BEND PASSWORDS: USING GESTURES TO AUTHENTICATE ON FLEXIBLE DEVICES

by
Sana Maqsood

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF COMPUTER SCIENCE

Human Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
May, 2014

Abstract

Upcoming mobile devices will have flexible displays, allowing us to explore new forms of user authentication. On flexible displays, users interact with the device by deforming the surface of the display through bending. In this thesis, we present a new type of user authentication that uses bend gestures as its input modality.

We ran three user studies to evaluate the usability and security of our new authentication scheme and compared it to PINs on a mobile phone. Our first two studies evaluated the creation and memorability of bend passwords and PINs. The third study looked at the security problem of shoulder-surfing passwords on mobile devices.

Our results show that bend passwords are a promising authentication mechanism for flexible display devices. We also provide eight design recommendations for implementing bend passwords on flexible display devices, based on our results.

Acknowledgements

First, I would like to thank my supervisor Sonia Chiasson for her advice, feedback and support throughout this thesis. Sonia, I admire your dedication to your students. You are not only a great supervisor but also a great mentor. Thank you for the informal chats and advice about graduate school and academia. I am grateful to have worked with you for the last two years.

I would also like to thank my co-supervisor Audrey Girouard for her help and guidance throughout this thesis. Thanks for introducing me to the world of physical computing, Arduino, prototyping, and soldering. Thanks for your patience and feedback.

Thanks to the members of my committee Robert Biddle, Lois Frankel and Chris Joslin for their time and feedback.

I would like to thank NSERC ISSNet for funding this research, which allowed me to attend conferences and receive valuable feedback on my work from researchers in the community.

Last but not least, I would like to thank my sister Sumbal for listening to me talk about my thesis and graduate school even though she had not begun her grad studies. I will gladly play this role as you go through your studies.

Finally, thanks to my family and friends for their support and encouragement.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

Upcoming mobile devices will include flexible displays and many companies have announced release dates in the near future [2]. In these devices, users interact with the device by deforming (i.e., bending) the surface of the display. These devices have a number of advantages over current rigid mobile devices, such as being lightweight and power efficient. Many researchers have explored using bend gestures as an input technique on flexible display devices [21, 23, 32]. Bend gestures have been used successfully in the context of smartphones, e-books and maps [21, 23, 32, 39, 41]. The success of bend gestures is largely explained by the inherent tactile feedback provided by the display when a bend gesture is performed. Bend gestures can be discrete or continuous, with a large number of degrees of freedom, such as the angle of the bend, the speed of the bend, the distance to the corner, and the location of the bend [38].

Current rigid mobile devices have many authentication schemes that can be used to protect the data on these devices. Users can use PINs, text passwords, or gesture-based passwords to authenticate on these devices. However, all of these authentication mechanisms have weaknesses that lead to insecure passwords. Text passwords and PINs are difficult to remember, which makes users' resort to insecure coping strategies [3]. Pattern Lock, a gesture-based authentication scheme commonly used on Android devices, leads to low entropy passwords [1] that are susceptible to smudge attacks [4]. Biometric authentication systems have high false rejection rates and stolen passwords are difficult to replace. New interaction modalities, such as bend gestures on flexible displays, provide us with an opportunity to explore new forms of user authentication on mobile devices.

1.2 Research Question

Our main research question explores this opportunity:

1. Can bend gestures be used to develop a secure and usable authentication scheme on flexible display devices?

We will address our research question by developing a bend-gesture authentication scheme, and implementing it on a custom-built flexible display prototype. After developing our prototypes, we will conduct user studies to evaluate the usability and security of our authentication scheme, and compare the results with PINs (a common authentication mechanism on mobile devices).

1.3 Contributions

The main contributions of this thesis are enumerated and explained below:

1. A bend-gesture authentication scheme for flexible display devices.

2. Empirical evaluation of the usability and security of our bend-gesture authentication scheme compared to PINs. We assess the usability and memorability of both user chosen and system assigned passwords, as well as the shoulder-surfing susceptibility of passwords.

3. Preliminary design recommendations for bend password authentication on flexible displays.

1.3.1 A bend-gesture based authentication scheme for flexible display devices

We designed a new authentication scheme utilizing the bend-gesture interaction modality of flexible displays. As flexible displays are not commercially available and we did not have access to working prototypes, we developed a flexible display prototype. We implemented our gesture-based authentication scheme on this prototype.

1.3.2 Empirical evaluation of the usability and security of our bend-gesture authentication scheme compared to PINs

We conducted three user studies to evaluate the usability and security of our authentication scheme compared to PINs. Users performed various password tasks on our prototype, and we used quantitative and qualitative methods to analyse their task performance and perceptions of our authentication scheme.

The following summarizes our user studies:

- User chosen password study — Two week study with 25 participants
- System assigned password study — Two week study with 21 participants
- Shoulder-surfing susceptibility study — One session study with 9 participants

1.3.3 Preliminary design recommendations for bend password authentication on flexible displays

Using insight gained from our studies, we present eight design recommendations for bend authentication on flexible displays.

1.4 Thesis Outline

This thesis is organized into eight chapters. In Chapter 2, we provide a literature review of flexible displays and usable authentication, with a focus on gesture-based authentication schemes. In Chapter 3, we present the design and development of our flexible display prototype and a mobile phone prototype. The mobile phone prototype was implemented on a commercially available Android device, and was used to evaluate the comparison PIN condition in our user studies. In this chapter, we also present the design of our bend-gesture based authentication scheme. In Chapter 4, we present the user study evaluating the usability and security of user chosen bend passwords and PINs. In Chapter 5, we present a user study to evaluate the usability of system-assigned bend passwords and PINs. In Chapter 6, we compare the findings from our user chosen and system-assigned user studies. In Chapter 7, we present a user study evaluating the shoulder-surfing susceptibility of bend passwords and PINs.

Finally in Chapter 8, we present a discussion of the results from our three user studies, and set of preliminary guidelines for creating secure bend passwords. In this section, we also present the conclusion of the thesis and our future work.

1.5 Associated Publications

Portions of this work have already led to the following publications:

1. S. Maqsood. Shoulder Surfing Susceptibility of Bend Passwords (2014). ACM SIGCHI Conference on Human Factors in Computing Systems (CHI) Student Research Competition (SRC) (6-page paper in ACM Digital Library, poster).

2. S. Maqsood, S. Chiasson, A. Girouard (2014). A First Exploration of a Gesture Based Authentication Scheme for Flexible Displays. GRAND NCE Annual Conference (4 page paper).

3. S.Maqsood, S. Chiasson, A. Girouard (2013). Passwords on Flexible Display Devices. ACM CCS Poster (3-page paper in ACM Digital Library, poster).

Chapter 2

Background

Before developing a bend gesture authentication scheme, we review prior work on bend gesture interaction techniques for flexible displays, and authentication methods using novel inputs in the area of usable security.

2.1 Flexible Displays and Bend Gestures

Users interact with flexible display devices by deforming the surface of the device to trigger a command [23]. Application areas for flexible display devices include gaming [43], control of media and home appliances [21, 23], e-readers [23, 39, 41], maps [11, 23, 32], and smart phones [21, 23].

Schwesig et al. [32] pioneered the concept of a flexible device which used bending the device as an input and interaction technique. They tested their concept with a rigid screen where they affixed a flexible substrate with bend and touch sensors. The authors demonstrated that users could easily understand deformation as a basic interaction technique.

Two research groups have used functional flexible displays augmented with sensors to study deformable interaction techniques. Lahey et al. [23] created PaperPhone, a flexible smartphone using an electrophoretic display. In their study, participants defined bend gestures and associated them with functionalities. The authors 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. [21] 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.

Other researchers have created flexible prototypes without a functional screen to

evaluate their interaction techniques, because access to flexible technologies is currently limited. While Lee et al. [24] presented completely non-functional prototypes to participants, most researchers embed or affix sensors to a flexible plastic substrate, and use either an external screen [20] or projection [34, 39, 43] to present a graphical interface to the user. We followed their prototyping recommendations to build our own flexible prototype.

2.2 Usable Authentication

The importance of usable authentication was first highlighted by Saltzer and Schroeder [29] in 1975. Nearly four decades later, text passwords remain popular despite their inadequacies [3, 42] because no universally viable alternative has emerged. A different approach may be to target types of authentication for different usages. 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.

2.2.1 Tangible and Haptic Authentication

A first category includes schemes that use specialized hardware. Haptic Wheel [9] and the Secure Haptic Keypad [8] use custom hardware to produce a series of vibrotactile cues not apparent to a casual observer. These systems were designed for authentication in public spaces, such as entering PINs in an ATM. Users enter their tangible password by pressing keys or rotating a dial in response to the challenge produced by randomized vibrotactile cues. The primary advantage of these systems is that they are resistant to observation attacks such as shoulder-surfing [1] because shoulder-surfers are unable to observe the haptic feedback produced by the system. In addition, the system also randomizes the location of the vibrotactile cues on the Haptic Wheel and Keypad, making it difficult for shoulder-surfers to steal passwords by observing their entry on the Keypad or Wheel. However, password entry on these systems takes considerably more time than traditional authentication mechanisms,

[1] Shoulder-surfing is an attack where malicious users learn a password by observing its entry on the device. These attacks are common in public places such as bus stops and coffee shops.

such as PINs and text passwords.

Mott et al. [27] developed TangibleRubik, an authentication mechanism that takes advantage of the human ability to memorize repeated motor actions. In this system, users authenticate by performing a series of rotations on a tangible Rubik's Cube. In a user study, participants were assigned a 7 or 10-move password and learned the passwords by re-entering them consecutively multiple times. After a short distractor task (10 minutes), participants re-entered their password once in the system. Results from the study showed that participants made a large number of errors in the learning stage, but successfully remembered their passwords after the distractor task. However, participants took considerably more time to enter their passwords compared to traditional authentication mechanisms. While this work showed the application of a tangible authentication scheme, several issues need to be addressed before such a system can be used. These include evaluating participants' long-term memorability of tangible passwords, evaluating the shoulder-surfing susceptibility of these passwords, and comparing them with existing authentication schemes.

2.2.2 Biometric and Gesture-based Authentication

Behavioural biometrics such as signature-recognition [19], speech recognition [19], or keystroke dynamics [7] 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. However, a common problem with biometric authentication systems is that they have high false rejection rates. Also, it is very difficult to assign a new password if a user's biometric password is stolen. Users also cannot use different passwords for different applications and contexts.

Several gesture-based schemes for mobile devices have been proposed recently. GesturePIN [12] is a device authentication mechanism for connecting two or more mobile devices together. In this scheme, passwords are created by moving the mobile device in 3D space to perform a series of gestures. GesturePIN has the same theoretical password space as numerical PINs, but a user study found that it has longer entry times and less accuracy than PINs. In addition, it is also very susceptible to

shoulder-surfing attacks because the 3D gestures can easily be observed by malicious users.

A related mobile authentication system which has seen wide deployment is the Android screen unlock, where users authenticate by drawing a graphical pattern on a touch-screen. Passwords in this scheme are recognized by the series of dots touched rather than by biometric measures, but the system still makes use of users' fine motor skills. Zezschwitz et al. [37] conducted a longitudinal field study (spanning three weeks) to evaluate the usability and security of the Android screen unlock and compared the results with PINs. They found that users took more time and made more errors when entering their pattern passwords, but preferred them over PINs. Despite their likeability, pattern passwords are not very secure and are vulnerable to shoulder-surfing [13, 35] and "smudge" attacks [5]. In smudge attacks, passwords are stolen by observing the smudge stains left on the display by the user's fingers. In addition to this, pattern passwords have a small password space which means that attackers could guess the password after stealing the mobile device.

To the best of our knowledge, there has not been any work investigating authentication schemes on flexible display devices.

2.2.3 Shoulder-Surfing Susceptibility

Authentication systems must protect users against several security threats, including password guessing attacks, interception, social engineering, and malware. Since no scheme is immune to all attacks, the context of use and threat model needs to be carefully considered to choose the most effective scheme given the circumstances. With all mobile devices, including flexible devices, one particularly relevant threat is shoulder surfing, an attack characterized by learning a password through maliciously observing password entry, since devices are frequently used in public spaces.

Tari et al. [35] conducted a user study to look at the shoulder-surfing susceptibility of the graphical password PassFaces on desktop computers, and compared the results with alphanumeric passwords. In their study, participants played the role of shoulder-surfers and the experimenter played the role of a victim. Participants shoulder-surfed two configurations of PassFaces (mouse or keyboard input) and two configurations of

alphanumeric passwords (dictionary or non-dictionary), and could take notes during observation. The results showed that participants had high shoulder-surfing success rates for non-dictionary alphanumeric passwords, and Passfaces with the mouse input. For alphanumeric passwords, the slow entry speed of non-dictionary passwords made them easy to shoulder-surf, and for PassFaces the mouse input allowed observers to easily see the selections made in the password. Thus, the results from this study suggest that authentication systems should hide password input from observers, and overload their working memory to make it difficult for them to shoulder-surf passwords.

Shaub et al. [30] looked at the usability and shoulder-surfing susceptibility of alphanumeric passwords on eight virtual keyboards on five mobile platforms. Their study methodology was very similar to Tari et al.'s [35] shoulder-surfing study for graphical passwords. Participants shoulder-surfed three alphanumeric passwords using one of the eight virtual keyboards. They found that keyboards which were most usable were also the easiest to shoulder-surf. Specifically, keyboards where the user did not have to switch through different characters (e.g., lowercase, uppercase, special characters) were the easiest to shoulder-surf and also the most usable.

2.2.4 Selecting Passwords

Most authentication schemes allow users to pick their own passwords. However, research has shown that users often choose predictable passwords [10, 14], reuse them across multiple accounts [16], and write them down [18, 28, 44]. These behaviours result in insecure user chosen passwords. Several techniques have been suggested to help users create secure passwords. These include password composition policies and password strength meters. Password composition policies consist of a set of rules (e.g., be a specific length, contain certain characters) that passwords must comply with. However, users often satisfy these requirements in predictable ways which results in weak passwords [33, 40]. These policies also overburden users and lead to frustration [18]. Password strength meters rate the strength of users' passwords, and sometimes provide them with suggestions on how to improve their password strength. These meters are used by many websites including Gmail, Facebook and Twitter,

however their effectiveness depends on their design [36] and context of use [15].

As users often choose insecure passwords, an alternative is to let the system choose a password for them. While this approach ensures password security, research has shown that users have difficulty remembering system-assigned passwords because they cannot associate them with something memorable [42].

In summary, authentication schemes can generate passwords in two ways: they can allow users to pick their own passwords or have the system assign them a password. Both approaches have their strengths and weaknesses, and new authentication schemes should evaluate both approaches and select the method which produces the most secure and usable passwords.

2.2.5 Password Space

Authentication schemes have a theoretical password space and an effective password space. The theoretical password space contains the set of all passwords that can be created in the authentication scheme. However, most users create passwords that fall into a subset of the theoretical password space. This subset of the theoretical password space is known as the effective password space of the authentication scheme. Thus, the effective password space is smaller than the theoretical password space.

As it is very difficult to measure the effective password space of an authentication scheme, the measure of theoretical password space is often used instead. The theoretical password space can be computed using the formula $\log(c^{\mathrm{n}})$, where c = number of available gestures or digits in the password scheme and n = password length.

2.3 Statistical Analysis

In this thesis, we used various statistical tests to analyse the data collected from our user studies. Table 2.1 outlines the statistical tests used in this thesis.

Name	**Description**	**Example**
Wilcoxon signed-rank	Non-parametric test that compares the distributions from a matched-pairs design.	Z = n, $p < .05$ n = value of the test statistic Z p = significance level
McNemar	Compares the nominal data of two related samples.	$\chi^2(m, N = s) = n$, $p < .05$ m = degrees of freedom n = value of the chi test statistic s = sample size p = significance level
Mann-Whitney U	Non-parametric test that compares the distributions from two unrelated samples.	U = n, $p < .05$ p = significance level n = value of the test statistic U
Fisher's Exact	Compares the nominal data of two unrelated samples. This test is used for small sample sizes (i.e., less than 5 in each category).	$p < .05$ p = significance level

Table 2.1: Summary of statistics used in the thesis

Chapter 3

Prototypes

We developed two prototypes, a flexible display prototype for creating gesture-based passwords and a mobile phone prototype for creating PINs. In this section, we describe these prototypes.

3.1 Mobile Phone PIN Authentication Scheme

We developed an Android application for creating and re-entering PINs on a mobile phone. The application was developed using the Processing programming language and was implemented on a commercial Samsung Galaxy SIII (I9300) Android phone. Figure 3.1 shows the user interface (UI) of the mobile phone prototype. The UI displays a standard password entry field where each entered digit is obfuscated by an asterisk.

The PIN entry can be reset by pressing the reset button displayed below the password entry field. Users can remove the last entered digit of their PIN by pressing the delete key on the keyboard. Similarly, a password entry can be confirmed by pressing the Done key on the keyboard.

3.2 Flexible Display

Figure 3.2 shows the components of the flexible display prototype. Our flexible display prototype is composed of a flexible PVC sheet with the dimensions 135 x 95 x 1.5 mm. We selected this malleable material because users have shown a preference for less-stiff materials [22]. 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. An LED light is located on the middle left of the display to provide users with visual feedback about the system. The display is connected to an Arduino Uno

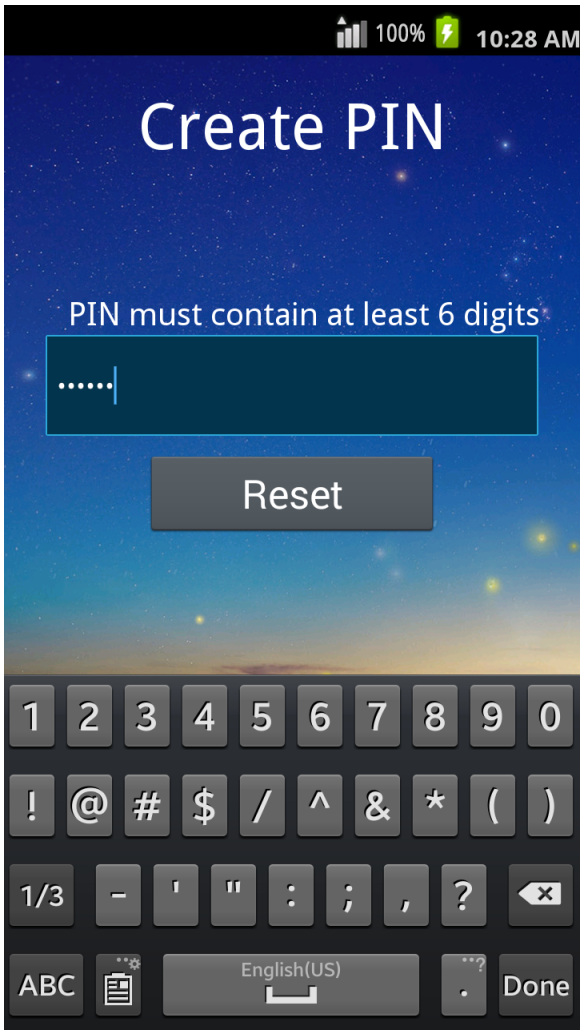

Figure 3.1: User interface of the mobile phone prototype

Microcontroller, which is connected to a computer.

A pico-projector projects a user interface on the display or on the wall in front of the display. We allowed users to choose the location of the UI projection to find a set-up that worked best for them. Most users in our study chose to project the UI on the wall in front of the flexible display. The pico-projector also outputs audio feedback for the prototype.

The prototype also consists of an external control panel to control the authentication process on the prototype. The control panel is composed of two push buttons: a start/stop button and an undo/reset button. The start/stop button is used to start

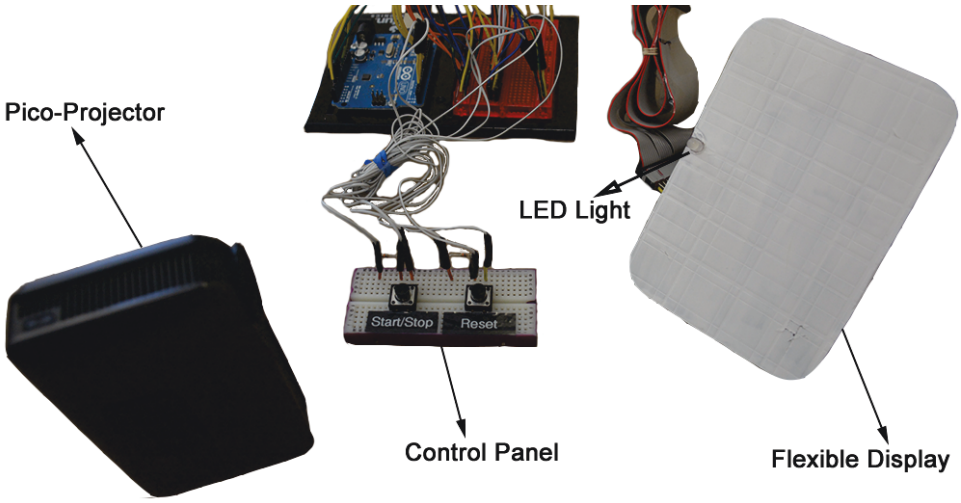

Figure 3.2: Components of the flexible display prototype

or confirm a password entry, and the undo/reset button is used to undo (i.e., delete) a gesture or reset a password entry in case of errors. The "undo" command is triggered when the undo/reset button is pressed once and the "reset" command is triggered when the undo/reset button is pressed and held for a few milliseconds.

