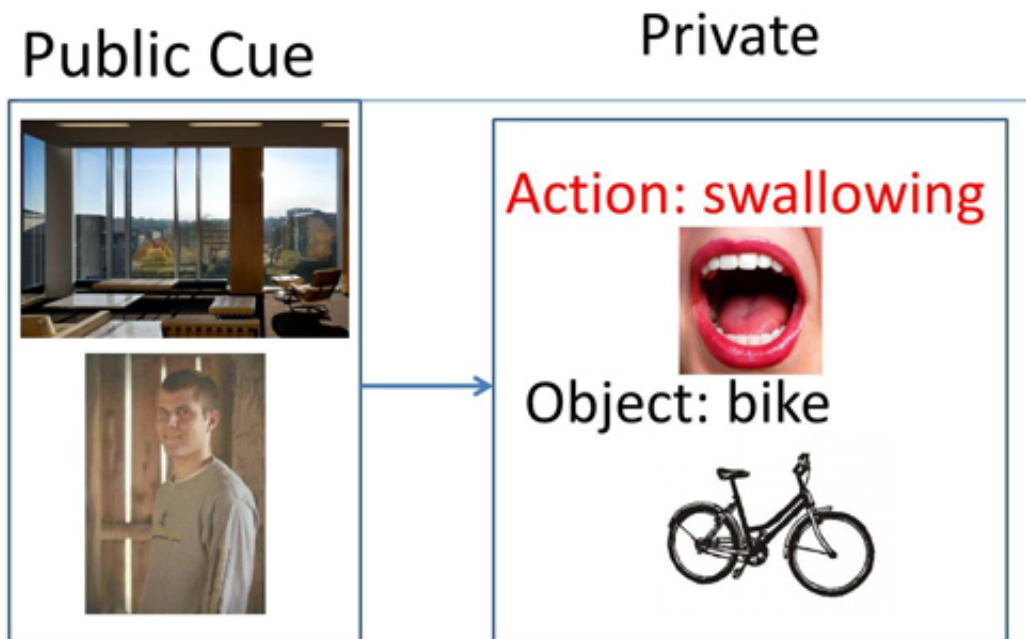# New scheme uses shared visual cues to help people remember multiple passwords

December 4 2013, by Byron Spice

The image combination could be used to generate the sentence, "Jeremiah Blocki swallowing a bike." A password scheme devised by Carnegie Mellon researchers uses a series of such images to create online passwords and to serve as prompts for remembering them.

(Phys.org) —It turns out that the way to keep track of your many passwords to online accounts is the same as how to get to Carnegie Hall—practice, practice, practice. So researchers at Carnegie Mellon University have devised a scheme that enables users to create 100 or

more passwords by remembering—and regularly rehearsing—a small number of one-sentence stories.

The story sentences become the basis for password fragments that are randomly combined to create unique, strong passwords for multiple accounts. The scheme ensures that people remember these sentences by pairing them with photos, which serve as mnemonic devices, and by making sure that people either use or rehearse these sentences frequently enough to keep their memories fresh. These "naturally rehearsing passwords" require a bit more work for the user at the outset than existing password practices, acknowledged Jeremiah Blocki, a Ph.D. student in Carnegie Mellon's Computer Science Department.

"But if you can memorize nine stories, our system can generate distinct passwords for 126 accounts," Blocki said. By memorizing more stories, users can create even more passwords or can make their passwords even more secure. And by reusing and recombining those stories for each password, people naturally rehearse them more often and thus remember them better.

Blocki will present a research paper on naturally rehearsing passwords on Dec. 5 at ASIACRYPT 2013, a scientific conference on cryptology in Bangalore, India.

Blocki and his collaborators—Manuel Blum, professor of computer science, and Anupam Datta, associate professor of computer science and electrical and computer engineering—say the scheme addresses a major usability and security problem posed by the Internet's reliance on passwords. Even casual Internet users accumulate so many passwords that they are difficult or impossible to remember. As a result, too many people simply use the same password over and over, or write down their passwords or use other shortcuts that leave their accounts vulnerable to attackers.

Rather than require websites to revise password practices, the researchers have created an application that helps prompt the memory of users. It is in the process of being implemented as a mobile app as part of an undergraduate research project.

Blum said the researchers based their approach on cognitive research on the relationship between memory retention and the frequency at which those memories are rehearsed. They also drew inspiration from "Moonwalking with Einstein," a 2011 bestseller in which author Joshua Foer recounts his experiences in the world of competitive memorization. In particular, they borrowed the concept of the Person-Action-Object, or PAO, System, in which long sequences of numbers or letters are memorized by associating them with images.

In their scheme, a user initially selects a photo of a person and a photo of an evocative scene; the computer then randomly selects a photo of an object and a photo of an action. With those photos, the user then creates a PAO story that is as vivid and unusual as possible. For instance, photos of President Bill Clinton, a piranha and someone kissing might result in a story, "Bill Clinton kissing a piranha," or "President smooches a fish." By taking the first letter from each word, or the first three letters from the first two words, the user could generate part of a password.

For each account, the application would randomly assign several such photo combinations and the user would create a password using the letters associated with each photo. During subsequent logons, the application would provide the photos as a memory prompt; even if the user forgets the password, he can reconstruct the password by looking at the photos and recalling the associated story.

Though the photos could be public and unprotected, the exact stories associated with each and the ways they are translated into passwords would be known only to the user. Datta said even if an attacker

discovered one complete password, it wouldn't compromise any other passwords.

The application would keep track of the time intervals between uses of each photo/story pair. Blocki said cognitive research suggests that as memories are created, a person may initially need to rehearse the story every day or two; over time, the intervals can grow much longer. If a person didn't see a photo compilation and rehearse the associated story within the appropriate interval, the application would prompt the person to rehearse it. Over time, however, as the memory becomes consolidated, normal password use likely will give users all of the rehearsal time necessary, he added. Blocki said users might have as few as nine photo/story pairs, though he personally has opted to use 43 stories to maintain greater security.

"The most annoying thing about using the system isn't remembering the stories, but the password restrictions of some sites," said Blocki, who noted that some sites, for instance, require use of numbers, figures or capital letters in passwords, or have maximum character counts.

"In those cases, I just make a note to, for instance, add a '1' to the password," he said. Writing down password information normally is a bad practice, but Blocki said these notes aren't a problem with naturally rehearsing passwords. "The security is inherent in the [passwords](#) themselves," he explained, "and the notes don't affect that." This research was supported by the National Science Foundation and the Air Force Office of Scientific Research.

More information: www.iacr.org/conferences/asiacrypt2013/

Provided by Carnegie Mellon University