USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION

Anil H. Rokade*, Zafar Ul Hasan, Sonali A. Mahajan*****
Hi-Tech Institute of Technology, Aurangabad, India, email: mr.anil2097@rediffmail.com*
Sandip Foundation, Nashik, India, email: zafarulhasan@rediffmail.com**
Govt. Engg College, Aurangabad, India, email: mahajansonali8@gmail.com***

Abstract— **Graphical password is very strong password as compare to the text password and which is easily we can remember. Those who are use this system, authenticate themselves by identifying correct images fro set of displayed images. However, despite the impressive results of user studies on experimental graphical passwords schemes, their overall commercial adaptations have been relatively less. In this paper, we have searched reasons behind the less commercial acceptance of graphical password and we have invent such technique to overcome the limitation of existing system. Based on this technique we design graphical password Main goal of this system is to work as a cued recognition based graphical authentication scheme that allows users to make combination of text , images and numbers as their password, we have the strengths of Numbers, Alphabets and Pictures together to effectively defeat prevalent forms of social hacking. We have taken sample test of a user study with 65 participants to evaluate the viability of our proposed design. Results of the test are very good which indicates that our proposed systems early starting is secure**.

Keywords- **authentication, Graphical User passwords, Usable security, high probability**.

I. INTRODUCTION

User authentication is a major problem in every system providing secure access to confidential information and personalized services. Although, today there exists numerous ways to authenticate a person [1, 2], the most popular method amongst them is with passwords. In this knowledge based authentication scheme, user authenticates herself by presenting the knowledge of a secret string of alphanumeric characters. The secret string is called as *password* and it is assumed to be known only to the claimed identity and hence her identity gets verified. However, in practice, anyone who knows or guesses the password is also able to authenticate as the legitimate user. Passwords represent simple, cost effective and user friendly authentication solution since its usage requires no special hardware or training and passwords can be easily distributed, maintained and updated via telephone, fax or email. However, passwords are effective only if following two conflicting requirements are satisfied simultaneously [3].

- *Usability:* Passwords should be easy to remember and user authentication process should easy for humans and should take less time.
- *Security:* Passwords should be secure; that is, they should look random and should be hard to guess; they should be changed frequently and should be different on different accounts of the same user; they should not be written or stored down in plain text. remembered for a longer time, better than the text. An illustrative example is shown in Figure 1.

Figure 1: What is easy to remember, a picture of *Golden Temple* or a set of numbers?

As we can see in Figure 1, the task of memorizing a list of ten random digits, after a few seconds of inspection, would be impossible for most of us. On the other hand, the aerial picture of *Golden Temple could* easily be memorized so that at some future time, it could be distinguished from variety of other scenes.
The fact that images are better remembered than text and can potentially be chosen from an infinite set of images makes graphical passwords an ideal replacement to text passwords, especially in environments where the text entry is awkward or limited (For example, mobile phones, Point of sale (POS) devices and ATMs) . Even though the area of graphical passwords is actively discussed in the academic arena and experimental graphical password schemes [3,6, 7] present promising results in terms of improved memorability, overall commercial adaptations of graphical passwords has been low.
The aim of this paper is to investigate the reasons behind low commercial acceptance and provide suitable recommendations to overcome them. In the second half of this paper, based on these recommendations, we design a simple graphical password scheme, called USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION. USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION is a cued recognition based graphical authentication scheme, which allows users to choose both text as well as images as passwords without any specific alternations to underlying authentication design and process. It also blends together the strengths of Numbers, Alphabets and Pictures (NAP) to effectively defeat prevalent forms of social hacking. In this paper we describe the complete design of USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION and argue for its potential benefits in terms of security and usability. We then provide results of user study and security analysis. Finally, we conclude with the summary of our contribution.