We used an iterative design to develop our flexible display prototype, and the final prototype was the result of several iterations.

3.3 Bend Gesture Language

Warren et al. [38] 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 [23, 38], to classify the gestures in our system. A set of 20 gestures can be performed on our flexible display prototype: each corner of the display can be bent up or down (8 gestures) and pairs of corners can 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. Figure 3.3 shows the set of bend gestures available on the flexible display prototype.

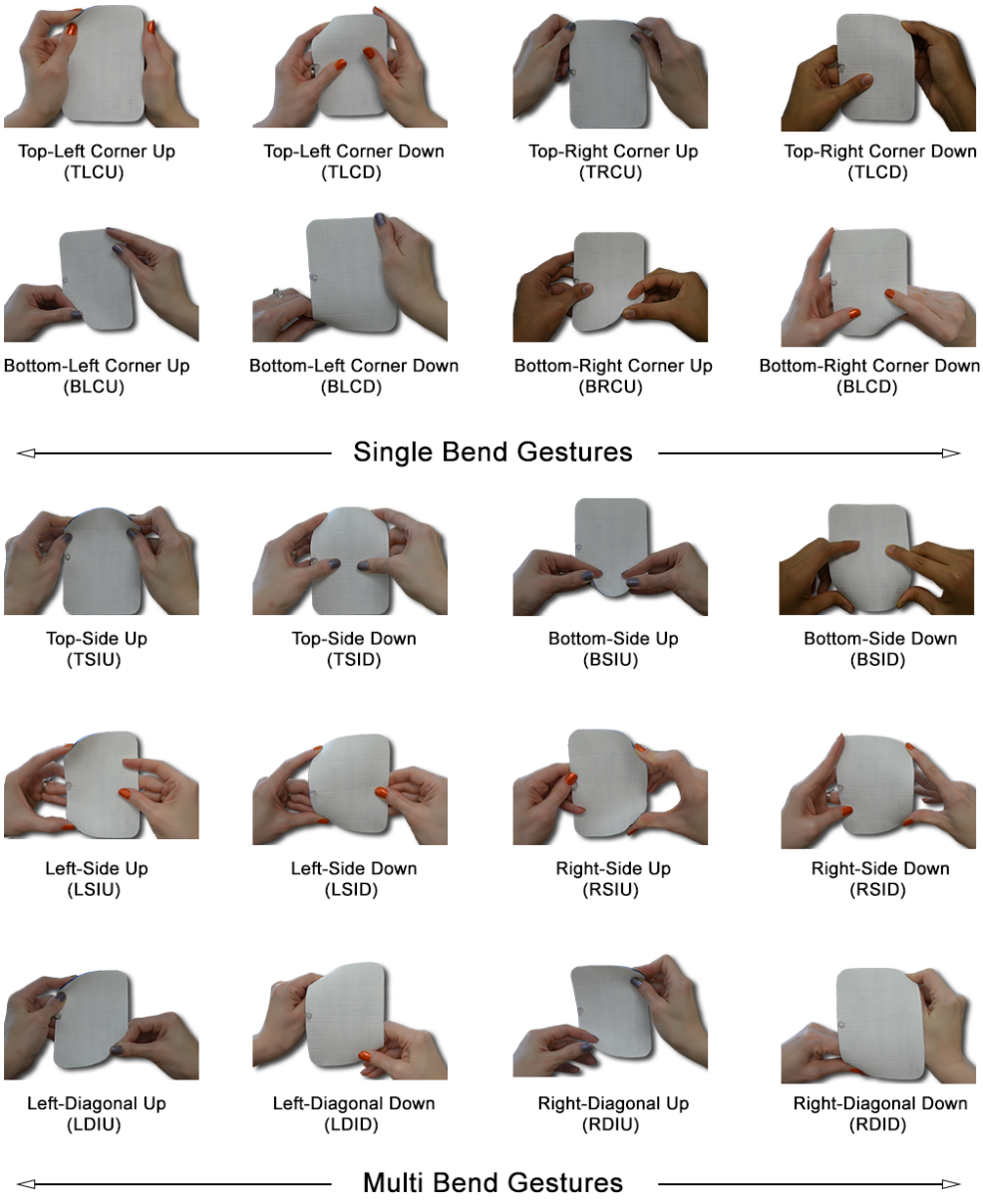

Figure 3.3: The set of bend gestures available on the flexible display prototype

Sensor	Location on the Display	Example Threshold Range
1	Top-left corner	500 - 700
2	Top-right corner	410 - 500
3	Bottom-right corner	450 - 550
4	Bottom-left corner	450 - 750

Table 3.1: Example sensor thresholds for the flexible display prototype

3.3.1 Gesture Recognition Algorithm

We developed an algorithm for recognizing bend gestures on the flexible display. In this section, we describe the details of our algorithm. Specifically, we describe how data from the bend sensors is mapped to the gestures in our gesture language.

The four bend sensors affixed to the flexible display change their resistance when a sensor is bent up or down. Since these sensors are affixed to each corner of the flexible display, this means that a sensor changes resistance when its respective corner is bent up or down. Arduino maps the resistance of each sensor to an integer value between 0 and 1023. When a sensor's value is within a particular range the sensor is stationary, when its value is above the range it is bent upwards and when its value is below the range it is bent downwards.

Our algorithm checks the values of the sensors every 250ms and maps them to a gesture shown in Figure 3.3. When new bend sensors are installed in the display, their thresholds are very similar. However, as they get used their thresholds change. The thresholds of the sensors change depending on how much the sensor has been used, and it is possible for one sensor to have very different thresholds than another sensor. Table 3.1 shows an example of the sensor thresholds after a significant amount of use.

To ensure an optimal and consistent performance of our prototype, we calibrated the sensor thresholds before each use. Calibration was done by reading the values of each sensor for a few seconds, at different degrees of bend. Using these values we determined the thresholds of the sensors and updated them in our gesture recognition algorithm.

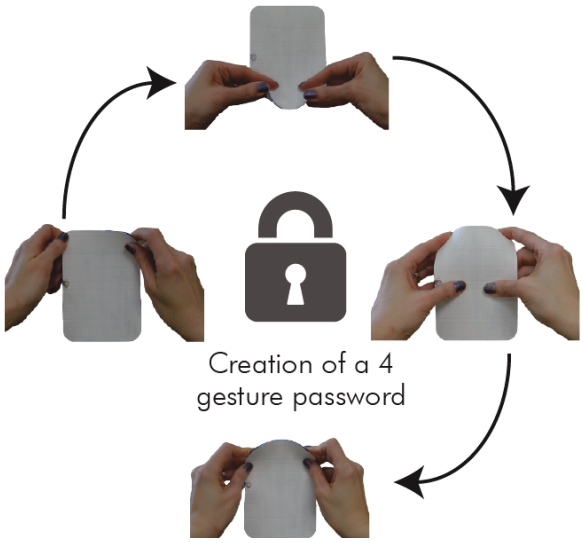

Figure 3.4: Creation of a 4-gesture bend password

Single vs. Multi Bend Gestures

When a sensor is bent up or down, the algorithm waits for 100ms for another sensor to be bent before registering a gesture. If no other sensor is bent, the system registers a single gesture corresponding to the sensor that was bent.

If another sensor is bent within 100ms, the algorithm checks to see if the two bent sensors map to a valid multi gesture in the bend gesture language. If a corresponding gesture is found, the system registers the multi gesture. If a corresponding gesture is not found, the system does not register a gesture, which indicates the entry of an invalid bend gesture.

3.4 Bend Gesture Authentication Scheme

In our authentication scheme, passwords are created by performing a series of bend gestures on the flexible display. Figure 3.4 shows the creation of a 4-gesture bend password. When a gesture is performed on the flexible display, the LED light changes color (blue for a single gesture and pink for multi gesture), the projector emits a clicking sound and an asterisk appears in the password entry field of the UI. We designed the UI of the flexible display to match the UI of the mobile phone prototype (Figure 3.1), and the user interfaces look the same with the exception of the virtual

keyboard displayed on the screen in the mobile UI. After entering a password on the flexible display, users confirm their password entry by pressing the *Start/Stop* button on the external control panel.

The *Undo/Reset* button allows users to correct their password entry. When this button is pressed once, the system deletes the last gesture entered in the password. Thus, the reset button is similar to the backspace key on a keyboard. When the *Undo/Reset* button is pressed and held for a few milliseconds the system resets the password entry. When a password entry is modified, the system updates the contents of the password field in the UI.

The authentication scheme was developed using Arduino and the Processing language. The Arduino module was deployed on the Arduino Uno Microcontroller, and it controlled the physical components of our prototype (e.g., LED light, sensors, control panel). The Processing module ran on the computer and it displayed the UI, received messages from the Arduino module and saved instrumented data in log files on the computer. The Arduino and Processing modules communicated via the USB port of the computer.

Chapter 4

User Chosen Passwords

The goal of our first user study was to evaluate the usability of our bend gesture authentication scheme, in comparison to a PIN based scheme. We used a within-subjects design where participants created two passwords, one for a flexible device and one for a rigid mobile device. Participants returned to the lab one week later to re-enter their passwords. As this is an exploratory study, we do not state any specific hypotheses for the study.

4.1 Methodology

Our two part study was constructed following a standard usable security protocol and was approved by Carleton University's Research Ethics Board. In the first session, participants created, confirmed, and rehearsed their passwords. The second session took place after a week and in this session participants re-entered their passwords. The second session was designed to evaluate the memorability of the passwords created in the first session. Figure 4.1 illustrates our methodology.

4.1.1 Session 1: Creating Passwords

In the first session, participants were trained on how to use the flexible display prototype and bend gesture authentication scheme. We gave a demonstration of how the prototype worked, and provided them with the opportunity to familiarize themselves with it. Participants were instructed to practice each bend gesture at least twice or until they were comfortable with performing the gesture. After training, participants created either a bend password on the flexible display or a PIN on the mobile phone. We configured the two prototypes so that their theoretical password spaces [1] were as

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

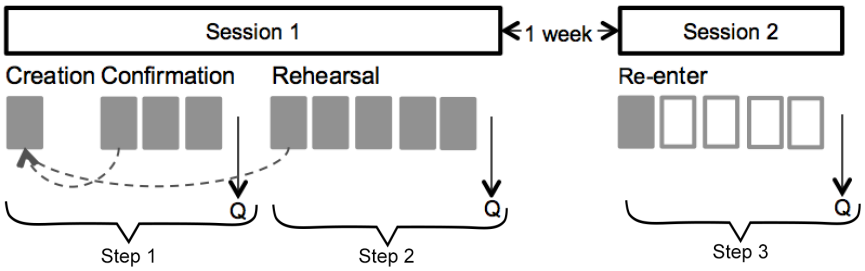

Figure 4.1: There were three main steps in the user study and each step was completed on both devices before moving on to the next step. In the first step, participants created a password and confirmed it three times. In the second step, they rehearsed their password five times. At any time during the confirmation or rehearsal period, participants could create a new password, which resulted in starting the process again. A week later, participants completed step 3 where they had up to 5 tries to re-enter their password correctly.

close as possible to the suggested minimum of 20 bits [17]. Bend passwords had a minimum of 5 gestures, giving a theoretical password space of 21.6 bits. PINs needed to be at least 6 digits long, for a 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 did not have any previous experience with the system.

After creation, participants confirmed their passwords by successfully entering them three times. Participants then completed several online post-task questionnaires providing their opinions and perceptions of the prototypes. Finally, we asked participants to correctly rehearse their password five times. This last step was designed to help with password memorization. If participants forgot their password during the confirmation or rehearsal stage, they could go back to create a new password. When participants chose this option, they had to complete the confirmation and rehearsal stages again with the new password, but did not complete the questionnaires again.

Once the rehearsal procedure was completed, participants completed the online post-task questionnaires. After this, participants were presented with the second device, where they followed the same protocol. The order of presentation of the devices was counter-balanced to reduce learning effects. Finally, participants were told they would have to re-enter their passwords during the second session. Our methodology for Session 1 closely followed Mott et al.'s usability study of TangibleRubik [27] where

users were also presented with a novel tangible password system.

4.1.2 Session 2: Log-in

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 the password re-entry tasks, participants completed post-task questionnaires collecting their perceptions and feedback for each system.

4.2 Participants

We recruited 25 participants (12 female) with an average age of 24.6 years. Twenty two were students and three worked in sales or retail. Nineteen owned at least one smart phone and fourteen had a 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 tested individually in a quite room of our lab, and were given $15 compensation for completing both sessions.

4.3 Results

We analysed data from both sessions to compare our flexible display authentication scheme with PINs. For session 1, we evaluated the composition of the passwords created, password creation time and number of times a password was created. We also look at the time and number of tries participant took to confirm and rehearse their passwords. For session 2, we evaluated the success rates, login time and number of login tries.

4.3.1 Session 1: Creating Passwords

Creation Time and Number of Passwords Created

Figure 4.2 shows the creation time for bend passwords and PINs. For both passwords, the creation time includes the time participants spent coming up with their new

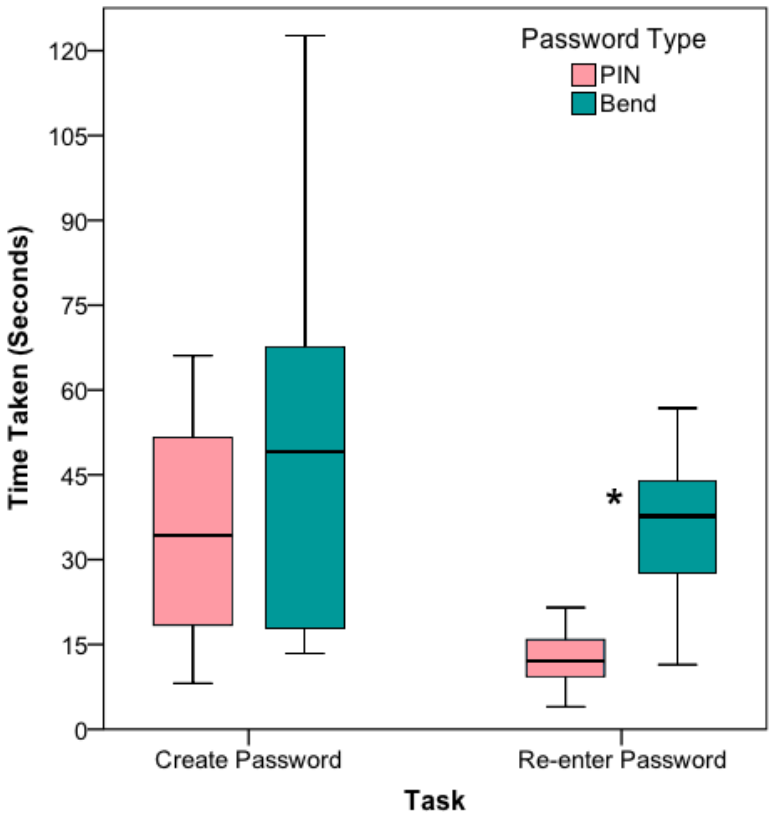

Figure 4.2: Password creation and re-enter times. The re-enter times between conditions are significantly different (*).

password and entering it into the system. Thus, creation time includes thinking time as well as password entry time. A Wilcoxon Signed-Rank test found no significant difference between the creation time of bend passwords (M = 52s, Md = 49s, SD = 42) and PINs (M = 49s, Md = 36s, SD = 44s) (Z = -861, p = 0.389).

While participants could easily create bend passwords, they had difficulty initially creating memorable passwords, which led them to create multiple bend passwords. We observed that 92% of participants created only one PIN during the study while only 56% of participants created one bend password. A Wilcoxon Signed-Rank test found that participants created more bend passwords (M = 1.92, Md = 1, SD = 1.29) than PINs (M = 1.12, Md = 1, SD = 0.44) (Z = -2.848, p = 0.004). Most participants who forgot their bend passwords forgot them at the confirmation stage (92%) and only one (8%) forgot it at the rehearsal stage.

Password Creation Strategies

Bend Passwords: Participants used a variety of strategies to create their gesture-based passwords, all with the idea to create a secure password that was "easy to remember". Their strategies can be grouped into one of the following categories:

- *Repeating Gestures* (16%): Selecting two or three gestures and using them repeatedly in the password.
- *Natural Movements* (8%): Selecting gestures that felt natural based on hand movements.
- *Patterns* (44%): Creating a pattern using the gestures. The following are the types of patterns participants created:
  - *Clockwise* (8%): Bending the corners of the display up or down consecutively in a clockwise manner.
  - *Mirror* (16%): Performing a series of bends on one side of the display, and then performing the exact same sequence of bends on the opposite side.
  - *Other* (20%): Did not explain the type of pattern used. However, all these participants remembered their bend passwords after one week, which indicates that they used a good password creation strategy.
- *Number Mapping* (12%): Assigning numbers to each gesture and using the numbers to create a sequence for a bend password.
- *Drawing* (16%): 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 Drawing strategy produced the longest bend passwords.

PINs: 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.

Confirming Password

Participants were asked to confirm their passwords by successfully re-entering them a total of three times. They had an unlimited number of tries to re-enter their passwords successfully and if they forgot their passwords, they could go back to create a new password. When this option was chosen, participants had to complete the confirmation stage again.

Confirmation Time: We looked at the time participants took to confirm their password once. For each participant, we selected the fastest time out of their three successful confirmations. On average, participants took 6s (M = 6s, Md = 6s, SD = 2s) to successfully confirm their PINs once and 19s to confirm their bend passwords (M = 19s, Md = 17s, SD = 8s). A Wilcoxon Signed-Rank test found that participants took significantly more time to confirm their bend passwords than their PINs (Z = -4.290, p = .000).

Incorrect Confirmation Attempts: We looked at the number of incorrect attempts participants made while confirming their final password three times. For each participant, we looked at the total number of incorrect attempts made over three confirmations. Participants made very few incorrect attempts while confirming both PINs (M = .12, Md = 0, SD = .332) and bend passwords (M = .32, Md = 0, SD = .476). A Wilcoxon Signed-Rank test found no significant difference between the number of incorrect confirmation attempts of PINs and bend passwords (Z = -1.667, p = .096), once participants had selected a memorable password.

Rehearsing Password

Participants were asked to rehearse their passwords by successfully re-entering them for a total of five times. As with the confirmation stage, participants had an unlimited number of attempts to successfully re-enter their passwords. If they forgot their passwords, participants could go back to the password creation stage to create a new password. When they chose this option, participants had to complete the confirmation and rehearsal stages again.

Rehearsal Time: We looked at the time participants took to rehearse their passwords once. For each participant, we selected the fastest time out of their five successful rehearsals. On average, participants took 5s (M = 5s, Md = 5s, SD = 2s) to successfully rehearse their PINs and 15s to rehearse their bend passwords (M = 16s, Md = 15s, SD = 7s) once. A Wilcoxon Signed-Rank test found that participants took significantly more time to rehearse their bend passwords than their PINs (Z = -4.374, p = .000).

Incorrect Rehearsal Attempts: For each participant, we looked at the total

Password Type	Length M (SD)	Unique Entries M (SD)
PIN	7.08 (1.29)	5.08 (1.15)
Bend	6.64 (2.38)	5.08 (1.63)

Table 4.1: Password Characteristics. Unique entries are the number of unique digits or gestures in the user chosen PINs and bend passwords respectively.

number of incorrect rehearsal attempts they made while rehearsing their passwords five times. Participants made very few errors while rehearsing both their PINs (M = .08, Md = 0, SD = .277) and bend passwords (M = .84, Md = 0, SD = 1.405). However, a Wilcoxon Signed-Rank test found that participants made significantly more errors while rehearsing their bend passwords than their PINs (Z = -2.654, p = .008). After successfully confirming their passwords, very few participants forgot them at the rehearsal stage. All remembered their PINs and two forgot their bend passwords. These participants went back to the creation stage, created a new password, confirmed it three times and rehearsed it five times again. No one completed the rehearsal stage more than twice.

