Headline: Identifying people by eye movements potential replacement for passwords

Authors: Michael Brooks1, Cecilia R. Aragon1, and Oleg V. Komogortsev2

1University of Washington, Seattle, WA,

2Texas State University, San Marcos, TX

{mjbrooks, aragon}@uw.edu, ok11@txstate.edu

Summary: People's perceptions of an emerging biometric authentication technique based on unique eye movement patterns suggest that it could be preferred over passwords if certain lingering barriers can be overcome.

Passwords, currently the most ubiquitous authentication mechanism in general-purpose applications, are hard to remember and easy to steal. Biometric authentication—identification through a person's distinctive physical or behavioral characteristics—offers a more convenient alternative which requires no memorization. However, biometric systems have failed to gain widespread adoption, in part due to usability and cultural acceptability issues (1).

The ways in which a person's eyes move are, to some extent, unique. In the past few years, biometric authentication based on eye movement has emerged as an active area of research and development, giving rise to promising new algorithms and techniques with ever increasing performance (2, 3). We have conducted a study on how potential users of such an eye movement biometric authentication system perceive its usability, security, and overall desirability (4). The aim of this work is to provide a human-centered perspective early in the development of this technology, leading to more user-friendly, socially acceptable authentication systems in the future.

Several distinct technical approaches to biometric authentication through eye movement characteristics have been proposed in the past few years, with varying levels of performance, but all involve the use of an eye tracker, a device that uses reflection of infrared light to measure the direction of a person's gaze many times per second. The person being identified gazes at some changing visual stimulus on a computer screen, while the eye tracker observes the movement of their eyes. The exact nature of the stimulus, and the algorithm that reduces the raw gaze observations to a biometric "template" that can be matched against a database of authorized individuals, are both subjects of ongoing research.

We developed a series of high-fidelity prototypes of user interfaces for authenticating people at an ATM (automated teller machine). Because the underlying algorithms for recognizing users are still rapidly evolving, we focused on the design of the user interface, simulating the authentication mechanism; the system's decision to recognize or deny the user was determined ahead of time. The key difference between the designs tested was the visual stimulus shown on the screen while the eye tracker captured the user's eye movement data. One prototype used an array of stationary targets that the user activated in sequence (Figure 1), using their gaze, while another displayed a passage of text which the user was required to read. For comparison, we also constructed a traditional authentication prototype using a PIN (personal identification number), the ATM analog of a password.

***Figure 1**. The user activates each circle using their gaze, while the eye tracker records eye movement data for authentication.*

A group of 22 people were recruited to participate in a lab study wherein they were asked to authenticate several times with each of the prototype designs (Figure 2). Participants were not aware that the acceptance or rejection of their biometric signature was predetermined, believing it to be a fully working system. We recorded the time taken to authenticate and any problems encountered, such as poor eye tracking accuracy. We also asked participants to rate and comment on the usability and security of each of the systems tested. Their comments revealed an expectation that biometric authentication can provide stronger security than PINs, both because PINs can be stolen easily and reused, and because biometrics are perceived as newer and more sophisticated. Between the two eye movement designs we tested, there were subtle differences in the level of security perceived by participants. Some believed that the reading-based design would capture more personally unique, identifiable features than the target-activation interface, making it more resilient to certain kinds of attacks. On the other hand, others felt that patterns of eye movement during a general activity like reading would be easier for a malicious third party to capture.

***Figure 2**. The prototype ATM authentication interface running on a computer in our usability lab. The eye tracker is positioned beneath the display.*

As for usability, the targeting design was usually preferred over reading because of its game-like quality of interaction requiring little attentiveness; the text took longer to read and was difficult to process for some participants. However, overshadowing these findings was the fact that eye trackers still must be calibrated to the user's eyes before each session, which adds 10-20 seconds of overhead to the authentication process. This barrier must be overcome in order for eye movement biometrics to achieve the speed and convenience of PIN- or password-based authentication.

Human-centered design, design that is principally guided by the needs and constraints of humans and social systems, has played a relatively small role in the field of biometric systems research and development, a field historically driven by objective technology-centered metrics such as statistical accuracy and security of identification algorithms and sensors. We have taken the first look at how people might interact with a biometric authentication system based on unique eye movement characteristics. Our findings demonstrate the important effect that user interface design can have on usability and perceived security, both of which are critically important to the ultimate success or failure of a security system outside of the lab (5, 6). We hope that this work inspires further human-centered investigations of biometric security systems, and a greater appreciation of the human and social context in which security systems operate.

Acknowledgments: This research was supported by the National Institute of Standards and Technology (NIST) under grant 60NANB10D213. We thank the Laboratory for Usability Testing and Evaluation at the University of Washington for equipment. In addition we would like to acknowledge NSF CAREER Grant #CNS-1250718 award given to Dr. Komogortsev.

References

1. L. Coventry, *Usable biometrics*, in L. F. Cranor and S. Garfinkel (eds.) Security and usability: designing secure systems that people can use, O'Reilly Media, 2005.

2. P. Kasprowski, *Human identification using eye movements*, Praca doktorska, Politechnika Œląska, 2004.

3. O. V. Komogortsev, S. Jayarathna, C. R. Aragon, and M. Mahmoud, *Biometric identification via an oculomotor plant mathematical model*, Proc. Eye Tracking Research and Applications, 2010.

4. M. Brooks, C. R. Aragon, O. V. Komogortsev, *Perceptions of Interfaces for Eye Movement Biometrics*, Proc. International Conference on Biometrics, 2013.

5. M. A. Sasse, *Usability and trust in information systems*, in Robin Mansell and B. S. Collins (eds.) Trust and Crime in Information Societies, pp. 319–348, Edward Elgar, 2005.

6. M. E. Zurko and R. T. Simon, *User-centered security*, Proc. New Security Paradigms Workshop, 1996. doi: 10.1145/304851.304859