MAT JOURNALS

Journal of Web Development and Web Designing
Volume 2 Issue 1

Figurine Key Based User Authentication Using Bright Pass Method

Nirosha, Priyanka, Deepa.R
Department of Computer Science and Engineering.
Prince Dr.K.Vasudevan College Of Engineering and Technology,
Chennai, Tamil Nadu, India
E-mail: nirosheetha28@gmail.com

Abstract

The Social Network sites, shows that weak password and single factor authentication are still the main security weakness. The presence of malware in various application can seriously impact the user's privacy and security reducing the users trust. In existing system , pass window, CAPTCHA, drawing CAPTCHA, etc., have been used to provide security. The spyware injection are possible. Spyware injection to bypass classic authentication and steals user credentials. In order to avoid spyware Bright pass method is proposed. It allows users to authenticate safely with a PIN based confirmation in the presence of specific operations on sensitive data. In net-banking adding features to the OTP. It contains 4 digit PIN and in bright pass we are including the 7 digit PIN as 4 PIN is OTP and other 3 PIN is the fake PIN. Fake sequence depends on user oriented detail like their vehicle number , date of birth, marks. Based on brightness we have to enter the PIN. So, using this method user can securely carry out their sensitive data.

Index Terms*: Virtual Keyboard ,OTP, Spyware, Bright pass, net-banking.*

INTRODUCTION

A recent study from the Gmail and Twitter accounts hacks shows that the single factor authentication and the weak password are the still main security weakness faced by the online application users. The single factor authentication is a process of securing access to the given system such as network or website, that identifies the party requesting access through only one category of credentials. It actually needs the user ID and passwords only for authentication process. The most common example of SFA is password - based authentication. One of the main problem some kind of people stores the password in their pc's this can be hacked by the hackers. In the second case of weak password, some people have the habit of having password as his/her names or parents or friends this kind of possibilities can be tracked by any kind of persons. [8]So solution for this problem they have to use the alpha – numeric characters as their password for example if the person name is "Abdul" means they can have password as "Abdul$109".[10] In order to avoid problems occurring in SFA, two factor authentication method is proposed. These 2FA gathers additional information from the users.

Example one time password(OTP). This OTP can be sent via SMS or Gmail.[4] This 2FA is proposed in order to provide additional security to the online applications.[5]And it improves the users trust in order to use the internet for banking transactions or any other online based applications. And they can carry out their details in secured manner.

RELATED WORK

Some business owners or individual user may not feel comfortable with the idea of placing vital financial or sensitive

information into an online account, or may be apprehensive about using the Internet. Most of the application using the static password or the PIN codes for the authentication purposed in order to handle the sensitive data. But it is not much secure as the dynamic password. Spyware is a major problem which is occurring in the social network site and in online applications. Spyware is software that aims to gather information about a person or organization or that asserts control over a device without the consumer's knowledge.Spyware" is classified into four types:Adware ,cookies ,system monitors, tracking and Trojans.[6] In order to avoid spyware they introduce the pass- window technique, Re-CAPTCHA, clickable CAPTCHA, Drawing CAPTCHA etc., Even though using these methods spyware are also possible. [7]

The first proposed method is an pass window approach, this is an authentication method which uses the pre-selected image and the PIN number which is call pass-icon which can be used as an password. These pass icons are displayed to the user and these icons are displayed in random manner and the user has to memorize the location.

Fig 1: *Pass window,Re-CAPTCHA, Clickable CAPTCHA, Drawing CAPTCHA.*

These techniques prevent the shoulder surfing attacks and increases the security against the side channel attacks. The major problem in these techniques is it takes the longer time for authentication process. And it is an weak against multiple spyware based recording attacks. Second approach is an Re-CAPTCHA, CAPTCHA is an automated bot(simulated user), In order find whether the resource requestor is an human or an machine we are using the CAPTCHA technique.[7] In these technique user have to recognize the unknown word The user inputs the two words via keyboard which displayed in the screen. if the input is an valid one further process can be carried out. It prevents the automated bots. And this technique can provide the accuracy of 99.8% only and this is not applicable for the mobile devices. Third approach is an clickable CAPTCHA, in these the user have to recognize the targeted image. And the targeted image are displaced first and the grid contains the different kinds of images from this the user have to choose the targeted image. These method are also helps to prevent the automated bots, but the error rate is more. And the fourth approach is the Drawing CAPTCHA, in this methods the user have to recognize the shapes and they have to join the shapes in order to get the triangle shape.[7] It contains collection of squares and diamond shapes and the user have to choose the diamond shapes and join them, user can join the triangle in any sequence what there want. It is alternate to text-based CAPTCHA and this is suitable for the mobile devices. It has broken with the accuracy of 75%.

