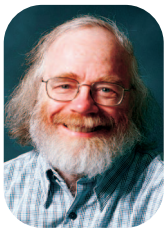
CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Columbia University Academic Commons

Unconventional Wisdom

We're told that passwords are evil, to change them frequently, and never to write them down. We're even told that if you work for most US corporations, frequent password changes are required by law. How much of this is true, and how much is mythology? Remarkably enough, the conventional wisdom might be wrong on all these points.



Steve Bellovin
Columbia University

I'm sure many of you are wondering how I can say that passwords might not be evil. After all, just a few years ago I wrote that "the easiest way to attack ... is user passwords" and "a better answer is to get rid of passwords entirely."[1] The answer is that passwords must be seen as part of a *system*; whether they're a risk depends on how they're used and what they're protecting. More precisely, the well-known weaknesses of passwords—that they can be guessed, stolen, shared, or written down—might not be the system's weak point. Alternatively, stronger authentication mechanisms might not be cost-effective with low-value resources.

This last point is most obvious with password-protected Web sites. If you forget your password, you can have it emailed to you, unencrypted. This is in no sense of the word "secure"; rather, it's *secure enough* for the resource being protected. That someone might guess or steal one of these passwords is irrelevant; to the site owner, the real issue is whether the actual resource being protected—the subscriber's demographic data—is accurate. The US Defense Department recognized this 20 years ago; its Password Management Guideline said

> [P]asswords should be protected in a manner that is consistent with the damage that would be caused by their compromise. Since passwords are no more sensitive than the data they provide access to, there is generally no reason to protect them, during transmission, to any greater degree (e.g., encryption) than regular data is protected.[2]

The more interesting question, though, is how to treat important passwords. One oft-cited defensive measure—changing your password frequently—is now being pushed as necessary for compliance with the Sarbanes-Oxley Act (www.careerjournal.com/myc/officelife/20041214-thurm.html). Is such behavior necessary? In most situations, it actually hurts security; as such, frequent mandatory password changes are probably harmful and hence *prohibited* by the act. (The act simply mandates "internal controls" to prevent fraud; it says nothing about passwords.)

The reason, again, is that security is a system property. Users have to remember too many passwords these days; if they're forced to change them too often, evasive behavior results. Password patterns—secret1, secret2, Secret1, Secret2, and so on—can't be detected unless cleartext of old passwords is stored (on yellow stickies or in plaintext files on insecure machines, for example). We'll see more recourse to insecure backup authentication schemes designed for password recovery or reset. (Many rely on such "secrets" as your social security number, which can be purchased for as little as US$35.[3]) And all of this information is much more accessible to those with the greatest motive to commit the sort of fraud that Sarbanes-Oxley was designed to prevent: your coworkers.

What is the right answer, then? The best answer is to use a more secure authentication scheme in the first place. If you must use passwords, make sure they're strong and memorable. Use single-sign-on techniques to avoid the "101 passwords" problem. And change your password occasionally—but not too often, or you'll drive yourself crazy. □

References

1. W. Cheswick, S. Bellovin, and A. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker*, 2nd ed., Addison-Wesley, 2003.
2. *Password Management Guideline*, US Department of Defense, CSC-STD-002-85, 1985.
3. J. Krim, "Net Aids Theft of Sensitive ID Data," *Washington Post*, 4 Apr. 2005; www.washingtonpost.com/wp-dyn/articles/A23686-2005Apr3.html.

Steve Bellovin *is a professor of computer science at Columbia University. His research interests are networks, security, and why the two don't get along. He helped create or usenet news, and is coauthor of* Firewalls and Internet Security: Repelling the Wily Hacker (Addison-Wesley, 2003). *Contact him via www.cs.columbia.edu/~smb.*