Journal of Information Security and Applications 40 (2018) 1–8

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Incognito: Shoulder-surfing resistant selection method

Jeremiah D. Still[a,*], Jarad Bell[b]

[a] Old Dominion University, Norfolk, VA 23529-0267, United States
[b] San Jose State University, San Jose, CA, United States

ARTICLE INFO

Article history:

Keywords:
Shoulder-surfing
Authentication
PIN
Privacy
Usable security

ABSTRACT

Authentication methods need to, at minimum, prevent casual attackers with limited resources from gaining access to our private information. Although, Personal Identification Numbers (PIN) have been ubiquitously implemented to validate a user's identity, it is surprisingly easy for PINs to be stolen by casual shoulder-surfing attackers. We offer Incognito, a selection technique, which is resistant to casual shoulder-surfing and extendable to emerging graphical authentication methods. This was achieved by employing indirect interactions and masking standard cursor feedback. We show this selection technique effectively prevents casual shoulder-surfing attacks. The users controlled Incognito with either a mouse or eye tracker. We examined its usability by measuring effectiveness, performance, and user satisfaction in contrast with a conventional PIN approach. Our results show marginal login performance differences between the conventional method and Incognito with mouse-based interactions, but not for eye tracker based interactions. Incognito shows promise as a viable selection technique within public spaces.

1. Introduction

We value the convenience of being able to access services virtually and publicly, but this connectivity comes with potential security risks [17,36]. Therefore, it is critically important for online services to validate a user's identity successfully and privately. This validation occurs during the authentication process. Typically, users are prompted to provide both public (e.g., username) and private (e.g., password) information. E-mail addresses are often used as usernames, which are usually available to the public. This leaves passwords as the only barrier between one's private information and an attacker, therefore, passwords are often the focus of an attack.

One specific type of password – the PIN – is commonly used in both virtual and physical environments (e.g., PassFaces; Gate Access). Successful employment of this method requires users maintain a private Personal Identification Number (PIN) for authentication. However, PINs are often easy to capture through an observation attack known as shoulder-surfing [17,39,42,46]. These attacks are performed by a wide variety of predators. We are focusing on preventing casual attackers, which represent those without training, with limited resources, and a lack of strong motivation. They are simply opportunistic. The conventional design of PIN interfaces provides clear visibility of a user's input. This makes stealing PIN information too easy. De Luca et al. [17] note that 65% of users do not effectively conceal their authentication process when others are nearby. Thus, users often reveal their PINs unintentionally in public environments, because they are carrying items (e.g., bags or phone) or simply trust persons perceived as normal. Designers need to search for alternative interactions that offer additional protection from potentially malicious onlookers.

As human-centered designers, we need to create interfaces that exploit the user's natural abilities and design-out security issues. Some authors suggest that usable security is very difficult to achieve (c.f., [40,47]). For instance, as authentication complexity increases (i.e., length, complexity, shorter renewal rates) typically the usability decreases in step (i.e., harmed learnability and memorability). High failure rates and low compliance rates are reflective of the poor usability of traditional authentication systems. Findings like these can lead authentication developers to believe that usability and security are competing views. We suggest, like others [44], that usable security is possible if viewed as a design challenge. Stakeholders can simply ask users to behave a certain way – even provide extensive training – and sell the idea that it is personally and socially responsible to behave in that way, but, if the design they are using does not directly support or encourage that behavior, change will not occur. Also, the threats to private authentication are constantly evolving and adapting to new design solutions.

Beyond casual shoulder-surfing, some experts employ technology to enhance their attacks. These resources pose a more covert threat [12,33,36]. Optical devices, such as cameras within phones

[*] Corresponding author.
E-mail address: jstill@odu.edu (J.D. Still).

https://doi.org/10.1016/j.jisa.2018.02.006
2214-2126/© 2018 Elsevier Ltd. All rights reserved.

and wearable devices, enhance the distance at which a potential attacker can successfully capture the user's selections [42]. In one study, camera-enabled devices were found to successfully observe users authentication process up to 144 feet away [37]. In some instances, however, the user may block an observer's line of sight. This blockage prevents optical attacks, but not the capture of thermal traces [33]. After the keys have been pressed by the user, technology such as the FLIR One can recover the user's PIN and sequence from the trace heat residue left behind [12]. Despite the alarming ability of technology-based shoulder-surfing methods, it is not known how prevalent the attacks are [51].

The need and interest in a shoulder-surfing resistant input methods has rapidly grown over the last decade as researchers have developed an array of graphical solutions for authentication that focus on greater usability than conventional approaches [9,21,26,34,51]. The hope is greater usability will lead to better policy compliance, thereby producing more secure information systems. Numerous alternative graphic based methods for authentications exist in the literature [5,14–16,18,21,27,38,39,50]. These new graphical approaches often take advantage of how our information processing system works. They have users complete recognition tasks rather than recall. For example, users chose a familiar object from a set rather than retrieving an object from memory. In addition, they use images rich with visual information to ease later retrieval taking advantage of the well-known picture superiority effect [32]. Unfortunately, one of the main security issues in both graphical and PIN entry based authentication is casual shoulder-surfing attacks.

For example, Passfaces [35] a popular graphical authentication layout is similar to a PIN, but instead of button labeled with numbers they used faces. They have shown that faces are more easily remembered, compared with passwords [8], as humans are social creatures and have a specialized brain region that specificity supports face processing [25]. Others have users select pictures representing their passcode from within a grid containing decoy images [13]. Clearly, there exists a need to make interface button selection invisible to causal onlookers.

