

Developing and Evaluating a Gestural and Tactile Mobile Interface to Support User Authentication

Abdullah Ali¹, Ravi Kuber¹ and Adam J. Aviv²

¹Department of Information Systems, UMBC, Baltimore, MD 21250, USA

²Department of Computer Science, USNA, Annapolis, MD 21402, USA

Abstract

As awareness grows surrounding the importance of protecting sensitive data, stored on or accessed through a mobile device, a need has been identified to develop authentication schemes which better match the needs of users, and are more resistant to observer attacks. This paper describes the design and evaluation of H4Plock (pronounced “Hap-lock”), a novel authentication mechanism to address the situation. In order to authenticate, the user enters up to four pre-selected on-screen gestures, informed by tactile prompts. The system has been designed in such a way that the sequence of gestures will vary on each authentication attempt, reducing the capability of a shoulder surfer to recreate entry. 94.1% of participants were able to properly authenticate using H4Plock, with 73.3% successfully accessing the system after a gap of five days without rehearsal. Only 23.5% of participants were able to successfully recreate passcodes in a video-based attack scenario, where gestures were unique in design and entered at different locations around the interface.

Keywords: Gestural Interfaces; Haptic Interfaces; Mobile Interface Development; Tactile Interfaces; User Authentication

Citation: Editor will add citation

Copyright: Copyright is held by the authors.

Acknowledgements: The authors thank Flynn Wolf (UMBC) for his assistance with the project. This work was supported by the Office of Naval Research - Award: N00014-15-1-2776.

Contact:{aali6, rkuber}@umbc.edu¹, aviv@usna.edu²

1 Introduction

As mobile technologies reduce in size, increase in fidelity, and offer access to PC-like functionality (e.g. email, web access), mobile devices, such as smartphones and tablets, are fast becoming an attractive option for performing work on-the-go. These technologies hold large amounts of private and potentially sensitive user data which could be misused unless suitably protected (De Luca et al., 2014). If users neglect to log-out of their personal accounts (e.g. web, email, or on-device application accounts), illegitimate access to a mobile device may jeopardize a legitimate user’s information and communication security (Chen et al., 2015). While knowledge-based authentication mechanisms provide one method of reducing unauthorized entry to a mobile device (e.g. through an alphanumeric password, PIN or unlock pattern), users are known to trade-off security to achieve memorability and usability of their passwords by selecting weak and guessable passwords that are easier to remember and/or enter, as compared to stronger passwords that are harder to remember and/or enter on a compact mobile device. Input errors are often made when entering passwords into mobile interfaces, particularly if the virtual keyboard is small in size or if the user is ambulatory. As a result, users may choose passwords that are easier to input (von Zezschwitz et al., 2014).

In this paper, we describe the design and evaluation of a novel authentication mechanism, H4Plock, pronounced “Hap-lock”, developed to address a number of the challenges faced when users attempt to authenticate on mobile devices. In contrast to other authentication mechanisms, H4Plock relies on the user making small on-screen gestures in response to tactile feedback presented via the mobile device. The authentication process requires users to enter up to four pre-selected gestures in sequence (a so-called “passcode”). The choice of passcode is determined based on the tactile prompts presented, indicating that the user should enter specific gestures from a pre-selected primary or secondary passcode. The sequence of gestural cues may vary on each authentication attempt, making it very difficult for an observer (termed: shoulder surfer) to precisely recreate the authentication sequence. It is also the case that gestures and tactile effects are known to be personal to each user, and are therefore difficult to describe or write down, further limiting the ability for third parties to fraudulently gain access to the system. H4Plock is thought to benefit mobile device users aiming to access personal data in scenarios where observer threats are prevalent (e.g. using a mobile device on a busy train or in a crowded shopping mall). It could also offer considerable value as a secondary method of authentication to secure access to a mobile interface (e.g. using a PIN and then a H4Plock passcode).

The research described in this paper addresses three areas: (1) the feasibility of recalling and entering a combination of gestural and tactile cues for purposes of authentication; (2) the viability of

remembering these cues after periods without using the system; (3) assessing the susceptibility of the solution to video-based attacks.

2 Related Work

Gestural solutions have been developed to support the authentication process. Examples include PassShapes, an application where simple geometric shapes are constructed of an arbitrary combination of different strokes (De Luca et al., 2007). These included horizontal, vertical, and diagonal strokes. Chong et al. (2010) used a similar concept to PassShapes, enabling the user to make discrete gestures using a mobile device in a 3D space. Users were required to produce a string of multiple gesture elements in a required order, to authenticate entry to the solution. Password elements included moving the device forwards, backwards, up, down, left, right, or tilting/swinging left and right. Although participants could use kinesthetic memory to remember gesture sequences, the researchers identified that retention of PINs was superior to gestures. In contrast to their findings, Weiss and De Luca (2008) identified that using a repeated drawing strategy could lead to better retention of gestures compared to PINs after a ten day period.

