

Phishing Attack Prevention using Site Privileges

Ramesh R

*Department of Information Technology
Adi Shankara Institute of Engineering and Technology
Kalady, Ernakulam, Kerala, India*

Divya G

*Department of Information Technology
Adi Shankara Institute of Engineering and Technology
Kalady, Ernakulam, Kerala, India*

Abstract

Phishing attacks can be mitigated effectively by utilizing the existing services offered by websites in the form of referrals. Phishing attack prevention methods are so far based upon browser integrated third party software. Our proposed methodology effectively provides clients willing to access financial websites an indirect path to their target site securely.

Keywords: Referral; Phishing

I. INTRODUCTION

It is important to know that the phisher who has sent the email in the first place is after your personal information in order to use it for fraudulent purposes. Emails are not the most secure form of communication available for people to use on the Internet. Certainly many scammers are quite capable of producing an email that looks legitimate and so will be easily able to forge such a document and then gain your information in this way.

If you do have to transmit any personal information over the Internet then ensure that the site you are providing it to is completely secure. The best way for a person to identify if a site is secure or not is by looking at the site address. All sites which are considered to be secure should start with “https://” and not “http://”. Also if you look in the browser status bar you will see the lock icon being displayed. In fact in recent months there has been an increase in the number of phishing emails and instant messages being sent to people so that the scammers can gain their personal details relating to their credit card or bank accounts. Normally most phishing attacks use a spoof email or instant message which, when you look at it, appears to have come from a legitimate source that you already have dealings with online. Generally they will send it either from your bank, credit card or a site which requires you to provide them with personal details or you have an account with them. This includes such sites as eBay, Amazon and PayPal. In the message that you receive you will find that they are asking you to respond to their message and to provide them with your personal account details in order that they can update their files or update security measures. However what in fact you are doing is providing the scammer with your personal details which they can then put to fraudulent use. Instead, what you need to do rather than clicking on the link that is provided within the email or message that has been sent to you, type in the website’s URL directly on to the computer yourself. This should be the url of the correct website that the email or message seems to have been sent from. Most phishers today will have a link within their email that is very similar to the address that you would normally use in order to gain access to your bank, credit card or other online account. If you look closely, you just might see that the url linked within the email is actually not the correct url for your bank or whatever.

Today bank phishing scams are becoming ever more sophisticated. In recent months, phishers have been able to gain access using a genuine domain name to set up a website which people are then going to because they believe it to be a real bank.

In another phishing scam relating to banks, an email will be sent to the bank’s clients whom they think is from the bank. It then asks them to verify their phone number with them and they are asked to call a specific telephone number. However what the customer does not realize is that as soon as they call the number they are then redirected to a number in another country. Once connected to the number the scammer now has access to all incoming calls to that person’s phone and the victim will not realize anything has occurred until they find that their phone service becomes suspended. Plus using this method the scammer is also able to contact the person back to inform them that their account details have been verified which makes the scam seem even more legitimate.

Most of the anti-phishing mechanisms necessitate us to install a third party toolbar software or browser controlled plug-in. Each methodology has its own drawbacks which clearly show that not all phishing attacks can be prevented. This indeed creates a sense of insecurity in users for using online banking system. Online banking is not a new buzz word for computer enthusiasts like us but it is indeed a new thing for users who actually started using Internet and unaware about phishing attacks, even not necessitating for the creation of similar looking websites for stealing user information. We are proposing an idea that can be implemented in web search sites like Google as a way to attract new users apart from users willing to join social networking or other fun related sites. The idea is to implement a tool in web search engines with the help of a centralized database system that can be used to mitigate phishing attacks. This centralized system can provide a secure way to perform online banking transactions. This method will not require installing any anti-phishing software in the user’s side. The entire security system is going to be implemented at source server itself. Anti-phishing attacks are normally handled using inbuilt tools used in Internet browsers or by installing other toolbars integrated with the web browser. There are several approaches available to avert phishing attacks.

II. RELATED WORKS

A. What Is Anti Phishing Software?

All anti phishing software is made up of computer programs which will attempt to identify the phishing content that may be contained in a website or email that has been sent to you. This software is normally to be found as an integrated tool within web browsers and email servers and will display the real name of the domain for the website that you are visiting. In doing this it is hoped it will prevent sites which are fraudulent from being able to masquerade as ones that are actually legitimate. Today such a function may well be included as a built in feature of a lot of web browsers.