2. Related work

2.1. Shoulder-surfing resistant PIN entries

PIN entry redesigns have focused on disguising observable interactions through indirect input and through cursor camouflage [5,14–16,18,26,39,50]. The underlying concept for both methods is to decrease visual information provided to a casual observer that could be used to discover the user's PIN [18]. Indirect input methods achieve this by preventing users from directly selecting each PIN digit, whereas cursor camouflage methods mask a user's input with multiple dummy cursors.

An example of indirect input is the Cognitive Trapdoor game proposed by Roth et al. [38]. The authentication approach divides a standard 10-digit keypad into a random black or white assignment. Users then select the color that contains their PIN number. After the selection has been made, a new color assignment is presented to the user. The user repeats this process of selecting their PIN number for several rounds to enter a single digit for their PIN. This is continued until the user's PIN has been completely entered. The method takes advantage of the casual attacker's short-term memory limitations [38]. However, if multiple logins were observed over time, an attacker would be able to rule out numbers that did not fall into the users input [23]. In addition, due to the very nature of this design, the process of authentication takes considerably more effort compared to traditional PIN entry methods.

Another form of indirect input is the use of different input modalities such as head tracking or eye tracking to eliminate the need to use fingers for the PIN entry [14]. Removal of the physical interaction (i.e., finger input) in conjunction with a decrease in the amount of visual information provided on screen serves to increase the difficulty for a casual observer to steal a PIN [14,26].

2.1.1. Eye tracker based PIN entry

The EyePIN technique is one eye gesture-based authentication method [14]. To enter a digit, the user must press a control key to indicate an eye movement based gesture is about to be offered to the system. The user must then perform guided eye movements to create a single path drawing. Each of these drawings, created with their eye movements, represents a component of their passcode. This process continues until all of the components in the user's PIN are entered and verified by the system. In evaluating the resilience to shoulder-surfing attacks, De Luca et al. [14] found that 42% of attacks were successful against EyePIN. This is a significant improvement in casual shoulder-surfing resilience. However, users perceived the systems as cumbersome as it required them to memorize novel gestures.

Using eye tracker based interactions to hide passcode selections by not displaying cursor input on the screen is not a new idea [20,30,48]. For instance, Kumar et al. [27], systematically explored the employment of an eye tracker to reduce shoulder surfing during a traditional password entry using a virtual keyboard. They explore two interaction types using only gaze with dwell or gaze with key press to select buttons. It was found that using a key press to select buttons in conjunction with gaze produced more errors compared with using only dwell time. Also, they suggested that an eye tracker is a viable method for entering passwords in terms of error rates compared with using a traditional keyboard. Notably, over 80% of the participants reported preferring to use the eye tracker based interaction instead of the physical keyboard in public places to provide password privacy. Eye tracker based interactions have also been used to prevent shoulder surfing attackers within the PIN entry domain. De Luca et al. [19] examined making button selections using an 800 ms dwell time or by using eye gaze in combination with a space bar press to select buttons. In both cases, participants only had asterisks for digit entry feedback, otherwise the screen was static. Performance was high for both eye tracker based interactions (~76–80% successful PIN entry) and no difference was found between interaction types. Others have attempted to improve eye tracker based PIN entry by modifying the interface.

Best and Duchowski [4] proposed a circular layout similar to a rotary telephone dial instead of the conventional keypad grid for eye tracker based interactions. The purpose of the new rotary layout was to avoid the use of dwell time for button selection, and instead, employ a boundary-crossing approach. The new approach was empirically contrasted with the conventional method. Notably, no feedback in real-time was presented to participants; they viewed a still image for a set duration of either 10 or 15 seconds depending on layout type. Interestingly, they did not find a difference in accuracy between the two layouts (64–71% successful entry).

These eye tracker based interactions studies aim to decrease shoulder surfing attacks by nearby casual observers. This was achieved by removing feedback and, in some cases, by only presenting a still image. Across these studies it is clear eye tracker based interactions employing dwell time for button selection is a viable interaction technique for PIN entry.

2.1.2. Mouse based PIN entry

The first instance of cursor camouflage was proposed by Watanabe et al. [50]. The concept utilized multiple recordings of cursor movement that would play at the beginning of the user's PIN entry process. The underlying assumption of this design is that the user would be able to correlate their hand movements with the on screen movements, in order to identify their cursor amongst the dummy cursors. Because of this, the user could login knowing which cursor was his, but an observer would not be able to recognize the "real" cursor without performing the motor movement themselves [18,50].

There are a few challenges in implementing cursor camouflage. One is the physical screen requirements. Also, for the dummy cursors to be effective, their motions need to be similar to that of the actual cursor. While this might be accomplished using dummy cursors there would need to be a library of recorded cursors to be generated for each unique screen layout to ensure the motions were similar to actual user movements. Additionally, if the recorded cursor's movement exceeded the keypad screen, or did not land on a key when a selection is made, it would be quickly recognized as a dummy cursor [18]. We believe there is promise in modeling cursor movement and generating them as distractors, but implementing this would require a heavy amount of computational resources and a wide variety of user movement records. De Luca et al. [18] partially addressed this computational issue in their authentication method by restricting cursor movement to the keypad boundaries. They required dummy cursors to be on a key when the user's cursor was hovering over a digit. This was accomplished by building an algorithm to control the cursors behaviors. They examined the extent to which the number of fake cursors decreased shoulder-surfing performance. To assess this, a video showing a PIN input was presented to an attacker. When only one decoy cursor was used, 90% of the passwords could be identified correctly. However, with four decoy cursors, shoulder-surfing performance dropped to 50%. The most successful cases were with 16 and 24 decoy cursors, which decreased the success rate of a shoulder-surfing attack to 5% [18]. Clearly, this method is effective, but it still requires a large number of decoy cursors traveling across the interface limiting its portability.

