A First Exploration of a Gesture Based Authentication Scheme for Flexible Displays

ABSTRACT

The emergence of flexible displays provides us with an opportunity to explore new forms of user authentication on mobile devices. In this paper, we present a first exploration of a bend gesture-based authentication scheme that takes advantage of users' motor learning capabilities. We ran a user study to evaluate our authentication scheme and compared the results with PINs. Our results were comparable between bend passwords and PINs. Bend passwords were stronger than PINs, though participants required more attempts to create a memorable password. Our work demonstrates that an authentication scheme using bend passwords has potential, both from a usability and security point of view.

Author Keywords

Usable Security, Authentication, Deformable User Interface

INTRODUCTION

With the emergence of flexible displays, researchers are increasingly exploring the use of bend gestures as an input technique [12, 13, 16]. As an interaction technique, bend gestures have been successfully used in the context of smartphones, e-books and maps [12, 13]. When flexible displays become mainstream handheld wireless devices, they will require a means of authenticating legitimate users. Current mobile authentication schemes have weaknesses which cause users to create insecure passwords. Text passwords and PINs are difficult to remember, leading users to resort to insecure coping strategies [3]. Pattern Lock, a touch-based authentication scheme commonly used on Android devices creates low entropy passwords [1] susceptible to smudge attacks [2]. Hence, we have an opportunity to explore new forms of authentication on flexible displays by utilizing the bend interaction modality of these devices.

In this paper, we present a first exploration of a bend gesture-based authentication scheme that takes advantage of users' motor learning capabilities. After reviewing the state of the art, we propose a user study to evaluate the usability and security of our authentication scheme on a flexible display prototype. We asked participants to create and remember bend passwords, and compared the usability and security of our system to a PIN based system on a mobile phone. From the results of our user study we present insights and guidelines for the design of bend passwords.

RELATED WORK

We review prior work in the areas of flexible displays, specifically bend gestures interaction techniques, and in the area of usable security, with authentication methods using novel inputs.

Flexible Displays and Bend Gestures: Flexible display devices allow users to interact with the device by deforming its surface to trigger a command [13]. Two research groups have used functional flexible displays augmented with sensors to study deformable interaction techniques. Lahey et al. [13] created PaperPhone, a flexible smartphone using an electrophoretic display. In their study, participants defined bend gestures and associated them with functionalities. They proposed a basic classification scheme, categorizing the gestures by location (top corner, side, or bottom corner) and their direction (towards the user, often referred to as up, and away from the user, otherwise known as down). In turn, Kildal et al. [12] developed the Kinetic device, a deformable mobile phone using an OLED display. They used this device to explore bending and twisting, and proposed a set of design guidelines for deformable devices.

Usable Authentication: New technologies allow researchers to experiment with novel forms of user authentication that utilize previously unavailable modalities. Of particular interest here are authentication schemes that use the tactile and fine-motor skills of users. A first category includes schemes that use specialized hardware. Haptic Wheel [6] and the Secure Haptic Keypad [5] use custom hardware to produce a series of vibrotactile cues not apparent to a casual observer. Users enter their tangible password by pressing keys or rotating a dial in response to the challenge produced by randomized vibrotactile cues. Mott et al. [15] developed TangibleRubik, an authentication mechanism that requires users to physically manipulate a Rubik's Cube to authenticate. TangibleRubik takes advantage of the human ability to memorize repeated motor actions.

Behavioural biometrics such as signature-recognition [10], speech recognition [10], or keystroke dynamics [4] aim to authenticate users by matching observed behavioural characteristics to a previously stored model, balancing between accommodating for natural variances while distinguishing intruders trying to mimic the behaviour. Several gesture-based schemes for mobile devices have also been proposed recently. In GesturePIN [7], gestures are performed by moving the mobile device in 3D space. The Android screen unlock allows users to authenticate by drawing a pattern using a series of dots on a touchscreen. To the best of our knowledge, however, there has not been any work investigating authentication schemes on flexible display devices.

PROTOTYPES

We developed two prototypes, a flexible display prototype for creating gesture-based passwords (Figure 1) and a mobile phone prototype for creating PINs.

GRAND 2014, May 14-16, 2014, Ottawa, ON, Canada.