If you are looking for a web browser which has anti phishing software as an integral tool within its system then you should look at installing such ones as follows:

- Microsoft Windows Internet Explorer v 7.
- Firefox v 2.0.0.4.
- Google Safe Browsing (which can be used with Firefox).

All of these are highly effective in helping to prevent you from becoming another victim of this latest trend in people obtaining your personal information fraudulently to then use it for criminal purposes.

However if you are looking for a software program that is completely free but acts like a firewall for websites and will help to protect you from any kind of online attack then you may want to consider downloading FraudEliminator. This software has been developed in order to provide you with comprehensive protection while you are using the internet in your home from any kind of online fraud scheme or phishing attack.

This particular anti phishing software package when downloaded installs a toolbar that then protects you by automatically identifying and blocking anything that is considered to be online fraud. Also it provides you with the chance to fight back against what has occurred by allowing you to report the incident to company who developed the software at their central database. But not only is it helping to protect you from fraud schemes and phishing attacks, you will find that it comes with other toolbar functions that we all require today. These include capabilities to search for information as well as a protection system to protect the user against pop ups which they can configure to their own particular requirements. However the biggest advantage to this particular software package compared to all the others on the market today is that this one will actually identify the country where every website that you look at has originated from. When browsing the net it compares each website that you view against their list of URLs which might be either phishing websites or sites which have been hacked. Plus each hour you will discover that the software contacts the company's main database in order to update the blocked list so you know that you are constantly being protected against any possible scams in the future. Thus you have several different anti phishing software programs to choose from.

However there are several anti-phishing tools a person can now use in order to help prevent such attacks from occurring in the future. Below we will be taking a closer look at just what some of these are.

- 1) PhishTank SiteChecker This tool blocks any phishing websites whose details are held by the PhishTank Community. Should you unexpectedly visit a website that is known to PhishTank then the SiteChecker displays a page stating that this site has been blocked rather than actually displaying it. This anti phishing tool can easily be downloaded on to your PC.
- 2) Google Safe Browsing This tool will alert the user when the page that they are visiting is requesting personal or financial information under what it considers to be false pretences. It uses a combination of advanced algorithms as well as reports that have been provided to it regarding pages which are misleading and will usually be able to inform the user automatically that they have gained access to a site which is trying to gain their personal or financial information in a fraudulent way. Again this particular tool can be downloaded directly from the internet on to your PC.
- 3) WOT This particular tool allows the user to ensure that they steer well clear of fraudulent and phishing websites by letting you see what the reputation of the website is like through your browser. By being able to see what kind of reputation a site has, a person is then better able to distinguish a legitimate site from one which is phishing. All the testimonies that are contained within this site have been provided by people who have become part of the WOT community and are looking for ways to prevent other people from becoming victims of those sites that perpetrate such scams. All throughout the paper target server means the banking website the user willing to access and source server means the website that offers the anti-phishing service.

Using the proposed system we can abate Phishing attacks [5] in financial net-banking segment. Existing anti-phishing methods includes Blacklist, heuristic detection (Spoof Guard [13]), the page similarity assessment etc. All have their own short comings. Blacklist is actually Google toolbar integrated software which can be made active within the web browser for providing security from phishing attacks. By using this method instead of installing third party programs for Phishing attack security, we can have a centralized program in source servers for averting such attacks. So financial institutions can make use of this referral service in order to constantly inform registered source servers about the changes in IP addresses. So initially clients after getting authentication details from their respective bank, they can use anyone of the source servers registered with the bank for getting privilege channel. This method provides security to clients from phishing attacks. The overhead that the source servers bear can be compensated by making clients register at the particular source server in order to enable the service.

III. DESIGN

PRS (Persistent Referral Service) can be used to implement an architecture using popular search engines like Google, Yahoo etc, such that sites can register with these search sites on contract basis. These search engines provides a privilege channel to target web server for valid clients only.

The proposed system mainly focuses on providing valid clients a privilege or reliable service channel to target server through search sites. The client after authenticating with the particular search site gets referral service to other valid registered sites. When the client search for the target site, normal search results will be displayed. Whenever the client clicks on the target site's URL, search engine performs a validation check of that particular target website. If it is a registered site, depending upon the privilege of valid client, a privilege URL (containing the capability token) will be generated at the target server and will be forwarded to the source server requesting service and using meta-refresh redirection command, browser will be redirected to target website. If the clicked target server is not registered, then a normal hyperlink will be provided.

