IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Efficient Framework For Internet Banking.

P.Malathi[*1], Dr.P.Vivekanandan[2]
[*1]Research Scholar, CEG Campus, Anna University, Chennai, India
[2]A.C.Tech, Computer centre, Anna University, Chennai, India
malathip2006@gmail.com

Abstract

Detecting and identifying any phishing websites in real-time, particularly for e-banking, is really a complex and dynamic problem involving many factors and criteria. Because of the subjective considerations and the ambiguities involved in the detection, data mining techniques can be an effective tool in assessing and identifying phishing websites for e- banking since it offers a more natural way of dealing with quality factors rather than exact values. This paper presents the authentication environment defined for securing E- Banking applications. The validation model has been designed to be easily applicable with minimum impact to the current Internet banking systems. The key point of this model is the need for multifactor mutual authentication, instead of simply basing the security on the digital certificate of the financial entity, since in many cases users are not able to discern the validity of a certificate, and may not even pay attention to it. By subsequent the rules defined in this proposal, the security level of the Web Banking environment will increase and customers' trust will be enhanced, thus allowing a more beneficial use of this service.

Keywords: OTP(One Time Password), URL(Uniform Resource Locator), CISCO (Chief Information Security Officers), SMS(Short Message Service).

Introduction

E-banking phishing websites are fake websites that are created by malicious people to mimic valid e-banking websites. Most of these kinds of web pages have high visual similarities to scam their victims. Some of these web pages look exactly like the real ones. Unwary Internet users may be easily deceived by this kind of scam. Victims of e-banking phishing websites may expose their bank account, password, credit card number, or other important information to the phishing web page owners. The impact is the breach of information security through the compromise of confidential data, and the victims may finally suffer losses of money or other kinds. Phishing is a relatively new Internet crime in comparison with other forms, e.g., virus and hacking. E- banking phishing website is a very complex issue to understand and to analyze, since it is joining technical and social problem with each other for which there is no known single silver bullet to entirely solve it. The motivation behind this study is to create a resilient and effective method that uses fuzzy data mining algorithms and tools to detect e-banking phishing websites in an automated manner.

One may receive an e-mail from his/her credit card company informing that his/her account has been deactivated because of suspicious activity. The message requests the person to click a web link and log in to verify his/her account information. Following the instructions, the persons are directed to what appears to be the "Online Update" page of his/her credit card company. Here the person is asked to enter his name, password, account number, social security number, and PIN. It all seems legitimate: the logos look proper, the web address of the page looks convincing, and the format of the site is the same as he remembers. However, this is a scam; the e-mail is a fraud, and now a cyber-criminal has his/her personal information. He or she can now use or change the person account or open new accounts in your name. You have become a victim of a growing crime called phishing.

Cyber- thieves are using these same systems to manipulate us and steal our private information; they take advantage of people's trusting nature, or, in some cases, their naiveté. In this analysis we will be explain the concepts and technology behind phishing, show how the threat is much more than just a nuisance or passing trend, and discuss how gangs of criminals are using these scams to make a great deal of money.

Related Work For Internet Banking

If compared with other expense channels, the Internet affords many advantages to both banks and customers, particularly in terms of its low cost, ease of access in terms of time and space, ease and user control. Accordingly, banks have increased investments in Internet banking services and reduced the number of branch offices and payment automated teller machines (ATMs). This has encouraged better service offerings to a growing customer base with a preference for Internet banking applications.

Despite Internet banking's fast growth and improved, local banks are still mandatory to maintain a wide network of physical bank branches and ATMs in spite of the intrinsic low cost advantages of Internet banking transactions. This is mainly due to the conflict of assured segments of users in adopting Internet banking due to a wide array of issues and barriers which are not properly identified by industry players. At the same time as the literature is flooded with studies on user adoption of technologies such as Internet banking, studies that focus on user resistance or refusal of technical innovations are limited.

