ISSN (Online) : 0974-5645
ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(S2), 123–126, January 2015* DOI : 10.17485/ijst/2015/v8iS2/59167

Securing Online Bank Transactions from Phishing Attacks using MFA and Secure Session Key

S. Manasa*, P. Mullaimalar, G. B. Gnanaprakash Singh and S. S. Manivannan

School of Information Technology, VIT University Vellore-632014, Tamilnadu, India; manasa.jamuna@gmail.com

Abstract

Phishing is an online criminal activity using the collection of social engineering methods such as messages and emails to make the users to disclose their sensitive information such as personal details, username /password[4], etc. Since 2007 Net-Banking transactions are the target of the phishers. The strong techniques are required to avoid phishing attacks. In our paper, we proposed Multi Factor Authentication (MFA) and secure session key generation using Gaussian distribution to reduce the attacks caused by the phishers. Multi Factor Authentication technique authenticates the users using user's signature image recognition[8] and secret question answer. After successful authentication of user using Multi Factor Authentication technique, session key generated using Gaussian distribution is sent to user's mobile phone. User proceeds with the transaction only after entering the session key received[1]. By incorporating above mentioned techniques users can perform online transactions safely and securely.

Keywords: Gaussian Distribution, Multi Factor Authentication, Phishing, Session Key, Social Engineering

1. Introduction

Phishing is a social engineering attack where the attacker looks for weakness in the users and steals their personal information. The term Phishing originated from two words Phreaking (hacking of Phone calls which are the earliest method of hacking) and Fishing (fishers use bait to fish).

Phishing started in the year 1995 which targeted America On-Line (AOL) users. In the year 2001 phishers targeted on users of EBay and banks and by used key logger programs to gather account details and credit card information. From 2007 phishers major targets were banks and PayPal.

Phishers set up phishing web server, start sending emails to users and make them trust that these emails are from the actual banks[7]. When users respond to the mail by clicking the fake links provided in the mail, users are redirected to the fake website and provides all the sensitive information in that website. Phishers accesses the web server database where user's details will be stored and uses their details in the original bank's website and performs the transaction on behalf of the actual users[6].

Phishing attacks are classified in to 2 major types. Malware and deceptive phishing attacks. Malware phishing attack happens by installing the destructive software in the system of the user[2]. In Deceptive phishing attacks, false emails are sent to the user's inbox[2]. There exist 2 approaches to overcome phishing attacks. One is through educating users about the false emails and messages receiving in their inbox and other one is through making the software strong enough to identify such fake emails and websites and alerting the users.

User authentication is done in 2 ways. First, Single Factor Authentication[3] (SFA) which uses traditional username and password[4] to authenticate the users. Second, Multi Factor Authentication (MFA) which uses hardware, software or out-of-band such as email or SMS methods to verify the authenticity of the users[5]. In our paper, we have proposed user authenticity based on MFA such as user's signature image recognition and secret question answer. After successfully authenticating the user, session key is sent to registered user's mobile phone number. User uses the received session key to proceed with the transaction. In our paper, we have used Gaussian distribution to generate the session key which is used for single transaction.

*Author for correspondence

2. Proposed Work

In our paper, we proposed Multi Factor Authentication (MFA) and secure session key generation using Gaussian distribution to reduce the attacks caused by the phishers. MFA technique authenticates the users using user's signature image recognition and secret question answer. The user needs to enter username in the bank's login web page; if it is matched the user is provided with exact registered user's signature image along with 3 altered signature images and is asked to select his correct signature image for authentication. If it is successfully matched, the user is redirected to answer the secret question which is known only to him. In the above 2 steps of authentication, user tries to attempt wrong credentials, his/her net banking account will be blocked. After successful authentication of user using MFA technique, session key is generated using Gaussian distribution and sent to user's mobile phone. User proceeds with the transaction only after entering the session key received. Finally, user successfully logs out after performing secure and safe transaction