2. RETHINKING GRAPHICAL PASSWORDS DESIGN

When graphical passwords were first introduced, it was conceived that the picture superiority effect coupled with the large password space offered by images, would solve the password problem entirely (the conflict between the security and usability) and people would choose graphical passwords that are stronger than the text passwords they typically select. However, in practice, results were not as expected. Graphical passwords have issues in both usability and security [13, 14] Balancing them together is as difficult as it was in text passwords. As a result, even after a lot of academic attention and recommendations, graphical passwords are rarely used in practice.
In this section, we review some of the common problems associated with graphical passwords. Our focus is mainly on Co geometric graphical password schemes.

2.1 Usability Issues

Security experts often say that users are the weakest link in a security system [1, 7]. Users misunderstand how to use security mechanisms and do not realize the need for such a protection. User behavior is essentially goal driven and security is usually a supportive task. Users are happy to circumvent the security measures, if security measures try to impede their primary tasks. It is imperative therefore to consider carefully the usability of the proposed authentication scheme. As explained earlier, authentication process should take less time, it should be easy and stress free for the users. However, graphical passwords present some problems in terms of the efficiency (time to execute) and affordance.

2.2 Security

Compared to text passwords, graphical passwords are weak against some of the common attacks on passwords schemes. We list down some of the common attacks and how related proposals have tried to mitigate them.

2.2.1 Brute force and dictionary based attack

Simplest of the attack against any authentication scheme is to randomly guess the correct password. For example, an attacker needs 10,000 attempts to correctly guess a four digit Personal Identification Number PIN. Dictionary attack is more sophisticated attack than brute force. Here, instead of random guessing, attacker tries to crack the password using a dictionary of most common passwords.

3. LITURATURE SURVEY

Existing literature and experience in graphical passwords design have led us to following observations that laid the foundation for this work.

3.1 Personal vs. Random images

The success of the graphical password scheme strongly depends on the type of images used [12]. For example, user can create a portfolio using personal images or random images. Both approaches have advantages and disadvantages. Psychological results show that self-generated or personal images are better recognized than those that are not [25]. However, such images are insecure in practical setting due to their vulnerability against guessing attacks. System-chosen random images on the other hand, are more secure against guessing attacks, but they are difficult to remember than personal images [8, 9, 36]. Ideally, we desire an authentication scheme that can merge together the security benefits of system-chosen images and memorability gains of self-chosen images.

3.2 Cognitive flexibility

We must realize that cognitive flexibility is important to accommodate people with different cognitive ability [13]. For users who do not want the visual way of working or prefer the traditional text passwords, graphical passwords should inhabit some alternate mechanism that allows them to select and enter text passwords.

3.3 Selection of decoy images

As we said earlier, locating password images involves visual search which consumes time. In order to improve the efficiency, the selection of decoy images becomes crucial, in a sense that these images should be both visually and semantically distinct so that users are not confused while locating their password images.

3.4 Cued Recognition

A cued recognition is an interesting approach to graphical passwords design. In such schemes, a cue is given to the user that helps her in the recognition of portfolio images. Best example of such a scheme is a Story scheme [16], where the story or the semantic relationship between the images assists user in the recognition of chosen password images. However, the cue should be designed carefully so that it only helps the legitimate user and not the attacker.

4. USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION: OUR PROPOSED SCHEME

USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION is a novel co geometric graphical authentication scheme which involves recognition of portfolio images. During account setup user creates a portfolio of 4 images or 4 characters or a 4-character word as her password and recognizes the images that corresponds to the chosen password to login. Motivation behind USER AUTHENTICATION

BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION came from Alphabet charts used in kindergarten schools to teach alphabets with the help of illustrative pictures (For example, A for Apple, B for ball etc.). We adopt the same concept to develop a novel authentication scheme that can serve both alphanumeric and pictorial passwords with same underlying design and interaction.
We explain the steps during registration and login below.

4.1 Steps during registration

Registration is one time event. During registration, we present user with a 5×5grid consisting of 25letters from the English alphabet set along with their pictorial representations as shown in Figure 6. In the current prototype (for testing purpose), we have used pictures from the publically available picture dictionary.

