ISSN:0975-9646

A Preventive Anti-Phishing Technique using Code word

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

Abstract: The technique used to perform online theft/stealing of user credentials is termed a phishing in cyber world. 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 been eradicated completely yet. Seeing the fact that phished pages generally asks for entering and submitting the credentials but is not able to retrieved any user known data, here we propose a preventive anti-phishing technique avoid to be victims of phishing attacks

I. INTRODUCTION

phishing is a type of cyber crime where computer is used as instrument, Pronounced as "fishing," it is a method of stealing credential information such as password, user id, credit card details of victim/user . It is also called called as "brand spoofing," where an official-looking e-mail (having fake created link) is sent to victims pretending to be from their legitimate website[1]. Email can be send to the randomly selected list or some selected one assuming that some of them are actually having account on legitimate website Once one victim/user falls for the scheme and enters its sensitive information, it can be used to gain access to more of the company's resources to which he belongs. [1].

Phishing attacks involve six stages:

1. To perform phishing attack phisher obtains the email address of victim which he can search in several ways .
2. The phisher then generates an phished page that looks like exactly same as legitimate webpage but that is a fake one.
3. Phisher then send mails having the link to the fake web page to many victims.
4. Victim/user, after receiving and reading the e-mail follow to the fake link.
5. There he fills /enters his credentials and submit them.
6. Phisher then steal the personal information and perform their 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 second half of 2011 [3],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[3].

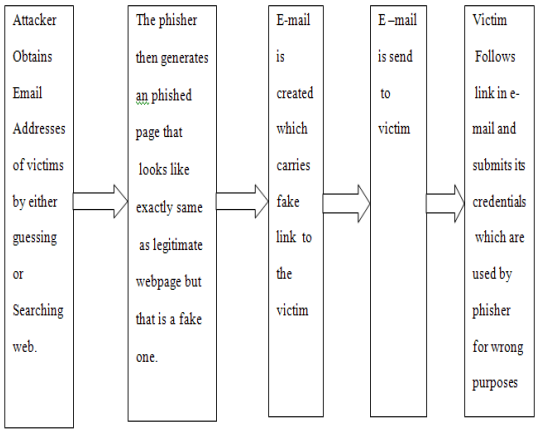

Fig 1: flow of phishing process

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[2,,4,5,6,7,8,9] work after the creation of phishing page and determine whether a page is phished or not whereas prevention methods like Yahoo Sigh-In Seal [10] works before phishing and do not let phishing to happen. There are many detection techniques available like attribute based detection(Attribute-based anti-phishing strategy implements both reactive and proactive anti-phishing defenses. This technique has been implemented in PhishBouncer [5]), character based detection(Character based anti- phishing technique uses characteristics of

hyperlink in order to detect phishing links. Linkguard [7] is a tool that implements this technique.),content based anti-phishing (GoldPhish[8] tool implements content based anti-phishing.this tool analysis the rank of the concerned web page using Google page ranking algorithm as phished has lower rank and legitimate page has higher rank.) etc with their own merits and demerits respectively. Preventive techniques mean the methodologies employed by organizations to avoid the phishing attacks.

III. Preventive Technique Of Anti-Phishing Via Code Retrieval in Detail

We have studied and analyzed that in maximum no. of cases phisher's aim is to acquire the credential from victims, and in order to accomplish this phisher make phishing pages in such a way that pages only has submission query which submits user's data to the database and does not retrieve any information related to user or website.

