International Journal of Linguistics and Computational Applications (IJLCA) ISSN 2394-6385 (Print)
Volume 4, Issue 1, January – March 2017 ISSN 2394-6393 (Online)

A Survey on Trusted Corroboration System for Shoulder Surfing using Pass Matrix

Sindhujaa.R[#1],Tharini.L[*2],Vasagiri Pragna[*3], A.Jerrin Simla[*4], Dr.S.Hemalatha[*5], Dr.T.Kalaichelvi[*6]

[1,2,3]*Final Year, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, India.*
[4]*Assistant Professor, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai, India.*
[5,6]*Professor, ,Department of Computer Science & Engineering, Panimalar Institute of Technology, Chennai, India.*

Abstract— Human actions like selecting incorrect password, entering the password in an insecure way it will leads to weakest link in authentication. Due to the weakest link, an attacker can damage the hardware, software or theft the information. So our aim is to provide the smart way to authenticate the user's bank account. Authentication based password is used in computer security or IT security. Instead of using the alphanumeric as a password, rather than the user can selects the password as a image. With mobile application the user can expose the shoulder surfing attack. Attackers can observe the passwords via shoulder, spyware. To overcome the problem, an authentication system Pass Matrix is proposed based on graphical passwords to resist shoulder surfing attack. With a one-time valid login indicator and navigation buttons covering the entire scope of pass-image, pass matrix does not offer any hint or figure even they conduct camera- based attacks. As a result, the proposed system achieves the better resistance to shoulder surfing attacks.

Keywords— Pass Matrix; Login Indicator; Shoulder surfing Attack; Authentication; Spyware

1. Introduction

Textual passwords are mostly used for authentication. They are considered strong enough to resist[4][5].However, it is hard to memorize and recollect. Therefore, users tend to choose passwords that are short, rather than random alphanumeric strings and prefer to use same password for multiple accounts. Hence it is easy to crack the passwords [2].Textual passwords are often insecure due to the difficulty of maintaining strong ones. Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically[8]. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). It either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information[6]. The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are regarded as the weakest link in the authentication chain. Therefore, an authentication scheme should be designed to overcome these vulnerabilities. A secure graphical authentication system named Pass Matrix that protects users from becoming victims of shoulder surfing attacks is presented. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

2. Literature Survey

Fake Pointer: An Authentication Scheme for a Better Security against a Peeping Attack by a Video Camera byTetsuji TAKADA - Peeping attack in the real world is one of threats to a user authentication. What is worse is that an emerging attack method such as video capturing makes traditional measures against peeping attack insufficient. A unique user authentication scheme is named "fake- Pointer" for a solution to a peeping attack by video capturing. It makes hard for attackers to get a secret even if he/she captures an authentication scene using a video camera. The fake Pointer has two unique features to ensure a security against such a peeping attack. One is that fake- Pointer provides a double-layered interface for a secret input. This interface makes it hard for attackers to identify a legitimate user's secret even if they had a video record about target user's authentication action. The other feature is that the fake Pointer uses two secrets. One is a fixed secret and the other is a disposal secret. This feature enables to change a secret input operation in each authentication. This is also a necessary feature for ensuring security because if an attacker has many video records about a same user, an attacker can extract a secret by statistical analysis.

Honey, I Shrunk the Keys: Influences of Mobile Devices on Password Composition and Authentication Performancece by Emanuel von Zezschwitz - The paper summarizes that the results of two studies on the influence of mobile devices on authentication performance and password composition. A pre-study in the lab (n = 24) showed that the performance for password-entry on mobile devices is lower, in particular on smartphones. The main

study (n = 450) showed a trend that alphanumeric passwords are increasingly created on smart phones and tablets. Moreover, a negative effect on password security could be observed as users fall back to using passwords that are easier to enter on the respective devices. It contributes to the use of mobile password-entry and its effects on security in the following ways: (a) Different types of commonly used passwords are tested (b) on all relevant devices, and (c) Analytic and empirical evidence for the differences that (d) are likely to influence overall security or reduce secure behavior with respect to password-entry on mobile devices.

PAS: Predicate-based Authentication Services Against Powerful Passive Adversaries by XiaoleBai - Adversaries are those that can passively monitor and analyze each and every part of the authentication procedure, except for an initial secret shared between the user and the server. For PAS scheme, for the first time, the concept of a predicate is introduced for authentication. Analysis on the proposed scheme was conducted and its prototype system was implemented. The analytical and experimental data demonstrate that the PAS scheme can achieve a desired level of security and user friendliness.

