The End of Passwords:
Inadequate Solutions

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In my previous article on this subject, I ranted about how awful passwords are as a mechanism for authentication of identity. Practically everyone already knows that the for fundamental mechanisms for binding social identity to user ID -- that is, authentication -- are

- What you know: passwords or passphrases such as nonsense strings or supposedly private information (e.g., your first love’s pet name).
- What you are (static biometrics): characteristics of your body such as retinal patterns, iris patterns, hand geometry, fingerprints, face, height-to-weight ratio.
- What you do (dynamic biometrics): e.g., dynamics of voice, speech, signatures and typing.
- What you have (tokens); e.g., keys, passcards, badges, photo IDs, or anything unique or nearly unique that is difficult to obtain or counterfeit.

I'm not going to go into the details of these systems in this essay. What I want to point out is that most of these systems are good for session initiation but not so great for automatic session termination. One can place one's finger on a fingerprint reader, insert a magnetic card into a reader, look into an iris scanner, speak into a microphone, type on a keyboard, sign one's name -- all of these methods can allow an authorized user to log on to a system.

The problem is that once the interaction is complete, there is usually no mechanism for automatically detecting the departure of the authorized user. Indeed, if one tries to use tokens such as magnetic cards to detect departure by forcing the user to leave the card in the reader while the session is in progress, one of two unpleasant consequences will result: either the user will leave the card in the reader and walk away or the user will walk away with the card attached to his or her wrist and either be yanked backward or pull the equipment onto the floor with a clatter.

One promising biometric technology to allow automatic session initiation and termination is face recognition. Theoretically, it ought to be possible to set up a camera-based facial recognition system that can correctly detect the departure of an authorized user. However, I don't know of such a system in use (let me know if you do).

Another technology that should allow the kind of automatic logon and logoff I've been dreaming of is proximity cards. We already have long-established access-control systems that use Wiegand cards, which have metal particles embedded in plastic so they produce a unique signature in response to radio waves. Proximity sensors can be placed in the wall to control door locks and allow people to go in and out without having to touch their cards.

For the last 20 years, I have wanted to see a proximity sensor used with workstations to control automatic logon and logoff. This week, I learned of the authentication equivalent of the Holy
Grail: we finally have a good method for fast, effective password-free access control using proximity badges and sensors. And the results are even better than I had imagined.

More in the next article.

* * *

For further reading:


<http://www.mekabay.com/courses/academic/norwich/is340/14_I&A.ppt>

What is a Wiegand card? 
<http://whatis.techtarget.com/definition/0,,sid9_gci852292,00.html>

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see 

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 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.