Authentication on Public Terminals with Private Devices

Andrea Bianchi
Korea Advanced Institute of Science and Technology
Daejeon, Korea
andrea@kaist.ac.kr

ABSTRACT

Authentication in public spaces, such as ATM PIN entry, is inherently susceptible to security attacks based on observation in person or via cameras. This paper briefly introduces the idea of decoupling the authentication process in two separate sub-tasks (the interaction needed for PIN input and its transmission to the terminal), each with different usability and security goals. In order to support this idea, we present two research projects based on multimodal feedback and physical proximity and explain how they fit into this model.

Author Keywords
PIN entry, password, security, usability, observation.

ACM Classification Keywords
H5.2. User Interfaces: Input devices and strategies.

General Terms
Design, Security.

INTRODUCTION

Authentication by means of passwords or numerical PINs to public terminals, such as ATMs and credit card kiosks, is commonplace. Although such systems have long been the object of studies and systematic improvements, public terminals are still prone to a wide range of security threats [8]. Paradoxically, the most effective attacks simply rely on the hazardous behavior of users who unintentionally expose themselves to attackers: a typical example is the observation attack, in which passwords are stolen by means of camera or shoulder-surfing [4].

Recently researchers in usability and security have devoted substantial efforts towards finding methods to resist observation attacks during authentications on public terminals. These methods include systems that use non-visual modalities such as haptics to obfuscate displayed cues [2], the use of eye-trackers as an input technology [5] and a range of techniques to indirectly type PINs [e.g. 3].

These methods are clearly effective, but they also introduce higher complexity for users, which is often mitigated by compromising security for improved usability. It is furthermore clear that most methods proposed to counter observation attacks, despite the approach chosen, operate under the same underlying assumption: public terminals are intrinsically vulnerable to observation attacks because they take the form of physical installations situated in public spaces (e.g., public kiosks).

In this paper we argue that, by simply shifting the authentication process from a public terminal to a safer user-owned private device (e.g. [7]), such as a mobile phone, we can achieve better security without compromising usability. In fact, by decoupling the authentication process into two modular and independent sub-tasks - the input-interaction and the PIN-transmission - we can achieve a highly usable front-end PIN entry interface backed up by a secure system for transmitting it to the terminal. A running theme through this work is an emphasis on physical and multi-sensory input which relies on techniques such as haptic feedback and physical proximity to ensure security. We believe that this approach makes the interfaces described in this work particular salient to the research area of tangible interaction.

OUR APPROACH IN PRACTICE

By subdividing the authentication process into two modular and independent components, the input method and the transmission of the PIN to the terminal, we can simultaneously improve usability of the input interface and achieve a secure transmission channel between the private device and the terminal. We present briefly two prototypes, the Phone Lock [1] and LuxPass: the former shows an example of how users can choose different PIN modalities (haptics or audio) according to their preferences and security levels; the latter shows an example of how we can transmit a PIN from the phone to the terminal, without need of pairing the two and avoiding eavesdropping by third parties (known as the Man-In-The-Middle (MITM) attack).

Phone Lock

The Phone Lock is a PIN entry system for mobile phones resistant to visual observation because is based on locating and identifying auditory or tactile cues rather than visual ones. Phone Lock provides users an interaction technique in two modalities (audio and haptic) and leaves the choice of which to select to the users themselves.

In general, the Phone Lock interaction is based on a paradigm of randomization of cue location prior to user search and selection for a password item. The user directly manipulates a dial drawn on the display of a touch screen phone. Different segments of the dial are associated with different cues, each of which is played in response to a

TEI'11, January 22–26, 2011, Funchal, Portugal.
ACM 978-1-4503-0478-8/11/01.

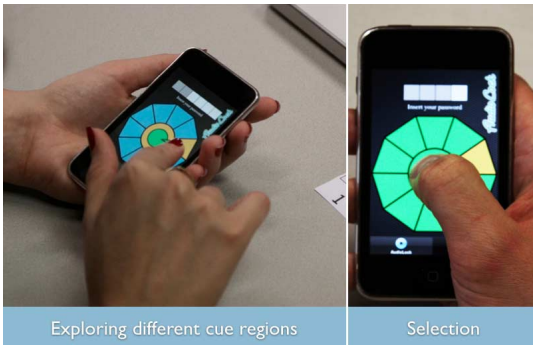

Figure 1 Phone Lock interface and interaction: exploring the cues (left) and selection of a cue (right).

