AUTHENTICATION SCHEME USING ILLUSION PIN TO PREVENT SHOULDER SURFER ATTACK

MAGESHWARI[1], PRIYA.M[2]

[1]*PG Student, Dept of CSE, Bharathiyar College of Engineering and Technology, Karaikal.*

[2] *Professor, Dept. of CSE, Bharathiyar College of Engineering and Technology, Karaikal.*

Abstract

Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as ”the weakest link” in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a Pass Matrix prototype on Android and carried out real user experiments to evaluate its memorability and usability.

Keywords- Shoulder Surfing Attack, Graphical Passwords, Authentication, Color Rings, and Biometric based authentication system.

1.INTRODCUTION

Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect .Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds .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. Based on some studies such as those in humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. 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. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack 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 .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. In this paper, we present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the

usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

In an information system, input is the raw data that is processed to produce output. During the input design, the developers must consider the input devices such as PC, MICR, OMR, etc. Therefore, the quality of system input determines the quality of system output. Well designed input forms and screens have following properties. It should serve specific purpose effectively such as storing, recording, and retrieving the information. It ensures proper completion with accuracy. It should be easy to fill and straightforward. It should focus on user's attention, consistency, and simplicity. All these objectives are obtained using the knowledge of basic design principles regarding what are the inputs needed for the system? How end users respond to different elements of forms and screens.

2. RELATED WORK

Enhancing security and privacy in biometrics-based authentication systems

Reliable user authentication is becoming an increasingly important task in the Web-enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer or network access. Many other applications in everyday life also require user authentication, such as banking, ecommerce, and physical access control to computer resources, and could benefit from enhanced security. It is important that such biometrics-based authentication systems be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as ecommerce. In this paper we outline the inherent strengths of biometrics-based authentication, identify the weak links in systems employing biometrics-based authentication, and present new solutions for eliminating some of these weak links. Although, for illustration purposes, fingerprint authentication is used throughout, our analysis extends to other biometrics-based methods.

Graphical Password Authentication: Implementation and Evaluation of Personalized Persuasive Cued Click Points

Persuasive Cued Click-Points (PCCP) is an integrated evaluation of the graphical password scheme, including usability and security evaluations, and implementation considerations. The systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. This research work explores the possibility of designing and constructing a module that is easily pluggable into the existing authentication systems being used as of now. The working prototype is an open source simulation consisting of all the necessary modules to build the authentication system. This system is built using Java and Oracle 10g Express Edition as the database although most database systems can be used.

Forgery Biometrics can be used for verification. digital signature are the weak laws regarding cyber security which might cause any unnecessary hassles in case of a court case and that both parties have to purchase the certificates for the digital signature in order to use it instead of the one party courier charge.

A Smart User Interface to Prevent Shoulder Surfing Attack Using Color Code

Classical PIN entry mechanism is broadly used for authenticating a user. It is a popular scheme because it properly balances the usability and safety aspects of a organism. However, if this scheme is to be used in a public system then the design might endure since accept surfing attack. In this attack, an unauthorized user can

completely or partially watch the login session .Even the activities of the login gathering can be recorded which the attacker can use it soon after to get the actual PIN. In this paper suggest an intelligent user interface, known as Color Pass to oppose the accept surfing attack so that any authentic user can enter the session PIN without disclosing the authentic PIN. The Color Pass is based on a partially noticeable attacker model.

Limitations on digit recognition rate that its performance in behavioral biometric verification Security is entirely based on confidentiality and the strength of the password and also it does not provide strong identity check (only based on password).

Biometric Online Signature Verification

Person identification can be done precisely by Biometrical method, where physiological or behavioral characteristics are used for this purpose. Handwritten signature is a behavioral trait it can be used for person identification accurately. There are two types of identification modes either online or offline mode. Which depends upon the signature acquisition method? In offline acquisition method the shape of the signature is used for authenticating signer. While in online signature verification uses dynamic characters that are dynamic time dependent of the signature to authenticate the signer. This paper describes the implementation on field programmable gate arrays (FPGAs) of an embedded system for online signature verification. The online signature recognition algorithm mainly consists of three stages. Initial pre-processing is the first stage which is applied on the captured signature for removing noise and normalizing information related to horizontal and vertical positions. Dynamic time warping algorithm is used to align this processed signature with its template previously stored in a database. Finally, a set of features is extracted and passed through a Gaussian Mixture Model. Degree of similarity between both signatures can be found out from this. For fast computation of floating point calculations vector floating point unit is used (VFPU). Additionally system consists of a microprocessor which interacts with the VFPU. All the procedures of verification can be done in software. Furthermore this paper studies about online signature verification on touch interface-based mobile devices. A simple and effective method for signature verification is developed. An online signature is represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time. The resulting signature template is compact and requires constant space.

