Users' perceptions of password security do not always match reality

23 May 2016, by Daniel Tkacik

Credit: Carnegie Mellon University Electrical and Computer Engineering

Think your password is secure? You may need to think again. People's perceptions of password strength may not always match reality, according to a recent study by CyLab, Carnegie Mellon's Security and Privacy Institute.

For example, study participants expected *ieatkale88* to be roughly as secure as *iloveyou88;* one said "both are a combination of dictionary words and are appended by numbers." However, when researchers used a model to predict the number of guesses an attacker would need to crack each password, *ieatkale88* would require four billion times more guesses to crack because the string "iloveyou" is one of the most common in passwords.

"Although participants generally had a good understanding on what makes passwords stronger or weaker, they also had some critical misunderstandings of how passwords are attacked and assumed incorrectly that their passwords need to withstand only a small number of guesses," said Blase Ur, the study's lead author and a Ph.D. student studying societal computing in Carnegie Mellon's School of Computer Science.

Participants, on average, also believed any password with numbers and symbols was a strong password, which is not always true. For example, *p@ssw0rd* was thought to be more secure than *pAsswOrd*, but the researchers' attacker model predicted that it would take 4,000 times more guesses to crack *pAsswOrd* than *p@ssw0rd*. In modern day password-cracking tools, replacing letters with numbers or symbols is predictable.

"In order to help guide users to make stronger passwords, it is important for us to understand their perceptions and misperceptions so we know where interventions are needed," said Lujo Bauer, a co-author on the study and a professor in Carnegie Mellon's Department of Electrical and Computer Engineering and Institute for Software Research.

The CyLab researchers' study was presented and awarded an honorable mention at this week's Association for Computing Machinery (ACM) Conference on Human Factors in Computing Systems in San Jose, California.

The team of researchers, based in the CyLab Usable Privacy and Security (CUPS) Lab, asked 165 online participants—51% male, 49% female from 33 U.S. states ranging from 18 to 66 years of age—to rate the comparative security and memorability of 25 carefully juxtaposed password pairs. In addition, participants were asked to articulate how they would expect attackers to try to guess their passwords.

"As companies are designing tools that help people make passwords, they should not only be giving users real-time feedback on the strength of their passwords, but also be providing data-driven feedback on how to make them stronger," Ur said.

The team will incorporate these findings into an open-source password feedback tool, which they aim to release before the end of the year.

Other authors of the study included Research Assistant Sean Segreti, Institute for Software Research and Engineering and Public Policy professor Lorrie Cranor, Electrical and Computer Engineering Assistant Research Professor Nicolas Christin and Penn State undergraduate engineering student Jonathan Bees.

Test your perceptions of password security through an online passwords quiz, produced by *Nature.*

Provided by Carnegie Mellon University Electrical and Computer Engineering