SEPTEMBER 15, 2020

VPS Article

Why Password Length is More Important than Complexity

JOHN STREFF, IT SECURITY SPECIALIST

In today's digital world, we access sensitive information and systems frequently. Administrators protect sensitive systems from unauthorized access by implementing some form of authentication mechanism, which requires users to prove their identity before being granted access. There are three primary methods of authentication: something you know, something you have, and something you are. "Something you know" refers to a piece of information that only an authorized person would know, such as a password. "Something you have" refers to a unique token or code that only an authorized person would possess. An example of this would be an RSA SecurID token with a six-digit code that changes every 30 seconds and must be entered following a successful password entry. An example of a system using "something you are" would be a fingerprint reader. The most common form of authentication is a password (something you know), so we will consider password security today. Passwords provide an effective authentication mechanism, but they can be misused. Since a weak password is not much better than a blank password, taking the time to understand what makes a password secure will assist you in ensuring that all your passwords provide sufficient protection.

Passwords such as "dog," "cat," "password", and "computer" are inadequate because they are simple dictionary words. Attackers often use a "dictionary attack" to test each of thousands or millions of words from a word list at a login prompt in a matter of minutes. This allows an attacker to quickly discover a password that is a simple dictionary word.

When a dictionary attack fails, attackers may attempt a "brute force attack," in which every possible combination of characters, numbers, and symbols is tried sequentially. The attacker's password-cracking software starts with one-character passwords and gradually increases until the correct password is found. Knowing this, passwords such as "dog74," "$%ab18," and "123456" are still inadequate. Even though these are not dictionary words, they are very short. A computer can guess thousands of passwords per second. Some computers may even guess millions of passwords per second. This means that a computer will not require much time to try every combination of characters up to the correct password.

The best way to enhance a password's security is to increase its entropy. Entropy is a measure of the amount of randomness in a piece of data. In the context of passwords, entropy refers to the number of possible passwords that could be created with the given password's length. Suppose that we can use 26 different letters (both upper and lowercase), 10 digits, and 10 special characters in a password. This means that each character in a password

VANTAGEPNT.com 605-995-1777
2211 N Minnesota Street Mitchell SD 57301

can be one of 72 different characters. Let's round this to 70 for easier math. A two-character password could have 70 x 70 or 4,900 possible passwords. A three-character password could have 70 x 70 x 70 or 343,000 possible passwords. Notice how dramatically the number of possible combinations increases for each additional character. The current best practice is to use at least twelve characters, which results in approximately 13.84 sextillion possible passwords, which is not feasible to crack! To put this number into perspective, if using a three-character password is like driving 100 miles, then using a twelve-character password is like driving around the entire world 162 trillion times! From this information, we can conclude that a password's length / entropy provides its security.

When increasing a password's length, it is advisable to avoid passwords such as "dydf%#45Hywq1@." Such a password is nearly impossible to remember and prompts the user to write the password down on a sticky note and store it near his/her keyboard, thus defeating the password's purpose. A better approach is to use a passphrase, which is a chain of words. To add some additional complexity, a few digits or special characters may be added to the end. For example, "PenCarpetComputer115!" is an excellent passphrase because it is at least twelve characters long (highly entropic), is not a single dictionary word, contains both upper and lowercase letters, contains some numbers and special characters, and is not so complex that it is impossible to remember.

Once secure passphrases have been set, they should never be re-used for an additional login account. An attacker who discovers one passphrase will then be able to use it to log in to other accounts as well. Each login should have its own, unique passphrase. If the number of unique passphrases becomes so large that it is difficult to remember them all, password management software may be used. For more critical logins, it may be wise to enable multifactor authentication to add another layer of protection.

Passwords provide a powerful and effective authentication mechanism, but we must use them properly. Passwords that are too short or too simple are not safe to use and are not much better than a blank password in the face of a determined attacker. Organizations concerned that their network passwords may not be sufficiently strong may wish to consider a Password Audit. This audit can help an organization discover and change weak passwords as well as configure settings to prevent weak passwords from being set again. Vantage Point Solutions offers an affordable Password Audit and has assisted several clients with this process. Paying attention to password security will help ensure that your organization's sensitive systems and data receive the protection that their sensitivity requires.

Additional Information

For more information or if you would like VPS guidance, please contact the Vantage Point Solutions banking team:

Kelly Pfeifer at (605) 995-1796, Kelly.Pfeifer@vantagepnt.com

John Streff

IT SECURITY SPECIALIST

As both a meticulous security analyst and a dedicated educator, John Streff brings tremendous strength to the Vantage Point IT Security Team. In his role as IT Security Specialist, he helps banks and credit unions secure their data networks through penetration testing, vulnerability management, policy, and other measures. Beyond technical mastery, John is especially strong at helping communicate the risks of cybersecurity breaches; and combined with his gift for training, this helps companies secure the human side of the organization – protecting entire teams and businesses from individual errors. He specializes in social engineering, security awareness training and publication, and malware analysis.

"I AM PASSIONATE ABOUT SECURITY EDUCATION AND TRAINING BECAUSE THEY PROVIDE A CRITICAL LAYER OF PROTECTION FOR A CLIENT'S CYBERSECURITY BY ENSURING SECURE USER PRACTICES."

EDUCATION

Bachelor of Science in Cyber Operations from Dakota State University, a Master of Science in Cyber Defense, and an Ethical Hacking Graduate Certificate

Kelly Pfeifer

CUSTOMER RELATIONS MANAGER

Kelly Pfeifer assumes a primary role as the problem solver for all client needs. He is committed to helping financial institutions deal with regulatory, network and security issues. Not only does Kelly provide a professional and helpful line of communication for the client, he also participates in social engineering testing. He is a master of disguise and an accomplished dumpster diver. His role as customer service manager is a central part of the financial services division at Vantage Point Solutions. Kelly double majored in Elementary Education and Business Finance at Dakota Wesleyan University. He began his career at Wells Fargo where he was twice named their top performer. He enjoys helping with Special Olympics and Junior Achievement. Kelly is also a Division I men's college basketball referee.

"I'M PASSIONATE ABOUT DEVELOPING RELATIONSHIPS BECAUSE THAT'S HOW I GET TO KNOW THE CLIENTS' PRIORITIES."

EDUCATION

Elementary Education and Business Finance at Dakota Wesleyan University