The Process of Secure Login using Hardware Device for Various Phishing Prevention Systems

Amit Solanki[1], S. R. Dogiwal[2]
[1,2]Department of Computer Science & Engineering,
Swami Keshvanand Institute of Technology Management & Gramothan, Jaipur, India
Email- [1]amit.solanki48@gmail.com, [2]dogiwal@gmail.com
Received 6 Feb 2015, received in revised from 2 April 2015, accepted 2 April 2015

Abstract: **Phishing websites are faked web pages which are developed by people to mimic web pages of original websites and it seek to deceive people of their personal information. The affect of phishing is quite forceful since it needs the threat of identity theft and financial losses. A lot of organizations and groups are attempting to study this problem and also inform and update the people on the latest tactics being used in the phishing sector. This paper explains the phishing prevention using USB Login technique to prevent phishing from unauthorized users.**

Key Words: **Security, Phishing, Anti-phishing techniques, Hardware.**

1. INTRODUCTION

The word 'Phishing' initially emerged in 1990s. The previously hackers frequently use 'ph' to replace 'f' to produce new words in the hacker's community since they mainly hack by cell phones. Phishing is a new word introduced from 'fishing' which refers to the fact that the attacker visit a forged website by mailing the faked e-mails and stealthy get user's personal information such as user name, password and secure number etc. This collectively information will be used by the attacker for future theft or also used for some kind of identity theft attacks (e.g., sending money from original user's bank account). The phishers frequently used this technique to send e-mails to possible victims, which likely to be sent by legitimate organizations. After accessing the e-mails which was send by phishers, this mail can make some problems e.g. it will ask the users to enter their credit card number and password many times unless if user entered it correctly, or also they are allowing promoting services, to ensure the user to visit their faked websites to conform or modify the user itself account number and password with the help of hyperlink which was provided in the e-mail messages. As user click on the hyperlink, it will transfer or linked the user to a counterfeited website. The overall design, functionality, performance of the websites is too much similar to the original websites even though the URL of these faked websites is much similar to the real website. It's very difficult for the user to identify the difference between the real website and malicious site. The attackers successfully gather all the data which the user is entered in the website such as inputting the account number and password and with some of user personal information[1].

2. PROBLEM STATEMENT

Today a wide range of Anti phishing software and techniques are available but the most important problem is to find the best anti-phishing technique which solves the problem faced by the user, and also which is compatible with the runtime environment and easily modified as per need. Students always try to find such application which can solve their problem easily. Anti-phishing techniques which exists provides the best solution but different technique can be implemented that will be more efficient.

3. CLASSIFICATION TECHNIQUES AND ATTACKS

After getting the identification, personal information and various profiles of the individual spam group, the developer now can try to modify and discern the purpose of phishers. In current scenario there are eight specific top-level spam classifications including these four:

- *Unsolicited commercial e-mail (UCE)* This classification is mainly developed by the company or organisations which are trying to be in conversation with the existing or potential regular customers. The True UCE is now using worldwide very rarely, it accounting for less than one-tenth of 1 percent of all generated spam. So today its vanishes fast as phishers are developed new techniques to access the user personal information.
- *Nonresponsive commercial e-mail (NCE)* NCE is manly sent by a legitimate company that want to continue to contact a user after it remove itself from that group or organizations, NCE mailer will continue to contact the user. The only problem with NCE is that, those user which are subscribe to many services, purchase items online, or initiate contact with the NCE Company. The key differences between UCE and NCE are:
  a) The user initiated contact and
  b) The user later opted out from future communication.
- *List makers* are spam groups that make money by harvesting email addresses and then use the list for profit such as selling the list to other spammers or marketing agencies.
- *Scams* constitute the majority of spam. The goal of the scam is to acquire valuable assets through misrepresentation [2].

A. *Impersonation attack*

Impersonation is the simplest and the popular method of deception. It consists of a completely fake website that receiver

is deceived to visit. This fake site contains images from the real Web site and might even be associated to the real site.

The impersonation type of phish is the most frequent method and is straightforward, valuable and fast. The characteristic approach is to mirror the target first. There are a couple of rapid ways to perform a mirror but since we are base our attack on actual profile of precise phishers this example uses the same technique used by a phisher, a web mirroring tool spread with most Linux and BSD platform scaled, which is once again trouble-free to use and efficient [3].