We compared participants' performance at the rehearsal stage with their performance at the confirmation stage to determine whether their performance improved with experience. A Wilcoxon Signed-Rank test found that participants took significantly less time per attempt to rehearse both their PINs (Z = -3.884, p = .000) and bend passwords (Z = -3.354, p = .001) than to confirm them.

Password Characteristics

We looked at the length of passwords created as well the number of unique digits or gestures they contained. Table 4.1 shows the mean length and the number of unique entries (gestures or digits) of bend passwords and PINs.

We observed that the average length of both passwords was close to the required minimum (6 for PINs and 5 for bend passwords). It is interesting to note that the longest PIN had 11 digits while the longest bend password had 14 gestures. A Wilcoxon Signed-Rank test found no significant difference between the number of unique gestures or digits used in bend passwords and PINs (Z = -.327, p = 0.744).

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 frequently than others. The top four most frequently used gestures were the top-right-corner-up (19%), top-left-corner-up (13%), top-side-up (8%), and bottom-left-corner-up (7%). The least used gestures were the left-diagonal-down (0.58%), bottom-side-down (1%), top-side-down (2%), and right-side-up (2%). Generally, participants preferred up gestures more than down gestures. Out of all the gestures used, 72% were up gestures and 28% were down gestures. Participants used more single bend gestures (63%) than multi bend gestures (37%). Overall, these results are consistent with the findings of Lahey et al. [23] and Warren et al. [38].

4.3.2 Session 2: Log-in

21 participants completed the second session, 15 remembered both bend and PIN passwords, 5 forgot either their bend or PIN password and 1 forgot both passwords.

Success Rate

We evaluated the login success rate by assessing if participants were able to enter their password correctly in any of the 5 tries. The success rate of PINs was 86%, and that of bend passwords was 81%. A McNemar test with the continuity correction found no significant difference between the success rate of bend passwords and PINs ($\chi^2(1, \mathrm{N} = 15) = 0.00$, $p = 1.00$, the odds ratio is 0.67).

All three participants who forgot their PINs used personal information in their PINs and appended a random number or sequence of numbers at the end. The type of personal information used included old phone numbers, old street addresses, close family members' birthdays, car licence plate numbers, student numbers and favourite course codes. These participants either forgot the random part of their PIN or the structure they used to create it.

All four participants who forgot their bend passwords, used a different password creation strategy. They used the clockwise, mirror, drawing and natural movements

password creation strategies. This shows that the type of password creation strategy used to create bend passwords did not have an effect on their success rates.

Number of Tries

The majority of participants successfully re-entered their PINs (M = 1.80, Md = 1, SD = 1.21) and bend passwords (M = 1.53, Md = 1, SD = 0.83) in one try. A Wilcoxon Signed-Rank test found no significant difference between the number of tries participants took to successfully re-enter their bend passwords and PINs (Z = -.540, p = 0.589).

Re-enter Time

We analysed the login time of participants who successfully remembered their passwords, and only included the time of their successful login attempt. Figure 4.2 shows the login time for bend passwords and PINs. For both passwords, the log-in time includes the time participants spent recalling their passwords and re-entering them into the system. The median login time for bend passwords was 37.69 seconds, while PIN passwords took 12.06 seconds to re-enter. A Wilcoxon Signed-Rank test found that participants took longer to login with their bend passwords than their PINs (Z = -3.294, p = 0.001).

Bend Password Memorability Strategies

We note a few different participant strategies for remembering their bend password after a week. A few participants (29%) mentally rehearsed their passwords on their own throughout the week. Another few (12%) only rehearsed it before coming to the second session. Finally, most participants (59%) did not report having a strategy, writing their password down, or rehearsing it in any way. These participants remembered their passwords via muscle memory and some were surprised that they were able to remember their passwords.

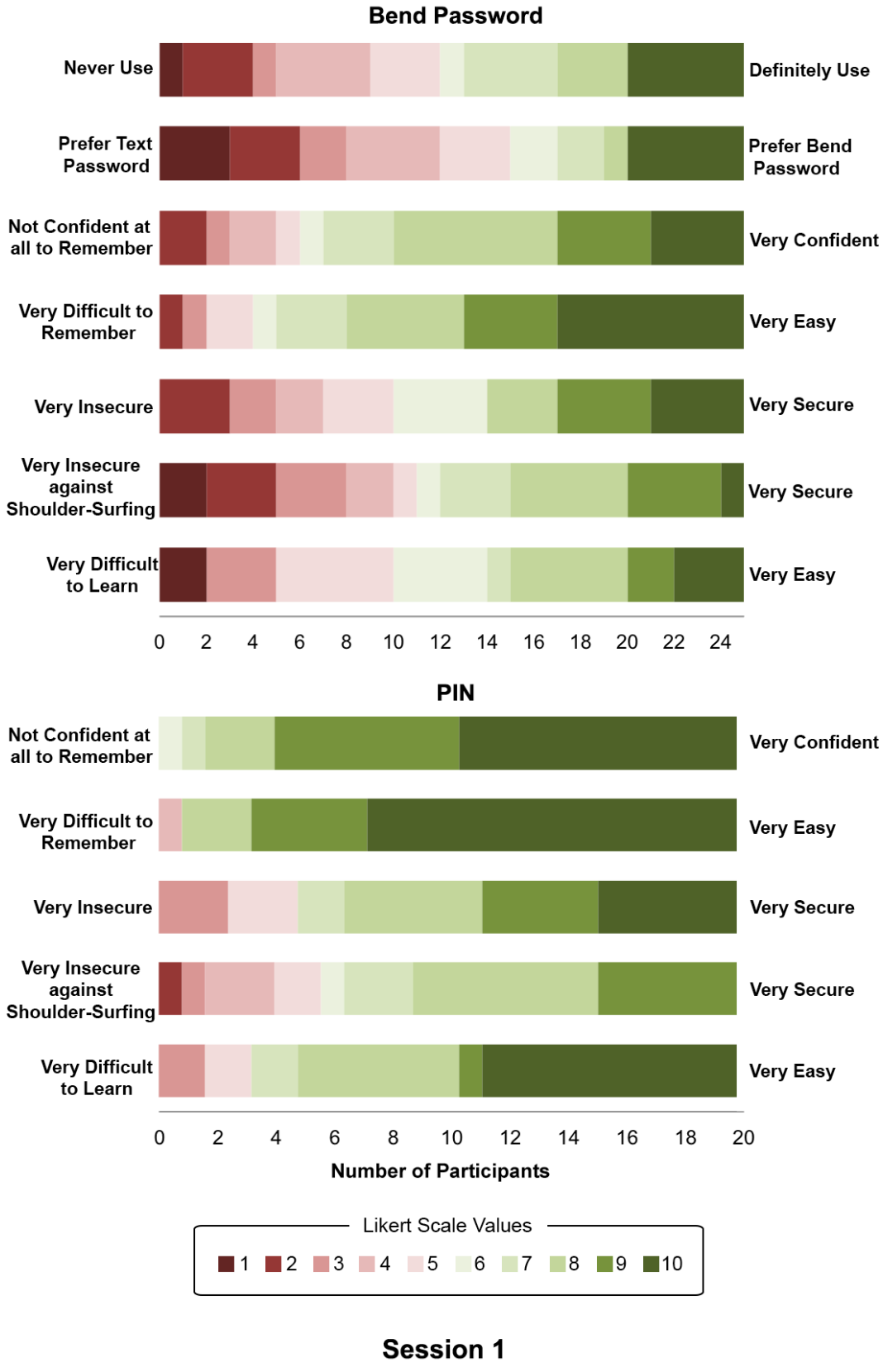

Figure 4.3: Distribution of session 1 Likert scale responses for user chosen passwords

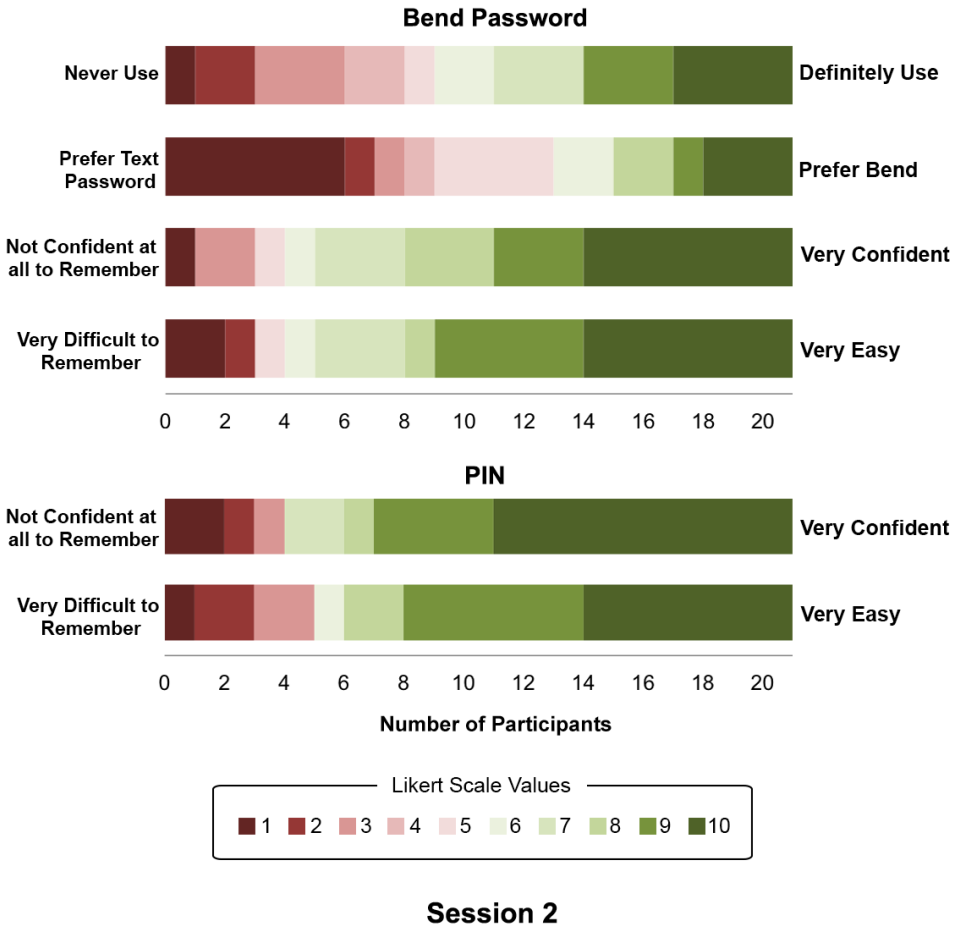

Figure 4.4: Distribution of session 2 Likert scale responses for user chosen passwords

4.3.3 Questionnaire Responses

Participants completed questionnaires at the end of both sessions. We grouped their responses into five categories: ease of use, memorability, perceived shoulder-surfing, perceived security and likelihood of using bend passwords.

Figures 4.3 and 4.4 show the distribution of participants' responses to the questionnaires in session 1 and 2 respectively. The questions in the questionnaires belong to one of the categories defined above. Table 4.2 shows results from the statistical analysis of the Likert scale questions across session 1 and 2.

Question	Session	PIN Md (SD)	Bend Md (SD)	Stats
Ease of Use				
Ease of Password Creation	1	8.5 (2.18)	6 (2.65)	**(Z = -2.822, p = 0.005)***
Memorability				
Ease of Remembering	1	10 (1.31)	8 (2.25)	**(Z = -2.927, p = 0.003)***
	2	9 (3.19)	9 (2.99)	($Z = -.134, p = 0.893$)
Confidence in Remembering	1	9 (1.07)	8 (2.48)	**(Z = -3.312, p = 0.001)***
	2	9 (3.20)	8 (2.67)	($Z = -.357, p = 0.721$)
Perceived Shoulder-Surfing				
Secure against Shoulder-Surfing	1	8 (2.13)	7 (2.94)	($Z = -1.763, p = 0.078$)
Perceived Security				
How Secure	1	8 (2.33)	6 (2.78)	**(Z = -2.108, p = 0.035)***
Likelihood of Using Bend Passwords				
Use if Available	1	—	6 (2.87)	—
	2	—	6 (3.06)	—
Bend vs. Text	1	—	5 (3.10)	—
	2	—	5 (3.32)	—

Table 4.2: User chosen passwords - Questionnaire Likert scale responses grouped by category. Bold and * indicates statistical significance.

Ease of Use

At the end of session 1, we used a 10-point Likert scale (1 = very difficult and 10 = very easy) to ask participants how easy it was for them to create a bend password on the flexible display and a PIN on the mobile phone. Participants found it significantly easier to create their PINs than their bend passwords (Table 4.2).

Memorability

At the end of both sessions, we asked participants two 10-point Likert scale questions to measure their ease and confidence about remembering their passwords (Bend and PIN). The first question asked them how easy it was for them to remember their new

password (PIN and Bend). The Likert-scale values for this questions were 1 = very difficult and 10 = very easy. The second question asked participants how confident they felt about remembering their passwords after one week. The Likert scale values for this question were 1 = not confident at all and 10 = very confident. Table 4.2 shows participants' responses to these questions in session 1 and 2.

Ease of Remembering: We compared participants' responses to the first question across session 1 and 2 for both passwords. We used the Bonferroni adjusted alpha levels of .0125 (.05/4) to do this comparison. Participants found it fairly easy to remember their PINs in both session 1 and 2, and their responses to this question did not significantly change between the sessions (Z = -2.216, p = .027). Similarly, participants found it easy to remember their bend passwords in both sessions and their response to this question did not significantly change between the sessions (Z = -.392, p = .695). In session 1, participants found it significantly easier to remember their PINs than their bend passwords (Table 4.2). However, no such difference was found in session 2.

Confidence in Remembering: We compared participants' responses to the second question across session 1 and 2, and used the Bonferroni adjusted alpha levels of .0125 (.05/4) to do the comparison. In both sessions, participants were fairly confident about being able to remember their PINs, and there was no significant difference between their response across the two sessions (Z = -1.578, p = .115). Similarly, participants were fairly confident about being able to remember their bend passwords a week after session 1 and 2. Their responses to this question did not significantly change across both sessions (Z = -.967, p = .334). In session 1, participants were significantly more confident about remembering their PINs after a week than their bend passwords (Table 4.2). However, no such difference was found in session 2.

Shoulder Surfing

At the end of session 1, we used a 10-point Likert scale (1 = very insecure and 10 = very secure) to ask participants how secure their password was against shoulder-surfing attacks. Participants thought that both passwords would be difficult to shoulder-surf by malicious users.

Perceived Security

At the end of session 1, we used a 10-point Likert scale (1 = very insecure and 10 = very secure) asking participants to rate the security of their PIN or bend password. Participants thought PINs to be significantly more secure than bend passwords (Table 4.2).

Likelihood of Using Bend Passwords

At the end of both sessions, we used a 10-point Likert scale (1 = never and 10 = definitely) to ask participants whether they would use a bend password if it was available. In both sessions, participants were slightly in favour of using bend passwords and there was no significant difference in their responses between the two sessions (Z = -.222, p = .824).

Bend vs. Text

We used a 10-point Likert scale (1 = prefer text and 10 = prefer bend) to further ask participants whether they would prefer a bend or text password on a flexible display device. We asked this question in each session. In both sessions, participants were neutral in their response and there was no significant difference between their responses across the two sessions (Z = -.281, p = .779).

Application Areas of Bend Passwords

We provided participants with several application areas of bend passwords and asked them to select areas where they would use a bend password. Participants could select multiple areas of application. Figure 4.5 shows participants' responses. Participants thought bend passwords would be useful for unlocking their mobile device but were less enthusiastic about using them for other purposes.

4.3.4 User Feedback

At the end of session 1, we asked participants two open-ended questions about what worked well with our system and what could be improved. Since these questions

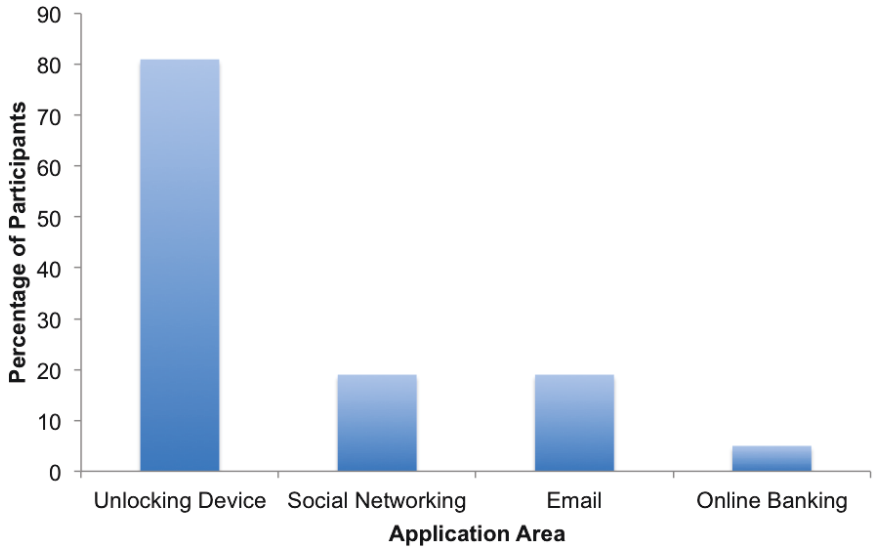

Figure 4.5: Application areas of user chosen bend passwords

were also asked in our second study, we grouped the responses from both studies and analysed the combined responses. The results from this analysis are presented in section 5.3.4.

4.4 Summary of Results

Participants could quickly create their bend passwords but they had trouble initially creating passwords that were memorable. Because of this, many participants forgot their bend passwords at the confirmation stage, and went back to the password creation stage to create a new password. The same result was not found with PINs, which is not surprising because participants had well developed strategies for creating memorable PINs. Although many participants forgot their bend passwords at the confirmation stage, only two forgot them at the rehearsal stage. In both the confirmation and rehearsal stages, participants were allowed to make any number of unsuccessful confirmation/rehearsal attempts before entering their password successfully. For example, it was possible for participants to make several incorrect password entries before remembering their password. This happened when participants forgot parts of their password (i.e., direction of a gesture) and tried various combinations until they found the correct password. We looked at the number of incorrect attempts

participants' made in the confirmation and rehearsal stages, to determine whether participants partially forgot their passwords in these stages. In the confirmation stage, participants made very few incorrect confirmation attempts for both PINs and bend passwords. In the rehearsal stage, participants made significantly more incorrect attempts before successfully re-entering their bend passwords than their PINs. Thus, although participants initially had a hard time creating memorable bend passwords, once they settled on a password they could easily remember it.

Most participants were able to remember their bend passwords and PINs a week after creating them, and there were no significant differences between the success rates of both passwords. However, participants took more time to re-enter their bend passwords than their PINs. This could be because participants were using personal or familiar information in their PINs, which aided in memory compared to bend passwords which were completely new. In addition to this, participants had much more practice re-entering PINs on a mobile phone, and could re-enter them faster than their bend passwords on the flexible display. In session 1, participants found it easier to remember their PINs than their bend passwords. They were also more confident about remembering them a week later. However, these results changed in session 2 where no differences were found. This shows that as participants became more comfortable with our new authentication scheme, they found bend passwords to be as memorable as PINs.

4.5 Discussion

In this study, we user tested our bend gesture authentication scheme on a flexible display prototype and compared the results with PINs. We found that most participants could easily create bend passwords and PINs. There were no significant differences in the amount of time participants took to create their bend passwords and PINs. We see this as a positive result, considering that most participants were new to our authentication scheme and were novice users on flexible display devices. In fact, many had not even heard of flexible display devices before coming to our study. It is also important to note that most participants created their PINs using parts of their personal information or parts of existing PINs.

Usable passwords have two main properties: they are secure and easy to remember for users. Many guidelines have been developed for creating usable passwords in traditional authentication schemes, such as PINs and text passwords. One of the goals of our study was to determine the properties of a usable bend password. Thus, we gave participants very few instructions on how to create a "good" bend password, and only asked them to create a memorable and secure bend password. We told them that a password is considered secure if it has a variety and large number of bend gestures. We found that participants created bend passwords using a variety of different strategies, which is good from a security perspective.

