International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 6, Issue 8 (April 2013), PP. 88-92

Fingerprint Authentication Technique to Prevent Phishing using Pattern Matrix

Yamal Patel[1], Ms. S.Christobel Diana[2]
[1]Department of Information Technology , SRM University, Chennai.
[2]Assistant Professor, Department of Information Technology, SRM University, Chennai.

Abstract:- Phishing is an automated form of identity theft, targeted primarily at the casual e-mail user. It 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. To stop phishing many detection and prevention techniques has been applied with their own advantages and disadvantages respectively, but phishing has not been prevented completely yet. So if a website has been authenticated with user before user enters its credentials then phishing attack can be prevented. I am proposing anti-phishing technique which will authenticate website with user using fingerprint**.**

I. 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.

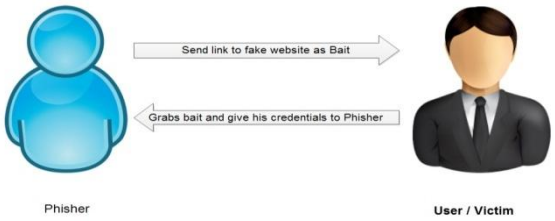

Fig.1 Phishing Attack.

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) Initiation :
This includes the Phisher preparing for the attack in order to steal the personal information of the Internet users. Phisher creates a fake web site which looks exactly like the legitimate Web site which acts as bait.
2) Execution:
In this stage the phisher tries to lure the victim to accept the bait he/she sends through 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) User Action :
Any action from the user which makes him vulnerable towards the loss of his user credentials, account balance and his other sensitive information.
Means Victims then grab the bait and he visit the fake web site by clicking on the link and input its useful information there.
4) Completion :
The attack is completed when the 'phisher' receives the personal information entered by the user and perform his/her fraud such as transferring money from the victims' account.

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 4th quarter of 2012 [2],there were 72,586 unique phishing attacks done worldwide in top level domains. It also stated that 46,895 attacks used unique 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.

II. 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.

Among the many biometric features, the fingerprint is considered one of the most practical ones. Fingerprint recognition requires a minimal effort from the user, does not capture other information than strictly necessary for the recognition process, and provides relatively good performance.

III. PRAPOSED TECHNIQUE

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.

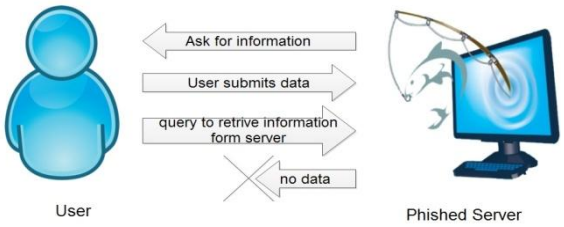

Fig.2 Exchange of data during communication between user and Phished server

So 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 I propose a method 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. In this method a code and pattern generation facility is provided at the time of registration , retrieval of which is necessary during login fron the server. If the page is able to retrieve the correct code and pattern then it is 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 :

Initial Registration or Sign Up :

1. User manually visits the original legitimate site for initial registration process.
2. Organization provides the registration form with fingerprint scanning facility.
3. User fills the registration form , scan his fingerprint 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 code.
7. User submits the form.
8. Registration complete.

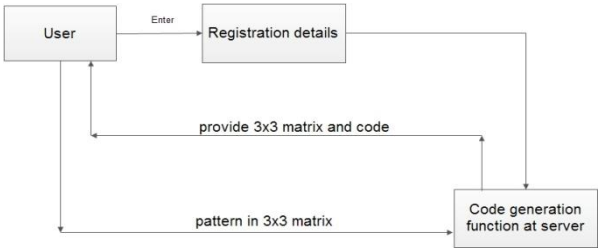

Fig.3 block diagram of registration with 3x3 matrix

Code Generation:
Code generated via calculation for user:
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). (at the time of registration)
Code = concatenation of values of x and y that is xy.

Code generation at server side:

Using classification technique describe in [10] fingerprint is classified in four types using Core and Delta singular points.(a)Left loop(b)Right loop(c)Whorl(d)Arch. we will assign a number to this types according to the table no.1

Table 1. Fingerprint classification value

Value	**Fingerprint classification**
0	Left Loop
1	Right Loop
2	Whorl
3	Arch

As proved in [11] we can extract real 40 to 60 minutiae of a fingerprint image from the 2000 to 3000 contained in typical skeletonized and binarized image.