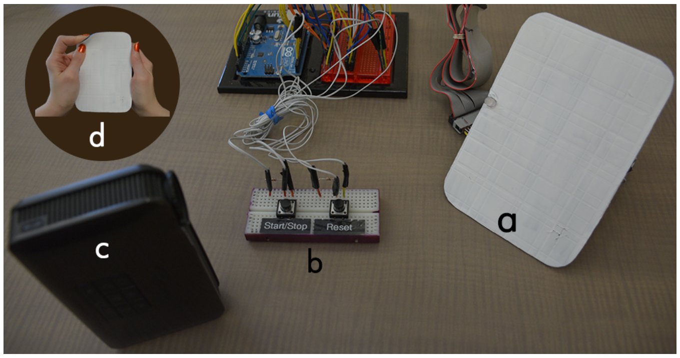

Figure 1. Flexible Display Prototype: (a) Flexible Display (b) Control Panel (c) Projector (d) A bend gesture performed on the display

Our flexible display prototype is composed of a flexible PVC with the dimensions of 135 x 95 x 1.5 mm. Four 2” Flexpoint bidirectional bend sensors are placed in the top-left corner, top-right corner, bottom-left corner and bottom-right corner of the display. The display is connected to an Arduino Uno Microcontroller which is connected to a computer. A user interface is projected onto the display via a pico-projector. When a gesture is entered, an asterisk appears in the standard password entry field of the UI, the projector emits a clicking sound, and the LED light changes color. Designed to control the authentication process on the flexible prototype, the control panel is composed of two buttons: one to start and stop the password input, and the second to reset the password in case of errors.

The mobile phone prototype was a commercial Samsung Galaxy SIII (I9300) Android phone. We designed an Android application to match the UI of the flexible display prototype.

Bend Gesture Authentication Scheme

Passwords on the flexible display are created by performing a series of bend gestures. Warren et al. [17] proposed a classification scheme for bend gestures which includes the location of the bend, its direction, the distance to the corner (size of bent area), the angle of the bend, the edge on which the bend is performed, and the speed and duration of the bend. We chose to use the two more popular bend characteristics, location and direction [13, 17], to classify the gestures in our system. A total of 20 gestures are available in our authentication scheme: each corner of the display could be bent up or down (8 gestures) and pairs of corners could be bent up or down simultaneously (12 gestures). When a corner is bent up or down it is referred to as “single bend gesture” and when pairs of corners are bent together it is referred to as a “multi bend gesture”.

USER STUDY

We conducted a university ethics approved two part user study to evaluate the usability of our bend gesture authentication scheme, in comparison to a PIN based scheme. In the first part, participants created a password on a flexible device and a PIN on a mobile phone. Participants returned to the lab one week later for the second part to re-enter their passwords.

Session 1: In the first session, we presented participants with one of the prototypes and gave them a demonstration of how to create a password. Participants were provided with the opportunity to familiarize themselves with the prototype and its authentication scheme. After training, participants created either a bend password on the flexible display or a PIN on the mobile phone. The theoretical password spaces [1] of PINs and bend passwords were set as closely as possible and met the recommended minimum of 20 bits [8]. Bend passwords had a minimum of 5 gestures (theoretical password space of 21.6 bits) and PINs had 6 digits (theoretical password space of 19.9 bits). Participants were asked to create a new PIN rather than reuse an existing one; reuse was not possible with bend passwords because participants had no previous experience with the system.

After creating a password, participants successfully confirmed it three times and completed several questionnaires providing their opinions and perceptions of the prototype. Next, they rehearsed their password five times by successfully re-entering it in the system. If participants forgot their password at any stage (confirm or rehearsal), they could create a new password but would have to repeat the confirmation stage. Once this procedure was completed, participants were presented with the second device, where they followed the same protocol. Order of presentation was counter-balanced to reduce learning effects. Participants were told they would have to re-enter their password during the second session.

Session 2: Approximately one week later, participants returned to the lab to re-enter their passwords. Participants had five tries to correctly re-enter their password on each prototype. After completing these tasks, participants completed several post-task questionnaires providing their perceptions and feedback for each prototype.

Participants

25 participants (12 female) with an average age of 24.6 years completed the study. Nineteen owned at least one smart phone and fourteen had a screen lock enabled on their phone. Of these, thirteen used an authentication mechanism (9 PIN and 5 graphical/pattern) to unlock their phone at least four times per day. Three participants had completed another bend gesture study within the last year, the remainder had no previous experience with flexible displays. Participants were given $15 compensation for completing both sessions.

RESULTS

We analysed data from both sessions. We evaluated the passwords created, password strength and login success rates. Our analysis was done on the final password created by participants.

Strength: The strength of a password (bend or PIN) is determined by its length and available digit/gesture set (10 digits or 20 gestures). Password strength is also affected by the number of unique characters or gestures it contains. Table 1 shows the mean length, the number of unique entries (gestures or digits) and the entropy of bend passwords and PINs.

[1] the total number of password combinations possible for a given configuration, usually reported in base-2 or bits.

Table 1. Password Characteristics. Bold indicates significance.

Pwd Type	Length *M* (*SD*)	**Entropy *** *M* (*SD*)	Unique Gestures/Digits *M* (*SD*)
PIN	7.08 (1.29)	23.52 (4.28)	5.08 (1.15)
Bend	6.64 (2.38)	28.70 (10.28)	5.08 (1.63)

Table 2. Ease of remembering passwords. Bold indicates significance.