Although both single and multi-gestures were used, participants used significantly more single gestures. Participants preferred "up" gestures because they were easier to perform and required applying less physical force on the display (pull requires less physical force than push). Participants found it easier to perform single gestures than multi-gestures. Even though multi-gestures were harder to perform, 86% of participants used at least one in their password. When asked why they used a multi-gesture, many participants responded that they used it to increase the strength of their password. Thus, participants associated the use of multi-gestures with password strength. Some even compared them to using special characters in text-based passwords. Participants thought that because multi-gestures are harder to perform, they would make their passwords more resilient to malicious attacks. This result also indicates that participants were motivated to create strong bend passwords.

Qualitative data revealed that participants found their PINs significantly more secure than their bend passwords. However, this difference was not due to the shoulder-surfing susceptibility of bend passwords. In fact, participants thought that both their PINs and bend passwords would be fairly difficult to shoulder-surf, and there were no significant differences between the passwords. Participants may have rated bend passwords lower on security as a precaution, because it is a new authentication scheme and they were not aware of all its security vulnerabilities.

When asked about whether they would use bend passwords in the future, participants were slightly positive in their response. However, they were neutral in their response when asked if they would prefer bend passwords over text-based passwords.

In addition to this, when asked to select an application of bend passwords on flexible displays, most participants answered that they would use bend passwords to unlock their mobile devices. These results show that participants were slightly positive about using bend passwords on their mobile devices. Since, most of our participants were novice or beginners with flexible displays, we expect these results to improve as participants get more experience with these devices.

In summary, the results from our user study show that participants could easily create passwords using our gesture based authentication scheme. Bend passwords were fairly secure and most users remembered them after one week. With the exception of timing, participants' performance with bend passwords was comparable to PINs. We implemented our authentication scheme on a very early version of a medium-fidelity flexible display prototype and believe that some limitations of our prototype may have affected participants' impressions of bend passwords. Specifically, gesture speed and accuracy was an issue. Thus, given the limitations of our prototype, we see the results from our study as positive and believe these results, including user impressions, can be improved by fixing some of the limitations of our prototype.

We observed that that many participants in our user study created weak PINs and some created weak bend passwords. This is a common problem when users are given the ability to choose their own passwords. A solution to this problem is to let the system choose a user's password which would ensure that their password is secure. In the next chapter, we look at system-assigned bend passwords and compare the results with system-assigned PINs.

4.6 Limitations

In this section, we address the limitations of our prototypes and the user study.

4.6.1 Prototypes

The user interface and control panel of our flexible display prototype was decoupled from the flexible display, which could have affected users' performance and perceptions. The user interface was projected onto a wall and users had to shift their attention between the flexible display and the user interface projection when completing the password task. This led to larger entry times for bend passwords and negatively affected users' perception of bend passwords. Similarly, when users used the control panel for the undo/reset functions, they shifted their attention away from the flexible display, which negatively affected task completion times and user perceptions of bend passwords.

Our prototype did not allow participants to perform a series of gestures quickly and sometimes the gestures did not register properly when participants performed them too quickly. This partially contributed to the longer bend password entry times. In addition to this, multi-gestures had to be performed in a specific way on the prototype to be registered properly. To perform multi-gestures, participants had to bend two corners up or down simultaneously. If one corner was not bent "enough" the gestures were not registered properly. These limitations can be addressed by improving the gesture recognition algorithm, and utilizing a more malleable material for the flexible display.

4.6.2 User Study

The main limitation of our user study was that participants were novice users of our authentication scheme and flexible displays. Most had not even heard of flexible displays prior to participating in our study. We believe this affected participants' performance on the password task, because they were learning how to use the flexible display while creating their bend passwords. With regards to password memorability, we only tested participants' memorability a week after they created their passwords. During this time, participants did not use their passwords at all. In real life, users who have a lock enabled on their phone use their password at least once day to unlock their phone. Thus, it is possible that with more usage participants may be able to remember their passwords better than the results found in our user study.

Chapter 5

System Assigned Passwords

In our first study, most participants created a weak PIN and some created a weak bend password. For PINs, participants used existing numerical passwords or parts of their personal information (i.e., birthdate, phone number etc.), while for bend passwords, they chose passwords with repeating gestures on one side of the display. These results are not surprising: when users are given the opportunity to choose their passwords, they often select passwords that are easy for them to remember, regardless of their security [3]. A solution to this problem is to let the system decide users' passwords, which would ensure that users' passwords are resistant to malicious password guessing attacks. However, such passwords have potential memory drawbacks. Specifically, users have trouble remembering these passwords because they have no memorable patterns within them [25]. In this study, we look at the usability of system assigned bend passwords to determine whether they are prone to the same memorability drawbacks as other types of system assigned passwords (e.g., PINs, text passwords). We also compare the results from our study with system assigned PINs.

5.1 Methodology

We conducted a two part user study with a similar methodology to our first study. In the first session, participants learned how to use the flexible display prototype to create a bend password. After the initial training phase, participants learned a system assigned bend password on the flexible display and a system assigned PIN on a mobile phone. The second session took place approximately one week later. In the second session, participants returned to the lab to re-enter their previously learned passwords (Bend and PIN). Figure 5.1 illustrates our study methodology. This work was approved by Carleton University's Research Ethics Board.

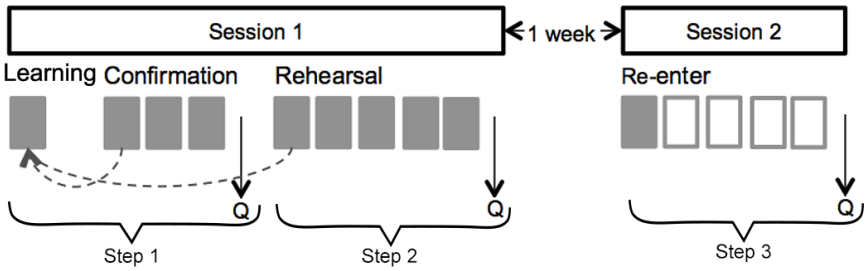

Figure 5.1: Participants completed three steps in the user study, and each step was completed on both devices before moving on to the next step. In the first step, participants learned a password and confirmed it three times. In the second step, they rehearsed it five times. Participants could go back to the learning stage to view their password again at any time during the confirmation or rehearsal period. The third step was completed after a week where participants had five tries to correctly re-enter their password.

5.1.1 Session 1: Learning Passwords

In the first session, participants were trained on how to use the flexible display prototype before proceeding to the password tasks. In the training phase, participants were shown the flexible display prototype and provided a demonstration of how it works. After this, the experimenter demonstrated the set of available bend gestures on the flexible display and asked participants to practice each gesture at least twice or until they were comfortable performing the gesture. Participants next learned how to use the gestures in a bend password. They also familiarized themselves with the different feedback mechanisms available on the system (i.e., LED light, audio, and UI) and the functions of the control panel (i.e., Undo/Reset and Start/Stop buttons). During the training session, participants used a password entry UI similar to Figure 3.1 but without the virtual keyboard displayed on the screen.

After the training session, participants completed two password tasks (Bend and PIN). One of the tasks was on the flexible display and other was on a mobile phone. The order of the tasks and prototypes was counterbalanced, and both tasks followed the methodology outlined in this section. Participants were either shown a random 5 gesture bend password on the flexible display (Figure 5.2) or a 6 digit PIN on the mobile phone (Figure 5.3), and were asked to learn the password. They were told that they would have to re-enter their password in both sessions so it was important for

them to learn and remember it well. Participants were allowed to use any strategy to learn their password. When learning bend passwords, participants could enter a bend gesture on the flexible display and the gesture was highlighted on the user interface (Figure 5.2). This functionality was included to ensure that participants understood each gesture, and how to perform it correctly. We chose passwords with 5 gestures and 6 digits because these were the minimum password lengths required in our first study, and it ensures that the two have similar theoretical password spaces closer to the recommended minimum of 20 bits [17].

After learning their password, participants were asked to successfully confirm it three times. They had an unlimited number of tries to successfully confirm their password. If they forgot their password, participants could go back to the learning stage to view it again. If they chose this option, participants had to complete the confirmation stage again. After successful confirmation, participants completed an online questionnaire providing their opinions and feedback about learning and re-entering their password.

The experimenter switched the prototype (i.e., flexible display or mobile phone) and participants completed the password learning and confirmation tasks on the other prototype, and completed an online questionnaire. Participants then rehearsed their first password five times on the first prototype and completed an online questionnaire. They were given an unlimited number of times to successfully rehearse their password five times. If they forgot their password, participants could go back to the learning stage to view it again. If they chose this option, participants had to complete the confirmation and rehearsal stages again. After this, participants rehearsed their second password five times on the second prototype and completed an online questionnaire. The presentation order of the two prototypes was counter-balanced.

5.1.2 Session 2: Log-in

The second session took place after a week. Participants were asked to correctly re-enter each password. Participants had five tries to correctly re-enter their password on each prototype. After completing each password task, participants completed an online questionnaire providing their perceptions and feedback of the prototype.

At the end of the session, participants completed a short semi-structured post-task interview.

5.2 Participants

20 participants (5 female) with an average age of 23 years completed the study. 19 owned at least one smartphone and 12 had a screen lock enabled on their phone. Of these, 11 used an authentication mechanism (8 PIN and 3 graphical/pattern) to unlock their phone at least four times per day. 3 participants had previous experience with flexible displays: 1 tried the device at a Samsung Expo, 1 worked in the field, and 1 had participated in another bend gesture study within the last year. The remainder had no previous experience with flexible displays. Participants were tested individually in a quite room of our lab, and were given $15 compensation for completing both sessions.

5.3 Results

We analysed data from both sessions. For session 1, we evaluated the time and number of tries participant took to learn, confirm and rehearse their passwords. We also look at the strategies they used to learn their passwords. For session 2, we evaluated the success rate, number of tries and time it took to complete the password re-entry task. We also look at the questionnaire data from both sessions and the post-task interview data from session 2. All statistical analyses are done using a Wilcoxon Signed-Rank test unless otherwise specified.

5.3.1 Session 1: Learning Passwords

Participants were first shown their system-assigned password and given the opportunity to learn their password. Participants learned their bend passwords by sequentially entering the gestures shown on screen (Figure 5.2) repeatedly until they had the sequence memorized. Participants could not practice re-entering their PINs. Many participants memorized their PINs by mentally rehearsing the digit sequence repeatedly.

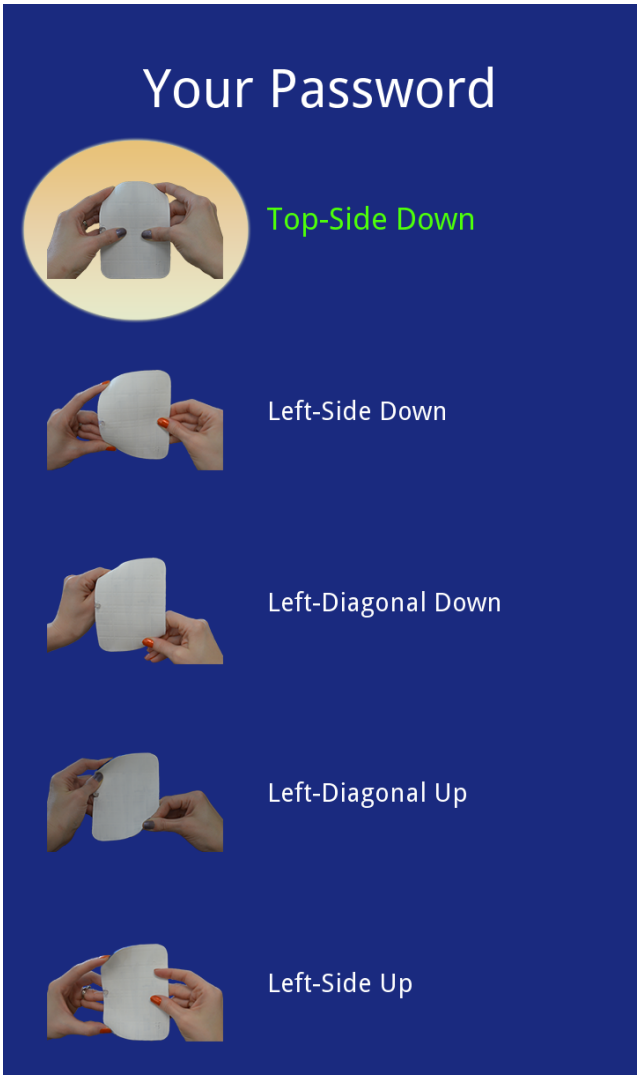

Figure 5.2: Presentation of a random 5 gesture bend password, with the entered gesture (i.e., Top-Side Down) highlighted on the screen

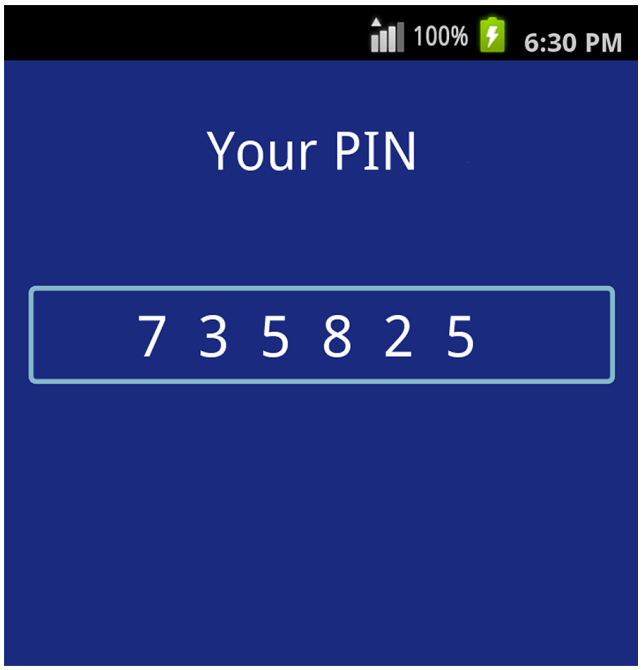

Figure 5.3: Presentation of a random 5 digit PIN

Participants took significantly (Z = -3.920, p = .000) more time to learn their bend password (M = 3.16min, Md = 2.26min, SD = 2.0min) than their PIN password (M = 28s, Md = 17s, SD = 30s). From our observations, we note that differences occurred because participants had to form a new strategy for remembering the bend password, while they already had a well developed strategy for remembering PINs. Participants also took learning time to further familiarize themselves with the bend gestures, assessing how much to bend, and determining the best positions to place their hands. On average participants entered 43 gestures while learning their bend password (Md = 34.50, SD = 35.46).

A linear regression found that the number of gestures participants entered significantly predicted their password learning time, b = .89, $t(18)$ = 8.37, $p < .000$. The number of gestures entered also explained a significant proportion of variance in password learning time, R^2 = .80, $F(1, 18)$ = 70.06, $p < .000$. As expected, the repetitive entry of bend gestures contributed to the longer learning times.

Learning Strategies

Participants used a variety of strategies to remember their passwords. For PINs, 5% of participants reported no strategy and others reported using one of the following strategies. All of these strategies involve some type of rehearsal and the type of strategy participants used was dependent on the set of digits assigned in their PINs.

- *Mental Rehearsal*: 35% mentally rehearsed their PIN repeatedly until they had it memorized. This is a "brute-force" method of memorization.
- *Finding a Pattern*: 25% found and memorized a pattern between the digits. Some of the patterns included: using a mathematical formula to add or multiply digits, treating the digits as a date (YY/MM/DD), or treating the PIN as a set of ages in life (e.g., 20 45 89).
- *Chunking*: 20% broke the PIN into chunks [6] of two digits and remembered the order between the chunks.
- *Keypad Pattern*: 15% memorized the pattern made by the PIN on a numerical keypad. Since, we did not use a numerical keypad in our study, these participants memorized the pattern made by the PIN on their mental representation of a numerical keypad.

Most participants also used some type of strategy to remember their bend passwords. Only 5% stated not using any strategies and others used one of the following strategies:

- *Repeated Entry*: 55% repeatedly entered their password into the device during the learning stage, until they had it memorized. These participants memorized the movements (gestures) of their password by repeatedly performing the movements. Some verbally rehearsed the gestures (e.g., "Top corner up") while entering them.
- *Finding a Pattern*: 15% found and memorized a pattern between the gestures.
- *Password Composition*: 15% broke the password down by its composition. They first memorized the location of the gestures on the display (i.e., top, bottom, right or left) and then memorized the direction of the gesture (i.e., up or down).

- *Mapping*: 10% mapped the gestures to an internal representation. These included assigning numbers to each gesture and memorizing the sequence of numbers, assigning musical notes to gestures and memorizing the "melody" formed by the gestures, or drawing a letter (e.g., initial of first name) using the gestures.

Confirming Password

Participants were asked to successfully confirm their passwords a total of three times, and had an unlimited number of tries to correctly confirm their password. If they forgot their password, participants could go back to the previous stage to view their password again. When they chose this option, participants were required to complete the confirmation stage again, but not the questionnaires. In this section, we look at the amount time participants took to confirm their passwords and the number of incorrect attempts they made while confirming their passwords.

Confirmation Time: We evaluated the time participants took to successfully confirm their password once. For each participant, we selected the fastest time out of their three successful confirmations. On average, participants took 5s to successfully confirm their PINs (M = 5s, Md = 4s, SD = 1s) and 21s to confirm their bend passwords (M = 21s, Md = 18s, SD = 12s). A Wilcoxon Signed-Rank test found that participants took significantly more time to confirm their bend passwords than their PINs (Z = -3.298, p = 0.000).

A potential reason for the longer bend password confirmation times could be the use of the undo/reset buttons located on the external control panel. During password entry, participants used these buttons to delete a gesture (undo) or reset their password entry. As these buttons are external to the display, participants had to divert their attention from the display in order to use them. Many participants used the undo button (M = 1.55, Md = 0, SD = 3.05) while confirming their password and very few used the reset button (M = .05, Md = 0, SD = .224). A linear regression found that the number of undo button presses significantly predicted the confirmation time of bend passwords, $b = 3.91$, $t(18) = 10.35$, $p < .000$. The number of undo button presses also explained a significant proportion of variance in password confirmation time, $R^2 = .86$, $F(1, 18) = 107.13$, $p < .000$.

Incorrect Confirmation Attempts: We looked at the number of unsuccessful attempts participants made before successfully confirming their passwords three times. Participants made very few incorrect attempts before successfully confirming both their PINs (M = .15, Md = 0, SD = .489) and bend passwords (M = .50, Md = 0, SD = .688). A Wilcoxon Signed-Rank test found no statistically significant difference between the number of unsuccessful attempts of PINs and bend passwords (Z = -1.539, p = .124).

After learning their passwords, most participants completed the confirmation stage only once for both PINs (95%) and bend passwords (75%). Some completed it twice (PINs: 5%, Bend: 20%) and only one completed it three times for their bend password.

Rehearsing Password

After confirming their passwords three times, participants were asked to successfully re-enter them five times. This step was to ensure that participants successfully learned and memorized their passwords before leaving the first session. If participants forgot their password, they could keep re-entering it until they were successful or they could go back to the learning stage to view their password again. If they chose to view their password again, they had to complete the confirmation stage again.

Rehearsal Time: We looked at the time participants took to successfully re-enter their password once in the rehearsal stage. Out of five successful password rehearsals, we selected the rehearsal which took the least amount of time. On average, participants took 3s to successfully re-enter their PINs (M = 3s, Md = 4s, SD = 1s) and 13s to re-enter their bend passwords (M = 13s, Md = 11s, SD = 6s) once. A Wilcoxon Signed-Rank test found that participants took significantly more time to rehearse their bend passwords than their PINs (Z = -3.930, p = 0.000). A linear regression found that the number of undo button presses did not significantly predict the rehearsal time of bend passwords, b = .128, $t(18)$ = .088, p = .931. The number of undo button presses also does not explain a significant proportion of variance in password rehearsal time, R^2 = .000, $F(1, 18)$ = .088, p = .931. Thus, the longer rehearsal times for bend passwords were not due to the use of the undo button.

Incorrect Rehearsal Attempts: Participants made very few incorrect attempts before successfully re-entering both their PINs (M = .20, Md = 0, SD = .696) and bend passwords (M = .75, Md = 0, SD = 1.372) five times. A Wilcoxon Signed-Rank test found no statistically significant difference between the number of unsuccessful attempts for PINs and bend passwords (Z = -1.761, p = .078). Only two participants forgot their passwords (PIN: 1, Bend: 1) and had to go back to the learning stage to view them again.

We compared the time participants took to confirm and rehearse their passwords to determine whether their performance improved at the rehearsal stage. We found that participants took significantly less time to rehearse both their bend passwords (Z = -3.087, p = 0.002) and PINs (Z = -3.831, p = 0.000) than to confirm them. This shows that by the end of the first session participants had learned their passwords well and got progressively faster with more practice.