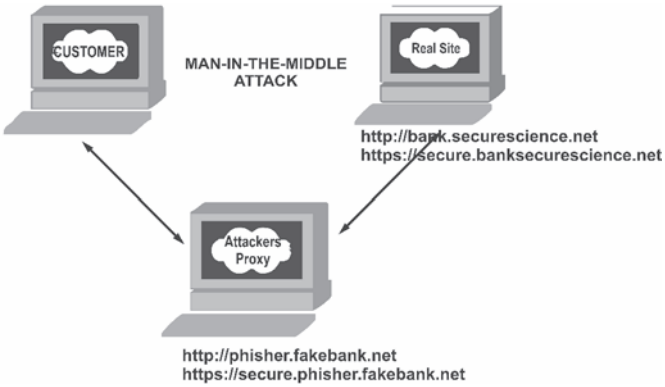

Fig 1: Man-in-the-Middle Attack

B. Forwarding Attack

In the forward phishing technique the model approach is to gather the data and forward the victim to the actual site. This is one of the further sophisticated types of phishing attack since there is no collection Web page, no images and the only server is concerned it has just a redirect script. The user is prompted for his or her information inside the e-mail itself.

This phishing style is popular with eBay, PayPal and e-retail companies such as Amazon. These companies are more likely to e-mail you regarding possible benefits and new services offered so it would make more sense to imitate the approach that is more comfortable to customers of e-retail. Phishers take advantage of e-retail because those businesses are more likely to put out newsletters and on a regular basis more marketing information is provided to their customers by them. Throwing a phishing e-mail in there once in a while might not raise customer's suspicion. E-Retail targets have more ROI due to the flexibility of possible ventures they could employ to lure victims.

C. Popup Attack

The Popup phishing technique introduces a pop-up window on the actual site that will forward the intended victim to the objective phishing server. This approach is the most unusual type of attack today because popup blockers are broadly used and included as default setting by numerous browsers existing in the market which lowers the success rate of this process.

In the popup attack scheme our phishing server will be set up to introduce a popup window while redirecting the victim to the real target. For our case we will disable our popup blocker to state this method. We will not be using the MITM POST technique but that does not indicate we cannot. The popup is a more creative approach since in essence we are using JavaScript to open an evil window capture the victim's information and really placing the legitimate site following it. This adds to the illusion of authenticity and since we are not performing the MITM technique detection becomes more complex [4].

4. EXISTING ANTI PHISHING TOOLBARS

There are a range of methods that can be used to recognize a page as a phishing site, together with white lists (lists of known safe sites), blacklists (lists of recognized fraudulent sites), different heuristics to see if a URL is approximating to a well-known URL and community ratings [5]. We used openly available information provided on the toolbar download web sites as well as our observations from using every toolbar to catch a basic understanding of how each toolbar functions.

A. Cloudmark Anti-Fraud Toolbar

The Cloudmark Anti-Fraud Toolbar, shown in fig 2 relies on user ratings. When visiting a site user have the choice of reporting the site as superior or bad. Therefore the toolbar will display a colour icon for every site visited. Green icons shows that the site has been rated as legitimate, red icons point out that the site has been determined to be fake and yellow icons specify that not sufficient information is known about the site to construct a determination. In addition the users themselves are rated according to their record of accurately identifying phishing sites [5]. Each site rating is calculated by aggregating all ratings given for that site, with each user's rating of a site weighted according to that user's status. The Cloud mark Anti-Fraud Toolbar executes on Microsoft Windows 98/NT/2000/ XP with Internet Explorer.