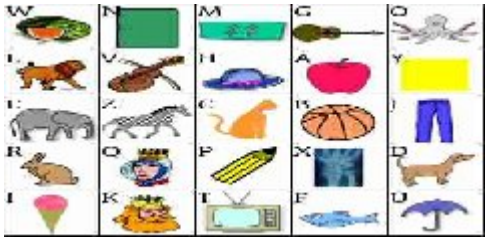

Figure 2: Registration step: User picks four images or characters as password and enters the corresponding alphabet in the textbox shown below the image grid.

User is then free to choose any four images or four characters as her password. Irrespective of the selection (images or characters), she is allowed to enter only the four characters in the textbox provided below. To illustrate, even if user chooses images of King, Fish, Pencil and TV as her password (Refer Figure 6); she must enter KFPT (The associated characters with those images) in the textbox. Once the user has submitted four characters, a confirmation message is displayed about successful completion of registration.

4.2 Steps during Login

During login, user sees the same 25 pictures randomly placed in the 5×5 image grid. However this time, the alphabets are replaced with numbers in the range of 0 to 9. In other words, each cell has a number instead of an alphabet associated with it as shown in Figure 7. In order to login, user needs to recognize her password (four images or four password characters) and enter the associated number in the textbox below. Users, who have chosen characters as their password, should recall those characters and then perform a visual search for images that correspond to the characters since the characters are not visible on screen during login. The images here act as a cue
for recalling the password characters.

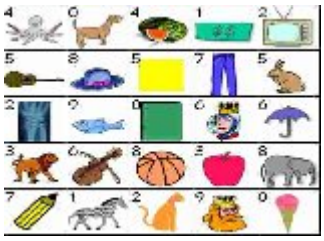

Figure3: Login Step: User recognizes the four password images and enters the corresponding numbers in the textbox shown below the image grid.

For example, for the password as KFPT, user must locate the images of King, Fish, Pencil and TV in Figure 7, user must enter 9972 (the four numbers associated with the four images) as his password to login. The numbers associated with the images keep changing with each login session and thus become the one time access code for a particular login session. Moreover, the numbers are repeated multiple times in the 5×5 image grid to thwart observation attacks.

4.3 Usability features of

USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION

USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION is a simple graphical password scheme, easy for users to grasp, but at the same time, it provides good levels of security to keep fraudsters at bay. The main usability features are listed below.

• **Improved memorability:** In the image set, we have specifically chosen images of the very first objects that come to mind when we think of the letter associated with it. For example, A for Apple, B for Ball etc. These images are very easy to remember and recall.

• **Cognitive scalability:** Our proposed scheme is language independent. Use of pictures and symbols makes the scheme ideal for use by the people of all abilities and age with any level of literacy. It also provides both textual and pictorial support to accommodate people with different cognitive abilities.

• **Simple, cost effective and stress free login experience:** Our proposed scheme achieves the desired security without the aid of any extra hardware or token. USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION also do not need costly software installations or dedicated hardware to run. The login interface is intuitive and specially designed, keeping the cognitive abilities of the users in mind.

• **Software as a Service (SaaS):** USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION can easily be integrated into current secure online authentication architecture and can replace passwords or serve as a second form of authentication. It is compatible (Adaptive) across various financial domains and transaction types like ATM, ecommerce, and mobile commerce.

• **Configurable:** Various attributes of USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION (number of images, length of the password etc) can be customized to increase security and to meet the specific needs of the customer.

• **Advertising opportunities:** Industries can leverage the opportunities to advertise on the USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION by allowing their images inside USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION. The ad images can be tailored to meet the needs of the user demographic.

5. SECURITY OF USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION

We recommend that USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION, should be implemented and deployed in systems where offline attacks are not possible and where number of guess attempts are limited per account in a given time period (For example, ATMs). We assume that all communication between the user and the server is made secure through SSL, thereby avoiding simple attacks based on network sniffing. Below, we enlist countermeasures against possible attacks on USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION.

