Exploring the Use of Discrete Gestures for Authentication

Ming Ki Chong and Gary Marsden

Department of Computer Science, University of Cape Town,
Rondebosch, Cape Town, South Africa
{mchong,gaz}@cs.uct.ac.za

Abstract. Research in user authentication has been a growing field in HCI. Previous studies have shown that peoples' graphical memory can be used to increase password memorability. On the other hand, with the increasing number of devices with built-in motion sensors, kinesthetic memory (or muscle memory) can also be exploited for authentication. This paper presents a novel knowledge-based authentication scheme, called gesture password, which uses discrete gestures as password elements. The research presents a study of multiple password retention using PINs and gesture passwords. The study reports that although participants could use kinesthetic memory to remember gesture passwords, retention of PINs is far superior to retention of gesture passwords.

Keywords: User authentication, gesture passwords, discrete gestures.

1 Introduction

User authentication is a fundamental requirement for most remote access services. Most often, a user is required to provide a knowledge-based password as evidence of the user's identity. Traditionally, alphanumerical passwords or PINs (Personal Identification Numbers) are used for user authentication. However, the use of a text-based password requires a trade-off between security and memorability. This trade-off arises from the limitation of human memory and, as a result, 'secure' passwords (long and random sequences of characters) are easily forgotten. To avoid the risk of forgetting passwords, users often adopt insecure behaviours such as writing down their passwords or disclosing their passwords to perceived trusted parties [1].

Usable security is a growing field of research in HCI. Concepts and ideas from earlier research have suggested that alternative authentication schemes, other than the knowledge-based schemes, are possible. Schemes such as token-based and/or biometric-based solutions were introduced as alternatives to passwords. Since these schemes do not require the users to memorize passwords, they have an advantage over knowledge-based systems by reducing the load on users' memory. However, these solutions are introduced at the expense of accessibility and cost of hardware [2], and, as a result, knowledge-based verification remains the preferred form of user authentication.

In the search to improve password usability, the use of graphical passwords has emerged as an alternative solution. Graphical passwords exploit the *picture superiority effect* [3]. Cognitive studies have shown that people are much better at recognizing

T. Gross et al. (Eds.): INTERACT 2009, Part II, LNCS 5727, pp. 205–213, 2009.

previously seen images than at recalling text precisely [4]. Graphical images provide a rich and detailed representation in memory, which also make the images distinctive at time of retrieval [3]. And hence graphical passwords can be particularly useful in addressing the weakness of memorability in text-based passwords. This is confirmed by findings from earlier research which have shown that graphical images can increase password memorability through users' visual memory [5]. Moreover, a previous study by Moncur and Leplâtre [6] examined subjects' retention of multiple PINs compare to multiple graphical passwords. Their results demonstrate that multiple graphical passwords are substantially more memorable.

Although previous studies on graphical passwords have shown that using visual aids can help users to encode passwords into their long-term memory, there are other retention approaches that can be exploited to increase password memorability, and kinesthetic memory (or muscle memory) is a one of those approaches. Instead of using text-characters or images, a password can be made up of multiple gestures: through practice and repetition, the password movements can gradually consolidate into the user's memory. However, so far no research was done to investigate how kinesthetic memory can assist users in remembering passwords.

This paper addresses a new authentication approach, called gesture password, which exploits kinesthetic memory for password retention. It aims to answer the following question:

Can people remember gesture passwords successfully?

In addition, we are particularly interested in exploring the use of gesture passwords for mobile authentications such as mobile banking; therefore, mobile phones are selected as the input devices in this research.

In the rest of this paper, we present a new gesture password design that uses arm movements as a set of password elements. We report an empirical study of gesture passwords and a discussion of the results before conclusions are drawn and future directions for research are identified.

2 Design

In recent years, accelerometers have been increasingly integrated into mobile phones (such as Apple's iPhone, Nokia N95, etc.). A built-in accelerometer allows the mobile device to sense users' movements and, as a result, it provides a new modality for user input. At the moment (2008), there are a small number of mobile applications which make use of this: for example, Williamson et al. introduced Shoogle, an interface for sensing data within a mobile device as the device is shaken [7]. As more uses of accelerometers are being discovered, we confidently predict that more mobile phones will be equipped with built-in accelerometers in the near future.

