3-22-2019

An Exploration of Countermeasures for Augmented Reality Shoulder Surfing Attacks

Christopher Kreider
Christopher Newport University, chris.kreider@cnu.edu

AN EXPLORATION OF COUNTERMEASURES FOR AUGMENTED REALITY SHOULDER SURFING ATTACKS

Christopher Kreider
Christopher Newport University
chris.kreider@cnu.edu

Keywords

Information security, passwords, shoulder surfing, augmented reality

ABSTRACT

Information security is an area that IS researchers can and should contribute to (Zafar and Clark, 2009), including password related research (Kreider, 2018; Kreider and Rao, 2010). One common attack against password entry, the shoulder surfing attack, occurs when an attacker unknowingly observes a user while entering their password (Tari et al., 2006), which has been shown to be a feasible attack using the Microsoft Hololens augmented reality wearable. While the attack was shown to be feasible, no countermeasures were explored. This paper will explore potential countermeasure to the shoulder surfing attack presented by Kreider (2018). The countermeasures will be explored both from an efficacy perspective, as well as a usability perspective. While other studies exploring this phenomena focus on the importance of discreet input, such as a haptic sensor (Roesner et al., 2014) and gesture control armbands utilizing electromyography (Zhang et al., 2017), our study will explore mechanisms not requiring discreetness.

The shoulder surfing attacks identified by Kreider (2018) take advantage of the fact that the users selection of the characters in the Microsoft Hololens augmented reality wearable are easily observable. Specifically, the user must move their head to center the cursor on the character in the AR keyboard, and "air tap" within the purview of the front facing characters to select each character. Finally, once completed, the user selects "close keyboard" key on the AR keyboard, which is always located in the same location relative to the keyboard. While an observer cannot see the keyboard the user is viewing, they can observe the user during entry, and reverse the path the head takes when selecting the characters, starting at the "close keyboard" character.

To counter this ability to reverse the course taken to identify the characters selected, we have identified three potential counter measures: keyboard randomization, keyboard jitter, and keyboard warping. Keyboard randomization will alter the location of keys within the keyboard after each character is selected, and has been explored by (Zhang et al. 2017). Keyboard jitter will alter the location of the keyboard as a whole randomly in the AR space after each character is selected. Finally, keyboard warping will alter the way in which the keyboard is presented so that it is not a perfect rectangle, but instead, is randomly changed in shape for each password entry. Each of these is designed to alter the keyboards arrangement and/or location within the AR space viewable by the user. For each of these counter measures, we seek to explore how efficient they are disabling the shoulder surfing attack described above, while also exploring the usability of such countermeasures from the users perspective. Finally, we will explore how difficult each countermeasure would be to implement.

REFERENCES

1. Kreider, C. (2018) The Discoverability of Password Entry Using Virtual Keyboards in an Augmented Reality Wearable: An Initial Proof of Concept, *Southern Association for Information Systems*, St. Simons Island.
2. Kreider, C., and Rao, V. S. (2010) User Acceptance of Multiple Password Systems: A Proposed Study, *Americas Conference on Information Systems*, Lima, Peru.
3. Roesner, F., Kohno, T., and Molnar, D. (2014) Security and Privacy for Augmented Reality Systems, *Communications of the ACM,* 57, 4, 88-96.
4. Tari, F., Ozok, A., and Holden, S. H. (2006) A Comparison of Perceived and Real Shoulder-Surfing Risks between Alphanumeric and Graphical Passwords, *Proceedings of the second symposium on Usable privacy and security*: *ACM*, 56-66.
5. Zafar, H., and Clark, J. G. (2009) Current State of Information Security Research in Is, *Communications of the Association for Information Systems,* 24, 34, 557-596.
6. Zhang, R., Zhang, N., Du, C., Lou, W., Hou, Y. T., and Kawamoto, Y. (2017) Augauth: Shoulder-Surfing Resistant Authentication for Augmented Reality, *Communications (ICC), 2017 IEEE International Conference on*: *IEEE*, 1-6.