Poster: Preliminary Investigation of Gesture-Based Password: Integrating Additional User Behavioral Features

Lakshmidevi Sreeramareddy[1]
[1]Dept. of Computer and Info. Science
Towson University
Towson, MD 21252
lsreeramareddy@towson.edu

Jinjuan Feng[1,2]
[2]Dept. of Information Systems
UMBC
Baltimore, MD21250
jfeng@towson.edu

Andrew Sears[3]
[3]Rochester Institute of Technology
Rochester, NY 14623
alsics@rit.edu

1. INTRODUCTION

Effective user authentication applications are crucial to protect information security. In response to the growing number of threats to data security, a wide variety of authentication mechanisms have been developed. Many existing authentication methods (e.g., alphanumeric passwords) are difficult to remember, especially for individuals with cognitive disabilities that affect memory (e.g., Down syndrome, mild Traumatic Brian Injury, and dementia). We propose a gesture-based password approach aiming to reduce the memory load of the authentication process. This approach just uses the mouse for input and no additional device is required. Users draw an image using the mouse as their password. In addition to the image drawn, we also examine additional measures such as password length, size, angles, and speed to authenticate the user. We have collected initial data to investigate the potential of this approach.

2. RELATED WORK

Alphanumeric passwords, although widely adopted, have fundamental limitations regarding the actual password space and the difficulty in remembering the passwords [1]. Graphical passwords have been proposed in the past decades. The major advantage of graphical-based passwords is that they are easier to remember than alphanumeric password [3]. The disadvantage of graphical passwords, especially recognition-based passwords, is the smaller password space, making them more vulnerable to brute force attack. In addition, graphical passwords are also highly susceptible to shoulder surfing.

The DAS (Draw A Secret) scheme [5] is closely related to the proposed gesture password approach. A DAS password is a picture drawn on a grid mapped to a sequence of coordinate pairs using the cells through which the drawing passes. The DAS scheme offers a theoretically large password space and is easily repeatable. However, similar to textual passwords, users tend to underutilize the password space made available through the DAS scheme. In addition, 29% of the password created were invalid because they followed the grid lines or cross grid corners [7].

Two gesture password prototypes have been developed that take one or multiple strokes as passwords. The Passdoodles method [9] considers the shape of the stroke and the movement speed. The gesture-based touchpad system [6] considers the shape of the strokes and the length of pause between strokes. Neither system was formally evaluated via empirical user studies.

More recently, researchers started to explore the possibility of using behavioral measures to enhance the authentication process. For example, De Luca et al. used pressure, coordinates, size, speed, and time as an additional layer to authenticate a user on a touch screen smartphone [4]. Sae-Bae et al. examined fingertip dynamics (e.g., all fingertip moving or partial fingertip moving) as an additional authentication component and tested the idea using an iPad [8]. Preliminary studies suggest that the use of behavioral factors is promising. However, both studies required pre-defined shapes or gestures or the strokes being created in reference to specific locations on the screen.

3. APPLICATION DESIGN

Different from most existing gesture-based authentication methods used on touchscreen devices that require pre-defined shapes or gestures, our application allows users to draw their passwords freely on a canvas using the mouse. There is no limitation on the password images that the users create. The users do not need to limit the strokes of the password to pre-defined shapes such as a line or a circle. Once a password is created, we use specific algorithm to determine how similar the newly entered password is to the original password. In addition to the similarity between the password images, we also explore behavioral measures to enhance the authentication.

In the intial study, we used $1 gesture recognizer to determine the similarity between the original password and the re-entries. $1 recognizer uses a template matching approach to match input gestures to a set of stored gestures [2]. $1 is well-suited for security applications because users can define their own templates (i.e., passwords). Since the gesture set required for security applications is small, high recognition accuracy is expected. The similarity between the original passwords and the re-entries is measured through a confidence score (ranging between 0 and 1).

We explore multiple behavioral measures to enhance the gesture-based authentication application. The measures that we initially examined include: password length, size (the area of the bounding box around the password image), speed of mouse movement, and angles. We computed two angles: start angle and end angle. The start angle is the angle formed between the initial line of a gesture (point 0 to point 7) and the horizontal line. The end angle is the angle formed between the ending line of a gesture and the horizontal line.

4. INITIAL EVALUATION

We collected data through a preliminary user study to examine the nature of the passwords created and whether users can easily adopt the proposed method. We also wanted to study the nature the behavioral measures. In this study, each password only contains one stroke. Twenty neurotypical participants took part in

the study. Each participant created six gesture passwords and re-entered each password ten times.