5.1 Brute force attack

To crack USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION password, attacker must guess the four password images from 5x5 grid. However, in USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION, there are 3,03,600 (25P4) possible patterns of selecting four images out of 25 images. Alternatively an attacker can try to randomly guess the one time access code. The access code is a combination of four digits (each digit can be any number between 0 - 9). Therefore, the total number of valid combination of one time access code is 10,000, if the ordering constraint is kept. Without the ordering constraint, the number of possible valid combinations reduces by a factor of 4! Furthermore, limiting the login attempts can strengthen security of USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION.

5.2 Dictionary attack

In USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION, each user authenticates herself with a set of four random images. She can either choose these images directly or use them as a cue for her text password of four letters. Users are free to use dictionary words as password. Although this may appear as a threat since an attacker can build a dictionary of most common four-letter words, we wanted to note that, according to scribble [17], there exist around 3,957 possible four-letter English words (excluding names of person, places and abbreviations). Therefore, building such dictionary may not be economical if we guard the number of successive login attempts.

5.3 Social engineering attack

We employ Probabilistic one time password strategy [18] described earlier to defeat prevalent forms of identity theft through social engineering. Explaining the theory behind the Probabilistic one time password strategy is beyond the scope of this paper. Interested readers can refer to the work of Bedworth [18] and Brostoff et al. [19].
At every login, images are randomly placed in the grid with a different set of numbers associated with them. With every login, the positions of images as well as the associated numbers within the grid change, making the password unique per session. Further, the position of images in the grid is irrelevant to the authentication process. Thus identity theft using following social engineering techniques is difficult.
5.3.1 Resistance against Shoulder surfing:
User never actually selects her true password images, by clicking on it. So anyone who is piping over the shoulder or even with hidden cameras can only be able to see the one time access code, which changes with each login session. Thus should ensuring is not effective.
5.3.2 Protection against malware attacks:
Our proposed scheme can be made effective even without the keyboard, therefore no advantage with key loggers. Even if someone captures and records the screen, she will still not be able to deduce your password as every time grid pattern is randomly generated and the password that is formed with given pattern is used only once.

6. USER STUDY OF USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION

One aspect of our user study aimed to test the usability of USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION. Is it simple? Is it easy to understand and convenient to use? Another goal of our user study was to learn the characteristics of user-chosen passwords in real system (i.e., in an environment where the passwords will be used frequently over a period of time). For example, do they contain dictionary words, do users prefer stories while creating passwords, what patterns they exhibit. In short, will they be easy to guess? If answers to most of these questions are affirmative then, our scheme can aid to memory benefits of earlier graphical authentication schemes.

6.1 Outline of the user study

We integrated USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION with a simple online course management portal. The access to the course content such as lecture notes, weekly exercise etc. was protected with USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION authentication scheme. The user study was conducted in the fall semester of 2009 in a second year computer Science Engineering university class, over a month's period, from late November to late December. In total 35 subjects participated, including 32 undergraduate students, 2 graduate students (Teaching

Assistants) and 1 professor. Twenty-five participants are male and 10 participants are female; the ages range from 20 to 45 with average of 22. The participants were from different regions of India, so apparently our participants represent a multicultural community.

At the start of the study, participants were given a 15-minute tutorial in the class by the first author of this paper. Because our user group consists of experienced computer users with solid computer knowledge and represents a relatively high education level, they might perform better than the general population in understanding our scheme. To somewhat compensate for this, we only used plain language in the tutorial (no technical terms were mentioned, such as mapping of pictures to passwords or how a password is encoded). We estimate the attendance rate on the day of the tutorial was approximately 85%. Our password scheme was then explained. Students were not given suggestions about how to choose a secure password or use any mnemonic strategy. A FAQ page was made available on the website in case they need help.

