World Applied Sciences Journal 31 (7): 1297-1304, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.31.07.378

Shoulder Surfing Resistant Virtual Keyboard for Internet Banking

[1]S. Rajarajan, [2]K. Maheswari, [2]R. Hemapriya and [2]S. Sriharilakshmi

[1]Department of Computer Science and Engineering, SASTRA University, Thanjavur, India
[2]B. Tech CSE, SASTRA University, Thanjavur, India

Abstract: Today the prevalence of online banking is enormous. People prefer to accomplish their financial transactions through the online banking services offered by their banks. This method of accessing is more convenient, quicker and secured. Banks are also encouraging their customers to opt for this mode of e-banking facilities since that result in cost savings for the banks and there is better customer satisfaction. An important aspect of online banking is the precise authentication of users before allowing them to access their accounts. Typically this is done by asking the customers to enter their unique login id and password combination. The success of this authentication relies on the ability of customers to maintain the secrecy of their passwords. Since the customer login to the banking portals normally occur in public environments, the passwords are prone to key logging attacks. To avoid this, virtual keyboards are provided. But virtual keyboards are vulnerable to shoulder surfing based attacks. In this paper, a secured virtual keyboard scheme that withstands such attacks is proposed. Elaborate user studies carried out on the proposed scheme have testified the security and the usability of the proposed approach.

Key words: Virtual keyboard · Password · Authentication · Security · E-banking · Shoulder Surfing

INTRODUCTION

Motivation and Background: Banks without e-banking facilities are rare today. Online banking has become very popular and has been used by millions of users every day. It has revolutionized the way bank accounts are operated by customers. People may operate their accounts while they are in the office or at home with the help of a computer or mobile phone with internet connection. A number of services are provided through online banking to the account holders. There are also mobile applications to utilize online banking services through the mobile phones.

In spite of the enthusiasm among customers for utilizing the internet based banking services, they are also apprehensive about the security of their online transactions [10, 18]. There are a number of security threats confronting the online banking model. One of the common problems with online banking is the weakness in authentication systems and attackers exploit such weaknesses to steal the user's passwords [14]. This an identity theft and it could lead to looting of money from the user's bank account [15]. Several banks today provide virtual keyboards to enter passwords of online bank accounts. This is meant to prevent keystroke logging. But this aggravates the problem of shoulder surfing. It is much easier to attack through shoulder surfing when passwords entered through the on-screen keyboard.

This paper presents a novel solution to the problem of shoulder surfing attacks on virtual keyboards. The secured virtual keyboard proposed by us could successfully withstand all types of shoulder surfing including the camera recorded ones. Our solution is simple and effective. The user studies have vindicated that.

Challenges in Password Usage: The common method by which the user is authenticated during an online banking operation is with a combination of user id and password entries. The user id is either the email id of the user or any other value chosen by the user or suggested by the system. Passwords are alphanumeric string of a particular length. They normally include alphabets, numbers and special characters. Choosing a strong password that is not easy to guess or attacked through dictionary attacks is the responsibility the user. There are guidelines for

Corresponding Author: S. Rajarajan, Department of Computer Science and Engineering, SASTRA University, Thanjavur, India. Tel: +91-9994522260.

choosing a proper password that it hard for an attacker to break. But even with a strong password selected, it could still get revealed to an attacker while it is entered by the user at the bank's login page in a public place.

Poor Selection and Management of Passwords: Passwords should be chosen carefully so that they make it harder for anybody to crack them. Users should avoid using commonly known terms or values as their passwords [5]. Many times people use one of their personal credentials like first names, names of home towns, streets, family members, pets, date of birth, celebrity names etc. as their passwords. They choose such passwords in order to easily remember their passwords. These are normally termed as weak passwords [4]. Strong passwords are those that comprise of randomly selected characters, special symbols, numbers and few upper case letters. The length of passwords is also an important factor in determining the strength of the passwords. Passwords are also inadvertently revealed to others by the acts of writing them on note books, diaries, desktops etc. Maintaining infallible passwords involve the following some good practices in choosing and managing passwords.

