Pers Ubiquit Comput
DOI 10.1007/s00779-016-0928-6

ORIGINAL ARTICLE

Bend Passwords: using gestures to authenticate on flexible devices

Sana Maqsood[1] · **Sonia Chiasson**[1] · **Audrey Girouard**[2]

Received: 16 July 2015 / Accepted: 15 February 2016

Abstract Upcoming mobile devices will have flexible displays, allowing us to explore alternate forms of user authentication. On flexible displays, users can interact with the device by deforming the surface of the display through bending. In this paper, we present Bend Passwords, 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 Bend Passwords and compared it to PINs on a mobile phone. Our first two studies evaluated the creation and memorability of user-chosen and system-assigned passwords. 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 provide eight design recommendations for implementing Bend Passwords on flexible display devices.

Keywords Usable security · Authentication · Deformable user interfaces · Bend gestures

✉ Sonia Chiasson
chiasson@scs.carleton.ca

Sana Maqsood
sana.maqsood@carleton.ca

Audrey Girouard
audrey.girouard@carleton.ca

[1] School of Computer Science, Carleton University, Ottawa, Canada

[2] School of Information Technology, Carleton University, Ottawa, Canada

1 Introduction

A Pew Internet study found that over 64 % of American adults owned smartphones in 2014 and 42 % owned a tablet computer [1]. The increased use of mobile devices has resulted in a higher volume of sensitive data stored on these devices, needing protection from unauthorized access. Many authentication schemes are available on mobile devices to help users protect their data from undesired access, including PINs, alphanumeric passwords, gesture-based passwords, and biometric authentication (e.g., Android Face Unlock, iPhone Touch ID). However, all of these authentication schemes either have usability or security issues that lead to insecure passwords or poor user adoption. Alphanumeric passwords and PINs are difficult to remember, which makes users resort to insecure coping strategies [2]. Pattern Lock, a gesture-based authentication scheme commonly used on Android devices, leads to low entropy passwords [3] that are susceptible to smudge attacks [4]. Biometric authentication systems have high false rejection rates, and stolen passwords are difficult to replace. Since no authentication scheme is perfect, there remains a need for novel authentication schemes. New interaction modalities provide an opportunity to explore new forms of user authentication. One such interaction modality is the inclusion of a flexible display, which will be integrated into mobile devices in the near future [5].

On flexible display devices, users interact with the device by deforming (i.e., bending) the surface of the display. These devices have several advantages, including being lightweight, power efficient, and providing a new input/output modality. Many researchers have explored using bend gestures as an input technique [6–8] on smartphones, e-books and maps [6–10] within a research context. The success of bend gestures is largely explained

Published online: 26 April 2016

by the inherent tactile feedback provided by the display when a gesture is performed. Bend gestures can be discrete or continuous, with several degrees of freedom, such as the angle of the bend, the speed of the motion, the distance to the corner, and the location of the bend [11].

In our work, we utilized bend interaction to design a new authentication scheme and evaluated its security and usability. Our work is exploratory in nature, investigating the use of bend interaction in the user authentication domain. In our scheme, passwords are created by performing a series of bend gestures on the flexible display. As flexible display devices are not commercially available, we implemented our authentication scheme on a custom built flexible display prototype. We conducted three user studies to evaluate the usability and security of our authentication scheme compared to PINs, which are commonly used on mobile devices. Users performed various password tasks, and we used quantitative and qualitative methods to analyze their task performance and perceptions of our authentication scheme. The first two studies evaluated the usability and security of user-chosen and system-assigned Bend Passwords, respectively. Our third study evaluated the shoulder-surfing[1] susceptibility of Bend Passwords. In this paper, we present the design and implementation of our authentication scheme, results from the user studies, lessons learned, and design recommendations for future work.

2 Related work

We first discuss prior work on bend gesture interaction techniques for flexible displays. We also compare the authentication schemes available on mobile devices, review authentication methods using novel inputs, and provide an overview of the techniques involved in evaluating new authentication schemes.

2.1 Flexible displays and bend gestures

Users can interact with flexible display devices by deforming the surface of the device to trigger a command [7]. Application areas for flexible display devices include gaming [12], control of media and home appliances [6], [7], e-readers [7, 9, 10], maps [7, 8, 13], and smart phones [6, 7].

Schwesig et al. [8] pioneered the concept of a flexible device which used bending as an input and interaction technique. They tested their concept with a rigid screen to which 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. [7] 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, i.e., *down*). In turn, Kildal et al. [6] 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. [14] presented completely non-functional prototypes to participants, most researchers embed or affix sensors to a flexible plastic substrate, and use either an external screen [15] or projection [9, 12, 16] to present a graphical interface to the user. We followed Watanabe et al.'s [9] and Ye et al.'s [12] prototyping recommendations to build our prototype.

Warren et al. [11] 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. Girouard et al. [17] explored the use of one-handed gestures on flexible displays and found that users preferred the top right up and centre squeeze up gestures, as they were faster and more comfortable than the other six gestures. The authors recommend associating these gestures with quick and important actions on flexible mobile devices. We used the two most popular bend characteristics, location and direction [7, 11], to classify the gestures in our system.

2.2 Usable authentication

The importance of usable authentication was first highlighted by Saltzer and Schroeder [18]. Nearly four decades later, text passwords remain popular despite their inadequacies [2, 19] 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.

[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.

2.2.1 Comparison of current mobile authentication schemes

Current mobile devices have several authentication schemes available. These include PINs, alphanumeric passwords, graphical passwords (e.g., Android Pattern Lock), and biometric authentication. Authentication schemes usually have a trade-off between usability and security; thus, passwords with high usability generally have low security and vice versa.

Table 1 compares current authentication schemes for mobile devices, using data summarized from multiple sources [2, 4, 20–24].

At over 78 %, the most popular authentication scheme on mobile devices is PINs [25]. The popularity of PINs is due to their high usability. They can easily be shared with other users (e.g., friends, family) and can be reused on multiple devices and applications. The biggest disadvantage of PINs is that they have low security. Specifically, they have a small theoretical password space, which means that attackers could potentially guess the password after stealing the mobile device.

PINs are also susceptible to shoulder-surfing attacks, when used in a public place [20]. This is especially problematic given the widespread availability of cameras to record entry.

Text passwords are popular in the desktop environment and thus are also frequently used in the mobile domain. Despite their advantages, secure text passwords are difficult to remember which leads users to use insecure password creation and coping strategies [2]. They also have high entry times and rate of input errors on mobile devices, because of the need to switch virtual keyboards during password entry [21, 22]. Similar to PINs, text passwords are also highly susceptible to shoulder-surfing attacks [21].

Pattern Lock is widely used on Android devices and is preferred by users over PINs [23]. In this scheme, users authenticate by drawing a graphical pattern on a touch-screen. However, Pattern Lock has low security because of a small password space, and its vulnerability to shoulder-surfing [24] and smudge attacks [4]. In smudge attacks, passwords are stolen by observing the smudge stains left on the display by the user's fingers. von Zezschwitz et al. [23] conducted a longitudinal field study (spanning 3 weeks) to evaluate the usability and security of the Android Pattern Lock 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.

Several biometric authentication schemes are also available on mobile devices, including Apple's Touch ID [26] and Android's FaceUnlock [27]. An advantage of biometric authentication is that the passwords are less susceptible to shoulder-surfing and guessing attacks, as the biometric data are unique to an individual and are therefore difficult to steal or replicate. These authentication schemes also place very little load on users' memory. Their disadvantages include high false rejection rates, trust and privacy issues, and the inability to share the password with other users.

Since no authentication scheme is perfect, the type of scheme used on mobile devices often depends on the users' needs and preferences.

2.2.2 Overview of novel authentication schemes

We review four types of novel authentication schemes relevant to our proposal, including tangible, haptic,

Table 1 Comparison of current mobile authentication schemes assuming randomly generated passwords and typical configuration

Authentication scheme	Advantages	Disadvantages
PINs	Ability to reuse and share[a]	Small theoretical password space
	Fast entry times	Susceptible to shoulder-surfing attacks
	Infrequent entry errors	
	Easy to remember	
Alphanumeric	Ability to reuse and share[a]	Difficult to remember
	Large theoretical password space	High number of entry errors
		Susceptible to shoulder-surfing attacks
Graphical	High perceived usability	Small theoretical password space
		Susceptible to smudge attacks
		Susceptible to shoulder-surfing attacks
Biometric	Resistant to shoulder-surfing attacks	High false rejection rates
	Low susceptibility to guessing attacks	Trust and privacy issues
	No memorability issues	Devices cannot be shared[a]

[a] Password reuse and sharing are typically viewed as an advantage by users, but these also pose a security risk

behavioural biometric, and gesture-based authentication schemes.

Tangible and haptic authentication The first category includes schemes that use specialized hardware. Haptic Wheel [28] and the Secure Haptic Keypad [29] 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 at 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 because attackers are unable to observe the haptic feedback, 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. However, password entry on these systems takes considerably more time than traditional authentication mechanisms.

Mott et al. [30] developed TangibleRubik, an authentication mechanism that takes advantage of the human ability to memorize repeated motor actions. 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 entering them repeatedly. After a short distractor task (10 min), participants re-entered their password once in the system. Participants made a large number of errors in the learning stage, but successfully remembered their passwords after the distractor task. 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 shoulder-surfing susceptibility, and comparing them with existing authentication schemes.

Behavioural biometric and gesture-based authentication Behavioural biometrics such as signature-recognition [31], speech recognition [31], or keystroke dynamics [32] also rely on user movements as a means of authentication, but recognize users based on variances in behaviour rather than on their ability to recall specific gestures. They match 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 is their high false rejection rates when configured for reasonably low false accept rates.

Several gesture-based schemes for mobile devices have been proposed. GesturePIN [33] is an authentication mechanism for connecting two or more mobile devices together. Passwords are created by moving the mobile device in 3D space to perform gestures. GesturePIN has the same theoretical password space as numerical PINs, but a user study found that it had longer entry times and less accuracy than PINs. In addition, it was very susceptible to shoulder-surfing attacks because the 3D gestures could easily be observed. GesturePass [34] uses common touchscreen gestures as the components of a password. A user study shows that users preferred GesturePass over PINs and preferred single-touch gestures (e.g., drag, tap) compared to multi-touch gestures (e.g., turn-left, pinch-in). Recently, the Back-of-Device (BoD) [35] and XSides [24] authentication schemes have been proposed to protect against shoulder surfing. With BoD, users enter their stroke-based password on a touchscreen at the back of a mobile device, hiding it from prying eyes. XSides works similarly, except that users may use either the front or back touchscreen (or combination thereof) to enter their password, allowing users to adapt their behaviour based on their current environment.

To the best of our knowledge, there has been no work investigating authentication schemes on flexible display devices.

2.2.3 *Evaluating authentication schemes*

When evaluating new authentication schemes, the first step is usually to test in a controlled environment with lab studies and [36]. This allows discovery of problems before the scheme is deployed in the field, which reduces the risk of security and privacy breaches to users' real resources. Results are usually compared with those of existing authentication schemes, to establish baseline usability and security measures. Lab studies are usually conducted with at least 20 participants to provide statistically significant results [37]. Typically, users are provided training on the new authentication scheme followed by a password initialization task (user-chosen or system-assigned) [36]. Next, users confirm their password to ensure that they have not made any trivial entry errors and can accurately remember their password after a short time (measure of short-term memorability). They are usually asked to return to the lab to complete a login task after several days, weeks or months, which measures the long-term memorability of the authentication scheme and contributes to its ecological validity. In each session, several usability and security measures are collected to evaluate the authentication scheme. Hypotheses are sometimes explicitly defined, but most often are not included.