In light of these previous techniques, we propose Incognito, a new PIN entry method. It combines the use of indirect input and cursor camouflage. However, Incognito is uniquely different from previous designs, because it employs simpler distractors (no modeling of real behavior required) to disguise the users input and allows implementation in non-screen displays. A major difference between our work and the work of Watanabe et al. [50] and De Luca et al. [18], is the design of our distractors. While their proposed designs attempt to model human cursor movements, either though records or complex algorithms, our distractors simply cycle through active and inactive states. They are designed only to make it difficult for an observer to detect the real cursor by masking the users' actual movements. Indeed, this reflects the definition of camouflage. But, we are not attempting to replicate human behavior by using naturalistic decoys. Therefore, very little computational resources are required for implementation. It can also be used without a screen display (i.e., employ LED lights to highlight physical buttons instead). We will examine Incognito's resilience to casual shoulder-surfing attacks and explore its usability while being controlled by a mouse and eye tracker.

3. Incognito: prototype design

The primary design goal was to decrease the performance of shoulder-surfing attacks on a 10-digit keypad. To achieve this goal, the mouse cursor is hidden when over the keypad, and is transformed into a border selecting a key. Each individual numeric key can alternate between an active and inactive state. At any given moment multiple keys are in an active state. This provides camouflage for the actual number being selected by the user (see Fig. 1). Notably, clicking a targeted key does not result in any additional feedback.

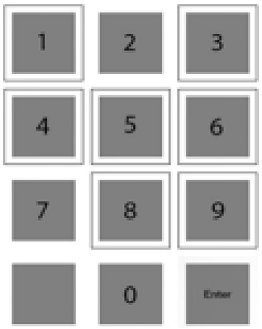

Fig. 1. Keypad example with numbers; one, three, four, five, six, eight, and nine in active feedback state.

The active feedback is created by adding a border around a key. In Fig. 1, you can see that numbers: one, three, four, five, six, eight, and nine are in an active state. The active state duration ranged from 500 to 1800 ms. The inactive state duration ranged from 650 to 6000 ms. A prototype was deployed in an internet browser using gif-images with a JavaScript to hide the mouse cursor. The user was still able to use the active state of their "real" cursor selected key as current location feedback. The animated gif-images were set to the following state timing in milliseconds across both studies (Button Active State: 1. 1770, 2. 1300, 3. 1400, 4. 970, 5. 800, 6. 1800, 7. 1200, 8. 600, 9. 500, 0. 900; Button Inactive State: 1. 6000, 2. 2500, 3. 2100, 4. 2200, 5. 2000, 6. 650, 7. 2200, 8. 1200, 9. 700, 0. 2400). For instance, button "1" would be in active state for 1770 ms followed by an inactive state for 6000 ms. All gif-images would infinitely loop between states and start on page load. The difference in active state timing camouflages the "real" cursor by preventing join blinking of decoys. Notably, a mouse-over event causes the gif-image to refresh. These timing resets act to off-set the state cycles as the user interacts with the display making it more difficult for a casual viewer to learn the distractor cursor pattern.

Upon entering the keypad, the cursor's visual feedback is limited to only the display of the keys active state (i.e., the mouse cursor disappears). This process is demonstrated in Fig. 2 as a user selected '5'. The first pane shows the user's mouse cursor initially outside of the table. This provides the user with an entry point before the transition from mouse point to key border. Across the next three panes, the cursor progresses through the keys nine, eight, and finally five. By design, it is difficult to determine which keys have been selected. In Fig. 2, the selected keys are shown with a white circle. Each time the user cursor rolls over a new key two important design elements support this interaction. The key being selected enters an active state and a soft click sound indicates a key selection.

Having multiple keys in an active state makes the actual key selection ambiguous to a casual observer. Similar to Watanabe et al. [50] and De Luca et al. [18] our assumption is that the users will be able to correlate their movements (i.e. hand) with the on screen activity in order to identify and utilize their cursor effectively. This coordination between motor movements and selection expectations are completed naturally for the operator. But, the observer has to watch hand movements and attempt to spatially map it on a key pad. This seems improbable for a casual attacker to coordinate in real-time. However, with a resourced expert attacker, which is motivated might be able to take advantage of current leaks (i.e., sound feedback and mouse entry location) in the prototype [28,45].

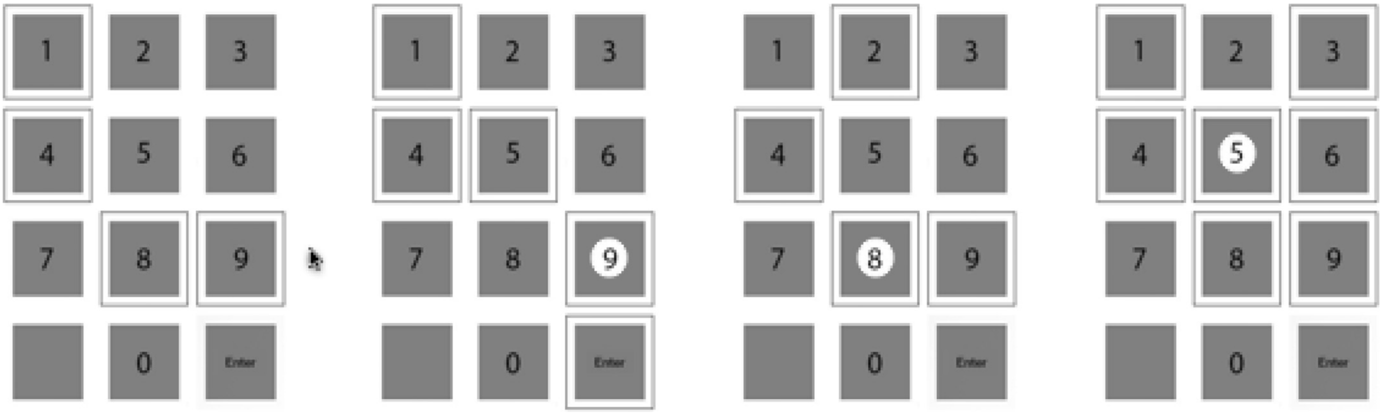

Fig. 2. Progression of the cursor from outside of the table to digits 9, 8, and 5. The white circles are for illustration purposes only.

