in the email and the linked website to appear official and legitimate and hide the actual link addresses.
- Invisible content: Phishers insert information into the phishing mail or website, which is invisible to the user and aimed at fooling automatic filtering approaches.
- Image content: Phishers create images that contain the text of the message only in graphical form.

III. DESIGN OF ANTI PHISHING APPLICATION

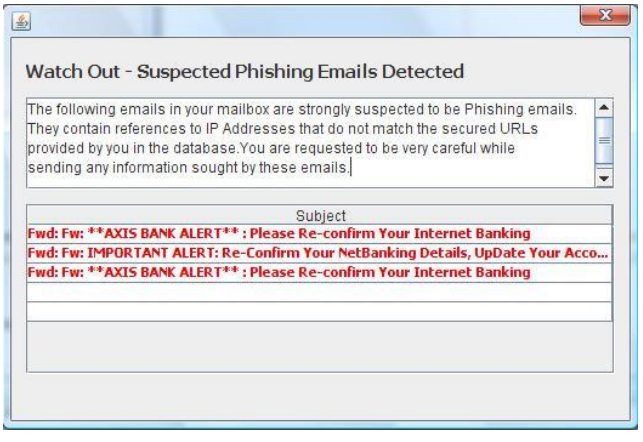
This anti phishing module is based on the following premise:-

(a) Generally naive user is more likely to fall victim to a phishing attack if the phishing e-mail received by him is from a financial/trading institution with which the user has a transaction relationship.

(b) For this kind of users, an application for checking the authenticity of the URLs embedded in the e-mail is required, by the use of which they cannot be fooled by the techniques employed by the phishers.

A. Main Functionality

This application works on the premise that a user is more worried about the authenticity of the emails which appear to have come from institutions with which he has a relationship, rather than e-mails received from all and sundry. As an example, consider a user who has an account with the ICICI Bank and not with Axis Bank. This user then is more likely to spoofed by a phishing mail which claims to be from ICICI Bank rather than a mail from Axis Bank. To ascertain the websites which are of interest to a user, there is thus a need of user interaction with the application. This application initially asks the user to enter the name and the trusted URLs of such institutions/websites where he sends his login details, i.e., username and password and application fetches the IP Address corresponding to the URL from the DNS server calculates its message digest (using MD5) and stores this data in a table within the database. On its subsequent run, the application connects to the email service provider of the user (in this case Gmail from Google) and scans for URLs in the message bodies of only those messages which appear/claim to have been sent by the websites of interest to the user. IP Addresses of URLs so located are fetched by the application and their MD5 values calculated. These values are compared against the values stored in the database for that institution. A warning message which includes subject fields of all the e-mails which report a mismatch in the values of message digest are then displayed, giving warning to the user that these mails are suspected to be phishing mails, as shown in figure 1 below.



B. Connecting to E-Mail Server

POP3 (Post Office Protocol version 3) and IMAP4 (Internet Message Access Protocol) are the two most prevalent Internet standard protocols used by the local e-mail clients for e-mail retrieval from a remote server over a TCP/IP connection. Although IMAP4 is more user friendly and offers a host of facilities to the users, it is not supported by most of the ISPs (e.g. Yahoo mail does not support IMAP4). The wide popularity of the POP3 protocol is largely due to its appeal to ISPs, not to the users. Using the POP3 protocol, ISPs can elect not to allow the user to leave a copy of the mail on the Mail Server, thus minimizing hard drive storage space. The present prototype of the Anti-Phishing Module uses POP3 to connect to the Gmail account of the user to retrieve the desired information (Gmail incidentally supports both POP3 and IMAP4). POP3 works over a TCP/IP connection using TCP on network port 110. Gmail however uses the deprecated alternate-port method, which uses TCP port 995. One of the major disadvantages of using POP3 for mail retrieval is that it does not distinguish between a new message and a message which has already been fetched. As a result every call made to run the application results in it checking the e-mail inbox folder from the very beginning. Although this

does not seem to be much of a problem in case there are a limited number of messages in the user's inbox, the time taken to complete run of the application increases manifold in case there are say a couple of thousand messages in the inbox folder. To get over the problem, this application makes use of the Sent Date field of the e-mail header (POP3 does not support Received Date field). The maximum value of the Sent Date field of all the messages checked is saved by the application and in the next run is starts checking the messages whose Sent Date is 5 days behind this maximum value. This is done because: It might so happen that due to some problem, the mails sent to user's e-mail server get delayed and are not delivered by the time when the application is run. The average life time of a phishing site is 5-6 days. Thus it may safely be assumed that if a mail is sent 5 days back and is yet to be delivered to the user it would have been rendered harmless by the time it arrives in his mailbox. The workflow chart of the application is given in Fig 2.