The target web servers in need of this service have to register with the search engines or other social networking websites. Since this is a value added service, contracts similar to ad-click service like Google ads can be offered. The main security issue for target servers is to protect their port number from being identified. Here the search engines are referred as Source servers. A small program at the source server calculates the privilege level of valid clients depending on several factors like account access rate by viewing his/her login information , then checking number of emails sent or received, number of linked email accounts etc. We have come-up with a solution, which not only eliminates client-side modifications, but also consider normal users for establishing privilege channel. That is the proposed method is implemented within source site, third party server and target site.

In the initial design, the automatic referral calculator was invoked only at search time. But this method can be improved by reducing the background programming overhead while searching, by providing an option of enabling or disabling referrals from the settings option. Whenever referral service from settings is enabled, the referral level is automatically calculated from his/her social behaviour. The activities of the user automatically update the privilege level. This way we can reduce the overhead at runtime for the calculation of privilege level.

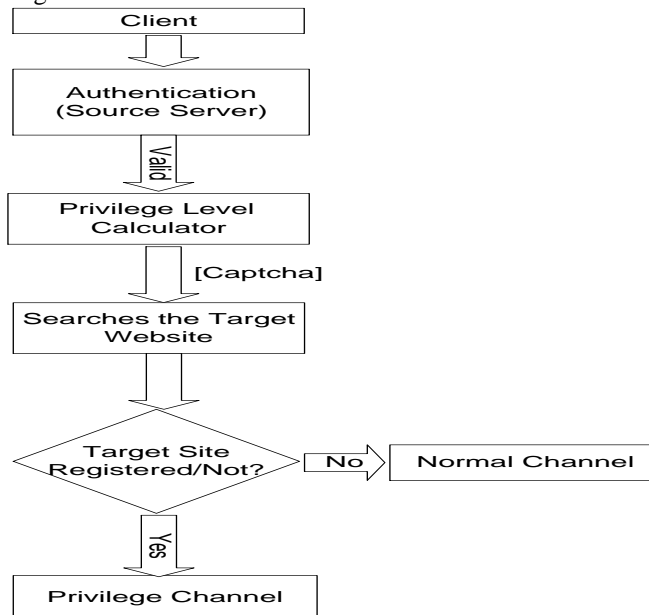


Fig. 2: Referral service

In order to prevent new users from misusing PRS system to launch DDoS attack against a registered site, we are using one Captcha test [12] for getting the search page. So that even if numerous users try to create new accounts and launch DDoS attack, Captcha test will further delay the propagation of packets from individual requests. Hence DDoS attacks by creating newer accounts can be prevented.

Each site uses different parameters for calculating the privilege level. Facebook may take factors like number of pictures, number of friends in his/her network, his/her normal interaction within the site (activity pattern) etc. yahoo may use factors like number of valid mails received or sent, number of friends, linking accounts etc.

IV. PRIVILEGE LEVEL ESTIMATOR

In today's World Wide Web, features of one site differ from another considerably. As such the methodologies employed in the calculation of privilege levels by the respective source servers also differ. In this paper, we assume the source server to be

Google. Google is one of the best and popular search engines presently outshining all other search engines which is evident from its huge share in the advertisement business in the Internet. Also the widely accepted social networking site presently is Facebook.com which has around 750 million registered users. Then Twitter.com which is the best in the blogging segment of the Internet. All these sites produces considerable traffic and in order to protect their reputation, these sites not only offers uninterrupted 24X7 service but also ensures users, the best serviceability in terms of speed while offering referral and other services to neighboring sites.

If the privilege level is calculated by the respective source servers only, a problem may arise. If the user is going to search for a referral service from Google without a valid Google account then the service will not be available. In order to avoid this scenario, we have come up with an idea of integrating account verification of popular websites. This feature is already in use in Yahoo.com, as it can verify account information of user’s Google, Facebook, and Twitter as well as all popular sites and can display their respective inbox or front page in the same webpage itself. In India, Yahoo.com has its reputation for having millions of members registered. Also Yahoo.com is widely used in India along with Google, Facebook, and Twitter etc. The notable features of Yahoo are news presentation, sports-cricket related information etc.