Incognito camouflages the actual cursor from observers, while still providing valuable feedback to users – visual and auditory 'click' following selection. This allows users to be confident about their current key selections and correct for poor eye tracking. We predict that our dynamic Incognito prototype will produce a higher entry success rate compared to previously discussed static prototypes.

Incognito's usability and effectiveness to resist casual and resourced shoulder-surfing attacks is examined. In addition, we explored mouse and eye-tracking inputs as potential controllers. Usability was examined by measuring effectiveness, performance, and user satisfaction in contrast with a conventional PIN approach.

4. Study methodology

We employed a within-subjects design with two conditions where either participants interacted with the conventional PIN or Incognito. The usability of these two versions of a 4-digit PIN entry method was assessed by measuring login ability and the associated usage satisfaction ratings. Across two experiments we explore the Incognito method with input from a mouse and eye tracker. The effectiveness of the method was determined by its resilience to shoulder surfing attacks. The mouse study, contained twenty unique PIN entry trials. The eye tracker study, contained ten unique PIN entry trials. These experiments always began with a block of practice and two experimental blocks – one the conventional PIN, one Incognito. Of the two experimental blocks, half of participants completed the conventional PIN block first. To compare the usability of each condition type we recorded the users' performance in terms of the number of PIN entry attempts and surveyed the participants using the System Usability Scale (SUS) [7]. The SUS is a ten-question likert scale widely used to assess the subjective usability of products. Finally, participants were asked, "whether they felt vulnerable to an over-the-shoulder attack in the last year" and "whether they would accept additional authentication entry effort in order to prevent an over-the-shoulder attack" .

4.1. Threat model

Incognito is aimed at decreasing shoulder-surfing attacks performed by a casual observer [10,27,31]. According to De Luca et al. [14], users do not actively conceal their authentication process. Thus, our causal attackers have clear visibility of the screen, users' hand movement in relation to the on screen interactions. This scenario represents a public environment with typical unsafe user behaviors.

The effectiveness of the Incognito was examined at the end of the study by having participants become the shoulder-surfing attackers. They watched a single video with audio that showed an Incognito login alongside the user's hand employing a mouse. This one attempt approach is common within the literature [9,16,24,29,49,52]. In addition, we explored Incognito's ability to resist attackers given three guesses and an unlimited number of video rewinds. The results were used to assess the shoulder surfing resilience of the PIN-Entry method.

4.2. Participants

4.2.1. Mouse study

Thirty undergraduate students enrolled in an introductory psychology course were compensated with course research credit for their participation.

4.2.2. Eye tracker study

Eighteen undergraduate students were compensated with course research credit for their participation. The system had an eye tracking accuracy of < 0.5 visual degree of angle based on the initial calibration.

4.2.3. Shoulder surfing attack: unlimited viewing and allowed three guesses

Twenty undergraduate students were given course research credit for their participation.

4.3. Apparatus

The two prototypes were built using HTML, JavaScript, and animated gif-images (size: 100 × 100 px) to simulate a PIN entry authentication system. A windows workstation with a 19 inch monitor, laser mouse, and the Eye Tribe system were employed. The prototypes were run within a Firefox browser on a display with a resolution of 1600 × 900. Notably, during practice participants had a number display above the keypad. This was intended to enhance learnability by providing real-time feedback. Critically, this numerical feedback was not present during the following experimental blocks. Data was collected in real-time by an observer. The number of attempts was clearly shown on the screen following each failed attempt to login, which was recorded by a research assistant. A pilot study with ten participants using a mouse revealed that it took them an average of 7962 ms to complete an Incognito login following 70 practice logins. The traditional PIN entry method took participants an average of 4855 ms to login after 10 practice trials. The successful login performance was 8% lower for the participants interacting with Incognito. Previous research shows it typically takes users 5000–10,000 ms to enter a conventional PIN [6].

4.4. Eye tracker prototype setup

We employed a low-cost Eye Tribe system in conjunction with Dragger (a mouse accessibility tool) to create a high fidelity prototype. The Dragger software was adjusted to yield better results following some informal pilot testing. A nine point calibration process was employed using Eye Tribe's default development kit system settings (i.e., 30 Hz sampling rate). The low-cost eye tracker system's fixation data is shaky and does not provide a GUI feature for auto-click based on dwell time. The Dragger software allowed us to steady the cursor by defining a 25 by 25 pixel area and 800 ms dwell time as an automatic left click. The prototype presented a click sound indicating a dwell time selection has occurred. A pilot study with ten participants revealed that it took participants an average of 11,859 ms to login using Incognito and 10,529 ms to login using the traditional PIN entry method after 10 practice logins. The successful login performance was 1% lower for the participants interacting with Incognito.

4.5. Procedure

Participants completed three blocks of trials. They began with practice trials in which participants became familiar with the novel invisible cursor condition. Before each trial, they were given a unique 4-digit PIN to be entered. After completing the experimental trials and associated survey questions, they were shown a video of a confederate entering a 4-digit PIN. The video offered an ideal viewpoint of the screen and hand movements along with the associated audio feedback. The participants were instructed to watch the authentication process closely in order to determine the PIN entered.

