Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Identification and Prevention of Phishing Attacks in web Application

M.Varun Kumar*
Assistant Professor
SITE, VIT University
Vellore,Tamilnadu, India

S.Subbasri
MCA
SITE, VIT University
Vellore,Tamilnadu, India

S.Subathra
MCA
SITE, VIT University
Vellore,Tamilnadu, India

R.Jayakumar
M.S(Software Engg)
SITE, VIT UNIVERSITY
Vellore,Tamilnadu, India

Abstract- ***In this real world scenario, phishing attack is the main problem which occurs in the client side. Mostly, social networks email, financial websites are affected by the phishing attackers. Many encrypting algorithms are used for preventing from the phishing attack. But even though, the hackers are easily get the user's password and their sensitive information. Due to overcome this crisis, In this paper, we are presenting a solution, for identifying the original web page, creating a secure password and providing a random password in user mobile device, while using internet banking, even if the user get the password they cannot be able to use it. According to this, we are implementing the efficient encryption algorithm in real time applications such as online banking, social network etc. With required software based techniques for security.***

Keywords:

I. Introduction:

Phishing attack is the main problem which occurs in the user side. Mostly, social networks email, financial websites are affected by the phishing attackers. Many encrypting algorithms are used for preventing from the phishing attack. But even though, the hackers are easily get the user's password and their sensitive information. So we have to prevent from these victims. We are detailed discuss about the fake page, how to identify, the current using page is duplicate page. We have given some suggestions to provide key, and how to generate with an example. We are presented Implementation and Experimental results. A small part should be implemented in this paper by using some software based techniques.

A. IDENTIFYING THE FAKE WEBSITE:

Different types of hacking which occurs in both users side and sever side. Moreover people couldn't be known our webpages are attacked by unauthorized person. Because those fake webpages are similarly like real page. For this sake, email tracking, transfer the money, video tracking, image tracking are these unwanted criminal actions are happening in this society by a hacker. People must be in aware about these sites and if any illegals actions are held means they have to know the way, to overcome, for these activities.

REAL WEBSITE:

FAKE WEBSITE:

Generally, people cannot be predicting the real webpages for many reasons. The first one is less consciousness or less awareness about it and the second one is user doingknow how to analyze or identify the page. The fake web pages are identified through web address and images. Initially we have to check the domain name, interdomain name and IPaddress. Now a question should be arise "how to check?" the solution is given.

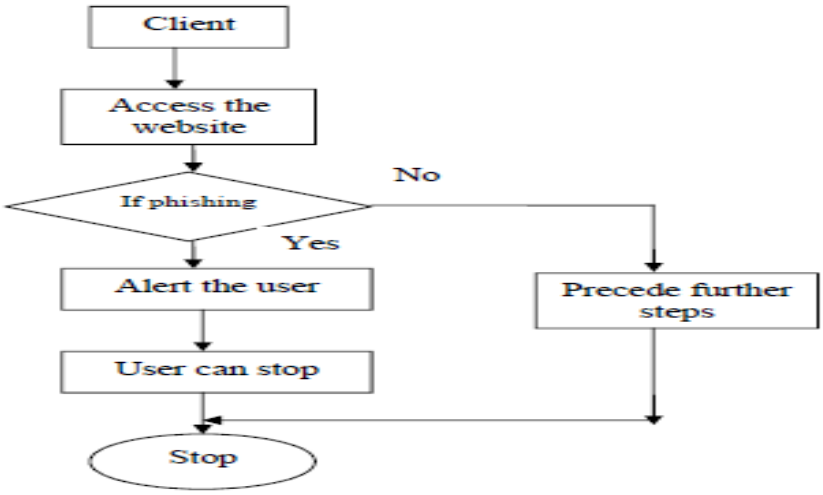

Fig 1-Identification

For example we take to any website address like http://www.123.co.in/666.com here domain name is co.in likewise .com,.edu,.tech are the examples of domain name will be enter automatically it will connect to the associated IP address is which protocol it depends on like email is based on SMTP protocol, file transferring protocol FTP, we are collecting the information in worldwide so we are using www.The user see the domain name and IP address identify the fake pages, if it is a real page means authorized domain name are present, else it is not real. In case if the domain name may be right but it is hacked by someone how have to find out? Yes it is very difficult because the hacker create an own web page and establish a link to the real page. So user may be failing to identify the real one. In this situation we have to overwhelm, creating a unique key we have detail discuss in 1.2. The other way to find out the fake page by analyzing the image. The image is validating by a comparing the real one with fake one by a pixel by pixel. There are two methods such as content and visual contents for analyzing the images. In textual method we have to compare the image frequency value. Both methods are used to compare the website is authenticated or phishing website. These methods are technically possible but practically it is difficult to do [3].

