Eye-tracking could outshine passwords if made user-friendly

July 16 2013, by Michelle Ma

The prototype was built to simulate an ATM screen. In this scenario, users followed the highlighted dots with their eyes and the technology tracked their unique eye movements. Credit: Michael Brooks

(Phys.org) —It's a wonder we still put up with passwords. We forget our

highly secretive combinations, so we frequently have them reset and sent to our cellphones and alternative email addresses. We come up with clever jumbles of letters and words, only to mess up the order. We sit there on the login screen, desperately punching in a code we should know by heart.

Despite their inefficiencies, passwords are still the most common electronic authentication systems, protecting everything from our bank accounts, laptops and email to health information, utility bills and, of course, our Facebook profiles. While fingerprint- and eye- and face-recognition authentication technology is progressing, these biometric security systems haven't yet gone mainstream.

University of Washington engineers are trying to figure out why. They found in a recent study that the user's experience could be key to creating a system that doesn't rely on passwords.

"How humans interact with biometric devices is critically important for their future success," said lead researcher Cecilia Aragon, a UW associate professor of human centered design and engineering. "This is the beginning of looking at biometric authentication as a socio-technical system, where not only does it require that it be efficient and accurate, but also something that people trust, accept and don't get frustrated with."

Aragon believes one of the reasons face- and eye-recognition systems haven't taken off is because the user's experience often isn't factored into the design. Her team presented its study, one of the first in the field to look at user preferences, at the International Association for Pattern Recognition's International Conference on Biometrics in June. The researchers found that speed, accuracy and choice of error messages were all important for the success of an eye-tracking system.

"If you develop the technology and user interface in parallel, you can make sure the technology fits the users rather than the other way around," Aragon said. "It's very important to have feedback from all stakeholders in the process while you're designing a biometric identification system."

Researchers developed this prototype to test eye-tracking authentication. The monitor shows a welcome screen and the eye tracker is positioned below. Credit: Michael Brooks, U of Wash.

The UW team in collaboration with Oleg Komogortsev at Texas State University developed a new biometric authentication technique that identifies people based on their eye movements. They ran subjects through several types of authentication, then asked for feedback on the usability and perceived security.

In the study, users simulated withdrawing money from an ATM. The prototype – an ATM-lookalike computer screen with eye-tracking technology – presented three separate types of authentication: a standard four-number PIN, a target-based game that tracks a person's gaze, and a reading exercise that follows how a user's eyes move past each word. With each, researchers measured how long it took and how often the system had to recalibrate.

Eye-tracking technology uses infrared light and cameras. The light reflects off the surface of the eyeball back to the camera when a user's eye is following a dot or words on the computer screen. The tracking device picks up the unique way each person's eye moves.

The UW research team chose the ATM scenario because it's familiar to most people and many machines already have a basic security camera installed.

"The goal of eye-tracking signatures is to enable inexpensive cameras instead of specialized eye-tracking hardware," Aragon said. "This system can be used by basically any technology that has a camera, even a low-quality webcam."

When interviewed afterward, most of the study subjects said they don't trust the standard push-button PIN used in most ATMs, and most assumed that the more advanced technologies would offer the best security.

But when authentication failed – the research team deliberately caused it to not recognize users during one trial – they lost faith in the eye-tracking systems. This study showed that future eye-tracking technology should give clear error messages or directions on how users should proceed if they get off track.

"The error messages we provided and the feedback we gave were really important for making it usable," said Michael Brooks, a UW doctoral student in human centered design and engineering. "It would have been difficult to design these prototypes without getting feedback from users early on."

The standard PIN authentication won for its speed and user-friendliness, but the dot targeting exercise also scored high among users and didn't take nearly as long as the reading exercise. This game-like option could be a model for future versions, Brooks said.

The researchers plan to look next at developing similar eye-tracking authentication for other systems that use basic cameras such as desktop computers. A similar design could be used to log in or gain access to a secure website.

More information: Paper: faculty.washington.edu/aragon/ … Biometrics-ICB13.pdf

Provided by University of Washington