Why are password rules so annoying?

John MacCormick, October 2015

Try to think back to a time that you created or updated a password for some online service or account. [For me: think of creating MTB account.] How many people reused an existing password? How many people failed on the first attempt (i.e. the password was rejected because it was too short or didn't contain symbols or something like that)? How many failed on the second attempt? The third attempt? How many people wrote down the password on paper? How many recorded it electronically? [2m]

What can we conclude from these results? 1. People often reuse passwords and/or record them, even if they're asked not to. 2. It's hard to choose passwords that conform to specific password policies. More generally, we can infer that password systems are often hard to use and frustrating -- sometimes even infuriating.

Why? Firstly, why do we need passwords at all? [Ask audience.] I think the answer is obvious: we need some way of stopping strangers and/or criminals from accessing our bank accounts and reading our email. There do exist other technologies for authenticating people (think fingerprints, eye scanners etc.), but none is fool-proof and none can be deployed as easily as passwords. Therefore, in this talk I will assume we are stuck with using textual passwords. [3m]

So let's ask the main question again: why are textual password systems frustrating? [Ask audience.] The high-level answer is that passwords can only stop criminals if they are hard to guess. But a password that is hard to guess is hard to remember. So at the heart of all password problems lies this trade-off: somehow we want to increase ease-of-remembering without increasing ease-of-guessing.

Back to a more specific version of the original question about why password systems are frustrating. Why do some organizations have specific rules such as requiring digits or symbols in a password? [Ask audience.] Because, compared to passwords that people usually choose, passwords with digits or symbols are harder to guess. [4m]

The math here is actually very simple. When a criminal is trying to guess your password, they usually use a technique that security researchers call "brute force". This just means that the criminals guess different possible passwords until they get it right. The total number of passwords they have to guess is therefore a good measure of how long it will take them to crack your password. For example, let's suppose you're using a system that enforces no password rules whatsoever, and you plan to use an English word as your password. The bad news is that you actually don't know that many words – at most, probably about 10,000 of them. So the criminal needs to only make 10,000 guesses, which on a modern computer (and subject to certain technical assumptions that won't be discussed here) might take only 10 seconds. BUT if the password system requires you to use two digits, how long will it take the cracker now? [Ask audience.] Well, there are 100 combinations of two digits, so it's going to be at least 100 times longer, which is 1000 seconds or about 20 minutes. Adding a symbol creates even more combinations, as does a requirement for upper case letters. And another common requirement is to disallow dictionary words. If you do the math carefully, then it turns out these extra rules (no dictionary words, must contain uppercase, lowercase, symbol, and number) increases the difficulty of guessing an

eight character password by a factor of about 4 thousand (NIST 2013, p109). *That* is why many organizations use these rules. [7m] For an even more concrete demonstration of this, we can look at a 2011 study by a research group at Carnegie Mellon University (Komanduri 2011). They compared three different approaches to password rules: (a) allowing any eight character password; (b) disallowing dictionary words; (c) requiring digits, symbols and disallowing dictionary words. Real users created passwords with these rules, then they used a popular password guessing program to try and guess the passwords. They found that when users can choose their own 8-character password without any other restrictions, nearly 20% of them could be guessed. Adding the dictionary check brought this down to 3%, and requiring digits and symbols reduced the percentage to essentially zero.

So I guess that's the bad news. The rules are there to slow down criminals by a factor of 4 thousand, but they do create a headache for us, since the resulting passwords are hard to remember. What's the good news? There are actually several flavors of good news. [10m]

First piece of good news: not all organizations care very much about password security. For example, has anyone tried to sign up for Netflix recently? What is their password policy? [Ask audience.] Answer: password must be at least four characters long. ***No other requirements.*** [Actually, there is a maximum length too, but no need to mention that.] Why not? [Ask audience.] Because it really doesn't matter much. Netflix is much more interested in making their system friendly for customers and in deterring criminals. There's not much they can steal from your Netflix account anyway! The same goes for other low-stakes sites. [11m]

Second piece of good news: there is a more friendly way of forcing users to choose hard-to-guess passwords -- does anyone know what I'm talking about? [Ask audience.] Answer: password meters. As you type the password, a meter shows you how good your password is. This online feedback makes it much easier to quickly find a password that is acceptable to the system. Gmail, Facebook, and Citibank all use systems like this currently. It seems clear that password meters are a reasonable solution and it is reasonable to expect that many organizations will migrate to password meters over time. [12m] Based on a very small informal survey, it seems that organizations still enforcing a complex suite of password requirements without a feedback meter mostly include organizations that need to be conservative for legal reasons (e.g. financial institutions) and organizations that don't face direct competition (e.g. corporate systems for employees, university systems for students). [13m]

Third piece of good news: password policies and interfaces are areas of active research, and computer scientists are testing and assessing new ideas all the time. Many of the interesting papers are published in a conference called CHI (ACM Conference on Human Factors in Computing Systems). For example, in CHI 2015, a group from Carnegie Mellon published a paper called "A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior" (Shay et al., 2015). In a study of over 6000 participants, they concluded that password meters and other real-time guidance can help to increase usability or strength of passwords (though not necessarily both at the same time). The same group 2 years earlier demonstrated that password meters help to improve the strength of passwords for

accounts that users consider important, but not for unimportant accounts (Egelman et al 2013). If we have time, or during the questions, I can tell you about some other recent research on password security.

But maybe that's a good time to wrap up and go into a question-and-answer session. To summarize: those annoying rules about uppercase letters and symbols slow down the bad guys by a factor of about 4 thousand, reducing the percentage of guessable passwords from around 20% to near 0%. But those same rules make it hard for us to even choose a legal password, let alone remember it. Online password meters and real-time feedback are helping to alleviate that problem. [18m]

Appendix: CHI 2015 password session paper titles:

- Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues
- ActivPass: Your Daily Activity is Your Password
- Constructing Secure Audio CAPTCHAs by Exploiting Differences between Humans and Machines
- Easy to Draw, but Hard to Trace? On of the Observability of Grid-based (Un)lock Patterns
- On the Effectiveness of Pattern Lock Strength Meters – Measuring the Strength of Real World Pattern Locks

Bibliography

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., & Herley, C. (2013, April). Does my password go up to eleven?: the impact of password meters on password selection. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2379-2388). ACM.

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., ... & Egelman, S. (2011, May). Of passwords and people: measuring the effect of password-composition policies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2595-2604). ACM.

NIST 2013. Burr et al., Electronic Authentication Guideline, http://dx.doi.org/10.6028/NIST.SP.800-63-2.

Shay, R., Bauer, L., Christin, N., Cranor, L. F., Forget, A., Komanduri, S., ... & Ur, B. (2015, April). A spoonful of sugar? The impact of guidance and feedback on password-creation behavior. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 2903-2912). ACM.