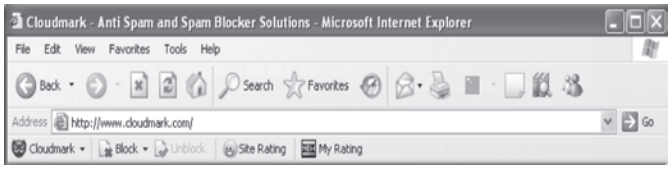

Fig 2: Cloudmark Anti-Fraud Toolbar demonstrating a legitimate site

B. EarthLink Toolbar

The EarthLink Toolbar, represented in fig 3 appears to rely on a grouping of heuristics user ratings and manual verification. Little information is showed on the EarthLink website however we used the toolbar and observed how it functions. The toolbar allows users to report suspected phishing sites to EarthLink. These sites are then verified and added to a blacklist. The toolbar also appears to observe domain registration information such as the owner age and nation. The toolbar shows a thumb that changes colour and location. A green thumbs up represents a established legitimate site whereas a gray thumbs up indicates that the site is not doubtful but it has not been verified. The red thumbs down shows that a site has been verified to be fraudulent whereas the yellow thumbs down indicates that the site is “doubtful.” The EathLink Toolbar runs under Internet Explorer as well as Firefox [6].

Fig 3: EarthLink Toolbar showing a legitimate site

C. eBay Toolbar

The eBay Toolbar, shown in fig 4 uses a combination of heuristics and blacklists. The Account Guard indicator has three modes: green, red and gray. The icon is indicated with a green background when the user looks a site known to be operated by eBay (or PayPal). The icon is indicated with a red background when the site is a recognized phishing site [7]. The icon is indicated with a gray background when the site is not operated through eBay and not recognized to be a phishing site. The toolbar also gives users the capacity to report phishing sites which will then be verified before being blacklisted. The eBay Toolbar runs under Microsoft Windows 98/ME/NT/2000/XP with Internet Explorer.

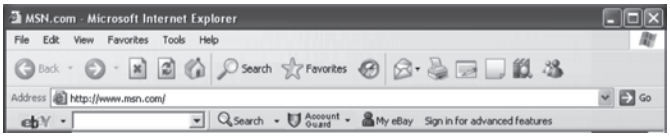

Fig 4: eBay Toolbar at a site not owned by eBay that is not identified to be a phishing site

D. GeoTrustTrustWatch Toolbar

Geo Trust's Trust Watch Toolbar, shown in fig 5 labels sites as green (confirmed as trusted), yellow (not verified) or red (verified as fraudulent). Geo Trust workings with several third-party status services and certificate authorities to confirm sites as trusted. Geo Trust's web site provides no information regarding how Trust Watch determines if a site is fake, however we suppose that the company compiles a blacklist that includes sites reported by users through a button showed on the toolbar. The toolbar also allows the user to store a convention image or bit of text that is regularly displayed so that he or she knows that the toolbar is not being spoofed. Trust Watch runs on Microsoft Windows 98/NT/2000/XP with Internet Explorer.

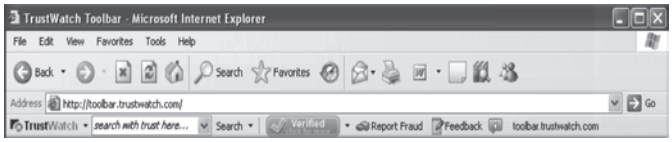

Fig 5: Geo Trusts Trust Watch Toolbar at a verified site

E. Google Safe Browsing

The Google Toolbar, shown in fig 6 includes a tool called "Google Safe Browsing" designed to recognize fraudulent web sites. Google Safe Browsing was originally a Firefox extension but it has since been included into the full toolbar and is expected to be built into Firefox 2.0. Google gives the source code for the Safe Browsing characteristic and says that it checks URLs against a blacklist. However, it is not identified how URLs are added to the blacklist. According to the download site the tool combines "advanced algorithms with reports about misleading pages from a number of sources." We expect that this means that the tool uses blacklists as well as heuristics. The toolbar also includes a Page Rank characteristic (which essentially denotes the popularity of a specified site) that can be useful in identify phishing sites as mainly phishing sites have a very low Page Rank [5]. The toolbar shows a popup if it suspects the visited site to be fraudulent and provides users with a option of leaving the site or ignoring the word of warning. The toolbar includes an "superior Protection" option which the software claims "will provide more advanced protection by sending the URLs of sites that you visit and partial information about the site content to Google for evaluation." This option is enabled by default. The toolbar runs on Microsoft Internet Explorer under WindowsXP/2000 SP3+, or Firefox on most platforms.