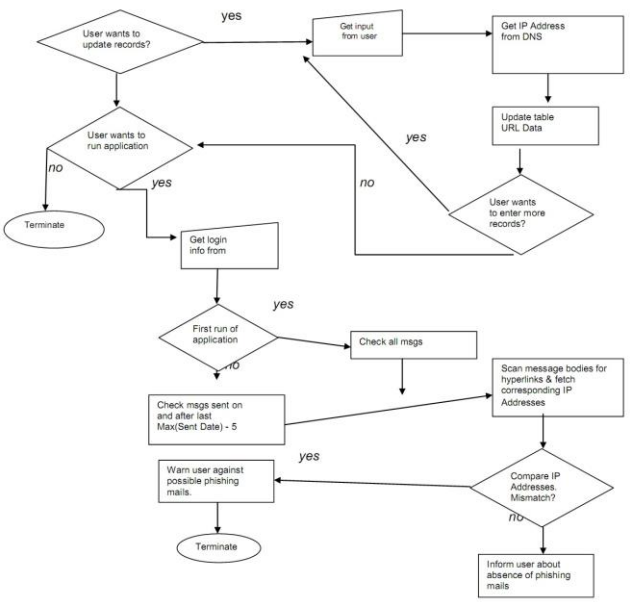


Figure 2. Workflow Chart of the Application

D. Working Example

Suppose a naive user is a customer of Axis Bank and has registered for their online banking services. Also suppose that the said user chooses to use this Anti Phishing application. When the user runs the application for the first time, he is asked to enter the organization's name and its secure URL address (as provide to the user by the bank). Accordingly he enters the bank's name as ICICI bank and the URL as www.icicibank.com. The application now contacts the DNS and retrieves the corresponding IP address which in this case is 210.210.17.218. The MD5 value of this IP address is then calculated and is stored in the database. In the next stage of the application, if the user wants to check his e-mail account, he is asked to provide his username and password to logon to his account. Once connected, the application shortlists the mails to be checked, i.e., either all the mails in the user's inbox (if it the first run of the application) or only those whose sent date is at the most 5 days less than the maximum sent date that was stored when the application was run the last time. The application looks for the substring "icici" in the 'From' header field of the short listed messages.

Let there be a mail from onlineservice@alerts.icici.com with its subject being "IMPORTANT ALERT: Re-Confirm Your Net Banking Details, Update Your Account to Avoid Violation" (refer fig 3).

The message body of this e-mail is scanned for embedded URLs. It should be noted from the phishing e-mail shown in fig 3 that the phisher has tried to hide the identity of the destination URL behind a button titled "Update your account". The trick might fool a naive or even an experienced internet user but

the application's search returns the destination URL as http://www.erainfo.es. The corresponding IP address of this URL is fetched from the DNS and its MD5 value is matched against the value stored in the database provided by the user. A mismatch produces a warning against suspected phishing e-mails (as shown in fig 1 above). The user is thus warned against the existence of likely phishing e-mails in his account even before he physically opens his e-mail service. Forewarned about the same, he is unlikely to fall victim of the phisher's trap set for him.

