Gaurav, Madhuresh Mishra, Anurag Jain / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.1825-1828

A Preventive Anti-Phishing Technique Using Pattern Matrix

Gaurav*, Madhuresh Mishra,Anurag Jain*****
*(University School of Information Technology, GGSIPU, Delhi)
** (University School of Information Technology, GGSIPU, Delhi)
*** (University School of Information Technology, GGSIPU, Delhi)

I.ABSTRACT
Today one of the highly used techniques to pursue online stealing of data and to do fraudulent transactions is phishing. Phishing is defined as a technique to take the user to fake website via fake link in order to make him enter its credentials and to use that information illegally for own benefit. It is affecting all the major sectors of industry day by day with a lot of misuse of user credentials. To stop phishing many detection and prevention techniques has been made with their own advantages and disadvantages respectively, but phishing has not been eradicated completely yet. Seeing the fact that phished pages generally asks for entering and submitting the credentials but is not able to retrieve any user known data, here we propose a preventive anti-phishing technique to avoid to be victim of phishing attacks.

II.INTRODUCTION
Phishing is one of the cyber crime which is done to illegally carry out fraudulent transactions where victim/user is carried, using a forged email that contains a URL to a fake web site masquerading as a legitimate entity. A phisher may lure a victim into giving his/her user id, passwords and other credential information, which can then be used to transactions like financial ,social etc on the victim's behalf .

Attacker/phisher uses replica of original website as bait that is send to the user. When user grabs the bait by filling and submitting his useful information attacker pulls the bait means saves the data for its own use illegally.

In general, phishing attacks are performed with the following four steps:

1) A fake web site which looks exactly like the legitimate Web site is set up by phisher and which acts as bait.

2) Phisher then send link of the fake web site in spoofed e-mails to target users in the name of legitimate companies and organizations, trying to convince the victims to visit their web sites.

3) Victims then grab the bait, means he visit the fake web site by clicking on the link and input its useful information there.

4) Phishers then steal the personal information and perform their fraud such as transferring money from the victims' account.

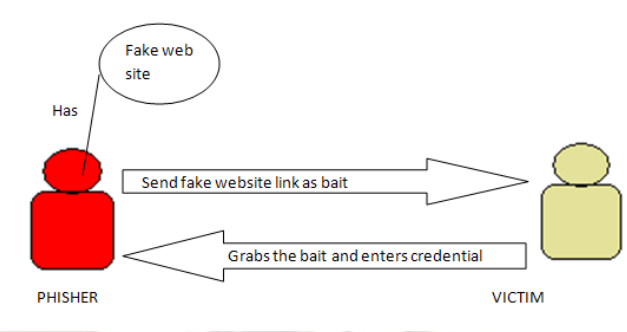

Fig.1: process of phishing attack.

There are a lot of fake phishing websites created and uploaded online every day, luring a number of customers. According to a global phishing survey done by APWG(anti-phishing working group),for the period of second half of 2011 [2],there were 83,083 unique phishing attacks done worldwide in second half of 2011in 200 top level domains. It also stated that 50,298 attacks used unique domain names and 2,288 attacks were detected on 1,618 unique IP addresses rather than domain names[2].

As it can be generally seen that financial service sector and payment service sector is targeted most and financial service sector and payment service sectors deals with money transactions ,so it can be concluded that main objective of phishers is to steal financial details of victims and misuse that for their own gain. So phishing attacks are emerging as one of the major area

where immediate concern is needed as it is affecting all the major sectors of industry creating a lot of loss.

III. RELATED WORK

There is a lot of work that has been done in order to curb the phishing attack. Broadly there can be two categories of techniques/methods to curb a phishing attack that is detection method and prevention method. Detection methods[1,3,4,5,6,7,8] work after the creation of phishing page and determine whether a page is phished or not whereas prevention methods like Yahoo Sigh-In Seal [9] works before phishing and do not let phishing to happen. There are many detection techniques available like attribute based detection, character based detection etc with their own merits and demerits respectively. Preventive techniques mean the methodologies employed by organizations to avoid the phishing attacks.