Password Memorability: People have difficulty in remembering passwords that are in alphanumeric form [4]. As a result, they generally choose short, simple and easy passwords. One of the effective ways to mitigate password guessing is choosing long passwords that contain random characters with numbers and special characters. But that further complicates the ability for remembering and recalling them for authentication. Many systems enforce a rule that the users have to change their passwords periodically to ensure the sustained security of the system. This causes the users to get confused with their past and present passwords resulting in password forgotten option to get invoked. So clearly there is a conflict between strong passwords and memorable passwords.

Password Attacks

Key Logging: Keyboard logging or keystroke logging is the process of recording the key entries of the legitimate users without their knowledge [1, 3]. This could be carried out by using special keyboard that retrieves all the key entries and pass it on to an attacker who remotely monitors the login process. There are also programs developed and installed in the systems that covertly store the ASCII values of the keys typed by the users [6]. Trojans are available that could extract the user id/passwords of users and broadcast them to some mischievous people who would benefit by them. To overcome the problem of key logging, several banks provide virtual keyboards in their e-banking applications. Virtual keyboards are software components that contain all the keys present in the actual keyboard, but the keys could be entered by simply clicking them using the mouse. [9] have mentioned that keyboard logging could also be carried out using the browser plug ins also.

Shoulder Surfing: This is an attack in which an observer simply watches the keyboard entries to learn the password characters typed by the user [2, 16, 17]. Shoulder surfing could be carried out in a number of ways. The potential of shoulder surfing is elevated when virtual keyboards are used. Since the keyboard is openly displayed on the screen, it makes it much easier to observe the key entries. Shoulder surfing could be instigated either by simply watching the keyboard entry from a distance or by recording the whole process through CCTV cameras or by taking screen shots of key presses through special programs. The problem of shoulder surfing is particularly significant in public systems where the login process could be monitored by numerous people and the systems are not fully under the control of the user.

Password Cracking: It is the attempt of trying to recover the password of a particular user id by applying various possibilities. Textual passwords are more vulnerable to these attacks than biometric and graphical passwords. The time to crack the password depends upon the password strength. One of the common methods applied for cracking passwords is the brute-force attack. In a brute force attack, the computer tries every possible password value until it succeeds in finding the correct password. Brute force attack is efficient in detecting passwords in a reasonable time for short passwords. But for long passwords, a dictionary attack is more effective. In a dictionary attack, the computer program applies a list of words which are commonly used as passwords. The reason for the good success rate of dictionary attack is due to the tendency of people to choose their passwords in an easily predictable manner.

Phishing: Phishing is a type of attack in which the attacker attempts to acquire the information such as user id, password, pin no, credit card no. etc. by deceiving the user to believe that he is interacting with a trustworthy person [19]. The users would normally receive a phishing email with a link. Clicking that like will take them to a fake

web site which could insert malicious programs into the user's compute [2]. Sometimes a phishing email might ask the users to provide their account details for some verification purpose.

Virtual Keyboards: In order to overcome the potential problem of password stealing by keyboard logging, several banks provide a virtual keyboard option in their online banking portals to enter passwords. A virtual keyboard is an on-screen keyboard that lets users enter their passwords through mouse clicks and thereby avoiding the keyboard usage. Generally it is not compulsory for users to use virtual keyboards. Users are advised to use them to prevent any malicious key logging program that could have infected their computer. In touch screen devices without keyboards, virtual keyboards are the only method of entering data. Though virtual keyboards are quite effective in curbing the key-logging problem, they inflate the possibility of shoulder surfing. It is much easier to view or record the onscreen password entry than the entry by a normal keyboard. Especially when online banking operations are carried out at public places like Internet cafes, computer centers at educational institutions, computer labs at organizations etc., the potential of shoulder surfing is significantly elevated.