Other notable gestural mechanisms include SwiPIN (von Zezschwitz et al., 2015), a system based on a random assignment of simple touch gestures to specific digits. To enter a digit, instead of tapping a specific button, the user performs a gesture, usually at a different location than the respective button. The solution is thought to serve as an alternative input method for risky situations (i.e. when the user feels that observer threats are prevalent). Kwon and Na (2014) have aimed to address issues associated with smudge-based attacks on pattern lock screens through the design of TinyLock. Instead of entering a pattern on a 3x3 grid, users can draw their patterns on a smaller version of the grid, and then rotate a virtual wheel to finalize the unlock process. Smudges are confined to a small spot and are masked during this process, making the process of replication more challenging for a third party. Sae-Bae et al. (2012) developed a multi-touch gesture based authentication technique, where five-finger touch gestures are made. Biometric information is collected. Pattern recognition techniques are used to identify movement characteristics of the center of the palm and fingertips. The mechanism was thought to offer considerable promise to users, as the system itself would be able to identify interaction by third parties. However, further refinement would be needed to raise the accuracy level for detecting cues.

Oakley and Bianchi (2012) have examined ways to augment authentication for mobile devices using a multi-touch approach. MT-Lock implements novel functionalities extending the Android Pattern system. Strokes can start and end off-target, and multiple taps and strokes can take place simultaneously. Findings from a small usability study showed that participants were able to select a wide variety of passcodes based on taps and strokes. More complex stroke based passcodes are suggested to support access to mobile devices. Kuribara et al. (2014) developed a two-step PIN entry system (VibraInput) to defend users from shoulder surfing attacks. The user enters his/her PIN by matching the digits with symbols on the interface. To do this, they either interact with a dial or bar on the interface. Vibration patterns are mapped to each of the symbols. Authentication failure was found to be low (4%) when using the solution. Chen et al. (2015) developed a two factor rhythm-based scheme for multi-touch mobile devices. The user is required to perform a sequence of rhythmic taps/slides to unlock the device. Similar to Sae-Bae et al. (2012), the authentication process relies on behavioral metrics for inputting the rhythm. The solution was thought to offer security benefits against attacks, and offer an accessible alternative to support blind and visually impaired users. Zakaria et al. (2011) examined ways to minimize attacks from shoulder surfers. The researchers investigated three shoulder surfing defense techniques for gestural passcodes: a decoy stroke, a disappearing stroke, and line snaking the gesture traces. The latter was found to be most effective method against observer attacks.

Researchers have examined the integration of other channels, such as touch, to support the authentication process. Examples include the Haptic Wheel (Bianchi et al., 2010), where the user positions their hand around a rotary dial. After each input, the system randomizes the vibration it emits to protect the user from observer attacks. Kuber and Yu (2010) examined the feasibility of using raised pin patterns presented via a tactile mouse to authenticate entry to a system. A recognition-based mechanism was selected to address issues of workload faced by users accessing other recall-based systems. Findings from the researchers' study highlighted the ability to accurately select tactile stimuli to authenticate entry over a long term period. As information was presented underneath the fingertips, onlookers were unable to view stimuli and therefore unable to recreate entry. The solution was found to offer promise to individuals who are blind (Kuber and Sharma, 2010, 2012), similar to the PassChords system developed by Azenkot et al. (2012). De Luca et al. (2009) developed the VibraPass system, enabling a user to connect a mobile telephone or PDA to a terminal. As the user enters his/her

password, a vibration is perceived from his/her mobile device indicating whether he/she should enter the correct PIN digit or password character, or enter redundant information instead. As a result, the user's password or PIN will appear to be different to the previous entry, making it more difficult for an observer to recreate the authentication sequence. Low rates of error were reported, with comparable entry speed to entering a randomly generated PIN.

Non-traditional authentication mechanisms offer considerable potential to mobile device users, who are burdened to recall a vast array of alphanumeric passwords and PINs to access secure information stored within applications on phones. Our research specifically seeks to integrate both gestures and tactile cues to determine whether a resulting solution can augment the subjective authentication experience. Using both types of cue can additionally support levels of perceived security among users, compared with mechanisms focusing solely on gesture-based authentication which are subject to other forms of attack (e.g. smudge attacks (Aviv et al., 2010)). More specifically, our research aims to advance prior work by examining the utility of an interactive solution where the user needs to respond accordingly to tactile prompts from the interface.

3 Interface Design

The aim of our prototype is to demonstrate that an alternative authentication method for mobile devices based on gestural input and tactile feedback is feasible, and that users will accept the authentication process.