S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Huanyu Zhao and Xiaolin Li - This study summaries that textual password is vulnerable to shoulder surfing, hidden camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text based scheme. However, they are mostly vulnerable to shoulder surfing. In this a Scalable Shoulder Surfing Resistant Textual Graphical Password Authentication Scheme (S3PAS). S3PAS integrates graphical and textual password schemes and provides perfect resistant to shoulder-surfing, hidden-camera and spyware attacks. It can replace or coexist with conventional password schemes without changing existing passwords. Moreover, it is immune to brute-force attacks through dynamic and volatile session passwords. S3PAS bridges the gap between textual password and graphical password. Further enhancements of S3PAS scheme are proposed and briefly discussed. Theoretical analysis of the security level using S3PAS is also investigated.

Against Spyware Using CAPTCHA in Graphical Password Scheme by Liming Wang, Xiuling Chang, ZhongjieRen,HaichangGao andXiyang Liu - Textual password schemes have usability problems, leading to the development of graphical password schemes. However, most of these alternate schemes are vulnerable to spyware attacks. A scheme is introduced called CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) that retaining the advantages of graphical password schemes, while simultaneously raising the cost of adversaries by orders of magnitude.

Reducing shoulder-surfing by using gaze-based password entrybyM.Kumar, T.Garfinkel, D.Boneh and T.Winograd - Looking over someone's shoulder, to get their passwords and other personal information - is a difficult problem to overcome. When a user enters information or any traditional input device, a malicious observer may be able to acquire the user's password credentials. Eye Password, a system that mitigates the issues of shoulder surfing via a novel approach to user input is presented. With Eye Password, a user enters sensitive input (password) using only the orientation of their pupils (i.e. the position of their gaze on screen), making eavesdropping by a malicious observer largely impractical. A number of design choices and their effect on usability and security are presented and discussed. To evaluate the speed, accuracy and user acceptance of approach, user studies are conducted. Our results demonstrate that gaze-based password entry requires marginal additional time over using a keyboard, error rates are similar to those of using a keyboard and subjects preferred the gaze-based password entry approach over traditional methods.

A PIN Entry Method Resilient Against Shoulder Surfing by Volker Roth - Magnetic stripe cards are most widely used for epayments and withdrawals. Reported incidents document that criminals easily pickpocket cards or skim them by swiping them through additional readers. Personal identification numbers (PINs) are identified by shoulder surfing, through the use of mirrors or concealed miniature cameras. Both elements, the PIN and the card, are generally sufficient to give the criminal full access to the victim's account. Alternative PIN entry methods referred as cognitive trapdoor games are presented. These method makes harder for a criminal to identify PINs even if he predicts the input PIN entry procedure.The idea of probabilistic cognitive trapdoor games, which offer resilience to shoulder surfing even if the criminal records a PIN entry procedure with a camera are introduced.

Image Based System To Resist Shoulder Surfing Attack Over Web by RohanRao, Ajay Tambe, Rama Khude and DigambarPatil - Authentication based on passwords is used largely in applications for computer security and privacy. As the number of web and mobile applications are rising exponentially, people can access these applications anytime and anywhere with various devices. People may log into web services and applications in public to access their personal and confidential accounts with their laptops, smartphones, tablets or public devices, like bank ATM. All these things bring great convenience but at the same time increase the risk of exposing passwords to shoulder surfing attacks. A shoulder surfing is a kind of attack where attackers can observe directly or use external recording devices to collect user's credentials. Shoulder surfing attackers can observe how the passwords were entered with the help of reflecting glass windows or let recording devices like CCTV camera hanging everywhere in public places. Passwords are exposed to risky environments, even if the passwords themselves are complex and secure. To overcome this problem of shoulder surfing, an image-based

authentication system along with encryption is proposed. With one-time valid login indicator / token, horizontal and vertical bars covering the entire scope of an image, proposed system offers no hint for attackers to figure out or narrow down a password even when they conduct multiple camera based attacks. In addition to this, the login indicator is completely random and valid only for short period of time. The proposed system also contains an android application which will receive login indicator. The goal of the android application is to receive the login indicator and display it to the user. In addition to this to protect the mobile application from theft, only one email id is allowed per application and an easy-to-remember randomly generated password required for logging into the application is also sent to the user. This password is completely encrypted and valid only for single login.