B. PROVIDING A SESSION KEY:

Nowadays, Passwords are easily hacked by the victims. Many efficient algorithms are produced for password secureness, initially we have to know what are the process is happening in between the user and sever. In existing system, a cookie is created in sever side it contains all the information, if any user give the request to sever, it will reply but it does not know the particular user which user give the request so it is the problem arise here. So we have to avoid this user side a cookie is created for storing the information, if it exchanges the data between user and distribute the data should not be changed but the process should be exchanged very exactly [2].

The distributer could be accepting the user request it will produce a session key for that user with session identity. Sever will be replying the request with session id to the user. At the same time the user also accepts the reply and sent the acknowledgment to the server with the session ID. With the help of html, php and JavaScript hacking is occurred. The hacker does some modification and gives link to original webpage by "ahref. ahref is used for linking the webpage from one to another. Here GET method is used for getting the password from the user by the unauthenticated person. The post method is used for the user will post their username and password to the distributer. The distributer will accept the request, check the cookies what the appropriate data is stored after it get. To make a distrustful protection against such attacks they have introduced the anti-phishing technique. The current anti phishing technique is Password hash technique. In this technique some verification code is added with the original password of the user to increase defence against hacker by using efficient algorithms[2][3]. It is mandatory for some applications such as internet banking, e-mails social network etc.

Create password with session key, Creating a unique identity purpose is if the victim hacked the password in spite of that, they can't access because we created a unique id for every request, in online banking application the user send the request to the server, before it goes to access send the unique identity, if the client get back the session key, the webpage is real, else the user understand it is a fake page. Similarly the server gets the password with the session key then only it will establish a link between the regarding concern and the user.

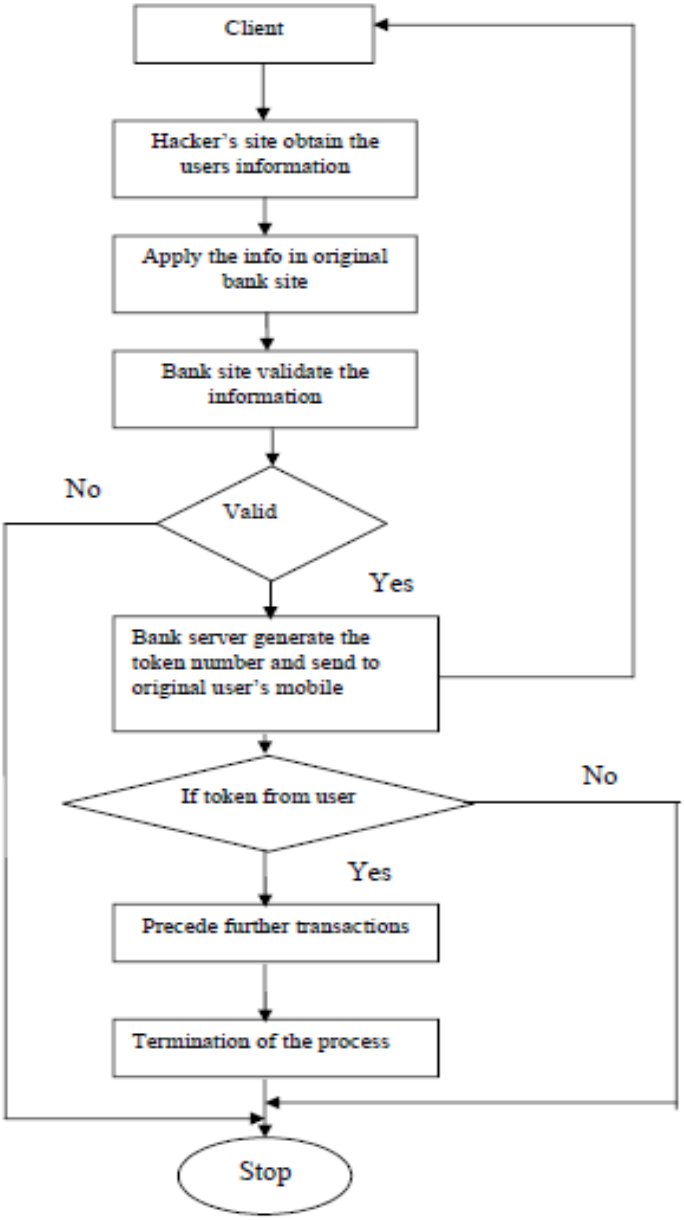

Fig 2- data flow diagram for prevention

Along with session login a token [2] is proposed for avoiding unauthenticated user processing the application. The purpose of token usage is the hacker cannot easily find out the password and it is used for safely money transactions on net banking. The request is associated with the particular token then only the process will be proceeds else it does not process. If the request does not have token it will be generate the new token for that request and send into along with the session id. Create the cookies and set the token for each user request, in this parent location host was not accessible.