In the design of this research, an accelerometer is used to detect directional movements as gesture inputs for user authentication for mobile devices.

2.1 Related Work

Although there is no research that investigates the use of kinesthetic memory to increase password memorability, there is some work which exploits the use of gesture

movements for authentication. In an attempt to create PIN-less authentication environments, researchers have designed methods that use gestures for pairing devices. In [8], Patel et al. suggested an authentication scheme by shaking a device. Their authentication scheme is based on a user authenticating his/her device when using a public terminal by mimicking a sequence of gestures that is generated by the device and displayed on the terminal. Similar work by Mayrhofer and Gellersen suggests a method which uses accelerometer data to pair two mobile devices [9]. Their authentication method requires a user to hold the pairing devices tightly together and shake the devices for a short period. The built-in accelerometers within the devices are used for measuring the movement as the devices are shaken; the devices will only be paired if the accelerometers readings are similar.

Research by De Luca et al. discovered that many people memorize their PINs by remembering the resulting shape of the spatial relations on the number pad [10]. From their findings, Weiss and De Luca introduced a concept, called PassShapes, of replacing PIN numbers with directional strokes in a two-dimensional plane. The strokes of a password are made up of many horizontal, vertical, and diagonal strokes. The strokes can form specific shapes, and the shapes are suggested as password mnemonics [11].

2.2 Gesture Password Elements

The gestures used for this study are discrete gestures. A discrete gesture can be distinguished as a movement from a starting position to a stopping position. Here, a discrete gesture is defined as *a distinctive singular movement that can be perceived individually and not connected to, or part of another motion*. In other words, a motion that cannot be further decomposed as units of actions can be classified as a discrete gesture. Since it has the property of a discrete structure, multiple singular gesture units can be combined to form a string of discrete gestures.

In this study, we apply a concept similar to PassShapes. Gesture strokes in a three-dimensional space are used as passwords. Ten discrete gestures (illustrated in Fig. 1) are defined as password elements. The elements were designed based on the spatial orientation of a mobile phone, and they were also designed with the intention that each gesture must have a symmetrical gesture in the mirror direction. The *forward* gesture (Fig. 1.a), for example, has a symmetrical gesture element *backward* (Fig. 1.b) in the mirror direction. The reason for the design with symmetry is to ease the process of learning the gestures. As novice users learn a gesture element they can apply the reverse movement to learn the mirror gesture, thus simplifying the learning process for the users.

Due to the articulation structure of a human arm, motion is limited in certain ways. This implies that some strings of gestures could be impossible for people to reproduce. For example, when a user holds a device perpendicular to the ground, the maximum tilting angle the user can rotate the device is about 180 degrees. Beyond that point it is uncomfortable or impossible to tilt further. Thus a string of tilt left or tilt right is not replicable by a user (Fig. 2 illustrates an example of a string of tilt left gestures. Tilting left beyond fig. 2.c is impossible). This problem manifested during our initial design stage, so a decision had to be taken that after each element entry, the device must be moved back to its starting position; hence the next element entry must start from the initial position. As a result, a valid password element entry is a string of paired discrete gestures, where a given pair is made up of a gesture element and its reverse.

