Client-Side Defense against Phishing with PageSafe

P. K. Sengar
ECD, Deptt
IIT, Roorkee

Vijay Kumar
ECD, Deptt
IIT, Roorkee

ABSTRACT
Every day, a number of attacks are launched with the aim of making web users believe that they are communicating with a trusted entity for the purpose of stealing account information, logon credentials, and identity information in general. These attacks, commonly known as "phishing attacks," are most commonly initiated by sending out emails with links to spoofed websites that harvest information. Many anti-phishing schemes have recently been proposed in literature. Despite all those efforts, the threat of phishing attacks is not mitigated. Solutions based on blacklists of phishing web sites are partially effective. Such solutions require the anti-phishing organizations to be much faster than the attackers. And the effectiveness of private information preserving approach is totally dependent on users. To keep their private information could be irritating works for users Solution based on automatic classification have the problems of false positives and false negatives.
In this paper, proposes PageSafe – an anti-phishing tool that prevents accesses to phishing sites through URL validation and also detects DNS poisoning attacks? PageSafe also examines the anomalies in web pages and uses a machine learning approach for automatic classification. PageSafe does not preserve any secret information and requires very less input from user. PageSafe performs automatic classification but by taking advantage of user assistance and external repositories, hence the number of false positives is reduced by a significant value. PageSafe is based on an approach opposite to blacklist approach removing the race between phishers and anti-phishing organizations. PageSafe maintains a whitelist of URLs with the mapping of corresponding IPs. This list is referenced first for resolving IP of a URL to protect user from DNS poisoning attacks. With PageSafe users help to decide whether or not a web page is legitimate. This report also present an analysis on effectiveness of PageSafe based on an experiment done on a set of phishing pages.

Categories and Subject Descriptors
K.4.4 [**Computers and Society**]: Electronic Commerce—Security; I.5.2 [**Pattern Recognition**]: Design Methodology—Feature evaluation and selection

General Terms
Security, PageSafe

Keywords: Phishing, anti-phishing, learning.

1. INTRODUCTION
Identity theft through phishing scams has become a growing concern. Phishing is a process where an attacker masquerades as a trustworthy organization in order to obtain personal financial information from an individual, and use it for malicious purposes [1]. Phishing attackers use various tactics to lure or hijack a browser to visit bogus sites. They may choose social engineering, such as phishing emails that leads users to fraudulent website designed to trick recipient into divulging financial data , or/and technical subterfuge, such as trojan horses, pharming crimeware to steal consumer's personal identity data and financial account credentials. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning [2]. The Pharming technique modifies the user's DNS file to relate the web addresses of well-known banks and financial institutions with the IP address of a pharming site, so when users open their browsers and enter the address of their bank, they get sent to the Phishing site instead.
Although many anti-phishing schemes have been proposed, none of them effectively solves the authentication challenge. Relying on automatic ways to identify phishing attacks makes these tools suffer from both false positives and false negatives. Attackers can easily find new ways to bypass these automatic filters. Other schemes, such as automatic password managers, face significant practical hurdles: they must allow users to temporarily deactivate them to handle backward compatibility issues or password resets. Many banks use visual cues such as customized login pages to prevent phishing, yet inattentive users can still are phished. Although automation introduces simple alternate ways for phishing attacks to continue, still automation makes these anti-phishing tools more user-friendly.
In this paper, we introduce the PageSafe -a novel tool that does not completely rely on automation to detect phishing. Instead, PageSafe relies on user input to decide on the legitimacy of a URL. It uses external information repositories on the Internet to help the user with decision-making. PageSafe also examines anomalies in web pages and uses a machine learning approach for automatic classification. PageSafe prevents accesses to phishing sites and warns against DNS pharming attacks. PageSafe maintains a Whitelist-a list of domains with mapping to corresponding IP addresses. Whitelist is encrypted by a master password. Whitelist is used as local DNS file for name IP resolution.