We built the H4Plock prototype on Android using the built-in gesture library¹ and the vibration motor interface. This library provides both gesture storage and matching, using a technique similar to dynamic time warping that allows for exact and inexact matching, up to a threshold. In real-world scenarios, gestures may vary slightly in size, shape, or position on the interface when entered. Pilot testing revealed gestures could be recognized even if there were slight deviations from the originals. No additional libraries or software are required. Furthermore, modifications do not need to be made to the underlying hardware.

The basic design of the user interface is presented in Figure 1, where the user is required to enter a sequence of up to four pre-selected on-screen gestures while responding to tactile prompts. These vibratory prompts are presented to the user's hand via the mobile device. In contrast with auditory prompts, tactile feedback can be perceived in noisy environments where a phone may be carried.

The authentication procedure occurs over four quadrants of the phone where each quadrant can recognize a separate gesture. Multiple quadrants are used to increase the entropy of the resulting passcode. While the user only needs to start their gesture within a quadrant, not contain their gesture within it, many of our participants from the study used gestures that fitted neatly within a single quadrant. Each gesture was required to be a single continuous stroke where the user maintained contact with the screen throughout. Lifting one's finger and re-contacting the screen would initiate a separate gesture. The device will give a confirmation vibrating pulse (duration: 100 ms) when a gesture has been entered properly.

The process begins with the user selecting two sets of passcodes, a primary and secondary passcode. A passcode must contain at least 1 and up to 4 gestures. Users may choose to use a subset of quadrants for a passcode, or just one quadrant, or all the quadrants. The specific gesture shapes may also repeat across quadrants if so desired. Two passcodes are needed because the user will receive tactile feedback, in the form of vibrations, indicating which of the passcodes should be used.

A tactile prompt will be presented, signaling that a gesture from the primary or secondary passcode should be entered. After the user enters in the gesture, another tactile prompt will then indicate which passcode the following gesture will need to come from. The process will continue until up to four gestures have been entered. Consequently, the sequence of gestural cues may vary on each authentication attempt, making it very difficult for a shoulder surfer to precisely recreate the authentication sequence. The tactile stimuli have been informed using guidance from Qian et al. (2009) who had studied ways to differentiate pairs of tactile cues presented using a mobile device.

If the user fails to enter the correct sequence of gestures in the correct areas, resulting in a mismatch between the required passcode and the one entered, the device provides further haptic feedback by vibrating one long continuous vibration (duration: 500 ms).

H4Plock does not depend on specific metrics, such as pressure and acceleration described by Serwadda and Phoha (2013). However, these factors may be incorporated in a future version of the system. Instead, the current prototype simply requires the user to recreate the path with the same

¹ Gesture library - <http://goo.gl/zxOIND>

starting and ending points (relative to the gesture shape), disregarding the size and location, except that the gesture must begin within one of the quadrants.

The user has the ability to abort an entry attempt by selecting the back key on the system, if he/she thinks that an erroneous gesture has been entered. Similarly, should the user forget a passcode, this can be reset using the system. Further details are described in Ali et al. (2015).



Figure 1. Example of first three steps when entering H4Plock. The user is presented with a vibration cue after entering a gesture, to indicate whether the following gesture to be entered should be selected from the primary or secondary passcode. This process will continue until up to a total of four gestures have been entered.

3.1 Usage Scenarios

The solution could offer considerable potential when the user needs to authenticate in an environment where he/she may be under the threat of observer attack. For example, accessing the mobile device when in close proximity to unfamiliar individuals who may attempt to memorize the user's password in order to fraudulently recreate entry. Alternative scenarios include accessing a mobile device in locations where camera-based attacks may be prevalent (e.g. in the foyer of a bank near the ATM). It could also provide a secondary level of protection for instances when highly sensitive data needs to be accessed (e.g. when accessing financial information using a mobile device). H4Plock could easily be integrated into the unlock sequence, either as a replacement for unlock patterns on the 3x3 grid, or as a supplement (e.g. as a secondary or tertiary authentication process occurring after PIN or pattern entry had too many failed attempts).

An exploratory study was conducted to investigate the efficacy of the mechanism, which we describe next.

4 Methodology

4.1 Study Design and Objectives

The within-subjects study conducted was composed of two tasks. The first task was designed to investigate the feasibility of a gestural and tactile authentication mechanism as well as the memorability of the stimuli and passcodes after a period without accessing the system. The second task related to the susceptibility of the system to observer attacks, (e.g. shoulder surfers). More specifically, we examined this through video replays of the authentication from the researchers. Participants were asked to replicate the observed entry to the system.

4.2 Hypotheses

(H1) Participants using H4Plock will be able to enter pre-selected gestural cues based on tactile feedback presented, over 90% of the time, similar to other gestural authentication solutions (e.g. Weiss and De Luca, 2008).