White noise signals may be unpleasant for the user**.** Practically the only disadvantages of using digital signature are the weak laws regarding cyber security which might cause any unnecessary hassles in case of a court case and that both parties have to purchase the certificates for the digital signature in order to use it instead of the one party courier charge.

Touchscreen Mobile Authentication Using Multi-Touch Sequential Gestures

Recently all handheld devices are touch screen and the popularity of touch screen devices increases more and more due to the easy fast Internet access and large storage capacity. People may store their all personal information such as banking detail, password, confidential documents, trade secrets etc. on the handheld devices. In any case such handheld device is lost or stolen then security of such handheld device are more important because it contains users personals, banking information, secrets of user and that can be misuse by unauthorized person in any terrorist activity or other purposes that harm to user financially and socially. Securing the personal data stored and accessed from android touchscreen mobile makes user authentication a problem of paramount importance. The rigidity between security and usability renders however the task of user authentication on mobile devices a challenging task. This paper introduces Multi-Touch Authentication and unauthorized user tracking technique to protect mobile banking data stored on touch screen mobile devices (Finger gestures with priority Authentication System using Touch screen Devices), a behavioural touch screen based authentication approach on mobile devices. Besides extracting touch data from touch

screen equipped smart phones. This system complements and validates this data using a touch screen mobile device. A addressable feature in the system is its continuity, users transparent post login authentication and tracing of location of mobile devices. Artificial neural networks require processors with parallel processing power, in accordance with their structure. For this reason, the realization of the equipment is dependent. This is the most important problem of ANN. When ANN produces a probing solution, it does not give a clue as to why and how. This reduces trust in the network.

3. PROPOSED SYSTEM

Shoulder-surfing is a big threat for PIN authentication in particular, because it is relatively easy for an observer to follow the PIN authentication process. PINs are short and require just a small numeric keypad instead of the usual alphanumeric keyboard. In addition, PIN authentication is often performed in crowded places, e.g., when someone is unlocking her mobile phone on the street or in the subway. Shoulder-surfing is facilitated in such scenarios since it is easier for an attacker to stand close to the user while escaping her attention. Illusion PIN is a PIN-based authentication scheme for touch screen devices which offers shoulder-surfing resistance. The design of Illusion PIN is based on the simple observation that the user is always viewing the screen of her device from a smaller distance than a shoulder-surfer. Based on this, the core idea of Illusion PIN is to make the keypad on the touch screen to be interpreted with a different digit ordering when the viewing distance is adequately large. This way, when the shoulder surfer is standing far enough, he is viewing the keypad as being different from the one that the user is utilizing for her authentication, and consequently he is unable to extract the user's PIN.

Information and computer security is supported largely by passwords which are the principle part of the authentication process. The most common computer authentication method is to use alphanumerical username and password which has significant drawbacks. To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text based scheme. A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords. When users input their passwords in a public place, they may be at risk of attackers stealing their password

Shoulder surfing attack is the direct observation of user from far distance by hacker. Traditional methods use personal identification number (pin) consists of a sequence of digits for authentication. This method is used for Digital Authentication of touch screen devices. The applications of touch screen devices include ATM machines, Smart phones and Kiosk. Shoulder surfing attack suffers from various issues, Challenges and limitations like security and privacy. There are various algorithms and techniques have been proposed in the literature to overcome these difficulties and still needs improvement. Hence in this work a novel algorithm using illusion pin with hybrid images for shoulder surfing attack authentication scheme has been proposed. This proposed method using Illusion-pin (I-pin) blends of two keypads with different ordering digits using hybrid images. The user keypads are shuffled in every authentication attempt. This method is used to restrict the shoulder surfing attack by implementing this visibility algorithm. Hence hackers are unable to recognize or learning the user pin which provides more security and authentication.

Because it is difficult to mentally "revert" a degraded image, without knowledge of the original image, our scheme provides a strong line of defense against impostor access, while preserving the desirable memorability properties of graphical password schemes. Using low-fidelity tests to aid in the design, we implement prototypes of Use Your Illusion as an Ajax-based web service and ii) on Nokia N70 cellular phones. We conduct a between-subjects usability study of the cellular phone prototype with a total of 99 participants in two experiments. We demonstrate that, regardless of their age or gender, users are very skilled at recognizing degraded versions of

self-chosen images, even on small displays and after time periods of one month. Our results indicate that graphical passwords with distorted images can achieve equivalent error rates to those using traditional images, but only when the original image is known.

