Graphical Password Authentication Using Image Segmentation

Rohitkumar Kolay, Animesh Vora, Vinaykumar Yadav

Department of Information Technology,
Universal College of Engineering, Vasai, Maharashtra, India

---***---

Abstract - *Authentication is performed using passwords that are alphanumeric in nature. However, users find it difficult in remembering a password that is long and needs to be recalled again and again while implementing it. Instead, they create short, simple, and insecure passwords that make the user's data vulnerable to outside attacks. Graphical passwords provide a way out of this dilemma by making passwords more rememberable and easier for people to use as a password and, therefore, makes it more secure. Using a graphical password, users clicks on images rather than typing text passwords which contains alphanumeric characters. A new and more secure graphical password system has been developed which uses image segmentation. The image segmentation system presents the user with an image upon which the user selects a number of grids on this image; when entered in a proper sequence these points authenticate the user. The findings showed alphanumeric passwords and graphical passwords both worked in similar time but the graphical passwords were easier to recall and remember.[1] Thus, Graphical passwords were found to be hard to crack as they are newly implemented and not many algorithms have been devised to break through them.*

Key Words: **Authentication, Encryption, Graphical, Password, Image, Login, Segmentation**

1.INTRODUCTION

[1]Computer, network, data and information security has been consider as a major technical problem faced nowadays. However, it is now widely recognized and accepted that most security mechanisms cannot succeed without taking into account the user's views [2].Various graphical password schemes are used as alternatives to alphanumeric passwords [3]. Research has shown that alphanumeric passwords are filled with both security and usability problems that make them less than desirable solutions [4]. A key area in security research is authentication which deals with the determination of whether a particular user should be granted access to a given system or resource. This paper aims at providing understanding about a new graphical password authentication system using image segmentation. The significance of this study paper is the comprehension of a flexible graphical password authentication system with extensive findings to support it. Graphical password authentication can be implemented using two techniques - Recall based and Recognition based. The basic idea of using the image segmentation system is that using images as a security will lead to high memorability and decrease the chances to choose insecure passwords. This, in turn, should increase overall password security. Our primary question is the following: Are graphical passwords competitive to alphanumeric passwords in terms of security, performance and retention?

1.1 Background and Related work

We refer to the security and usability problems involved with alphanumeric passwords as "the password problem." The problem rises because passwords are expected to act with two conflicting requirements, namely: (1)Passwords should be easy to remember, and the authentication protocol should be executable quickly and easily by humans. (2) Passwords should be secure, i.e. they should be hard to guess and should look random; they should be changed frequently, and it should be different on different or multiple accounts of the same user; they should not be written down or stored in plain text. Meeting such requirements is almost impossible for users. The problem is well known in the security community. Classical studies going back over 25 years[5] have shown that, as a result, human users tend to choose and handle alphanumeric passwords insecurely. Recent studies confirm these results[6]. The password problem arises primarily from fundamental limitations of human's long-term memory (LTM). Once a password has been chosen and learned the user must be able to remember and recall it to log in. However, people usually forget their passwords. The Power Law of Forgetting describes rapid forgetting soon after learning, followed by very slow drop-off thereafter[7]. Psychological theories have attributed forgetting to decay through the passage of time and to interference, in which new items in memory interrupt existing ones (retroactive interference). A recent review emphasizes the importance of retroactive interference in everyday forgetting[8]. Decay and interference help to explain why people forget passwords. Users are expected to learn and recall a password and remember it over time. However, other items in memory compete with the password and makes it difficult to recall. If a password is not used frequently it will be especially susceptible to forgetting. Recent research has shown that when users fail to recall a password, they often are able to recall parts of it correctly[9]. However, the use of passwords in the password authentication is predicated on completely accurate recall, so a partially correct password has no value now. Furthermore, today users have many passwords for computers, networks, web sites, and many more. In addition, some system requires frequent password changes, in a probably misguided effort to increase security. This use of passwords increases potential interference and is likely to lead either to forgetting passwords or forgetting in which system a password is associated with. What is a user to do? Most often a user will decrease the burden in its memory at the expense of security. Perhaps most commonly, the user will write down passwords and keep them in a convenient place, which will prevent in compromising of the passwords. One approach to increasing password security is education of the[10]. However, given the mismatch between passwords and human capabilities, the likelihood of fundamental change is not great[11]. A better way to overcome the password problem is to develop password systems that reduces thel memory problems while preserving security. Recall based techniques ask the user to recreate something that he/she has previously created in the registration stage. An example of Recall based system includes Draw-A-Secret scheme which asks user to draw a simple picture on a 2-D grid at the time of registration and it stores the co-ordinates of the grid in the order that it has been drawn. This technique has a drawback attached to it-Redrawing the image has to touch the same grids in exactly the same sequence during authentication. Recognition based techniques present the user with a set of images and the user is asked to recognize and identify the images he selected during the registration stage. One such example which lies between Recall and Recognition based techniques is the Passpoint technique. The system allows any random image to be used which should enable to have many possible click points. The role of the image is just to provide a clue to the user which helps in remembering the click points. During login, the click points should be selected in the same order asit was in registration phase inside some adjustable tolerable distance. This is very time consuming and requires to recall those certain points. The setbacks attached to this technique can be addressed by using the image segmentation system. Image segmentation is a recall based system as it offers a point which should establish context and trigger the stored memory[13].