The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices Andrea Bianchi, Ian Oakley,VassilisKostakos and Dong Soo Kwon - Digital informationhave portals like tangible user interfaces.In the future, securing access to such material will be an important concern. This paper describes the design, implementation and evaluation of a PIN based on audio or haptic cues. The current implementation links movements on a mobile phone touch screen; selection of these cues composes a password. Studies reveal the validity of this approach in terms of task times and error rates. In sum, the paper describes potential of non-visual PINs as a mechanism for securing access to a range of systems, ultimately incorporating mobile, ubiquitous or tangible interfaces.

The Design and Analysis of Graphical Passwords by Ian Jermyn, Alain Mayer, Fabian Monrose and Michael K. Reiter - The paper summaries that the graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and it shows that this decoupling can be used to generate passwords with larger spaces. In order to evaluate the security of one of the schemes, a novel way to capture a subset of the "memorable" passwords is devised. In this work, devices such as personal digital assistants (PDAs) that offer graphical input capabilities via a stylus, and prototype implementation of one of password schemes namely the Palm Pilot are described.

3. Proposed System

In proposed system, a concept called Pass Matrix is used. In a Pass Matrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images is user-defined. Blocking of the user account is held if wrong password injected to the server frequently and intimate, then the user through Email and user's alternate mobile number via SMS about current location of the mobile. Proposed model provide the user friendly and the interactive environment for the user. The efficient and the innovative banking service is provided for the authentication system. The forget password module is designed with an innovative idea. Based on idea of framing forget password questions on the user's handheld device.

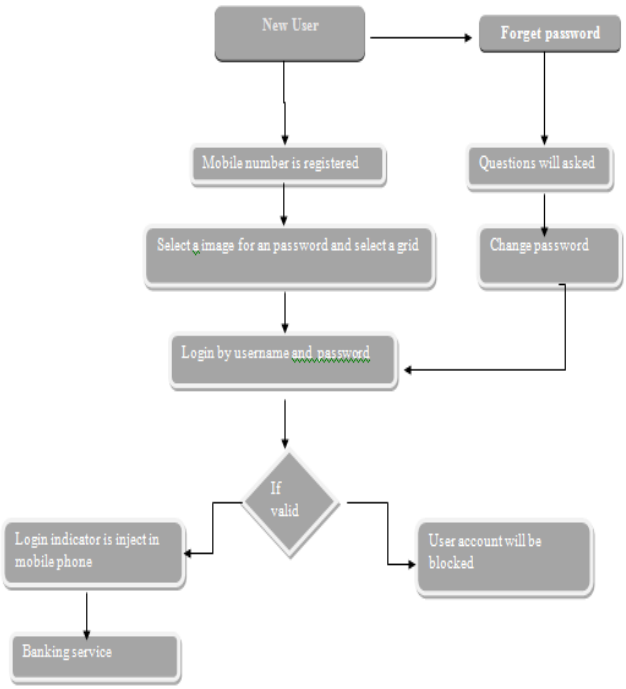

Fig.1: Flow chart for authentication

4. Conclusion

The efficient banking application to inject the account password to the server in the indirect manner is using some temporary login indicator in the user interactive manner, and effective banking service using the virtual money concept. Securing the bank account is possible while entering the wrong password frequently through blocking accounts, the innovative idea of forgotten password and recover module.

References

[1] T. Takada, "fakepointer: An authentication scheme for improving security against peeping attacks using video cameras," in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM' 08.The Second International Conference on. IEEE, 2008, pp. 395–400.

[2] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance," in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI '14. New York, NY, USA: ACM, 2014, pp. 461–47

[3] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma,"Pas: predicate-based authentication services against powerful passive

adversaries," in 2008 Annual Computer Security Applications Conference. IEEE, 2008, pp. 433–442.

[4] H. Zhao and X. Li, "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, vol. 2. IEEE, 2007, pp. 467–472.

[5] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using captcha in graphical password scheme," in 2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE, 2010, pp. 760–767.

[6] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 13–19.

[7] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in Proceedings of the 11th ACM conference on Computer and communications security, ser. CCS '04.New York, NY, USA: ACM, 2004, pp. 236–245.

[8] Image Based System To Resist Shoulder Surfing Attack Over Web International Journel of Emerging TechnologyAnd Computer Science ISSN:2455-9954 Volume: 1 Issue: 4 2017.

[9] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phonelock: Audio and haptic shoulder-surfing resistant pin entry methodsfor mobile devices," in Proceedings of the Fifth InternationalConference on Tangible, Embedded, and Embodied Interaction, ser. TEI'11. New York, USA: ACM, 2011, pp. 197–200.

[10] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," inProceedings of the 8th conference on USENIX Sec.