Usability The most common usability measures are password creation time, login time, and memorability.

Memorability measures include login success rates and number of errors [36]. User perceptions and opinions are also collected.

Security Common measures of security include the size of the theoretical password space, anticipated exploitable patterns in user choice, and evaluation of the scheme against known online and offline attacks [36]. Every authentication scheme has a theoretical password space and an effective password space. The theoretical password space contains the set of all passwords that can be created. However, most users create passwords that fall into a subset of the theoretical password space, which is known as the effective password space. Thus, the effective password space is usually smaller than the theoretical password space. As it is very difficult to measure the effective password space, the measure of theoretical password space is often used instead, which can be computed using the formula log (c^n), where c = number of available gestures or digits in the password scheme and n = password length. For example, a 4 digit PIN has a theoretical password space of log (10^4) = 13.29 bits, while a standard 8-character alphanumeric text password has log (95^8) = 52.56 bits. Larger passwords spaces usually mean that authentication schemes are more resistant to guessing attacks. However, secondary protection mechanisms such as lock-outs after a small number of incorrect entries can also help protect against guessing attacks in certain circumstances. Florencio and Herley [38] recommend that the theoretical password space of authentication schemes should be at least 20 bits.

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. [39] 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 the slow entry speed of non-dictionary alphanumeric passwords made them easy to shoulder-surf, and mouse input for PassFaces allowed observers to easily see the selections made in the password. Results suggest that authentication systems should hide password input from observers and overload observers' working memory to increase the difficulty of shoulder surfing.

Schaub et al. [21] 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 [39]. Participants shoulder-surfed three alphanumeric passwords using one of the eight virtual keyboards. They found that 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.

Most authentication schemes allow users to choose their own passwords. However, research has shown that users often choose predictable passwords [40, 41], reuse them across multiple accounts [42], and write them down [43–45]. These behaviours result in insecure user-chosen passwords. Several techniques have been suggested to help users create secure passwords. Password composition policies consist of rules (e.g., be a specific length, contain certain characters) with which a password must comply. However, users often satisfy these requirements in predictable ways which results in weak passwords [46, 47]. These policies also overburden users and lead to frustration [43]. Password strength metres rate the strength of users' passwords, and sometimes provide suggestions on how to improve their password strength. However, their effectiveness depends on their design [48] and context of use [49]. An alternative is to let the system assign randomly generated passwords. While this approach increases resistance against guessing attacks, research has shown that users have difficulty remembering system-assigned passwords because they cannot associate them with something memorable [19]. As both user-chosen and system-assigned passwords have their strengths and weaknesses, new authentication schemes should ideally find an alternative that promotes both high usability and security.

3 User authentication prototypes

Given the new interaction possibilities afforded by flexible displays, we designed a novel authentication scheme using bend gestures. We envision that this new scheme could act as an alternative authentication mechanism for unlocking mobile devices or could be used in combination with existing schemes. We used PINs as our baseline comparison as it is a well-established unlock mechanism for mobile devices. For our studies, we developed two

prototypes: a Bend Password interface on a custom flexible display and a PIN interface for existing mobile phones.

3.1 Flexible display Bend Password prototype

Our flexible display prototype has two main components: the hardware and software for controlling the authentication tasks. We developed our own flexible display hardware using an iterative design process.

3.1.1 Hardware

Figure 1 shows the hardware components of the flexible display. Our prototype is composed of a flexible (135 × 95 × 1.5 mm) PVC sheet. We selected this malleable material because users have shown a preference for less-stiff materials [50]. Four 2-inch Flexpoint bidirectional bend sensors are placed on the corners of the display. An LED light is located on the middle left of the display to provide users with visual feedback. The display is connected to an Arduino Uno 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. Users could choose the location of the UI projection to find a set-up that worked best for them. Most participants chose to project the UI on the wall in front of the flexible display. The pico-projector also outputs audio feedback and is connected to a computer.

An external panel controls the authentication process and is composed of two push buttons: a start/stop button and an undo/reset button. The start/stop button starts or confirms a password entry, and the undo/reset button deletes (i.e., undo) a gesture or resets a password entry. 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 251 ms.

3.1.2 Authentication software

The authentication software was developed using Arduino and the Processing language. The Arduino module controlled the physical components of our prototype (e.g., LED light, bend sensors, control panel), and the Processing module displayed the UI, received messages from the Arduino module and saved data from the instrumented prototype in log files.

In our authentication scheme, passwords are a series of bend gestures on the flexible display (Fig. 2). A set of 20 bend gestures was available (Appendix: Fig. 12). Each corner of the display can be bent up or down, referred to as

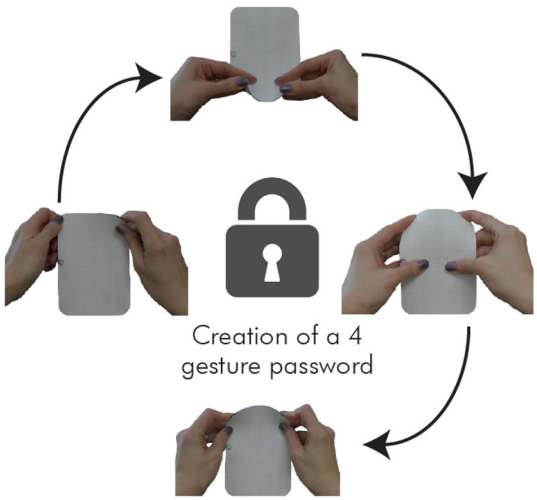


Fig. 2 Creation of a 4-gesture Bend Password

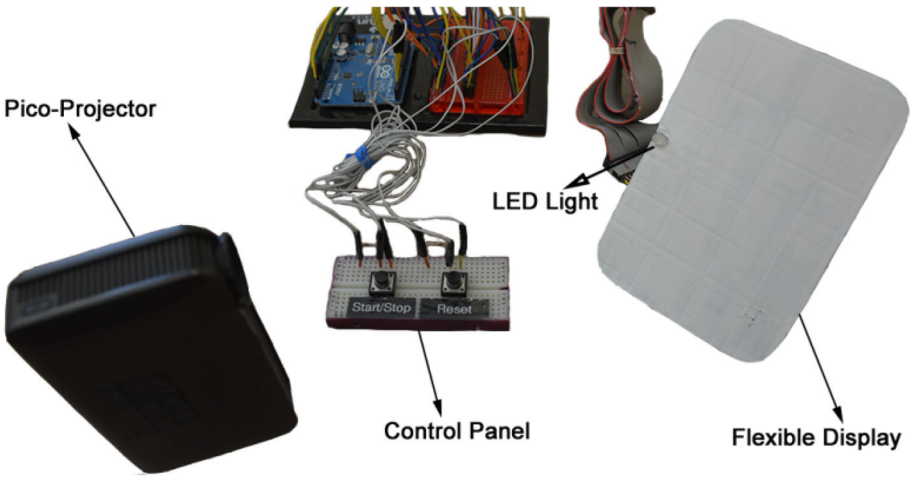
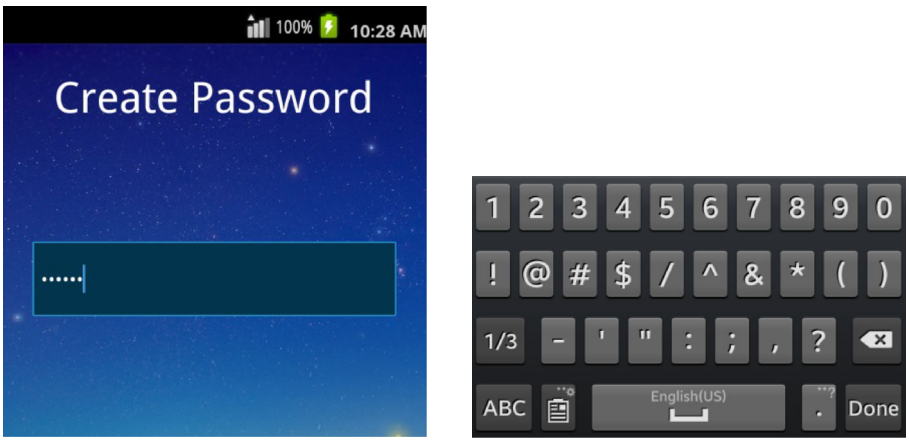


Fig. 1 Hardware components of the flexible display prototype



(a) (b)

Fig. 3 User interface components of the prototypes. **a** Authentication UI of the mobile phone and flexible display prototypes. **b** Keyboard used in the mobile phone prototype

a *single* bend gesture, and pairs of corners can be bent up or down simultaneously, referred to as a *multi* bend gesture.

A standard password entry field is displayed in the graphical user interface (GUI) (Fig. 3a). When a gesture is performed on the flexible display, the LED light changes colour (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 GUI. Password entries are confirmed by pressing the *Start/Stop* button on the external control panel.

Gesture recognition algorithm When a corner of the display is bent, the sensor on that corner changes its resistance value, which determines whether the sensor is flat, bent upwards, or downwards. Our algorithm samples the integer value of each sensor every 250 ms and waits 100 ms before mapping it to a gesture shown in Fig. 12. If another sensor is activated within 100 ms, the algorithm registers a multi-gesture corresponding to the two bent sensors; otherwise, it registers a single gesture corresponding to the one bent sensor. If a gesture corresponding to the sensor values is not found, no gesture is registered, indicating an invalid gesture entry.

Sensor thresholds As bend sensors get used, sometimes their sensitivity changes. To ensure an optimal and consistent performance of our prototype, we calibrated the sensors before each experimental session: we selected the sensor thresholds by reading the values of each sensor for a few seconds, at different degrees of bend (flat, up, down).

3.2 Mobile phone PIN prototype

We developed an Android application using Processing to create and re-enter PINs on a commercial Samsung Galaxy SIII (I9300) phone. Figure 3a shows the user interface (UI) components of the mobile phone prototype. We designed the UI to match the UI of the flexible display prototype. A PIN entry on the mobile phone is reset by pressing the reset button displayed below the password entry field, and the last entered digit is removed by pressing the Delete key on the keyboard. Similarly, a password is confirmed by pressing the Done key on the keyboard.

4 User study 1: user-chosen passwords

Our first study[2] evaluates the usability of Bend Passwords on a flexible display compared to PINs on a rigid mobile phone. Participants created one password per scheme and returned to the lab one week later to re-enter their passwords.

4.1 Methodology

Our two part study used a within-subjects design and was reviewed by Carleton University's Research Ethics Board. In the first session, participants learned to use our system and then created, confirmed, and rehearsed a Bend Password and a PIN. After one week, participants returned and re-entered their passwords. This second session was designed to evaluate the memorability of the passwords created in the first session. Figure 4 illustrates our methodology.

4.1.1 Session 1: creating passwords

In the first 1-h session, participants completed the training, creation, confirmation, and rehearsal phases. Our methodology for Session 1 closely followed Mott et al.'s [30]

[2] Parts of this user study were published as a poster with an extended abstract [56].

