POSTER: Passwords on Flexible Display Devices

Sana Maqsood, Sonia Chiasson, Audrey Girouard
Carleton University, Ottawa, Canada
{sana.maqsood, audrey.girouard}@carleton.ca, chiasson@scs.carleton.ca

ABSTRACT

Flexible display devices allow users to interact with the device by deforming the surface of the display to trigger a command. When these devices become mainstream, for example as smart phones, e-readers, or tablets, they will require a means of authenticating legitimate users. In this poster, we present an authentication scheme for flexible display devices, its implementation on a flexible display prototype and an ongoing user study evaluating the usability and security of our system.

Categories and Subject Descriptors

H.5.2 [**Interfaces and Representation**]: User Interfaces—*Input devices and strategies*

Keywords

Usable Security, Flexible Displays, Authentication

1. INTRODUCTION

Flexible display devices allow users to interact with the device by deforming the surface of the display to trigger a command. Application areas for flexible display devices include gaming, control of media and home appliances, and smart phones [4]. While these devices are currently not available to consumers, several prototypes have been developed to explore their interaction modalities. Lahey et al. created PaperPhone, a flexible display smart phone [5]. In their user studies, participants defined bend gestures and associated them with functionalities. Based on the results from their user studies, Lahey et al. proposed a classification scheme that categorized bend gestures by location (top corner, side, or bottom corner) and their polarity (up or down). Kildal et al. developed the Kinetic device, a deformable mobile phone [4]. They used this device to explore bending and twisting, and proposed a set of design guidelines for deformable devices [4]. When flexible display devices become mainstream, for example as smart phones, as e-readers, or tablets, they will require a means of authenticating legitimate users. In this poster, we present an authentication scheme for flexible display devices that takes advantage of users' motor learning capabilities. We also show the implementation of our authentication scheme on a flexible display prototype. To the best of our knowledge, there has not been any work investigating authentication schemes on flexible display devices. Our main contributions are as follows:

- We designed and implemented an authentication scheme on a flexible display prototype.
- We are conducting a user study to evaluate the usability and security of our authentication scheme and flexible display prototype. We are also comparing the usability and security of our system with a PIN based password system.

2. RELATED WORK

While no work has looked at authentication mechanisms on flexible display devices, some work explores the creation of passwords utilizing the motor learning capabilities of users. Bianchi et al. developed the Haptic Wheel [2] and the Secure Haptic Keypad [1]. Passwords in these systems use a series of vibrotactile cues called tactons. Users authenticate on these systems by placing their finger on one of three keys (Haptic Keypad) or their hand around a rotary dial (Haptic Wheel). After each input, the system randomizes the vibrations it emits to protect the system from shoulder surfing. Chong et al. [3] developed GesturePIN, a mobile authentication system that allows users to create a PIN by performing a series of gestures on their mobile device. Gestures are performed by moving the mobile device in 3D (three dimensional) space, and users can perform a total of 10 gestures. Mott et al. [6] developed TangibleRubik, an authentication mechanism that requires users to physically manipulate a Rubik's Cube to authenticate a system. The various combinations of moves act as the users' password. By having users physically manipulate the cube, the system takes advantage of humans' innate ability to recall motor actions through repetition. Mott et al. conducted a user study to evaluate the usability and security of their system. Participants completed a training session requiring them to successfully enter their password three times before moving on to the experimental trials. Textual representations of the passwords were visible to the user at all times during the training trials. This was done to aid in the learning of the password. In the experimental trials, which directly followed training, participants had to correctly enter their password five times.

CCS'13, November 4–8, 2013, Berlin, Germany.
ACM 978-1-4503-2477-9/13/11.
http://dx.doi.org/10.1145/2508859.2512528.

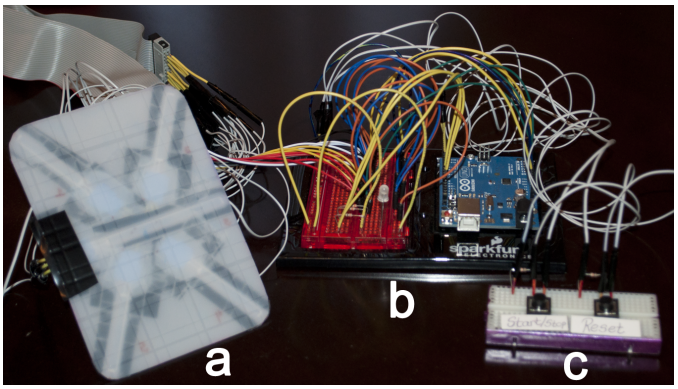

Figure 1: (a) Flexible Display, (b) Arduino Uno Microcontroller, (c) Control Panel.

