

Passphrases A Viable Alternative To Passwords?

<http://www.darkreading.com/authentication/167901072/security/news/232400013/passphrases-a-viable-alternative-to-passwords.html>

January 2012

By Ericka Chickowski

Some experts say yes, but technological and cultural issues bar the path to passphrases

Two-factor authentication may be a great way to bolster log-in processes across the enterprise and even on the Web, but when it comes down to it the typical authentication process using something someone knows--typically a password--isn't going anywhere any time soon. Nevertheless, some security professionals wonder if it is time that the industry at least take stock of the typical password. They think organizations should at least consider replacing these difficult-to-remember, difficult-to-secure jumble of alphanumeric characters with more memorable and secure passphrases.

Sure, passphrases are not as secure as a token or some other two-factor authentication method, but they're more secure than 12345 and much easier to remember than some strange concoction like b4x87g-m. While it may be tempting to blame end users for coming up with crummy passwords, Nick Selby, a Texas police officer and managing director of enterprise security consultancy TRM Partners, believes strongly that the problem is not because users are too dumb to absorb security training but because security practices put them in an impossible situation.

"What can't be trained is demanding that people use something which is impossible to remember. And then demanding that they remember that. And attendant with that is not writing it down. You can't remember it, and you can't write it down," Selby says. "Is that a user issue? I don't think so."

His argument is that passphrases, such as a sentence from a favorite book--are easier to remember and harder to crack than most passwords today, even without special characters. Many within the industry back him up on the matter.

"Pass phrases are a much better solution to shared secrets compared to simple one word passwords," says Phil Lieberman, president of Lieberman Software. "Making passphrases more secure than one word passwords is simple mathematics. The ability to reverse a single word password is simply a matter of the length of the password itself--hash lookups. By having the phrase go beyond 14 characters in length make hash lookups very expensive. Fundamentally there are very few long English single words that are memorable, but a phrase or sentence is easy to create and remember that goes beyond the 14 or so characters in length."

Abbas Haider Ali agrees, explaining that even without any special characters a long passphrase keeps brute force attacks at bay far better than a shorter mix of alphanumeric soup.

"I like to use <http://howsecureismypassword.net/> site as a litmus test of how secure a password is," says Ali, vice president and technology evangelist for xMatters, a relevance engine firm. "(According to the site), 'b4x87g-m' would take 2 days to crack. My random pass phrase of 'This password is easy to remember, and crazy to break!' would take 36 octovigintillion years to break."

So what's the hold up? Why aren't organizations using passphrases if they're more difficult to hack? According to Ali, a lot of the problem is the cultural view that shorter is easier to remember and that increasing complexity is better than increasing length, in spite of research that users can remember passphrases more easily and proof that it is harder to crack longer passphrases.

"That's where we continue to see that rules that force complexity instead of recognizing research that clearly shows that length would be better," Ali says. "I've seen capital letters, special characters, numbers, common word checking, 'leet' character replacement, et cetera. All futile and painful, to boot."

According to Selby, the reluctance to transition to passphrases is partially due to the security industry becoming a victim of its own success.

"For years talking heads have said that the key, the foundation, the bedrock to good security is a strong password. Mixed upper and lower case, at least 8 characters, including special characters and numbers that no one can remember and use," Selby says. "Great. So everybody believes it. Now what's the point in investing in passphrases?"

This attitude has manifested itself into technical limitations that are "reinforced over again since no one big tech company or provider has decisively broken ranks," Ali says.

There is a wish among some enterprise users that they could institute phrases, but they're experiencing a technology lag within the software and identity management worlds that stymies the urge

"One reason (organizations don't use passphrases) is the number of software applications that do not support long or complex passphrases," says J. Wolfgang Goerlich, Network Operations and Security Manager for a midwest financial services firm. "Length and special characters seem to be a challenge for some vendors. Sometimes referred to as technological debt, many IT departments must maintain a suite of apps that have not been updated with modern security recommendations."

That's not to say that there is no technology whatsoever that supports passphrases. It does exist, says Mike Geide of Zscaler ThreatLabZ, who points to Microsoft Active Directory's LDAP solution's support of 128-character passwords as an example.

"Application developers have to be encouraged to ensure their applications support this shift, users have to be educated on the benefits and senior leadership has to be made aware of the solutions that are currently available to make an effective transition from password to passphrase," Geide says.

It is not nearly a button-press transition, either.

"We are continually fighting tomorrows battles with yesterday's or yesteryears technology or technological approaches and philosophy," Selby says. "It just means you have to re-architect something to accommodate a passphrase and not a password. Try typing a space into half the things you sign up for on the internet and you break it."

Organizations need to change user interfaces if they want to make it easy for users to enter longer phrases that might be more prone to fat-finger mistakes, perhaps dropping some of the conventions of today's password entry interface.

"I know that the bullets or stars are there to prevent someone from shoulder-surfing your password, but they really make it hard to use passwords of more than about a dozen characters in length," says Andrew Brandt, director of Threat Research at Solera Networks Research Labs. "How on earth would anyone know, after typing a 50-60 character phrase that is obfuscated with bullets, where the typo is? I certainly don't want to have to type the opening monologue from Hamlet five times just to log back in after lunch. "

What's more, it isn't just technology that needs to change. So do password policies, says Nishant Kaushik, chief architect of Identropy. As he explains it good password policies often introduce requirements like use of mixed case, numbers and special characters.

"Incorporating these into a passphrase is actually quite hard for users and makes them quite unusable (because) it's difficult to remember the correct substitutions," he says. "Password policies are a necessary protection factor introduced by many applications/security tools to ensure higher complexity and therefore lower guessability (or) crackability when combined with lockout policies. We still haven't figured out a way to define password policies that are passphrase friendly."

However, it may be worth the extra effort. Marcus Carey, security researcher at Rapid7, agrees with Selby that organizations need to roll up their sleeves and start finding creative ways to tackle both the cultural and technological obstacles for passphrases.

"For a long time the security industry has told organizations that short complex passwords are better. It's hard to teach an old dog new tricks, and there are certainly those in the security industry that can't admit, 'Hey, what we've been telling you for years is actually not that effective.' Also, software such as identity management solutions would have to be re-written and updated to support longer text strings," he says. "I think we should think about alternatives to the user login interface. For example, a login interface where a user could enter a series of simple words which makes up a larger passphrase."