IV. TECHNIQUE IN DETAIL

Generally a phished page only accepts the data but is not able to retrieve any information on the basis of given data. The phished pages are created generally with submit button only that means only to save the data entered by victim/user on the server, they do not have any link to search or retrieve any information from the server as shown in fig 2.

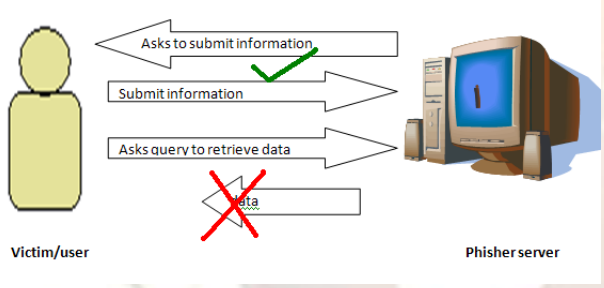

Fig.2: Exchange of data during communication between victim and phishing server

On the basis of above fact, during registration if we make the login page able to retrieve the known data then it is very less probable to make the phished page. Here we proposed a method named as VYATS (Verify Yourself And Then Submit) that is preventive in nature to avoid phishing attacks. In this method user is allowed to verify the legitimacy of the website by retrieving the known information and then he can submit the details/credentials. We have provided a code and pattern generation facility, retrieval of which is necessary during registration by the server. If the page is able to retrieve the correct code and pattern then it is almost not possible that the page is phished .This method works for those websites where the user is already registered and the website is known to the user.

Steps:

A. Initial registration with the website (sign-up)

1. User manually visits the original legitimate site for initial registration process
2. Organization provides the registration form.
3. User fills the registration form and creates its user id and password.
4. On the basis of code generation techniques(explained below) organization generates code and saves it with user details
5. Organization provide code to user
6. User select pattern of cells in 3*3 matrix to place 4 digits of its code
7. User summits form
8. Registration complete

B. After Registration (Sign-In)

1. User gets page link via email or any other method.
2. User enters its user id then 3*3 matrix is displayed.
3. In matrix, user is requested to enter first digit of respective code word.
4. After entering first digit the next cell in which second digit of code word is to be entered automatically get selected to enter the next digit.
5. With this user becomes sure of legitimacy of the page and can freely enter its other credentials

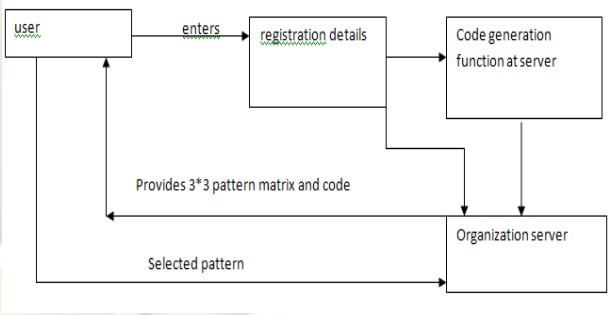

Fig.3: Block diagram of preventive technique.

Code generation methods:

1. Hashing

1.1 Text hashing

Code generation on the basis of hash value of user id concatenated with password

1.2 image hashing

code generation on the basis of hash value of screenshot at the time of registration

2. code generated via calculation

X=no. of characters of user id + no. of characters of password

Y=no. of characters in date (date) + no. of characters in month (date)

Code = concatenation of values of x and y that is xy.

After code generation first four digits are chosen by user for pattern making .The code word generated using hashing will be unique to each user but the codeword generated via calculation will not be unique, means more than one user can have same codeword but this does not cause problem as we are interested in ability of website in retrieving the user known user.

Working

After generation of code words a 3*3 matrix of 9 cells is shown to the user as shown below:-

Cell 1	Cell 2	Cell 3
Cell 4	Cell 5	Cell 6
Cell 7	Cell 8	Cell 9

Fig.4: example matrix.

