

RISK ASSESSMENT / SECURITY & HACKTIVISM

Password complexity rules more annoying, less effective than lengthy ones

Symbol, number, and cap requirements: do not want. Might not need.

by Casey Johnston - Jun 28, 2013 3:25 pm UTC

HARDENING

Few Internet frustrations are so familiar as the [password restriction](#). After creating a few (dozen) logins for all our Web presences, the use of symbols, mixed cases, and numbers seems less like a security measure and more like a torture device when it comes to remembering a complex password on a little-used site. But at least that variety of characters keeps you safe, right? As it turns out, there is some contrary research that supports both how frustrating these restrictions are and suggests it's possible that the positive effect of complexity rules on security may not be as great as long length requirements.

Let's preface this with a reminder: the conventional wisdom is that complexity trumps length every time, and this notion is overwhelmingly true. Every security expert will tell you that "Supercalifragilistic" is less secure than "gj7B!!!bhrdc." Few password creation schemes will render any password uncrackable, but in general, length does less to guard against crackability than complexity.

A password is not immune from cracking simply by virtue of being long—44,991 passwords recovered from a dump of LinkedIn hashes last year were 16 characters or more. The research we describe below refers specifically to the effects of restrictions placed by administrators on password construction on their crackability. By no means does it suggest that a long password is, by default, more secure than a complex one.

In April, Ars [checked in with a few companies](#) that place a range of restrictions on how passwords must be constructed, from Charles Schwab's 8-character maximum to Evernote's "use any character but spaces." Reasons ranged from whether customers can stand typing certain characters with a mobile phone to password-cracking being the last of a company's concerns compared to phishing or malware.

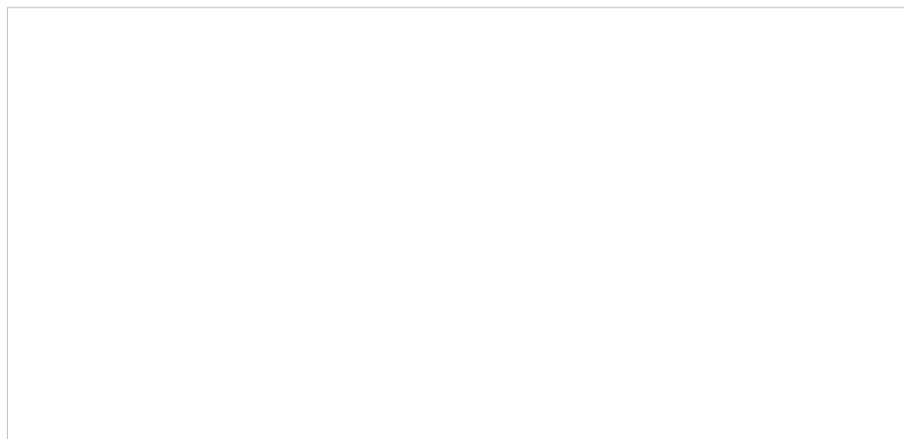
A pair of studies done in 2011 and 2012 on password length and construction showed two things: first, customer frustration increases significantly with complexity, but less so with length. Second, a number of password cracking algorithms can be more easily thwarted by a long password that is created without number, symbol, or case requirements than are shorter passwords that are required to be complex, particularly for a large number of guesses. That is, shorter, more complex password restrictions beget passwords that can be more frustrating to everyone except the only entity who shouldn't have it: the password cracker.

The [first study in 2011](#) specifically addressed the problems of usability in password complexity (full disclosure: both studies mentioned in this article were conducted in part by Michelle L. Mazurek, wife of Ars Gaming Editor Kyle Orland). The study authors looked at 12,000 passwords created by participants under a variety of construction methods, including comprehensive8, where passwords must be at least 8 characters and include both an uppercase and lowercase letter, as well as a digit and a symbol, and must not contain dictionary words; basic8, where passwords must be 8 characters with no other restrictions; and basic16, where passwords must be 16 characters with no other restrictions.