2. RELATED WORK
Phishing attacks are rapidly growing in number. Though a number of anti-phishing browser toolbars are available but unfortunately no one fully solves phishing attacks problem. For

example, Antiphish [3] stores mapping of secret information with mapping to corresponding domain, but it is not good idea to store secret information which is memorized by user. Anitphish cannot protect user against pharming attack and to keep their secret information could be irritating work for user. Spoof Guard [4] applies three tests to all downloaded pages and combines the results using a scoring mechanism; Stateless methods that determine whether a downloaded page is suspicious, stateful methods that evaluate a downloaded page in light of previous user activity, and methods that evaluate outgoing html post data. Spoof guard calculates spoof index and warns user if this is greater than the threshold selected by user. Spoof guard raises false alarm when user opens a new account with same username and password or as a result of redirection. Microsoft and Google integrated [5] the blacklisted phishing domains into browser and browser warns user against these URLs. But there is always a window of vulnerability because of race between phishers and anti-phishing organizations. PwdHash [6] authenticates a user with domain specific password. It computes hash of password with domain which is used as site specific password. But it is susceptible to offline dictionary attack and pharming attack. Phish Guard [7] maintains trustlist containing mapping of trusted domains and corresponding IP addresses and examines similarity of a URL with the URLs in trustlist. It detects pharming attacks and raises phishing warning if similarity of URL is greater than a threshold. ItrustPage [8] validates a URL through external information repositories. But user is susceptible to attack if system is compromised and also it cannot protect user if phishing site is hosted on a legitimate domain.

3. PAGESAFE MODEL

PageSafe performs automatic classification but does not completely rely on automation to detect phishing. Instead, PageSafe asks for user input and also examines anomalies in web page to perform automatic classification to decide on the legitimacy of a web page. It uses external information repositories on the Internet to help the user with decision-making. PageSafe prevents accesses to phishing sites and warns against DNS poisoning attacks. PageSafe maintains a Whitelist-a list of domains with mapping to corresponding IP addresses. Whitelist is encrypted by a master password to protect it from corruption through malicious softwares. It maintains a dynamic whitelist containing domains with mapping to corresponding IP addresses. It considers that phishing sites are short lived and only allows those sites that are not short lived. This section presents the PageSafe model for preventing accesses to Phishing sites as well as Pharming detection. PageSafe uses artificial neural network approach for automatic classification after identifying anomalies in a web page.

3.1 Classification of Phishing Attacks

We analyzed various phishing attacks and found that users accessed phishing sites in following ways:

- DNS poisoning: Here the attacker corrupt the local DNS file and changes the mapping of legitimate URL with phishing site IP on user machine by installing some malicious software. When user types a legitimate URL request is directed to phishing site.
- Newly Registered Domains: The attacker registers a fresh domain and divulge user to follow the URL.
- Compromised legitimate Domains: Attacker hosts phishing sites on a legitimate server. User visits a legitimate domain but phishing page is appeared.

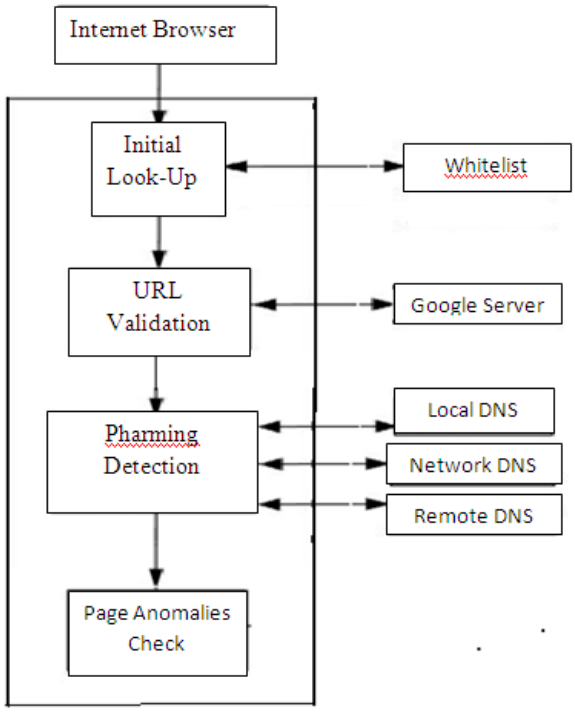

Figure 1: PageSafe Model

3.2 Neural Network

ANNs develop their own solutions from examples for a class of problems. Artificial neural network consists of a collection of processing elements (neurons) that are highly interconnected and transform a set of inputs to a set of desired outputs. The neurons process information parallelly and collectively within the structure of the network. The result of the transformation is determined by the characteristics of the elements and the weights associated with the interconnections among them. A neural network conducts an analysis of the information and provides a probability estimate that it matches with the data it has been trained to recognize. The neural network gains the experience initially by training the system with both the input and output of the desired problem. The network configuration is refined until satisfactory results are obtained. Artificial neural networks have different types of architectures, which consequently require different types of algorithms. In this thesis work Scaled Conjugate Gradient Backpropagation (trainscg) algorithm is used for training neural network.