5.3.2 Session 2: Log-in

19 participants completed the second part of the study where they re-entered their passwords one week later.

Success Rate

We define success rate as the number of participants who successfully re-entered their password within 5 tries. The success rate of PINs was 74%, and the success rate of bend passwords was 63%. Out of 19 participants, 12 remembered their bend passwords and 14 remembered their PINs. The rest either forgot both passwords (3), their PINs (2) or bend passwords (4). A McNemar test found no statistically significant difference between the success rates (χ^2(1, N = 19) = 0.688, p = 1.00, the odds ratio is 1.63).

Number of Tries

Most participants took one try to successfully re-enter their bend passwords (M = 1.90, Md = 1, SD = 1.45) and PINs (M = 1.20, Md = 1, SD = .422). A Wilcoxon

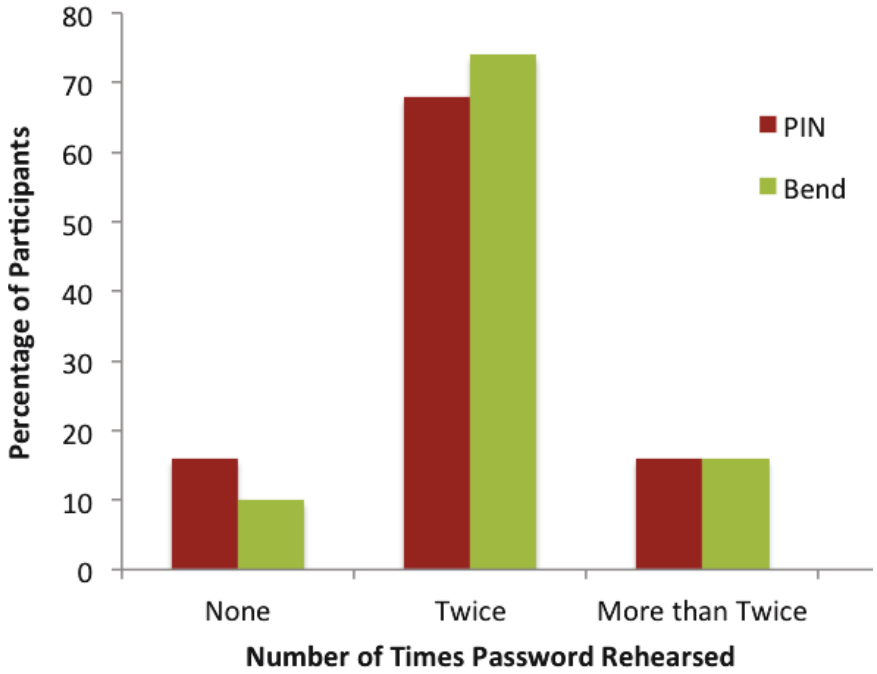

Figure 5.4: Rehearsal frequency of system assigned passwords after session 1

Signed-Rank test found no statistically significant difference between the number of tries taken to re-enter PINs and bend passwords (Z = -1.289, p = .197).

Log-in Time

The average log-in time was 34s for bend passwords (M = 34s, Md = 32s, SD = 19s) and 13s (M = 13s, Md = 9s, SD = 8s) for PINs. A Wilcoxon Signed-Rank test found that participants took more time to re-enter their bend passwords than their PINs (Z = -1.599, p = .009).

Post-Task Rehearsal

At the end of the second session, we asked participants whether they rehearsed their passwords after leaving the first session. Figure 5.4 shows participants' responses. Only one participant admitted to writing down their PIN. No participant reported writing their bend passwords; most participants stated that they did not know how to write down a bend password. This challenge in writing down bend passwords is a disadvantage for usability, but may in fact be an advantage for security because it

reduces likelihood that passwords are shared between users or that a written password is discovered and stolen.

5.3.3 Questionnaire and Interview Responses

Participants completed a questionnaire at the end of session 1, and a questionnaire and interview at the end of session 2. We grouped the responses from the questionnaires and interview into six categories: attitudes toward system assigned passwords, learnability, memorability, perceived shoulder-surfing, perceived security and likelihood of using bend passwords.

Figures 5.5 and 5.6 show the distribution of responses for the Likert scale questions in session 1 and session 2 questionnaires respectively. These questions belong to one of the five categories defined above. Table 5.1 shows results from the statistical analysis of the Likert scale questions across session 1 and 2.

Attitudes toward System Assigned Passwords

We asked participants the question "Do you prefer system assigned passwords or do you like choosing your own?" For PINs, most preferred to create their own (84%), some preferred system assigned PINs (5%) and others did not have a preference (11%). Similarly, for bend passwords most preferred to create their own passwords (84%) and others preferred system assigned passwords (16%).

Participants would prefer to choose their own PINs because they could use current PINs, existing PIN creation strategies, or personal information to make their PINs more memorable. They would prefer to choose their bend passwords because they want to use a strategy to make them more memorable. Some of their proposed strategies for creating memorable bend passwords include: choosing easy gestures or gestures located on only one side of the display and creating a pattern among the gestures (i.e., drawing a letter or picking gestures in a clockwise sequence).

Given participants' answers to our first question, we asked them "Do you think you would have remembered the passwords better if you created them yourself?". Most answered Yes for PINs (74%) and bend passwords (69%). Some answered No (Bend: 26%, PIN: 21%) and others (Bend: 5%, PIN: 5%) were undecided.

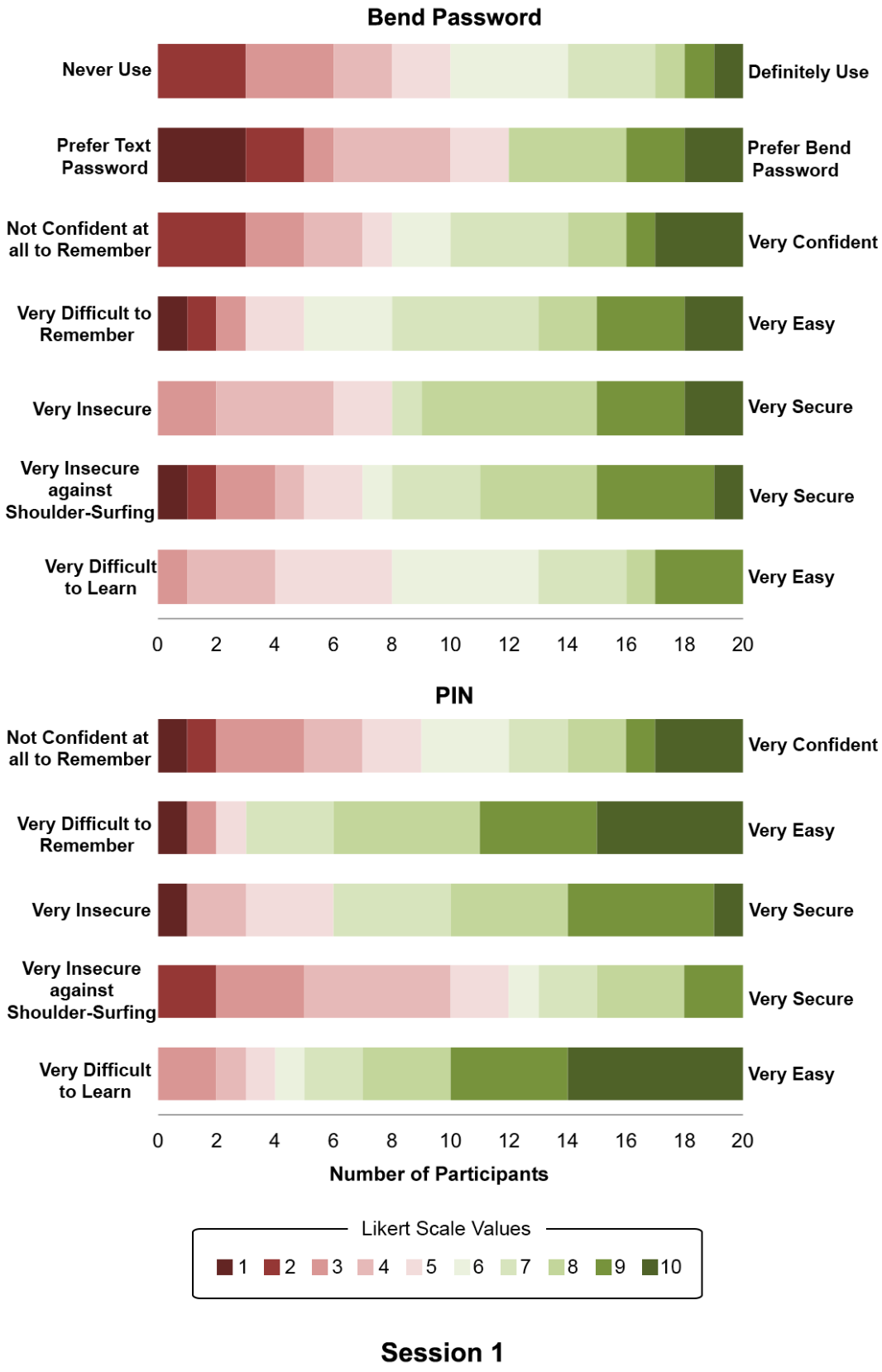

Figure 5.5: Distribution of session 1 Likert scale responses for system assigned passwords

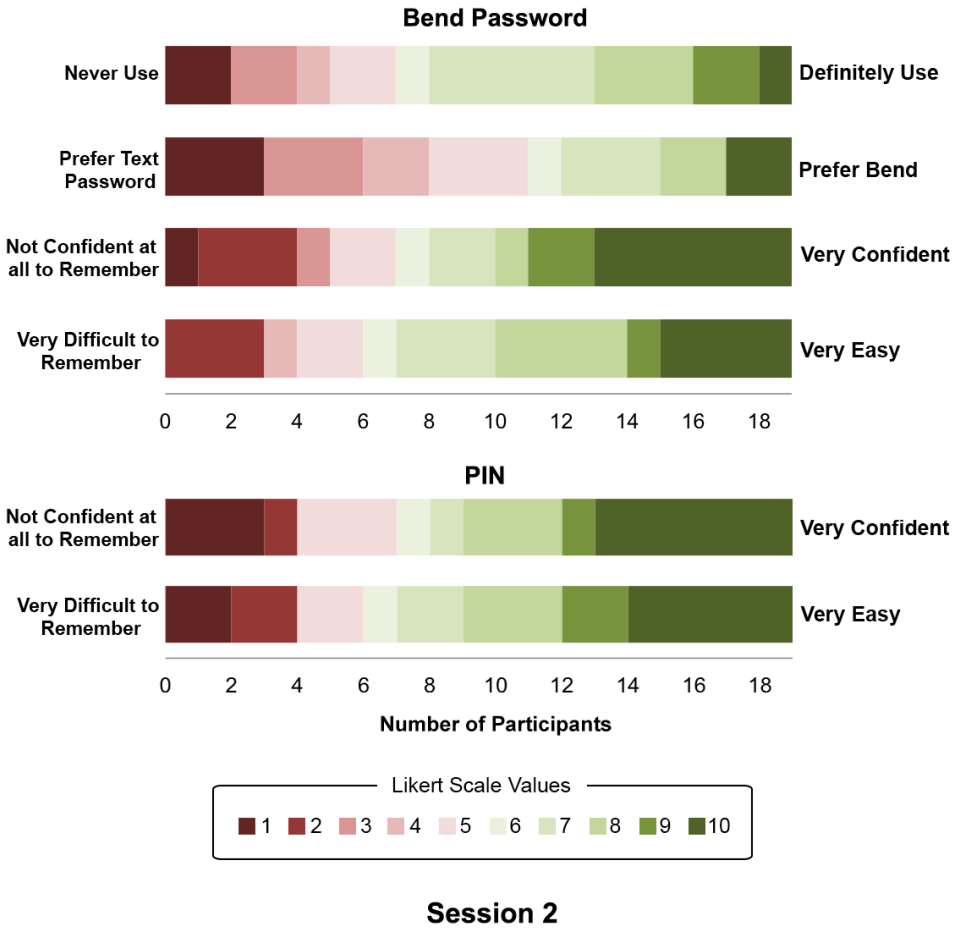

Figure 5.6: Distribution of session 2 Likert scale responses for system assigned passwords

Learnability

At the end of session 1, we used a 10-point Likert scale (1 = very difficult and 10 = very easy) to ask participants how easy it was for them to learn their bend passwords and PINs. Participants found it significantly easier to learn their PINs than their bend passwords (Table 5.1).

Memorability

At the end of both sessions, participants assessed the ease with which they remembered their new passwords (1 = very difficult and 10 = very easy) and their confidence in remembering the passwords in one week (1 = not confident at all and 10 = very

Question	Session	PIN Md (SD)	Bend Md (SD)	Stats
Learnability				
Ease of Learning	1	8.5 (2.38)	6 (1.76)	**(Z = -2.876, p = 0.004)***
Memorability				
Ease of	1	8 (2.41)	7 (2.48)	($Z = -2.127, p = 0.033$)
Remembering	2	8 (3.21)	7 (2.75)	($Z = -.506, p = 0.613$)
Confidence in	1	6 (2.76)	6.50 (2.75)	($Z = -.356, p = 0.722$)
Remembering	2	8 (3.37)	7 (3.30)	($Z = -.142, p = 0.887$)
Perceived Shoulder-Surfing				
Secure against Shoulder Surfing	1	4.50 (2.31)	7 (2.64)	($Z = -1.394, p = 0.163$)
Perceived Security				
How Secure	1	8 (2.41)	8 (2.24)	($Z = -.520, p = 0.603$)
Likelihood of Using Bend Passwords				
Use if Available	1	—	5.50 (2.34)	—
	2	—	7 (2.64)	—
Bend vs. Text	1	—	4.50 (3.16)	—
	2	—	5 (2.81)	—

Table 5.1: System assigned passwords - Questionnaire Likert scale responses grouped by category. Bold and * indicates significance.

confident). Participant responses for each session are summarized in Table 5.1.

Ease of Remembering: Using a Bonferroni adjusted alpha levels of .0125 (.05/4), we compared responses to the ease of remembering question across session 1 and 2 for bend passwords and PINs. Participants thought that it was fairly easy to remember their PINs in both sessions, and their answers did not significantly change between the sessions (Z = -2.026, p = .043). Participants also found it easy to remember their bend passwords and there was no significant change between sessions (Z = .000, p = 1.000). When comparing schemes, participants found it equally easy to remember their PINs and bend passwords (Table 5.1).

Confidence in Remembering: We also compared their confidence in remembering passwords across sessions. Bonferroni-corrected results show no statistical differences for participants' confidence at remembering PINs between sessions (Z =

-1.389, $p = .165$). In both sessions, participants were fairly confident about being able to remember their PINs. Similar results were found for bend passwords (Z = -.471, $p = .638$). When comparing PINs versus bend passwords, no significant differences were found either; participants were equally confident about being able to remember their PINs and bend passwords (statistics are available in Table 5.1).

Shoulder Surfing

At the end of session 1, participants assessed how secure their PIN and bend password were against shoulder-surfing attacks (1 = very insecure and 10 = very secure). Participants thought that both passwords would be difficult for malicious users to shoulder-surf. Statistical results are summarized in Table 5.1

Perceived Security

At the end of session 1, participants also rated the perceived security of their PIN and bend password (1 = very insecure and 10 = very secure) As shown in Table 5.1, participants felt that both passwords were very secure.

Likelihood of Using Bend Passwords

At the end of both sessions, participants reported the likelihood that they would use a bend password if it was available (1 = never and 10 = definitely). In session 1, participants were neutral and in session 2 they were slightly in favour of using bend passwords. However, no statistically significant difference were found between the two sessions (Z = -.967, $p = .334$).

Bend vs. Text

At the end of both sessions, participants identified whether they would prefer to use a text password or a bend password on a flexible display (1 = prefer text and 10 = prefer bend). In both sessions, participants were undecided and there was no significant difference between their responses across the two sessions (Z = -.071, p = .944).

Bend vs. PIN

In the post-task interview at the end of session 2, we asked participants "If you had a flexible device, would you use a bend password or a PIN?". 32% said that they would use a bend password, 32% would use a PIN, 4% would use neither and 32% were undecided.

Participants' reasons for choosing a bend password for a flexible device include the following:

- *Natural*: Using a bend password would be more "natural" to use.
- *Easy to Remember*: Bend passwords would be easier to remember than PINs because they would not interfere with other passwords users' have learned.
- *Novel*: Bend passwords would be fun and interesting to use.
- *Secure*: Bend passwords would be more secure than PINs because of their complexity (i.e., possible combination of gestures) and uniqueness.

Participants' reasons for choosing a PIN for a flexible device include the following:

- *Familiarity*: Users' are more familiar with creating and using PINs and know how to use them well. They can use their well developed PIN creation strategies to create new PINs.
- *Use of Existing PINs*: Users' have a collection of existing PINs that they can reuse. Most admitted that this was an insecure strategy for creating PINs but used it anyway because of its convenience.
- *Disadvantages of bend passwords*: Some disadvantages of bend passwords were mentioned, namely that they take more time to enter, do not allow one handed gestures, and would be easy to shoulder-surf.

Participants who were undecided stated that they would need more experience with the system before choosing the type of password they would use. Their choice was also dependent on the context of use. For secure applications, they would use a bend password because its complexity would make it more secure but for insecure applications, they would use a PIN because it is faster to enter.

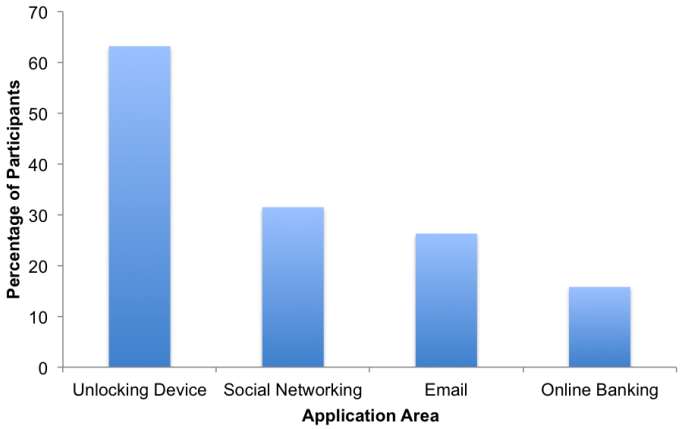

Figure 5.7: Application areas of system assigned bend passwords

Application Areas of Bend Passwords

We provided participants with several application areas of bend passwords and asked them to select areas where they would use a bend password. Participants could select multiple application areas. Figure 5.7 shows participants' responses. Participants liked using bend passwords for unlocking their device, and thought that they could also be used for email and social networking websites.

5.3.4 User Feedback

We asked participants two open-ended questions in the questionnaire for session 1 in both our studies. The first question was "what do think worked well with the bend password system?" and the second was "what do you think could be improved with the bend password system?". Since we asked these questions in both of our studies (user chosen and system assigned), we decided to group the responses from both studies. 25 participants answered these questions in our first study and 20 answered it in the second study, giving us a total of 45 responses.

Features that Worked Well

During our thematic analysis, six themes emerged for the question "what do think worked well with the bend password system?": ease of use, system feedback, gestures, security, preference over touch and novelty.

Ease of Use: Some participants (28%) commented that the system was easy to use. They found the gestures easy to learn and perform, and thought that they registered well in the system. They also found it easy to remember the passwords created by using the available gesture set. Some of their comments were "the gestures work very well with this password system, as they are relatively more enjoyable and easier to remember", "the device itself was pleasant to use, and bending it was very easy once you became accustomed to it" and "the gestures were fairly easy to remember, which was good".

Gestures: 18% of participants liked the type and variety of gestures available on the prototype. They thought that the variety of gestures would allow them to create a more secure password. Participants preferred some gestures over others. Specifically, they liked single gestures (i.e., bending corners up or down) and diagonal gestures. Some of their comments include "[I liked] the fact that there were many different gestures. Compared to numbers this makes this password system relatively safer", "there were various combinations that could be made, allowing for variety" and "the bend combinations are neat".

System Feedback: 13% of participants liked the type of feedback provided by the system upon password entry. Specifically, they liked the visual feedback provided by the LED light and the UI, and the audio feedback provided by the pico-projector. Some of their comments include "the sound and visual (LED) response when inputting the password was very helpful in picking it up quickly", "[I liked] the multi-light response coupled with the on-screen readout showed when input was received and what kind it was" and "[I liked] the sound and LED flash while creating the password".