Study participants experienced the most difficulty with the comprehensive8 requirements from beginning to end. Only 17.7 percent were able to create a password that met all of the requirements in the first try, compared to well over 50 percent for the rest of the conditions. Twenty-five percent of comprehensive8 testers gave up before they could even make a password that satisfied the requirements, compared to 18.3 percent or less for other conditions. Over 50 percent of comprehensive8 participants stored their password either on paper or electronically, compared to 33 percent for those with the 16-character minimum and less for the rest of the conditions.

Despite the fact that passwords that impose a lot of requirements on content are harder to make and harder to remember, their use could be justified if they proved to be significantly more secure than, say, basic8 or basic 16. But contrary to password creation advice external to site-based creation rules, that did not seem to be the case.

Using 12,000 passwords sourced from Mechanical Turk participants, the researchers applied two cracking algorithms to see which types tended to stand up best to attacks. One was based on a Markov model that makes guesses based on character frequency, and the other was developed by another team of researchers and takes “training data” from password and dictionary word lists and then applies mangling rules to the text to form guesses.



[Enlarge](#) / The percent of passwords cracked vs. the number of guesses, using the second, more robust cracking method.

Carnegie Mellon University

Per the researchers’ tests, the basic 16-character passwords were the hardest to crack for a “powerful attacker.” After 10 billion guesses, only around 12 percent of the 16-character passwords had been cracked, compared to 22 percent of the comprehensive8 passwords and almost 60 percent of the basic8 passwords.

It's worth noting that the cracking algorithms used in this experiment differ from those Ars detailed in its story on real-world password crackers: one algorithm is a modified mask attack, while the other is based on the publicly available Weir algorithm. In either case, the results of using these cracking methods may differ from those used by real-world password crackers.

While the study casts doubt on whether complex and short password requirements result in passwords that are more secure than ones that just require length, it did find an interesting effect from the password restrictions. When the researchers compared passwords created under basic8 restrictions that happened to meet comprehensive8 restrictions to passwords actually created under comprehensive8 restrictions, the latter were significantly harder to guess.

Mazurek suggests two reasons to Ars for apparent resilience of passwords created under long-length restrictions versus short-and-complex ones. One is that there may not be enough good guessing data for long passwords due to the dearth of long-password requirements, which she said is true for both her own team and crackers in the wild. "It won't remain true long-term if people start requiring (and using) long passwords everywhere," Mazurek told Ars in an e-mail. The second reason is that "the space of possible passwords is just bigger... so relatively common long passwords are still less common than relatively common short passwords."

Between the two studies, it's less clear why those in charge of setting password rules should ever lower length restrictions while raising complexity restrictions. If those people are interested both in more security and less frustration for users, the better solution seems to be setting a higher character limit and leaving all of the other restrictions out.

But from our brief survey of sites, 16 characters seems to be the maximum more often than the minimum, and complexity rules abound. Ironically, Microsoft, which sponsored both of these studies in part, sets its own maximum at 16 characters. If admins are interested in a more secure restriction, a (long) flat length requirement could go further than one that allows short passwords but requires complications.

Further reading

- [How I became a password cracker](#)
- [Anatomy of a hack: How crackers ransack passwords like “qeadzcrwsfxv1331”](#)
- [Why your password can't have symbols—or be longer than 16 characters](#)
- [It's official: Password strength meters aren't security theater](#)

Listing image by [Reid Rosenberg](#)



Casey Johnston / Casey Johnston is an Associate Writer for Ars Technica covering gadgets, privacy, and tech culture. She graduated from Columbia University with a degree in Applied Physics.



@caseyjohnston

© 2013 Condé Nast. All rights reserved

Use of this Site constitutes acceptance of our [User Agreement](#) (effective 3/21/12) and [Privacy Policy](#) (effective 3/21/12)

[Your California Privacy Rights](#)

The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.