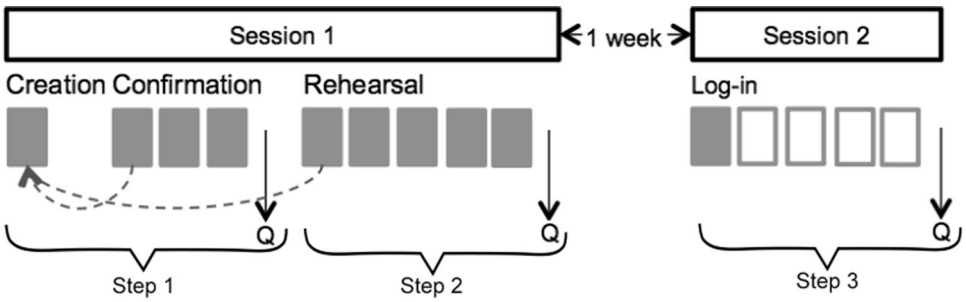


Fig. 4 Study 1 and Study 2—research methodology. There were three main steps (across two sessions): creation and confirmation, rehearsal, and login

usability study of TangibleRubik where users were also presented with a novel tangible password system.

Training Participants were trained on how to use the flexible display prototype and Bend Passwords. We gave a demonstration and then provided participants with an opportunity to familiarize themselves with the prototype. After this, we demonstrated the available bend gestures on the flexible display and asked participants to practice each gesture at least twice or until they were comfortable with performing the gesture. Participants also familiarized themselves with the various feedback mechanisms (i.e., LED light, audio, and GUI) and the control panel (i.e., Undo/Reset and Start/Stop buttons).

Creation Participants completed two password tasks: one on the flexible display and the other on the mobile phone. Task order was counterbalanced. Participants created a password on their first device. They were given very minimal instructions on how to create their passwords and were only instructed to create a secure and memorable password. Participants were told that they would have to re-enter their password in this session and after one week. We configured the two prototypes so that their theoretical password spaces were as close as possible to the suggested minimum of 20 bits [41]. Bend Passwords had a minimum of 5 gestures, giving a theoretical password space of log $(20^5) = 21.6$ bits. PINs were at least 6 digits long, for a theoretical password space of log $(10^6) = 19.9$ bits. Participants were asked to create a new PIN rather than reuse an existing one (although this was not enforceable); reuse was not possible with Bend Passwords because participants did not have any previous experience with the system.

Confirmation Participants confirmed their password by successfully re-entering it three times, with an unlimited number of tries. If they forgot their password, participants went back to the creation stage to create a new password and completed the confirmation stage again with the new password. After successful confirmation, participants completed an online questionnaire providing their opinions and feedback. Participants repeated the password creation and confirmation tasks on the other prototype and completed an online questionnaire.

Rehearsal Participants then rehearsed their first password five times and completed an online questionnaire. This step was designed to help with password memorization. Participants had an unlimited number of tries to successfully rehearse their password five times. If they forgot their password, participants went back to the creation stage to create a new password, and completed the confirmation and rehearsal stages again with the new password, but did not complete the questionnaires again. Participants repeated the rehearsal process with the second password.

4.1.2 Session 2: log-in

Approximately 1 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. The session ended with a short semi-structured interview.

4.2 Participants

Twenty-five participants (12 females) with an average age of 24 years completed the first session and twenty-one returned for the second session. Twenty-two were students and three worked in sales or retail. Nineteen owned at least one smart phone and 14 had a lock enabled on their phone. Of these, 13 (8 PIN and 5 graphical/pattern) unlocked 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 quiet room of our lab and were given $15 compensation for completing both sessions.

4.3 Results

We analysed data from both sessions to compare Bend Passwords with PINs. For session 1, we evaluated the password creation time, password entry time, number of passwords created before successful memorization, and composition of passwords. For session 2, we evaluated the login success rates, login time, and number of login tries. We also evaluated the questionnaire data from both sessions. All statistical analyses are done using a Wilcoxon signed-rank test unless otherwise specified.

4.3.1 Password creation time

Figure 5 shows the creation time of Bend Passwords and PINs. For both passwords, creation time includes the time participants took to come up with their new password and enter it into the system. No significant differences were found between the creation time of Bend Passwords ($M = 52$ s, Md $= 49$ s, SD $= 42$) and PINs ($M = 49$ s, Md $= 36$ s, SD $= 44$ s) ($Z = -861$, $p = 0.389$).

4.3.2 Password entry time

We looked at the password rehearsal time to obtain a measure of password entry time. As participants had mastered their passwords by the rehearsal stage, we believe it is an accurate measure of password entry time. For each participant, we selected the fastest time out of their five successful rehearsals. On average, participants took 15 s ($M = 16$ s, Md $= 15$ s, SD $= 7$ s) to successfully rehearse their Bend Passwords and 5 s ($M = 5$ s, Md $= 5$ s, SD $= 2$ s) to rehearse their PINs. Participants took significantly more time to rehearse their Bend Passwords than their PINs ($Z = -4.374$, $p = 0.000$).

We compared participants' performance at the rehearsal stage with their performance at the confirmation stage to determine whether their performance improved with experience. Participants took significantly less time to rehearse both their PINs ($Z = -3.884$, $p = 0.000$) and Bend Passwords ($Z = -3.354$, $p = 0.001$) than to confirm them. This shows that the password entry time for both PINs and Bend Passwords improved with experience.

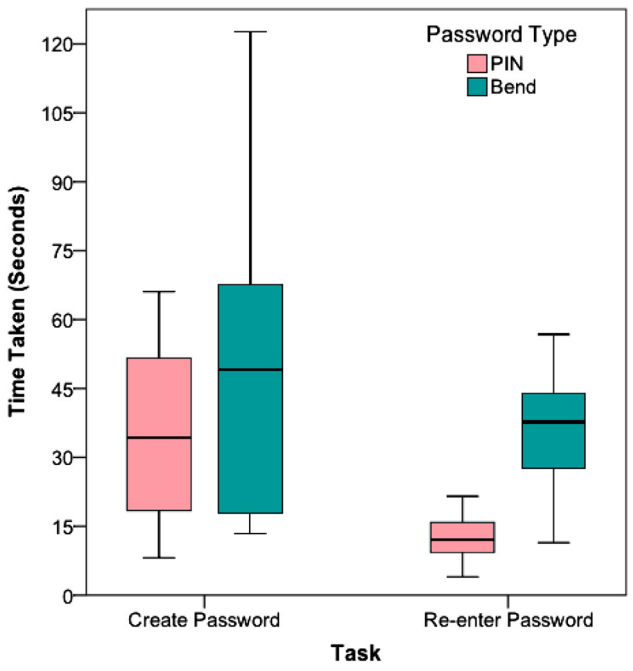


Fig. 5 Study 1—password creation and login times. The login times between conditions are significantly different (*asterisk*)

4.3.3 Number of passwords created

While participants could easily create Bend Passwords, they had difficulty initially creating *memorable* passwords, which led to multiple attempts. We observed that 92 % of participants created only one PIN during the study while 56 % of participants created only one Bend Password. Overall, 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.

4.3.4 Password creation strategies

In the post-task questionnaire of session 1, we asked participants to describe their strategy to create their final passwords. We analysed the responses to this question and the composition of the passwords created.

Bend Passwords Our analysis identified five strategies for Bend Passwords. In the *patterns strategy* (44 %), passwords consist of a series of gestures that form a particular pattern. Patterns observed included the clockwise and mirror patterns. In the clockwise pattern, corners of the display are bent up or down in a clockwise manner, and in the mirror pattern the set of gestures performed on one side of the display are repeated on the opposite side. In the *repeating gestures strategy* (16 %), passwords are created by repeating two or three selected gestures, while in the *drawing strategy* (16 %), bend gestures are used to "draw" a letter (e.g., A), symbol (e.g., sigma) or mental picture (e.g., a five-point star) on the display. Users assigned numbers to each gesture in the *number mapping strategy* (12 %), and passwords are created by performing the series of gestures corresponding to a numerical sequence. In the

natural movements strategy (8 %), passwords are composed of gestures that feel "natural" for the user's hand movements.

PINs Despite being asked to avoid existing PINs, a significant number of participants later admitted to reusing familiar sequences. Participants created their PINs using parts of existing PINs or their personal information. The personal information included old phone numbers, old street addresses, close family members' birthdays, car licence plate numbers, student numbers and favourite course codes.

4.3.5 Password characteristics

Participants created Bend Passwords with an average length of 6 gestures, and PINs with an average length of 7 digits. We observed that the average length of both passwords was close to the required minimum (5 for Bend Passwords and 6 for PINs). The longest Bend Password had 14 gestures, while the longest PIN had 11 digits.

We analysed the composition of Bend Passwords to determine the types of gestures participants used in their passwords. We found that 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 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 %). Participants used more up gestures (72 %) and single bend gestures (63 %). Overall, these results are consistent with the findings of Lahey et al. [7] and Warren et al. [11].

4.3.6 Session 2 login success rate

We evaluated the login success rate by assessing whether participants were able to enter their password correctly in any of the 5 login tries. The success rate was 81 % for Bend Passwords and 86 % for PIN. A McNemar test with continuity correction found no significant difference between the success rates of the two schemes ($\chi^2(1, N = 15) = 0.00$, $p = 1.00$, the odds ratio is 0.67).

The three participants who forgot their PINs used personal information in their PINs and appended random digits. These participants either forgot the random part of their PIN or the structure they used to create it. No commonality was apparent for the four users who forgot their Bend Password. This suggests that password creation strategy did not have an effect on the login success rate of Bend Passwords.

4.3.7 Session 2 login attempts

The majority of participants successfully re-entered their Bend Passwords ($M = 1.53$, $\text{Md} = 1$, $\text{SD} = 0.83$) and PINs ($M = 1.80$, $\text{Md} = 1$, $\text{SD} = 1.21$) in one try. No significant differences were found between the two schemes ($Z = -0.540$, $p = 0.589$).

4.3.8 Session 2 login time

We analysed the login time of participants who successfully remembered their passwords, and only included the time of their successful login attempt. Figure 5 shows the login time for both schemes. Login 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 and 12 s for PINs. Participants took significantly longer to login with their Bend Passwords than their PINs ($Z = -3.294$, $p = 0.001$).

4.3.9 Bend password memorability strategies

We noted different participant strategies for remembering Bend Passwords after a week. 29 % of participants mentally rehearsed their passwords throughout the week, while 12 % only rehearsed them before coming to the second session. Finally, most participants (59 %) reported no explicit strategy or rehearsal. These participants remembered their passwords via muscle memory [51], and some were surprised that they were able to remember their passwords. No participant wrote down their Bend Password.

4.3.10 Questionnaire responses

Participants completed questionnaires at the end of both sessions. We first present the results from six 10-point Likert scale questions measuring the ease of use, perceived security, and likelihood of use of our authentication schemes. Higher Likert scale responses are more positive. Table 2 shows the statistical analysis, and Fig. 6 shows the distribution of the responses. We note that while user perception is important, it does not necessarily reflect the actual security of the system.

Ease of use Participants found it significantly easier to create their PINs than their Bend Passwords. Participants also responded that it was fairly easy to remember both their Bend Passwords and PINs after 1 week, and we found no significant differences between the passwords.

