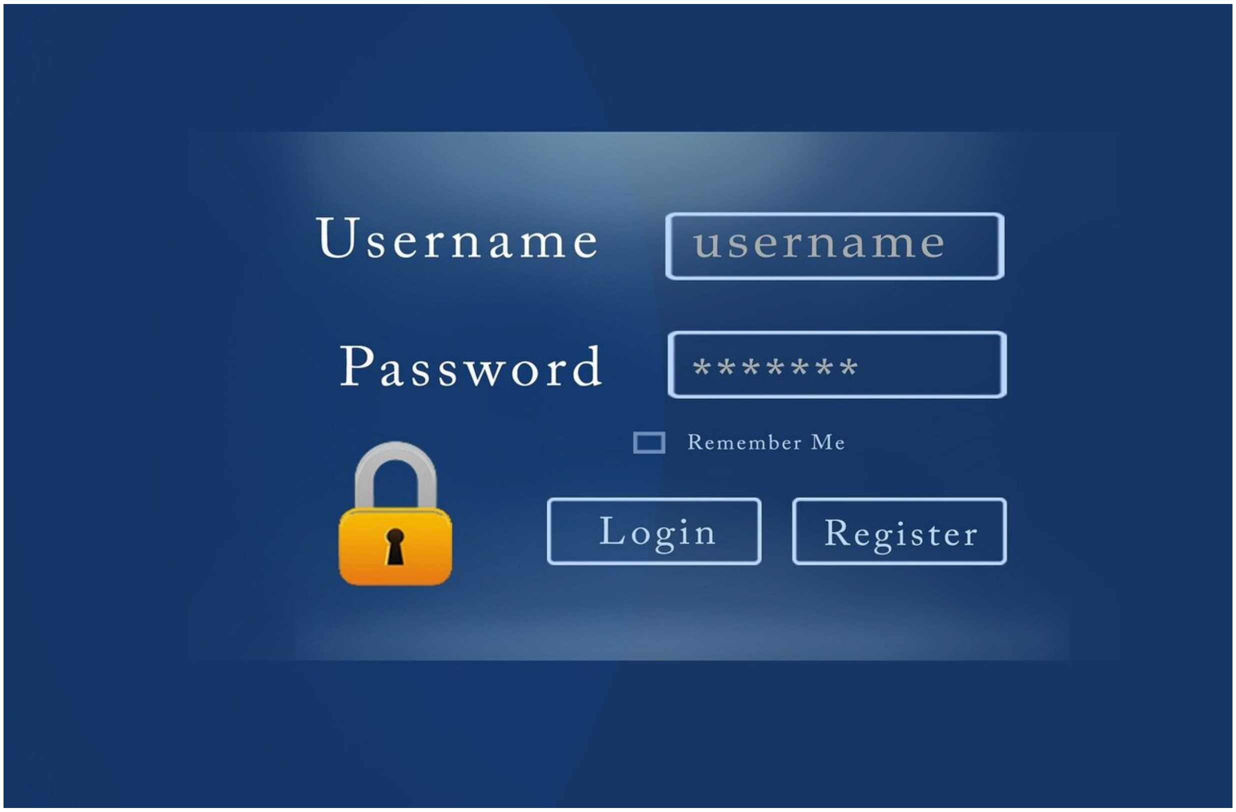
TechXplore

Finally: a usable and secure password policy backed by science

October 21 2020, by Daniel Tkacik



Credit: CC0 Public Domain

After nearly a decade of studies, the passwords research group in Carnegie Mellon's CyLab Security and Privacy Institute has developed a policy for creating passwords that maintains balance between security and usability—one backed by hard science.

Forget all the rules about uppercase and lowercase letters, numbers and symbols; your password just needs to be at least 12 characters, and it needs to pass a real-time strength test developed by the researchers.

The study will be presented at next month's ACM Conference on Computer and Communications Security, which will be held virtually.

"The policy we developed allows users to create passwords that are both easier to remember and more secure against sophisticated attackers," says Lorrie Cranor, director of CyLab and a professor in the Institute for Software Research (ISR) and the department of Engineering and Public Policy (EPP). "Interestingly, our data show that requiring more character classes—uppercase letters, symbols, and digits—doesn't increase password strength as much as other requirements and it tends to have negative impacts on password usability."

In 2016, the researchers developed a password-strength meter powered by an artificial neural network that was relatively small in size—a few hundred kilobytes, which is small enough to encode into a web browser. The strength meter gave users a strength score and offered suggestions in real-time. View a demo of the meter.

"It was kind of a game changer," says Lujo Bauer, a professor in electrical and computer engineering (ECE) and ISR, "… because no other password meters until then offered accurate, data-driven, real-time feedback on how to make the passwords stronger."

Equipped with this state-of-the-art password meter, the researchers then approached password policies from a whole new perspective: with the idea that a password must achieve a certain threshold score on their password meter. This new perspective led the researchers to discover a threshold between password strength and length—one that causes users to create passwords that are both stronger and more usable than they would under common password policies.

To reach this discovery, the researchers conducted online experiments, evaluating combinations of minimum-length requirements, character-class requirements, minimum-strength requirements, and password blocklists—lists of words that shouldn't be allowed to be used in passwords due to their common use.

In the online experiments, study participants were asked to create and recall passwords under randomly assigned password policies. First, participants assumed the role of someone whose email provider had been breached and needed to create a new password according to their assigned policy. Then, a few days later, they were asked to recall their password as a way to measure the usability of the password policy.

"We found that a policy requiring *both* a minimum strength and a minimum length of 12 characters achieved a good balance between security and usability," says Nicolas Christin, a professor in ISR and EPP.

Although blocklist and minimum-strength policies can produce similar results, minimum-strength policies are flexibly configured to a desired security level, and they are easier to deploy alongside real-time requirements feedback in high-security settings.

"Now that we are providing concrete guidance on password policies, we're optimistic that companies and organizations may adopt our recommendations," says Joshua Tan, a postdoctoral researcher in ISR and CyLab.

More information: ACM Conference on Computer and Communications Security, www.andrew.cmu.edu/user/nicola … ations/Tan-CCS20.pdf

Provided by Carnegie Mellon University

Citation: Finally: a usable and secure password policy backed by science (2020, October 21) retrieved 2 May 2024 from https://techxplore.com/news/2020-10-usable-password-policy-science.html