PROPOSED SYSTEM

Achieving higher levels of security for online transaction access we introduce these concept. An untrusted platforms requires to enhance and secure the classic widespread PIN authentication method. Especially, it is used in “Internet banking over the money transaction”. The idea consists in inserting a combination of the PIN digits and some misleading values, i.e. the lies. The order of the PIN digits

positions is randomly generated by the SE and then secretly shared with the user via an alternating circle's brightness displayed on the device. If the circle's brightness value is high, the user must insert a correct PIN digit. Whenever it looks dark the user, is required to enter a fake digit.

SECURE ELEMENT

User enter the fake sequence along swith the OTP generated using the Virtual Keyboard. OTP contain the 4 -Digits pin value. Balance 3-Digits can be of user memorable settings. It can be of last or first or random in which way they can memorable. User have to change periodically.

B. BRIGHT PASS METHOD

The Bright Pass Method achieves the higher levels of security and it is an wide spread PIN authentication method. In this method the secure element knows the fake PIN along with its position. And the position of the PIN's are randomly generated. Usual OTP contains 4 digits in this concepts we are adding the 7 digits. The 7 digits contains 4 OTP PIN as usual and 3 digits are of fake PIN. When the circle displayed in dark color user have to enter the fake PIN and in bright place user have to enter the original OTP.[4] The position of the PIN's are randomly changed. Fake PIN can be of vehicle number, date of birth or it can be of ration card number i.e the number which is easily memorable to the user are stored in the database. And the position of the circles are changed each and every time.[1] And the hacker try to view the digit means all the bright circle are 1's and dark circles tends to 0's and this produce the result as 0's at last. Using this method we can avoid the shoulder surfing attacks, brute force attack and the recording attacks.

Fig. 2: *E-Banking.*

C. 2FA- TWO FACTOR AUTHENTICATION.

The traditional method of authentication requires the user to enter only a username and password. They discussed the two factor authentication, it requires the user to have additional information before access to the system is granted. The information required to authenticate users includes one of the following methods Knowledge Based, Biometric, and Hardware/Software Tokens. In knowledge based method, involves the use of secret and open knowledge. i.e. a piece of information the user knows such as Personal Identification Number (PIN) or password. Second method is Biometric in this they discussed for authentication they were using the biological components of the user such as finger prints, face recognition. And the third method is something within the possession of the user with this method, the user may need to carry a token or smart cards in order to have the authorized access into the system. 2FA also reduce the risk of brute force attack, shoulder surfing attack, recording attack etc.[5] With the implementation of 2FA, organizations and individuals will worry less about the security of the online applications they use for personal or business purpose.

SYSTEM ARCHITECTURE

- The account holder of an corresponding bank creates and

account for online banking. For example IOB, SBI.