Related Works: So far there have been several research proposals for mitigating the shoulder surfing problem of virtual keyboards. [1] have proposed an anti-screen shot virtual keyboard. In this idea, the keys on a particular row of the keyboard would be replaced by some special characters when the mouse cursor moves over it. When the user click on a particular key, all the keys would be replaced by the special character such that a screen shot at that moment will not reveal the actual key aimed by the user. In another work, [7] have proposed a colored keyboard implementation. The alphabets and numbers in the keyboard are given different colors. The whole keys on the keyboard are shuffled every time after the user clicks a particular key. Before clicking on the desired key, the users have to note down the position of the key. Then a button captioned 'Hide Keys' have to be pressed. That will hide the characters from the keys and empty keys will be displayed. Users have to click on the key that contained the desired key earlier. They may utilize the key color for remembering this. A spy-resistant virtual keyboard for password entry in public touch screen displays was proposed in [13]. This approach is based on creating a tile of characters underlined in red, blue and green colors and hiding the keys at the moment when user makes a key selection.

Fig. 1: Comparison of the keyboard snapshots reveals that user clicked the character 'w'.

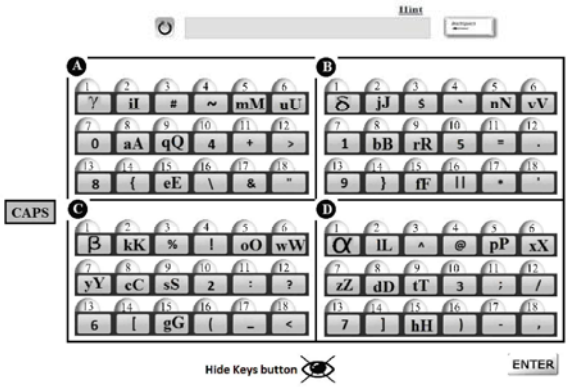

Fig. 2: Design of the proposed Virtual Keyboard with 72 keys with index numbers and group ids

The problem with most of these approaches is that they could only prevent only simple attacks by attackers who simply stand behind the users and watch the password entry. It is assumed that he will not be able to remember the positions of all the characters on the keyboard before they are hidden. But in case, if the attacker uses mobile cameras to take photo shots of the keyboard instances before and after the key entries, it is possible to compare the two keyboards and easily detect which key was actually pressed. This vulnerability also exists when the whole password entry process gets recorded through a CCTV camera or a malware records the whole process. This kind of attack is depicted in Fig 2 on the proposed method of [7].

A secured keypad based on tactile cues was proposed in [11]. Here the keys are represented through random vibration patterns. The password entry takes place through a sequence of tactons displayed through three keys. Since not visual feedback is provided on the pressed keys, visual attacks are prevented. A scalable shoulder surfing resistant password scheme which is a combination of graphical and textual password schemes was proposed by [17]. In this, the user need to click on a image consisting of characters The approach by [12] is based on tracking user's eye movement to determine the shape to be conceived based on the movements. Finally the shape constructed is compared with the shape in the

database to complete the authentication. A survey of the various virtual keyboards of smart phones provided by the various platforms such as Android, iOs, Windows, Symbian and MeeGo for their usability and shoulder surfing vulnerability was carried out by [8]. Their results show that some design variations are required in the design of virtual keyboards to withstand the shoulder surfing attacks on smart phones.

Our proposed approach relatively stronger than many of the proposed approaches in protecting against all types of shoulder surfing attacks and it is also easier to implement. We have introduced a second level of randomization of the keys before presenting the hidden keys to the users. This randomization is only known to the actual users since it was selected by them at the time of sign up and without the knowledge of it no one can know the expected position of the required key to be pressed next. We have also introduced a set of special characters called "virtual special characters" which are not available in the keyboards and are unique to the virtual keyboard. This is meant to enhance the security of passwords.

