ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

SOTCOT-Secure online transaction using co-ordination technique

Sujatha. E (Associate Professor), Kings Engineering College
Priyanka. B. M, Rohini. M, Shiny Kezia . S
(Computer Science and Engineering, UG scholar), Kings Engineering College

***Abstract*—: In internet banking websites security images are used often for login purpose in order to avoid phishing attack. So in this paper we are going to make internet banking more secure. we use security images to make more secure for internet banking. We provide secure online transaction using coordination technique. The Coordination technique is nothing but selecting particular coordinates from the given security images**

I. INTRODUCTION

Phishing is a cyber security threat which is performed with the help of social engineering techniques to trick Internet users into revealing personal and secret information. Detection and prevention of phishing attacks is a big challenge as the attacker performs these attacks in such a way that it can bypass the existing anti-phishing techniques. Security images and caption are used by the user each time for login purpose in internet banking.the user first register their account, he/she has to select security image from given list of images and also to create a caption with that image. Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. The security image and caption are shown to the user on all subsequent logins, and the user is instructed not to log in if she notices that the image or caption are missing or incorrect. This strategy is believed to help protect users from phishing attacks: During a phishing attack, a user might be attracted to a fake web site that mimics a real one in all ways except that it does not show the user's chosen security image; a vigilant user might notice the absence of the security image and refuse to log in.

Despite the almost ubiquitous use of security images on banking websites, their effectiveness at preventing phishing attacks is uncertain. Even setting aside strategies that a sophisticated attacker might use to show the perfect security image on a phishing site, users' ability to notice that an expected image is missing and then refuse to log in is not well understood.

Step 1: The attacker copies the content from the website of a well-known company or a bank and creates a phishing website. The attacker keeps a visual similarity of the
phishing website similar to the corresponding legitimate website to attract more users.

Step 2: The attacker writes an email and includes the link of the phishing website and sends it to a large number of users. In the case of spear phishing, a mail is sent to only selected targeted users.

Step 3: The user opens the email and visits the phishing website. The phishing ebsite asks the user to input personal information, for example, if the attacker mimics the phishing website of a well-known bank, thewn the users of bank are very likely to give up their credentials to the fake website.

Step 4: The attacker gets personal information of the user via the fake website and uses this information of the user for financial or some other benefits

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

Fig:life cycle for phishing attack

Previous studies of the effectiveness of security images have reached divergent conclusions: in one, 92% of partic- ipants proceeded to log into their bank account even when the security image was absent [5]; in another, 60% of users of an online assignment-submission system noticed missing security images and refused to log in These previous studies used different methodologies, making it difficult to reconcile their results or isolate specific reasons for their divergence. Additionally, both studies were carried out in settings sufficiently different from real-world online banking scenarios that it is difficult to generalize from their results. And here are some classification for phishing attack:

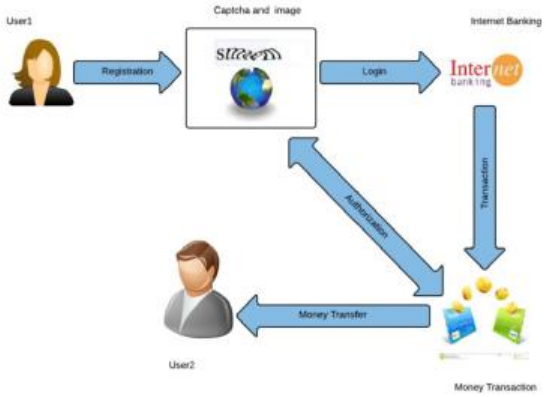
The zero-hour phishing attack: A zero-hour vulnerability refers to a hole in anti-phishing technique that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it.

- *Embedded objects:* A real webpage is downloaded to build the phishing webpage which appears just similar to a genuine webpage in appearance. Attackers cover the address bar by using an image or script which makes the online user believe that they have input to the right website. Attackers also use the embedded objects (flash, images, etc.) instead of HTML codes to avoid phishing detection techniques.
- *Domain Name System (DNS) attack:* DNS cache poisoning exploits vulnerabilities in the domain name system. In this attack, attackers divert Internet traffic from the legitimate website to the phishing website.

Architecture Diagram:

The user he/she has to register the account before login. For registration the user must give security images along with the caption in it.

Then the user login into their account which they already created .After login the webpage gets open in that the user may deposit,withdraw,transact,get balance.for transaction the user has to give again the captcha and image co-ordinates which they given earlier.if the co-ordinates are matched then the money will transferred to another account. [8] proposed a system about Efficient Sensor Network for Vehicle Security. Today vehicle theft rate is very high, greater challenges are coming from thieves thus tracking/ alarming systems are being deployed with an increasingly popularity .As per as security is concerned today most of the vehicles are running on the LPG so it is necessary to monitor any leakage or level of LPG in order to provide safety to passenger. Also in this fast running world everybody is in hurry so it is required to provide fully automated maintenance system to make the journey of the passenger safe, comfortable and economical. To make the system more intelligent and advanced it is required to introduce some important developments that can help to promote not only the luxurious but also safety drive to the owner. The system "Efficient Sensor Network for Vehicle Security", introduces a new trend in automobile industry.