Perceived security We asked participants to rate the overall security of their passwords and found that participants thought their PINs were significantly more secure

Table 2 Study 1: Likert scale responses for user-chosen passwords

Question	Session	PIN Md (SD)	Bend Md (SD)	Stats
Ease of use				
Ease of password creation	1	8.5 (2.18)	6 (2.65)	**($Z = -2.822$, $p = 0.005$)***
Ease of remembering	2	9 (3.19)	9 (2.99)	($Z = -0.134$, $p = 0.893$)
Perceived security				
Overall security	1	8 (2.33)	6 (2.78)	**($Z = -2.108$, $p = 0.035$)***
Secure against shoulder surfing	1	8 (2.13)	7 (2.94)	($Z = -1.763$, $p = 0.078$)
Likelihood of using Bend Passwords				
Use if available	2	–	6 (3.06)	–
Bend versus text	2	–	5 (3.32)	–

Bold and * indicates significance

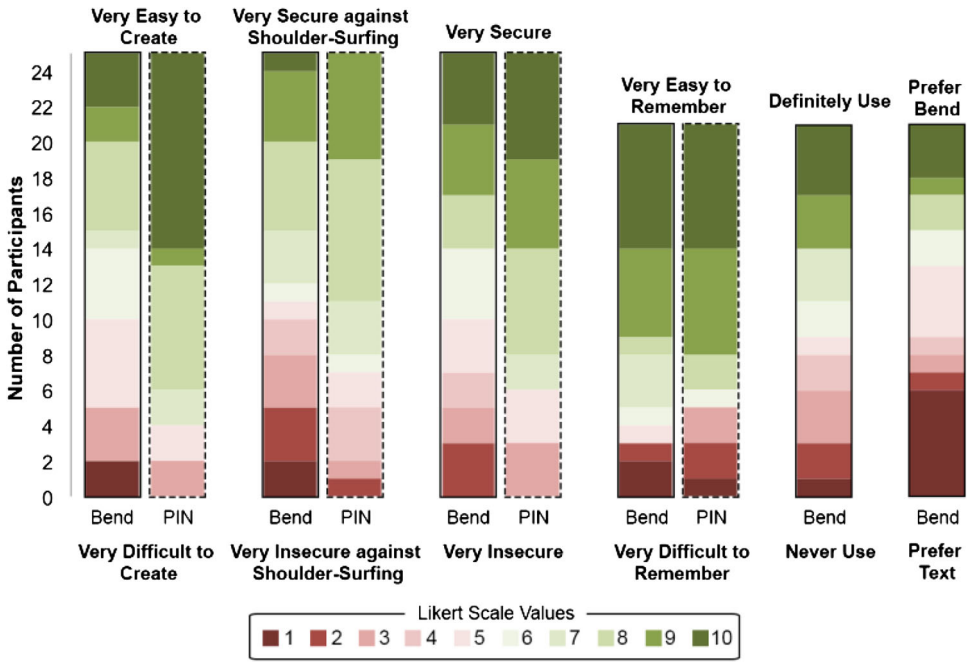


Fig. 6 Study 1—distribution of Likert scale responses for user-chosen passwords

than their Bend Passwords. Participants thought that both passwords would be difficult to shoulder-surf by a malicious user.

Likelihood of using Bend Passwords We asked participants whether they would use a Bend Password if it was available in the future and found that participants were slightly in favour of using Bend Passwords. We further asked participants whether they would prefer a bend or text password on flexible display devices. Participants were neutral in their response.

User feedback We asked participants two open-ended questions about what worked well with our Bend Password system and what could be improved. These questions were also asked in our second study, and a thematic analysis of the responses from both studies revealed common themes. Therefore, we decided to combine the responses and present a combined analysis in Sect. 5.3.10.

4.4 Summary of findings

In Study 1, we evaluated the usability and security of user-chosen bend gesture authentication and compared the results with PINs on a mobile phone. We found that the usability of Bend Passwords was lower than PINs. We believe the lower usability was due to participants' inexperience with our system and limitations of our prototype (Sect. 7). In contrast with PINs, users found it difficult to create memorable Bend Passwords because they had no preconceived password creation strategies. This result

should improve as users gain more experience with Bend Passwords. The higher login times were partially due to higher recall times for Bend Passwords, particularly because many participants admitted to using existing PINs. Prototype limitations, such as the decoupled control panel and lower gesture speed and accuracy, contributed to higher login times. We observed that users frequently used the undo/reset buttons on the control panel to correct errors during password entry, contributing to the higher entry times. Password entry time improved significantly with experience in a single study session. Thus, entry time should further improve as users gain more experience with Bend Passwords.

Bend Passwords were more secure than PINs because participants used secure password creation strategies and were unable to reuse existing passwords. These results are in contrast to users' perception of Bend Password security, which they felt was lower than the security of PINs. It is important that users have a positive perception of the scheme and its security. Users may have rated Bend Passwords lower in security as a precaution because they did not understand their security risks, or because of unfamiliarity.

5 User study 2: system assigned passwords

In our first study, most participants created weak PINs and some created weak Bend Passwords. For PINs, participants used existing numerical passwords or parts of their personal information (e.g., birthdate, phone number). For Bend Passwords, they chose passwords with repeating gestures on one side of the display. 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 compare against system-assigned PINs.

5.1 Methodology

We used a similar methodology to our first study. The only difference was that instead of creating their own passwords, participants were assigned a system generated random Bend Password and PIN. In the first session, participants learned how to use our flexible display prototype and then learned, confirmed and rehearsed a Bend password on the flexible display and a PIN on the mobile phone. If participants forgot their password during confirmation or rehearsal, they could go back to the learning stage to view their password. After a week, participants returned to the lab to complete the second session where they re-entered their passwords.

5.1.1 *Learning passwords*

During the learning phase, participants were shown a random system-assigned password and were asked to memorize the password. Participants were told that they would have to re-enter their password during this session and after one week. They could use any strategy to learn and memorize their passwords.

Bend Passwords Participants were assigned a random 5-gesture Bend Password, which was presented as a sequence of images on the screen (Fig. 7a). Each image represented a bend gesture in the password, and the order of the images represented the order of the gestures in the Bend Password. While learning their passwords, participants could enter bend gestures on the flexible display, and if an entered gesture was included in their password it would get highlighted on the screen (Fig. 7a). We added this functionality to ensure that participants understood each gesture in their password and knew how to perform it correctly.

PINs Figure 7b shows the presentation of a random 6-digit PIN assigned to participants on a mobile phone. Participants learned their PIN through mental rehearsal.

5.2 Participants

Twenty participants (5 females) with an average age of 23 years completed the study. Nineteen owned at least one

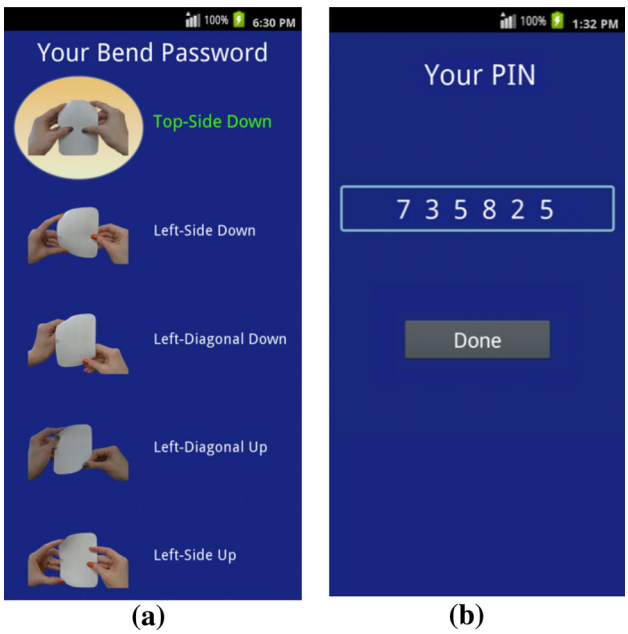


Fig. 7 Presentation of system-assigned passwords. **a** Random 5 gesture Bend Password, with the entered gesture (i.e., Top-Side Down) highlighted. **b** Random 6-digit PIN on a mobile phone

smartphone and 12 had a screen lock enabled on their phone. Of these, 11 (8 PIN and 3 graphical/pattern) unlocked their phone at least four times per day. Only three participants had previous experience with flexible displays: one tried the device at a Samsung Expo, one worked in the field, and one had participated in another bend gesture study within the last year.

5.3 Results

We analysed data from both sessions. For session 1, we evaluated the password learning time, number of times password was viewed, password learning strategies, and password confirmation and rehearsal time. For session 2, we evaluated the success rate, login time, and login attempts. We also looked at the questionnaire data from both sessions, and the post-task interview data from session 2. Twenty participants completed the first session and 19 completed the second session after 1 week. All statistical analyses are done using a Wilcoxon signed-rank test unless otherwise specified.

5.3.1 Password learning time

Participants took significantly ($Z = -3.920$, $p = 0.000$) more time to learn their Bend Passwords ($M = 3.16$ min, Md = 2.26 min, SD = 2.0 min) than their PINs ($M = 28$ s, Md = 17 s, SD = 30 s). From our observations, we note that participants 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 Passwords ($M = 43$, Md = 34.50, SD = 35.46).

A linear regression found that the number of gestures entered significantly predicted participants' password learning time, $b = 0.89$, $t(18) = 8.37$, $p < 0.000$. The number of gestures entered also explained a significant proportion of variance in password learning time, $R^2 = 0.80$, $F(1, 18) = 70.06$, $p < 0.000$. Thus, as expected, the repetitive entry of bend gestures contributed to the longer learning times of Bend Passwords.

5.3.2 Password entry time

Similar to our first study, we used the password rehearsal phase to measure password entry time. Participants took 13 s ($M = 13$ s, Md = 11 s, SD = 6 s) to successfully re-enter their Bend Passwords and 3 s ($M = 3$ s, Md = 4 s, SD = 1 s) to re-enter their PINs. Participants took significantly more time to re-enter their Bend Passwords than their PINs ($Z = -3.930$, $p = 0.000$).

We compared participants' password confirmation and rehearsal times, and found that participants took significantly less time to rehearse their PINs ($Z = -3.831$, $p = 0.000$) and Bend Passwords ($Z = -3.087$, $p = 0.002$) than to confirm them. These results show that by the end of session 1, participants had learned their passwords well and were getting progressively faster with practice.

5.3.3 Number of times password viewed

We looked at the number of times participants visited the learning stage to view their passwords. Most viewed their PINs (95 %) and Bend Passwords (75 %) only once and few forgot them at the confirmation or rehearsal stage. However, we found that participants visited the learning stage significantly more ($Z = -2.24$, $p = 0.025$) for Bend Passwords ($M = 1.30$, Md = 1, SD = 0.571) than for PINs ($M = 1.05$, Md = 1, SD = 0.224).

5.3.4 Password learning strategies

In the post-task questionnaire of session 1, we asked participants to describe the strategies they used to learn their passwords. 95 % of participants reported using a strategy.

Bend Passwords Our thematic analysis revealed four strategies for Bend Passwords. Participants repeatedly entered their password into the device during the learning stage, until they memorized the gesture sequence in the *repeated entry strategy* (55 %). They memorized the movements (gestures) of their password by performing the movements multiple times. Some verbally rehearsed the gestures (e.g., "Top corner up") while entering them. Participants found and memorized a pattern between the gestures in the *patterns strategy* (15 %).