4.5.1. Shoulder surfing attack: unlimited viewing and allowed three guesses study

Again, the Incognito prototype was run within a Firefox browser on a display with a resolution of 1600 × 900. During training participants had a number display above the keypad and then performed the PIN entry without the number selection feedback. The video recording was created by capturing the screen and hand movements from an ideal viewpoint. To provide the best video recording possible, the audio amplitude was increased, the screen and hand movement recordings were presented side-by-side at a high resolution.

4.5.2. Procedure

Participants were trained on Incognito. Then, they played the role of attackers, and were allowed to freely control a video recording using the QuickTime player. They were encouraged to take notes and use the video player (i.e., rewind, pause, go frame-by-frame) to discover the PIN. Participants were allowed to make three guesses.

5. Results

A paired-sample t-test was employed to compare the performance and ratings between the convention PIN and Incognito prototypes. The results are organized by input type (mouse and eye tracker) and these dependent measures: performance (number of login attempts; successful logins), user satisfaction (SUS survey), and security strength (shoulder-surfing performance). Figure error bars represent standard error of the mean.

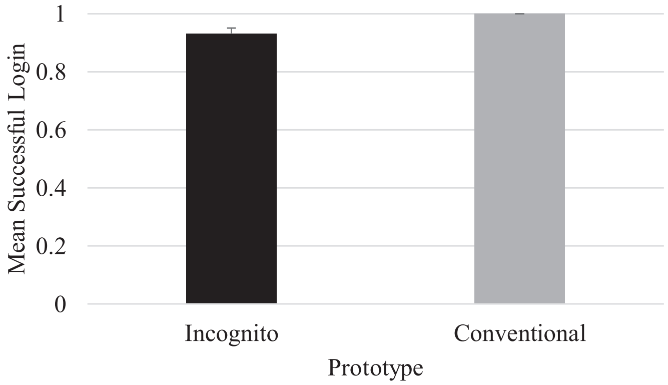

Fig. 3. Displays the successful login performance by prototype.

5.1. Mouse study

5.1.1. Performance

5.1.2. Number of login attempts

A paired sample t-test revealed that it took users more attempts using Incognito ($M = 1.42$, $SEM = 0.08$) compared to the conventional PIN entry method ($M = 1.03$, $SEM = 0.007$), $t(29) = 4.9$, $p < .001$, $d = 0.9$.

5.1.3. Successful logins

Keeping with research tradition a successful login was defined as a participant being able to login within three attempts (c.f., [18]). Therefore, on each trial a participant was able to login or not. The average of successful logins was our dependent measure. The paired sample t-test revealed Incognito ($M = 0.93$, $SEM = 0.02$) had a slightly lower successful login rate than the conventional PIN prototype ($M = 1$, $SEM = 0.00$), $t(29) = -3.69$, $p < .001$, $d = -0.67$.

Although the two conditions yielded significantly different results it is clear that participants were able to enter their 4-digit PIN using Incognito at a high-success rate (see Fig. 3). Given that this was novel interaction and each trial required a unique PIN be entered we predict that with regular practice, performance would improve as the cognitive process becomes automatic [43].

5.1.4. User satisfaction

Analysis of the completed SUS survey ratings revealed Incognito ($M = 52.48$, $SEM = 2.94$) was perceived to be less usable than the conventional PIN ($M = 80.9$, $SEM = 2.21$) prototype, $t(29) = -8.22$, $p < .001$, $d = -1.5$. The participants clearly preferred using the convention PIN entry method.

If we represent these SUS mean ratings as a grade Incognito earned an 'F' in terms of user satisfaction [3]. One possible explanation for this subjective difference could be due to familiarity with the conventional PIN. We expect that with additional practice, users would become more familiar and comfortable with Incognito and their subjective preference would increase.

It is important to note, that 83% of participants reported feeling they were vulnerable to a shoulder-surfing attack, and 93% reported a willingness to accept additional PIN entry effort for an increase in privacy.

5.1.5. Security strength (casual attacker): single viewing and guess

No participant playing the role of a casual over-the-shoulder attacker was able to determine the PIN in the video. This was true even though an ideal over-the-shoulder viewpoint was provided.

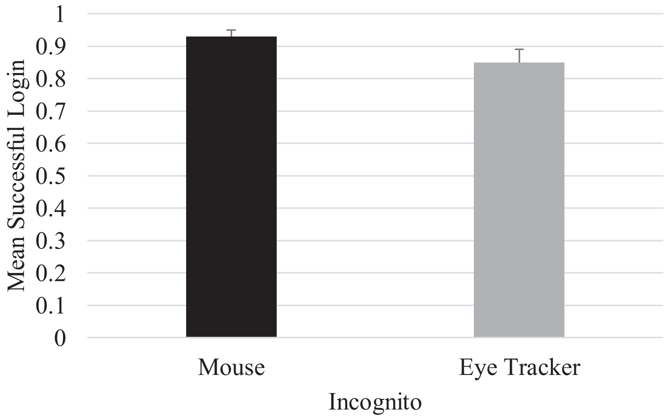

Fig. 4. Displays the successful login performance by interaction type.

5.2. Eye tracker study

5.2.1. Performance

The eye tracking system failed to track on 18 out of the 360 total PIN entry trials. This resulted in 5% of the login performance data being excluded from the analyses.

5.2.2. Number of login attempts

A paired sample *t*-test did not reveal a difference between the number of attempts to login between Incognito ($M = 1.65$, $SEM = 0.11$) and the conventional PIN entry method ($M = 1.61$, $SEM = 0.11$), $t(17) = 0.337$, $p = .74$, $d = 0.079$.