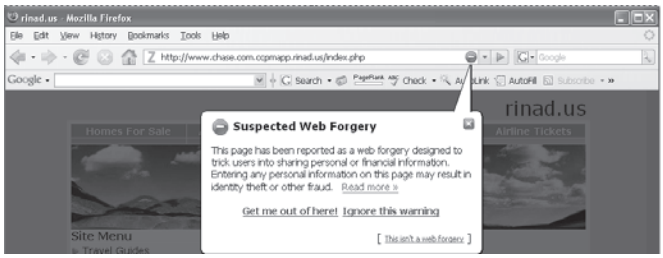

Fig 6: Google Toolbar at a fraudulent site

5. PROPOSED ANTI-PHISHING TECHNIQUE

This section describes the different steps in process for implementation of my proposed anti-phishing technique as follows:

A. Registration Process

The registration process used by the bank requires the following field to authorize the given client during login.

- Username (Account Number)
- Password
- Full name
- Email address
- Secret Code
- Serial Number of USB

Detail Steps for Registration:

Step-1: For the registration process bank requires the serial number of USB. To get the serial number of USB bank will choose the USB in random fashion and through the GET_USB method and then find out the serial number of USB after plug in the USB. This serial number is unique for each USB.

The below fig 7 shows various serial no. of the external drives, that are present in the system. When we begins the process named as GET USB, it will shows the serial no. of all the drives, by selecting the appropriate drive where the USB is connected, and show the drive name along with the serial no. of USB drive in the text box in the bottom of the diagram as shown "Drive Name :E:\ || Serial No : 842117". The current drive where USB is connected is drive 'E' and the serial no. of the USB is '842117' as shown in fig 7 below.

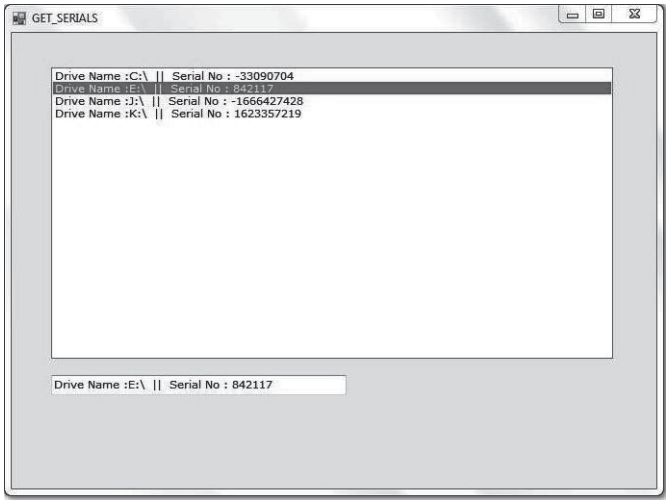

Fig 7: Detecting Serial Number of USB

After getting the serial number of USB which is unique for each USB bank will save this serial number for the future reference.

Step-2: Now after the success of step 1 bank will require the account number of the user who applied for the online facility. The Bank also having the account number of user, so bank will save the account no. in the text file and copied it to the USB in the step1 of registration process. For the reference we used the name of text file as CHINTAL.TXT here. The below fig 8 gives the details of the text file which contains the account no. of the user that is '28011985' which is saved in the USB with the file name CHINTAL.TXT.

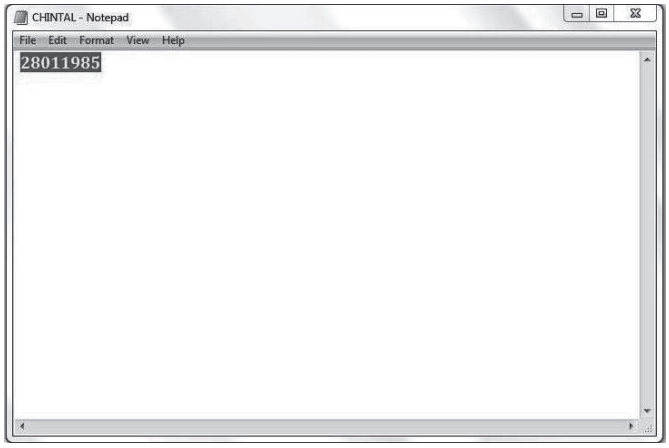

Fig 8: Display of User Account number in Text Format

Step-3: For enhanced the security user wants the security of the information which is stored in the USB. So here we use the RSA encryption and decryption algorithm to encrypt and decrypt the information (Account Number) stored in the USB. RSA algorithm will encrypt the information (account number) so nobody can read the information saved into the USB.