1.2 Image Segmentation: A new graphical password scheme

PassPoints Scheme is similar in many respects to the Blonder's scheme but uses only a single image. This scheme is flexible because it allows to use any type of image i.e it may either be provided by the system or chosen by the user. The proposed system allows user to change to put an image as its password and only the user knows what image he or she has put in. On receiving the image, the system segments the image into an array of images in the grid format and stores them accordingly. The next time, the user logs on to the system, the segmented image is received by the system in a jumbled order. Now if users chooses parts of an image in an order so as to make the original image he sent, the user is considered authenticate. Else the user is not considered authentic. The only practical requirement in selecting a particular image is that an image should not comprise of a major portion of a single coloured object. For example: a wall or the picture of sea or ocean or a cloudless sky. That way, it will be not be easy for the user to guess the right sequence of grids to form a complete image. Rather an image should be rich in content and contain various components and objects that define a pattern only recognizable to the user.

Fig -1: Original Image

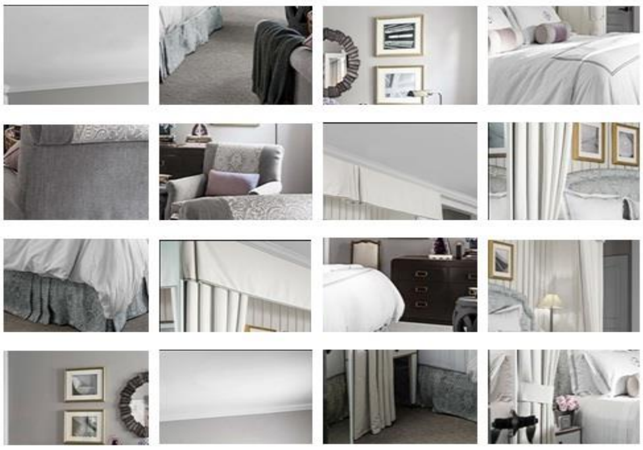

Fig -1: Segmented Image with sequence clues

2. DISCUSSION

Image segmentation has the security advantage of a large password space over alphanumeric passwords. It also has an advantage in password space over Blonder-style graphical passwords and recognition-based graphical password, such as Passfaces. In spite of the difficulties at the beginning of the implementation of graphical password authentication system, after some practice the users would feel comfortable implementing either alphanumeric or graphical based password as input. The people using graphical password authorization would be able to enter the password correctly with a much faster pace after they have improved with practice. This reflects that only a minority of graphical participants would have a serious difficulty in learning[15]. However, any authentication scheme needs to be evaluated in terms of possible threats. We recommend that Image be implemented and deployed in systems where online attacks are not possible, and where any attack made against an online system can limit the number of guesses made per account in a given time period. We assume that all communication between the server and client will be made securely through SSL, maintaining security of selected click-points and corresponding images, therefore avoiding simple attacks based on network sniffing. We suggest that the image mappings be done on a per-user basis as a function of the username i.e. grant a different image to different groups of people based on their username. We also suggest that the image set across all users is a multiple set containing a very large number of images and that users are assigned a subset of these images for their image-maps. Attacks against such a system, where attackers try to break into any account [16], are slowed due to the precautions mentioned above. Hotspot analysis might be used to increase the efficiency of an attack dictionary but images are need to be collected and such dictionary would need to be generated on a per user basis. Online attacks against specific users are more bothersome and require further examination.