Users broke down the password into components in the *password composition strategy* (15 %). 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). Gestures were mapped to a user's mental representation of an object or sequence, in the *mapping strategy* (10 %). Users assigned numbers to each gesture and memorized the sequence of numbers, assigned musical notes to gestures or memorized the "melody" formed by the gestures.

PINs Three strategies were found to learn PINs, and each involved some type of rehearsal. In the *mental rehearsal strategy* (35 %), PINs were mentally rehearsed until memorized. We consider this a "brute-force" method of memorization. Users found and memorized a pattern between the digits in the *finding a pattern strategy* (40 %). Patterns included using a mathematical formula to add or

multiply digits, treating the digits as a date (YY/MM/DD), and treating the PIN as a set of ages in life (e.g., 20 45 89). In the *chunking strategy* (20 %), users broke the PIN into chunks [52] of two digits and remembered the order between the chunks.

5.3.5 Session 2 login success rate

After 1 week, 63 % of participants successfully remembered their Bend Passwords and 74 % remembered their PINs. We define success rate as the number of participants who successfully re-entered their password within 5 tries. A McNemar test found no statistically significant difference between the success rates ($\chi^2(1, N = 19) = 0.688$, $p = 1.00$, the odds ratio is 1.63).

At the end of the second session, we asked participants whether they rehearsed their passwords after leaving the first session. Most mentally rehearsed their Bend Passwords (74 %) and PINs (68 %) at least twice. Only one participant admitted to writing down their PIN. As in the first study, no participant reported writing their Bend Passwords; most 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.

5.3.6 Session 2 login time

The average login time for Bend Passwords was 34 s ($M = 34$ s, Md = 32 s, SD = 19 s) and 13 s for PINs ($M = 13$ s, Md = 9 s, SD = 8 s). Participants took significantly more time to re-enter their Bend Passwords than their PINs ($Z = -1.599$, $p = 0.009$).

5.3.7 Session 2 login attempts

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 = 0.422). We found no statistically significant difference between the login attempts of Bend Passwords and PINs ($Z = -1.289$, $p = 0.197$).

5.3.8 Questionnaire responses

Participants completed the same questionnaires as in our user-chosen password study, and we analysed their responses using the same method. Figure 8 shows the distribution of responses for the Likert scale questions and Table 3 shows the statistical analysis.

Ease of use Participants found it significantly easier to learn their PINs than their Bend Passwords, but there was no difference in their perceived memorability. Participants found it easy to remember both their Bend Passwords and PINs. *Perceived Security:* Participants felt that both their PINs and Bend Passwords were very secure overall and would be difficult for malicious users to shoulder-surf.

Likelihood of using Bend Passwords Participants were slightly in favour of using Bend Passwords in the future, but when asked whether they would use a bend or text password, participants were neutral in their responses.

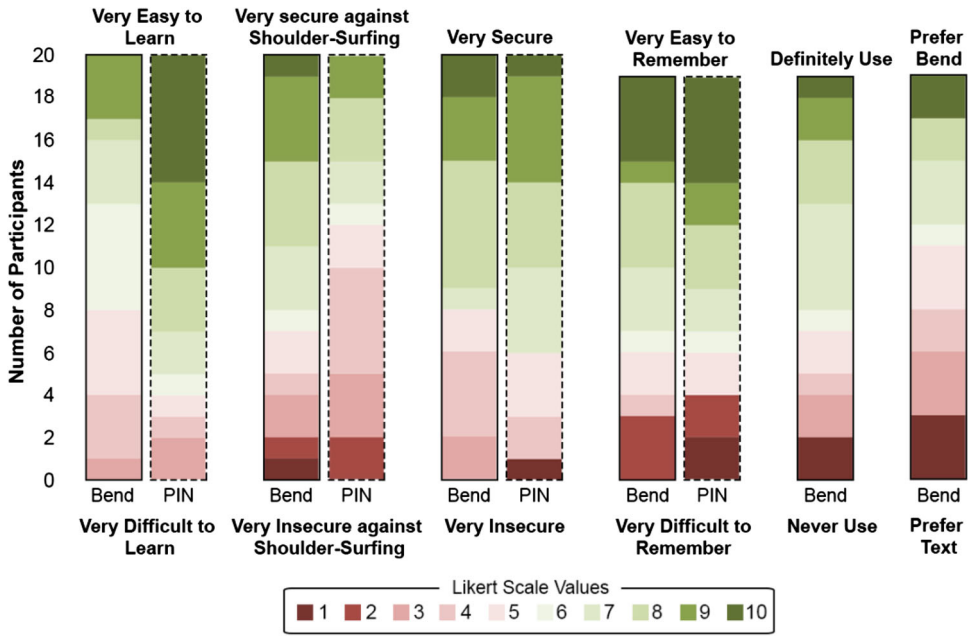


Fig. 8 Study 2—distribution of Likert scale responses for system-assigned passwords

Table 3 Study 2: Likert scale responses for system-assigned passwords

Question	Session	PIN Md (SD)	Bend Md (SD)	Stats
East of use				
Ease of learning	1	8.5 (2.38)	6 (1.76)	**($Z = -2.876$, $p = 0.004$)***
Ease of remembering	2	8 (3.21)	7 (2.75)	($Z = -0.506$, $p = 0.613$)
Perceived security				
Overall security	1	8 (2.41)	8 (2.24)	($Z = -0.520$, $p = 0.603$)
Secure against shoulder surfing	1	4.50 (2.31)	7 (2.64)	($Z = -1.394$, $p = 0.163$)
Likelihood of using Bend Passwords				
Use if available	2	–	7 (2.64)	–
Bend versus text	2	–	5 (2.81)	–

Bold and * indicates significance

5.3.9 Interview responses

In this section, we analyse the responses from three interview questions at the end of the study. The first two questions assess participants' attitudes towards system-assigned passwords, and the third assesses their likelihood of using Bend Passwords compared to PINs.

Attitudes towards system assigned passwords We asked participants "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 passwords to make them more memorable. We further asked "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 %).

Bend versus PIN 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. Some participants chose Bend Passwords because they thought these passwords would be more natural to use, easier to remember (e.g., lack of interference), and more secure (because of complexity) than PINs. Others chose PINs because of familiarity and possibility of reuse. Some participants wanted more experience with the system before choosing a password type. These participants also stated that their choice would be 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 of its faster entry time.

5.3.10 User feedback

We asked participants two open-ended questions in the questionnaire for session 1. Since we asked these questions in both studies (user-chosen and system-assigned) and responses were similar, we grouped the responses together. A total of 45 responses were analysed.

Features that worked well During our thematic analysis, the following six themes emerged for the question "what do think worked well with the Bend Password system?"

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 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. In particular, 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 touch-based interaction on their mobile device. This would be beneficial in situations such as extreme weather (e.g., winter), where users currently 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 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 response to the question "what do you think could be improved with the Bend Password system?"

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 and used the improved prototype in our second study.

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 including adding smaller (i.e., more subtle) gestures and increasing the speed with which users can enter gestures.

5.4 Summary of findings

We explored system-assigned Bend Passwords and compared the results with system-assigned PINs. The usability of system-assigned Bend Passwords was lower than system-assigned PINs. Participants took more time to learn their Bend Passwords because of their learning strategy (repeated entry) and inexperience with our system. Although users forgot their Bend Passwords more often than PINs in the confirmation/rehearsal stages of session 1, they remembered both passwords equally well in session 2. Thus, users found it difficult to initially learn the Bend Passwords, but once learned they remembered them well after one week. Similar to our first study, users had high login times for Bend Passwords, which we believe can be improved with experience and by correcting some limitations of our prototype.

Similar to our first study, user perception of Bend Passwords was neutral. Participants liked the available bend gestures and the feedback provided by the system. They also liked the novelty of the system and the ability to enter passwords without using the touch-based input of the device. Many participants wanted to see improvements in the speed and accuracy of gestures, and some wanted the ability to use more complex gestures in their passwords.

5.5 Comparison of user-chosen and system assigned passwords

We compared the measures of password creation/learning time, login success rates, login time, perceived memorability, and perceived risk of shoulder surfing from our two studies. We used the Mann–Whitney U test to compare the password creation/learning time, perceived memorability and perceived risk of shoulder surfing, and we used Fisher's Exact test to compare the success rates. Table 4 shows these comparisons.

Table 4 Comparison of results from the user-chosen (UCP) and system-assigned (SAP) password studies

Measure	Password	Session	UCP	SAP	Stats
Creation time	Bend	1	26 s (55 s)	146 s (108 s)	**($U = 24$, $p = 0.000$)***
	PIN		35 s (15 s)	17 s (30 s)	($U = 73.0$, $p = 0.067$)
Login success rate	Bend	2	67 %	63 %	($p = 1.000$)
	PIN		89 %	74 %	($p = 0.630$)
Login time	Bend	2	35 s (9 s)	32 s (19 s)	($U = 27$, $p = 0.398$)
	PIN		10 s (2 s)	9 s (7 s)	($U = 55$, $p = 0.973$)
Perceived memorability	Bend	2	7 (3.43)	7 (2.75)	($U = 79$, $p = 0.746$)
	PIN		10 (2.32)	8 (3.21)	**($U = 44.5$, $p = 0.037$)***
Perceived risk of shoulder surfing	Bend	2	4 (2.84)	7 (2.64)	($U = 77.5$, $p = 0.175$)
	PIN		8 (1.96)	4.50 (2.31)	**($U = 63.0$, $p = 0.024$)***

Bold and * indicates significance. Login success rates are expressed as a percentage and all other measure are represented by their medians (SD)

5.5.1 Participants

In the user-chosen password (UCP) study, participants created passwords of varying lengths while in the system-assigned (SAP) study, the password length was fixed (Bend: 5 gestures, PINs: 6 digits). To compare the results, we selected participants from the user-chosen study who either created a 5-gesture Bend Password or a 6-digit PIN and compared their results with all participants in the system-assigned study. For Bend Passwords, we compared 11 UCP and 20 SAP participants, and for PINs, we compared 12 UCP with 20 SAP participants.

5.5.2 Bend Passwords

Participants took significantly more time to learn their system-assigned Bend Passwords ($M = 188$ s) than to create their user-chosen Bend Passwords ($M = 54$ s). The majority successfully remembered both their system-assigned (63 %) and user-chosen (67 %) Bend Passwords after 1 week, and there were no significant differences between the success rates ($p = 1.000$) or the login time. No significant differences were found between the perceived memorability and perceived risk of shoulder surfing of both Bend Passwords.

5.5.3 PINs

On average, participants took 35 s to create their user-chosen PINs and 28 s to learn their system-assigned PINs. There were no significant differences between the creation and learning time of user-chosen and system-assigned PINs. After 1 week, the success rates of PINs in both studies were fairly high (UCP: 89 %, SAP: 74 %) and there were no significant differences between the success rates ($p = 0.630$). Similarly, no significant differences were found for login time. Participants thought that their user-chosen PINs were more memorable after 1 week and believed that they would be harder to shoulder-surf compared to system-assigned PINs.