We can see in detail how various sites calculate privilege level based on user’s social interaction. Google.com is one of the popular search engines used globally. It offers Gmail email service, Youtube video service, Orkut social networking service etc. Orkut and Gmail service uses same account verification in Google. Notable features taken into account for the formulation of privilege level are linked email accounts, number of valid email accounts in the contact list, frequency of emails sent or received per week, number of friends in the friends list of Orkut service and chat service etc. So privilege level is estimated by properly taking into consideration of the above features. Facebook can use features like number of friends in the friends-list or number of neighbors in any of the social networking game, number of people tagged on the user’s picture etc. In Twitter, most notable features are number of people following the user, number of people followed by this user, number of friends etc. All these websites can integrate their service in providing privilege level of users by authenticating the accounts. As such, a Facebook user not having a Google account can login to Facebook from Google itself and get his/her privilege level.

But there arise another concern. Privilege level calculated from these websites differs. We are using a range for privilege level from 0 to 10. Level-0 means the user have no valid account or the account was newly created. Highest level-10 indicates the user is having high privilege level. But in order to make the range in more general format, 3-level range can be employed-Low, Medium and High. Low level range includes privilege levels 1 and 2, medium level range includes privilege levels 3, 4, 5 and 6 and finally privilege levels 7, 8, 9 and 10 included in high level. So depending upon different levels, separate privilege channel can be allocated. We will be using 2 bits for representing the privilege level, and the privilege level is meaningful only if the target or searched site is registered with the source site. If the target is not registered with the source site, it is denoted as 00. Then low, medium and high privilege level is represented as 01, 10 and 11 respectively.

But even after generalizing the privilege levels, again their do exist some vital information ie; the social behaviour within the target website to which the user may be willing to get privilege service. Users not, at all times may be having accounts in the target website, in that case above discussions are meant to provide such users privilege service from source search or social networking website to the target website. But if the user is indeed a valid account holder of the target site, his/her privilege level from target server should also be taken into consideration.

V. PROPOSED ALGORITHM

In our proposed method, we are implementing a centralized system at a server which provides the user interface for inputting the target URL. If the user needs anti-phishing mechanism, he/she can enable the option in the settings. After enabling this option, the user will be requested to enter the URLs of his/her banking websites. The URLs entered will be checked by a centralized database and the IP address of each of the mentioned bank websites will be checked. In future if the user wants to visit his account in bank website, he can login to his personal account in the source server first (which offers the anti-phishing service), then the user selects the target site link from the list of websites he had already mentioned.

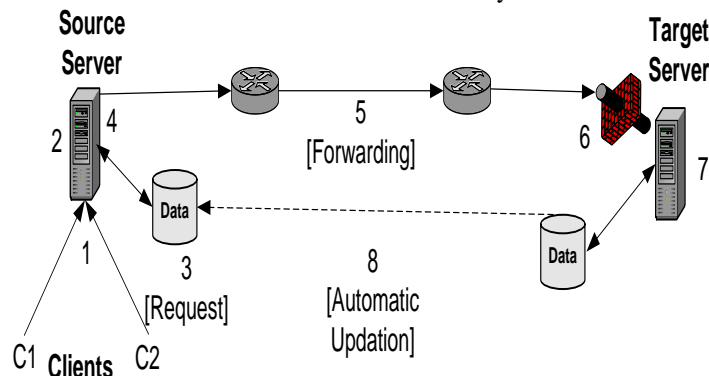


Fig. 3: Referral service

VI. LIMITATIONS

Firstly, users having no valid accounts in a particular search site will not get privilege service. This can be sorted out by embedding features like integrated account verification from other websites and obtaining privilege level from that website. Secondly compromised normal users should be properly dealt with. For this their social behavior parameters like number of valid emails in inbox, number of valid emails address in contacts, period of existence of mail, activity behavior etc. should be properly studied and privilege level should be estimated with at most care as privilege parameters differ from site to site.

VII. CONCLUSION

We are considering a method for providing normal web surfing users a chance to get privilege channel service using PRS. The user's validity is checked by authenticating websites which in turn provide the valid users a privilege channel to target websites. The privilege level of the valid user is cautiously calculated by taking into account his/her social behaviour. So by effectively implementing this system in existing social networking and search engines, clients will be given privilege channel service even when target website is under DDoS attacks. Hence we can improve the serviceability of web servers even under DDoS attacks. More powerful encryption method is indeed an option to be considered.