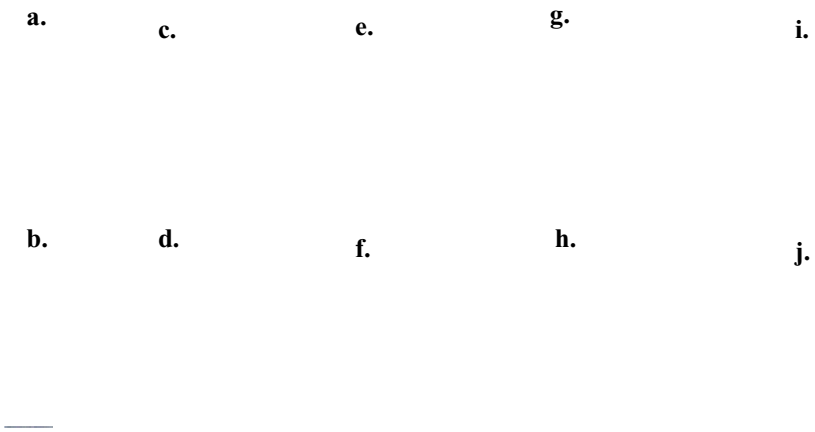

Fig. 1. Gesture password elements. (a) *Forward*, (b) *Backward*, (c) *Up*, (d) *Down*, (e) *Left*, (f) *Right*, (g) *Tilt Left*, (h) *Tilt Right*, (i) *Swing Left*, (j) *Swing Right*

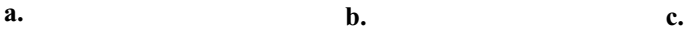

Fig. 2. A string of tilt left gestures before adjustment. (a) *Initial position*, (b) *Tilt left from position (a)*, (c) *Tilt left from position (b)*.

2.3 Security

A *string* is an ordered list of elements in which the same elements can appear multiple times at different positions. In this study, a *gesture password* is defined as a string of multiple gesture elements. For a user to authenticate, that user is required to produce a string of gesture password elements in the correct order. Since our system supports ten different gestures, it has the same password space as standard PINs, thus both systems have the same statistical guessability.

One of the drawbacks of gesture passwords compares to PINs is that the system is susceptible to shoulder surfing attacks. Due to the nature of using movements as inputs, an attacker can observe and record a user's gesture password entry easily. We therefore recommend gesture passwords are only to be used in private secure areas.

2.4 User Interaction

A gesture entry is entered as a movement that starts and stops in the same position. A complete gesture is defined as the change of state from a motionless state to a moving state and then a motionless state to identify the end of the gesture. Consequently, for the system to register a motionless state, the user needs to pause between each gesture elements during password entry.

3 Study

Human memory has a limited capacity to remember the arbitrary text and number strings that make up a password. This results in password retention deficiency and to overcome this deficiency, people select passwords to which they can attach meaning. Although memory cues help users to memorize their passwords, the passwords can also become more guessable and raise security vulnerabilities. To avoid this weakness, many security systems disallow the use of personalized passwords, generating and enforcing random passwords for their users.

In this study, we therefore restrict ourselves to the issue of retention of multiple system generated passwords. As previously mentioned, a study by Moncur and Leplâtre [6] compared subjects' retention of multiple PINs compared to multiple graphical passwords. Following on from their study, we investigate users' retention of multiple passwords of PINs and gesture passwords. We therefore conducted a one week longitudinal study to measure passwords retention. Furthermore, we are particularly interested in the memory strategies of users of the evaluating authentication systems.

3.1 Passwords Retention Test

In this study, we tested for users' retention of multiple passwords. 12 learners from a skill training centre in Khayelitsha, Cape Town, were recruited as participants. The subjects participated in the study during their class hours, so each subject was paid R60[1] at the end of the study for remuneration. We recruited adult subjects; their ages range between 17 to 39 years old and with a mean age of 24.9.

One of the aims of this study is to learn the strategies that the subjects adopt to memorize passwords of each testing system. To avoid any learning effects (such that the subjects applying a strategy learned from one system to another), the between-groups experiment approach was adopted. Therefore, six subjects were assigned to a group using PINs (Group 1) and the other six were assigned to a group using gesture passwords (Group 2).

To simplify the experiment process, the experiment was conducted without using digital prototypes. Instead, the *wizard of Oz* prototyping technique [12] was adopted. All participants first undertook a training session to familiarize themselves with the allocated password system; each subject was trained by the experiment facilitator. For the gesture password group, the movements of the ten gestures elements were illustrated to the subject by the facilitator. To simulate inputting gesture passwords using a mobile device, a block of a rectangular object (we used a mobile phone) was given to

[1] The symbol "R" represents South African currency "Rand".

