Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Erratum or Corrigendum

“It’s all about the start” classifying eyes-free mobile authentication techniques

Flynn Wolf[a], Adam J. Aviv[b,*], Ravi Kuber[a]

[a] University of Maryland, Baltimore County, United States
[b] United States Naval Academy, United States

ARTICLE INFO

Article history:

Keywords:
Authentication
Eyes free
Unlock authentication
Non-visual

ABSTRACT

Mobile device users avoiding observational attacks and coping with situational impairments may employ techniques for eyes-free mobile unlock authentication, where a user enters his/her passcode without looking at the device. This study supplies an initial description of user accuracy in performing this authentication behavior with PIN and pattern passcodes, with varying lengths and visual characteristics. Additionally, we inquire if tactile-only feedback can provide assistive spatialization, finding that orientation cues prior to unlocking do not help. Measurements of edit distance and dynamic time warping accuracy were collected, using a within-group, randomized study of 26 participants. 1021 passcode entry gestures were collected and classified, identifying six user strategies for using the pre-entry tactile feedback, and ten codes for types of events and errors that occurred during entry. We found that users who focused on orienting themselves to position the first digit of the passcode using the tactile feedback performed better in the task. These results could be applied to better define eyes-free behavior in further research, and to design better and more secure methods for eyes-free authentication.

Published by Elsevier Ltd.

1. Introduction

The threat of observational attacks in shared or public spaces may influence or modify the way smartphone users interact with their devices. In particular, users may favor unlocking their mobile devices out-of-view, without looking at the screen to avoid others from *surfing* the authenticator. Purposeful user obfuscation (e.g. keeping the screen out of sight from third parties or hidden cameras by hiding the device in the pocket or bag [1]) for purposes of the initial stages of the interaction, limits the likelihood of the authentication sequence being viewed. This can put users at some level of ease, even if the remainder of the interaction is performed in-view of third parties.

Eyes-free authentication behaviors may also be performed when the situation, context or environment demands it. For example, in situations where glare may be factor, or the environment is inappropriate for mobile device usage and discretion is needed (e.g. [2], the interaction may be performed away from view). While eyes-free interactions for different types of mobile device have been studied by researchers in the past [3–13], studies have yet to examine real world eyes-free authentication behaviors; investigating the performance with common authentication mechanisms when the phone is out-of-view, and user coping strategies to enter passcodes in an eyes-free manner.

To address this knowledge gap, we conducted a randomized, multi-factor study with 26 participants entering PINs and gesture-based patterns (termed: “patterns” in this paper). Participants entered passcodes under both in-view and eyes-free conditions, as well as eyes-free using an additional training module for spatialization based on tactile feedback.

The tactile channel was chosen to discreetly offer cues directly to the user’s hand, without drawing attention during interaction, as would likely occur with auditory or visual cues. Existing assistive aids aid to eyes-free PIN authentication, such as iOS VoiceOver, rely on audio feedback (audio readout of PIN number buttons when touched, allowing selection). However, audio cues impose usability and security penalties in shared and public spaces.

Biometric authentication such as fingerprint identification can greatly expedite this task for many users. However, fingerprint identification remains only a secondary means of authentication, which is generally tied to a PIN or patterns for screen unlocking. Essentially, even biometric authentication users must necessarily enter conventional passcodes on a semi-regular basis, and eyes-free conditions may apply in some instances.

In light of this, tactile-only feedback was designed for this study as a research device for understanding authentication performance

[*] Corresponding author.
E-mail addresses: flynn.wolf@umbc.edu (F. Wolf), aviv@usna.edu (A.J. Aviv), rkuber@umbc.edu (R. Kuber).

https://doi.org/10.1016/j.jisa.2018.05.004
2214-2126/Published by Elsevier Ltd.

with strictly eyes-free interaction. Its functionality, and our evaluation of its performance, is not intended to propose a workable real-world tool in the present form. Instead, we tried to capture how users develop techniques that use additional spatial cues to locate key screen features. This spatialization might then assist the accuracy and precision of eyes-free authentication gestures, especially for situations where the user may feel at risk of being a victim of an observer attack or be at risk of a situational impairment.

Given these assumptions, we have undertaken these research questions:

- *RQ1*: How well are users able to perform eyes-free authentication (without tactile feedback) with common methods, such as PIN and pattern entry, and how is this affected by the length and visual features of passcodes?
- *RQ2*: Will the relationship between spatial cues to screen layout features (e.g. position of buttons), presented by tactile interaction, enhance the user's performance when authenticating eyes-free?
- *RQ3*: When tactile feedback is presented, what approaches will users develop for using it?