We are using this minutiae value of endpoints or bifurcation as authentication code from server side. Both of this values , from Table 1 and minutiae value , are sent only after user entered fingerprint is verified with fingerprint image in organization's database. We are using server side code for more randomness of authentication.

Working :
After Registration (Login or Sign-In) :
1. User gets page link via email or any other method.
2. User enters its user id & then put his fingerprint in specified location on the touch screen.
3. After verifying fingerprint in organization database 3*3 matrix is displayed.
4. In matrix, user is requested to enter first digit of code generated by calculation.
5. If the first digit of code is correct then only the next cell in which second digit of code word is to be entered automatically get selected.

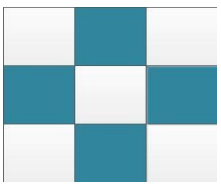

Fig.3 Example of User selected pattern

6. But before that one of above fingerprint classification value from table no.1 will be sent from server according to user fingerprint type to the matrix at random location other than user code pattern in 3x3 matrix after user enter first digit of its code.
7. User enters the next digit of its code in next location in pattern matrix.
8. Again for more randomness of authentication, location of pattern created by user is selected and user enter 3rd digit of code generated by calculation.

9. The next two digit from server side code is value of minutiae (endpoints or bifurcation) entered automatically in matrix.
10. User enter his last digit of code in pattern.

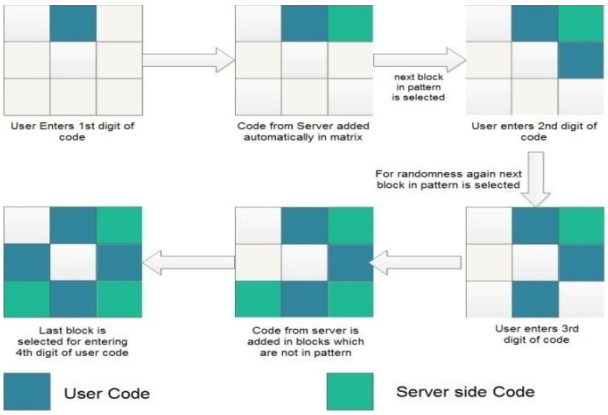

Fig.4 Example of verifying code and authentication

If user entered code is right then the respected page is retrieve from server.With this user becomes sure of legitimacy of the page and can freely enter its other credentials.

This technique is more reliable because of its randomness. Matrix is displayed to user only and only after user's fingerprint is matched with fingerprint in database.And we are using that data of fingerprint as authentication code from server side. So if attacker will get your 4 digit code and pattern then also he cannot access to account without server side authentication.

And for security of code, 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.

Advantage :

As it connected with the user account, it is not browser dependent to identify phished pages. No phisher can get access to user account because of two level of authentication and verification technique. (A) Fingerprint verification and (B) Code verification with pattern matrix.

This technique can be very useful in financial sector where big transactions are done online everyday.

Disadvantage :

Main disadvantage of this technique is fingerprint extraction which has to be done with another device integrated with PC and user browser.

Now a days many laptops are having touch screen facility so in future with fingerprint extraction using laptop screen can be revolutionary for this technique

IV. 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. 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.

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
[10]. M. Ezhilarasan, D. Suresh Kumar, S. Santhanakrishnan, S. Dhanabalan and A.Vinod, "Person Identification Using Fingerprint by Hybridizing Core Point and Minutiae Features", International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 3075-3078.
[11]. Alessandro Farina, Zsolt M. Kovacs-Vajna, Alberto Leone "Fingerprint minutiae extraction from skeletonised binary images" Pattern Recognition 32 (1999) 877 to 889
[12]. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition", 2003 Springer.
[13]. Roli Bansal , Priti Sehgal , Punam Bedi ,Minutiae Extraction from Fingerprint Images - a Review , International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.
[14]. Monowar Hussain Bhuyan, Sarat Saharia, and Dhruba Kr Bhattacharyya "An Effective Method for Fingerprint Classification" International Arab Journal of e-Technology, Vol. 1, No. 3, January 2010.