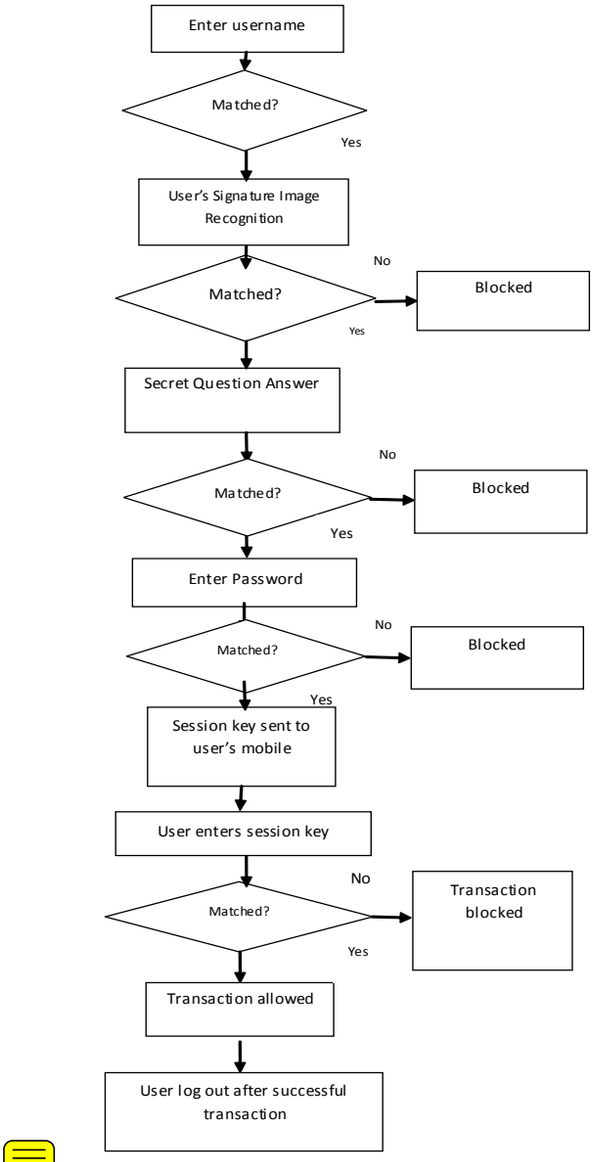

Figure 1. Flow of secure bank transaction.

2.1 Generation of Random Numbers using Gaussian Distribution

The session key used in our application is generated using Gaussian distribution. This distribution is also called Normal Distribution. In this distribution, the generated values tend to group around the average. The default shape of the distribution is obtained with average value of 0 and standard deviation of 1. This default shape can be changed by altering the values of average and standard deviation.

In order to change default average value, we add the required number to the returned value from the default function which is generating values with default average and standard deviation and to change standard deviation we multiply returned value from the function with the required number.

3. Discussion

Screenshots of Online Bank Transactions using MFA Technique.

The user need to enter his/her name in the login authenication page and the entered name will be matched with the database.

After successful match of username, the user will be redirected to the signature page where he has to select the correct signature image among the four images displayed. This is the first phase of authentication.

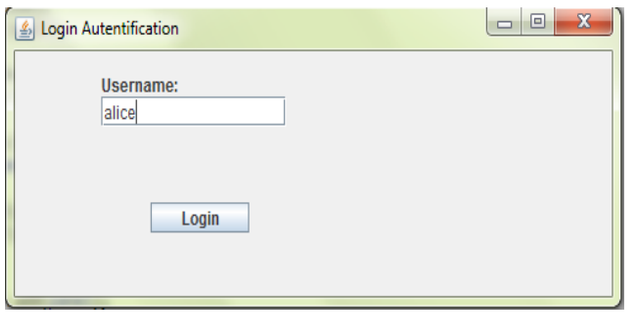

Figure 2. Login authentication page.

This screen shot displays the wrong signature image selection by the user.

This is the second phase of authentication. The user will be displayed with the list of secret questions.

Figure 3. Signature image identification page.

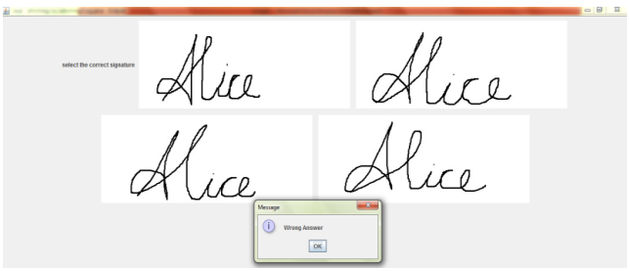

Figure 4. Signature image identification page .

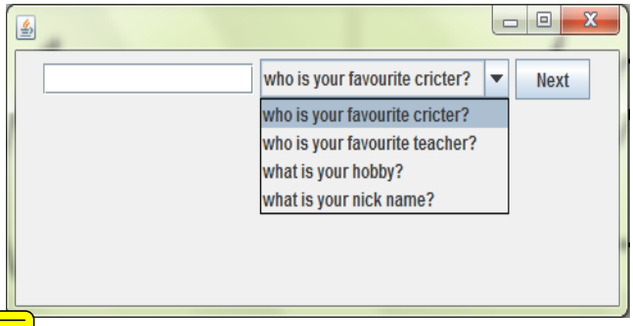

Figure 5. Secret question page.