When the process is started, the below fig 9 shows the bank has to select various fields such as select drive, select folder and select file. For the Encryption process, the drive 'E' is selected, also select the folder and the file which contain the account information of user

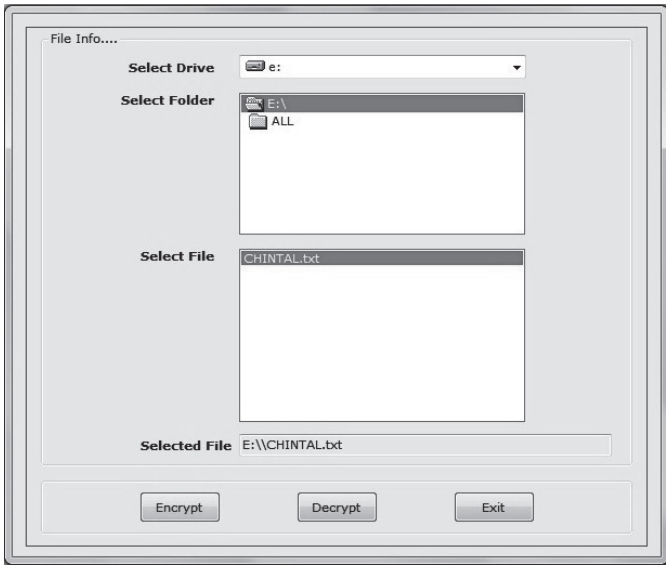

Fig 9: Encryption Process using RSA Algorithm

To encrypt the account no. of user, click on the encrypt button present in the above fig 9 to start the encryption process, after clicking the account number is now converted to encrypted form, and the status of the encryption is shown in fig 10 by the message window as 'Encryption Is Complete'.

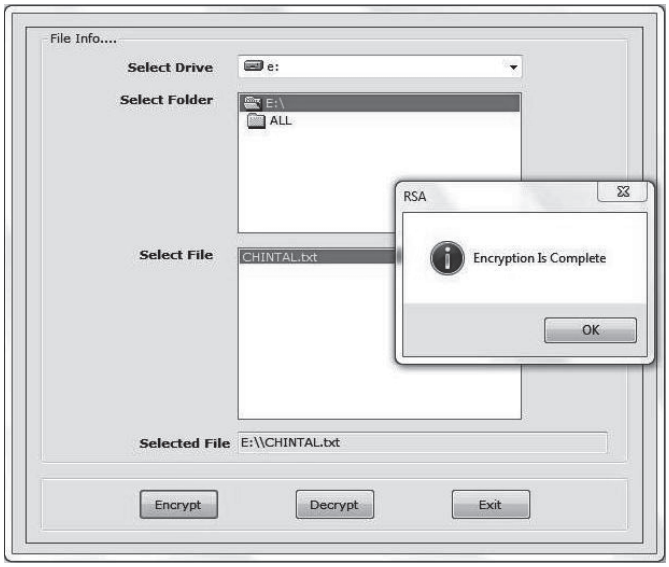

Fig 10: Successful Completion of Encryption Process

Step-4: Now bank will go for the registration process. For the registration process bank will require the following information:

- Username (Account Number)
- Password
- Full name
- Email address
- Secret Code
- Serial Number of USB

Bank is also having all the information about the user. Bank will have the user ID, password, Email ID, Secret Number (to reset

the password) and the Serial Number is also which is saved in the step 1.

After filling all the information necessary for the registration process bank will click on the proceed button shown in fig 11 to confirm the registration of the user on this serial number of USB and the Account number.

Fig 11: Registration Process for Bank

Step-5: After successful registration of user bank will provide the USB to the user for the transaction process and user can use the User ID, password and USB given by bank for the Login.