(H2) Participants will be less likely to successfully recreate H4Plock passcodes from video sequences, where non-repeating gestures are presented in all four quadrants.

4.3 Participants

Seventeen participants (9 male, 8 female) aged between 18-69 were recruited for the study. All participants reported normal levels of auditory and tactile perception. All seventeen participants were smartphone users. In terms of authentication mechanisms, six participants stated that they used a PIN to access their mobile device, two used the Android Unlock pattern to connect a series of dots in a specific pattern, and four used biometric information (e.g. fingerprint reader). The other four participants favored

not securing their mobile devices. Only 8 of our participants had sensitive information such as passwords, social security numbers, and credit card information stored on their mobile devices.

4.4 Training

Participants were seated and presented with a mobile device running the Android OS (Samsung Galaxy Nexus). They were then shown ways to create an on-screen gesture using H4Plock, and were then asked to develop one or more gestures of their own. The gestures created would not need to be used in future tasks, and the aim was to practice entering gestures composed of a single stroke. Twenty four gestures were created during this process, forming a library of gestures (Figure 2). Participants were then introduced to the tactile feedback presented by the mobile device and given the opportunity to learn associations between each vibrational cue and intended meaning (e.g. confirmation that a gesture has been entered, enter primary/secondary passcode, successful/failed entry to the authentication system). The researchers then conducted a walkthrough of the authentication process.

4.5 Task 1: Authenticating with H4Plock

Participants were first asked to set up a primary passcode. The passcode would be composed of a sequence of four on-screen gestures, each formed from a continuous stroke. Participants were free to select from the gesture(s) they created themselves during the training stage, those created by other users in the gesture library, or they could create new gestures if so inclined. They were given the option of entering gestures in any of the quadrants on the mobile device, as well as the number of gestures they wished to use (up to four). To enter the passcode accurately, participants had to recall the right gestures in the right quadrants. They were asked to follow the same steps to create a secondary passcode and rehearse both sequences, and finally, they were encouraged to practice both of the passcodes as many times as needed to feel comfortable with them.

In order to evaluate the feasibility of the authentication mechanism, participants were told that they would be tactually prompted by the mobile device to enter gestures from either their primary or secondary passcodes. For example, if the first gesture from the primary passcode was entered and a vibration stimulus was perceived to prompt entering cues from the secondary passcode, the second gesture from the secondary passcode sequence would be entered. This process would continue until four gestures had been entered. The decision of which passcode they needed to enter was determined using a random Boolean generator. The time taken to enter four gestures, and the number of errors were logged automatically using the system. After completion of this part of the task, participants were interviewed to gain insights into the usability of H4Plock.

Similar to the method employed by Chong et al. (2010), participants were asked to attempt authenticating entry to H4Plock after a period without usage of the system. A five day period was selected, as this was thought to reflect a real-world gap without practice of alphanumeric passwords. The number of attempts made to the system and number of errors were logged on "Day 6", along with time taken to enter the system.

4.6 Task 2: Determining the Impact of Video-Attacks on H4Plock

Six short video recordings were made showing the researchers attempting to successfully authenticate entry to H4Plock using a range of passcodes. Passcodes differed by design and position of gestures on the mobile interface. Participants were asked to view each video in sequence, and try to recreate the passcodes. In other words, they were asked to adopt the role of an attacker. All videos were taken at the same angle, which simulated an over the shoulder view. Setting up the videos in this manner ensured that the attackers would not be affected by inconsistency caused by the target (De Luca et al., 2014; Sherman et al., 2014).

The passcodes varied considerably in complexity. For example, two of the simpler passcodes were comprised of two gestures, each entered twice within the same quadrant. Other passcodes were composed of four different gestures spatially-distributed across up to all four of the quadrants. Participants were shown pairs of videos, and similar to Sherman et al. (2014), participants were given five attempts to recreate the passcode after watching the videos. The three pairs of videos were presented in a randomized order to users. The number of attempts made, time taken to enter the passcode, and number of errors made were logged. No maximum time limits were imposed on participants when recreating the passcodes. After completing the task, participants were presented with a questionnaire examining their experiences. Questions were presented using Likert scales (from 1-7, with 1 representing strongly agree and 7 representing strongly disagree). Follow-up interviews were conducted to solicit suggestions on improving the strength of the authentication mechanism.

In order to reduce the likelihood of an order effect, approximately half of the participants conducted task 2 prior to task 1, while the other half conducted tasks in the reverse order. On average, the study took 45 minutes to conduct (Day 1). A further 15 minutes was taken on Day 6.