5.5.4 Summary of comparisons

We found that participants took more time to learn their system-assigned Bend Passwords than to create their own Bend Passwords. Except this, no differences in user performance were found between user-chosen and system-assigned Bend Passwords. We found that users preferred their user-chosen PINs and found them to be more memorable and secure than their system-assigned PINs. Interestingly, no such differences were found for Bend Passwords.

6 User study 3: shoulder-surfing susceptibility of passwords

In our third study[3] we evaluated the shoulder-surfing susceptibility of Bend Passwords compared to PINs. In our study, the experimenter played the role of a victim and participants played the role of malicious users, similar to Tari et al. [39] and Schaub et al.'s [53] 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.

[3] Parts of this user study were published as a poster with an extended abstract [57].

6.1 Methodology

In the 1-h study, participants were trained on our flexible display prototype and Bend Password scheme before proceeding to the shoulder-surfing tasks. The training session followed the same methodology as our first two studies.

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 the right or left, and observed the password entry. They were allowed to move around and change their position to find the best viewing angle. Figure 9 shows the set-up of the experiment. During observation, participants could take notes on a provided piece of paper. After observing each password entry, participants were given three tries to correctly guess the observed password. After observing and guessing eight passwords on the first device, the experimenter switched devices 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 passwords.

6.1.1 Passwords

Participants observed 8 passwords of each type. These passwords were selected using a factorial design, with password type (Bend or PIN), hand position (moving or stationary) and password strength (low or medium) as variables. The experimenter entered two passwords for each combination of factors, for a total of 16 passwords per participant (2 password types $\times$ 2 hand positions $\times$ 2 strength levels $\times$ 2 trials). For each password type (Bend or PIN), 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 PINs with no obvious pattern, but tried to incorporate digits from across the keyboard.

Hand position For hand position, *moving* means the experimenter's hands were moving across the device during password entry and *stationary* means their hands were stationary.

Bend In the moving condition, passwords contained gestures on all four corners of the device so that the experimenter's hand moved across the device during password entry. In the stationary condition, the experimenter positioned their hands on two corners of the device and performed gestures using only these corners.

PIN In the moving condition, the experimenter held the phone in their left hand and entered PINs using their right hand, which moved across the device. For the stationary condition, the experimenter held the phone in their right hand and entered PINs using only their right thumb.

Password strength 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 (low) and 34 bits (medium). We chose 20 bits as low strength because it is the recommended password space in the literature [38], and we chose 34 bits as medium strength to match the length of Bend Passwords to commonly used 8 character alphanumeric text passwords. Table 5 shows the length of the Bend Passwords and PINs.

6.1.2 User interface/visual feedback

When the experimenter entered passwords on the flexible display, participants did not receive any feedback from the system, such as the asterisk appearing in the password

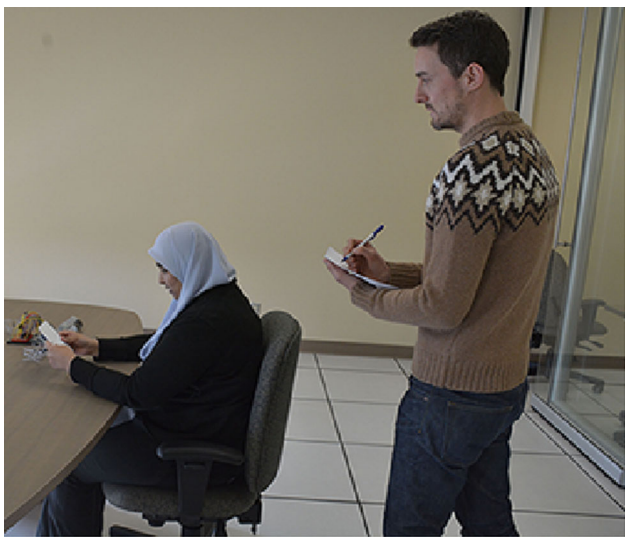


Fig. 9 Shoulder-surfing study setup

Table 5 Length of the passwords shoulder-surfed

Password type	Password strength	
	Low (20 bits)	Medium (34 bits)
Bend	5 gestures	8 gestures
PIN	6 digits	10 digits

field. However, they did receive this feedback while guessing the observed passwords. 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 flexible display rather than the projected UI.

For PINs, we used the alphanumeric keyboard of the mobile device (Fig. 3b) rather than the larger commonly used PIN keypad due to technical limitations. However, we believe the smaller keys of the alphanumeric keyboard would make it harder to shoulder-surf PINs, therefore increasing the threshold against which our scheme was assessed. 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 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. Only a dot was displayed with each digit entry during the observation and guessing of PINs. In effect, we tried to devise the most difficult comparison condition possible to avoid overstating Bend Passwords' resistance to shoulder surfing.

6.2 Participants

Our nine participants (seven males) had an average age of 28 years. All participants had participated in a prior study on bend gestures within the last 6 months (six had participated in the user-chosen password 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 quiet room of our lab and were given $10 compensation.

6.3 Results

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

6.3.1 Success rates

We define 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 × 9 participants), a total of 3 were guessed correctly: one bend and two PINs. Users found it extremely difficult to shoulder-surf both Bend Passwords and PINs.

6.3.2 Degree of correctness

Given the low success rates and apparent floor effects, we conducted a post hoc analysis to explore the composition of users' guesses using Levenshtein distance [54]. 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 Bend Passwords. 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 (i.e., most accurate), which gave us an end result of 8 passwords per participant (4 Bend Passwords and 4 PINs).

Figure 10 shows the Levenshtein distances for PINs and Bend Passwords. As this was post hoc exploration with a small sample, we opted not to conduct any statistical analysis. However, the figure shows that most users had

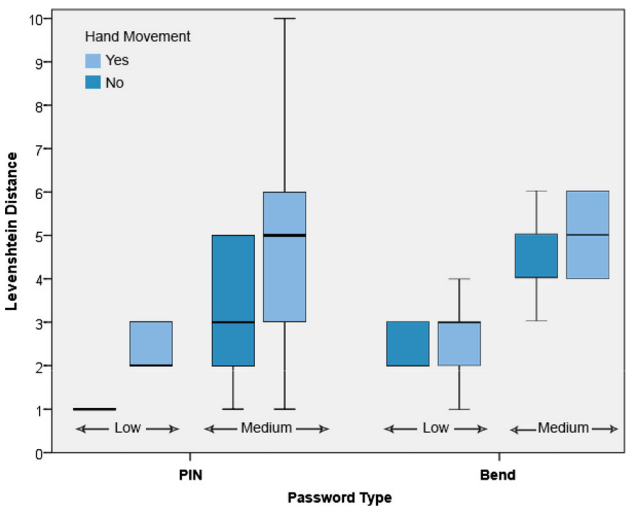


Fig. 10 Levenshtein distance for PINs and Bend Passwords. Low and medium are the theoretical passwords strengths

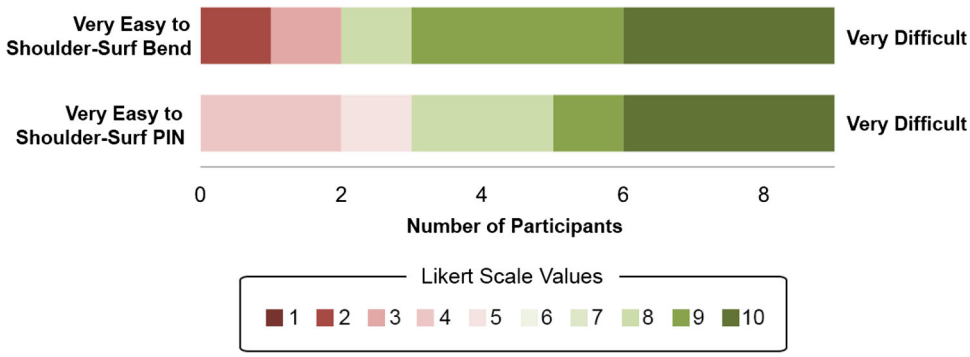


Fig. 11 Distribution of Likert scale responses for the shoulder-surfing study

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 to shoulder-surf. Compared to PINs, Bend Passwords seemed to be more difficult to shoulder-surf, but this needs further testing.

6.3.3 Questionnaire responses

We asked participants two questions in the post-task questionnaire. The first question used a 10-point Likert scale (1 = very easy, 10 = very difficult) to measure participants' ease of shoulder-surfing the passwords. The second question was open-ended and participants described their shoulder-surfing strategies.

Ease of shoulder surfing Figure 11 shows the distribution of responses to the first question. Participants found it very difficult to observe and replicate both Bend Passwords ($M = 7.78$, $\text{Md} = 9$, $\text{SD} = 3.07$) and PINs ($M = 7.56$, $\text{Md} = 8$, $\text{SD} = 2.55$). A Wilcoxon signed-rank test showed that there was no significant difference between the difficulty of shoulder-surfing PINs and Bend Passwords ($Z = -0.212$ $p = 0.832$).

Strategies used for shoulder surfing For PINs, participants mostly 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. Most participants (78 %) did not change their PIN shoulder-surfing strategy during the study. 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 and kept them in their working memory instead of taking notes. They mentally rehearsed the digit sequence 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.

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 effective, 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, because they have too many components to remember. 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.

6.4 Summary of findings

In this study, we evaluated the shoulder-surfing susceptibility of Bend Passwords and PINs. We found that the shoulder-surfing success rates of both Bend Passwords and PINs were extremely low, but certain types of passwords were easier to shoulder-surf. Specifically, PINs, shorter passwords, and passwords where the experimenter's hand was not moving on the device were easier to shoulder-surf. 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). 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. Qualitative data revealed that participants

found both Bend Passwords and PINs very difficult to shoulder-surf.

7 Limitations

In this section, we address the limitations of our work. The prototype limitations apply to all three studies.

7.1 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. Although it could be projected onto the device, most users chose to project the GUI onto the wall. Users had to shift their attention between the flexible display, the user interface projection, and the control panel when completing the password tasks. This led to longer entry times for Bend Passwords and negatively affected users' perception. Our prototype sometimes registered gestures incorrectly if entered too fast. This also contributed to the longer Bend Password entry times. In addition, multi-gestures had to be performed simultaneously, and if a corner was not bent "enough" the gesture registered incorrectly. These limitations may be addressed through hardware improvements and by improving the gesture recognition algorithm.

The limitations of the prototypes negatively affected the results from our user studies. Other than a minor update to the algorithm after the first study, we chose to use the same prototype in all three studies because each study explored different aspects of Bend Passwords, and we needed a well-rounded evaluation in order to provide reasonable recommendations. We also wanted the ability to compare the results from our user studies to make reasonable conclusions and recommendations.

7.2 User-chosen and system-assigned password user studies

A main limitation of our user studies was that participants were novice users of flexible displays. Most had not even heard of flexible displays prior to participating in our study. We believe this affected participants' performance because they were learning how to use the flexible display while creating/learning their Bend Passwords. With regard to password memorability, we tested participants' retention a week after password creation. In real life, users typically use their password at least once a day to unlock their phone. Thus, it is possible that with more usage, participants may show improved retention. We used an alphanumeric keyboard for PINs instead of the regular numerical keypad, because of the technical limitations of the implementation platform. This may have affected the PIN entry speed, but since the PIN results were very positive, we believe this did not significantly affect the results.

