People are still the weakest link in computer and internet security, study finds

October 13 2009

Two decades ago, studies showed that computer users were violating best practices for setting up hack-proof passwords, and not much has changed since then. What's clear, say researchers at the University of Wisconsin-Madison and IT University in Copenhagen, is that until human factors/ergonomics methods are applied to the problem, it isn't likely to go away. They will present the results of their CIS study at the upcoming HFES 53rd Annual Meeting at the Grand Hyatt San Antonio in San Antonio, Texas on October 19.

The best software and hardware in the world can do only so much to safeguard data and protect security; it's up to users to follow best practices in creating passwords to authenticate their computer when logging in. For instance, the password should contain at least eight characters; people should not use the same password every time for every site; and unlike some of the 34,000 MySpace login IDs examined in 2006, their password should not be set as "password." But the more complicated — and therefore the more secure — the password, the harder it is to remember. In addition, the best practice recommendation to use multiple, difficult-to-remember passwords for different password-protected accounts causes interference ("Which password do I use for which site?"), not to mention frustration.

Researchers Peter Hoonakker, Nis Bornoe, and Pascale Carayon developed a questionnaire based on input from network administrators and CIS experts to examine people's password behavior. They obtained responses from 836 employees of an organization that handles very

sensitive private information. Respondents categorized themselves as novice, average, advanced, or expert users. Although some reported following best practices (for example, had 4 to 9 different passwords, used more complex passwords when needing special protection, changed their passwords 7 times per year, and logged off when not at the computer), 94% said they violate at least one (called a nonmalicious CIS deviation). "In reality," Hoonakker et al. said, "the results are probably worse, because respondents do not like to admit that they deviate from the rules." Perhaps not surprisingly, the less experienced the user, the more likely he or she was to violate computer authentication best practices.

But even close adherence to such best practices is compromised by human memory and information-processing limitations. A password that includes a picture may be easier to remember and presents one potential solution. Biometrics (fingerprint or retinal scans) is another alternative, or a combination of authentication methods (a smart card plus a PIN), but even these more expensive security measures are not "bullet-proof." As evidence of this, a 2009 study of a two-factor authentication approach to e-banking found that most participants preferred the least secure device because they perceived it as more user-friendly.

"A better balance has to be found between the limitations of human beings and the desire for increased security," the researchers concluded. "More research on how perceptions of usability, security, and convenience are related is needed."

More information: "Password Authentication from a Human Factors Perspective: Results of a Survey Among End-Users," (www.hfes.org/web/Newsroom/HFES09-Hoonaker-CIS.pdf) published in the Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting (p. 459).

Source: Human Factors and Ergonomics Society