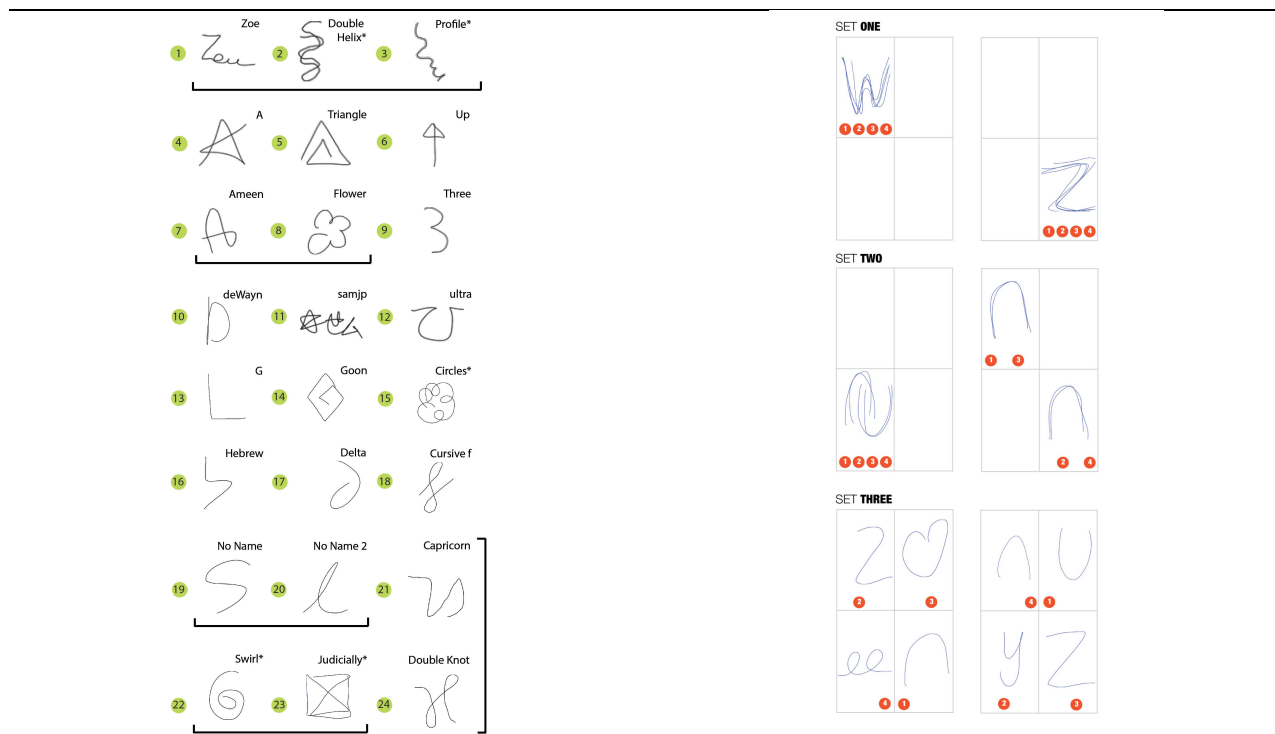


Figure 2. All the gestures created by the participants, and gestures grouped together are created by the same participant. *Unused gesture.

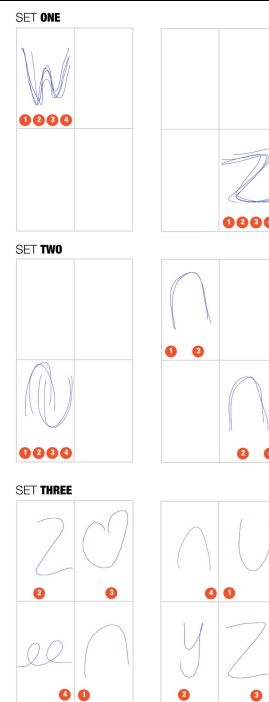


Figure 3. Security passcodes. The figure above details the sets of passcodes used in the security part of the study. Each set is made of 2 passcodes. A primary, and a secondary passcode. The numbers in the orange circles represent the sequence of gestures.

5 Results and Discussion

Passcode accuracy, input speed, and task times were automatically logged by the mobile device. Questionnaires were also analyzed, alongside subjective comments solicited from participants.

5.1 Passcode Creation

Participants were required to design their own primary and secondary passcodes, each composed of four gestures. During this process, they could either devise their own gestures or use gestures from our expanding library. In total, 24 unique gestures were created by participants. These ranged from gestures resembling alphanumeric or Greek characters, to designs which were personal to the user and therefore memorable (e.g. similar shape to a participant’s tattoo) (Figure 2).

