H4Plock: Supporting Mobile User Authentication through Gestural Input and Tactile Output

Abdullah Ali and Ravi Kuber
{aali6,kuber}@umbc.edu
University of Maryland, Baltimore County
Baltimore, MD, USA

Adam J. Aviv
aviv@usna.edu
United States Naval Academy
Annapolis, MD, USA

ABSTRACT

We have developed a novel authentication mechanism, H4Plock (pronounced "Hap-lock"), that leverages gestural input and tactile feedback to defend against casual observation attacks. Users enter up to four on-screen gestures based on receiving tactile prompts, in the form of vibrations, from the mobile device. These prompts inform the user as to which gestures should be entered. The style of vibrations, e.g., short versus long, indicate the specific gestures that should be entered from a previously chosen primary or secondary passcode. As a result, the sequence of gestures will vary on each authentication attempt, reducing the capability of an attacker to "shoulder surf" and accurately recreate the authentication process. We developed a protype of the application and conducted an IRB approved pilot study. Findings show that 94% of participants were able to properly authenticate using H4Plock, with 73% successfully accessing the system after a gap of five days without rehearsal. We also examined the security of the H4Plock where participants were asked to recreate passcodes through a video replay, simulating a shoulder surfing attack scenario. Even after direct observations, only 25% of the pascodes could be successfully recreated.

1. INTRODUCTION

This poster abstract describes the design and evaluation of a novel authentication mechanism, H4Plock, pronounced "Hap-lock", developed to address a number of the challenges when users attempt to authenticate on mobile devices (Figure 1). In contrast to other authentication mechanisms, H4Plock relies on the user making small, on-screen gestures based on tactile feedback from the mobile device in the form of vibrations that inform which gestures should be entered. 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, indicating that the user should enter specific gestures from a pre-selected primary or secondary passcode. Prompts are presented 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 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.

The research progress described herein addresses three areas: (1) the feasibility of using both 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.

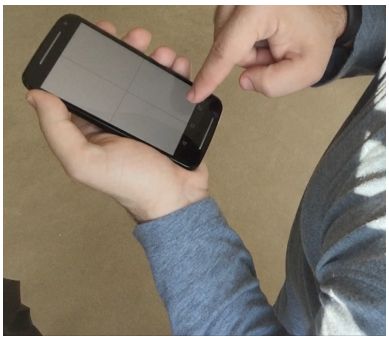

Figure 1: Screenshot of H4Plock as used in the videos for security testing session

2. PROTOTYPE H4PLOCK

We built the H4Plock prototype on Android using the built-in gesture library and the vibration motor interface. The basic design of the user interface is presented in Figure 2, where the user is required to enter a sequence of up to four pre-selected on-screen gestures while responding to tactile prompts in the form of vibrations. The authentication procedure occurs over four quadrants of the phone where each quadrant can recognize 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. When authenticating, a tactile prompt will be presented indicating that a gesture from the primary or secondary passcode should be 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 designed using guidance from [2] who had studied ways to differentiate pairs of tactile cues presented using a mobile device.

3. PILOT STUDY

The pilot study recruited 17 participants (9 male, 8 female) between the ages of 18-69. Participants completed two tasks: first, we measured participants ability to use, create, and remember their own passcodes, and secondly, we measured the susceptibility of the system to observer attacks, e.g., shoulder surfers, through video replays of the authentication from the researchers, and the partic-

Figure 2: 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.

ipants were asked to replicate the observed entry to the system, similar to studies [3, 1].

In total, 24 unique gestures were created by participants comprising of 34 unique passcodes. Only two were similar in composition, largely composed of star-like symbols. 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. Participants were asked to return after a period of five days without use of their passcodes, to authenticate entry to the system. Fifteen of the seventeen participants were able to come back to do the follow-up study, and eleven out of fifteen (73.3%) were able to authenticate entry successfully within two attempts (Day 6).

To test the susceptibility to shoulder surfing attack, 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 gesture on the mobile interface (Figure 3). In the videos where the same gesture was entered four times in the same quadrant, 94% of participants were able to recreate entry. As passcodes developed in complexity (e.g. two gestures in different quadrants), fewer participants were able to replicate these to enter H4Plock (53%). Replicating passcodes composed of four unique gestures in different quadrants proved to be toughest for participants. Only 25% were able to replicate entry, with only a single participant managing to gain access on the first attempt.

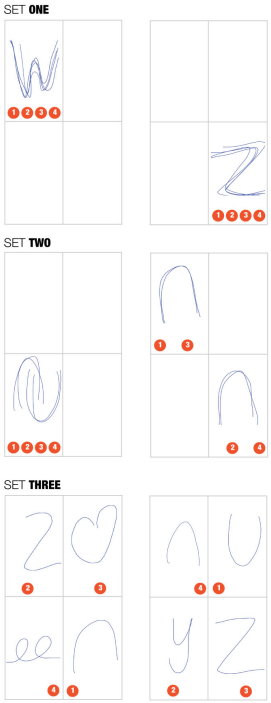

Figure 3: Security Passcodes. The figure above details the sets of passcodes used in the security part of the study. Each set is made of 2 passcodes. A primary, and a secondary passcode. The numbers in the orange circles represent the sequence of gestures

4. CONCLUSION

This poster abstract describes H4PLock that combines tactile feedback and gestural authentication to create a system that is usable and secure against observation (shoulder-surfing) attacks. 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. The next steps for this research include examining ways to strengthen the interface, a longitudinal study, and additional investigation into the memorability and perceived security of the system.

5. REFERENCES

[1] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith. Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, 2014.

[2] H. Qian, R. Kuber, and A. Sears. Towards identifying distinguishable tactons for use with mobile devices. In *Proceedings of the 11th international ACM SIGACCESS conference on Computers and accessibility*, 2009.

[3] M. Sherman, G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvirta, and T. Roos. User-generated free-form gestures for authentication: Security and memorability. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, 2014.