Doodles Using Cued Click Points As An Effective Authentication System

R.Bhuvanya, S.Nirupa shri, R.Suganya, K.Vishnu priya

Abstract:

The leak of sensitive data on computer systems poses a serious threat to organizational security due to human errors. This detection is paired with a comparable sampling algorithm, which allows one to compare the similarity of two separately sampled sequences. Our system achieves good detection accuracy in recognizing transformed leaks. We implement a parallelized version of our algorithms in graphics processing unit that achieves high analysis throughput. We demonstrate the high multithreading scalability of our data leak detection method required by a sizable organization. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image. System showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points. A total of 5 images are used whereby the user clicks on each image at the right point and then next image is shown. This is more accurate than traditional password based systems.

I. INTRODUCTION

Passwords provide security mechanism for authentication and protection services against unwanted access to resources. A graphical based password is one promising alternatives of textual passwords. According to human psychology, humans are able to remember pictures easily. In this paper, we have proposed a new hybrid graphical password based system, which is a combination of recognition and recall based techniques that offers many advantages over the existing systems and may be more convenient for the user. Our scheme is resistant to shoulder surfing attack and many other attacks on graphical passwords.

One of the major functions of any security system is the control of people in or out of protected areas, such as physical buildings, information systems, and our national borders. Computer systems and the information they store and process are valuable resources which need to be protected. Computer security systems must also consider the human factors such as ease of a use and accessibility.

To the extent of our knowledge, this is the first analysis of user authentication on touchscreens based on free-form gestures, using a publicly available database (DooDB Graphical Password Database [3]). The contributions of this paper are as follows.

1) Two approaches from the signature verification state of the art, namely Gaussian mixture models (GMM) and dynamic time warping (DTW), are evaluated using graphical passwords. We analyze the performance of these systems against random forgeries (when attackers claim to be another user but use their own password) and intentional forgeries (when attackers have visual access to the password being forged).
2) Feature selection identifies which features provide the highest discriminative power.
3) The effects of intersession variability (i.e., the time lapse between enrollment and authentication) are studied.
4) We study the impact of the number of available training samples during enrollment on the verification performance.
5) An improved authentication system based on the fusion of GMMs and DTW is presented.

II. EXISTING SYSTEM

Current secure systems suffer because they mostly ignore the importance of human factors in security. An ideal security system considers security, reliability, usability, and human factors. All current security systems have flaws which make them specific for well trained and skilled users only. A password is a secret that is shared by the verifier and the customer. "Passwords are simply secrets that are provided by the user upon request by a recipient." They are often stored on a server in an encrypted form so that a penetration of the file system does not reveal password lists.
Passwords are the most common means of authentication because they do not require any special hardware. Typically, passwords are strings of letters and digits, i.e., they are alphanumeric. Such passwords have the disadvantage of being hard to remember. Weak passwords are vulnerable to dictionary attacks and brute force attacks where as Strong passwords are harder to remember.

III. PROPOSED SYSTEM

To overcome the problems associated with password based authentication systems, the researchers have proposed the concept of graphical passwords and developed the alternative authentication mechanisms. Graphical passwords systems are the most promising alternative to conventional password based authentication systems. Graphical passwords (GP) use pictures instead of textual passwords and are partially motivated by the fact that humans can remember pictures more easily than a string of characters. The idea of graphical passwords was originally described by Greg Blonder in 1996. An important advantage of GP is that they are easier to remember than textual passwords. Human beings have the ability to remember faces of people, places they visit and things they have seen for a longer duration. Thus, graphical passwords provide a means for making more user-friendly passwords while increasing the level of security. Besides these advantages, the most common problem with graphical passwords is the shoulder surfing problem: an onlooker can steal user’s graphical password by watching in the user’s vicinity. Graphical passwords serve the same purpose as textual passwords differing in consisting of handwritten designs (drawing), possibly in addition to text.

IV. LITERATURE SURVEY


Current secure systems suffer because they neglect the importance of human factors in security. We address a fundamental weakness of knowledge-based authentication schemes, which is the human limitation to remember secret passwords. Our approach to improve the security of these systems relies on recognition-based, rather than recall-based authentication. We examine the requirements of a recognition-based authentication system and propose Dëjä Vu, which authenticates a user through her ability to recognize previously seen images. Dëjä Vu is more reliable and easier to use than traditional recall-based schemes, which require the user to precisely recall passwords or PINs. Furthermore, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to write down or share passwords with others.