Pwd Type	**Session 1 *** *Md* (*SD*)	Session 2 *Md* (*SD*)
PIN *	10 (1.31)	9 (3.19)
Flexible	8 (2.25)	9 (2.99)

We used Wilcoxon signed-rank tests to look at the differences between the strength, length and number of unique gestures/digits of bend passwords and PINs. We found that bend passwords had a significantly higher bit entropy than PINs (Z = -2.846, p = 0.004). No difference was found between the length (Z = -1.883, p = 0.060) or number of unique gestures/digits (Z = -.327, p = 0.744) of PINs and bend passwords.

Bend Gestures Selection: Each bend gesture was used at least once (i.e., by at least one participant in one password). However, some gestures were used more than others. The top four most frequently used gestures were the top-right-corner-up (19%), the top-left-corner-up (13%), the top-side-up (8%), and the bottom-left-corner-up (7%). Participants used more single bend gestures (63%) than multi bend gestures (37%). These results are consistent with the findings of Lahey et al. [13] and Warren et al. [17].

Password Creation Strategies: Participants used a variety of strategies to create their secure and memorable bend password. Commonly used strategies include the following:

- Clockwise: Bending the corners of the display up or down consecutively in a clockwise manner.
- All on One Side: Performing all gestures on one side of the display using a specific pattern.
- Number Mapping: Assigning numbers to each gesture and using the numbers to create a bend password.
- Drawing: Using the gestures to “draw” a letter (e.g., A), symbol (e.g., sigma) or mental picture (e.g., a five point star) on the display.

The Number Mapping and Drawing strategies are the most secure because the mapping or drawing is internal to participants. The Drawing strategy produces the longest passwords. For PINs, participants used parts of an existing PIN or created a PIN using their personal information, such as birth date, phone number or student ID.

Log-in Success Rate: Out of 25 participants, 21 completed the second session. We evaluated the login success rate by assessing whether participants were able to enter their password correctly in any of the 5 tries. The success rate of PIN passwords was 86%, and that of bend passwords was 81%. A McNemar test with the continuity correction found no difference between the success rates (χ^2(1, N = 15) = 0.00, p = 1.00, the odds ratio is 0.67).

Questionnaire Responses

In both sessions, we asked users to complete questionnaires. We grouped the Likert scale questions into three categories: password preference, memorability and shoulder surfing. All statistical analysis are done using a Wilcoxon signed-rank test.

Password Preference: At the end of session 2, we asked participants *Would you use a bend password if it was available* on a 10-point Likert scale (1 = never and 10 = definitely). Participants were slightly positive on whether they would use a bend password (M = 6, SD = 3.06).

Memorability: At the end of both sessions, we used a 10-point Likert scale (1 = very difficult and 10 = very easy) to ask participants how easy it was for them to remember their new password (PIN and Bend). Table 2 shows participants’ responses.

We used the Bonferroni adjusted alpha levels of .0125 (.05/4) to compare the results of this question across session 1 and session 2 for PIN and bend passwords. At the end of session 1, participants found it easier to remember their PINs than bend passwords (Z = -2.927, p = 0.001). However, no such difference was found at the end of session 2 (Z = -.134, p = 0.223). Participants found it more difficult to remember their PIN in the second session that the first (Z = -2.216, p = 0.007).

Shoulder Surfing: At the end of session 1, we used a 10-point Likert scale (1 = very difficult and 10 = very easy) to ask participants how easily someone could shoulder surf their bend password or PIN. Participants thought both their PINs (Md = 3, SD = 2.13) and bend passwords (Md = 4, SD = 2.94) would be difficult to shoulder surf. There was no difference between the rated difficulty of shoulder surfing PINs and bend passwords (Z = -1.763, p = 0.078).

User Feedback

Overall, users liked bend passwords and stated they would used them on a flexible display device if available. Specifically, they would use them to unlock a phone, or a system with low-security. Users found the system user friendly, easy to use, and enjoyed the its novelty. One said that it was “accessible to even new users” and another stated that it was a “promising password entry technique”. Others stated they would not use bend passwords at the moment because they do not have adequate mental strategies to create such passwords. However, many stated that with more practice they would be able to use them in the future. For instance, one user said “that it is a new technology was a definite hurdle, but with familiarity I believe it will be easy to learn and the gestures are fairly simple”.

DISCUSSION

Participants showed interest in a bend gesture based authentication scheme. They were able to successfully create and remember a bend password with very little training and experience with our system. Our results show comparable results between bend passwords and PINs (the most common form of authentication on mobile devices). We found no significant difference between password memorability, however bend passwords were stronger than PINs.