Proposed Virtual Keyboard

Keyboard Design: The proposed approach of this paper aimed to be foolproof against all possible shoulder surfing attacks both involving human observers, screen shots and camera recordings. The keyboard of the proposed approach consist of 72 keys, out of which there are 26 alphabets (a-z), 10 numbers (0-9), 32 special characters ($, #, ? etc.) and 4 virtual additional special characters introduced by us. In order to authenticate themselves to use the online banking account, users should first provide their user Id and the date of birth which were enrolled at the time of sign up or login creation. Once those details are verified with the database records, users will be shown the virtual keyboard to key in their passwords.

The authentication process of the proposed scheme involves the following steps:

- User enrolment: User creates a login for him providing his personal and account details.
- Selection of key-group transfer: User will have to choose from a list of methods during the login creation and that will be employed during the password entry.
- User login: User enters the user id and date of birth to initiate authentication.
- Virtual keyboard: Once the user id and date of birth are verified at the server, the virtual keyboard is shown to user.
- Password entry: User enters the password string and submits it for verification.

Operating the Virtual Keyboard for Password Entry: The keys in the virtual keyboard are logically divided into four groups- A, B, C and D, each comprising of 18 keys. When the keyboard is shown to the user, the keys are randomized such that they are not in any fixed positions. But to reduce the difficulty in locating the keys from the keyboard, the randomization is confined at the group levels and not at the entire keyboard level. That is, the 18 keys in each group are randomized only within themselves not across other groups. Then the user has to locate and remember the current position of the target key that is the next password character to be entered. To simplify the process of remembering key positions, an index for each key numbered from 1 to 18 are associated with each key in the keyboard. Similarly the group ids are also attached with each group. So the user simply needs to note down the index value and group id pertaining to the required key, for example A4 where A is the group id the 4 is the index of the required key.

Once they are noted down, user should click on the button captioned as "Hide Keys". Then a key transfer operation carried out according to the user's selection during the sign up phase. Accordingly, all the 18 keys in the 4 groups are transferred to other groups. The different options for the method of key transfer are given below.

Clockwise Circular Transfer: In this option, the 18 keys in each key group are transferred to their next key groups in a clockwise manner. But the column positions of the keys in the transferred groups remain unchanged. So the user only needs to predict the new group number of the target key after the transfer in order to select it. This is shown in Figure 3.

Anti-Clockwise Circular Transfer: In this option, the key transfers just happen in the anti-clock wise order. Figure 4 indicates this transfer method.

Cross-X Transfer: Here, the key transfers are happening in a cross wise manner. So the 1st and the 4th group keys are swapped with each other. Similarly the keys in the 2nd and 3rd groups are swapped with each other. This is presented in Figure 5.

Straight Transfer: In this scheme, the two groups in the same row are interchanged with each other. Figure 5 pertains to this way of keys transfer.