E-Banking Fraud System:

Most online banking fraud schemes involve two steps. First, the criminal obtains the customer's account access data, i.e. logon name and password. Second, the criminal uses this information to transfer money to other accounts and withdrawals the funds. For the first step, criminals have employed different schemes in the past:

The "over the shoulder looking" scheme occurs when a customer performs financial transactions while being observed by a criminal. A fair number of cases have been reported where customer's account access data was obtained by the criminal just by observing customers at a public Internet access point. The "phishing" scheme involves using fake emails and/or fake websites. The word "phishing" stems from combining the words "password" and "fishing". Criminals send emails that appear to be from the customer's bank that direct customers to a fake website. This website impersonates the bank's website and prompts customers for their account access data. Over the past months, most banks have executed customer education programs, thereby reducing the effectiveness of this scheme. It will, however, take awhile before all customers are smart enough to extinct phishing.

Implementation of An Anti-Phishing System

To overcome the above problems, we can identify Phishers strive to mimic web pages of most well-known international banks, economic organizations, or other brands, because unwary online users may be easily scammed by these fake web pages. This motivates us to develop detection tools to protect the legitimate web pages from being frequently attacked. In this way, the web page that is designed for customers or users to access needs to be examined by matching the restored legitimate web pages. For example, a customer may usually use "eBay" to do shopping. Thus, we need protect the user from being phished by comparing the content of the given web pages with that of the real "eBay" web page. If both two web pages exhibit highly matched content, we claim the given web page is phishing. We can integrate our solution into a browser plug-in for the user to maintain and protect a list of frequently used web pages that need high security attention. Another alternative approach is to provide a class library application programming interfaces (APIs) for enterprises that build their own anti-phishing systems for detecting suspicious web pages. For example, "eBay" probably only cares about their own site, so it makes sense for them to detect fake versions of their own brand. On the other hand, our proposed approach is easy to be embedded into the current anti-phishing system. Since almost all phishings start from sending phishing emails to Internet users who are deceived by this kind of e-mails to access their fake web site and results in exposing their personal information, we can build an anti-phishing engine into the anti-phishing proxy to keep the phishing characteristics updated from the anti-phishing database server so as to filter all traffic going through the email server. The anti-phishing database server is the center for registration of legitimate web sites that need protection. The registered legitimate web pages are preprocessed in advance. Their content features and historical anti-phishing statistics are extracted from the pages and saved in the database such that this design makes the system efficient and scalable. The overall implementation of such an anti-phishing system can be found in.

Improving Security for Online Banking:

If any person is an Internet Banking user, he/she probably is aware of phishing. Statistics indicate that more than 1000 phishing attacks are launched every month. To minimize impact of phishing attacks we need to look at protection, detection and response measures. Some measures to explore include:

1. What can we do to save my users from falling wounded to phishers ? [safeguard]

2. How do we identify when a phisher is building a false website and communicating to users? [recognition]
3. What can we do to decrease the impact once a successful phish has been launched? [Response]

Anti-phishing measures:

a) Improving Site Authenticity:

The source of the phishing problem is that users are not proficient to recognize if the website is original or fake.

Looking at the URL and SSL certificate carefully can really help but not all users have the time or technological ability to analyze and make the correct decision.

One method is to personalize the login page for each user. We do the login in two stages. First the user enters only the user-id and not the password. Once user-id is submitted, server returns a page where user gets to see an image which he had selected at time of registration. If the image is matching, he supplies the password and all is fine. If the image is not being showing, it raises an alert and customer does not provide the password. Phisher doesn't know which image to show in this middle page. Yes it depends on user being alert. Can a phisher setup a phishing site that acts like a man-in-the-middle- intercept the user-id , send to original site and fetch the image, send image back to user and get the password. Yes, it is technically possible.

b) One-time passwords

The user requires a login-id/static password [often called PIN] and a dynamic one time password for successful login. This one time password is generated on hardware token [or software token] provided to each user. These tokens automatically generate a new one-time-password every 60 seconds.

We are not fighting the actual problem here. Users will still get tricked into providing their passwords at the phishing site. But these passwords are only valid for 60 seconds. If the phisher is not able to use it in near-real-time [within 60 seconds] the stolen password is useless. However, as was proven recently, phishers are getting more real-time.