Scaled Conjugate Gradient Backpropagation Algorithm: The scaled conjugate gradient algorithm [9] is an implementation of avoiding the complicated line search procedure of conventional

conjugate gradient algorithm (CGA). The scaled conjugate gradient algorithm is an implementation of avoiding the complicated line search procedure of conventional conjugate gradient algorithm (CGA). According to the SCGA, the Hessian matrix is approximated by:

$$E''(wk)pk = \frac{E'(wk + \sigma kpk) - E'(wk)}{\sigma k} - \lambda kpk$$

Where E' and E'' are the first and second derivative information of global error function E (wk). The other terms p_k, σ_k and λ_k represent the weights, search direction, parameter controlling the change in weight for second derivative approximation and parameter for regulating the indefiniteness of the Hessian.

3.3 PageSafe Functionality

PageSafe has four modules-Initial look up, URL validation, Pharming detection and Page anomalies check. When a user requests a URL, these modules becomes active and performs different functions:

3.3.1 Initial Look-Up Module

The Initial look-up module looks up the domains of URL in whitelist and picks up the corresponding IP from the whitelist if domain is found in whitelist. URL is passed to URL validation module if URL is not found on whitelist.

3.3.2 URL Validation Module

URL validation module issues a search query to Google for The URL. If the top 10 search results contain the URL, then it infers that the URL is legitimate [8]. The average life time of a phishing site is 5-6 days [10]. The fact that the site appears in the top 10 search results means that the Google crawler indexed the site, and that the site is not short-lived. Sometimes, the user reaches a web page by navigating to it from the Google search page. These domains are automatically added to whitelist after performing pharming detection. If URL is not found in top 10 results, PageSafe involves users to specify the search term for the web page they intend to visit. PageSafe performs a Google Search and provides the search results to users. Users can choose a URL from the search results. After URL validation it URL is passed to Pharming detection module.

3.3.3 Pharming Detection Module: Malicious softwares attached with emails or web pages can cause DNS poisoning or Pharming. There are 3 entities involved in resolving a URL to IP address [7]:

- Local DNS: means a local host file which is firstly referenced to resolve a web address to a specific IP address.
- Network DNS: means DNS server inside an organization. If the Local DNS doesn't know the corresponding IP address, the Network DNS is asked.
- Remote DNS: means the DNS servers of ISPs. We use these to check the Network DNS Pharming.

Pharming detection module compares the IP addresses from Local DNS and Network DNS with the IP address from remote DNS for the requested URL. If all are not same then pharming is detected and alert is made to user. We assume Remote DNSs such as ISP DNS are highly secured and are not contaminated. If no pharming is detected the URL is added to whitelist with mapping to its IP and web page is retrieved from the server. After retrieving the web page Page Anomalies Check module examines the page.

3.3.4 Page Anomalies Check Module

This module first selects high frequency words appearing in a web page and removes stop words from the set. This module checks anomalies in web page and applies the following rules:

1. URL Check: A web page's URL (Uniform Resource Location) is unique in the cyberspace. For a regular web site, its identity is usually part of its domain name. For a phishing site, its true URL is usually similar but different from its claimed identity. Suppose, S= {s1, s2, s3 …} is a set found after removing stop words from the set of high frequency words. We consider three cases: 1)For URL address L, no s_i is a substring of L for all $0 \le i \le k$, or the domain name looks obscured, e.g. http://www.paypal.com@123.123.123.123, or http://www.paypal.com.secure.login.cmd.path.hotelielsi.com/ cgi.bin/, F_1=1, 2) If one page only uses the IP address, F_1=0, 3) Otherwise , F_1= −1.
2. Link Check: Anchors in a normal web page usually point to pages in the same domain. For phishing pages, there are possible abnormalities listed below. In the following, let Aa be the total number of anchors in page.
   a. Nil anchors: An anchor is called a nil anchor if it points to nowhere. Examples are
      <a href="#">, <a href="javascript::void (0)">, etc.
   b. Foreign anchor: An anchor is called foreign anchor if it points to foreign domain. The attacker does not want to create the complete website. The percentage of nil and foreign anchors in a page reflects the degree of suspiciousness. Let The higher the percentage, the more likely that page is a phishing page. $A_{n/f}$ be the number of nil and foreign anchors in web page. F_2 is assigned as follows:

$$F_2 = \begin{cases} 0 & A_a = 0 \\ A_{n/f}/A_a & A_{n/f} > 0 \\ -1 & \text{otherwise} \end{cases}$$