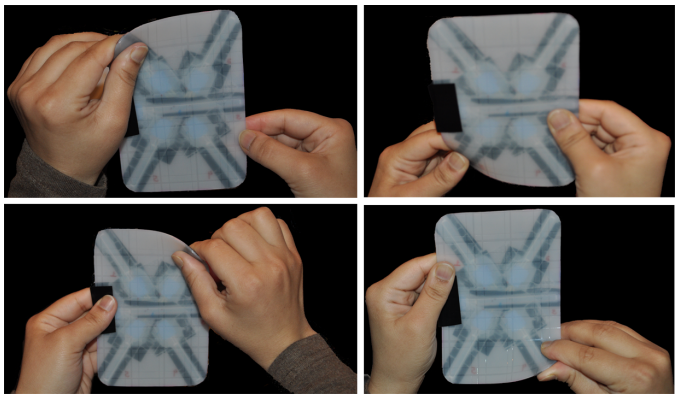

Figure 2: Four bend gestures performed on the flexible display.

After the experimental trials, participants were given a distractor task for a duration of 10 minutes, which consisted of a word search. After the distractor task, participants were asked to enter their password a final time as a test of password mastery. Mott et al. found that participants were able to effectively recall 7 and 10 gesture passwords after being removed from the system for a short time.

3. PROTOTYPES

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

3.1 Flexible Display

Our flexible display prototype is composed of four main components: flexible display, pico projector, Arduino Uno Microcontroller and a control panel. Three of these components are shown in Figure 1. The flexible display was created from a soft PVC and has four 2" Flexpoint bidirectional bend sensors attached to its back. These sensors are placed in the top-left corner, top-right corner, bottom-left corner and bottom-right corner of the display. The pico projector is used to display a UI onto the flexible display, and the control panel is used to start/stop the authentication process on the flexible display. The flexible display and the control panel are connected to an Arduino Uno Microcontroller which is connected to a computer running the software for creating a gesture based password.

3.1.1 Creating a Password

Passwords on the flexible display are created by performing a series of bend gestures. A set of 20 bend gestures are available. Each corner of the display can be bent upwards and downwards (8 gestures). Every two corners of the display can be bent upwards and downwards simultaneously (12 gestures). Figure 2 shows how some of these gestures can be performed. A standard password entry field is projected onto the display, with an asterisk appearing with each gesture (see Figure 3). Gesture passwords must have a minimum of 5 gestures (21.6 bits).

3.2 Mobile Phone

The mobile phone prototype was developed using Android and allows users to create a PIN. The UI of this prototype

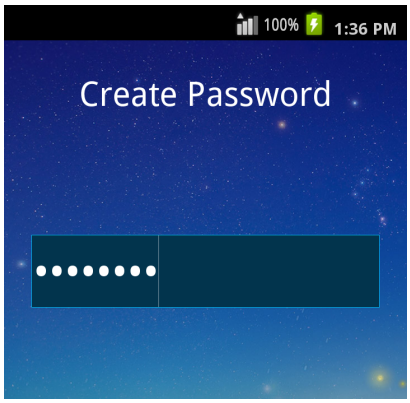

Figure 3: User Interface of the Flexible and mobile phone prototype.

was designed to match the UI of the flexible display prototype (see Figure 3). PINs must be at least 6 characters long (19.9 bits).

4. USER STUDY

We are currently running a user study to evaluate the usability and security of our proposed authentication mechanism. Participants are tested in two sessions. In the first session participants are asked to create a gesture based password on the flexible display prototype and a PIN based password on the mobile phone prototype. These prototypes are presented in a counterbalanced manner. Before creating a password, participants are given a demonstration of how the prototype works and are provided with an opportunity to familiarize themselves with its functions. After creating a password on each prototype, participants are asked to complete several post-task questionnaires providing their opinions and perceptions of the prototypes. After completing the questionnaires, participants are asked to correctly re-enter their password on each prototype five times. This allows participants to rehearse their passwords which aids in memorization.