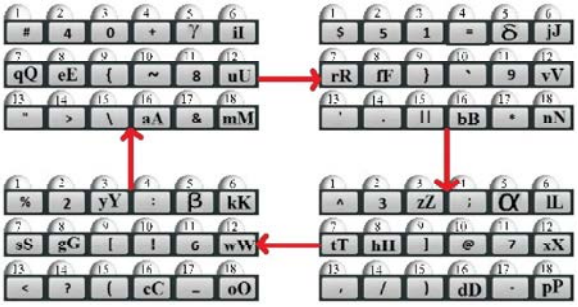

Fig. 3: Clockwise circular transfer

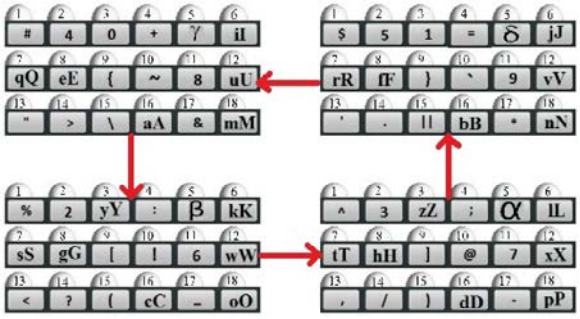

Fig. 4: Anti-clockwise circular transfer

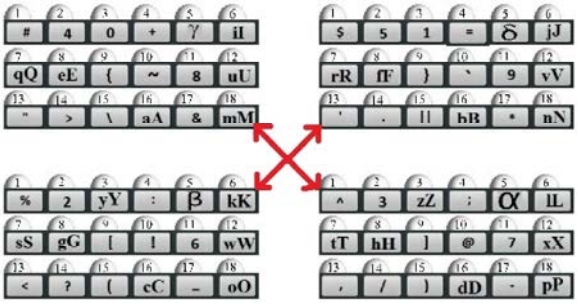

Fig. 5: Cross-X Transfer

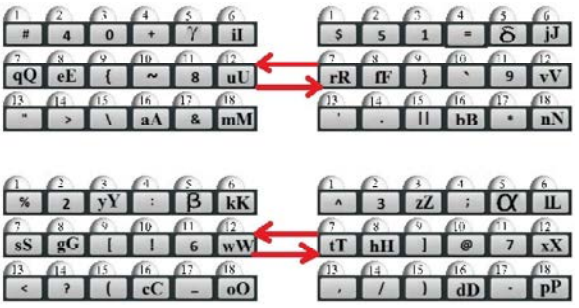

Fig. 6: Straight transfer

After the keys are transferred to other groups based on one of the above techniques, the user is shown a blank keyboard in which the key values are hidden. But the index values are shown to guide the user in clicking the needed key. With the knowledge of the key transfer method chosen by him previously, the user could guess

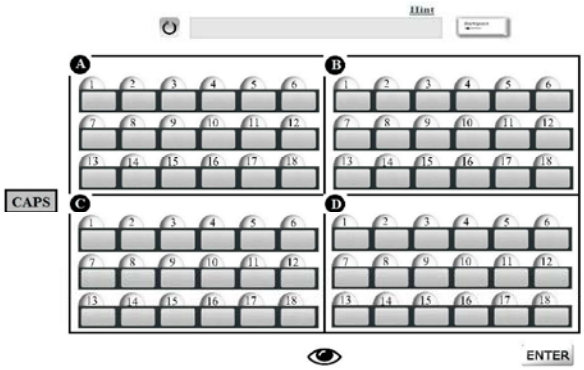

Fig. 7: Keyboard after Key group transfers and keys hidden

Fig. 8: Virtual Special Characters

the new key group into which his target key should have been transferred by now. He would now click on the blank key that is supposed to be the key of his password character. In case that the user has missed to note down key's index value or have forgotten that, he could just select the 'unhide' keys button to restart this process for that key.

After a key is entered, the keyboard is once again randomized and returns to visible mode. This process will continue till the user enters all the password characters and chooses to submit.

Virtual Special Characters: Along with the actual keys that are available in a normal keyboard and are used as password characters, we have introduced N new special characters into our proposed virtual keyboard. These keys are not actual keys and are not available in the conventional keyboards. If the banks want to enforce the usage of virtual keyboard to be mandatory for password entering, they may instruct the customers to include at least one of the Virtual special characters as part of their password strings. Since these characters can not be entered through normal keyboards, users will be forced to make use of the virtual keyboard every time they require to login. This eliminates the keyboard logging completely. It also enhances the password security since the meanings of these keys are only known to the system. So even if an attacker is able to extract the typed password, he will be clueless about which keys to be pressed to reproduce the virtual special characters. The four virtual special characters that are introduced in our implementation are presented in Figure 8.