Alternatively, instead of supplying tokens to users, the server can generate the one-time password. Once the login/static- password is validated the one time password can be generated by server and SMSed to user's cell phone. This virtually prevents phishing attacks because attackers can never receive this SMS.

c) Having separate login and transaction password

This will make sure that even if login password is lost to
phisher, transactions cannot be made.

Again we are not saving the users from being victims of phishing. We are just ensuring that even if the login password is lost, attacker can login and see the account details but cannot do rather like a fund transfer without knowing the transaction password. If the user has kept both passwords the same then there is no protection at all. Instead a onetime transaction password can also be generated dynamically by server and SMSed to user.

A. Transaction Specific One-Time Passwords

The shortcoming of both paper OTP lists and hardware tokens lies in the fact that each OTP is not transaction specific. That is, the same OTP can be used to verify either a genuine or a fraudulent transaction. One possible way to come by this flaw is to use a "key generator" device that generates an OTP based on primary transaction parameters.

A key generator looks similar to a pocket calculator. It has a keypad that lets the customer enter the source account, target account, transaction amount, and a PIN. Based on these parameters, the key generator generates a transaction specific OTP. The customer now enters the transaction parameters into the online banking application including the generated OTP. When the online transaction is received by the bank's server, it performs the same calculations as the key generator and thus verifies the OTP. If a criminal captures such an OTP, he cannot use it for a fraudulent transaction, since this OTP can only be used to verify a transaction with the same parameters as entered on the key generator. Because the key generator is a separate hardware device with no connection to the Internet, it is immune to getting attacked by malicious software.

For these reasons, key generators can be considered a highly effective fraud prevention measure for online banking capable of preventing all known fraud schemes. The disadvantages of key generators are, however, the cost of the device, the fact that the device must be physically present to perform online banking, and the fact that the customer basically has to enter each transaction two times.

B. OTP by SMS

Some of the disadvantages of using key generators are avoided by sending OTPs to the customer using SMS. With this approach, the customer first sends the complete transaction to the bank's server. The bank's server then creates a random number as OTP and sends it to the customer's mobile phone as text message. The customer now enters this transaction specific OTP into the online banking application, and sends it also to the bank's server. If the generated OTP matches the one transmitted by the customer, the transaction is verified.

Because the OTP transmitted can only be used to verify the transaction that is already received by the bank's server and cannot be altered from the outside, this OTP is of no use to a criminal. In theory, sending OTPs by SMS should hence be as effective a fraud prevention measure as a key generator. In reality, banks have experienced that the weak point is the mobile phone identification. Effective fraud prevention is only provided if any change of mobile phone number is performed only after thorough identity checking.

Another disadvantage of this approach is that banks need to tie in their infrastructure with the infrastructure of a wireless operator. Wireless operators all over the world are investigating ways to leverage their existing infrastructure into new sources of profit. Most operators hence look into providing financial transaction services of various kinds.

Banks hence may soon find themselves in a situation, where

wireless operators offer their customers financial transactions using just the mobile phone and nothing else. The bank's offering would involve using first an Internet browser, then wait for an SMS, read it, go back to the Internet browser, type in the OTP and erase the SMS. For a customer, the bank's offering appeals to be a lot more complex than the wireless operator's offering.

C. Transaction Monitoring

A completely different approach to secure online banking comes from the adaptation of fraud prevention systems used with credit card and debit card processing. In payment card processing, fraud is a known phenomenon since many years. Technical security measures introduced to payment cards, such as magnetic stripes or chips, have only provided temporary relief from fraud losses.

The only measure that has proved to limit fraud losses permanently was the deployment of transaction monitoring software. This has become the de-facto standard for fraud prevention with payment card processing worldwide. Transaction monitoring occurs in the bank's data centre. For each transaction, the transaction monitoring software scrutinizes the current transaction's parameters, and compares it with the previous transaction of both the customer and the counterparty of the transaction histories. By comparing the current transaction pattern to stored known fraud patterns, the software can flag suspicious transactions "on the fly". Such transactions are then referred to a call centre for manual verification.

D. Comparison

But what are the disadvantages of transaction monitoring? One problem arises when a new fraud pattern emerges, which is not stored in the transaction monitoring software. Another problem arises when by accident the current genuine transaction patterns resemble a known fraud pattern so much that the transaction monitoring system refers the genuine transaction to the call centre.

