The End of Passwords: Problems

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

I detest passwords. Why do I loathe passwords as a method for authentication? Let me count the ways:

1. Most systems allow users to choose their own passwords. Most users have no clue how to choose passwords that will resist even the mildest guessing based on elementary research of their interests (family, hobbies, pets, favorite sports teams) or simple dictionary-based attacks (ordinary short words). Many users choose the word "password" or their own name as their password.

2. If the system applies filters to passwords to impose content and structure requirements (e.g., minimum length, inclusion of numbers or special characters, exclusion of words in a dictionary) then most users use the same password over and over and for every possible application requiring a password including their external e-mail, offshore gambling sites, auction sites, book clubs, and pornography vendors.

3. Reasonable system administrators require periodic changes of passwords; paranoid system administrators require changes of passwords so often that the users become desperate because they keep forgetting their passwords.

4. Users faced with demands for changes of passwords adopt a policy of using the same password all the time, or possibly changing a single number in the password; e.g., ramo1bilu, ramo2bilu, ramo3bilu and so on.

5. Some administrators make the mistake of having a single day (e.g., once a month) on which all passwords expire; they thus create a flurry of interventions as support staff help users who forgotten their new passwords.

6. If the system applies password histories to prevent reuse of passwords [* see note] on a particular system, users write to passwords down on scraps of paper and stick them to every available surface, often with helpful identifying notes such as, "Password for accounting system."

7. Most users share their passwords with anyone who asks; e.g., technical support staff, the guy in the next cubicle, and even complete strangers on the street who offer them a chocolate or nothing at all.

8. Some system administrators still leave their password files accessible to any eight-year-old who wants to run a password cracker for fun and profit. A very few still use unencrypted password files.

9. Many system administrators still receive no (or ignore any) real time alert when attackers try online password guessing, especially if the attacker uses slow scans that attack many different user IDs, but only one of the time, over many hours or days.

10. Some system administrators still believe that inactivation of user IDs under password-guessing attack is a reasonable response; they thus hand their system over to attackers for a simple denial of service: try every account with a dummy password. Admittedly, most system administrators understand that requiring manual intervention to reset a lost account is not the cleverest policy in the world; therefore, they configure their systems to have a
reasonable timeout (e.g., a few minutes).

11. Sometimes organizations send users both their user ID and their password in the same unencrypted message, making it too easy for accidental or deliberate interception to break security.

12. In environments where time pressure is extreme, such as medical facilities, many users bypass the nuisance of constant logon/logoff cycles by having workstations logged on every morning by whoever gets there first and then simply using that session all day.

In the next article, I'll review the usual options for replacing passwords; in the last couple of articles in a short series I will present what I think of as the Holy Grail of identification authentication -- and it's here at last.

[* Note: I cannot resist my favorite error message of all time: Jean-Jacques Quisquater reported this gem to RISKS 21(37):

"Q276304 - Error Message: Your Password Must Be at Least 18770 Characters and Cannot Repeat Any of Your Previous 30689 Passwords"

Commented the correspondent dryly, "New level of security at Microsoft."]

***

For Further Reading


***

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

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.