Improved passphrases could make online experiences both user-friendly and secure

August 3 2018

Although passphrases, or phrase-based passwords, have been found to be more secure than traditional passwords, human factors issues such as typographical errors and memorability have slowed their wider adoption. Kevin Juang and Joel Greenstein, in their recently published *Human Factors* article, "Integrating Visual Mnemonics and Input Feedback With Passphrases to Improve the Usability and Security of Digital Authentication," developed and tested two new passphrase systems that seek to address these shortcomings and improve the usability and security of existing passphrase authentication systems.

The authors" first passphrase system incorporated, in part, a specialized wordlist using simple, common words; a six-word sentence structure that made meaningful sense; and a user-created mnemonic picture to assist with recall. The final result would be a passphrase such as "silly pet wolf ate our pizzas," with an accompanying user-generated illustration. The second passphrase system replaced the six-word sentence structure with four words randomly drawn from a customized 1,450-word list.

Juang and Greenstein assessed the usability of their systems against two existing passphrase systems: a user-generated passphrase containing at least 24 characters, and a system-generated passphrase using words randomly drawn from a list of 10,000. To gauge the success of their new systems, the authors asked 50 adult participants to create, in five minutes, a passphrase and any applicable mnemonic—without writing down what they created. The participants completed two recall sessions, one immediately following the creation of the four passphrases and one

7 to 11 days later.

The authors found that memorability was greatly improved under their new systems compared with the existing ones: Second-session recall success rates in this study were 82% for the six-word sentence and 80% for the customized word list, versus only 50% for the user-generated passphrase and 34% for the passphrase created using the 10,000-word list. Given that study participants were instructed not to write down or practice their passphrases, Juang and Greenstein note that in real-world settings, the success rates for their new systems would likely increase.

Juang, a user experience research manager at SunTrust Bank, says, "Passphrases are more secure than passwords and avoid the various issues with biometric systems like fingerprint or facial recognition. It's inevitable that we will eventually need to move past traditional passwords, but it's nothing to fear. Instead of asking users to juggle both usability and security, which is complicated, let's provide secure passphrases and allow users to do what they do best: make things easier for themselves. By truly understanding how users think, we can design systems that keep them secure while also being easy to use."

More information: Kevin Juang et al, Integrating Visual Mnemonics and Input Feedback With Passphrases to Improve the Usability and Security of Digital Authentication, *Human Factors: The Journal of the Human Factors and Ergonomics Society* (2018). DOI: 10.1177/0018720818767683

Provided by Human Factors and Ergonomics Society

online-user-friendly.html