Shoulder-surfing and other information capture from users. Most graphical passwords schemes are vulnerable to shoulder-surfing attacks [17]. With today's small cameras and camera phones, it is easy to capture a video of a user's screen or keyboard as they are logging in. Image segmentation is also susceptible to such attacks and its present form the change in images may be easier to see from further away than mouse pointer movements in Image segmentation. With knowledge of which images to look for in systems allowing sufficient numbers of guesses, attackers could try a brute-force attack of clicking on random grids until the correct sequence is achieved. If the username and the grid sequence are observed through shoulder-surfing then an attacker has all of the information needed to access the account, as is the case with most other password systems. Having a compromised computer is also a threat because some malwares may capture the login information and relay that information elsewhere. Whereas a keylogger success for text passwords, for graphical passwords software is needed to capture the images and the mouse cursor positions. When only limited information is known, it can be used to narrow the search for a correct guess. With the correct grid sequence, knowing the username is enough to retrieve the user's sole image. Hotspot analysis [18] can only be conducted on that particular images thus the images provided by the servers are safe from Hotspot analyzers. Thus Image segmentation is not suitable in environments where shoulder-surfing is a realistic threat, or environments where user images can be recorded (e.g., by insiders, malicious software on the client machine, etc.).

Hotspots and dictionary attacks. In some of the cases where attackers are not in a position to capture information from the user, they are limited to what they can conclude through image analysis. Hotspots are specific areas in the image that have a higher probability of being selected as part of their passwords by users. If attackers can accurately predict the hotspots in an image, then it becomes easier to built a dictionary of passwords containing combinations of these hotspots. Hotspots are known to be problematic for Image segmentation [19]; further analysis is needed to determine whether precautions such as carefully selecting grids can minimize this threat. A key advantage of Image Segmentation over any other graphical password authentication is that it is feasible to brute force and dictionary attacks. It also provides a way of making more human friendly but strong passwords. For example, if a user selects an image of buildings he is familiar with. That way, not only does a user is easily able to arrange the grids in the proper sequence but also manage to protect its data from infiltrators. As a result, the security of the system is very high. The major disadvantage however is that it takes a lot of time to register and log in to the system.

3. CONCLUSIONS AND FUTURE WORK

In conclusion, the study of Image segmentation indicates its strengths and weaknesses. Graphical password users would be able to easily create a valid password, but they would have to shell out more storage space than alphanumeric users, taking more trails and time. An area of interest with using Image Segmentation is that it satisfies both conflicting requirements that is, it is easy to remember and hard to guess. In principle, this could be an ideal solution for all kinds of devices as opposed to the difficulty of typing a long, secure alphanumeric password on the keyboard all the time. The challenge is to provide a large enough password space on a small image. However, this might be handled by magnifying an area of the image when the user moves his finger to a given area of the screen. In conclusion, Image Segmentation seems to hold out the prospect of a much more secure system as it is easy to gain large passwords spaces, based on complex, natural images. This reduces the chance of an attacker being able to guess passwords. The second most important thing this paper aims at is the usability of Image Segmentation, the Image Segmentation provides for the user not requiring to remember the different passwords. Psychological research indicates that interference can cause remarkable memory problems[8]. Security research [10] confirms that users have difficulty in remembering multiple passwords and produce unsafe practices to overcome the problem (writing passwords down, etc.)