3. Request URL check: Web pages are object rich, containing numerous objects including images, CSS files, scripts etc., a large percent of objects are loaded from its own domain. Only a small portion of them are from foreign domains. While in phishing pages, most objects are copied or loaded from the real sites since the attackers intend to reduce their cost of faking. We observe that more request URLs in page indicates a higher probability of page being faked.

$$F_3 = \begin{cases} 0 & R_a = 0 \\ R_f/R_a & R_f > 0 \\ -1 & \text{otherwise} \end{cases}$$

   Where R_f is the number of request URLs to foreign domains.
4. Form handler check: The ultimate goal of phishing attacks is to steal user's private information, such as user name and password. Phishing pages often contain forms requesting user inputs. It shows where the data is to be sent. However, the handler of such a form in a phishing page usually refers to the real site or simply is void or to some foreign domain. We set F_4 = 1, if there is an occurrence of any void handler (e.g.

<form action="#">, <form action="about: blank">, <form action="javascript: true">), or any handler referring to a foreign domain. If there is no handler in page, F_4=0 and F_4= −1 for other cases.

5. SSL Check: In a SSL transaction, the web client usually requests the server to present a public key certificate. For a legitimate web site, the presented certificate contains identity relevant information, e.g. the Distinguished Name (DN). Moreover, a certificate for web usage usually defines its serving URL explicitly. A phishing site may choose to use the same certificate as its victim's one. Otherwise, its own certificate would not match the identity it attempts to impersonate. So, F_5 = 1 if one of the claimed identities does not appear in the certificate attached to page or the URL specified in the certificate is different from L; F_5 = 0 if the SSL is not applied; and F_5 = −1 for other cases.
6. Hidden fields: Hidden fields can be used to steel information. These fields are not visible to user but can be used to hide information such as username, passwords etc using java scripts. A large number of hidden fields in a page lead suspiciousness of page being fake. F_6 is the number of hidden fields in a webpage.
7. Title check: The contents of title tag in HTML appear on the top of browser window. Attacker uses the name of real site to make user to believe that he is visiting a legitimate website. Suppose Y= {y_1, y_2, y_3 ...} is a set achieved by removing stop words from the contents of title tag. F_7 is assigned as follows:
   a. If no y_i is a substring of page domain, F_7=0
   b. Otherwise, F_7= -1.

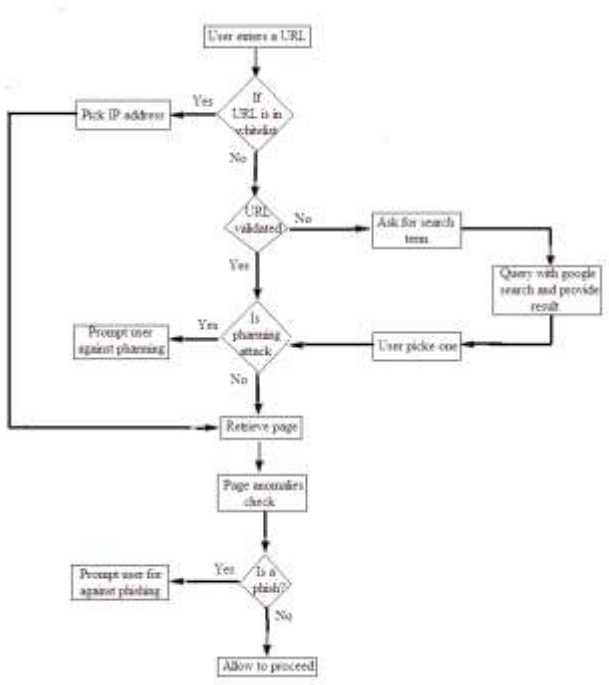

Figure 2: PageSafe Flow-Chart

4. RESULTS

PageSafe can successfully detect all phishing attacks taking place through DNS poisoning or pharming attacks. Phishing sites are short lived. PageSafe only allows those URLs that have been indexed by Google i.e. these URL related websites are not short lived. By doing this, a large percentage of total phishing sites, is removed. But a phishing website can be hosted on a compromised legitimate server indexed by Google. To cope up with phishing websites hosted on a legitimate domain, PageSafe performs automatic classification of web pages using artificial neural network.