Novelty: Others (11%) liked the system because of its novelty. Some of their comments include "it is a new system in which passwords can be created on which is very innovative and fresh" and "It is a lot more accessible to even new users. It is also new innovative technology, and new technology is always fun."

Security: A few participants (6%) mentioned bend passwords security. Specifically, they thought these passwords would be harder for attackers to break or shoulder-surf. With regards to shoulder-surfing, participants thought bend passwords would be hard to shoulder-surf when entered really quickly by the user.

Preference over Touch: A few participants (6%) liked that they could enter a password without using the touch-based interaction of their mobile device. This would be beneficial in situations such as extreme weather (e.g., winter), where users have to take off their gloves to unlock their phone. It would also be beneficial to users who have trouble pressing the small keys on a touch-based keypad (e.g., users with bigger hands). Some participant comments include "one does not need to touch the screen to enter a password, and it can be done with a few gestures" and "I liked that it was more interactive and generally I have problems hitting the small numbers on my smart phone for password entry but did not have this problem with this password system".

System Improvements

Our analysis revealed three general themes in responses to the question "what do you think could be improved with the bend password system?": gesture accuracy and speed, complex gestures, and security.

Gesture Accuracy and Speed: Many participants (44%) found that the accuracy and speed of the gestures could be improved. The accuracy issue applied more to multi-gestures. Sometimes when participants performed a multi-gesture (by simultaneously bending two corners), the system incorrectly registered it as a single gesture depending on the degree of "bend" applied to each corner. The prototype also had limits to how fast participants could perform a series of gestures.

However, it is important to note that most of the comments (70%) about gesture speed and accuracy were from our first user study, where we used a very early version of our prototype. After the first study, we improved our prototype using the comments provided by participants. We used the improved prototype in our second study, where very few participants had problems with gesture speed and accuracy.

Complex Gestures: Some participants (22%) wanted to see more complex gestures and a larger gesture set on the prototype. They wanted to see gestures such as twisting the display (e.g., bending one corner up and another down), rolling the display and bending the right and left sides of the display using only one hand. Their reasons for wanting these gestures include being able to perform one-handed gestures

and having a larger gesture set which would result in more secure passwords.

Security: A few participants (9%) expressed concern over the shoulder-surfing susceptibility of bend passwords. They believed that malicious users could easily observe the gesture entry of their passwords. Some suggested solutions to this problem include adding smaller (i.e., more subtle) gestures to the prototype and increasing the speed with which users can enter gestures.

5.4 Discussion

In this study, we looked at system assigned bend passwords and compared the results with system assigned PINs.

We found that participants took significantly more time to learn their bend passwords than their PINs. Some of these differences were due to the flexible display prototype, and because participants did not have an effective strategy for learning system assigned bend passwords. Most users had used system assigned PINs in the past and thus had strategies for learning them effectively. Participants used a variety of different strategies for learning and remembering their PINs and bend passwords. For PINs, the most common strategies were chunking, finding a memorable digit pattern and rehearsing the PIN verbally until it was memorized. All these strategies involved some type of rehearsal. For bend passwords, the most common strategy was repeatedly entering the password into the system until it was memorized. With this strategy, participants learned and remembered their bend passwords using their procedural memory. This strategy of repeatedly entering passwords into the system also contributed to the longer bend password learning times.

After learning their bend passwords, some participants forgot them at the confirmation stage and had to complete the learning stage again. We found that participants completed the learning stage significantly more for bend passwords than for PINs. After learning their passwords, most participants were able to successfully confirm and rehearse their bend passwords and PINs. Participants took significantly more time to confirm and rehearse their bend passwords than their PINs. The longer bend password learning times were due to the prototype, and do not represent participants' ability to recall their passwords. To validate this, we looked at the number

of incorrect password confirmation/rehearsal attempts, and found no significant difference between bend passwords and PINs.

Most participants successfully remembered their bend passwords and PINs within one try, a week after learning them. There were no significant differences between the success rates and number of tries taken to re-enter bend passwords and PINs. They also found it fairly easy to remember their passwords and were confident about remembering them in a week. However, participants took significantly more time to re-enter their bend passwords than their PINs. The longer bend re-enter times were due to the way participants' recalled their bend passwords. For PINs, most participants re-entered them immediately after starting the task, while for bend passwords they tried to remember the movements they made when they learned their password. These participants moved their hands on specific locations of the device and entered gestures that "felt" right. It is also important to note that participants could easily verbally rehearse/recall their PINs after leaving the first session, but had no easy way of rehearsing their bend passwords. Some participants rehearsed their bend passwords by performing the gestures on an imaginary flexible display, however we believe this was not an effective rehearsal method for bend passwords.

Qualitative data revealed that participants found both their PINs and bend passwords to be fairly secure. They found their PINs slightly easy to shoulder-surf and their bend passwords slightly difficult to shoulder-surf. However, no significant difference was found between participants' perception of the shoulder-surfing susceptibility of these passwords. When asked whether participants would use a bend password on flexible display devices in the future, participants were undecided in session 1 and were slightly positive in session 2. Participants were undecided on whether they would use a text or bend password. Similar results were found when we compared the likelihood of using bend passwords to PINs. We believe that participants were undecided because they need more experience with bend passwords before deciding whether to use them in the future. When asked which type of applications participants would use a bend password for, the majority answered they would use it to unlock their device.

We combined the user feedback from our user chosen and system assigned passwords' user studies to determine features of the system that participants liked and

features that could be improved. Some participants liked the available gestures in the system and felt that they could easily use them to create a memorable password. Others liked the feedback provided by the system, its novelty and the ability to enter a password without using the touch based input of the device. Many participants wanted to see improvements in the speed and accuracy of gestures, and others wanted the ability to use more complex gestures on the device. In our study, we provided participants with a set of simple and easy to learn gestures, because we wanted them to focus on the password task instead of trying to learn the gestures. However, many participants wanted to use complex gestures in their bend passwords, such as twisting (i.e., bend one corner up and another down) and rolling the display.

In the next chapter, we compare the results from our user chosen and system assigned password user studies to determine which password is viewed most favourably by users.

5.5 Limitations

Our study had the same prototype limitations outlined in chapter 4. Another limitation of our study is in the learning phase of the PIN condition. While learning their bend passwords, participants could practice their password by entering it repeatedly on the device. However, they memorized their PINs without entering them in the learning phase.

Chapter 6

Comparison of User Chosen and System Assigned Passwords

An advantage of system assigned passwords is that they are secure. However, one of their disadvantage is that users have trouble remembering them. In our second study, many users stated that they would like to create their own passwords rather than use something assigned by the system. Their choice applied to PINs and bend passwords, even though they did not have any good password creation strategies for bend passwords. In this section, we compare the results from our user chosen and system assigned passwords user studies to determine which type of password is viewed most favourably by users on different measures.

In our user chosen passwords study, participants created passwords of varying lengths. There was a required minimum length (6 digits for PINs and 5 for bend passwords), but many created passwords above the required minimum. Passwords in our system assigned user study had a fixed length (6 digits for PINs and 5 gestures for bend passwords). To compare data from both studies, we selected the set of participants in our first study (user chosen) who created a 5 gesture bend password or 6 digit PIN, and compared them with participants from our second study (system assigned). We first compare user chosen and system assigned PINs, followed by a comparison of user chosen and system assigned bend passwords.

We found no differences between user chosen and system assigned PINs on the performance measures. However, we uncovered several differences with respect to user opinions.

6.1 PINs

25 participants completed the user chosen passwords user study. Out of these 12 created a PIN with 6 digits. We compare these 12 participants with 20 participants from our system assigned user study. We compare the quantitative and qualitative

data of these participants. For quantitative data, we look at the PIN creation/learning time, confirmation time and number of tries, rehearsal time and number of tries, PIN re-enter time, re-enter success rates and number of tries taken for successful PIN re-entry. For qualitative data, we look at participants' responses to the Likert scale questions measuring perceived memorability, security and risk of shoulder-surfing.

6.1.1 Creation

We look at the amount of time participants took to create their password in the first study and learn their random password in the second study. On average, participants took 35s (M = 35s, Md = 35s, SD = 15s) to create their own password and 28s to learn their random password (M = 28s, Md = 17s, SD = 30s). A Mann-Whitney U test found no significant difference between the creation and learning times ($U = 73$, $p = .067$).

6.1.2 Confirmation

Participants confirmed their passwords three times in both studies. We look at the amount of time participants took to confirm their PINs once, and the number of times they completed the confirmation stage.

Time: On average, participants took 5s to confirm their user chosen PINs (M = 5s, Md = 5s, SD = 1s) and system assigned PINs (M = 5s, Md = 4s, SD = 1s). A Mann-Whitney U test found no significant difference between the confirmation times ($U = 118$, $p = .936$).

Number of Tries: Most participants completed the confirmation stage once for both their user chosen PINs ($M = 1.08$, $Md = 1$, $SD = .289$) and their system assigned PINs ($M = 1.05$, $Md = 1$, $SD = .224$). A Mann-Whitney U test found no significant difference between the number of times the confirmation stage was completed in both studies ($U = 116$, $p = .711$).

6.1.3 Rehearsal

In both studies, participants successfully rehearsed their passwords five times. We look at the amount of time participants took to rehearse their PIN once and the

number of times they completed the rehearsal stage.

Time: On average, participants took 4s (M = 4s, Md = 4s, SD = 0s) to successfully rehearse their user chosen PINs and 3s (M = 3s, Md = 4s, SD = 1s) to rehearse their system assigned PINs. A Mann-Whitney U test found no significant difference between the rehearsal times of the two studies (U = 103, p = .492).

Number of Tries: Most participants only completed the rehearsal stage once for both user chosen PINs (M = 1, Md = 1, SD = 0) and system assigned PINs (M = 1.05, Md = 1, SD = .224), and a Mann-Whitney U test found no significant difference between the two studies. (U = 114, p = .439).

6.1.4 Re-enter

A week after creating/learning their PINs, participants returned to the lab to re-enter them. They had five tries to successfully re-enter their PINs. 9 participants completed the PIN re-enter task for user chosen PINs, and 19 completed the task for system assigned PINs. In this section, we compare the re-enter success rates, time and number of tries across the user chosen and system assigned passwords user studies.

Success Rates: 89% of participants successfully remembered their user chosen PINs and 74% remembered their system assigned PINs. A Fisher's Exact test found no significant difference between the success rates of the two studies (p = .630).

Time: On average, participants took 10s to successfully re-enter their user chosen PINs (M = 10s, Md = 10s, SD = 2s) and 12s to re-enter their system assigned PINs (M = 12s, Md = 9s, SD = 7s), and a Mann-Whitney U test found no significant difference between the re-enter times (U = 55, p = .973).

Number of Tries: Most participants successfully remembered both their user chosen (M = 1.25, Md = 1, SD = .707) and system assigned PINs (M = 1.36, Md = 1, SD = .633) in one try. A Mann-Whitney U test found no significant difference between the number of tries participants took to successfully re-enter their user chosen and system assigned PINs (U = 48.5, p = .485).

Question	Session	UCP Md (SD)	SAP Md (SD)	Stats
Memorability				
Ease of Remembering	1	10 (.452)	8 (2.40)	**(U = 43.5, p = 0.002)***
	2	10 (2.32)	8 (3.21)	**(U = 44.5, p = 0.037)***
Confidence in Remembering	1	9.50 (.778)	6 (2.76)	**(U = 33.0, p = 0.001)***
	2	10 (2.42)	8 (3.37)	**(U = 46.5, p = 0.043)***
Perceived Shoulder-Surfing				
Secure against Shoulder Surfing	1	8 (1.96)	4.50 (2.31)	**(U = 63.0, p = 0.024)***
Perceived Security				
How Secure	1	7.50 (2.33)	7 (2.27)	$(U = 117.5, p = 0.921)$

Table 6.1: Comparison of User Chosen (UCP) and System Assigned PINs' (SAP) Likert scale responses. Bold and * indicates significance.

6.1.5 Questionnaire Responses

Participants completed questionnaires at the end of session 1 and 2 in both studies. In this section, we compare their responses to the Likert-scale questions in the questionnaires of both user studies. We grouped the Likert-scale questions into three categories: memorability, perceived security and perceived shoulder-surfing. Table 6.1 shows participants' responses to the Likert-scale questions in both user studies.

Memorability: We asked participants two questions to measure the perceived memorability of their PINs. The first question asked them how easily they could remember their PINs in session 1 and 2. The second question asked them how confident they felt about remembering their PINs a week after session 1 and 2. Participants answered these questions at the end of session 1 and 2 of both studies.

Participants found it significantly easier to remember their user chosen PINs than their system assigned PINs in both sessions. Participants were also significantly more confident about remembering their user chosen PINs than their system assigned PINs in both sessions.

Perceived Security: We asked participants to rate the security of their user

chosen and system assigned PINs. Participants found both their user chosen and system assigned PINs to be very secure, and there was no significant difference between participants' responses to this question in the two studies.

Perceived Shoulder-Surfing: We asked participants how easily malicious users could shoulder-surf their user chosen and system assigned PINs. Surprisingly, participants thought that it would be significantly easier for someone to shoulder-surf their system assigned PINs than their user chosen PINs.

6.1.6 Summary

We found no significant difference between participants' performance in the user chosen and system assigned passwords' user studies. However, results from their questionnaire data show that participants thought it was significantly easier to remember their user chosen PINs, were more confident about remembering them in the future, and thought that they would be difficult to shoulder-surf. Some of these results are not surprising, given that many participants in the user chosen passwords study, created PINs containing parts of their personal information (e.g., birth date, student number, phone number and street address) or parts of their existing PINs. Thus, they would definitely have an easier time remembering these PINs than random PINs assigned by the system. They would also be more confident about remembering these PINs in the future. It is interesting that participants thought their user chosen PINs would be harder to shoulder-surf than their system assigned PINs. One explanation of this result could be that, since participants can remember their user chosen PINs better, they may be able to re-enter them quickly on a keypad and make it difficult to shoulder-surf for malicious users. Another explanation could be that participants may have picked a sequence of digits for their user chosen PINs that would be difficult to shoulder-surf.

6.2 Bend Passwords

Out of 25 participants who completed the user chosen passwords user study, 11 created a bend password with 5 gestures. We compare these 11 participants with 20 participants from our system assigned user study. We compare the quantitative and

qualitative data of these participants.

6.2.1 Creation

On average, participants took 54s to create their bend passwords in the first study (M = 54s, Md = 26s, SD = 55s) and 188s to learn their system assigned passwords in the second study (M = 188s, Md = 146s, SD = 108s). A Mann-Whitney U test found that participants took significantly more time to learn a system assigned bend password than creating their own bend password (U = 24, p = .000).

6.2.2 Confirmation

In both studies, participants successfully confirmed their bend passwords three times in the first session. We compare the time taken to confirm a bend password once and the number of times the confirmation stage was completed.

Time: On average, participants took 16s to confirm their user chosen bend passwords (M = 16s, Md = 14s, SD = 7s) and 21s to confirm their system assigned bend passwords (M = 21s, Md = 18s, SD = 12s). A Mann-Whitney U test found no significant difference between the amount of time participants took to confirm their user chosen and system assigned bend passwords (U = 73.5, p = .131).

Number of Tries: Most participants completed the confirmation stage twice for their user chosen bend passwords (M = 2.27, Md = 2, SD = 1.49), and once for their system assigned bend passwords (M = 1.35, Md = 1, SD = .587). A Mann-Whitney U test found no significant difference between the number of times the confirmation stage was completed for user chosen and system assigned bend passwords (U = 72.5, p = .075).

These results show that participants were able to successfully confirm their bend passwords in both studies, and there were no significant differences between their performances across the two studies. Most participants were able to confirm their bend passwords quickly and remembered them after creating/learning them.

6.2.3 Rehearsal

In both studies, participants successfully rehearsed their bend passwords five times in the first session after confirmation. We compare the amount of time participants took to rehearse their bend passwords once and the number of times they completed the rehearsal stage.

Time: On average, participants took 15s to successfully rehearse their user chosen bend passwords (M = 15s, Md = 11s, SD = 6s) and 13s to rehearse their system assigned bend passwords (M = 13s, Md = 11s, SD = 6s). A Mann-Whitney U test found no significant difference between the amount of time participants took to rehearse their user chosen and system assigned bend passwords ($U = 95.5$, $p = .547$).

Number of Tries: Most participants completed the rehearsal stage once for both user chosen ($M = 1$, $Md = 1$, $SD = .000$) and system assigned bend passwords ($M = 1.05$, $Md = 1$, $SD = .224$). A Mann-Whitney U test found no significant difference between the number of times the rehearsal stage was completed in both studies ($U = 104.5$, $p = .458$).

These results show that participants were able to successfully rehearse their bend passwords in both studies, and there were no significant differences between their performance across the two studies. Most participants were able to rehearse their passwords quickly and remembered them after the confirmation stage.

6.2.4 Re-enter

In both studies, participants returned to the lab a week after creating/learning their bend passwords. 9 participants completed the re-enter task for user chosen bend passwords, and 19 completed it for system assigned bend passwords. We compare the success rates and time and number of tries taken to successfully re-enter the bend passwords.

Success Rates: 67% of participants successfully re-entered their user chosen bend passwords and 63% successfully re-entered their system assigned bend passwords. A Fisher's Exact test found no significant difference between the success rates of the two studies ($p = 1.000$).

Time: On average, participants took 34s to successfully re-enter their user chosen

Question	Session	UCP Md (SD)	SAP Md (SD)	Stats
Memorability				
Ease of Remembering	1	8 (1.99)	7 (2.48)	**(U = 61.0, p = 0.041)***
	2	7 (3.43)	7 (2.75)	($U = 79.0, p = 0.746$)
Confidence in Remembering	1	8 (2.02)	6.50 (2.75)	($U = 71.5, p = 0.109$)
	2	9 (3.13)	7 (3.30)	($U = 72.0, p = 0.496$)
Perceived Shoulder-Surfing				
Secure against Shoulder-Surfing	1	4 (2.84)	7 (2.64)	($U = 77.5, p = 0.175$)
Perceived Security				
How Secure	1	5 (1.97)	8 (2.41)	($U = 64.0, p = 0.054$)
Likelihood of Using Bend Passwords				
Use if Available	1	7 (2.07)	6 (2.82)	($U = 98.5, p = 0.632$)
	2	6 (2.83)	7 (2.64)	($U = 83.0, p = 0.901$)
Bend vs. Text	1	5 (2.77)	5 (2.75)	($U = 108.5, p = 0.950$)
	2	5 (2.86)	5 (2.81)	($U = 71.5, p = 0.486$)

Table 6.2: Comparison of User Chosen (UCP) and System Assigned Bend Passwords' (SAP) Likert scale responses. Bold and * indicates significance.

(M = 34s, Md = 35s, SD = 9s) and system assigned bend passwords (M = 34s, Md = 32s, SD = 19s). A Mann-Whitney U test found no significant difference between the password re-entry times of both studies (U = 27, p = .398).

Number of Tries: Most participants took one try to successfully re-enter their user chosen (M = 1.50, Md = 1.50, SD = .548) and system assigned bend passwords (M = 1.92, Md = 1, SD = 1.38). A Mann-Whitney U test found no significant difference between the number of tries participants took to successfully re-enter their user chosen and system assigned bend passwords (U = 34.5, p = .876).

These results show that after a week, most participants successfully remembered both their user chosen and system assigned bend passwords, and re-entered them quickly with very few errors. They also show no significant differences between participants' performance on the password re-enter task in the user chosen and system assigned passwords user studies.

6.2.5 Questionnaire Responses

Participants completed several questionnaires at end of session 1 and 2 in both user studies. In this section, we compare participants' responses to the Likert-scale questions in the questionnaires of both user studies. We grouped the Likert-scale questions into four categories: memorability, perceived security, perceived shoulder-surfing and likelihood of using bend passwords. Table 6.2 shows participants' responses to the Likert-scale questions in both user studies, and the statistical analysis of the responses.

Memorability: We asked participants two questions to measure their perceived memorability. In the first question, we asked participants how easily they remembered their bend passwords in session 1 and 2. Participants thought it was significantly easier to remember their user chosen bend passwords than their system assigned passwords in session 1. However, no such difference was found in session 2.

In the second question, we asked participants how confident they felt about remembering their bend passwords a week after session 1 and 2. Participants were fairly confident about remembering their user chosen and system assigned bend passwords in session 1 and session 2, and no significant differences were found between the passwords in either sessions.

Perceived Security: We asked participants to rate the security of their user chosen and system assigned bend passwords. Participants found both passwords to be fairly secure, and there was no significant difference between their perceived security of user chosen and system assigned bend passwords.