7.3 Shoulder-surfing user study

We would need to run the shoulder-surfing study with a larger sample size to validate and generalize our findings. Furthermore, participants did not receive any GUI feedback while shoulder-surfing Bend Passwords. 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. In addition to this, even if visual feedback had been provided, participants would have been unlikely to see it when the device was deformed for gesture entry.

8 Discussion and design recommendations

In this section, we address further usability and security implications of Bend Passwords and propose eight design recommendations.

8.1 Use of muscle memory

Several participants referred to "muscle memory" in relation to their Bend Passwords. Muscle memory, a type of procedural implicit memory, occurs through repeated practice when a person learns to perform a motor skill with little conscious thought [51]. This is indeed a powerful advantage to Bend Passwords since with additional usage, entering passwords would become an automatic action requiring little conscious effort and this may facilitate recall. Using muscle memory has long been advocated as a desirable characteristic of user interfaces when appropriate [55]. With the advantage of muscle memory, system-assigned Bend Passwords could be viable, which has the obvious security advantages of removing the predictability of user-chosen passwords.

8.2 Novelty effects

Results from the usability evaluations of new authentication schemes can sometimes be affected, positively or negatively, by the novelty of the scheme. Users may provide positive feedback for an authentication scheme because of increased interest in the scheme and not because of actual usability improvements. In our studies, it is possible that users may have provided positive feedback for Bend Passwords through the questionnaires and post-task interviews because of novelty effects. However, we believe these were tempered with negative novelty effects because

users were unfamiliar and inexperienced with Bend Passwords and our flexible display prototype.

8.3 Security

Three common threats to mobile authentication schemes are social engineering attacks, guessing attacks, and shoulder-surfing attacks. We discuss the security of Bend Passwords with respect to their resistance to these attacks.

8.3.1 Social engineering attacks

In social engineering, attackers psychologically manipulate users into divulging their password. Since users have no easy way of writing down their Bend Passwords or sharing them with other users (possibly an attacker), we believe that Bend Passwords are more resistant to social engineering attacks than PINs. Users may develop Bend Password sharing strategies (i.e., video recording gesture entry) as these passwords become mainstream, but these sharing strategies require significantly more effort.

8.3.2 Guessing attacks

Guessing attacks involve guessing a password by trying all possible combinations (*brute-force*), using personal information about the user (*targeted*), or trying commonly used passwords (i.e., *dictionary*, leaked password lists). Thus, these attacks are successful when users use short, simple passwords, use personal information in their passwords, reuse existing passwords, or create commonly used passwords (i.e., using predictable patterns).

Participants created Bend Passwords using a variety of different strategies with few obviously exploitable patterns. We did, however, note a slight preference for "up" gestures because these were easier to perform on our prototype. This could be used by attackers to prioritize guesses in an attack. A more realistic and usable prototype may eliminate this bias. On the other hand, most participants created their PINs using personal information or reused existing PINs even when advised against it.

Participants seemed motivated to create strong Bend Passwords. They included a variety of bend gestures in their passwords, which would make them more resistant to brute-force guessing attacks. Interestingly, 86 % of participants used at least one multi-gesture in their password, even though these were harder to perform, because they associated the use of multi-gestures with increased password security. Some even compared them to using special characters in text-based passwords. Participants believed that this strategy would make their passwords more resilient against malicious attacks.

Finally, we note that Bend Passwords have a larger theoretical password space than PINs, which means that for Bend Passwords and PINs of equal length, the Bend Password would take more time to guess using a brute-force attack.

With increased usage, it is possible that users may develop predictable password creation strategies, making their Bend passwords more susceptible to guessing attacks. Because of this concern, we looked at system-assigned Bend Passwords, which would eliminate this risk by making all passwords equi-probable. Other than longer learning times, system-assigned passwords were as usable as user-chosen ones. If security against guessing attacks is a concern, then we recommend system-chosen passwords.

8.3.3 Shoulder-surfing attacks

Bend Passwords were extremely difficult to shoulder-surf in our study explicitly exploring this attack. We believe this was because Bend Passwords have a large number of components to track (i.e., gesture type, location and direction), requiring observers to take notes during observation and increasing their memory load.

In our study, observers lacked effective note-taking strategies which made it difficult for them to track and reproduce the observed gestures. Shoulder surfers may eventually develop better strategies, but we see it as a positive result that our participants found it very difficult to shoulder-surf Bend Passwords despite some participants' initial assumptions that it would be easy. Even with additional experience, shoulder-surfing Bend Passwords should remain more labour-intensive and conspicuous than for traditional PINs.

We also found that certain password characteristics increased resistance to shoulder-surfing. Specifically, longer passwords with independent gestures/digits were more difficult to observe. Similarly, passwords requiring hand movement meant that observers had difficulty tracking the keys or gestures entered. Like most knowledge-based authentication schemes, Bend Passwords may still be susceptible to video recording attacks. However, Bend Password with hand movement may somewhat occlude password entry and provide some protection.

8.4 Real-world application

Our user studies show that Bend Passwords have an acceptable level of security, but lower usability than PINs, primarily due to the speed of password entry. In order for Bend Passwords to be a viable authentication scheme for flexible displays, the hardware of these devices must support a high password entry speed and gesture accuracy, which may be possible in the near future. When these

capabilities are supported by the hardware, we envision using Bend Passwords to unlock mobile devices, acting as PIN replacements. It may be possible to modify the configuration of the scheme to strengthen it sufficiently to make it suitable for password replacement, but this would require further exploration.

To maintain an acceptable level of security against the attacks described above, we recommend that future implementations use system-assigned passwords. This could ensure that passwords incorporate both single and multi-gestures, gesture in both directions (i.e., up and down), and all locations (i.e., all four corners) of the device. If user-chosen passwords are allowed, then the system should enforce minimum password rules, such as using at least one multi-gesture in the password, and requiring some gestures involving hand movement.

Bend Passwords could be used to complement existing authentication schemes such as PINs or the Android Pattern Lock. This would allow users to increase the security of their passwords by combining the theoretical password spaces of two authentication schemes. Because Bend Passwords have many possible gestures, users would only need to add a few bend gestures to their password to achieve the desired security level. Combining Bend Passwords with an existing authentication scheme could be more advantageous, in terms of usability, than combining two existing authentication schemes (i.e., PINs and Text passwords) because Bend Passwords use a different input modality than all existing touch-based authentication schemes.

8.5 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 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.

8.5.1 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 visual and auditory feedback to the user when they entered a gesture or their password. When a gesture was entered, the system changed the colour of an LED light affixed to the display, emitted a clicking sound, and displayed an asterisk on the projected UI. Participants used them extensively and user comments revealed that they 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 authenticating in a noisy place they can rely on the visual feedback instead of auditory feedback. However, the use of these feedback mechanisms should be optional and easily controllable by users. When users are in an environment where observation is a concern, they could temporarily turn off the feedback, and re-enable it when they are in a safe environment.

R2: Feedback should differentiate single and multi-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 colour 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 colour 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 to bend the corners of the display (degree and speed of bend) 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 to observe the characteristics of a password. 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.

8.5.2 Device characteristics

Our next set of recommendations relates 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 within the device.

In our user studies, we observed that each participant performed bend gestures 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 hands. Users with large hands applied more physical force to perform a bend gesture than users with small hands. Thus, 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 should 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 positioned to facilitate entering of one-handed bend gestures.

The dimensions of our flexible display were $135 \times 95 \times 1.5$ mm, which were slightly wider than the dimensions of the mobile phone used in our PIN condition ($136.6 \times 70.6 \times 8.6$ mm). 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 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 hands to perform many of our bend gestures, which many found inconvenient. Therefore, we recommend that bend sensors should be placed in the corners as well as the sides to recognize a wider range of gestures.

8.5.3 User interaction

Gesture language In this section we provide 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. 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, we recommend including the following types of gestures in the gesture set for Bend Passwords:

- Bending each corner of the display up or down.
- Folding and bending the sides of the display.
- Using gestures with different angles of bend.
- Bending multiple corners of the display simultaneously, either in the same or different directions. This gesture would require 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 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. 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 regard 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 decoupled from the flexible display, to confirm, reset or undo their password entry, which disrupted their password entry task and significantly affected password entry times. 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 from the flexible display. However, we believe that these effects will still exist in real flexible display devices (with no decoupling issues) and will affect user performance, if the transition between touch and bend is not seamless.

9 Conclusion

In summary, the results from our three 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 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 paper with design recommendations for the eventual implementation of bend authentication on real flexible display devices.

Acknowledgments This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC). Sonia Chiasson holds a Canada Research Chair in Human Oriented Computer Security and acknowledges funding for the Chair and Discovery Grants. Audrey Girouard also acknowledges funding for her Discovery Grant. The authors also acknowledge funding from NSERC ISSNet.

Appendix

See Fig. 12.