A sample of 500 websites including phishing as well as legitimate websites is taken from www.phishtank.com. We used this set for the training of neural network. The sample is used as: 350 sites in training, 100 sites for validation and 50 sites for testing the neural network. Percentage errors in training, validation and testing are 5.6, 0 and 0 respectively.

After training the neural network a new dataset of 200 sites was taken containing phishing as well as legitimate sites. The accuracy achieved was 97% i.e. only 3% sites are wrongly classified.

PageSafe warns when a user tries to visit a website which is not indexed by Google i.e. only allows those websites that are not short lived. Phishing sites are short lived hence by allowing only Google indexed web sites reduces the probability of a website being a phish. PageSafe performs automatic classification only for those phishing websites that are hosted on legitimate domains which are lesser in number hence false positives are reduced by a significant value.

5. CONCLUSION AND FUTURE WORK

Phishing have brought a dramatic increase in the number and sophistication of attacks involved in stealing user's secret information. This paper presents PageSafe for preventing user from filling out web phishing forms. PageSafe asks user's input to disambiguate between legitimate and phishing sites and Internet repositories of information to assist the user in decision making process. PageSafe does not preserve any secret information as information preserving approach completely dependent on user. PageSafe merges user assistance with automatic classification reducing the false positives by a significant value. PageSafe uses some new features and uses a machine learning approach (Artificial Neural Network) for automatic classification and achieves 97% accuracy. PageSafe protects user even if the system is compromised by detecting DNS poisoning and also from those phishing sites hosted on legitimate domains. PageSafe cannot protect user from key-loggers screen-grabbers and client side scripting.

More functionally can be added to PageSafe for protecting user against key-loggers and screen-grabbers and client side scripting attacks. PageSafe uses Google search to validate a URL which can be refined by using more external repositories such as Yahoo search etc. PageSafe uses artificial neural network approach and achieves 97% accuracy. This can be improved by adding more rules and using other machine learning approaches.

6. REFERENCES

[1] TippingPoint, "TippingPoint Phishing Point", *TippingPoint*, 2005.

[2] McAfee, "Understanding Phishing and Pharming", *McAfee White Paper*, 2006.

[3] E. Kirda and C. Kruegel, "Protecting Users against Phishing Attacks with AntiPhish", *29th Annual International Computer Software and Applications Conference*, ACM Press, Washington, USA, 2005, Vol. 01, pp. 517-524.

[4] N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. C.Mitchell, "Client-side defense against web-based identity theft", *11th Annual Network and Distributed System Security Symposium*, ACM Press, Ontario, Canada, 2004, Vol. 380.

[5] L. Sean M. Allister, E. Kirda, C. Kruegel , "On the Effectiveness of Techniques to Detect Phishing Sites ", *Proceedings of the 4th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, ACM Press, Switzerland, 2007, Vol. 4579, pp. 20-39.

[6] B. Ross, C. Jackson, N. Miyake, D. Boneh, J. C. Mitchell, "Stronger Password Authentication Using Browser Extensions", *Proceedings of the 14th conference on USENIX Security Symposium ,2005,* Vol. 14.

[7] J. Kang and D. Lee, " Advanced White List Approach for Preventing Access to phishing Sites " International Conference on Convergence Information Technology, Korea, 2007.

[8] T. Ronda, S. Saroiu, A. wolman, "Itrustpage: a user-assisted anti-phishing tool", ACM SIGOPS Operating System Reviews, ACM Press, 2008, Vol. 42.

[9] M.F. Moller, "A Scaled Conjugate Gradient Algorithm For Fast Supervised Learning", *Neural Network Letters*, ScienceDirect, 1993, vol.6, PP 525-533.

[10] K. Oberoi, A. K. Sarje, "An Anti-Phishing Application for the End User", *IIT Kanpur Hackers' Workshop 2009*, IIT Kanpur, UP, INDIA, March 2009.