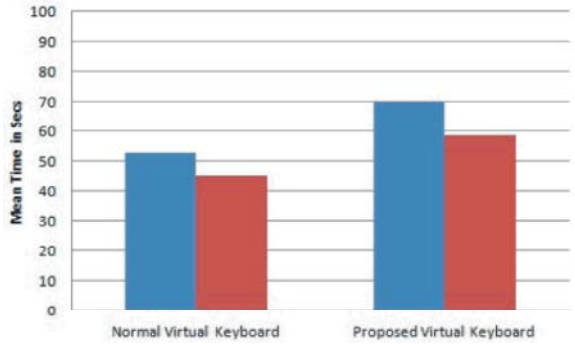

Chart 1: Average password entry time for students – blue and faculty members - brown

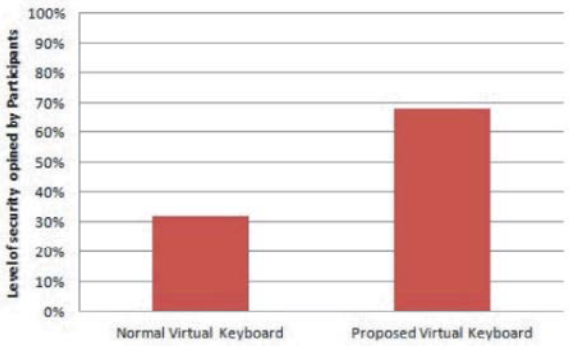

Chart 2: Participants opinion on relative security of proposed virtual keyboard

When these keys are pressed by users as their password characters, it will insert and s1 and and s2 and and s3 and and and s4 and respectively into the password string. The association with the key values and the keys are known to the virtual keyboard application and the server application that will carry out the password verification.

Safe Mode and Unsafe Mode: There is an option for the user to turn off the security mode of the virtual keyboard such that the keyboard appears and operates as a normal virtual keyboard without exercising any of the methods mentioned above. This could be opted by the users when they are ascertained to be logging in a safe location that is free of shoulder surfing possibility, probably in their own private environment using their personal systems. This relieves the users from going through the difficulty in entering their password using the secured virtual keyboard system. But it has to be cautiously exercised by the users. This is also useful when the users forget the key-group transfer method chosen by them earlier. They may simply turn off the security of virtual keyboard, log into the system and learn or reset the key-group transfer method.

RESULTS AND DISCUSSION

To evaluate the usability and efficiency of the proposed approach, a complete implementation of the secured virtual keyboard with all the mentioned functionalities was implemented in Asp.Net under Visual Studio 2010. Since this approach is proposed for online banking logins, running the application on a browser was desired. As a result, Asp.net was opted for the implementation.

The next step was to perform a hands-on user evaluation of our approach with participants. We identified 30 participants comprising of 15 students and 15 faculty members of our university. Since we wanted to assess the influence of age in the usage of our keyboard, we included staff members aged 40+ into our participants group. After giving all of them a presentation about our proposed approach, we sought their participation in analyzing the usability and security of our model. Then a computer with a projector connection was set up for the experiment so that every login process fully visible on a big screen. The 30 participants were requested to conceive a password of arbitrary length, comprising of alphabets, numbers and special characters. We told them to include one of our virtual special characters. They were then invited to come one by one to enter their passwords using the secured virtual keyboard. It has shown that the time taken for entering the correct password using our keyboard was relatively higher than the normal virtual keyboard. Chart 1 represents the time consumption. But given the higher security offered, the additional time is acceptable. It is also likely that it will take less time to complete password entry, once people start using it on a regular basis. The Participants were requested to answer for a question of "whether you consider the secured virtual keyboard providing better security for your e-banking login over your conventional virtual keyboard". More people have responded that they consider our proposed keyboard implementation to be offering higher security and were willing to adopt it for their Internet banking. Chart 2 shows that about 68% of participants were in favor of our approach.

CONCLUSION

Online banking usage is expected to grow in the years to come. It is the responsibility of the banks to guarantee the security of their customer's transactions carried out through their e-banking services. Though there are more secured biometric based authentications

available, the simple text passwords are likely to be the predominant method of user authentication due to their simplicity, cost and users friendliness. In this paper, we proposed an approach for designing a shoulder surfing resistant secured virtual keyboard for online banking logins. Through our evaluations, we learnt that the proposed approach offers superior password safety at the cost little complexity in password entry process and more time for completing password entry. To mitigate this added complexity and time, we provided an option to turn off and turn on the security mode of the keyboard. So, only when the users suspicious of shoulder surfing possibility, they need to enable the keyboard's security mode. In future, we wish to explore the possibility of extending our solution to touch screen based devices.