Passcodes were most commonly composed of two gestures, which were entered twice (48.5%). Some participants opted to select four unique gestures for both their primary and secondary passcodes. However, due to the novelty of the task, participants stated that repeating gestures would help them to more effectively commit passcodes to memory. Sixteen out of seventeen participants (94.1%) favored entering gestures in each of the four quadrants to form passcodes. To enter these passcodes, the majority of participants followed a ‘Z’ quadrant sequence (e.g. first gesture entered in top-left quadrant, second in top-right, third in bottom-left, and fourth in bottom-right). Out of the 34 passcodes created (17 primary and 17 secondary), only two were similar in composition, largely composed of star-like symbols.

5.2 Passcode Accuracy and Memorability

After setting up a primary and secondary passcode in Task 1, participants were presented with tactile prompts, signaling when gestures from either of the passcodes should be entered. Sixteen out of

seventeen participants (94.1%) were able to react appropriately to the tactile cues presented, and recall and enter gestures from their respective passcodes. On average, 2.7 attempts were made until passcodes were accurately entered. The results provided support for H1, as similar rates were identified when testing other gestural solutions proposed by researchers (e.g. Weiss and De Luca, 2008). Participants were asked to return after a period of five days without use of their passcodes, to authenticate entry to the system. Participants again had a total of five attempts to access the system, but they were not required to use all the attempts in case of a successful attempt. Fifteen of the seventeen participants were able to come back to do the follow-up study. Eleven out of fifteen (73.3%) were able to authenticate entry successfully within two attempts (Day 6). Issues were largely similar to the error categories defined by De Luca et al. (2014) including gestures entered in the wrong order or in the wrong quadrant.

5.3 Input Speed

Input time was measured from when the finger touched the screen to enter the first gesture in the sequence, and stopped when the finger was lifted up after the fourth gesture was entered. Participants spent on average 11 seconds entering four-gesture passcodes. Table 1 shows that as participants practiced entering gestural passcodes on Day 1 (e.g. entering a primary passcode and secondary passcode), time taken reduced. After a five-day period without rehearsal, participants spent on average 3 seconds longer authenticating entry to the system (average task time taken: 14 seconds). The results highlighted that similar to alphanumeric passwords or PINs, if there is a gap without rehearsal of gestures and tactile authentication stimuli, it can take additional time to precisely recall these cues.

Table 1: Average time taken to set-up and authenticate entry to H4Plock

	Average time taken (seconds)
Gesture creation	23
Set-up of primary code	21
Set-up of secondary code	15
Practice entry	10.5
Entry to H4Plock after rehearsal of cues	11
Entry to H4Plock after a period of five days	14
Recreation of passcodes from video-camera attacks	11

5.4 Replication of Passcodes from Videos

Six videos were presented to participants. Each of these videos showed a researcher attempting to authenticate using passcodes. Each passcode varied by design and position of gestures on the mobile interface (Figure 3). In the videos where the same gesture was entered four times in the same quadrant, 94.1% of participants were able to recreate entry. As passcodes developed in complexity (e.g. two gestures in different quadrants repeated twice (Set 2)), fewer participants were able to replicate these to enter H4Plock. Thirteen participants were able to recreate entry (76.5%), with only seven managing on their first attempt (41.2%). Replicating passcodes composed of four unique gestures in different quadrants proved to be toughest for participants. Only four participants (23.5%) were able to replicate entry, with only a single participant managing to gain access on the first attempt. As the number of non-repeating gestures which needed to be remembered increased along with the number of quadrants accessed, replication rates reduced, providing support for H2.

5.5 Usability of Solution

Findings from a post-task questionnaire offered insights into the usability of the solution. Although this was the first system encompassing both gestural and tactile cues that participants had accessed, they were able to express strong levels of confidence in using the system unaided, and found the system no less perceivably secure or trustable compared with entering alphanumeric passwords or PINs. The solution was thought to offer potential, as it could help users to feel more protected against observer and video-based attacks.

Participants responded largely neutrally to using passcodes composed of a sequence of four unique gestures (average of 3.2 on a 7 point Likert scale). When asked about their reasoning, they described the challenges committing multiple gestures and their respective locations for entry to memory.

Although using four unique gestures was considered perceivably more secure, particularly if these were located in separate quadrants, participants agreed that a trade-off needed to be made to foster memorability. When asked about strategies to remember passcodes, two participants described trying to write down the information. However, this was a challenging process due to the design of the gestures. The participants agreed that even if these had been written down, as gestures and tactile cues are personal in nature to each user, it may have been challenging for a third party to recreate entry. Other participants described developing stories involving each gesture, which could be recalled prior to when authentication needed to be performed.

The majority of participants strongly agreed with the statement that tactile cues contributed to increasing levels of perceived security of the system (average of 2.3 on a 7 point Likert scale). They expressed confidence in using the prototype in crowded areas where observers may be prevalent, with the knowledge that using two-factors of authentication (gestural input and tactile feedback) would reduce the risk of attack. The authentication sequence would vary on each successive entry due to the randomized nature of the Boolean generator indicating which passcode to enter. Around half of the participants (52.9%) voiced concerns that if tactile feedback was missed, or cues were attenuated (e.g. if the user's hand holding the phone was in motion), it could be challenging to identify whether gestures from the primary or secondary passcode would be entered. To reduce the issues encountered, suggestions were made to manipulate parameters of vibrations (e.g. amplitude) to make them more discernable.