Perceived Shoulder-Surfing: We asked participants how easily a malicious user could shoulder-surf their user chosen and system assigned bend passwords. Participants found their user chosen bend passwords slightly easy to shoulder-surf and their system assigned passwords slightly difficult to shoulder-surf. However, these differences were not statistically significant.

Likelihood of Using Bend Passwords: At the end of both sessions, we asked participants two questions measuring their likelihood of using user chosen and system assigned bend passwords in the future. In the first question, we asked participants if given the option would they use a bend password on a flexible display device. In

both sessions, participants were slightly positive in their response for user chosen and system assigned bend passwords, and there were no significant differences between their responses. Their responses also did not significantly change between session 1 and 2.

In the second question, we asked participants if given the choice, would they use a text or bend password on a flexible display device. In both sessions, participants were neutral in their response for user chosen and system assigned bend passwords, and there were no significant differences between their responses. Their responses also did not significantly change between session 1 and 2.

6.3 Discussion

In this section, we compared the results of our user chosen and system assigned passwords user studies to determine the differences between user chosen and system assigned passwords. For PINs, we did not find any significant differences between participants' performance on the user chosen and system assigned PIN tasks. However, questionnaire data revealed that participants' preferred user chosen PINs over system assigned PINs. Specifically, they found them easier to remember and were more confident about remembering them in the future. Because of this, we believe that if participants were required to remember their system assigned PINs for more than a week, their performance on the PIN re-enter task would have decreased.

For bend passwords, there were no significant differences between participants' performance on the user chosen and system assigned passwords tasks. Participants found their user chosen bend passwords significantly more memorable in session 1, but found them equally memorable in session 2. With the exception of this difference, there were no significant difference between participants' qualitative data for user chosen and system assigned bend passwords. Participants found both types of passwords easy to remember and were fairly confident about remembering them after a week. No significant differences were found in participants perception of password security, including their susceptibility to shoulder-surfing attacks. We see these results as positive. In the next chapter, we look at the real shoulder-surfing susceptibility of bend passwords and compare the results with PINs.

Chapter 7

Shoulder Surfing User Study

A common problem with any authentication scheme is its susceptibility to shoulder-surfing attacks. In these attacks, attackers learn passwords by observing users enter them. This can be especially problematic in a public space, such as a bus stop or a coffee shop. In the context of bend passwords, the visible physicality of bend gestures may make them susceptible to shoulder-surfing attacks, which in turn might reduce user adoption. To address this issue, we designed a user study to determine the shoulder-surfing susceptibility of bend passwords and compared the results with PINs. We chose PINs as our comparison group because they are the most commonly used authentication mechanism on mobile devices. In our study, the experimenter played the role of a victim and participants played the role of malicious users, similar to Tari et al.'s [35] and Schaub et al.'s [31] shoulder-surfing user studies. Participants observed the experimenter enter a series of bend passwords on a flexible display, and were given an opportunity to guess each of the observed passwords. This process was repeated for a series of PINs on a mobile phone. This work was approved by Carleton University's Research Ethics Board.

As this is an exploratory study investigating the shoulder-surfing susceptibility of bend passwords, we do not state a specific hypothesis for the study.

7.1 Methodology

We introduced participants to our flexible display prototype and bend gesture authentication scheme. Participants were shown all of the available bend gestures and were shown how to create a bend password using the gestures. After the demonstration, participants were given an opportunity to practice each gesture and ask any questions. Once participants were comfortable with the prototype and authentication scheme, they proceeded to the shoulder-surfing task.

Figure 7.1: Shoulder-surfing study setup

In the shoulder-surfing task, the right-handed experimenter sat at a desk and entered eight passwords on the first device. The order of the devices (flexible display or mobile phone) was counterbalanced. The experimenter privately reviewed each password immediately before entering it to ensure consistency and reduce the risk of errors. Participants stood behind the experimenter, to their right, or to their left and observed the password entry. They were allowed to move around and change their position to find the best viewing angle. Figure 7.1 shows the set-up of the experiment. During observation, participants could take notes on a piece of paper provided to them at the beginning of the study. After observing each password entry, participants were given three tries to correctly guess the observed password. After observing and guessing eight passwords on one device, the experimenter switched the device and the process was repeated on the second device. After completing the shoulder-surfing tasks, participants completed an online questionnaire and a short interview, providing their opinions and perceptions of shoulder-surfing bend passwords and PINs. Figure 7.2 illustrates our study methodology.

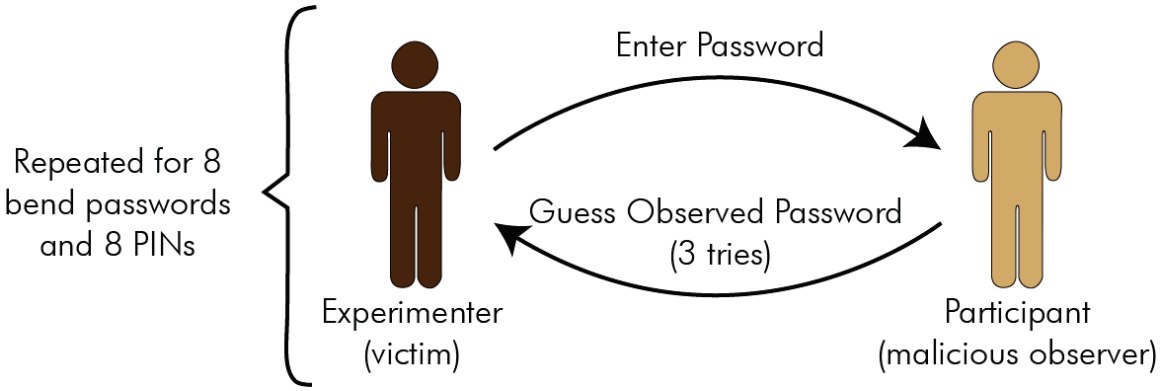

Figure 7.2: Participants observed and guessed eight passwords on a flexible display device and a mobile phone

7.1.1 Passwords

Participants observed 8 passwords on each the flexible display and mobile phone. These passwords were selected using a factorial design, with password type (bend or PIN), hand position (moving or not) and password strength (low or medium) as variables. This gives us four categories of passwords for each password type. The experimenter entered two passwords for each combination of factors, for a total of 16 passwords per participant (2 password types $\times$ 2 hand movements $\times$ 2 strength levels $\times$ 2 trials). For each type, the presentation order of passwords was counterbalanced using a Latin square design. We selected bend passwords with a variety of gesture locations and directions, representative of the passwords created in our user chosen password study. We selected random looking PINs with no obvious pattern.

For bend passwords, participants did not receive any visual feedback during observation, such as the asterisk appearing in the password field. However, they did receive this feedback when they guessed the password. This is a limitation of our study, but we believe it did not significantly affect the results because most participants focused on the placement of the experimenter's hands on the device rather than the UI. For PINs, we used the alphanumeric keyboard of the mobile device rather than the larger commonly used PIN keypad (Figure 7.3) because we believe the smaller keys of the alphanumeric keyboard would make it harder to shoulder-surf PINs. On mobile devices, the last character entered is normally displayed briefly before being obfuscated with a dot or star. We initially had this feature enabled for PINs and pilot tested our

Figure 7.3: (a) Large alphanumeric keyboard used in the shoulder-surfing study. (b) Small numerical keypad commonly used for PIN entry.

study with two participants. However, this made the PINs so easy to shoulder-surf that participants correctly guessed all PINs. We decided that this would not provide a very effective comparison condition and disabled this feature before running our actual study. For PINs, only a dot is displayed with each entered digit/gesture. In effect, we tried to devise the most difficult comparison condition possible to avoid overstating bend passwords' resistance to shoulder-surfing.

7.1.2 Hand Position

For hand position, *moving* means the experimenter's hands were moving across the device during password entry and *not-moving* means their hands were stationary. For bend passwords, the experimenter either positioned their hands on two corners of the device and performed gestures using only those corners (hand-not-moving) or performed gestures using all four corners of the device (hand moving), which required repositioning of the hands. For PINs, the experimenter either held the phone in their right hand and entered the PIN using only their right thumb (hand-not-moving) or held the phone in their left hand and entered the PIN using their right hand, moving it across the screen (hand moving).

	Password Strength	
Password Type	**Low (20 bits)**	**Medium (34 bits)**
PIN	6 digits	10 digits
Bend	5 gestures	8 gestures

Table 7.1: Length of passwords shoulder-surfed in the user study

7.1.3 Password Strength

On both the flexible display and mobile device, we selected passwords with two different theoretical password strengths to determine whether password strength affects shoulder-surfing success rates. Specifically, we chose passwords with a theoretical password strength of approximately 20 bits and 34 bits. We consider a password strength of approximately 20 bits to be "low" and a strength of 34 bits to be "medium". We chose 20 bits as low strength because it was the theoretical password space of passwords created in our user chosen passwords study, and we chose 34 bits as medium strength to match the length of bend passwords to 8 character alphanumeric text passwords. Table 7.1 shows the length of PINs and bend passwords used in our study.

7.2 Participants

Our 9 participants (7 male) had an average age of 28 years. All participants had participated in a prior study on bend gestures within the last 6 months (6 had participated in the user chosen passwords study). We selected participants with prior flexible display experience to ensure they had practice using bend gestures in the past, making them moderate users. We believe this would make them more realistic bend password shoulder-surfers. All participants were aware of shoulder-surfing attacks on mobile devices and were able to describe them. Participants completed the study in a quite room of our lab and were given $10 compensation.

7.3 Results

We measured shoulder-surfing success rates, degree of correctness of guessed passwords and user perceptions. Most participants stood behind and slightly to the right of the experimenter because this gave them the best viewing angle. Some changed their position to their improve viewing angle. None stood to the left of the experimenter.

7.3.1 Success Rates

We defined success rate as the number of passwords participants' successfully guessed within three attempts after shoulder-surfing the password. For both PINs and bend passwords, the success rates were very low. Out of 144 passwords (16 passwords $\times$ 9 participants), a total of 3 were guessed correctly: one bend and two PINs. This shows that users found it extremely difficult to shoulder-surf both bend passwords and PINs.

7.3.2 Degree of Correctness

Given the low success rates, we conducted post-hoc analysis to explore the composition of users' guesses using Levenshtein distance [26]. Levenshtein distance is commonly used to measure the dissimilarity of two strings. It computes the number of single character edits (inserts, deletes, substitutions) needed for one string to match another (e.g., *car* to *cat* = Levenshtein distance of 1). A distance of 0 indicates two identical strings. When two strings are completely different, the distance is equal to the length of the longest string.

In our study, PINs could be compared directly and we represented each bend gesture as a single character to form a string for a bend password. For each participant, the Levenshtein distance was calculated to compare the original password with each of their three guessed passwords. Since we performed two trials for each category of password, we selected the trial with the lowest Levenshtein distance, which gave us an end result of 8 passwords per participant (4 bend passwords and 4 PINs).

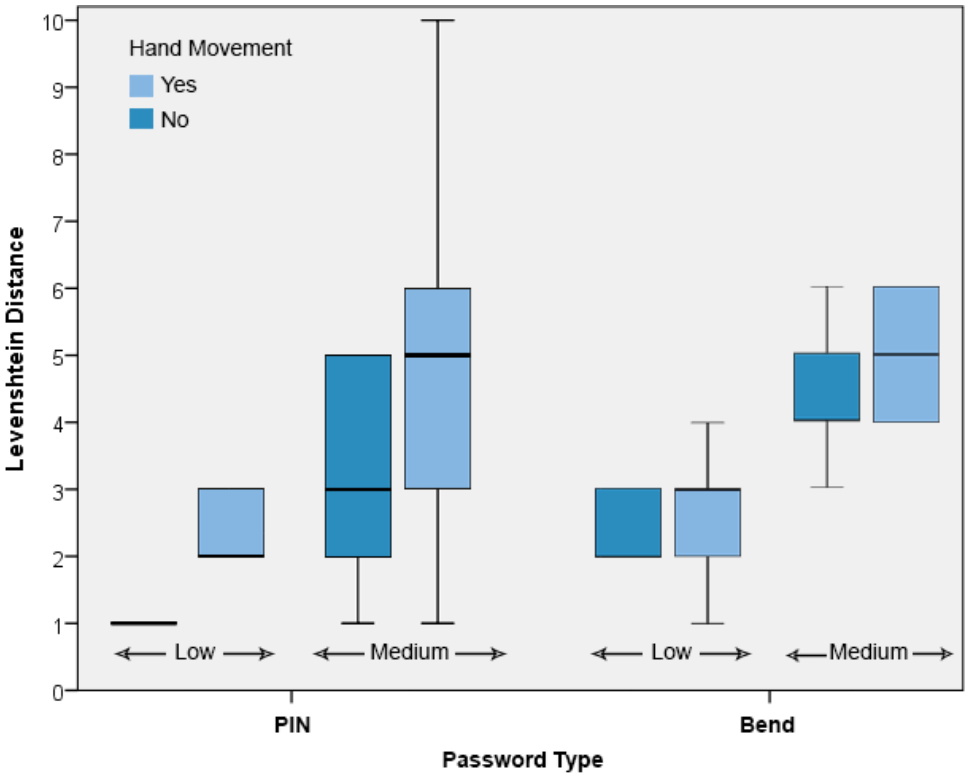

Figure 7.4: Levenshtein distance for PINs and bend passwords. Low and medium are the theoretical password strengths of the passwords.

Figure 7.4 shows the Levenshtein distances for PINs and bend passwords. Because this was post-hoc exploration with a small sample, we opted not to conduct any statistical analysis. However, the figure suggests that most users had several gestures/digits incorrect in their guesses; these were not simply one-off errors. It also suggests that passwords with hand movements or longer lengths were more difficult, but this needs further testing.

7.3.3 Strategies Used for Shoulder Surfing

Participants rated the difficulty of shoulder-surfing passwords using a 10-point Likert scale question (1 = very easy, 10 = very difficult). Figure 7.5 shows the distribution of their responses. Participants found it very difficult to observe and replicate both bend passwords ($M = 7.78$, $Md = 9$, $SD = 3.07$) and PINs ($M = 7.56$, $Md = 8$, $SD = 2.55$). A Wilcoxon Signed-Rank test showed that participants found both types of

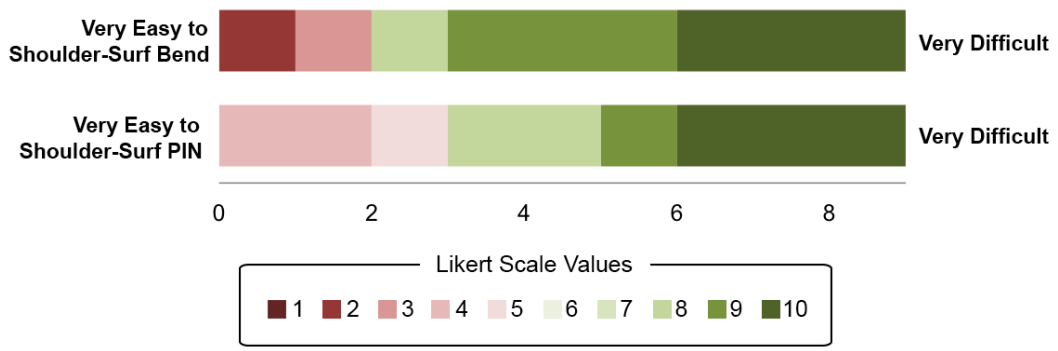

Figure 7.5: Distribution of Likert scale responses for the shoulder-surfing study

passwords equally difficult to shoulder-surf (Z = -.212 p = 0.832).

We further asked participants to describe their strategies for shoulder-surfing the passwords. For PINs, most observed the experimenter's hand movements and placement on the keys and made note of the keys pressed. A small majority (56%) wrote down the sequence of keys, and used them when entering their PIN. Participants used their notes mostly for the 10-digit PINs, because mentally remembering these PINs overloaded their working memory. For 6-digit PINs, participants shoulder-surfed individual digits of the PIN and kept them in their working memory instead of taking notes. They mentally rehearsed the digit sequence in their working memory repeatedly to help them remember the PIN. At the beginning of the study, many participants were confident that they would be able to easily shoulder-surf PINs and were quite surprised when they could not. It appears that they initially overestimated their ability to shoulder-surf PINs. Most (78%) did not change their PIN shoulder-surfing strategy throughout the study.

For bend passwords, participants used a variety of strategies and changed them throughout the session (89% changed, usually more than once). The most common strategy was drawing a rectangle on paper, assigning numbers to each of the corners, and marking the observed gestures. This strategy was ineffective because participants had difficulty keeping track of the direction of each gesture. In general, taking notes did not prove to be an effective strategy, because it was difficult for participants to observe and take notes simultaneously. However, participants also found that the bend passwords were too difficult to hold in working memory. This was because bend

passwords have too many components to remember which overloaded participants' working memory. For each gesture, participants had to remember the location(s) of the gesture, its direction (up or down) and type (single or multi). When asked which type of password was most difficult to shoulder-surf, most participants answered that bend passwords were harder than PINs. We believe that participants thought bend passwords were harder to shoulder-surf because they have more components to keep track of and remember than PINs.

7.4 Discussion

We found that bend passwords and PINs were equally difficult to shoulder-surf and success rates were extremely low for both. However, it is important to note that for PINs we used a set-up (smaller keyboard and no visual feedback) that is more resistant to shoulder-surfing attacks than the set-up (larger keyboard and feedback) most commonly used on mobile devices. In addition to this, we used longer PINs (6 and 10-digits) than what is commonly used (4-digits) on mobile devices. We chose this configuration to devise the strongest control condition and not to overstate bend passwords' resistance to shoulder-surfing attacks. Given this, we believe that bend passwords are more resistant to shoulder-surfing attacks than PINs. However, further research is required to confirm this.

For bend passwords, users found it difficult to observe gesture movements and identify exactly which gesture had been performed. Furthermore, participants had no easy way to write down the observed gestures whereas they were able to write down the PINs without looking at their notes. Shoulder-surfers may eventually develop better note-taking strategies, but we see it as a positive result that our participants found it very difficult to shoulder-surf bend passwords despite people's initial assumptions that it would be easy. We also observed that participants were able to shoulder-surf shorter PINs without writing them down. They simply observed the key presses on the keypad and kept track of the entered digits in their working memory. However, participants were unable to use this strategy for any of their bend passwords. Thus, the only way to successfully shoulder-surf bend passwords was to take some type of notes. Even if shoulder-surfers develop better note taking strategies, we believe that

they will still have a hard time shoulder-surfing bend passwords because it is more labour intensive to shoulder-surf passwords while taking notes. It is also more difficult to remain inconspicuous when using this strategy.

Our results also suggest that participants found it more difficult to shoulder-surf long passwords than short passwords. Our success rates do not show any difference since nearly no passwords were guessed correctly, however the Levenshtein distances were higher for longer passwords. In passwords where each gesture/digit is independent, it is reasonable to expect that longer passwords will be more difficult to shoulder-surf because there are more components to observe. User feedback revealed that participants found it more difficult to shoulder-surf passwords when hand movement was involved. Specifically, they had a hard time shoulder-surfing passwords when the experimenter's hand was moving across the device, because they were unable to keep track of which keys or gestures were pressed.

Even though our study had a small number of participants, we believe that it shows some interesting results that can be used to make recommendations for users to create shoulder-surfing resistant PINs and bend passwords. We suggest that for PINs, users should create longer PINs with independent digits (i.e., no repeating digits) that require hand movement. For bend passwords, we suggest that users create longer passwords that are complex, use independent gestures and require hand movement. For complexity, users should incorporate both single and multi-gestures in their passwords, use both gesture directions (i.e., up and down) and use all locations (i.e., all four corners) of the device. The complexity of a password increases its resistance to shoulder-surfing attacks by overloading the working memory of shoulder-surfers.

7.5 Limitations

Some limitations of our study include a small sample size, using novice shoulder-surfers, using a PIN set-up resistant to shoulder-surfing and lack of visual feedback during the shoulder-surfing of bend passwords. We had a small sample size of 9 participants, where each participant shoulder-surfed 16 passwords (8 on mobile and 8

on flexible display). While this small sample allowed us to test our research methodology, we would need to run the study with a larger sample size to validate and generalize our findings. We used novice shoulder-surfers in our study and it is possible that experienced shoulder-surfers may have better success rates and strategies for shoulder-surfing passwords. In future, we will test our study with expert shoulder-surfers to explore their strategies and performance. We used a PIN set-up (longer PINs, smaller keypad, no feedback for last entered digit) in our study, which may have overstated the shoulder-surfing resistance of PINs. In future, we will compare bend passwords to the more commonly used PIN set-up (i.e., shorter PINs, larger keypad, feedback for last entered digit) to determine whether there is a difference in the results.