Figure 2 LuxPass receiver unit prototypes (left) and software GUI. Simplified example of light encoding (right).

user's touch. The Phone Lock wheel is simple to configure with differently sized cue sets and segment sizes, but in our implementations we used a maximum of either 10 iconic audio cues (i.e., spoken numbers from zero to nine) or 10 distinguishable tactile patterns (i.e., vibration patterns). Audio cues are delivered via headphones to ensure they remain private, while tactile cues are rendered using a pager motor mounted on the phone.

We developed a prototype for the Apple iPhone (Figure 1) and run a user study [1], whose preliminary results suggests that, with the use of appropriate cues sets, the system maintains or improves upon the performance, usability and security of previous observation resistant PIN systems [2].

LuxPass

LuxPass (Figure 2) is a novel interaction method that allows users to authenticate to a public terminal using a mobile phone without requiring explicit pairing. The goal in this case is to shift in time and space the authentication procedure, enabling the user to authenticate on their mobile phone at a convenient time, and then to complete their transaction by transmitting the authentication data from the phone to the public terminal.

Although previous work in this direction has focused on either ensuring a direct communication channel with a pre-agreed third-party infrastructure, or by using out-of-band (OOB) side channels to establish a paired connection [6] between the phone and the terminal (e.g., using accelerometer data to establish a connection), LuxPass adopts a different approach in which physical proximity is sufficient to achieve a secure transaction.

LuxPass works by displaying messages through modulated patterns of light on a mobile phone screen that are then sensed by a device and decoded back into a PIN. LuxPass relies on close physical contact with a sensor terminal to ensure this channel is private. A key advantage of this approach is that it is based on standard component of a mobile device (the screen) making it economical and easy to deploy. Although further explorations are needed, results from in-progress studies seemed encouraging: users expressed positive consensus toward LuxPass. Moreover, a security user study in a lab setting demonstrated the strength of LuxPass against observation and MITM attacks.

CONCLUSIONS

In this paper we have briefly introduced a method to decouple the authentication process into two independent subtasks - the input interaction and the PIN transmission to the terminal - and we have presented our previous work to support this framework. Further research is needed for improving both the components of the system and in finding better ways to integrate them. Regardless, we believe that decoupling authentication into sub-tasks will become common practice in the design of secure public terminals.

ACKNOWLEDGMENTS

We thank Ian Oakley and Dong Soo Kwon for their valuable advice and contributions to this work.

REFERENCES

1. Bianchi, A., Oakley, I., Kostakos, V., Kwon, D., The Phone Lock: Audio and Haptic shoulder-surfing resistant PIN entry methods. In Proc of TEI'11.
2. Bianchi, A., Oakley, I., Kwon, D., The secure haptic keypad: a tactile password system. In Proc. of CHI'10, pp.1089-1092.
3. De Luca, A., Hertzschuch, K., Hussmann, H., ColorPIN: securing PIN entry through indirect input. In Proc. of CHI'10, pp.1103-1106.
4. De Luca, A., Langheinrich, M., and Hussmann, H., Towards understanding ATM security: a field study of real world ATM use. In Proc. of SOUPS'10, pp. 1-10.
5. Forget, A., Chiasson, S., Biddle, R., Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In Proc. of CHI'10, pp.1107-1110.
6. Kobsa, A., Sonawalla, R., Tsudik, G., Uzun, E., Wang, Y., Serial hook-ups: a comparative usability study of secure device pairing methods. In Proc. of SOUPS '09.
7. Mccune, J.M., Perrig, A., Reiter, M.K., Seeing-is-believing. In Proc. of IEEE Symposium on Security and Privacy, pp. 110–124, 2005.
8. Rogers, J. Please enter your 4-digit PIN. Financial Services Technology, U.S. Edition, Issue 4, Mar. 2007.