In terms of enhancements to the prototype, participants indicated that a contextually-aware system would offer considerable potential to them. For example, if the mobile device itself could detect that the user was in a "safe" location (e.g. at home), fewer tactile signals would need to be presented. If the phone could detect the presence of third parties in close proximity to the user, additional tactile cues presented would provide awareness to the user to maintain vigilance in their surroundings. Participants also described methods of deceiving onlookers. Our participants described entering redundant gestures which did not belong to their passcodes, in order to maintain deception, similar to an idea discussed by De Luca et al. (2009).

6 Contextualizing Findings

Findings from the studies described in this paper showed that 94.1% of participants were able to recall their passcodes using H4Plock, with minimal levels of training. Only one participant was unable to recall his passcode within the attempts presented. Research suggests that evaluation of other gestural mechanisms have shown similar rates of recall (e.g. Weiss and De Luca, 2008; Kuribara et al., 2014). In terms of input speed, performance using H4Plock (11s) was faster compared with similar systems designed to address shoulder surfing attacks. Kuribara et al. (2014) state that their results (23.8s) vary from Bianchi et al. (2011) - 20.2s, and Sasamoto et al. (2008) - 32s. In contrast to other solutions, H4Plock enables users to make free-form gestures in a range of quadrants of their choosing. This increases the entropy of the system, supporting levels of perceived security. The process of remembering gestures and entering them in response was found to be cognitively demanding, especially if four different (non-repeating) gestures were entered in all four quadrants on the screen. Freeform gestures were selected to increase the entropy of the solution. However, future work could examine the impact of selecting standardized gestures. The resulting system could then be evaluated against the wide range of usability, deployability, and security criteria proposed by Bonneau et al. (2012), to better assess the ability of the solution to match user needs and abilities.

Video-or photo-based attacks have been utilized by a range of researchers to evaluate authentication mechanisms (De Luca et al., 2010; Sherman et al., 2014; Kwon and Na, 2014). Findings from our studies highlighted that participants were able to recreate entry to H4Plock much more easily if fewer gestures which repeated themselves were entered in fewer quadrants. As gestures became more abstract in design (i.e. less similar to a geometric shape or recognizable alphanumeric character), greater challenges were faced when replicating these. There was also evidence of a primary effect, where participants were able to remember the initial gestures entered, but not the later ones. Participants highlighted that the design of the interface helped to make fraudulent entry by third parties much more difficult. Attackers would need to be able to learn the meanings associated with the tactile feedback presented, as well as remembering the gestures entered. In contrast to other solutions which rely on the user inputting erroneous information to confuse an observer (e.g. De Luca et al., 2009), H4Plock is one of the first solutions that relies on the user precisely recalling information from two known passcodes to authenticate.

7 Contributions from the Study

In this paper, we have described a study examining a novel authentication approach. The feasibility of using both gestural and tactile cues for purposes of authentication has been demonstrated. Participants were able to respond appropriately to tactile prompts, utilizing information from both primary and secondary passcodes. Findings have shown that these cues can be committed to memory and recalled after periods without using the system. Furthermore, we have assessed the susceptibility of the solution to video-based attacks. Findings have suggested that selecting passcodes which are diverse in gesture design and location would offer potential to heightening levels of perceived security, as it helps to reduce the likelihood of video-based (observer) attacks. However, care is needed in the selection of gestures, to minimize challenges replicating stimuli.

8 Conclusion and Future Work

This paper has described a novel approach that can enable users to authenticate entry to a system using gestural and tactile information. Results from an exploratory study have shown that participants were able to memorize and authenticate entry after a five day period, simulating real world usage. H4Plock proved to be secure against 76.5% of participants, who carried out attacks immediately after watching a set of videos where gestures were unique in design and entered at different locations around the interface. Participants were able to express strong levels of confidence in using the system, which could be used to support users from observer attacks.

The next steps for this research include examining ways to strengthen the interface; for example, providing more kinds and varied tactile feedback that are more detectable when in motion. A comparison study can then be undertaken against other mechanisms which are commonly used in conjunction with mobile devices (e.g. PIN, unlock patterns). This will help to identify the merits of H4Plock, along with areas for improvement.