IV. RELATED WORK

Engin Kirda et. al. [9] have developed an anti-phishing solution called AntiPhish to guard users against a spoofed web site based phishing attack. The tool keeps track of the sensitive information of a user and generates warnings whenever sensitive information is typed on a form generated by a website that is considered untrusted. One of the drawbacks of the solution is that it lets the user go up to a stage where he is allowed to type in sensitive information on a form and then if the tool finds out that the website is untrustworthy; it warns the user against it. The user is thus susceptible to losing his sensitive data if the phisher employs tools such as a key logger or a malware which is programmed to send screenshots of the user's console every few seconds. Neil Chou et. al. [10] have proposed an Anti-Phishing solution named Spoof guard, which is another plug-in solution developed to provide phishing protection to the end user. It uses a symptom based approach to judge whether a website is spoofed or not. The symptoms include similar sounding domain names, embedded obfuscated URL links, etc. Based on the number of symptoms detected, a phishing alert is generated to warn the user. Moher Aburrous et al. [11] have proposed a similar phishing website detection system using fuzzy logic techniques. Fuzzy logic is applied to determine the site status based on 27 parameters which are considered to be the hallmark of phishing sites. These parameters are subdivided into six criteria, (which are further categorized into three layers): URL & Domain identity (Layer 1), Security & Encryption, Source Code & Java Script (Layer 2), Page Style & Contents, Web Address Bar and Social Human Factor (Layer 3). Websites are analyzed based on their overall phishing rating generated and the alert is generated accordingly. Juan Chen et. al. [12] have proposed an algorithm named Link Guard which analyzes the generic characteristics of the hyperlinks in the phishing attacks to deduce whether a site is spoofed or not. The algorithm makes use of a set of rules to analyze the URL viz, mismatch between the actual destination link and the link as seen by the user, use of IP addresses in dotted decimal format, absence of destination information in the text as seen by the user, etc. How our approach differs from the approach suggested in LinkGuard is the fact that our application makes use of user provided data to check the authenticity of the destination URL and hence is able to give a more accurate prediction about the validity of the destination website. Besides latest web browsers come equipped with anti-phishing solutions wherein they maintain a list of black listed sites which are confirmed phishing sites. Every site which the user wishes to open is checked against this list and the operation blocked in case the site appears in the list. This however is, at best, a passive approach against phishing and provides no protection against newly created phishing sites. Also, the quality of protection provided relies heavily on the quality of black list maintained by the browser.

V. CONCLUSION

The specter of online identity threat was never so real as it is today primarily due to rapid growth of the Internet and increase in online trading activities which offer a cost effective method to service providers, such as banks, retailers etc., to reach out to their customers via this medium. This has also provided the phishing community an excellent tool to try and fool the citizens into disclosing sensitive information about their banking accounts, credit cards details, etc. Recent years have witnessed a host of phishing scams with each doing the other in terms of reach to the users and the level of sophistication. Indeed the best measure available against such scams is user awareness. Users should be trained against following blind links and the tendency to part with sensitive information over e-mails which may later cause heavy loss to them. However with the ever increasing reach of the Internet, this in itself is a Herculean task. There is thus a need to develop tools which may be of some assistance to the users in dealing with the menace of phishing. This work to try and develop an Anti-Phishing application for the end user is a small attempt in this direction.

VI .REFERENCES

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

[2] Rachna Dhamija, J.D.Tygar, "The Battle Against Phishing: Dynamic Security Skins" in Proceedings of the symposium on Usable privacy and security, pp. 77-88, yr 2005.

[3] Chenfeng Vincent Zhou, Leckie C., Karunasekara S. and Tao Peng, "A Self-healing, Self-protecting Collaborative Intrusion Detection Architecture to Traceback Fast-flux Phishing Domains" in Networks Operations and Management Symposium (NOMS) Workshops 2008, Salvador, Brazil. IEEE, pp. 321-327, 7-11 Apr 2008.

[4] Gartner Inc., "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks, 2007 Press Release, 17-Dec-2007,"

https://www.gartner.com/it/page.jsp?id=565125.

[5] Dhamija R., Tygar, J.D. and Hearst, M., "Why Phishing Works" in Conference on Human factors in Computing Systems (SIGCHI 2006), Montreal, Canada, pp. 581-590, 22-27 Apr 2006.

[6] SearchSecurity.com Definitions, http://searchsecurity.techtarget.com/dictionary/definition/1005812/attackvector.html

[7] The Honeynet Project & Research Alliance, "Know your Enemy: Phishing". The Honeynet Project & Research Alliance 2005, http://www.honeynet.org/papers/phis-hing/.

[8] Ollmann, G., "The Phishing Guide". NGS Software Insight Security Research 2005, http://www.ngssoftware.com/papers/NISRWPhishing.pdf.

[9] Engin Kirda and Christopher Kruegel, "Protecting Users Against Phishing Attacks" in Computer Software and Applications Conference, 2005 (COMPSAC 2005), Edinburgh, Scotland. 29th Annual International Volume 1,pp. 517 – 524, Issue: 26-28 July 2005.

[10] Neil Chou, Robert Ledesma, Yuka Teraguchi and John C. Mitchell, "Client-Side Defense Against Web-Based Identity Theft" in 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego,February, 2004.

[11] Maher Aburrous, M.A. Hossain, Fadi Thabatah and Keshav Dahal, "Intelligent Phishing Website Detection System using Fuzzy Techniques" in 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008 (ICTTA 2008), pp. 1-6, dt 7-11 Apr 2008.

[12] Juan Chen and Chuanxiong Guo, "Online Detectionand Prevention of Phishing Attacks" in Communications and Networking in China, 2006.