5.2.3. Successful logins

A paired sample *t*-test did not reveal a difference between Incognito ($M = 0.85$, $SEM = 0.03$) prototype and the conventional PIN prototype ($M = 0.83$, $SEM = 0.03$) in terms of successful login attempts, $t(17) = 0.511$, $p = .616$, $d = 0.121$.

5.2.4. User satisfaction

To avoid disrupting eye tracking system performance only one SUS survey was presented at the conclusion of both experimental blocks. Participants were instructed to rate their experience based on their last prototype interaction. An independent samples *t*-test, did not reveal SUS survey ratings differences between Incognito ($M = 70$, $SEM = 7.23$) and the conventional PIN ($M = 79.44$, $SEM = 2.99$) prototype, $t(16) = -1.21$, $p = .245$, $d = -0.57$.

5.3. Across experiment comparisons

These subjective ratings indicate that an eye tracker based interaction with Incognito earns a much better grade compared to a mouse based interaction (i.e., C vs. F). This suggests that eye tracking-based interactions are preferred by participants. However, the subjective ratings were made without a side-by-side comparison between the mouse and eye tracking prototypes. Therefore, these across experiment SUS reflections provide only anecdotal evidence. Interestingly, the objective performance data is comparable across experiments suggesting better performance for mouse-based interactions (see Fig. 4). A one-tailed independent samples *t*-test, reveals eye tracking interactions ($M = 1.66$, $SEM = 0.14$) are approaching a significantly higher number of login attempts compared with mouse interactions ($M = 1.42$, $SEM = 0.08$), $t(46) = 1.59$, $p = .059$, $d = 0.464$. Further, the mouse-based interactions ($M = 0.93$, $SEM = 0.02$) produced a higher successful login rate than eye tracker-based interactions ($M = 0.85$, $SEM = 0.04$), $t(46) = 1.94$, $p = .029$, $d = 0.579$.

5.4. Security strength (resourced attacker): unlimited viewing and three guesses

Three participants were able to determine the PIN following one guess. Two additional participants discovered it after two guesses and another determined the PIN given a third guess. Therefore, six participants were able to discover the PIN given three guesses. Attacker video rewinds averaged 5.26 ($SD = 2.15$). Incognito was able to prevent 70% of attackers with access to an optimal video recording from determining the PIN.

6. Conclusion

Conventional PIN based authentication methods are widely implemented to help ensure the security of our private information. However, it is well known in the field of cyber security that this method is highly susceptible to shoulder-surfing attacks [18,46]. In fact, 83% of our participants felt PIN entry methods were vulnerable to shoulder-surfing attacks. Unfortunately, users still often involuntarily reveal their PIN due to the nature of the input scheme and poor security behaviors [15]. It is evident there is a need for a new shoulder-surfing resistant method. Therefore, we introduced and assessed Incognito as a possible solution. Our security strength results indicate that Incognito is resilient to casual shoulder-surfing attacks. However, Incognito was not designed to prevent expert attackers who have more time and high-tech resources at their disposal (such as eye tracking). But, we did examined the resourced attacker's ability to extract information from Incognito by allowing unlimited rewinds and three guesses. It was discovered that our method still prevented 70% of the attackers from identifying the PIN. However, our attackers lacked hacker expertise and motivation. We hope future work explores the resilience of our method to such expert attackers and further improves its resistance.

Incognito was assessed during mouse and eye tracker based interactions. Clearly, both methods of interaction yielded acceptable performance. Notably, eye tracker based interactions with Incognito showed better performance (the increase reflects a 5–14% improvement, respectively) than previous eye tracker based techniques that provide no visual cursor feedback [4,19]. However, our data suggest mouse-based interactions yield higher successful interactions.

Future work needs to explore the use of Incognito with different input devices and in a variety of implementation contexts (e.g., physical compared with virtual). One avenue for this may involve haptic instead of audio feedback. Previous work has shown that users are able to successfully authenticate themselves by mapping their onscreen activity with haptic feedback provided through a trackball [5]. A benefit of using haptic feedback is that it provides another sensory input into their cursor location without offering more information to a potential attacker. As a result, the critical feedback information is kept private.

It is worth recognizing that Incognito attempts to stop causal shoulder-surfing like other graphical authentication methods [38]. It is integrated into existing graphical authentication to simplify methods. Often approaches that prevent shoulder-surfing require users to complete multiple trials, so the system can achieve an appropriate level of identity confidence and maintain privacy within public spaces. According to Widenbeck et al. [51], the Convex Hull Click (CHC) method protects users from casual shoulder-surfing attacks. Users are presented with five pass-icons to remember. They are then shown a display of cluttered with icons. First, users must visually search through the complex display to find their pass-icons. Second, they mentally connect their pass icons. Third, they click on icons within the mentally projected convex hull boundary. The CHC system takes users through a series of ten challenge-response sessions. Given this lengthy login process this might not be the best design for frequent daily logins. However, the majority of users remembered several of their pass-icons a week later. So, it might be a good solution for accessing an infrequently used system. As a caveat, if an attacker is able to observe a few authentication sessions. Discovering a passcode is simpler than a traditional brute force attack [1]. Thus, we only recommend the CHC method for accessing information that is considered to have little value.

6.1. Incognito: uses within graphical authentication schemes

We have already highlighted the use of Incognito within the conventional PIN entry scheme. Now to further exemplify the potential of Incognito as a new selection technique, we offer extensions to other popular graphical authentication schemes. This is important as many of the new authentication schemes use graphical elements rather than alphanumeric; this shift has come about in part due to increased memorability and ease of use associated with graphical elements. Numerous studies have shown the visual ease of recognizing objects versus text (c.f., picture superiority effect). Further, humans are neurologically specialized to recognize faces (i.e., the Fusiform Face Area; [25]). In an attempt to take advantage of this natural ability, Passfaces is an authentication scheme that allows users to login by selecting a series of familiar faces amongst distractors [8]. These faces are arranged in a 3 by 3 grid. To authenticate, participants must directly select the familiar face. This makes Passfaces highly susceptible to over-the-shoulder attacks through casual observation. By applying techniques used in Incognito to Passfaces, resistance to over-the-shoulder attacks could greatly be improved.