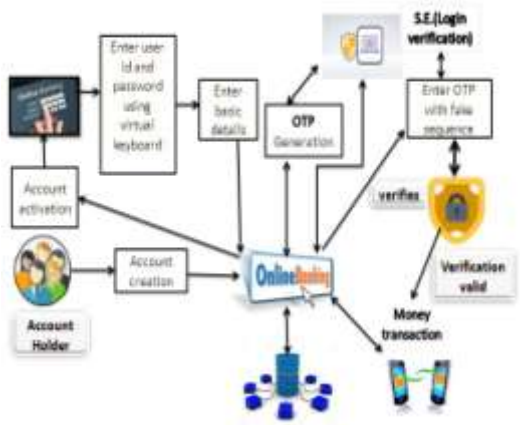

fig. 3: *system architecture*

- After account creation the account are activated by the corresponding bank.
- First the user have to enter their User Id and Password using the virtual keyboard. [8]
- After log in into their account the user can check their balance details, user can make transaction, user can check balance history etc.,
- In order transfer money user have to select the transfer option.
- The user select the payee is available other wise the user have to Add payee.
- In order to add the payee user have to fill the payee details of Account number, IFSC code, Account type , Bank name etc.,
- After adding payee the user have to click proceed in order to get the OTP.
- The OTP are generated and the user receives the OTP via SMS or Gmail.[4]
- Now, the user have to enter the OTP along with the fake digit using the virtual keyboard.[2],[9]
- At dark place user have to enter the fake digit and at the bright place user have to enter the original OTP.
- These original and the fake PIN are under goes verification process to the Secure Element. And the secure element verifies the PIN if it is an valid one it transfer the money. Other wise, it again re-generate the OTP the process repeated from the Transaction

PERFORMANCE EVALUATION

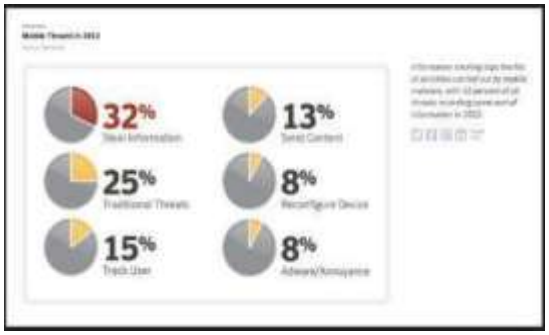

Fig. 4: *Evaluation.*

We have used a Bright pass technique in order to reduce the spyware . It can be using a single system interact with online transaction and the transaction makes safe through using this method. In this method fake sequence depends on the user own details so no one can't guess your data and additional we are entering OTP using virtual keypad if they view the position of your entering also no use. Using this method the spyware rate have been reduced.

CONCLUSION

In the existing system spyware injection is possible in online transaction even user has a OTP. Spywares are able to bypass classic authentication measures and steal user credential. It includes the feature of OTP to adding extra 3 digits as fake digit . It can be used to secure transactions protected by PIN verification codes**.**

REFERENCES

1. Meriem Guerar, Mauro Migliardi, Alessio Merlo, Mohamed Benmohammed Francesco Palmieri, and Aniello Castiglione Member, Using Screen Brightness to Improve Security in Mobile Social Network Access ,IEEE(2016).

2. Aviv, A. J., Sapp, B., Blaze, M., Smith, J. M.: Practicality of accelerometer side channels on smartphones. In ACSAC'12:Proceedings of the 28th Annual Computer Security ApplicationsConference, pp. 41-50. ACM, New York, NY, USA (2012).
3. Caviglione, L., Coccoli, M., Merlo, A.: A taxonomy-based model of security and privacy in online social networks (2014) International Journal of Computational Science and Engineering, 9 (4), pp. 325-338
4. Dinne, H., Mandava, K., (2010). "Two Way Mobile Authentication System". M.A. *Blekinge Institute of Technology: Karlskrona, Sweden*.
5. [5] Ikhalia, E., Imafidon, C. O.: The need for two factor authentication in social media. In Proceedings of the International Conference on Future Trends in Computing and Communication-FTCC, (2013).
6. [6] Kim, T., Yi, J.H., Seo, C.: Spyware Resistant Smartphone User Authentication Scheme.
7. [7] Lin, R., Huang, S., Bell, G.B. and Lee, Y. A new captcha interface design for mobile devices. In ACSW 2011: Australasian User Interface Conference, Curtin, Australia. (2011).
8. [8] Owusu, E., Han, J., Das, S., Perrig, A., Zhang, J.: ACCessory: password inference usingConference, pp. 41-50. ACM, New York, NY, USA (2012).
9. Simon, L., Anderson, R., PIN Skimmer: Inferring PINs Through The Camera and Microphone. In SPSM' 13: Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices, pp. 67-78. ACM, New York, NY, USA (2013).
10. Xu, z., bai K.,Zhu, S.: Taplogger: Inferring user inputs on smartphone touchscreens using on- board motion sensors. In WISEC '12 : Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, pp.113-124. Tucson, Arizona, USA (2012)