Carnegie Mellon Researchers Use Inkblots to Improve Security of Online Passwords

Byron Spice, Carnegie Mellon University

GOTCHA scheme could foil growing problem of automated brute force attacks.

Pittsburgh—Carnegie Mellon University [1] computer scientists have developed a new password system that incorporates inkblots to provide an extra measure of protection when, as so often occurs, lists of passwords get stolen from websites.

View: Inkblots Add Security to Passwords [2]

This new type of password, dubbed a GOTCHA (Generating panOptic Turing Tests to Tell Computers and Humans Apart), would be suitable for protecting high-value accounts, such as bank accounts, medical records and other sensitive information.

To create a GOTCHA, a user chooses a password and a computer then generates several random, multi-colored inkblots. The user describes each inkblot with a text phrase. These phrases are then stored in a random order along with the password.

When the user returns to the site and signs in with the password, the inkblots are displayed again along with the list of descriptive phrases; the user then matches each phrase with the appropriate inkblot.

"These are puzzles that are easy for a human to solve, but hard for a computer to solve, even if it has the random bits used to generate the puzzle," said Jeremiah Blocki, a Ph.D. student in computer science who developed GOTCHAs along with Manuel Blum, professor of computer science, and Anupam Datta, associate professor of computer science and electrical and computer engineering.

These puzzles would prove significant when security breaches of websites result in the loss of millions of user passwords — a common occurrence that has plagued such companies as LinkedIn, Sony and Gawker. These passwords are stored as cryptographic hash functions, in which passwords of any length are converted into strings of bits of uniform length. A thief can't readily decipher these hashes, but can mount what's called an automated offline dictionary attack. Computers today can evaluate as many as 250 million possible hash values every second, Blocki noted.

Given the continued popularity of easy passwords, such as "123456" or "password," it's not always difficult to crack these hashes. But even hard passwords are vulnerable to the latest brute force methods, Blocki said.

In the case of a GOTCHA, however, a computer program alone wouldn't be enough to break into an account.

"To crack the user's password offline, the adversary must simultaneously guess the user's password and the answer to the corresponding puzzle," Datta said. "A computer can't do that alone. And if the computer must constantly interact with a human to solve the puzzle, it no longer can bring its brute force to bear to crack hashes."

The researchers described GOTCHAs at the Association for Computing Machinery's Workshop on Artificial Intelligence and Security in Berlin, Germany, Nov. 4.

Because the user's descriptive phrases for inkblots are stored, users don't have to memorize their descriptions, but have to be able to pick them out from a list. To see if people could do this reliably, the researchers performed a user study with 70 people hired through Mechanical Turk. First, each user was asked to describe 10 inkblots with creative titles, such as "evil clown" or "lady with poofy dress." Ten days later, they were asked to match those titles with the inkblots. Of the 58 participants who participated in the second round of testing, one-third correctly matched all of the inkblots and more than two-thirds got half right.

Blocki said the design of the user study, including financial incentives that were too low, might account for the less-than-stellar performance. But he said there also are ways to make descriptions more memorable. One way would be to use more elaborate stories, such as "a happy guy on the ground protecting himself from ticklers."

The researchers also have invited fellow security researchers to apply artificial intelligence techniques to try to attack the GOTCHA password scheme. Their GOTCHA Challenge is online at http://www.cs.cmu.edu/~jblocki/GOTCHA-Challenge.html
GOTCHAs sound much like CAPTCHAs, the scrambled-letter puzzles that Blum and his CMU colleagues created to protect websites from rogue automated programs. Like GOTCHAs, the widely used CAPTCHAs rely on people having visual skills that are superior to those of computers. But the researchers emphasized that GOTCHAs don't do the same task and are not an alternative to CAPTCHAs. This research was supported by the National Science Foundation and the Air Force Office of Scientific Research. Follow the School of Computer Science on Twitter @SCSatCMU.

For more information visit http://www.cmu.edu [1].

Source URL (retrieved on *04/16/2014 - 8:06pm*):
http://www.wirelessdesignmag.com/news/2013/11/carnegie-mellon-researchers-use-inkblots-improve-security-online-passwords?qt-digital_editions=0

Links:
[1] http://www.cmu.edu
[2] http://www.wirelessdesignmag.com/news/2013/11/photo-day-inkblots-add-security-passwords