The first problem exists with any fraud prevention measure. Once criminals find a way to circumvent the measure, the door to fraud is open. The question becomes what can be done in this case. If the fraud prevention measure involves devices that are distributed to the customers, fixing the security problem becomes difficult. When the French credit card chip system was hacked, retrofitting point of sales terminals to patch up security was estimated to cost 5 billion U.S. dollars. Transaction monitoring provides a significant advantage in this case because it is centralized. By adding the new fraud pattern to the fraud detection logic in the bank's data centre, the entire system becomes instantly "immunized".

The second problem also occurs with any fraud prevention measure. Any measure will impose a certain customer disturbance. Smart cards and USB tokens may cause trouble when their hardware driver becomes incompatible with any change of the customer's PC. And like hardware tokens and key generators, all extra electronic devices have certain likelihood to fail or get lost. OTPs send by SMS may get lost or delayed, in particular with International roaming. Transaction monitoring software will inevitable generate a certain rate of false alarms. Banks must carefully determine which level of customer disturbance they consider acceptable for the security level needed.

Should we implement all of these?

This is the predicament we face with most of safety technologies. Several recent surveys indicate that lack of

security is leading to loss of customer confidence in Internet commerce. Users want appropriate security controls in place even if it means carrying a password token or getting their passwords on SMS. Today phishing is familiar by users as a

real and potentially harmful threat. If we do not put in place

suitable anti-phishing controls our customers might go elsewhere to do business.

Overview of Our Framework

As a rule, banks have now started issuing instructions on their website about the dos and don’ts of Internet banking and have also started mailing customers on the necessary precautions that need to be taken to secure their financial information.

Banks are also taking the initiative to remind customers to update their anti-virus software and browser application, so that their PCs do not support any back door entries and Spyware installations. They have also initiated a 24-hour customer response team where customers can report any form of identity theft or account discrepancies. Presently, many leading banks have appointed agencies to carry out a 24X7 monitoring of the Internet, activities on the banks website and also the profile of the users and nature of their transactions at any given time. In addition, most banks have been partnering with law and enforcement agencies and organizations such as CERT-IN to shutdown spoofed sites quickly.

Public as well as private banks have started implementing dual factor or second factor authentication, 128- bit SSL (secure socket layer) encryption, scrambled keyboard, adding multiple layers of security which helps a user identify a fake website and not divulge his credentials.

Almost all banks today send out post transaction alerts to customers on their mobile and Email id, so that the customer response time is quick and any illegal transactions can be reported quickly. The post transaction alerts sent to customers is directly monitored by the risk management team.

Another key development is that banks have appointed Chief Information Security Officers (CISO) to manage all the security concerns within the bank. The CISO leads a team dedicated only to security and functions separately from the central IT team.

According to more than 57% of the banks still do not have a dedicated budget for online security, choosing instead to include online security as part of their overall IT budget. However, the appointing of CISOs is slated to reverse this trend going forward.

Though banks have been the pioneers in embracing the latest of technologies and have constantly been scaling up their security procedures, vulnerability to hackers remain. Threats are evolving and becoming more dynamic with the increasing number of customer touch points and delivery mechanisms.

Hence, phishing can no longer be handled by a technology solution alone. Banks have to put in place the right blend of technology, policy guidelines, and user awareness to keep pace with the increasing sophistication with which fraudsters operate.

Anti Phishing

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 and filter various types of phishing attacks. In general, anti-phishing techniques can be classified into following four categories.

Content Filtering- In this methodology Content/email are filtered as it enters in the victim's mail box using machine learning methods, such as Bayesian Additive Regression Trees (BART) or Support Vector Machines (SVM).

Black Listing- Blacklist is collection of known phishing Web sites/addresses published by trusted entities like google's and Microsoft's black list. It requires both a client and a server component. The client component is implemented as either an email or browser plug-in that interacts with a server component, which in this case is a public Web site that provides a list of known phishing sites.

Symptom-Based Prevention- It analyses the content of each Web page the user visits and generates phishing alerts according to the type and number of symptoms detected.

