Guide to Enterprise Password Management: 
NIST Needs Your Comments

by M. E. Kabay, PhD, CISSP-ISSMP 
Associate Professor of Information Assurance 
School of Business & Management 
Norwich University, Northfield VT

I hate passwords. I think passwords are a dreadful way of authenticating identity: they cost a lot <http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm>, they change too often (and so users write them down), the rules for preventing dictionary and brute-force attacks are generally easy for users to circumvent (da3isy*doggie, da4isy*doggie, da5isy*doggie…), there are too many of them (and so users write them… oh never mind), and nothing can stop users from writing them down (and sticking them in their wallets, behind their screens, in their desk drawers…). And yet we constantly hear non-technical managers resisting smart-token-based authentication or proximity cards because they are supposedly too expensive.<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17144&TEMPLATE=/ContentManagement/ContentDisplay.cfm>

Growl.


The blurb reads, “SP 800-118 is intended to help organizations understand and mitigate common threats against their character-based passwords. The guide focuses on topics such as defining password policy requirements and selecting centralized and local password management solutions.”

As always, this Special Publication is complete and thorough. After the usual introduction to the scope and structure of the document, the authors present a brief overview of passwords (section 2) followed by two major sections and their subsections:

3. Mitigating Threats Against Passwords
   3.1 Password Capturing
      3.1.1 Storage
      3.1.2 Transmission
      3.1.3 User Knowledge and Behavior
   3.2 Password Guessing and Cracking
      3.2.1 Guessing
      3.2.2 Cracking
      3.2.3 Password Strength
      3.2.4 User Password Selection
      3.2.5 Local Administrator Password Selection
   3.3 Password Replacing
3.3.1 Forgotten Password Recovery and Resets
3.3.2 Access to Stored Account Information and Passwords
3.3.3 Social Engineering
3.4 Using Compromised Passwords

4. Password Management
   4.1 Single Sign-On Technology
   4.2 Password Synchronization
   4.3 Local Password Management
   4.4 Comparison of Password Management Technologies

The document ends with appendices containing special considerations for firmware and hardware passwords, a glossary, and a list of common acronyms and abbreviations.

NIST requests comments on draft SP 800-118 by May 29, 2009. Please submit comments by e-mail <mailto:800-118comments@nist.gov> with "Comments SP 800-118" in the subject line.

I submitted six pages of comments and will inflict, er share, one of them in my next column.

* * *

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2009 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.