When shoulder-surfing bend passwords, participants did not receive any visual feedback from the display when a gesture was entered. This includes not seeing a "star" on the screen upon gesture entry. We believe this limitation did not affect our results, because users focused on the experimenter's hand as their primary visual cue. Similarly in the PIN condition, participants also focused on the placement of the experimenter's hand as it moved across the keyboard, despite having access to the visible "stars" on the screen. Therefore, we do not believe the lack of visual UI on the flexible display significantly affected our results. In addition to this, even if visual feedback had been provided participants would not have been able to see it well when the device was deformed for gesture entry. However, in the future we will run our study with the visual feedback enabled for bend passwords to see if it affects their shoulder-surfing success rates and performance.

Chapter 8

Discussion and Conclusion

In this thesis, we are interested in whether bend gestures can be used to create a secure and usable authentication scheme on flexible display devices. To answer our research question, we developed a bend-gesture based authentication scheme, implemented it on a flexible display device and conducted several user studies to evaluate its usability and security. In this chapter we provide a summary of the results from our user studies, and then present eight design recommendations.

8.1 Summary of Results

Current mobile devices have a variety of authentication mechanisms that can be used to protect the data on the device. These include alphanumeric passwords, PINs and gesture-based passwords such as the Android Unlock pattern. However, each of these authentication schemes have weaknesses that result in insecure passwords. Mobile devices with new forms of interaction modalities present us with an opportunity to explore new forms of authentication. In flexible display devices, users primarily interact with the device by deforming (i.e., bending) its display in various ways. In this thesis, we were interested in whether the "bend" interaction can be used to authenticate on these devices.

We developed an authentication scheme utilizing the bend gestures. In this scheme, passwords are created by performing a series of bend gestures on the flexible display. We developed a flexible display prototype to test our authentication scheme. We conducted several user studies to evaluate the security and usability of our authentication scheme and compared the results with PINs on a mobile phone device.

In our first study, we looked at whether users could create a bend password and remember it after one week. Users created a bend password on a flexible display and

a PIN on the mobile phone. After a week, users returned to the lab to re-enter their passwords. We found that users could easily create bend passwords, but took several attempts before creating a memorable password. We believe that this was because they were new to the system and were developing strategies for creating memorable bend passwords. After learning their passwords, most users successfully remembered them after a week and there were no significant differences between the memorability rate of PINs and bend passwords. Users created secure bend passwords but created insecure PINs, because they either reused existing PINs or used personal information in their PINs. Due to the speed limitations of our prototype, users took significantly more time to enter their bend passwords than their PINs.

In our second study, we looked at system assigned bend passwords and compared the results with system assigned PINs. Users were randomly assigned a 5-gesture bend password and a 6-digit PIN. Users took significantly more time to learn their bend passwords than their PINs because they had no pre-existing memory strategies for remembering the bend passwords. A week later, most users successfully remembered both their bend passwords and PINs, and there were no significant differences between the two authentication schemes.

We compared the results from our user chosen and system assigned password user studies. There were no differences in task performance between user chosen and system assigned PINs. However, users preferred to create their own PINs and had a higher perception of memorability for user chosen PINs. Surprisingly, users perceived their system assigned PINs to be easier to shoulder-surf than their own PINs. There were no significant differences in user performance or perception between user chosen and system assigned bend passwords. This is a positive result because it indicates that users may be receptive to system assigned bend passwords. This is encouraging because it improves the security of the system.

In our third study, we evaluated the shoulder-surfing susceptibility of bend passwords and compared the results with PINs on a mobile phone. Participants played the role of a malicious shoulder-surfer and the experimenter played the victim. The shoulder-surfing success rates for both PINs and bend passwords were extremely low,

however, certain types of passwords were easier to shoulder-surf than others. Specifically, shorter passwords and passwords where the experimenter's hand was not moving on the device were easier to shoulder-surf. Participants found bend passwords harder to shoulder-surf than PINs because bend passwords have many different components (e.g., location, direction and gesture type) that need to be observed.

8.2 Design Recommendations

Based on our experiences and insight gained while working with the prototype and running user studies, we have devised a set of eight preliminary design recommendations. We believe that these will generalize to bend gesture authentication schemes implemented on real flexible devices when they become available. We divide our recommendations into three categories: those relating to system feedback provided by the authentication scheme, those relating to physical device characteristics that would facilitate bend authentication, and those relating to the types of interactions allowed within the authentication scheme.

8.2.1 System Feedback

We begin with recommendations relating to the types of user feedback provided by the authentication scheme during regular use.

R1: System should provide multiple types of feedback

The system should provide users with multiple types of feedback (i.e., visual, audio and vibrotactile) upon gesture or password entry. The visual feedback should be shown on the display and could be external to display as well, such as an LED light embedded within the device.

Our system provided several forms of feedback to the user when they entered a gesture or their password. When a gesture was entered, the system changed the color of an LED light affixed to the display, emitted a clicking sound, and displayed an asterisk on the projected UI. User comments revealed that participants' liked all three types of feedback, and used them to recover from errors. Having multiple feedback

mechanisms tailors a system to a variety of users and environments. For example, if users are using the system in a noisy place they can rely on the visual feedback instead of the auditory feedback.

R2: Feedback should differentiate between multi and single gestures

Users should be able to use the feedback provided by the system to determine whether they have entered a single or a multi gesture. All feedback mechanisms should show this difference. If the system utilizes an LED light, the light could change color to show the distinction between the gesture types. Similarly, for vibrotactile feedback, the device could emit vibrations of different frequency to distinguish between gesture entry.

Our system used the LED light to provide a distinction between the two gesture types. The color of the light changed to blue when a single gesture was entered, and pink when a multi gesture was entered. User comments from user studies revealed that participants really liked gesture distinction in the feedback. This type of feedback was also instrumental when users were learning how to use bend gestures on the flexible display prototype. They used it to learn how (degree and speed of bend) to bend the corners of the display to enter a multi gesture versus entering a single gesture.

R3: The system should allow users to disable feedback

The system should provide users with an easy mechanism to disable each type of feedback. It should provide them with an option to turn-off all feedback or only specific types of feedback. For example, users should be able to disable the visual feedback while still keeping the other feedback mechanisms enabled.

The feedback provided by authentication systems is very useful to users, especially when they are first learning to use the system. However, these feedback mechanisms often make it easier for observers to shoulder-surf the authentication scheme, as observers use the feedback cues provided by the system to observe the characteristics of a password. Thus, authentication systems should allow users to disable the feedback at any time to reduce the risk of shoulder-surfing. When the system is used in

an environment (e.g., coffee shops, public transportation) that facilitates shoulder-surfing attacks, users can temporarily disable all feedback on their device to reduce the risk of their password being shoulder-surfed. Alternatively, users might instead enable the feedback mechanisms (e.g., vibrotactile) of their device that are resistant to shoulder-surfing attacks.

8.2.2 Device Characteristics

Our next set of recommendations relate to physical device characteristics that we feel would facilitate user authentication using bend gestures. We believe that they may also apply to interactions beyond authentication.

R4: Sensor activation thresholds should be customizable

Flexible display devices should allow users to easily customize the activation thresholds of the bend sensors located within the device.

In our user studies, we observed that each participant performed the same bend gesture in a different manner. Some applied more force than others or performed larger gestures. This led to unpredictable gesture behaviour when the same sensor activation thresholds were used for all participants. Some participants were able to easily perform a bend gesture while others struggled to get accurate results.

We observed that this behaviour was also affected by the size of the user's hand. Users with large hands applied more physical force to perform a bend gesture than users with small hands. Thus, we observed that using the same sensor activation thresholds led to unpredictable activation of bend gestures. This increased the password entry time and error rate of bend passwords. Based on these results, we recommend that flexible display devices allow users to calibrate the sensors according to their individual needs, which will lead to increased user performance and positive user experience of bend passwords. Although we tested with an early prototype, we believe that this advice would also apply to real devices.

R5: Displays should allow one-handed gestures

Several characteristics of flexible displays affect users' ability to effectively perform one-handed bend gestures. These include the size and malleability of the display, and location of the sensors within the display. The size and malleability of the display should be set to allow most users to hold the display in one hand, and perform a range of bend gestures with their other hand. Similarly, bend sensors should be placed within the device to facilitate entering of one-handed bend gestures.

The dimensions of our flexible display were $135 \times 95 \times 1.5mm$, which were slightly larger than the dimensions of the mobile phone used in our PIN condition ($136.6 \times 70.6 \times 8.6mm$). We observed that most users could not perform one-handed gestures with our display because it was too wide. Thus, we recommend that the width of the display should be smaller than what was used in our study. Further testing could determine the optimal size.

We only placed bend sensors in the corners of our flexible display prototype, which meant that users could only perform gestures by bending the corners of the display. Thus, participants had to use both their hands to perform many of the bend gestures in our authentication scheme, which many found inconvenient. Therefore, based on these results we recommend that bend sensors should be placed in the corners of the display as well as its sides to recognize a wider range of gestures.

8.2.3 User Interaction

Gesture Language

In this section we provide some design recommendations for the gesture-set of bend passwords.

R6: Gestures must be fast and distinct

All bend gestures must be relatively fast and be sufficiently distinct to enable a high rate of input accuracy. Gestures with low accuracy or that are slow to input negatively affect user experience, as we observed in our user studies. When given a set of gestures, it is possible that users may choose to avoid less distinct gestures in their passwords, which will reduce the effective password space of the scheme. In addition

to reducing user experience, slow gestures are also more likely to be shoulder-surfed because observers can more easily see the gesture being performed on the device.

R7: The gesture-set must include a variety of one-handed and two-handed gestures

In our user studies, participants could easily learn the gestures included in our gesture-set, but many wanted to see a greater variety of one-handed and two-handed gestures. Based on the feedback received from participants, we recommend including the following types of gestures in the gesture-set for bend passwords:

- Bending each corner of the display up or down are the simplest gestures. In addition to these, gestures such as folding and bending the sides of the display should also be included, as well as differentiating gestures by their angle of bend.
- Bending multiple corners of the display simultaneously, either in the same direction or different directions clearly requires two hands and is more complex.

In our authentication scheme, users could only use a limited set of gestures, which included bending a corner of the display up or down (8 gestures) and bending any *two* corners of the display in the *same direction* (i.e., up or down) simultaneously (12 gestures). Increasing the gesture-set of bend passwords will allow users to create a variety of different passwords, which will increase the theoretical password space of bend passwords.

Multiple Interaction Modalities

Real flexible display devices will most likely be equipped with multiple interaction modalities. We provide recommendations on the transition between two of these interaction modalities: bend and touch. We focus on bend and touch because we believe these will be the two most commonly used interaction modalities on flexible display devices, however, other transitions should also be considered.

R8: Seamless transition between bend and touch

The transition between bend and touch should be seamless and must not disrupt a user's primary task. With regards to bend passwords, users would enter their password by performing a series of bend gestures, and confirm it by pressing (i.e.,

touching) a button on the display. Users would also use touch-based buttons on the display to undo a gesture or reset their password entry. The transition between their bend and touch interaction should be easy and quick to accomplish, without requiring excessive hand repositioning.

In our user studies, participants used external push buttons to confirm, reset or undo their password entry. We found that using these buttons disrupted the password entry task and significantly affected password entry times because users had to divert their attention from the flexible display to use these buttons. It is possible that the negative effects of switching between two interaction modalities were more profound in our studies due to the decoupling of the buttons and the flexible display. However, we believe that these effects will still exist in real flexible display devices (with no decoupling issues) if the transition between touch and bend is not seamless. Thus, if the transition between bend and touch is disruptive (e.g., slow reaction times) to users' password task, it will likely affect their performance, opinion, and likelihood of using bend passwords.

8.3 Future Work

Future work on bend passwords should address the limitations of our prototype, such as improving the gesture recognition algorithm. When real flexible display devices become available, it would be interesting to implement and test the bend gesture authentication scheme on these devices.

Our user studies showed positive results on the short-term memorability (i.e., one week) of bend passwords. In real life, passwords are used for than one week and users often memorize and use multiple passwords. Thus, future research in this area should look at the long-term memorability of bend passwords and the potential interference of multiple bend passwords. However, such work will only be possible when flexible display devices are commercially available and can be used in longitudinal user studies.

In our work, we compared bend passwords to PINs and found comparable results between the two authentication schemes in specific areas. Future work should compare bend passwords with other commonly used authentication schemes on mobile devices, such as the Android Unlock Pattern.

8.4 Conclusion

In summary, the results from our user studies are mixed but indicate that bend passwords are worthy of further exploration. Although our scheme was implemented on a custom built prototype which may have impacted the user study results, we believe that several of our findings and the insight gained will generalize to eventual market quality devices. We conclude the thesis with design recommendations for the eventual implementation of bend authentication on real flexible display devices.

Bibliography

[1] Cedric's weblog: Android's locking pattern. `http://beust.com/weblog2/archives/000497.html`. Accessed: 2014-03-30.

[2] Samsung flexible display phone coming in 2015? `http://www.ibtimes.com/samsung-flexible-display-phone-coming-2015-manufacturer-secretly-showcases-foldable-amoled-display`. Accessed: 2014-04-04.

[3] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[4] Michael Arrington. Android's login is cool, but is it secure? `http://techcrunch.com/2008/10/12/androids-login-is-cool-but-is-it-secure`. Accessed: 2014-03-30.

[5] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies*, pages 1–7, 2010.

[6] Bernard J Baars. *A cognitive theory of consciousness*. Cambridge University Press, 1986.

[7] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security*, 5(4):367–397, 2002.

[8] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. The secure haptic keypad: A tactile password system. In *Proceedings of the 28th SIGCHI Conference on Human Factors in Computing Systems*, pages 1089–1092, 2010.

[9] Andrea Bianchi, Ian Oakley, Jong Keun Lee, and Dong Soo Kwon. The haptic wheel: Design and evaluation of a tactile password system. In *Proceedings of the 28th SIGCHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 625–630, 2010.

[10] Joseph Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, pages 538–552, 2012.

[11] Jesse Burstyn, Amartya Banerjee, and Roel Vertegaal. Flexview: An evaluation of depth navigation on deformable mobile devices. In *Proceedings of the 6th Conference on Tangible, Embedded Embodied Interaction*, pages 193–200, 2012.

[12] Ming Ki Chong, Gary Marsden, and Hans Gellersen. Gesturepin: Using discrete gestures for associating mobile devices. In *Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services*, pages 261–264, 2010.

[13] Alexander De Luca, Emanuel von Zezschwitz, and Heinrich Hussmann. Vibrapass: Secure authentication based on shared lies. In *Proceedings of the 27th SIGCHI Conference on Human Factors in Computing Systems*, pages 913–916, 2009.

[14] Matteo Dell'Amico, Pietro Michiardi, and Yves Roudier. Password strength: An empirical analysis. In *Proceedings of the 29th Conference on Information Communications*, pages 983–991, 2010.

[15] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. Does my password go up to eleven?: The impact of password meters on password selection. In *Proceedings of the 31st SIGCHI Conference on Human Factors in Computing Systems*, pages 2379–2388, 2013.

[16] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, pages 657–666, 2007.

[17] Dinei Florêncio, Cormac Herley, and Baris Coskun. Do strong web passwords accomplish anything? In *Proceedings of the 2nd USENIX Workshop on Hot Topics in Security*, pages 10:1–10:6, 2007.

[18] Philip G. Inglesant and M. Angela Sasse. The true cost of unusable password policies: Password use in the wild. In *Proceedings of the 28th SIGCHI Conference on Human Factors in Computing Systems*, pages 383–392, 2010.

[19] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. *Communications of the ACM*, 43(2):90–98, 2000.

[20] Johan Kildal, Andrés Lucero, and Marion Boberg. Twisting touch: Combining deformation and touch as input within the same interaction cycle on handheld devices. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pages 237–246, 2013.

[21] Johan Kildal, Susanna Paasovaara, and Viljakaisa Aaltonen. Kinetic device: Designing interactions with a deformable mobile interface. In *Proceedings of the 30th SIGCHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1871–1876, 2012.

[22] Johan Kildal and Graham Wilson. Feeling it: the roles of stiffness, deformation range and feedback in the control of deformable ui. In *Proceedings of the 14th ACM International Conference on Multimodal Interaction*, pages 393–400, 2012.

[23] Byron Lahey, Audrey Girouard, Winslow Burleson, and Roel Vertegaal. Paperphone: Understanding the use of bend gestures in mobile devices with flexible electronic paper displays. In *Proceedings of the 29th SIGCHI Conference on Human Factors in Computing Systems*, pages 1303–1312, 2011.

[24] Sang-Su Lee, Sohyun Kim, Bipil Jin, Eunji Choi, Boa Kim, Xu Jia, Daeeop Kim, and Kun-pyo Lee. How users manipulate deformable displays as input devices. In *Proceedings of the 28th SIGCHI Conference on Human Factors in Computing Systems*, pages 1647–1656, 2010.

[25] Michael D Leonhard and VN Venkatakrishnan. A comparative study of three random password generators. In *Proceedings of the IEEE International Conference on Electro/Information Technology*, pages 227–232, 2007.

[26] Vladimir I. Levenshtein. Binary codes capable of correcting deletions, insertions, and reversals. *Soviet Physics Doklady*, 10(8):707–710, 1966.

[27] Martez Mott, Thomas Donahue, G. Michael Poor, and Laura Leventhal. Leveraging motor learning for a tangible password system. In *Proceedings of the 30th SIGCHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 2597–2602, 2012.

[28] Shannon Riley. Password security: What users know and what they actually do. *Usability News*, 8(1):2833–2836, 2006.

[29] J. Saltzer and M. Schroeder. The protection of information in computer systems. In *Proceedings of the 4th Symposium on Operating System Principles*, volume 63, pages 1278–1308, 1975.

[30] Florian Schaub, Ruben Deyhle, and Michael Weber. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia*, pages 13:1–13:10, 2012.

[31] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. Exploring the design space of graphical passwords on smartphones. In *Proceedings of the 9th Symposium on Usable Privacy and Security*, pages 11:1–11:14, 2013.

[32] Carsten Schwesig, Ivan Poupyrev, and Eijiro Mori. Gummi: a bendable computer. In *Proceedings of the 22nd SIGCHI Conference on Human Factors in Computing Systems*, pages 263 – 270, 2004.

[33] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Encountering stronger password requirements: User attitudes and behaviors. In *Proceedings of the 6th Symposium on Usable Privacy and Security*, pages 2:1–2:20, 2010.

[34] Jürgen Steimle, Andreas Jordt, and Pattie Maes. Flexpad: Highly flexible bending interactions for projected handheld displays. In *Proceedings of the 31st SIGCHI Conference on Human Factors in Computing Systems*, pages 237–246, 2013.

[35] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the 2nd Symposium on Usable Privacy and Security*, pages 56–66, 2006.

[36] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. How does your password measure up? the effect of strength meters on password creation. In *Proceedings of the 21st USENIX Conference on Security Symposium*, pages 5–5, 2012.

[37] Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, pages 261–270, 2013.

[38] Kristen Warren, Jessica Lo, Vaibhav Vadgama, and Audrey Girouard. Bending the rules: bend gesture classification for flexible displays. In *Proceedings of the 31st SIGCHI Conference on Human Factors in Computing Systems*, pages 607–610, 2013.

[39] Jun-ichiro Watanabe, A. Mochizuki, and Y. Horry. Bookisheet: bendable device for browsing content using the metaphor of leafing through the pages. In *Proceedings of the 10th International Conference on Ubiquitous Computing*, pages 360–369, 2008.

[40] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, pages 162–175, 2010.

[41] Doug Wightman, Tim Ginn, and Roel Vertegaal. Bendflip: Examining input techniques for electronic book readers with flexible form factors. In *Proceedings of the 13th IFIP TC13 Conference on Human-Computer Interaction*, pages 117–133, 2011.

[42] J. Yan, R. Anderson, and A. Grant. *The memorability and security of passwords*, chapter 7, pages 129–142. Security and Usability: Designing Secure Systems That People Can Use. O'Reilly Media, 2005.

[43] Zi Ye and Hammad Khalid. Cobra: Flexible displays for mobile gaming scenarios. In *Proceedings of the 28th SIGCHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 4363–4367, 2010.

[44] Moshe Zviran and William J. Haga. Password security: An empirical study. *Journal of Management Information Systems*, 15(4):161–185, March 1999.