We develop a prototype of Dëjä Vu and conduct a user study that compares it to traditional password and PIN authentication. Our user study shows that 90% of all participants succeeded in the authentication tests using Dëjä Vu while only about 70% succeeded using passwords and PINS. Our findings indicate that Dëjä Vu has potential applications, especially where text input is hard (e.g., PDAs or ATMs), or in situations where passwords are infrequently used (e.g., web site passwords).

[2] The Design and Analysis of Graphical Passwords - Ian Jermy, Alain Mayer, Fabian Monrose, Michael K. Reiter and Aviel D. Rubin, In this paper we propose and evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text-based passwords. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of one of our schemes, we devise a novel way to capture a subset of the “memorable” passwords that, we believe, is itself a contribution. In this work we are primarily motivated by devices such as personal digital assistants (PDAs) that offer graphical input capabilities via a stylus, and we describe our prototype implementation of one of our password schemes on such a PDA, namely the Palm Pilot™.

[3] A User Identification System Using Signature Written with Mouse. F. Syukri, E. Okamoto, and M. Mambo-A user identification system is very important for protecting information from illegal access. There are identification systems using standard devices (keyboard or mouse) and systems using special devices. A user identification system using mouse is proposed in [6]. In their system, users write a simple figure object and the successful verification rate is 87%. However the simple object is too easy to prevent impersonation. In order to realize a more reliable user identification system using mouse, we propose a new system to identify users using a complex figure object, signature. New techniques we utilize in our system are as follows: the normalization of input data, the adoption of new signature-writing-parameters, the evaluation of verification data using geometric average means and the dynamical update of database. We have implemented our user identification system and conducted experiments of the implemented system. The successful verification rate in our system is 93%.

[4] Graphical Passwords: A Survey The most common computer authentication method is to use alphanumeric usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, we conduct a comprehensive survey of the existing graphical password techniques. We classify these techniques into two categories: recognition-based and recall-based approaches. We discuss the strengths and limitations of each method and point out the future research directions in this area. We also try to answer two important questions: “Are graphical
passwords as secure as text-based Passwords?”; “What are the major design and implementation issues for graphical passwords?” This survey will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication methods.

Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin.

Shoulder-surfing is a known risk where an attacker can capture a password by direct observation or by recording the authentication session. Due to the visual interface, this problem has become exacerbated in graphical passwords. There have been some graphical schemes resistant or immune to shoulder-surfing, but they have significant usability drawbacks, usually in the time and effort to log in. In this paper, we propose and evaluate a new shoulder-surfing resistant scheme which has a desirable usability for PDAs. Our inspiration comes from the drawing input method in DAS and the association mnemonics in Story for sequence retrieval. The new scheme requires users to draw a curve across their password images orderly rather than click directly on them. The drawing input trick along with the complementary measures, such as erasing the drawing trace, displaying degraded images, and starting and ending with randomly designated images provide a good resistance to shoulder surfing. A preliminary user study showed that users were able to enter their passwords accurately and to remember them over time.


Computer security depends largely on passwords to authenticate human users. However, users have difficulty remembering passwords over time if they choose a secure password, i.e. a password that is long and random. Therefore, they tend to choose short and insecure passwords. Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. In this paper we describe Pass Points, a new and more secure graphical password system. We report an empirical study comparing the use of Pass Points to alphanumeric passwords. Participants created and practiced either an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to input their password over the course of 6 weeks. The results show that the graphical password users created a valid password with fewer difficulties than the alphanumeric users. However, the graphical users took longer and made more invalid password inputs than the alphanumeric users while practicing their passwords. In the longitudinal trials the two groups performed similarly on memory of their password, but the graphical group took more time to input a password.


To provide adequate authentication to users is a constant problem, especially with mobile devices such as personal digital assistants (PDAs). However, these devices are also being used extensively by government agencies, hospitals and military and in businesses so there is a security risk not only because they contain sensitive information but they may also present means to access information on wireless networks. So user authentication is a main question for the security of mobile devices that may be caught by unauthorized individual. However traditional alphanumeric passwords do not provide high security level to mobile devices as they are more vulnerable to brute force and dictionary attacks. To overcome this problem visual authentication techniques were introduced. In this research paper we are going to analyze several visual techniques for authentication of mobile device users. And in the end we will describe our own technique which uses an alphanumeric string with pictures as passwords.