REFERENCES

[1] Birget, J.C., Hong, d., Memon, N.Robust discretization, with application to graphical passwords. Cryptology ePrint Archive,
http://eprint.iacr.org/2003/168, accessed Jan 17,2005 M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K.Generating and remembering passwords. Applied Cognitive Psychology 18 (2004), 641-651.

[3] Boroditsky, M.Passlogix Password Schemes. http://www.passlogix.com. Accessed Dec. 2, 2002.

[4] Brostoff, S. and Sasse, M.A. Are Passfaces more usable than passwords: A field trial investigation. In People and Computers XIV - Usability or Else: Proceedings of HCI 2000 (Bath, U.K., Sept. 8-12, 2000).

[5] Adams, A. and Sasse, M.A. Users are not the enemy. CACM 42, 12 (1999), 41-46.

[6] Blonder, G.E. Graphical passwords. United States Patent 5559961, (1996).

[7] Bradley, M.M., Grenwald, M.K., Petry, M.C. and Lang, P.J. Remembering pictures: Pleasure and arousal in memory. Journal of Experimental Psychology 81, 2 (1992), 379-390.

[8] Bahrick, H.P. semantic memory content in permastore: Fifty years of memory for Spanish learned in school.

Journal of Verbal Learning and Verbal Behavior 14 (1984), 1-24.

[9] Borges, M.A., Stepnowsky, M.A., and Holt, L.H. Recall and recognition of words and pictures by adults and children. Bulletin of the Psychonomic Society 9, 2 (1977), 113-114.

[10] Biederman, I., Glass, A.L. and Stacy, E.W. Searching for objects in real world scenes. Journal of Experimental Psychology 97 (1973), 22-27.

[11] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N.Memon, "PassPoints: design and longitudinal evaluation of agraphical password system," Int. Journal of HCI, vol. 63,2005, pp. 102–127.

[12] Real User Corporation. The science behind Passfaces. Whitepaper, http://www.realuser.com/published/ScienceBehindPassfaces.pdf, accessed Feb. 2012.

[13] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in 8th USENIX Security Symposium, 1999.

[14] H. Tao and C. Adams, "Pass-Go: A proposal to improve theusability of graphical passwords," Int. Journal of NetworkSecurity, vol. 7, no.

[15] P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in the- loop," ACM Trans. Info. System Security, vol. 9, no. 3,2006, pp. 235-258.

[16] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "Captcha: Using hard AI problems for security," in Eurocrypt, 2003, pp. 294-311.

[17] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in European Symposium on Research in Computer Security (ESORICS), 2007, pp. 359-374.

[18] E. Stobert, A. Forget, S. Chiasson, et al. Exploring usability effects of increasing security in click-based graphical passwords. In Annual Computer Security Applications Conference (ACSAC), 2010.

[19] Harsh Kumar Sarohi,Graphical Password Authentication Schemes: Current Status and Key Issues, International Journal of Computer Science Issues,2013, 437-443.

[20] S.Singh, G.Agrawal "Integration of sound signature in graphical password authentication system" Invertis University Bareilly,India, January ,2011.

BIOGRAPHIES

Mr. Rohitkumar Kolay is currently completing **B.E** in Information technology from the Universal College of Engineering, Vasai, Mumbai University, Mumbai, India.

Mr. Animesh Vora is currently completing **B.E** in Information technology from the Universal College of Engineering, Vasai, Mumbai University, Mumbai, India.

Mr. Vinaykumar Yadav is currently completing **B.E** in Information technology from the Universal College of Engineering, Vasai, Mumbai University, Mumbai, India.