

Password vs. Passphrase: Which is better?

Michael Sunderland, Security Analyst

So your company is using the latest patch management software. All of your workstations and servers have the most recent security patches and you keep them up to date. In addition, you have locked down the configurations for all systems, including network devices, on your network. But what about the passwords for the user accounts? Out of all the users on your network, chances are somebody is using a password that is easy to guess. What is worse, a user with administrative privileges may also be using a simple password, which puts the entire network at even more risk.

Passwords continue to be a source of weakness for networks and the bane of many network administrators and information security professionals. So what can you do to strengthen this critical area of network security? Many say that passwords are outdated and should be replaced with other forms of authentication. Bill Gates gave an address at a recent RSA Security conference calling for the end of passwords altogether. He envisions using more advanced authentication technology such as multifactor authentication that eliminates passwords as the sole means of securing systems. In fact, multifactor authentication will soon be a routine, everyday occurrence and certain regulatory bodies, including the Federal Financial Institutions Examination Council (FFIEC), are moving towards the requirement for multifactor authentication in the protection of sensitive data.

Even with the onset of multifactor authentication looming in the near future, much room for improvement exists in strengthening the user-created password. Passwords will remain one of the factors available for use in multifactor authentication. Complex passwords that require several types of characters (such as alpha with varying upper and lower case, numeric, and special characters) are ideal. Many times, however, the user community balks at complex passwords, claiming they are too hard to remember. This is a legitimate complaint and can lead to users writing down their passwords on sticky notes and putting them around their desk or under a keyboard, phone, etc. (if not already commonplace). This behavior exposes the company to increased risk of compromise, because anyone with physical access to the employee work areas could harvest these passwords and use them to gain unauthorized access to the network.

An age-old debate in the information security arena centers on using passphrases rather than passwords. If the authentication process of the operating system or application supports it, passphrases can be a valuable means to strengthen the security. Passphrases tend to be longer than passwords, but easier to remember because sentences can be used. Groups of words are easier to remember than a group of letters and numbers since words can bring images to mind. A passphrase such as "The snow capped mountain in the Rockies is a beautiful place!" allows the mind to picture the sentence, which helps to lock it into your memory.

Two problems arise out of passphrases, however. Applications may impose a limit on the maximum number of characters they will accept for password authentication. If the limit

is too small, then the application will not accept certain sentences since they will not fit within the bounds of the password field. Another problem is accuracy while typing. Increasing the number of characters makes it more difficult for a computer user to type in the full sentence without making typographical errors. If the user does not type the precise passphrase correctly, the application will refuse authentication. This can be especially frustrating for users. Their natural inclination will be to use fewer characters, which can lead back to the original problem of easy-to-guess passwords.

Another method that still utilizes sentences but reduces the number of characters to type is the use of mnemonics. If you take the passphrase used above and reduce it to just the first letter of each word, you would have “TscmitRiabp!”. Taken by itself, this group of characters would be very difficult to remember, however, if you make each of the characters represent something, you can simplify the memorization process. Additionally, by replacing characters within the mnemonic with numbers or special characters makes the password even stronger. Mnemonics utilize fewer characters than passphrases, making them easier to type accurately without making mistakes, while at the same time making passwords more complex.

You can also make passwords and passphrases stronger with high ASCII characters that you access by holding the key and typing three numbers above 128, but less than 255. Many brute force password-guessing utilities have a difficult time with these characters. Additionally, configuring password-cracking utilities to handle high ASCII characters within password hashes greatly increases the cracking time. However, problems arise with passwords using these characters as well. Often applications will not accept these characters. In addition, educating the user community about these characters could be a difficult task. Since one of the primary goals is to compel acceptance by the user community to make more secure passwords, educating them to use these ASCII characters may not be the best use of resources.

It is clear that multifactor authentication will likely become commonplace in the near future. Consequently, the use of passwords and passphrases will no longer be the sole authentication method for various information systems.. However, even with multifactor authentication, one of the factors used could still be a password or passphrase, which makes them an important part of the authentication process. Hence, passwords and passphrases should be made as complex as possible while remaining relatively straightforward for the user community to remember. As with other areas of information security, user education is a key component in accomplishing this goal. You can achieve stronger authentication by providing users with different methods to create better, stronger passwords that do not require a large amount of effort in their creation and memorization.