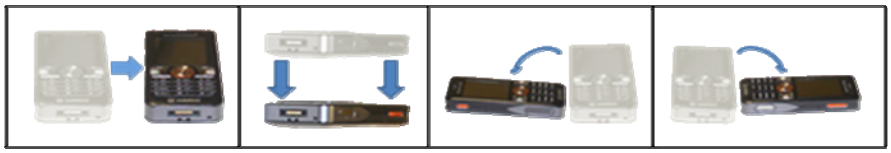

Fig. 3. An example of a random gesture password. The password is read from left to right (i.e. the left most gesture is the first element).

the subject to represent a sensor device. After demonstrations, the subject was requested to reproduce the ten gestures; this is to ensure the subject understands the system and knows how to enter gesture passwords.

Once the subject was familiar with the system, he/she was given three pre-generated random passwords (see fig. 3 for an example of a gesture password); each password was made up of four elements.

In [6], their participants undertook a rehearsal session by entering each of their assigned passwords correctly twice. However, we believe that entering the passwords twice is not sufficient for the subjects to register the gesture passwords into their kinesthetic memory. Instead, our subjects were given a 24 hour rehearsal period to memorize the passwords. To enable the subjects to have access to the passwords during the rehearsal period, the passwords were given to the subjects on paper.

After the rehearsal period expired, a facilitator returned to the subjects and collected the papers that contain the passwords. Six days later the facilitator returned again and requested the subjects to recall their given passwords. This was followed by a questionnaire session to determine the methods the subjects applied to remember the passwords.

Although 12 subjects were initially recruited for this study, one subject from group 1 had dropped out. Therefore, a total of 15 PINs and 18 gesture passwords were tested (the results are listed in Table 1). Given the participants with the defined periods, the results show that retention in group 1 was superior to retention in group 2. The result of group 1 could be influenced by the subjects' familiarity with PINs. Hence, the subjects have already adopted an effective strategy to remember PINs beforehand. The low scores archived by group 2 are suspected to have been caused by the subjects not having enough time to practise their passwords. One of the subjects had explicitly mentioned to us that she needed more time to memorize her given passwords.

Table 1. Results of the retention test

PINs		Gesture Passwords	
Subject ID	Score (Out of 3)	Subject ID	Score (Out of 3)
PIN1	3	GES1	0
PIN2	3	GES2	1
PIN3	3	GES3	1
PIN4	3	GES4	0
PIN5	3	GES5	0
PIN6	*dropped out*	GES6	1

3.2 Retention Strategies

Subsequent to the experiment, a questionnaire on users' retention strategies was conducted. Three subjects from group 1 indicated that they remembered PINs through visualizing the images of the numbers. One subject said he adopted a strategy by grouping the PINs' digits into groups of two numbers. He memorizes a PIN by remembering the first two digits and then the next two digits. Two subjects from group 1 adopted a strategy of rehearsing the numbers audibly in their mind. None of the subjects adopted the strategy of constructing a story using the given PINs, and neither did they adopt the strategy of memorising the PINs through the mnemonic of the numbers' position on a keypad. The former can be explained by the difficulty of constructing a story using only numbers, and the latter is because the PINs were given on paper, thus the subjects never entered the PINs on a number pad. The questionnaire with group 2 reported that all six participants have practised their gesture passwords by moving their hands in the passwords' directions. Five subjects reported to have adopted the strategy of rehearsing the gesture passwords audibly by speaking the directions, and three subjects memorized the passwords by visualising the directions, like the arrows of the gestures. The results show that participants attempted to use their kinesthetic memory to memorise gesture passwords through practice, in addition, some participants also opted to use their audio and graphical memory for gesture passwords. In other words, some people use their alternative memory to increase the memorability of gesture passwords. This could be because visual and audio memory complements muscle memory for gesture passwords; however, further study is required to confirm this.

4 Conclusions and Future Work

In conclusion, we suggested an alternative password authentication system for mobile devices that exploits users' kinesthetic memory to recall passwords. We defined a new password scheme which uses discrete movements as password elements, and we investigated the memorability and users' retention strategies of gesture passwords. The results from the empirical study suggest that users are more effective in remembering PINs than gesture passwords.

