

Forget passwords: How playing games can make computers more secure

A new security approach would let users input patterns instead of words to verify identity

Larry Greenemeier

05 September 2012

An article by *Scientific American*.

It seems like something out of a Robert Ludlum spy novel. Someone tries to coerce you into revealing your computer security passwords. You might be tempted to give in, but it is impossible for you to reveal your authentication credentials. You do not actually know them because they are safely buried deep within your subconscious.

Sounds a bit extreme just to make sure no one can log on to your laptop or smartphone, but a team of researchers from Stanford and Northwestern universities as well as SRI International is nonetheless experimenting at the computer-, cognitive- and neuroscience intersection to combat identity theft and shore up cyber security—by taking advantage of the human brain’s innate abilities to learn and recognize patterns.

The researchers are studying ways to covertly create and store secret data within the brain’s corticostriatal memory system, which is responsible for reminding us how to do things. When a person needs to access a computer, network or some other secure system, they would use special authentication software designed to tease out that secret data.

To test this concept, the researchers devised a computer game requiring players to tap buttons on a keyboard as large black dots descending down their screen cross a horizontal line—very similar in concept to the video game Guitar Hero. During an initial training session lasting from 30 minutes to an hour, the dots fall at different speeds and in various locations, forming patterns that repeat until participants become adept at hitting the appropriate buttons at the right time. In effect, users’ corticostriatal memory becomes adept at repeating a particular pattern over time, such as dialing a phone number or typing a word on a keyboard without looking at one’s fingers.

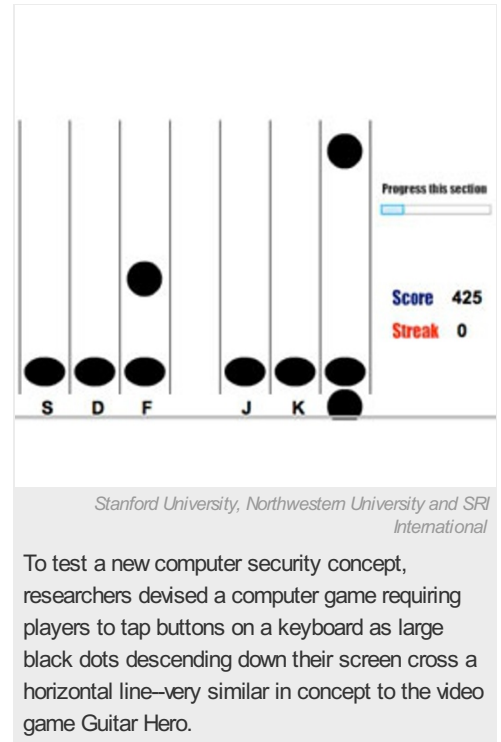
Brain training

The researchers refer to this as “serial interception sequence learning” training, during which a person unwittingly learns a specific sequence of keystrokes that can later be used to confirm that person’s identity. To log on to, for example, a Web site, the user would play the game the same each time that pattern of dots appears, proving his identity and allowing him access.

“While the planted secret can be used for authentication, the participant cannot be coerced into revealing it since he or she has no conscious knowledge of it,” according to the researchers in a study they presented August 8 at the USENIX Security Symposium in Bellevue, Wash. (pdf) As currently conceived, the implicit learning approach being studied might protect against someone either forcing or tricking you to reveal a password, says lead author Hristo Bojinov, a Stanford University Ph.D. computer science candidate. Such coercion could take the form of physical or verbal threats demanding your password or other security credentials, or it could be a seemingly legitimate phone call or e-mail designed to coax out this information.

The researchers say they have tested their approach on 370 players so far and continue to add new participants to their study. The test currently requires at least 30 minutes of training to get reliable results. “It is unlikely that training time can be shrunk much because this type of brain memory takes time to get trained,” Bojinov says. “It may be possible to reduce the authentication time [that follows training], but it is yet to be seen how much.”

Gaming the system



Whether this approach is practical depends upon the system being defended. It is unlikely, for example, that Yahoo or Google would implement this approach to security for their free e-mail services. Would someone want to play a game for several minutes every time they want to log onto their e-mail? A government facility housing nuclear weapons, however, could better justify the time commitment required to log in using the sequence learning method, particularly if users log in once each day and such an approach promises to improve security, says Nicolas Christin, associate director of Carnegie Mellon University's Information Networking Institute.

This implicit learning approach would not necessarily be effective against network hacks. Just as hackers can break into databases where passwords are stored, they could likewise steal information about a user's authentication pattern created during the training process. "Somewhere, the authentication sequence has to be stored so it can be verified, and that may be vulnerable to attack as well," Christin says.

Bojinov responds that the technique he and his colleagues are developing specifically targets the problem of coercion. "Most likely this mechanism will be used in conjunction with others," he says, adding that he and his colleagues are now planning to design a similar game for mobile device security that would create patterns using a broader number of actions, such as rotating or moving their gadgets in addition to pressing buttons on the keypad.

Password persistence

Despite years of predictions that passwords would eventually be phased out in favor of more secure approaches to authentication, they persist because "they are, to date, one of the better—or less bad—compromises between security and usability," Christin says. "They are cheap to implement, work pretty much in any situation, and everybody knows and understands them."

Yet as the number of passwords multiplies, the security technique become less effective because they strain the user's ability to remember them all, particularly if managing a plethora of passwords requires a user to request password resets to replace those that have been forgotten. Hackers have come to rely on password-reset features to hijack people's e-mail and other online services, locking those users out of their own accounts in the process.



Although the approach proposed by Bojinov and his colleagues requires a lot more work to be practical, it represents a welcome shift in how researchers approach security. The method that Bojinov and his colleagues pose turns the problem of usable security technology on its head, Christin says. "We may see more and more research in the space of understanding how certain human aptitudes can be used to improve security," he adds.

The most important thing to take from the research of Bojinov and his colleagues is not that this particular mechanism is the right one for embedding secrets or not, "but rather that the researchers are exploring neuro- and cognitive science as a means of engineering computer security interfaces," agrees Stefan Savage, a professor of computer science and engineering at the University of California, San Diego.

"They have found a way to shove a piece of information into your brain without your knowledge and then take it out," Savage says. "They have turned you into a DRAM, only you have no knowledge of what is stored there. This is Jason Bourne stuff."

Nature | doi:10.1038/nature.2012.11357