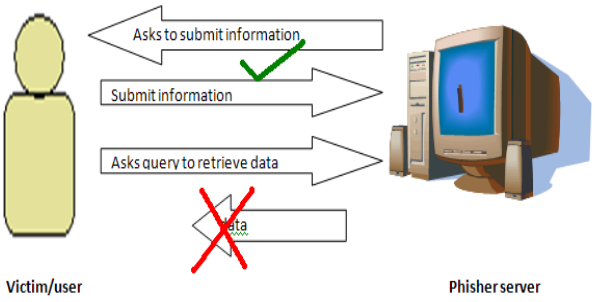

Fig.2: Exchange of data during communication between victim and phishing server

On the basis of above theory we made a prevention technique. Our main aim is to make web page to be able to retrieve some unique information from the server for every user whenever he visits the link . By the use of this technique users can get ensured themselves that they are logging on actual websites and not on the phished one. To use this technique one is required to get himself registered on the website which has implemented this technique.

The technique works in two phases as explained below:

A Sign-In Phase

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 unique code and saves it with user details
5. Organization provide code to user
6. User have to remember the code along with user id and password
7. Registration process complete

B. Sign-Up Phase

1. User gets page link via email or any other method.
2. User enters its user id and then she/he needs to enter any two digits (randomly generated sequence no.) of his unique code.
3. After that if digits enter by user is correct then full unique code is retrieved from server and then displayed on the user's screen.
4. User verifies the code and check that whether the same code is displayed which was created for user at the time of registration.
5. With this user becomes sure of legitimacy of the page and can freely enter its other credentials

Code Generation Technique.

In this technique the code is generated via calculation method using simple mathematics as follows:

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

Y=date(date)+ month(date)

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

Note: Here no. character in user id and password is not less than five characters and if the sum of date and month is less than 10 then add ten in sum of date and month.

After code generation first four digits are chosen by user for pattern making.the code word generated is unique to each user.

After generation of code word ,each digit of code word is displayed in four cells as shown below:

Fig 3: unique code cells

Whenever the user logs on the websites, after entering his user id (uid) he is asked to enter any of two digits (randomly chosen sequence no.)of his unique code. If the digits matches with the unique code saved in database then his complete unique code is displayed on the screen. Then User needs to verify that code for ensuring himself that he/she is logging on the actual website not on a phished website.

For example: if the codeword is 5678 and user enters values of 2nd and 4th cell then server automatically generates complete code by inserting values of cell 1st and 3rd cell as shown below.

Fig4: code retrieval form legitimate website

After verification user can enter its credentials on the website.This makes user to feel authentic about the web page.

Advantage

As it is connected with the user's 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 by hacking. This problem can be overcome by limiting the no. of of trails to enter values the code digits

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

We may make,After three attempts cells where code digit is entered to be blocked and user needs to enter whole code for logging by manually visiting the website.

IV.CONCLUSION AND FUTURE WORK

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.

As the time will passes no. of user will increase on the site so it may become difficult to give unique code to every user in only 4 digits so we can move up to six digits code(include one or two digits character) and map the old user's four digits code to the new one along with new users.

For ex: if a user's code is 3271 then it is mapped in to 31A8B7 here 'A' and 'B' can be initial letter of his name and password. And 3,1,8,7 are new sequence no. digits. Here user do not need to remember his new code. Whenever user login on the site he is asked to enter only two digits which is internally checked with the mapped code and if correct match is found then his old 4 digits code is retrieved.so here all the complexity we hide from the end user

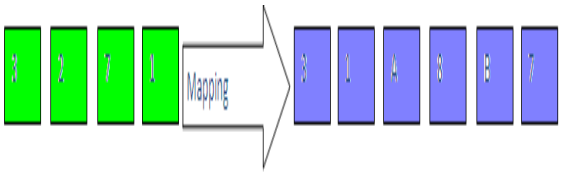

Fig5: mapping process

REFERENCES:

1. http://www.google.com/blogspot/phishing
2. 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 .
3. http://www.antiphishing.org.
4. 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.
5. Michael Atighetchi, Partha Pal "Attribute-based prevention of phishing attacks" Eighth IEEE international symposium on network computing and application, 2009.
6. 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.
7. 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.
8. 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.
9. 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.
10. http://security.yahoo.com/article.html?aid=2006102507