Currently, we can argue that computers and mobile phones are the most common devices that require authentication, but we should not limit ourselves in researching suitable authentication solutions for those devices only. As ubiquitous computing is becoming more popular, many new types of devices also require authentication. Although negative results of gesture passwords were shown in this research, it should not limit the adoption of gesture passwords. Our gesture password system is ideal for devices that are equipped with a built-in accelerometer and limited user input capabilities. Using Apple's fourth generation iPod Nano [13] for an example, instead of using its click-wheel to enter PINs, the system can adopt gesture passwords for authentication. One can argue that graphical authentication is a good option for iPods. However, much of the details of the graphical display may be lost due to the small resolution screen of the device; therefore, some pictures of a graphical authenticator may not be displayed properly.

In this project, the gesture elements were designed for mobile phones. This decision has restricted the gestures to be large and slow arm movements. Smaller sensors may be more appropriate to detect movements. In such a case, faster and more discreet gestures could be adopted as password elements and more flexible muscles could be used; for example, detecting finger movements as gestures.

One aspect of security not covered in Moncur and Leplâtre's work [6], nor any other HCI study we could find, was an investigation into the users' perception of trustworthiness of the systems being evaluated. Currently, password authentication is the most commonly used verification scheme and users have adapted to use passwords for authentication. Although alternatives, such as graphical passwords, have been proven to be more usable, it is arguable that users may prefer to use text-based passwords from the standpoint of familiarity. Therefore, investigation of perceived trust and preferences between password systems is essential.

Acknowledgements

We would like to thank Learn to Earn, Khayelitsha Branch, for their support during the study of this project. We would also like to acknowledge the National Research Foundation (NRF) for funding this research. Thanks also to Rob Mori of Sun Microsystems for dontaing the SunSpot equipment used to capture the gestures. This work was also supported by the Telkom/NSN Centre of Excellence in Broadband Networks and their Applications.

References

1. Adams, A., Sasse, M.: Users are not the enemy. Communications of the ACM 42(12), 41–46 (1999)
2. Renaud, K.: Evaluating Authentication Mechanisms. In: Cranor, L., Garfinkel, S. (eds.) Security and Usability, pp. 103–128. O'Reilly Media, Inc., Sebastopol (2005)
3. Nelson, D.L., Reed, U.S., Walling, J.R.: Picture Superiority Effect. Journal of Experimental Psychology: Human Learning & Memory 2, 523–528 (1976)
4. Paivio, A., Csapo, K.: Picture superiority in free recall: Imagery or dual coding? Cognitive Psychology 5(2), 176–206 (1973)
5. Dhamija, R., Perrig, A.: Déjà vu: A user study using images for authentication. In: Proceedings of the 9th USENIX Security Symposium (2000)
6. Moncur, W., Leplâtre, G.: Pictures at the ATM: Exploring the usability of multiple graphical passwords. In: Proceedings of the SIGCHI conference on Human factors in computing systems, pp. 887–894. ACM Press, New York (2007)
7. Williamson, J., Murray-Smith, R., Hughes, S.: Shoogle: Excitatory multimodal interaction on mobile devices. In: Proceedings of the SIGCHI conference on Human factors in computing systems, pp. 121–124. ACM Press, New York (2007)
8. Patel, S., Pierce, J., Abowd, G.: A gesture-based authentication scheme for untrusted public Terminals. In: Proceedings of the 17th annual ACM symposium on User interface software and technology, pp. 157–160. ACM Press, New York (2004)

9. Mayrhofer, R., Gellersen, H.: Shake well before use: Authentication based on accelerometer data. In: Proceedings of the 5th International Conference on Pervasive Computing, pp. 144–161. Springer, London (2007)
10. De Luca, A., Weiss, R., Hussmann, H.: PassShape: stroke based shape passwords. In: Proceedings of the 19th Australasian conference on Computer-Human Interaction, pp. 239–240. ACM Press, New York (2007)
11. Weiss, R., De Luca, A.: PassShapes: utilizing stroke based authentication to increase password memorability. In: Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges, pp. 383–392. ACM Press, New York (2008)
12. Sharp, H., Rogers, Y., Preece, J.: Interaction Design: Beyond Human-Computer Interaction, 2nd edn. John Wiley & Sons, Chichester (2007)
13. Apple iPod Nano, `http://www.apple.com/ipodnano/`