REFERENCES

- [1] Ramesh.R, Pankaj Kumar G," Persistent Referral Service for Mitigating DDoS Attacks using Search Engines:PRS",Appeared in Proc. of Int. Conf. Information Security ,2011.
- [2] Ramesh.R, Resmi Cherian "Unified Protection System to avert DDoS and Phishing Attacks using Persistent Referral Service", Appeared in Proc. of Int. Seminar on Wireless Communication, Mobile computing and Emerging technologies (WICOMET), Sep. 2011 .
- [3] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki "Distributed Denial of Service Attacks", The Internet Protocol Journal - Volume 7, Number 4, National Technical University of Athens, Cisco Systems Inc.
- [4] J.Wuand K.Aberer,"Using Siterank for p2p Web Retrieval," Technical Report IC/2004/31, SwissFed. Inst. Technology,Mar.2004.
- [5] X. WangandM.Reiter,"Wraps:Denial-of-ServiceDefense throughWebReferrals,"Proc.25thIEEESymp.ReliableDistributed Systems(SRDS),2006.
- [6] Anti-Phishing Working Group, "Phishing Activity Trends Report, 1st Half 2009". http://www.apwg.org/reports/apwg_report_h1_2009.pdf
- [7] T. Anderson,T.Roscoe,andD.Wetherall,"Preventing Internet Denial-of-Service with Capabilities,"Proc. Second Workshop Hot Topics in Networks (HotNets'03), Nov.2003.
- [8] A.Yaar, A.Perrig, and D.Song , "An End host Capability Mechanism to Mitigate DDoS Flooding Attacks," Proc. IEEE Symp. Security and Privacy (S&P '04), May 2004.
- [9] R. Stone, "An IP Overlay Network for Tracking Dos Floods," Proc. USENIX Security Symp., 2000.
- [10] M.Waldvogel and R.Rinaldi, "Efficient Topology-Aware Overlay Network," Proc. First Workshop Hot Topics in Networks (HotNets '02), Oct. 2002.
- [11] J.Han, D.Watson, and F.Jahanian, "Topology Aware Overlay Networks," Proc. IEEE INFOCOM '05, Mar. 2005.
- [12] Keromytis, V. Misra, and D. Rubenstein, "SOS: Secure Overlay Services," Proc. ACM SIGCOMM '02, Aug. 2002.
- [13] L.vonAhn,M.Blum,N.J.Hopper,andJ.Langford, "CAPTCHA:UsingHardAIProblemsforSecurity,"Advances inCryptography—EUROCRYPT'03.SpringerVerlag,2003.
- [14] Chou, N., R. Ledesma, Y. Teraguchi, D. Boneh, and J.C.Mitchell, "Client-Side Defense against Web-Based Identity Theft". In Proceedings of The 11th Annual Network and Distributed System Security Symposium (NDSS '04).
- [15] X. Yang, D. Wetherall, and T. Anderson, " A Dos-Limiting Network Architecture," Proc. ACM SIGCOMM '05, pp. 241-252, 2005.
- [16] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing Internet Denial-of-Service with Capabilities," Proc. Second Workshop Hot Topics in Networks (HotNets '03), Nov. 2003.
- [17] A.Yaar, A.Perrig, and D.Song, "Pi: A Path Identification Mechanism to Defend Against DDoS Attacks," Proc. IEEE Symp. Security and Privacy (S&P '03), <http://www.ece.cmu.edu/~adrian/projects/pi.ps>, May 2003.
- [18] H. Burch and B. Cheswick, "Tracing Anonymous Packets to Their Approximate Source," Proc. 14th USENIX System Administration Conf., Dec. 1999.
- [19] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network Support for IP Traceback," Proc. ACM SIGCOMM '00, Aug. 2000.
- [20] D.Song and A.Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," Proc. IEEE INFOCOM '01, Apr. 2001.
- [21] C.Jin, H.Wang, and K.Shin, "Hop-Count Filtering: An Effective Defense against Spoofed Traffic," Proc. 10th ACM Conf. Computer and Comm. Security (CCS), 2003.[spoofing]