With these considerations, during the experiment we collected complete movement traces, recording all participants' touch-based gestures during each authentication attempt, totaling 1021 eyes-free traces. To extend the work described in [14], we aimed to understand the input techniques and strategies the participants developed when completing the tasks. To do this, we classified all the traces, and developed a set of verified and grounded labels to describe the actions of the participants.

We further evaluated participants' performance in the eyes-free setting in two dimensions, accuracy and precision. For accuracy, we considered the edit-distance (or *Levenshtein distance*) between the input passcode and the true passcode. The edit-distance considers the number of additions or removals to transform one string sequence into another. For precision, we developed a geometric distance measure between in-view and eyes-free traces using *Dynamic Time Warping* (DTW), computing the average distance between temporally-associated points in the trace.

Based on this analysis, we found that participants using patterns were more accurate and precise in eyes-free settings, as compared to PINs. Additional tactile training was found to not improve the accuracy or precision of the participants' entries. We discuss users' observations regarding this distinction between task performances. When applying the classification results, we found that specific techniques in both training stages impacted performance. In particular, traces where participants used the additional tactile training aid to understand specifically the location of the starting digit of their passcode showed the most significant increase in performance, for both PINs and patterns. In addition to identifying techniques that improved performance, we also developed a set of classifications for eyes-free entry and training.

The results firstly contribute to an initial baseline of performance results and classifications of types for eyes-free interaction behaviors, events, and error types. We also show that the describe strategies for locating the starting location of authentication gestures (i.e. the screen position of the button for a passcode's first digit) that correspond with a number of significant effects on user performance. These results will help further research on eyes-free interaction make accurate comparisons and descriptions regarding this condition. Additionally, these insights will help iterate the design of targeted training aids for users, such as blind mobile technology users who rely on secure ubiquitous computing for privacy-sensitive tasks in shared spaces, who need to authenticate frequently in eyes-free settings (i.e. when at perceived risk of an observer attack described in [1]). Informing users of effective techniques will enable users to enter unlock authentication more confidently, securely, and accurately, away from adversarial observation.

While the tactile aid adopted for this study produced a mostly negative result from accuracy and edit distance measures, we assert several important contributions from this investigation:

1. A novel characterization of HCI and security performance conditions for eyes-free authentication tasks.
2. A systematic inquiry of accuracy, precision, and timing effects of input in eyes-free settings.
3. Establishing the unequivocal performance gap between eyes-free PIN and pattern entry (although unsurprising, this is the first time this has been shown empirically).
4. The extension of existing classification methodology for coding eyes-free unlock entry methods and events, similar to error codes established in von Zezschwitz et al. [15].
5. Identifying significant relationships between classification codes and authentication conditions (e.g. a decrease in Start-Hunt behavior for pattern passcodes ($\chi^2 = 8.17,\ p < 0.005$)).
6. Identifying passcodes features for which accuracy and/or precision significantly deviated from average (e.g. self-crossing pattern 743521).

We feel the relationship between the initial training methods that users develop using the tactile aid, such as those that help locate the starting point of the authentication gesture, are particularly illustrative. Strategies, such as the Start-Hunt trial code and Return to Start training code, offer an insight into the ways that users cope with the challenges of entering gestures under eyes-free conditions. By being able to better understand user strategies taken, along with events and error types made, this work could lead to the improved support of targeted training aids for users who interact with mobile authentication solutions under eyes-free conditions.

2. Related work

2.1. Eyes-free interaction techniques

As mobile technologies reduce in size and provide increasing amounts of PC-like functionality, these technologies become an attractive option for performing tasks while on-the-go. As information is predominantly presented via the graphical user interface, the user is heavily reliant on visual feedback to perform mobile tasks.

However, there are scenarios when difficulties are faced viewing the interface. One of the predominant issues relates to worries about third parties viewing content, and using this information without permission. Examples described by Yi et al. [16] include (1) environmental factors (e.g. excessive brightness impacting the user's ability to perceive screen content, and in scenarios where switching visual attention between the device and the physical environment poses safety concerns), (2) social factors (e.g. instances where it may be socially-inappropriate to view the screen, or multi-task in front of others), (3) constraints imposed by the mobile devices themselves (e.g. difficulties seeing content due to the crowded nature of content on mobile GUIs), and (4) personal factors (e.g. no perceived benefit to using vision to performing the task).

Additionally, if the user feels under threat of observer attacks, the screen may be hidden from view, either shielded by the hand [17], or placed within a garment or accessory [1]. The user can then attempt to use a combination of a mental image of the interface and muscle memory to attempt to interact with the device.

One of the fundamental motivations for eyes-free interaction is that as it leaves visual attention unoccupied, users are free to perform additional tasks [18]. However, performing mobile tasks