3.1 User Password Authentication

A password is a string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in conjuncture with a username; they are designed to be known only to the user and allow that user to gain access to a device, application or website... The User PIN Authentication page enables user to add user PIN records into the device one at a time, and to edit or delete user PIN records that have already been saved in the device. PINs are used in ATM or POS transactions, secure access control (e.g. computer access, smart phone access, door access, and car access), internet transactions, or to log into a restricted website. If PIN Authentication is selected for one or more Device Functions on the Authentication Manager page, the user will be prompted for a PIN before they can access those Device Functions. If the PIN is entered incorrectly the user will be returned to the previous screen. When a PIN is entered correctly all functions that use that PIN are then accessible to the user.

3.2 Shoulder Surfing Attack

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder. This attack can be performed either at close range (by directly looking over the victim's shoulder). To implement this technique attackers do not require any technical skills; keen observation of victims' surroundings and the typing pattern is sufficient. Crowded places are the more likely areas for an attacker to shoulder surf the victim. However, the advent of modern-day technologies like hidden cameras and secret microphones makes shoulder surfing easier and gives more scope for the attacker to perform long range shoulder surfing. A hidden camera allows the attacker to capture whole login process and other confidential data of the victim, which ultimately could lead to financial loss or identity theft.

3.3 Illusion PIN Generation

Illusion PIN is a PIN-based authentication scheme for touch screen devices which offers shoulder-surfing resistance. The design of Illusion PIN is based on the simple observation that the user is always viewing the device screen from a smaller distance.

Illusion PIN is a PIN-based authentication scheme for touch screen devices which offers shoulder-surfing resistance. The design of Illusion PIN is based on the simple observation that the user is always viewing the screen of her device from a smaller distance than a shoulder-surfer. Based on this, the core idea of Illusion PIN is to make the keypad on the touch screen to be interpreted with a different digit ordering when the viewing distance is adequately large. This way, when the shoulder surfer is standing far enough, he is viewing the keypad as being different from the one that the user is utilizing for her authentication, and consequently he is unable to extract the user's PIN. Also, the keypad is shuffled in every authentication attempt (or every digit entry) to avoid disclosing the spatial distribution of the pressed digits. We create the keypad of Illusion PIN with the method of hybrid images and are call a hybrid keypad.

Visibility Algorithm

The visibility algorithm receives as inputs a hybrid keypad I and a viewing position N in the 3D space. It returns a binary prediction on

whether the user's keypad of I is visible to an observer who is in position N. We use this prediction either to estimate the minimum safety. Distance that corresponds to a given hybrid keypad, or to create a hybrid keypad that respects a given safety distance. Algorithm 1 provides the pseudo code of the visibility algorithm

3.4 Distance-As-Filtering

The Distance Filter. The distance filter has specifically been designed for proximity sensors such as laser range-finders. Distance filters are based on a simple observation: In proximity sensing, UN modeled obstacles typically produce readings that are shorter than the distance expected from the map.

- **Visibility Index:**

The visibility index is the cornerstone of our algorithm and we would like to clarify its behavior and the intuition behind it. The visibility index is the mean value of the 10 MSSIM index (mean structural similarity index) values from the pairs of corresponding buttons. The maximum value of the MSSIM index is 1 and is obtained when I1 and I2 are identical, meaning that I2 is not distorted at all. The maximum value of the visibility index is 1 and is obtained when the user's keypad is completely out of perception. The MSSIM index follows the premise that the main function of the human eye is to extract structural information from the viewing field. This connection to human perception is the main reason that we decided to use the MSSIM index. An additional advantage is that MSSIM index is very easily computed.

- **Threshold Value of the Visibility Index**

Based on the aforementioned remarks, we set as a threshold vth the value of the visibility index when a particular observer is able to marginally recognize the digits of a user's keypad. Then, the visibility algorithm calculates the visibility index v for the inputs I and N, and compares it with vth. If v >=vth, we predict that the user's keypad cannot be interpreted by the observer. If v <= vth, we predict that the observer is able to interpret the digits of the user's keypad. Since the threshold value will vary for different observers, we universally use the vth value that corresponds to people with the strongest vision, because we don't want to mistakenly predict that the user's keypad is not visible

4. Performance Evaluation

Here developed an algorithm to estimate whether or not the user's keypad is visible to an observer at a given viewing position. Proposed method tested the estimated visibility of Illusion PIN through a user study of simulated shoulder-surfing attacks on smartphone devices. In total, we performed 84 attacks with 21 different people and none of the attacks was successful against our estimations.