Existing System

As a security measure, many banking websites

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

display a security image and caption each time a user logs into his or her account.1 When users first register for an account, they're prompted to pick a security image from a list of available images, and to create a caption to accompany the image. The user is presented with the security image and caption on all subsequent logins, and instructed not to log in if the image or caption is missing or incorrect. Despite the almost ubiquitous use of security images on banking sites, their effectiveness at preventing phishing attacks is uncertain. Even setting aside strategies that a sophisticated attacker
might use to show the correct security image on a phishing site, we don't have a good understanding of users' ability to notice that an expected image is missing and then refuse to log in.

Disadvantages of Existing System

- Low Security
- Slow Processing

Proposed System

We conducted an online study of security images' effectiveness that addresses some limitations of previous studies by accounting for habituation, addressing participant motivations, and varying security images' visual characteristics. We found that security images are only marginally effective — overall, 73 percent of our participants logged in even when the security image was absent. Moreover, our results suggest that varying the visual characteristics of security images has little to no impact on their effectiveness. The effectiveness of security images is similarly unchanged with varying levels of user habituation and motivation.

Advantages of Proposed System:

- High Security and Scalable
- Very Fast

Modules:

- Authentication and Authorization
- Grant Access
- Bank Manipulations
- Image Co-ordination

Authentication and Authorization:

In this module the User have to register first, then only he/she has to access the Online Banking. While registration the user can select the captcha and Image coordinators as they want. When the user login to the site, then he/she have to give correct captcha which they choose earlier. If the user gives wrong captcha, the account will be block. The authorization and authentication process facilitates the system to protect itself and besides it protects the whole mechanism from unauthorized usage. The Registration involves in getting the details of the users who wants to use this application.

Grant Access:

Admin will give permission to user accounts, once the user registered. Admin can Block and Unblock the user accounts. The user account will be blocked, if the user chooses wrong Captcha. Admin is the only person who can unblock the account.

Bank Manipulation:

We can do any manipulation like any other Banking Web sites such as deposit, transaction, withdrawal, Balance Checking etc. The user can create Savings or Current Account.

The user can deposit amount, withdrawal amount from their account. If the withdrawal amount is higher than the Balance amount, the user will not able to withdrawal the amount.

Image Coordination:

When the user try to transact the amount to other accounts, then they have to authorized using image co-ordination. The user

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

should enter correct image coordination to transfer the amount. He/She cannot transfer the amount using incorrect image co-ordination. It helps the user to secure the overall banking experience.

Conclusion:

The project 'Shape Recognition Using Image Processing' totally had acquired and it is the program that important to form a good database. The method that been used is the entire basic program from reading the image to acquiring the database from a binary image that already converted to an edge image. This image then is analyzing using Singular Value Decomposition to extract the identity of that particular image and finally the step of how the neural network forming recognition. Recognition is highly complex activity that can be done only in human brains. But in the name of Artificial Intelligence, thus the systems trained to recognize what the systems supposed to know and figure out.

Future Work:

Development of Advanced Techniques for Video Enhancement. Enhancement of the capability of already developed automatic face recognition system to handle large facial database with size of 100000 faces. Design & Evaluate face, Periocular and iris recognition algorithms to recognize images captured in both visible and near infrared domain at a distance up to 2 meters for periocular and Iris. And 5 meters for face. Design context switching algorithm for combining information obtained from face, Periocular and iris depending on the quality of images.

REFERENCES

[1] X. Xue, J. Jeon, and W. B. Croft, "The Effect of Haptic Support Systems on Driver

Performance," in Proc. 31st Annu. Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 2008, pp. 475–482.

[2] X. Cao, G. Cong, B. Cui, C. S. Jensen, and Q. Yuan, "Online security information," ACM Trans. Inf. Syst., vol. 30, no. 2, p. 7, 2012.

[3] J. H. Park and W. B. Croft, "Design and Analysis of a Graphical Password Scheme," in Proc. ACL, 2010, pp. 829–830.

[4] J. Allan, J. P. Callan, W. B. Croft, L. Ballesteros, J. Broglio, J. Xu, and H. Shu, "The Effectiveness of Intersection Attack Countermeasures for Graphical Passwords," in Proc. TREC, 1996, pp. 119– 132.

[5] J. P. Callan, W. B. Croft, and J. Broglio, "Enhancement of Password Authentication System Using Graphical Images," in Proc. Inf. Process. Manage., 2006, pp. 327–343.

[6] M. Bendersky and W. B. Croft, "An AGENT-BASED MODEL FOR CROWDSOURCING SYSTEMS," in Proc. 31st Annu. Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval, 2008, pp. 491–498.

[7] K. Collins-Thompson and J. Callan, "Forcing Johnny to login safely," in Proc. 14th ACM Int. Conf. Inf. Knowl. Manage., 2011, pp. 704–711.

[8] Christo Ananth, I.Uma Sankari, A.Vidhya, M.Vickneshwari, P.Karthiga, "Efficient Sensor Network for Vehicle Security", International Journal of Advanced Scientific and Technical Research (IJST), Volume 2, Issue 4, March-April 2014,pp – 871-877.

[9] J. Jeon, W. B. Croft, and J. H. Lee, "Graphical password authentication using cued click points," in Proc. 14th ACM Int. Conf. Inf. Knowl. Manage., 2005, pp. 84–90.

10] G. Zhou, L. Cai, J. Zhao, and K. Liu, "SSA makes online banking even more safe," in Proc. 49th Annu. Meeting Assoc. Comput. Linguistics: Human Lang. Technol. - Vol. 1, 2011, pp. 653–662.