The second session takes place a week later and evaluates the memorability of the passwords created in the first session. Participants are asked to correctly re-enter their passwords. Participants are given five tries to correctly re-

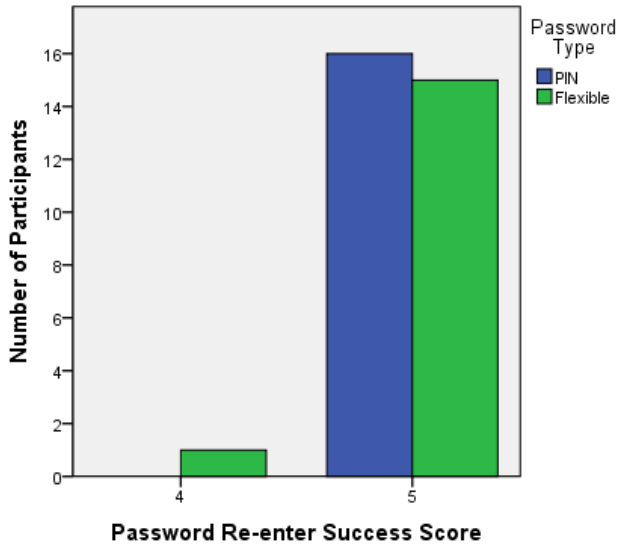

Figure 4: Day 1 Password Re-entry Success Scores (out of 5 tries) on the Flexible Display and Mobile Phone.

enter their passwords on each prototype. After completing the password re-entry tasks, participants complete several post-task questionnaires evaluating the memorability and security of their passwords.

Quantitative data collected includes the time participants took to complete each task, number of errors they made, passwords they created, strength of the passwords, number of tries taken to authenticate, and whether they were able to remember their passwords. Qualitative data is collected via post-task questionnaires.

4.1 Preliminary Results - Day 1

16 university students between the ages of 18 and 28 ($M = 22$, $SD = 3.42$) participated in the first session of our study. We analysed the time they took to re-enter their password averaged across five tries. We found that participants took longer to re-enter their password on the flexible display ($M = 31.2$s, $SD = 18.08$) than the mobile phone ($M = 7.2$s, $SD = 3.42$). One reason for the longer times is that participants were using an early prototype of a new technology which required careful handling. In addition to this, participants created new passwords on the flexible display, but post-task questionnaire data revealed that many created a known and familiar PIN on the mobile phone despite being asked to create something new. Therefore, participants had much more practice re-entering their PIN and could re-enter it faster than their password on the flexible display.

Success scores on the password re-entry task were calculated by giving participants a score out of 5, depending on the number of times they successfully re-entered their password. Figure 4 shows that most participants were able to successfully re-enter their password in both conditions.

Data from the post-task questionnaires revealed that overall participants had a positive experience in using the flexible display prototype to create a password. Some of their comments include "It's very cool!", "The flexible device is user friendly and will be easy device to use", "There were various combinations that could be made, allowing for variety. The device itself was pleasant to use, and bending it was very easy once you became accustomed to it", "That it is new technology was a definite hurdle, but with familiarity I believe it will be easy to learn and the gestures are fairly simple" and "At first, I had difficulty with mastering my intended password but after getting assistance, I determined the problem I made and was able to register my password successfully."

Further analysis of the data from both sessions is ongoing.

5. CONCLUSION AND FUTURE WORK

In this paper, we presented a password scheme for authenticating users on flexible display devices. We implemented this password scheme on a flexible display prototype and are running a user study to evaluate the usability and security of our system. Preliminary results from the first session of our study show that many users were able to easily create and re-enter their passwords, although they took longer to re-enter their gesture password than their PIN. This was mainly because users were using an early prototype of a flexible display which required careful handling. We believe that as flexible display prototypes improve in the future, password re-entry time will improve as well. Our future work will look at data from both sessions of the study. We will look at the security and memorability of passwords created on the flexible display as well as strategies and gestural patterns users employ to create their passwords.

6. REFERENCES

[1] A. Bianchi, I. Oakley, and D. S. Kwon. The secure haptic keypad: A tactile password system. In *CHI*, pages 1089–1092, 2010.

[2] A. Bianchi, I. Oakley, J. K. Lee, and D. S. Kwon. The haptic wheel: Design and evaluation of a tactile password system. In *CHI EA*, pages 625–630, 2010.

[3] M. K. Chong, G. Marsden, and H. Gellersen. Gesturepin: Using discrete gestures for associating mobile devices. In *MobileHCI*, pages 261–264, 2010.

[4] J. Kildal, S. Paasovaara, and V. Aaltonen. Kinetic device: Designing interactions with a deformable mobile interface. In *CHI EA*, pages 1871–1876, 2012.

[5] B. Lahey, A. Girouard, W. Burleson, and R. Vertegaal. Paperphone: Understanding the use of bend gestures in mobile devices with flexible electronic paper displays. In *CHI*, pages 1303–1312, 2011.

[6] M. Mott, T. Donahue, G. M. Poor, and L. Leventhal. Leveraging motor learning for a tangible password system. In *CHI EA*, pages 2597–2602, 2012.