Some participants were able to form fairly secure bend password creation strategies with very little training. Most participants created PINs that used parts of an existing PIN or their personal information, while they created new bend passwords. Thus, it is expected that they would remember their PINs well and would prefer to use them over bend passwords. We believe that if participants had created a new PIN for the study, their memorability and user opinion of PINs would have been lower.

We believe that when flexible displays become mainstream and user expertise improves, users would develop better bend password creation strategies which will lead to stronger and memorable passwords. However, malicious users will also develop better strategies for compromising bend passwords. Thus, we have a unique opportunity to explore the different security threats to a bend gesture authentication scheme and develop solutions to protect users from such threats. Since, currently users do not have any strategies for creating bend passwords, we can develop strategies that create secure and memorable passwords, and train users on these strategies.

CONCLUSION AND FUTURE WORK

In this paper, we presented a new password scheme for authenticating users on flexible display devices using bend gestures. We implemented this scheme on a flexible prototype and ran a two part user study to evaluate its usability and security in comparison with PINs on a mobile phone. In the first part, participants created, confirmed and rehearsed a bend password and PIN. In the second part, which took place a week later, participants re-entered their passwords from the first part. Participants showed interest in bend passwords and we found comparable results between bend passwords and PINs. Considering participants' familiarity with PINs, our work demonstrates that an authentication scheme using bend passwords has potential, both from a usability and security point of view, and warrants further exploration.

The visible physicality of bend gestures may make bend passwords susceptible to shoulder surfing attacks. We are currently looking at the shoulder surfing susceptibility of these passwords and comparing the results with PINs. A common problem with user assigned passwords (bend and PIN) is that users' tend to create weak passwords. We are also investigating system assigned bend passwords compared to system assigned PINs. We will also compare bend passwords with other gesture based passwords, such as touch gestures or 3D gestures. The bend gesture language could be improved to provide even stronger passwords to users. This could be accomplished by recording a higher number of bend gesture characteristics, such as the timing of each gesture, as well as a more detailed gesture magnitude.

REFERENCES

1. http://beust.com/weblog2/archives/000497.html.
2. http://techcrunch.com/2008/10/12/androids-login-is-cool-but-is-it-secure.
3. Adams, A., and Sasse, M. A. Users are not the enemy. *Commun. ACM 42*, 12 (1999), 40–46.
4. Bergadano, F., Gunetti, D., and Picardi, C. User authentication through keystroke dynamics. *ACM Trans. Inf. Syst. Secur. 5*, 4 (2002), 367–397.
5. Bianchi, A., Oakley, I., and Kwon, D. S. The secure haptic keypad: A tactile password system. In *Proc. CHI* (2010), 1089–1092.
6. Bianchi, A., Oakley, I., Lee, J. K., and Kwon, D. S. The haptic wheel: Design and evaluation of a tactile password system. In *Proc. CHI EA* (2010), 625–630.
7. Chong, M. K., Marsden, G., and Gellersen, H. Gesturepin: Using discrete gestures for associating mobile devices. In *Proc. MobileHCI* (2010), 261–264.
8. Florêncio, D., and Herley, C. Where do security policies come from? In *Proc. SOUPS* (2010), 10:1–10:14.
9. Herkenrath, G., Karrer, T., and Borchers, J. Twend: Twisting and Bending as new Interaction Gesture in Mobile Devices. *Proc. CHI* (2008), 3819–3824.
10. Jain, A., Hong, L., and Pankanti, S. Biometric identification. *Commun. ACM 43*, 2 (2000), 90–98.
11. Kildal, J., Lucero, A., and Boberg, M. Twisting Touch : Combining Deformation and Touch as Input within the Same Interaction Cycle on Handheld Devices. In *Proc. MobileHCI* (2013).
12. Kildal, J., Paasovaara, S., and Aaltonen, V. Kinetic Device : Designing Interactions with a Deformable Mobile Interface. In *Proc. CHI EA* (2012), 1871–1876.
13. Lahey, B., Girouard, A., Burleson, W., and Vertegaal, R. PaperPhone: Understanding the Use of Bend Gestures in Mobile Devices with Flexible Electronic Paper Displays. In *Proc. CHI* (2011), 1303–1312.
14. Lee, S.-S., Kim, S., Jin, B., Choi, E., Kim, B., Jia, X., Kim, D., and Lee, K.-p. How users manipulate deformable displays as input devices. *Proc. CHI* (2010), 1647–1656.
15. Mott, M., Donahue, T., Poor, G. M., and Leventhal, L. Leveraging motor learning for a tangible password system. In *CHI EA* (2012), 2597–2602.
16. Schwesig, C., Poupyrev, I., and Mori, E. Gummi: a bendable computer. In *Proc. CHI* (2004), 263 – 270.
17. Warren, K., Lo, J., Vadgama, V., and Girouard, A. Bending the rules: bend gesture classification for flexible displays. In *Proc. CHI* (2013).