Domain Binding- It is a client's browser based techniques where sensitive information (eg. name, password) is bind to a particular domains. It warns the user when he visits a domain to which user credential is not bind.

Anti-Phishing Techniques

Attribute based anti-phishing techniques:

It implements both reactive and proactive anti-phishing defenses. This technique has been implemented in Phish Bouncer tool. The various checks that phish bouncer does has been shown in figure 5.

The Image Attribution does a comparison of images of visiting site and the sites already registered with phish bouncer. The HTML Crosslink check looks at responses from nonregistered sites and counts the number of links the page has to any of the registered sites. A high number of cross- links is indicative of a phishing site. In false info feeder check, false information is input and if that information is accepted by site then it is probable that link is phished one. The Certificate Suspicious check validatessite certificates presented during SSL handshake and extends the typical usage by looking for Certification Authority (CA) consistency over time.URL suspicious check uses characteristics of the URL to identify phishing sites.

Advantage: As attribute based anti-phishing considers a lot of checks so it is able to detect more phished sites than other approaches. It can detect known as well as unknown attacks.

Disadvantage: As multiple checks perform to authenticate site this could result in slow response time.

Genetic Algorithm Based Anti Phishing Techniques:

It is an approach of detection of phishing web pages using genetic algorithm. Genetic algorithms can be used to evolve simple rules for preventing phishing attacks. These rules are used to differentiate normal website from anomalous website. These anomalous websites refer to events with probability of phishing attacks. The rules stored in the rule base are usually in the following form

if { condition } then { act }

For example, a rule can be defined as:

If { The IP address of the URL in the received e-mail finds any match in the Ruleset }
Then
{ Phishing e-mail
}

This rule can be explained as: if there exists an IP address of the URL in e-mail and it does not match the defined Rule Set for White List then the received mail is a phishing mail.

Advantage: It provides the feature of malicious status notification before the user reads the mail. It also provides malicious web link detection in addition of phishing detection.

Disadvantage: Single rule for phishing detection like in case of url is far from enough, so we need multiple rule set for only one type of url based phishing detection. Likewise for other parameter we need to write other rule this leads to more complex algorithm.

Character Based Anti Phishing Approach:

Many time phishers tries to steal information of users by convincing them to click on the hyperlink that they embed into phishing email. A hyperlink has a structure as follows.

<ahref="URI"> Anchor text <\a> where 'URI' (universal resource identifiers) provides the actual link where the user will be directed and 'Anchor text' is the text that will be displayed in user's Web browser and represents the visual link. Character nbased ant phishing technique uses characteristics of hyperlink in order to detect phishing links. Link guard [6] is a tool that implements this technique. After analyzing many phishing websites, the hyperlinks can be classified into various categories as shown in fig 6. For detection of phishing sites Link Guard, first extracts the DNS names from the actual and the visual links and then compares the actual and visual DNS names, if these names are not the same, then it is phishing of category 1 If dotted decimal IP address is directly used in actual DNS, it is then a possible phishing attack of category 2.

If the actual link or the visual link is encoded, then first the link is decoded and then analyzed. When there is no destination information (DNS name or dotted IP address) in the visual link then the hyperlink is analyzed. During analysis DNS name is searched in blacklist and white list .if it is present in white list 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.

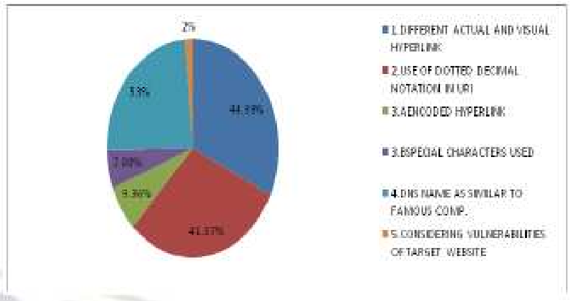

Fig 1: Linkgaurd Analysis In Various Classified Hyperlinks

If the actual dns is not contained in either white list or blacklist, Pattern Matching is done. During pattern matching first the sender email address is extracted and then it is searched in seed set where a list of address is maintained that are manually visited by the user. Similarity checks the maximum likelihood of actual DNS and the DNS names in seed-set.the similarity index between two strings are determined by calculating the minimal number of changes needed to transform a string to the other string.