II. Secure Transaction:

Each web page who has been informed along with IP address. WHOIS is all about web page approval, name to which the web page is registered along with organisation details. Phishing database is always promoted with phishing webpage information's for confirmation The DNS server will validate whether the requested web site is original or not. If the DNS server examine that the requested web site is of phishing website the server will confirm the user that requested website is phishing and so the user disagrees to give any secured data to the phishing web site If the website is original further verification is carried along with salting and hashing using effective algorithm, it sent as sms to authorized mobile number. Once the authorized user access with the verification code and if access granted only then the user is acquiesce for further transaction procedures ,the client further proceed and over check the transaction by term log in this system provides banking functions to genuine end user or user. user can access the needed function from this application . Consumer can access balance query and also start online transaction in a highly secured way.

III. Implementation:

We are using html with JavaScript, php language for analyzing the fake webpage and real page .These are user friendly for the client to communicate between the user and the distributor. The cookies are created on the user side for getting the information of the user. Useset cookie method for automatically store data. Here we are creating a sample phishing page by following methods. First we have to download the wamp, xamp server, after downloaded install the Xamp server. After completed the installation we just go to the path folder c:\xamp\www.in this folder we have to paste your phishing page. Next we have to start Xamp server.(Start->windows->allprograms->xampserver->startxampserver). Then we see the Xamp circle icon in system. Then we just make click on it and select all start all service. Now the phishing page is ready in our system. Whenever we open the website our phishing will be open. A well-practiced and technically sound person only have to well-known about this page is phishing page or not. It is a server side substitution. We have proposed a substitution which is kept on the side of distributor and placed between the web browser and our aimed application. It can be able to detect and change the user request. The purpose of substitution is used for maintain a token table with the entries. Tokens are added with session key reply to the user from the server [2]. For the safe of web pages we are adding the corresponding configure of apache and also we are identifying the cookies names for specified application within that we have to store the session login.

IV. Experimental Results:

For this experiment, we are downloading many web applications and tested the pages is fake or real by tracking the user name and password. While we are tracking the password the fake webpage doesn't ask the Uid and also we are changing the URL and giving link to the real page forms by using html. So it just links the fake page to the original and also hacked the password but it can't access the account because we are putting the Uid for each request. So the user given the request at the same time it replies the request with session id and along with token. If the request does not return Uid the distributor or user stop the work to proceed in the webpage because the user will know clearly it is a phishing page. If the request comes with Uid but did not have token it create the new token and posted in the token table whenever it need means it just fetch from it. We are successfully implemented time consuming is less, manually it will be done, and by the usage of connecting the http header automatically it will be updating transacting. Rewriting the URL is also given the very good result. But it little difficult to implementing in spite of attain a good solution.

V. Conclusion:

Phishing has become extreme network security issues which cause financial damage of even billion dollars to consumers and e-commerce companies. Perhaps this made e-commerce companies virtually distrusted and highly deformed to the consumers. In this paper, we are discussing the characteristic of the hyperlinks that were enclosed in phishing e-mails and overwhelm existing issues and successfully identifying the fake/duplicate page and offering. sessions with favor for secure password.

References:

[1] Cross-Site Request Forgeries: Exploitation and Prevention William Zeller and Edward W. Felton, technical report.
[2] Preventing Cross Site Request Forgery Attacks Nenad Jovanovic, Engin Kirda, and Christopher Kruegel
[3] Securepasswordgenerator.http://packitezier.com/
[4] Source Forge. http://sourceforge.net/, 2006.
[5] The Anti-phishing working group. http://www.antiphishing.org/.
[6] Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh, and John C. Mitchell. Client-side defense against web-based identity theft. In *Proc.NDSS 2004*, 2004.
[7] PhishGuard.com. Protect Against Internet Phishing Scams. http://www.phishguard.com/.
[8] Jonathan B. Postel. Simple Mail Transfer Protocol. RFC821: http://www.ietf.org/rfc/rfc0821.txt.
[9] Preventing phishing attacks is not just a technical issue http://www.acunetix.com/web-security-zone/preventing-phishing-attacks/