Another technique that could benefit from applying techniques used in Incognito is Use Your Illusion [22]. This system was designed to overcome an ironic problem with graphical authentication – the memorability and recognition benefits (recognizing an individual object is quick and effortless; [2]) the user gains through graphical authentication can also make over-the-shoulder attacks easier thereby benefiting attackers. Attackers can easily recognize the objects users are selecting. In Use Your Illusion [22] familiar images (a variety of objects and scenes) are displayed amongst distractors within a 3 by 3 grid. Critically, the images are blurred and abstracted, but remain recognizable to those familiar with the original images. Those unfamiliar with the untouched pictures have a difficult time recognizing the pictures. Nevertheless, this authentication scheme has been shown to still be susceptible to over-the-shoulder attacks (especially for short passcodes; [41]) as attackers recognize the distorted images even if they cannot name them. There are other authentication schemes also dependent on a grid-like layout that require participant responses that would be susceptible to over-the-shoulder attacks for similar reasons (e.g., [11,26,51]). Incognito could be used in these cases to help disguise participants' selections.

These popular examples provide a glimpse into possible uses within graphical authentication schemes. In future research, we encourage designers to consider adapting Incognito within the context of their scheme. Incognito offers value by providing a robust selection method that can be implemented in both physical and virtual environments, including emerging graphical authentication methods, while preventing casual shoulder-surfing attacks. It achieves this by employing indirect interactions and masking visual feedback.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.jisa.2018.02.006.

References

[1] Asghar HJ, Li S, Pieprzyk J, Wang H. Cryptanalysis of the convex hull click human identification protocol. Int J Inf Secur 2013;12:83–96.

[2] Biederman I. Recognition-by-components: a theory of human image understanding. J Psychol Rev 1987;94:115–47.

[3] Bangor A, Kortum P, Miller J. Determining what individual SUS scores mean: adding an adjective rating scale. J Usability Stud 2009;4:114–23.

[4] Best DS, Duchowski AT. A rotary dial for gaze-based PIN entry. In: The proceedings of ETRA; 2016. p. 69–76.

[5] Bianchi A, Oakley I, Kwon DS. Haptic security PIN entry system using magnetic repulsive force. In: The proceedings of 6th international workshop on haptic and audio interaction design; 2011. p. 1–3.

[6] Braz C, Robert JM. Security and usability: the case of the user authentication methods. In: The proceedings of 18th international conference of the association francophone d'interaction homme-machine; 2006. p. 199–203.

[7] Brooke J. SUS: a quick and dirty usability scale. Usability evaluation in industry. Jordan PW, Thomas B, Weerdmeester BA, McCelland AL, editors. London: Tylor and Francis; 1996.

[8] Brostoff S, Sasse MA. Are passfaces more usable than passwords? A field trial investigation. In: Chapter in: people and computers XIV – Usability or Else!. London: Springer; 2000. p. 405–24.

[9] Cain A, Still JD. A rapid serial visual presentation approach to graphical authentication. In: The proceedings of AHFE international conference on human factors in cybersecurity; 2016. p. 3–12.

[10] Cain A, Chiu L, Santiago F, Still JD. Swipe authentication: exploring over-the-shoulder-attack performance. In: The proceedings of AHFE international conference on human factors in cybersecurity; 2016. p. 327–36.

[11] Citty J, Hutchings DR. TAPI: Touch-screen authentication using partitioned images. Elon University Technical Report 2010–1; 2010. p. 1–6.

[12] Cluley G. This simple iPhone case can be used to steal ATM pins Retrieved from September http://www.intego.com/mac-security-blog/iphone-case-atm-pins/.

[13] Dhamija R, Perrig A. Déjà vu: a user study using images for authentication. The proceedings of 9th conference on USENIX security symposium Berkeley, CA; 2000. 4-4.

[14] De Luca A, Denzel M, Hussmann H. Look into my eyes! Can you guess my password?. In: The proceedings of SOUPS; 2009. p. 1–7.

[15] De Luca A, Frauendienst B, Boring S, Hussmann H. My phone is my keypad: privacy-enhanced PIN-entry on public terminals. In: The proceedings of 21st annual conference of the australian computer-human interaction special interest group; 2009. p. 401–4.

[16] De Luca A, Hertzschuch K, Hussmann H. ColorPIN: Securing PIN entry through indirect input. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems; 2010. p. 1103–6.

[17] De Luca A, Langheinrich M, Hussmann H. Towards understanding ATM security: a field study of real world ATM use. In: The proceedings of SOUPS; 2010. p. 1–10.

[18] De Luca A, von Zezschwitz E, Pichler L, Hussmann H. Using fake cursors to secure on-screen password entry. In: The proceedings of 31st CHI; 2013. p. 2399–402.

[19] De Luca A, Weiss R, Drewes H. Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In: The proceedings of 19th Australasian conference on computer-human interaction; 2007. p. 199–202.

[20] Dunphy P, Fitch A, Olivier P. Gaze-contingent password at the ATM. In: Proceedings of 4th conference on communication by gaze interaction; 2008. p. 1–4.

[21] Forget A, Chiasson S, Biddle R. Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In: The proceedings of 28th CHI; 2010. p. 1–4.

[22] Hayashi E, Dhamija R, Christin N, Perrig A. Use your illusion: secure authentication usable anywhere. In: The proceedings of 4th symposium on usable privacy and security; 2008. p. 35–45.

[23] Ho PF, Kam YH, Wee MC, Chong YN, Por LY. Preventing shoulder-surfing attack with the concept of concealing the password objects' information. Sci World J 2014:1–12.

[24] Jenkins R, McLachlan JL, Renaud K. Facelock: familiarity-based graphical authentication. PeerJ 2014;2:e444.

[25] Kanwisher N, McDermott, Chun MM. The fusiform face area: a module in human extrastriate cortex specialized for face perception. J Neurosci 1997;17:4302–11.

[26] Khot R, Kumaraguru P, Srinathan K. WYSWYE: shoulder surfing defense for recognition based graphical passwords. In: The proceedings of 24th Australian computer-human interaction conference; 2012. p. 285–94.

[27] Kumar M, Garfinkel T, Boneh D, Winograd T. Reducing shoulder-surfing by using gaze-based password entry. In: The proceedings of SOUPS conference; 2007. p. 13–19.

[28] Lee MK. Security notions and advanced method for human shoulder-surfing resistant PIN-entry. IEEE Trans Inf Forensics Secur 2014;9:695–708.

[29] Lin D, Dunphy P, Olivier P, Yan J. Graphical passwords and qualitative spatial relations. In: The proceedings of 3rd symposium on usable privacy and security; 2007. p. 161–2.

[30] Maeder A, Fookes C, Sridharan S. Gaze based user authentication for personal computer applications. In: The proceedings of international symposium on intelligent multimedia, video and speech processing; 2004. p. 727–30.

[31] Man S, Hong D, Mathews M. A shoulder-surfing resistant graphical password scheme. In: The proceedings of international conference on security and management; 2003. p. 1–6.

[32] Mintzer MZ, Snodgrass JG. The picture superiority effect: support for the distinctiveness model. Am J Psychol 1999;112:113–46.

[33] Mowery K, Meiklejohn S, Savage S. Heat of the moment: characterizing the efficacy of thermal camera-based attacks. The proceedings of 5th USENIX conference of offensive technologies Berkeley, CA; 2011. 6-6.

[34] Nicholson J, Coventry L, Briggs P. Faces and pictures: understanding age differences in two types of graphical authentications. Int J Hum Comput Stud 2013;71:958–66.

[35] Passfaces. Graphical authentication service http://www.passfaces.com.

[36] Pore R. Cyber security becoming more important as more Nebraskans get online The Grand Island Independent. Retrieved from http://www.theindependent.com/news/local/cyber-security-becoming-more-important-as-more-nebraskans-get-online/article_4ea57796-3c38-524d-b924-428643caabdf.html?mode=jqm.

[37] Rigg J. Researchers crack iPad PINs by tracking fingers that enter them Retrieved from http://www.engadget.com/2014/06/25/ipad-PIN-snooping/?ncid=txtlnkusaolp00000595.

[38] Roth V, Richter K, Freidinger R. A pin-entry method resilient against shoulder surfing. In: The proceedings of CCS; 2004. p. 1–10.

[39] Sasamoto H, Christin N, Hayashi E. Undercover: authentication usable in front of prying eyes. In: The proceedings of CHI; 2008. p. 1–10.

[40] Sasse MA, Brostoff S, Weirich D. Transforming the 'weakest link' — A human/computer interaction approach to usable and effective security. BT Technol. J. 2001;19(3):122–31.

[41] Schaub F, Walch M, Konings B, Weber M. Exploring the design space of graphical passwords on smartphones. In: Proceedings of the Ninth Symposium on Usable Privacy and Security; 2013. p. 1–15.

[42] Schaub F, Deyhle R, Weber M. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In: The proceedings of mobile and ubiquitous multimedia conference; 2012. p. 1–10.

[43] Shiffrin RN, Schneider W. Controlled and automatic human information processing: II. Perceptual learning, automatic, attending, and a general theory. Psychol Rev 1977;84:127–90.

[44] Still JD. Cybersecurity needs you!. ACM Interact (May + June: Feature) 2016;23:54–8.

[45] Taekyoung K, Shin So, Na S. Covert attentional shoulder surfing: Human adversaries are more powerful than expected. IEEE Trans. Syst. Man Cybern. Syst. 2014;44:716–27.

[46] Tari F, Ozok A, Holden SH. A comparison of perceived and real shoulder-surfing resistant risks between alphanumeric and graphical passwords. In: The proceedings of SOUPS; 2006. p. 56–66.

[47] Theofanos MF, Pfleeger SL. Guest editors' introduction: shouldn't all security be usable? IEEE Secur. Priv. Magazine 2011;9(2):12–17.

[48] Thorpe JP, van Oorschot, Somayaji A. Pass-thoughts: authenticating with our minds. In: The proceedings of new security paradigms workshop; 2005. p. 45–56.

[49] van Eekelen WA, van den Elst J, Khan VJ. Picassopass: a password scheme using a dynamically layered combination of graphical elements. In: Extended abstracts on human factors in computing systems; 2013. p. 1857–62.

[50] Watanabe K, Higuchi F, Inami M, Igarashi T. CursorCamouflage: multiple dummy cursors as a defense against shoulder surfing. In: The proceedings of SIGGRAPH Asia '12 emerging technologies; 2012. p. 1–2.

[51] Wiedenbeck S, Waters J, Sobrado L, Birget J-C. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In: The proceedings of advanced visual interfaces; 2006. p. 177–84.

[52] Zangooei T, Mansoori M, Welch I. A hybrid recognition and recall based approach in graphical passwords. In: The proceedings of 24th Australian computer-human interaction conference; 2012. p. 665–73.