USB contains the account number of the user in encrypting way and it is in unreadable form for outside the world.

The Serial number extract from the USB is now associated with the user's account number. If user will use another USB for login then user will not be able to achieve the successful login without the correct USB. If user will not use the USB and he will use only user ID and Password for the login, he cannot proceed. Now the login process is fail due to absence of the USB. So user needs the USB given by the bank every time when he wants the successful login into his account.

After the encryption the user's information is more secured & even if the USB is lost from user side, no one can read the information saved inside the USB.

6. RESULT ANALYSIS

To obtain the computational results for the implementation of anti phishing technique which is named as implementation of an anti-phishing technique for secure login using USB, which includes a USB device to provide more security and authentication to any system? I have studied various techniques for detection and prevention of phishing and they have defined and implemented various anti phishing techniques. I described the anti-phishing technique that is developed by summarizing our findings and offer observations about the usability and overall effectiveness of these techniques.

To design and implementation of this anti phishing technique i have used the Microsoft .net frame work 3.5 for coding as a front end and for the back end data base SQL server 2008 is used.

Initially after completion of registration process the bank will hand over the User_Id , password and the USB associated with the specific account number to the user

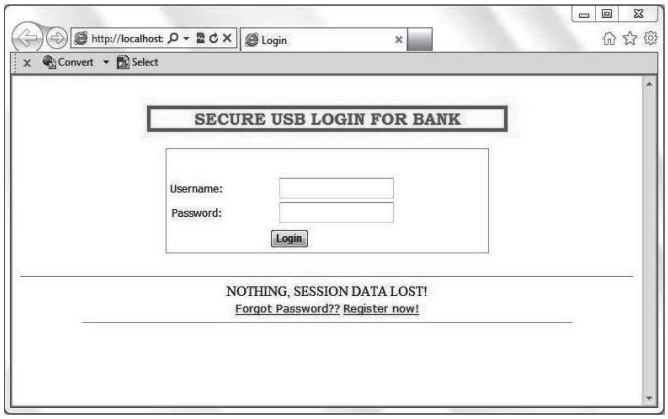

Fig 12: Secure USB Login Form for Bank

Now the user will open his own browser and then enter the URL of the concern bank for internet banking shown in fig 12. Then there will be a information on the desk for login.

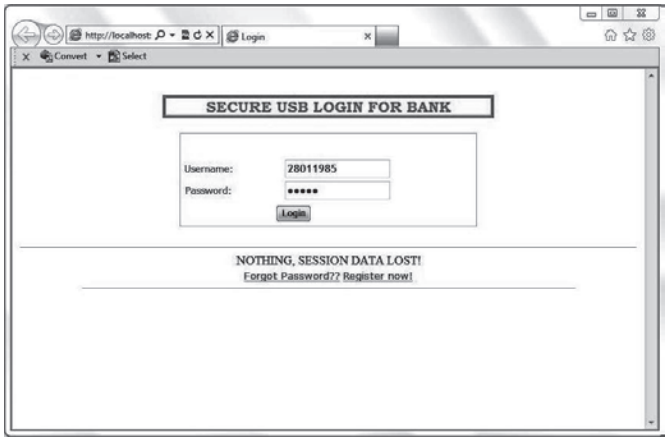

Fig 13: Secure USB Login Process with User's Information

Now user will enter his user-id and the password in the login window. User will have also the USB device provided by the bank. If user is not using the USB device and he is only using the user-id and password then he will be not able to accesss the successful login and window will show the warning message like " please plugin the USB for authorization" shown in fig14.

