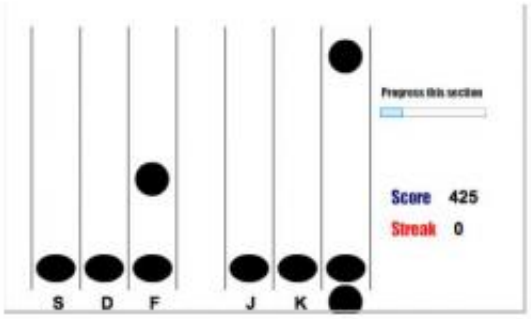
Neuroscience joins cryptography

July 19 2012, by Nancy Owano



Screenshot of the e Serial Interception Sequence Learning task in progress. Credit: Hristo Bojinov, Neuroscience Meets Cryptography: Designing Crypto Primitives Secure Against Rubber Hose Attacks, 21st USENIX Security Symposium.

(Phys.org) -- Security experts are turning to cognitive psychology for fresh ideas on authentication. Hristo Bojinov of Stanford University and others on his team have a new authentication design based on the concept of implicit learning. Implicit learning refers to learning patterns without any conscious knowledge of the learned pattern. An example of this is riding a bicycle. One knows how to ride a bicycle, but cannot explain how. The technique involves, through a crafted computer game, delivering a secret password in the user's brain without the user consciously knowing what the password is.

This, as the authors point out, represents a turning point in how security experts might treat authentication. Traditionally, it has been about either

who you are (biometrics), what you know (passwords) or what you have (tokens).

The newly added twist, as the research takes on further development, will also work at authentication based on what you really know but do not know. The research team suggests its authentication category as "a subclass of behavioral biometric measurement."

Bojinov sees the application in high-risk scenarios when the code-holder needs to be physically present, such as to gain access to a nuclear or military facility. "Now, suppose a clever attacker captures an authenticated user. The attacker can steal the user's hardware token, fake the user's biometrics, and coerce the victim into revealing his or her secret key. At this point the attacker can impersonate the victim and defeat the expensive authentication system deployed at the facility," the authors said.

The paper, which they intend to present next month at the 21st USENIX Security Symposium in Bellevue, Washington, is called "Designing Crypto Primitives Secure Against Rubber Hose Attacks." The authors are Hristo Bojinov, Daniel Sanchez, Paul Reber, Dan Boneh, and Patrick Lincoln. The team further explained what they mean by rubber hose attacks: "Cryptographic systems often rely on the secrecy of cryptographic keys given to users. Many schemes, however, cannot resist coercion attacks where the user is forcibly asked by an attacker to reveal the key. These attacks, known as rubber hose cryptanalysis, are often the easiest way to defeat cryptography. We present a defense against coercion attacks using the concept of implicit learning from cognitive psychology."

Bojinov and colleagues designed a game lasting 30 to 45 minutes in which players intercept falling objects by pressing a key. The objects appear in one of six positions, each corresponding to a different key.

Positions of objects were not always random. a hidden sequence of 30 successive positions was repeated over 100 times. Players made fewer errors when they encountered this sequence on successive rounds. This learning persisted when the players were tested two weeks later.

“We performed a number of user studies using Amazon’s Mechanical Turk to verify that participants can successfully re-authenticate over time and that they are unable to reconstruct or even recognize short fragments of the planted secret.”

If another person were to try to discover the sequence by forcing the password holder to play a similar game and watching to see when they make fewer errors, chances would be slim. The sequence consists of 30 key presses in six different positions. Testing 100 users nonstop for a year would result in less than a 1 in 60,000 chance of extracting the sequence.

So far, results of their research indicate the game could form the basis of a security system of this nature. Users would learn a sequence unique to them in an initial session and later prove that they know it by playing the same game. Nonetheless, the authors acknowledge that much work remains before the system can be deployed in a user-friendly state. The team hopes to further analyze the rate at which implicitly learned passwords are forgotten, and the required frequency of refresher sessions.

More information:
via Newscientist

https://phys.org/news/2012-07-neuroscience-cryptography.html