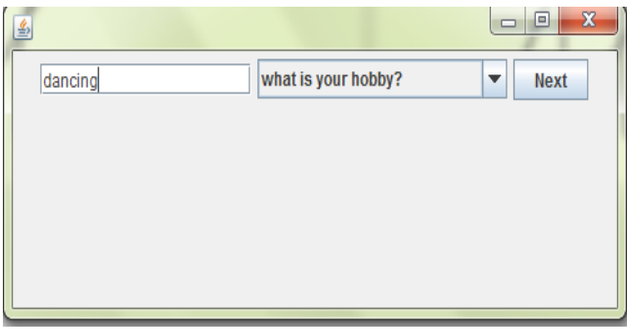

Figure 6. Secret question page.

After selecting the registered secret question, the user need to enter the correct answer and the same will be matched with database. If matched successfully he will redirected next phase of authentication.

This is the third phase of authentication in which user enters the password. After successful password match, session key is generated and sent to the user's registered mobile number.

The received session key is entered by the user. If matched the user proceeds with the transaction. This is the fourth phase of authentication.

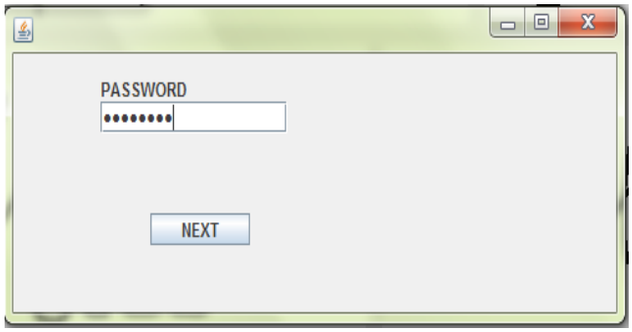

Figure 7. Password page.

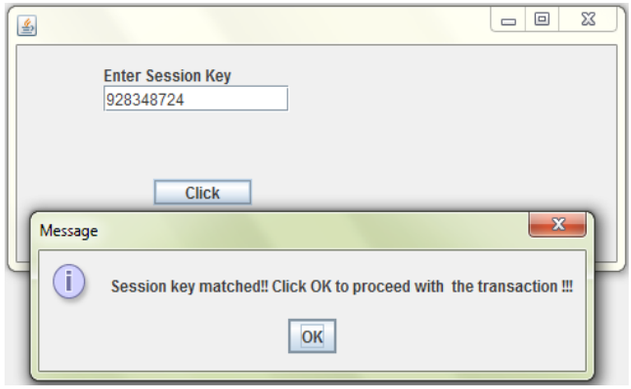

Figure 8. Session key page.

4. Conclusion

In this paper, Multi Factor Authentication (MFA) technique used has four phases of authentication as shown in the above section. The MFA enhanced the security level of online bank transactions against phishing attacks. Hackers are prevented successfully to a large extent from accessing the legitimate user's transactions. The Gaussian distribution based session key generation also enhances the security of online bank transactions.

5. Acknowledgement

We acknowledge VIT University, Vellore for the encouragement and permission to publish this paper. We would like thank Programme chair for M.Tech (IT), Prof. Sathiyamoorthy E., Associate Professor, for his support.

6. References

1. Dhanalakshmi R, Prabhu C, Chellapan C. Detection of phishing websites and secure transactions. IJCNS. 2011; 1(11):15–21.
2. Belabed A, Aimeur E, Chikh A. A personalized whitelist approach for phishing webpage detection. 2012 Seventh International Conference on Availability, Reliability and Security; 2012 Aug 20–24. p. 249–54.
3. Chaudhari S, Tomar SS, Rawat A. Design, implementation and analysis of multi layer, Multi Factor Authentication (MFA) setup for web mail access in multi trust networks. 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC); 2011 Apr 22–24. p. 27–32.
4. Hazlewood V, Kovatch P, Ezell M, Johnson M, Redd P. Improved grid security posture through multifactor authentication. 2011 12th IEEE/ACM International Conference on Grid Computing (GRID); 2011 Sept 21–23. p. 106–13.
5. Mohammed MM, Elsadig M. A multi-layer of multi factors authentication model for online banking services. 2013 International Conference on Computing, Electrical and Electronics Engineering (ICCEEE); 2013 Aug 26–28. p. 220–4.
6. Khonji M, Iraqi Y, Jones A. Phishing detection: a literature survey. IEEE Communications Surveys and Tutorials. Fourth Quarter 2013; 15(4):2091–121. doi: 10.1109/SURV.2013.032213.00009.
7. Ayodele T, Shoniregun CA, Akmayeva G. Anti-phishing prevention measure for email systems. World Congress on Internet Security (WorldCIS); 2012 Jun 10–12. p. 208–11.
8. Goyal P, Bansal N, Gupta N. Averting man in the browser attack using user-specific personal images. 2013 IEEE 3rd International Advance Computing Conference (IACC); 2013 Feb 22–23. p. 1283–6.