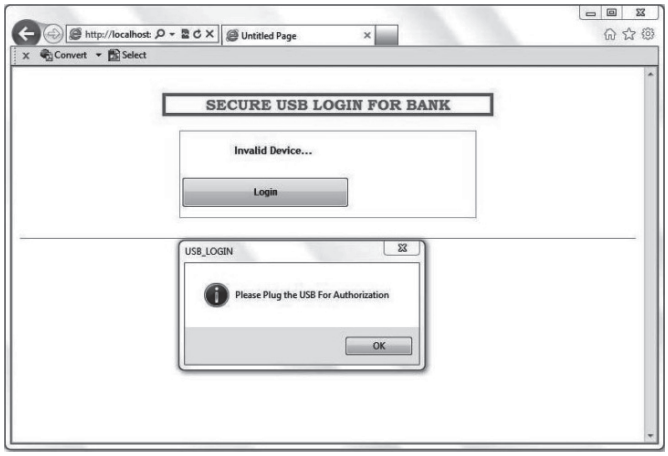

Fig 14: Invalid User Authorization

For the successful login it is very necessary that user must have to enter user-id, password along with plugin the appropriate USB device also. The user-id and password must be correct and the USB which is plugin must be associated with the account number of particular user.

User must take care of given correct entries and plugin the USB otherwise user can't access his account and window will show "un authorized entry".

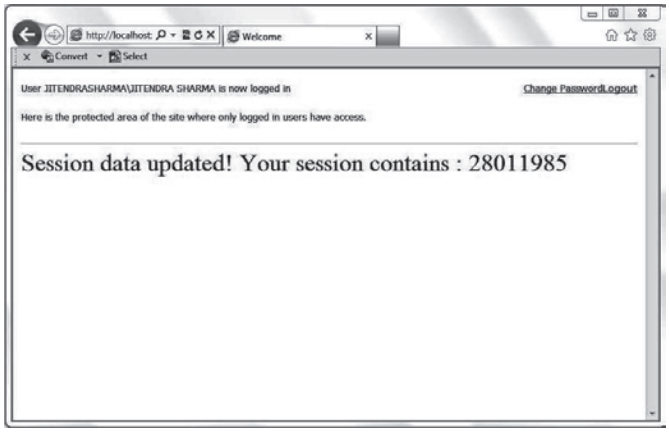

Fig 15: Successful Login of User

And if user will enter correct entries along with the correct USB which is provided by the bank then he will achieve the successful login given in the fig 15. Through the IATSLU phishing technique user can achieve the authentication and confidentiality to enhance the security.

7. CONCLUSION

The proposed anti- phishing technique gives detailed experienced towards its simplicity and it also setting up the various test cases. The extensive experimentation is performed for substantiation of implementation of all the components of the techniques work together. For this technique, the proposed work successfully implemented the various steps for anti-phishing technique such as Username (Account Number), Password, Full name, Email address, Secret Code, Serial Number of USB.

The GET USB method is to get the serial number of USB, and is executed successfully by providing the serial number to the user screen and this serial number is used for the registration process in future. The user account or user id in anti-phishing technique is securely encrypted using the RSA algorithm and copied to the respective USB which was issued to the customer for secure login. The main advantage of encrypting the user account is to protect the data from the other user, if in case USB is lost, other person get the USB and try to access the information contained within the USB, but now the data contained within the USB is in encrypted form or in more general we can say it is in non-readable format.

REFERENCES

[1] M.Madhuri, K.Yeseswini, U.Vidya sagar, "Intelligent phishing website detection and prevention system by using link guard algorithm" ISSN: 2231 – 1882, International Journal of Communication Network Security, 2013.

[2] By Pedro Latorre Carmona, J. Salvador Sánchez, Ana L.N. Fred," Pattern Recognition - Applications and Methods" ISBN 978-3-642-36529-4, Springer Heidelberg New York Dordrecht London,2013.

[3] Arne Padmos, "A Case of Sesame Seeds: Growing and Nurturing Credentials in the Face of Mimicry" Student NR:100693458, Royal Holloway, University of London,2011.

[4] Lance James, "Phishing Exposed" ISBN 159749030X, Syngress Publishing, Inc. USA. 2005.

[5] Lorrie Cranor, Serge Egelman, Jason Hong, and Yue Zhang, "Phinding Phish: An Evaluation of Anti-Phishing Toolbars", CyLab, Carnegie Mellon University' Pittsburgh, PA 15213,2006.

[6] EarthLink, Inc. EarthLink Toolbar. Accessed: November 9, 2006.

[7] eBay, Inc. Using eBay Toolbar's Account Guard. Accessed: June 13, 2006.

◆ ◆ ◆