REFERENCES

1. Ankit Parekh, Ajinkya Pawar, Pratik Munot and Piyush Mantri, 2011. Secure Authentication using Anti-Screenshot Virtual Keyboard, International Journal of Computer Science Issues, 8(5): 3, September 2011.
2. Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, 2012. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication, World Applied Sciences Journal, 19(4): 439-444.
3. Nairit Adhikary, Rohit Shrivastava, Ashwani Kumar, Sunil Kumar Verma, Monark Bag and Vrijendra Singh, "Battering Keyloggers and Screen Recording Software by Fabricating Passwords".
4. Atif Qureshi, M., Arjumand Younus and Arslan Ahmed Khan, 2009. Philosophical Survey of Passwords, IJCSI International Journal of Computer Science Issues, Vol. 2.
5. Adams, A. and M.A. Sasse, 1999. "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, 42: 41-46.
6. Canbek, G., 2005. "Analysis, design and implementation of keyloggers and anti-keyloggers" Gazi University, Institute Of Science and Technology, M.Sc. thesis (in Turkish), Sept. 2005, pp: 103.
7. Agarwal, M., *et al*., 2011. "Secure authentication using dynamic virtual keyboard layout." Proceedings of the International Conference and Workshop on Emerging Trends in Technology. ACM.
8. Schaub, Florian, Ruben Deyhle and Michael Weber, 2012. "Password entry usability and shoulder surfing susceptibility on different smartphone platforms." InProceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia, pp: 13. ACM.
9. Pemble, Matthew, 2005. "Evolutionary trends in bank customer-targeted malware."Network Security 2005, 10: 4-7.
10. Rachwald, Rob., 2008. "Is banking online safer than banking on the corner?."Computer Fraud and Security 2008, 3: 11-12.
11. Bianchi, Andrea, Ian Oakley and Dong Soo Kwon, 2010. "The secure haptic keypad: a tactile password system." In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp: 1089-1092. ACM.
12. De Luca, Alexander, Martin Denzel and Heinrich Hussmann, 2009. "Look into my eyes!: Can you guess my password?." In Proceedings of the 5th Symposium on Usable Privacy and Security, pp: 7. ACM.
13. Tan, Desney, S., Pedram Keyani and Mary Czerwinski, 2005. "Spy-resistant keyboard: more secure password entry on public touch screen displays." InProceedings of the 17th Australia conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future, pp: 1-10. Computer-Human Interaction Special Interest Group (CHISIG) of Australia.
14. Usman, Ahmad Kabir and Mahmood Hussain Shah, 2013. "Critical Success Factors for Preventing e-Banking Fraud." Journal of Internet Banking and Commerce, 18: 2.
15. Moskovitch, Robert, Clint Feher, Arik Messerman, Niklas Kirschnick, Tarik Mustafic, Ahmet Camtepe, B. Lohlein, *et al*., 2009. "Identity theft, computers and behavioral biometrics." In Intelligence and Security Informatics, 2009. ISI'09. IEEE International Conference on, pp: 155-160. IEEE.
16. Raza, Mudassar, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, 2012. "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication." World Applied Sciences Journal, 19(4): 439-444.
17. Zhao, Huanyu and Xiaolin Li, 2007. "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme." In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, 2: 467-472. IEEE.

18. Fujita, K. and Y. Hirakawa, 2008. A study of password authentication method against observing attacks. 6th International Symposium on Intelligent Systems and Informatics, SISY 2008.
19. Ilkka Uusitalo and Josep M. Catot, 2009. Phishing and countermeasures in Spanish online Banking. 3rd International conference on emerging security information, System and Technologies.
20. Anand Sharma and Vibha Ojha, 2010. Password based authentication: Philosophical Survey. IEEE.