V. ALGORITHM

VI. TECHNIQUES

PSEUDO-SK & DOODLE-SK: minimize the system EER against skilled forgeries. 2) PSEUDO-RD & DOODLE-RD: minimize the system EER against random forgeries. In all cases, the 15 doodles signatures from are used for genuine score computation, while the first 5 signatures from session 1 are used for enrollment.
Thus, intersession variability is taken into account. The best performance features sets selected by the SFFS algorithm for each data set optimization scenario are shown. Feature y"n(Vertical acceleration) is present in seven of the 8 sets and features y' n(vertical speed) and p' n(variation of log curvature radius) are present in 6 of the 8 sets. This indicates that vertical dynamic features may be more stable than horizontal features. However, features x" is presented in the four GMM optimal feature sets.

This implies that GMMs may be more robust to users that change the usual left to right drawing order of their sketches (GMMs, contrary to DTW, do not consider the temporal order of time series for matching).

The performance is terms of EER against random (EER rd) and skilled (EERsk) forgeries of the previously computed features is shown in table IV, both on the development and validation data sets. The average of the user-specific EERs (reference to as aEER) is also reported. It is computed by averaging the individual user EERs that are obtained with user-specific decision threshold.

This represent the best EER that can be obtained if user scores were optimally normalized. The verification performance on the development and on the validation set is similar in general.

VII. MODULES

USER REGISTRATION

In this module the user register with the system by giving His/her profile (like Name, Address, mail ID, contact No, etc.,) and selecting the click points on the images which user likes and store the image in the database in which No of images and order of the images should be mentioned during the registration.

All the data are stored in the database by the user. This calls for the user to select the appropriate images at the appropriate time by the user. Each user is given a unique identity by the system. This unique id is generated by the data server. The mobile contact number in case of wrong tries is also entered here.

GRAPHICAL PICTURE UPLOAD

Next the users upload the pictures and then click on the image to store the click points in vector format. Also the users are allowed to specify the image order of appearance. For each click the click point is stored into the database and then it is converted to a vector and stored in the database.

AUTHENTICATION

After the registration of user the next step is the users login in which the user have to choose the click points on the images which are given as password, if the user chooses correct click point on the first image then the next image will be shown, then the next image is shown to the user when they select the correct click point otherwise the system will not show the next image when any wrong click on the image.

VERIFICATION

During the wrong click of the click points the system send an alert message to the authorized user which helps in identification of illegal access of the system. When the user gives correct click point for all the images the system allows the user inside the account. The system validates the clicked points and then the authentication is done for processing the users system.

VERIFICATION MODULE

During this phase the system verifies if the combination is right for the text and color supplied for this session. If the password is accurate then the user is allowed entry into the system otherwise the login fails. As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable.