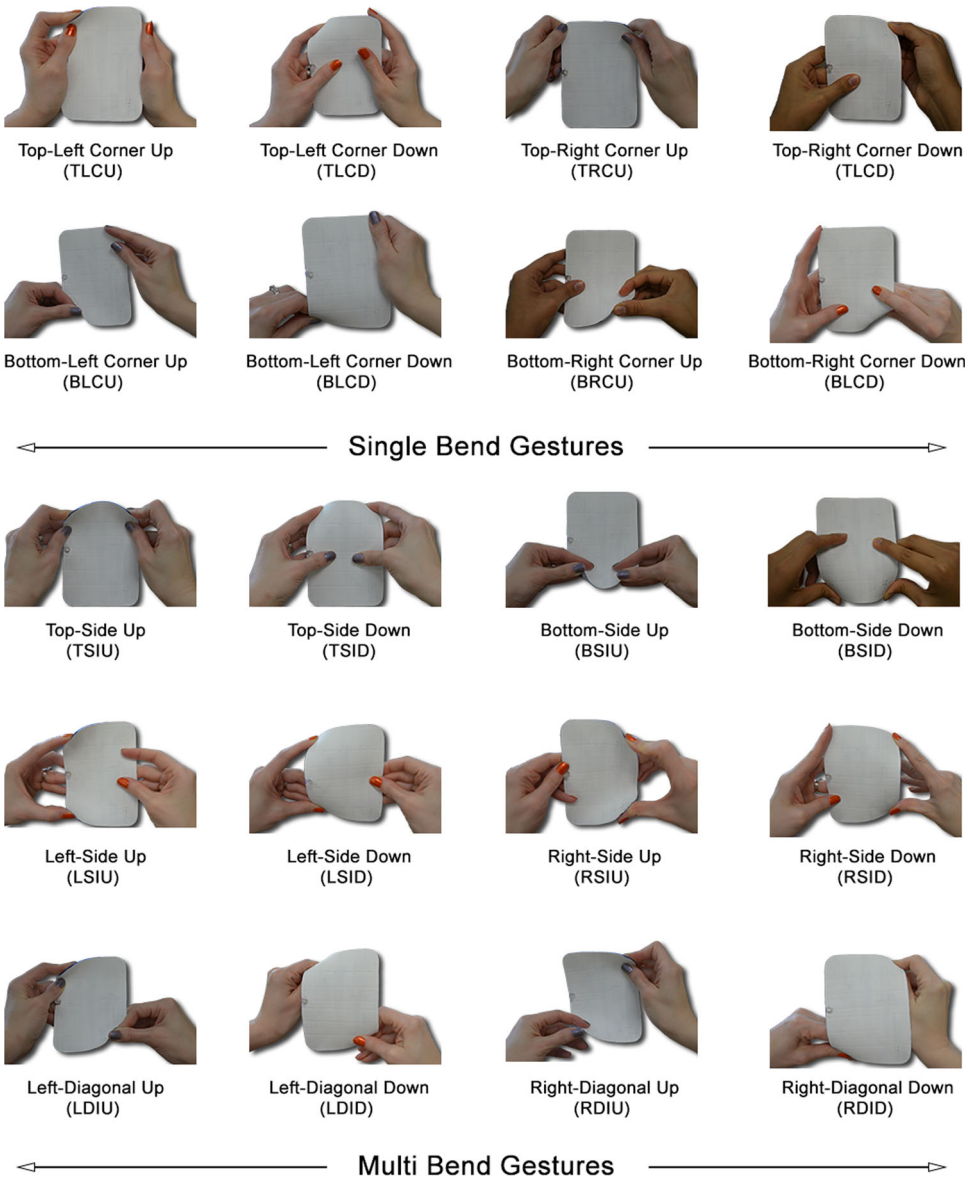


Fig. 12 The set of bend gestures available on the flexible display prototype

References

1. Mobile Technology Fact Sheet (2014) http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/. Accessed on 09 July 2015
2. Adams A, Sasse MA (1999) Users are not the enemy. Commun ACM 42(12):40–46
3. Beust C (2008) Cedric's weblog: Android's locking pattern. http://beust.com/weblog2/archives/000497.html. Accessed on 09 July 2015
4. Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM (2010) Smudge attacks on smartphone touch screens. In: Proceedings of the conference on offensive technologies, 2010, pp 1–7
5. Agomuoh F (2014) Samsung flexible display phone coming in 2015? http://www.ibtimes.com/samsung-flexible-display-phone-coming-2015-manufacturer-secretly-showcases-foldable-amoled-display. Accessed on 09-July 2015
6. Kildal J, Paasovaara S, Aaltonen V (2012) Kinetic device: designing interactions with a deformable mobile interface. In: Proceedings of the 30th SIGCHI conference on human factors in computing systems extended abstracts (CHI-EA), 2012, pp 1871–1876
7. Lahey B, Girouard A, Burleson W, Vertegaal R (2011) 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, 2011, pp 1303–1312
8. Schwesig C, Poupyrev I, Mori E (2004) Gummi: a bendable computer. In: Proceedings of the 22nd SIGCHI conference on human factors in computing systems, 2004, pp 263–270
9. Watanabe J, Mochizuki A, Horry Y (2008) Bookisheet: bendable device for browsing content using the metaphor of leafing through the pages. In: Proceedings of the 10th international conference on ubiquitous computing, 2008, pp 360–369
10. Wightman D, Ginn T, Vertegaal R (2011) BendFlip: examining input techniques for electronic book readers with flexible form factors. In: Proceedings of the 13th IFIP TC13 conference on human-computer interaction, 2011, pp 117–133

11. Warren K, Lo J, Vadgama V, Girouard A (2013) Bending the rules: bend gesture classification for flexible displays. In: Proceedings of the 31st SIGCHI conference on human factors in computing systems, 2013, pp 607–610
12. Ye Z, Khalid H (2010) Cobra: flexible displays for mobile gaming scenarios. In: Proceedings of the 28th SIGCHI conference on human factors in computing systems extended abstracts, 2010, pp 4363–4367
13. Burstyn J, Banerjee A, Vertegaal R (2012) FlexView: an evaluation of depth navigation on deformable mobile devices. In: Proceedings of the 6th conference on tangible, embedded, embodied interaction, 2012, pp 193–200
14. Lee S-S, Kim S, Jin B, Choi E, Kim B, Jia X, Kim D, Lee K (2010) How users manipulate deformable displays as input devices. In: Proceedings of the 28th SIGCHI conference on human factors in computing systems, 2010, pp 1647–1656
15. Kildal J, Lucero A, Boberg M (2013) Twisting touch: combining deformation and touch as input within the same interaction cycle on handheld devices. In: Proceedings of the international conference on human-computer interaction with mobile devices and services, 2013, pp 237–246
16. Steimle J, Jordt A, Maes P (2013) Flexpad: highly flexible bending interactions for projected handheld displays. In: Proceedings of the 31st SIGCHI conference on human factors in computing systems, 2013, pp 237–246
17. Girouard A, Lo J, Riyadh M, Daliri F, Eady AK, Pasquero J (2015) One-handed bend interactions with deformable smartphones. In: Proceedings of the 33rd annual ACM conference on human factors in computing systems, 2015, pp 1509–1518
18. Saltzer J, Schroeder M (1975) The protection of information in computer systems. In: Proceedings of the 4th symposium on operating system principles, 1975, vol 63, Issue 9, pp 1278–1308
19. Yan J, Anderson R, Grant A (2005) The memorability and security of passwords. In: Cranor L, Garfinkel S (eds) O'Reilly media, pp 129–142
20. Rogers J (2007) Please enter your 4-digit PIN. Financ. Serv. Technol. US Ed., no. 4
21. Schaub F, Deyhle R, Weber M (2012) Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In: Proceedings of the 11th international conference on mobile and ubiquitous multimedia, 2012, pp 13:1–13:10
22. von Zezschwitz E, De Luca A, Hussmann H (2014) Honey, I shrunk the keys: influences of mobile devices on password composition and authentication performance. In: Proceedings of the 8th nordic conference on human-computer interaction: fun, fast, foundational, 2014, pp 461–470
23. von Zezschwitz E, Dunphy P, De Luca A (2013) 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, 2013, pp 261–270
24. De Luca A, Harbach M, von Zezschwitz E, Maurer M-E, Slawik BE, Hussmann H, Smith M (2014) Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In: Proceedings of the 32nd SIGCHI conference on human factors in computing systems, 2014, pp 2937–2946
25. Harbach M, von Zezschwitz E, Fichtner A, De Luca A, Smith M (2014) It's a hard lock life: a field study of smartphone (un) locking behavior and risk perception. In: Symposium on usable privacy and security (SOUPS), 2014
26. Apple's TouchID (2015) https://www.apple.com/ca/iphone-6/touch-id/. Accessed on 09 July 2015
27. Kit (2015) Try face unlock. https://support.google.com/nexus/answer/2781894?hl=en-CA. Accessed on 09 July 2015
28. Bianchi A, Oakley I, Lee JK, Kwon DS (2010) 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, 2010, pp 625–630
29. Bianchi A, Oakley I, Kwon DS (2010) The secure haptic keypad: a tactile password system. In: Proceedings of the 28th SIGCHI conference on human factors in computing systems, 2010, pp 1089–1092
30. Mott M, Donahue T, Poor GM, Leventhal L (2012) Leveraging motor learning for a tangible password system. In: Proceedings of the 30th SIGCHI conference on human factors in computing systems extended abstracts, 2012, pp 2597–2602
31. Jain A, Hong L, Pankanti S (2000) Biometric identification. Commun ACM 43(2):90–98
32. Bergadano F, Gunetti D, Picardi C (2002) User authentication through keystroke dynamics. ACM Trans Inf Syst Secur 5(4):367–397
33. Chong MK, Marsden G, Gellersen H (2010) GesturePIN: using discrete gestures for associating mobile devices. In: Proceedings of the international conference on human computer interaction with mobile devices and services, 2010, pp 261–264
34. Shahzada S, Chiasson S, Biddle R (2014) Gesture authentication for mobile devices. In: Who are you?! Adventures in authentication: WAY workshop, 2014, pp 1–2
35. De Luca A, Von Zezschwitz E, Nguyen NDH, Maurer M-E, Rubegni E, Scipioni MP, Langheinrich M (2013) Back-of-device authentication on smartphones. In: Proceedings of the 31st SIGCHI conference on human factors in computing systems, 2013, pp 2389–2398
36. Biddle R, Chiasson S, Van Oorschot PC (2012) Graphical passwords: learning from the first twelve years. ACM Comput Surv 44(4):19:1–19:41
37. Faulkner L (2003) Beyond the five-user assumption: benefits of increased sample sizes in usability testing. Behav Res Methods Instrum Comput 35(3):379–383
38. Florêncio D, Herley C, Coskun B (2007) Do strong web passwords accomplish anything? In: Proceedings of the 2nd USENIX workshop on hot topics in security, 2007, pp 10:1–10:6
39. Tari F, Ozok AA, Holden SH (2006) 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, 2006, pp 56–66
40. Bonneau J (2012) The science of guessing: analyzing an anonymized corpus of 70 million passwords. In: Proceedings of the symposium on security and privacy, 2012, pp 538–552
41. Dell'Amico M, Michiardi P, Roudier Y (2010) Password strength: an empirical analysis. In: Proceedings of the 29th conference on information communications (INFOCOM), 2010, pp 983–991
42. Florencio D, Herley C (2007) A large-scale study of web password habits. In: Proceedings of the international conference on world wide web (WWW), 2007, pp 657–666
43. Inglesant PG, Sasse MA (2010) 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, 2010, pp 383–392
44. Riley S (2006) Password security: what users know and what they actually do. Usability News 8(1):2833–2836
45. Zviran M, Haga WJ (1999) Password security: an empirical study. J Manag Inf Syst 15(4):161–185
46. Shay R, Komanduri S, Kelley PG, Leon PG, Mazurek ML, Bauer L, Christin N, Cranor LF (2010) Encountering stronger password requirements: user attitudes and behaviors. In: Proceedings of the 6th symposium on usable privacy and security, 2010, pp 2:1–2:20
47. Weir M, Aggarwal S, Collins M, Stern H (2010) 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, 2010, pp 162–175

48. Ur B, Kelley PG, Komanduri S, Lee J, Maass M, Mazurek ML, Passaro T, Shay R, Vidas T, Bauer L, Christin N, Cranor LF (2012) How does your password measure up? The effect of strength meters on password creation. In Proceedings of the 21st USENIX conference on security symposium, 2012, p 5
49. Egelman S, Sotirakopoulos A, Muslukhov I, Beznosov K, Herley C (2013) 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, 2013, pp 2379–2388
50. Kildal J, Wilson G (2012) 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, 2012, pp 393–400
51. Eichenbaum H (2011) The cognitive neuroscience of memory: an introduction. Oxford University Press, Oxford
52. Baars BJ (1986) A cognitive theory of consciousness. Cambridge University Press, Cambridge
53. Schaub F, Walch M, Könings B, Weber M (2013) Exploring the design space of graphical passwords on smartphones. In: Proceedings of the 9th symposium on usable privacy and security, 2013, pp 11:1–11:14
54. Levenshtein VI (1966) Binary codes capable of correcting deletions, insertions, and reversals. Sov Phys Dokl 10(8):707–710
55. Hansen WJ (1971) User engineering principles for interactive systems. In: Proceedings of the fall joint computer conference, 1971, pp 523–532
56. Maqsood S, Chiasson S, Girouard A (2013) Poster: passwords on flexible display devices. In: Proceedings of the SIGSAC conference on Computer & communications security (CCS), 2013, pp 1469–1472
57. Maqsood S (2014) Poster: shoulder surfing susceptibility of bend passwords. In: Proceedings of the SIGCHI conference on human factors in computing systems extended abstracts (CHI-EA), 2014, pp 915–920