Advantage: it cannot only detect known attacks, but also is effective to the unknown ones. Experiments showed that Link Guard, can detect up to 96% unknown phishing attacks in real- time. For phishing attacks of category 1, it is sure that there is no false positive or false negatives .Link Guard handles categories 3 and 4 correctly since the encoded links are first decoded before further analysis.

Disadvantage: For category 2, Link Guard may result in false positives, since using dotted decimal IP addresses instead of domain names may be desirable in some special circumstances.

Conclusion

Phishing is the major drawback in the use of Internet banking transactions. Detection of phishing is very difficult one; we are using Attribute based Anti-phishing is used and it detects the known and unknown phishing attacks. Attribute based anti-phishing handles with lot of checks, which lead to delay in response time. In genetic algorithm based

Anti- phishing, we use multiple algorithm for detecting phishing and malicious web link. The usage of multiple algorithm will leads to error in detecting the phishing. In Character based Anti- phishing we use Link Guard algorithm for detecting the phishing, but the usage of the algorithm will change the URL. To improve the detection of phishing website and minimize the response time, the number of algorithms must be reduced, to stop modifying URL

References

[1] Alnajim A, Munro M. An evaluation of users' tips effectiveness for phishing websites detection, 978-1-4244- 2917-2/08, IEEE; 2008. p. 63–68.

[2] APWG. Phishing activity trends report.2005. http://antiphishing. org/reports/apwg_report_DEC2005_FINA pdf. Accessed 12 Apr 2007.

[3] APWG. Phishing activity trends report. 2008.http://antiphishing.org/reports/apwg_report_sep2008_final.pdf Accessed 9 March2009.

[4] Proceeding of the 11th annual Network and Distributed System Security Symposium (NDSS '04); 2004.

[5] Dhamija R, Tygar J. The battle against phishing: dynamic security skins. In: Proceedings of ACM Symposium on Usable Security and Privacy (SOUPS 2005); 2005. p. 77–88.

[6] Dhamija R, Tygar J, Marti H. Why phishing works. In: CHI '06: Proceedings of the SIGCHI conference on human factors in computing systems. ACM Press, New York; 2006. p. 581– 590.

[7] FDIC. Putting an end to account-hijacking identity theft, FDIC, Technical Report [Online]. 2004. Available: http://www.fdic.gov/consumers/consumer/idtheftstudy/identitytheft.pdf. Accessed 18Apr 2007.

[8] Anti-Phishing Working Group. Phishing Activity Trends Report. June, 2006. http://www.antiphishing.org/reports/apwg_report_june_06.pdf

[9] CallingID, Ltd. Accessed: December 1, 2006. http://www.callingid.com/DesktopSolutions/CallingIDT oolbar.aspx

[10] Chou, Neil, Robert Ledesma, Yuka Teraguchi, Dan Boneh and John C. Mitchell, "Client-Side Defense against Web-Based Identity Theft," in Proceedings of The 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego, CA February, 2004. http://crypto.stanford.edu/SpoofGuard/webspoof.pdf.

[11] Cloudmark, Inc. Accessed: September 5, 2006.http://www.cloudmark.com/desktop/download/.

[12] Computer Crime Research Center. "Netscape: Anti-Phishing Bundled." February 2, 2005. Accessed: November 9, 2006. http://www.crimeresearch. org/news/02.02.2005/938/.

[13] APWG.2009. http://www.apwg.org/reports/APWG_GlobalPhishing Survey_1H2009.pdf. Accessed 8 Aug 2009.

[14] Brooks J. Anti-phishing best practices: keys to aggressively and effectively protecting your organization from phishing attacks, White Paper, Cyveillance; 2006.

[15] Business Security Guidance. How to protect insiders from social engineering threats. 2006. www.microsoft.com/technet/security/ default.mspx. Accessed 8 Ap 2006.

[16] Chou N, Ledesma R, Teraguchi Y, Boneh D, Mitchell J. Client side defense against web-based identity theft. In: