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/

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