4.1 Passwords created

All participants easily mastered the method and were comfortable drawing the password according to the satisfaction survey. The passwords created by the participants were quite interesting. Some passwords were very simple (e.g., a straight line), while others contain images that represent specific objects or concepts. Figure 1 illustrates two passwords collected from the study, one associating to the word 'Love', the other illustrating a 'dog'. By associating the password to an object or a concept, the users can easily remember the password. In the meanwhile, because each user has a unique way in drawing the image, the password is much more secure than simple alphanumeric passwords such as 'love' or 'dog'.

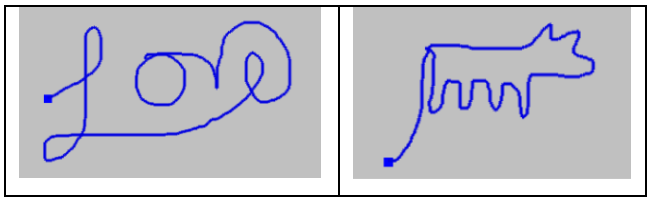

Figure 1. Sample passwords created (Left: Love. Right: Dog).

4.2 Confidence score and behavioral measures

The $1 recognizer recognized the re-entries with high accuracy. 83.3% of the re-entries received a confidence score higher than 0.8. Only 4% received a confidence score below 0.6.

Table 1. Distribution of variation in re-entries

Range	Length	Size	Speed
10%	1.9	19.3	16.6
20%	8.3	38.7	37.6
30%	21.7	54.5	60.6
40%	42.5	67.7	81.8
50%	70.4	76.9	92.0
60%	95.6	82.6	98.0
70%	99.8	86.6	98.9
80%	99.9	89.1	99.1

Since it is impossible for a human to draw two images in exactly the same way, the system has to allow variations between the re-entries and the original passwords. The degree of variation allowed is a crucial design feature because the passwords will be frequently rejected if the degree of variation allowed is too small. In contrary, if the variation allowed is too large, the password will be susceptible to shoulder surfing and hacking. We analyzed the degree of variations in the behavioral measures between the re-entries and the original password created (see to table 1). For length, size, and movement speed, the majority of the re-entries have variation within the 50% range. There is more variation in the end angles than the start angles. 80% re-entries have start angle variation within the (-25, 25) degree range, while only 49% have end angle variation within the (-25, 25) degree range. Although there is substantial variation in all measures, the measures can still be potentially informative for authentication, especially when multiple measures are combined.

5. FUTURE RESEARCH PLAN

In the next stages of the study, we will collect data on multi-stroke passwords using $N recognizer and study the distribution pattern of the confidence scores and the behavioral measures. We will explore the use of machine learning methods to determine the appropriate range allowed for different behavioral measures. We will also conduct user studies to investigate the security aspect of the gesture password (e.g., vulnerability to shoulder surfing, theoretical password space vs. actual password space).

After that, we plan to evaluate the gesture-based application used by individuals with cognitive disabilities and study how the application design and the recognition algorithm can be modified to fit the special needs of this population. We will also examine whether there is any difference in the behavioral measures between individuals with cognitive disabilities and neurotypical users.

Acknowledgement

The authors would like to thank Dr. Lisa Anthony for her input in the early stage of the project.

6. REFERENCES

[1] Adams, A. and Sasse, M. A. (1999). Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM, 42(12), 40-46.

[2] Anthony, L. and Wobbrock, J.O. (2010). A lightweight multistroke recognizer for user interface prototypes. *Proceedings of Graphics Interface (GI '10)*, Ottawa, Ontario, Canada (May 31-June 2, 2010). Toronto, Ontario: Canadian Information Processing Society, pp. 245-252.

[3] Brostoff, S. and Sasse, A. (2000). Are Passfaces More Usable Than Passwords? A Field Trial Investigation. *Proceedings of HCI 2000*, pp. 405-424.

[4] De Luca, A., Hang, A., Brudy, F., Lindner, C., and Hussmann, H. (2012) Touch me once and I know it's you! Implicit authentication based on touch screen pattern. Proceedings of CHI 2012. 987-996.

[5] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., and Rubin, A. (1999). The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX Security Symposium*.

[6] Mejia, D. and Doose, J. (2010). Gesture based touchpad security system. Last retrieved May 20, 2012 from http://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/s2010/jkd27_dm472/MyPage/index.html

[7] Nali, D. and Thorpe, J. (2004) Analyzing user choice in graphical passwords. Technical Report TR-04-01, School of Computer Science, Carleton University, Canada, 2004.

[8] Sae-Bae, N., Ahmed, K., Isbister, K., and Memon, N. (2012). Biometic-rich gestures: A novel approach to authentication on multi-touch devices. Proceedings of CHI2012. 977-986.

[9] Varenhorst, C., (2004). Passdoodles: A Lightweight Authentication Method. MIT Research Science Institute. Last Retrieved May 20, 2012 from http://people.csail.mit.edu/emax/public_html/papers/varenhorst.pdf