7. CONCLUSION

In this paper, we have presented USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION, a Secure graphical authentication scheme, strong enough for banking, finance ,e-commerce and sensitive organization. Its strength lies in its simplicity and unique graphical way of working. We have designed and secure prototype of USER AUTHENTICATION BY SECURED GRAPHICAL PASSWORD IMPLEMENTATION. We discussed possible attacks on our scheme and how we could defend each of them. Results of the user study provide evidences for improved usability and memorability. Our future work includes working on the feedbacks received by the participants (using personal pictures and improving the visual search) and testing the scheme with large audience of all ages and under secure password inferences.

8. ACKNOWLEDGMENTS

We would like to thank anonymous reviewers for their valuable comments. We also thank mu guide and my friend and the participants from the user study for their support and early feedbacks on the design. We also sincerely thank the members of Internet Picture Dictionary group for allowing us to use their images in the prototype design.

9. REFERENCES

[1] Chiasson, S. Usable Authentication and Click based Graphical passwords. Phd Thesis, Carlton University, Ottawa, Canada. Jan. 2009 .

[2] Cranor, L., and Garfinkel, S. 2005. Security and Usability: Designing Systems that People can use. O'reilly Media.

[3] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. 2005. PassPoints: design and longitudinal evaluation of a graphical password system. Int. J. Hum.- Comput. Stud. 63, 1-2 (Jul. 2005), 102-127.

[4] Feldmeier, D. C., and Karn, P. R. 1990. UNIX Password Security - Ten Years Later. In Proceedings of the 9th Annual international Cryptology Conference on Advances in Cryptology (1989). 44-63.

[5] Nelson, D. L., Reed, U. S., & Walling, J. R. (1976). Pictorial superiority effect. Journal of Experimental Psychology: Human Learning & Memory, 2, 523-528.

[6] Standing, L. Learning 10,000 pictures. Quarterly Journal of Experimental Psychology 25 (1973), 207-222.

[7] Davis, D., Monrose, F., and Reiter, M. K. 2004. On user choice in graphical password schemes. In Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13 (2004). 11-11.

[8] Shepard, R. Recognition memory for words, sentences, and pictures. Journal of Verbal Learning & Verbal Behavior. 6(1967),
156-163.

[9] Nali, D., and Thorpe, J. Analyzing user choice in graphical passwords. Technical report, TR-04-01, School of Computer Science, Carleton University, May 2004.

[10] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D. 1999. The design and analysis of graphical passwords. In Proceedings of the 8th Conference on USENIX Security Symposium. 8(1999). 1-1.

[11] Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. 2005. PassPoints: design and longitudinal evaluation of a graphical password system. Int. J. Hum.- Comput. Stud. 63, 1-2 (Jul. 2005), 102-127.

[12] Khot R. A., Srinathan K., Kumaraguru, P. Marasim: A Novel Jigsaw Based Authentication Scheme using Tagging , To appear, In the Proceedings of 29th Conference on Human Factors in Computing systems (CHI 2011). ACM.

[13] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D. 1999. The design and analysis of graphical passwords. In Proceedings of the 8th Conference on USENIX Security Symposium. 8(1999). 1-1.

[14] Dirik, A. E., Memon, N., and Birget, J. 2007. Modeling user choice in the PassPoints graphical password scheme. In Proceedings of the 3rd Symposium on Usable Privacy and Security (2007). SOUPS '07, 20-28.

[15] Renaud, K. and De Angeli, A. 2009. Visual passwords: cure- all or snake-oil? Commun. ACM 52, 12 (Dec. 2009), 135-140.

[16] Davis, D., Monrose, F., and Reiter, M. K. 2004. On user choice in graphical password schemes. In Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13 (2004). 11-11.

[17] Goldwasser, S., Micali, S., and Rackoff, C. 1985. The knowledge complexity of interactive proof-systems. In Proceedings of the seventeenth annual ACM symposium on

[18] Bedworth M. A. Theory of Probabilistic One-Time Passwords, http://www.pinoptic.com/downloads/wp002_a_theory_of_potp.pdf

[19] Brostoff, S., and Sasse, M.A. Are Passfaces more usable than passwords? A field trial investigation. Proceedings of HCI on people and Computers XIV, (HCI 2000), 405-424.