5. CONCLUSION

The main goal of our work is to design a PIN-based authentication scheme that would be resistant against shoulder surfing attacks. To this end, Illusion PIN created for authentication and quantified the level of resistance against shoulder-surfing by introducing the notion of safety distance that estimated with a visibility algorithm. In the context of the visibility algorithm, a model at a basic level explained the concept of how the human visual system works. Illusion PIN is a Hybrid PIN-based authentication scheme that would be resistant against shoulder surfing attacks. Two keypads are blended in a single key digit that will show different key pad to the attacker. Illusion PIN gives best results when compared to other PIN Authentication scheme.

Future Work

In future work, Illusion PIN creates for android application. This will help to improve mobile security. Illusion poses has a number of interesting questions, which warrant further investigation. Recall that our scheme does not mandate a given image processing filter the choice of an oil painting filter has been driven mostly by heuristic considerations. Further experimentation is also needed to better evidence the re-silience of the scheme to some types of attacks the low fidelity test conducted to determine optimal parameter selection, while highly encouraging, needs to be expanded to provide stronger staistical evidence that attackers are not easily able to "revert" a distorted image

back to its original meaning. While investigating how best to tune our filter during the course of our prototype design and implementation discovered that finding an optimal parameter set point for the lossy filter depends on the picture to be transformed.

REFERENCES:

[1] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012, pp. 553–567.

[2] M. Harbach, A. De Luca, and S. Egelman, "The anatomy of smartphone unlocking," in Proceedings of the 34th Annual ACM Conference on Human Factors in Computing Systems, CHI, 2016.

[3] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? the security of customer-chosen banking pins," in Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2012, vol. 7397, pp. 25–40.

[4] R. Anderson, "Why cryptosystems fail," in Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993, pp. 215–227.

[5] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens." WOOT, vol. 10, pp. 1–7, 2010.

[6] A. Oliva, A. Torralba, and P. G. Schyns, "Hybrid images," ACM Transactions on Graphics (TOG), vol. 25, no. 3, pp. 527–532, 2006.

[7] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010, pp. 1093–1102.

[8] L.-W. Chan, T.-T. Hu, J.-Y. Lin, Y.-P. Hung, and J. Hsu, "On top of tabletop: A virtual touch panel display," in Horizontal Interactive Human Computer Systems, 2008. TABLETOP 2008. 3rd IEEE International Workshop on. IEEE, 2008, pp. 169–176.

[9] W. Matusik, C. Forlines, and H. Pfister, "Multiview user interfaces with an automultiscopic display," in Proceedings of the working conference on Advanced visual interfaces. ACM, 2008, pp. 363–366.

[10] C. Harrison and S. E. Hudson, "A new angle on cheap lcds: making positive use of optical distortion," in Proceedings of the 24th annual ACM symposium on User interface software and technology. ACM, 2011, pp. 537–540.

[11] S. Kim, X. Cao, H. Zhang, and D. Tan, "Enabling concurrent dual views on common lcd screens," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2012, pp. 2175–2184.

[12] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig, "Use your illusion: secure authentication usable anywhere," in Proceedings of the 4th symposium on Usable privacy and security. ACM, 2008, pp. 35–45.

[13] I. Jermyn, A. J. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin et al., "The design and analysis of graphical passwords." in Usenix Security, 1999.

[14] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," in Proceedings of the Seventh Symposium on Usable Privacy and Security. ACM, 2011, p. 6.

[15] D. S. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: Towards more secure password entry on publicly observable touch screens," in Proceedings of OZCHI-Computer-Human Interaction Special Interest Group (CHISIG) of Australia. Canberra, Australia: ACM Press, 2005.

[16] 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. ACM, 2004, pp. 236–245.

[17] T. Pering, M. Sundar, J. Light, and R. Want, "Photographic authentication through untrusted terminals," IEEE Pervasive Computing, vol. 2, no. 1, pp. 30–36, 2003.

[18] D. K. Yadav, B. Ionascu, S. V. K. Ongole, A. Roy, and N. Memon, "Design and analysis of shoulder surfing resistant pin based authentication mechanisms on google glass," in International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015,pp. 281–297.

[19] R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentication." in USENIX Security Symposium, vol. 9, 2000, pp. 4–4.

[20] Z. Li, Q. Sun, Y. Lian, and D. D. Giusto, "An association-based graphical password design resistant to shoulder-surfing attack," in Multimedia and Expo, 2005. ICME 2005. IEEE International Conference on. IEEE, 2005, pp. 245–248.