References

- Ali, A., Kuber, R., & Aviv, A.J. (2015). H4Plock: supporting mobile user authentication through gestural input and tactile output. Poster Session of the 11th Symposium on Usable Privacy and Security.
- Aviv, A., Gibson, K., Mossop, E., & Blaze, M. (2010). Smudge attacks on smartphone touch screens. Proceedings of the 4th USENIX Conference on Offensive Technologies, USENIX Association, 1–7.
- Azenkot, S., Rector, K., Ladner, R., & Wobbrock, J. (2012). PassChords: secure multi-touch authentication for blind people. Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility. ACM, 159-166.
- Bianchi, A., Oakley, I., Kostakos, V., & Kwon, D.S. (2011). The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. Proceedings of the Fifth International Conference on Tangible, Embedded, And Embodied Interaction, ACM, 197-200.
- Bianchi, A., Oakley, I., Lee, J.K., & Kwon, D.S. (2010). The haptic wheel: design & evaluation of a tactile password system. Extended Abstracts on Human Factors in Computing Systems, ACM, 3625–3630.
- Bonneau, J., Herley, C., van Oorschot, P.C., & Stajano, F. (2012). The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. Proceedings of the 2012 IEEE Symposium on Security and Privacy. IEEE Computer Society, 553-567
- Chen, Y., Sun, J., Zhang, R., & Zhang, Y. (2015). Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices. Proceedings of the 34th IEEE International Conference on Computer Communications. (INFOCOM'15), IEEE.
- Chong, M.K., Marsden, G., & Gellersen, H. (2010). GesturePIN: Using discrete gestures for associating mobile devices. Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices & Services, ACM, 261–264.
- De Luca, A., Harbach, M., von Zezschwitz, E., et al. (2014). Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14). ACM, 2937-2946.
- De Luca, A., Weiss, R., & Hußmann, H. (2007). PassShape: stroke based shape passwords. Proceedings of the 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces, ACM, 239–240.

- De Luca, A., von Zezschwitz, E., & Hußmann, H. (2009). Vibrapass: secure authentication based on shared lies. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 913–916.
- De Luca, A., Hertzschuch, K., & Hußmann, H. (2010). ColorPIN – securing PIN entry through indirect input. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 1103–1106.
- Kuber, R. & Yu, W. (2010). Feasibility study of tactile-based authentication. *International Journal of Human-Computer Studies* 68, 3, 158–181.
- Kuber, R. & Sharma, S. (2010). Toward tactile authentication for blind users. *Proceedings of the 12th International ACM Conference on Computers and Accessibility*, ACM, 289–290.
- Kuber, R. & Sharma, S. (2012). Developing an extension to an existing tactile authentication mechanism to support non-visual interaction. *Proceedings of IASTED Conference on Human-Computer Interaction*, 190–198.
- Kuribara, T., Shizuki, B., & Tanaka, J. (2014). VibralInput: two-step PIN entry system based on vibration and visual information. *Extended Abstracts of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 2473–2478.
- Kwon, T. & Na, S. (2014). TinyLock: affordable defense against smudge attacks on smartphone pattern lock systems. *Computers & Security*, 42, 137–150.
- Oakley, I. & Bianchi, A. (2012). Multi-touch passwords for mobile device access. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, ACM, 611–612.
- Qian, H., Kuber, R., & Sears, A. (2009). Towards identifying distinguishable tactons for use with mobile devices. *Proceedings of the 11th International ACM SIGACCESS Conference on Computers and Accessibility*, ACM, 257–258.
- Sae-Bae, N., Ahmed, K., Isbister, K., & Memon, N. (2012). Biometric-rich gestures: a novel approach to authentication on multi-touch devices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 977–986.
- Sasamoto, H., Christin, N., & Hayashi, E. (2008). Undercover: authentication usable in front of prying eyes. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 183–192.
- Serwadda, A. & Phoha, V.V. (2013). When kids' toys breach mobile phone security. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ACM, 599–610.
- Sherman, M., Clark, G., Yang, Y., Sugrim, S., Modig, A., Lindqvist, J., Oulasvirta, A. & Roos, R. (2014). User-generated free-form gestures for authentication: security and memorability. *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*, ACM, 176–189.
- von Zezschwitz, E., De Luca, A., & Hußmann, H. (2014). Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance. *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, ACM, 461–470.
- von Zezschwitz, E., De Luca, A., Brunkow, B., & Hußmann, H. (2015). SwiPIN: fast and secure pin-entry on smartphones. *Proceedings of the Conference on Human Factors in Computing Systems*, ACM, 1403–1406.
- Weiss, R. & De Luca, A. (2008). PassShapes - utilizing stroke based authentication to increase password memorability. *Proceedings of NordiCHI*, ACM (2008).
- Zakaria, N.H., Griffiths, D., Brostoff, S., & Yan, J. (2011). Shoulder surfing defence for recall-based graphical passwords. *Proceedings of the Seventh Symposium on Usable Privacy and Security - SOUPS '11*.