DATA FLOW DIAGRAM

GRAPHICAL PASSWORDS CAN BE CLASSIFIED INTO THREE CATEGORIES: 1) RECALL; 2) RECOGNITION; AND 3) CUED-RECALL. IN RECALL-BASED SYSTEMS, USERS HAVE TO REMEMBER A GRAPHICAL PASSWORD AND PROVIDE IT DURING AUTHENTICATION. THIS APPROACH IS FOLLOWED IN THIS WORK. IN RECOGNITION SYSTEMS, GRAPHICAL INFORMATION IS PRESENTED TO THE USER DURING AUTHENTICATION FROM WHICH THE USER HAS TO PERFORM A SELECTION THAT MATCHES A SET OF INFORMATION PREVIOUSLY MEMORIZED (E.G., A PICTURE AMONG A
set of different pictures). Cued-recall systems combine the two aforementioned methods, providing graphical cues that help users recall the previously learned password (e.g., an image related to the password). Doodle-based authentication falls in the category of recall graphical passwords. A survey of graphical password authentication algorithms appears in [1]. A. Recall-Based Graphical Password Verification A range of approaches for recall-based graphical password authentication have been evaluated using measures including resilience to forgeries, memorability, user acceptance, error rates, and time to enroll [1]. Recall-based authentication can be divided in two categories. Exact-match approaches assume that during authentication, a user produces exactly the same drawing provided during enrollment (e.g., [4], [8]). Elastic approaches allow some variability between enrollment and authentication (e.g., [6], [9]). Graphical password authentication systems can be also divided into static and dynamic approaches. Static or offline systems use the doodle image for authentication, while dynamic or online systems use time functions extracted from the doodle trajectory. Dynamic approaches have yielded better verification performance than static systems in the related field of signature verification, since more levels of information are used for authentication [2]. The Draw-A-Secret system (DAS) [4] implements a rectangular 5 × 5 cell grid where users trace their graphical password. The cell sequence that the users follow is stored as a password. The Background Draw-a-Secret (BDAS) [7] shows a background image behind the cell grid. A higher complexity in the password choice and better memorability were reported. With the Pass-Go authentication scheme, a variation of DAS [8], the graphical password is defined by a sequence of grid intersections instead of grid cells, overcoming the limitation of the DAS scheme, where strokes too close to adjacent cell edges could be incorrectly assigned to multiple cells. The term “passdoodle” [5] refers to a free-form drawing. In [5], the memorability of doodles for user authentication was studied, as well as the user preference towards alphanumeric passwords or doodles. The passdoodle verification system proposed in [6] uses spatial distribution and speed for verification. A doodle authentication system that uses DTW for matching is described in [9]. The trajectory coordinates (x,y) and their first- and second-order derivatives are used as features to characterize each doodle. Recognition performance results are provided using Tamil characters, instead of doodles. In [10], a static authentication method where free-form sketches are stored as a sequence of cell relative positions is presented. The Levenshtein distance is used to compute distances between sequences. With the Scribble-A-Secret (SAS) scheme [11], the edge orientation patterns of the doodle static image are used as features. The PassShapes approach considers graphical passwords as sequences of straight strokes following eight possible directions, at 45° angles [12]. A verification scheme based on predefined visual shapes is described in [13]. The system presents a set of cues to the users (common shapes, e.g., squares, triangles), which the users can follow to define their own free-form password. Cryptographic keys are then generated from the passwords. A graphical password verification system based on a set of predefined symbols is proposed in [14]. During enrollment, the user first selects a set of predefined symbols (at least 3) and then draws them. The set of symbols constitutes the user password. The multitouch sketch-based authentication approach in [15] uses gestures drawn with several fingers at the same time. Since the proposed gestures are produced with all fingers, information from the hand geometry is also captured. The GEAT scheme [19] allows the user to draw a password composed of many multitouch gestures based on a set of ten predefined symbols. Support vector machines (SVM) are used for classification. In [18], an authentication scheme based on continuous touchscreen input, instead of specific gestures, is presented. SVMs and k-nearest neighbor (k-NN) classifiers are used. Two graphical password approaches have gained popularity: the pattern lock on the android operating system and the picture password on Windows 8 devices. The pattern lock method displays a square grid of 3 × 3 points on the screen, and users trace a pattern connecting them. Other approaches that use dynamic information from the pattern lock drawing process have been proposed [16], [17]. In the Windows 8 picture password method, a background image is shown, and users trace on it a password composed of symbols. A summary of the proposed methods is presented in Table I. B. Attacks to Recall-Based Graphical Passwords Several types of attacks against graphical password authentication systems have been studied. Smudge attacks occur when an attacker follows the finger grease path left by the user on the screen [20]. Shoulder-surfing attacks occur when the attacker has visual access to the password drawing process. Several techniques against shoulder surfing attacks are proposed in [21], including adding fake strokes during the drawing process or removing strokes as they are drawn. An alternative to finger-drawn graphical passwords based on capturing the gaze trajectory has been proposed in [22] as a means to prevent shoulder-surfing. In [23], dictionary attacks are studied against DAS-like systems. Users tend to select graphical passwords from a relatively small subspace of cell combinations. Thus, an attacker could be successful after a limited number of random attempts from that particular graphical subspace.

IX. CONCLUSION

The core element of computational trust is identity. Currently many authentication methods and techniques are available but each with its own advantages and shortcomings. There is a growing interest in using pictures as passwords rather than text passwords but very little research has been done on graphical based passwords so far. In view of the above, we have proposed authentication system which is based on graphical password schemes.

Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images. Thus the novel approach which uses recall graphical password click points is far better than previously developed system used this approach this system is helpful when user is logging after a long time.
X. FUTURE WORKS

In future systems other patterns may be used for recalling purpose to improve the efficiency of the system and to secure data with more implementation ideas.

REFERENCES