Creating really strong passwords

Paulo Fioravante, IT Director for SHMP and VDL

Key Points

- Computer processing power keeps increasing at an alarming rate, allowing hackers to greatly increase their password cracking capabilities.
- Hackers' password cracking tools are getting more sophisticated and can crack weak passwords in no more than a couple of hours of execution. The same tools will take millions of years to crack a strong password.
- Whenever password cracking is mentioned in this article, it should be assumed that the password is encrypted using a strong cryptographic hash algorithm such as scrypt: http://www.tarsnap.com/scrypt.html

---

Creating strong passwords yourself

When you create a password yourself, it must have the following characteristics:

1) Length

Longer passwords provide a greater combination of characters consequently making it more difficult for an attacker to guess the password. According to the National Institute of Standards and Technology (NIST), passwords shorter than 10 characters are weak.

2) Complexity

A common recommendation is that passwords include at least 3 of the following 4 complexity rules:

- 1 uppercase character (A-Z)
- 1 lowercase character (a-z)
- 1 digit (0-9)
- 1 special character (e.g., ~ ! @ # $ % ^ & ( ) _ + =), including spaces

Unfortunately, those rules are not enough to make passwords strong enough. It turns out that users have very predictable behavior when choosing passwords, and hackers take advantage of that. For instance:

- P4ssword13!
- N0vember24@
- P4triots99#

All these passwords have the same pattern: Uppercase, 1 number, 6 lowercase, 2 numbers, 1 special character, not to mention the very predictable pattern of replacing A for 4, O for 0, and E for 3. Patterns like these can dramatically reduce the time it takes to crack an encrypted password.

Rick Redman, a Security Consultant specialized in penetration testing at KoreLogic Security, analyzed the distribution of password patterns in a Fortune 100 company database. Using a $2000 machine, he was able to crack 99% of the encrypted passwords in that company's database in a couple of hours. He found the following password patterns:

Consider: *u = upper case character, l = lower case character, d = digit*

- 33,458: ullllldd (8 character) – 12.7%
- 33,394: ullllldd (9 character) – 12.7%
- 27,898: ulldddd – 10.6%
- 19,190: ullllllldd – 7.3%
- 13,204: ullldddd – 5.0%

The top 5 password patterns were used by 48% of all users. The top 100 password patterns were used by 85% of all users. 99.9% of passwords met their complexity requirements.

Therefore, when creating a strong password, it is important to avoid those predictable patterns. The 100 most common password patterns are available at: https://blog.korelogic.com/blog/2014/04/04/pathwell_topologies

3) Uniqueness per account

It is important not to recycle password variations for different needs. If one account is breached, repeated passwords allow easy access to your other accounts, no matter how strong that password is.

Creating strong passwords using password generating tools

Diceware

Diceware is a method for creating passphrases using ordinary dice as a random number generator. For each word in the passphrase, five rolls of the dice are required. The numbers from 1 to 6 that come up in the rolls are assembled as a five-digit number, e.g. 43146. That number is then used to look up a word in a word list. For example, in the English vocabulary, number 43146 corresponds to the word “munch”. By generating several words in sequence, a lengthy passphrase can be constructed. This technique may look silly, but because throwing a physical dice produces true randomness, the generated passphrase is actually very hard to crack.
You can generate Diceware passphrases at: https://www.rempe.us/diceware/#eff

LastPass Secure Password Generator

LastPass is a Password Manager which has an embedded secure password generator.

Summary

To create a really strong password, you can either use a password generating tool, such as Diceware or LastPass Password Generator, or you can create the password yourself, as long as your password is long, complex and you don’t reuse it for several accounts.

*Whenever password cracking is mentioned in this article, it should be assumed that the password is encrypted using a strong cryptogoraphic hash algorithm such as scrypt: http://www.tarsnap.com/scrypt.html

References

https://www.owasp.org/index.php/Authentication_Cheat_Sheet#Password_Length
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf
https://www.owasp.org/index.php/Authentication_Cheat_Sheet#Password_Complexity
https://www.korelogic.com/Resources/Presentations/bsidesavl_pathwell_2014-06.pdf
https://blog.korelogic.com/blog/2014/04/04/pathwell_topologies
https://en.wikipedia.org/wiki/Diceware
https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/
https://helpdesk.lastpass.com/generating-a-password/