User selects the pattern in 3*3 matrix. The pattern represents the places and the sequence of digits of code words in the matrix. The pattern along with unique id and password is saved in user's profile. During logging user is asked to enter his unique id then 3*3 matrix is displayed in which user is requested to enter first digit of respective code word. After entering first digit the next cell in which second digit of code word is to be entered automatically get selected to enter the digit. As we know that only the legitimate page will be having the correct sequence of pattern so a phished page can never tell where the next digit of code word is to be entered. With this user can fell sure about the legitimacy of the page and can freely enter his password.

For example- suppose the code word 1234 and the pattern is pattern is cell 1 ,cell 5,cell 9 and cell 3 as below

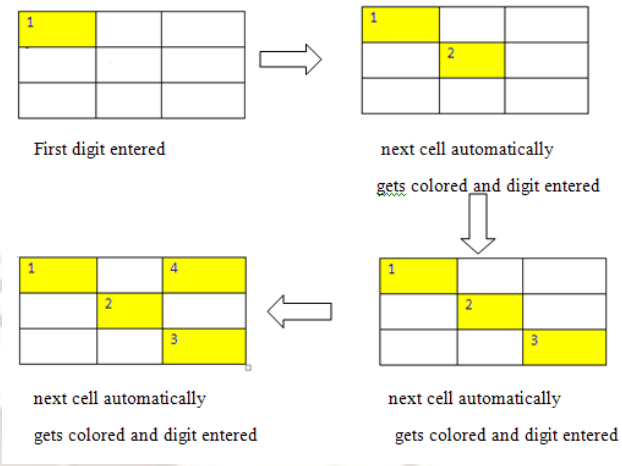

Fig.5:working example of verification.

Advantage

As it connected with the user account, it is not browser dependent to identify phished pages so user can log-in from any computer from anywhere.

Disadvantage

Technique may fail if phisher targets a particular victim and gets the code word and pattern by hacking. This problem can be overcome by limiting the no. of of trails to enter values the code digits in correct pattern chosen by user.

Generally a phisher targets victims on a large no. , so it is difficult for a phisher to hack the code words for the large no. victims

After the limiting no. of wrong attempts the matrix will block and then the user is ask to generate a new pattern by manually entering the URL of webpage in the browser.

V.CONCLUSION.

Here we have proposed a preventive anti-phishing technique which is helpful to keep users away from phished pages. This technique ensures users about the legitimacy of the webpage he visits where he is already registered and makes him aware about phishing. It is not browser dependent rather it is related with user's own saved information, so he can log on from any computer and from anywhere. This technique needs initial registration of the user to the correct website which has this facility. There is no chance of any false positive or negative as it is prevention based and not detection based.

VI.REFERENCES:

1. Hicham Tout, William Hafner "Phishpin: An identity-based anti-phishing approach" in proceedings of international conference on computational science and engineering, Vancouver, BC, pages 347-352, 2009 .

2. http://www.antiphishing.org.

3. Mather Aburrous, M.A. Hossain, Keshav Dahal, Fadi Thabtah "Prediction phishing websites using classification mining techniques with experimental case studies" in proceedings of Seventh International Conference on Information Technology, Las Vegas, NV, pages 176-181, 2010.

4. Michael Atighetchi, Partha Pal "Attribute-based prevention of phishing attacks" Eighth IEEE international symposium on network computing and application, 2009.

5. V.Shreeram, M.Suban, P.Shanthi, K.Manjula "Anti-phishing detection of phishing attacks using genetic algorithm" in proceedings of Communication control and computing technology(ICCCCT),IEEE international conference, Ramanathapuram , pages 447-450, 2010.

6. Juan Chen, Chuanxiong Guo-"Online Detection and Prevention of Phishing Attacks (Invited Paper)"in proceedings of Communicational and networking in china, first international conference, Beizing, pages 1-7, 2007.

7. Matthew Dunlop, Stephen Groat, and David Shelly" GoldPhish: Using Images for Content-Based Phishing Analysis", in proceedings of internet monitoring and protection (ICIMP), fifth international conference, Barcelona, Pages 123-128, 2010.

8. Huajun Huang Junshan Tan Lingxi Liu "Countermeasure Techniques for Deceptive Phishing Attack" International Conference on New Trends in Information and Service Science. NISS '09. June-2009.

9. http://security.yahoo.com/article.html?aid=2006102507