Global Information Assurance Certification Paper

Strong passwords
Craig Donovan

Introduction

Password authentication is a routine part of our everyday lives. We use passwords in our personal lives to gain access to financial data via the Internet, to use debit and ATM cards and to access our e-mail.

Likewise, we use passwords in our professional/work lives to access corporate computers, applications, documents and networks. Sadly, this first line, and all too often, only line of defense is the weakest link in the security chain. This is due in part to the "routineness" of it all. After all "who really wants to read my e-mail?" lament employees. It is the security professional's task to help employees understand the larger scope and implications for choosing strong passwords.

There are many pieces of the security puzzle that must come together to make password authenticated systems and applications less likely to be breached by intruders. I believe that passwords are only as strong as the effort put into making them as hard to guess as possible. The components to a successful implementation of strong passwords should include: new employee orientation/continuing education, written corporate policy and regular auditing.

Employee Education

In general, people want to follow the rules, if the rules are explained to them and the rules make sense. It is important to define expectations early and clearly with new employees. It is equally important to reiterate standards and expectations to seasoned employees without seeming dictatorial.

In my organization's situation it made sense to work with Human Resources to incorporate security basics into the New Employee Orientation program. We also refresh long-time employees by various on line avenues such as e-mail, newsgroup postings and a security Intranet site.

Each training track focuses on the fact that security is everyone's business in the organization. Choosing a strong password is something that everyone is able and expected to do and is an essential element in our organization's security philosophy based on defense in depth.

Written Corporate Policy

A clearly defined and written corporate policy created with upper management's support is essential for all areas of information security. It is particularly necessary to implement strong passwords, especially if password security was neglected for any length of time. It is much easier to initially implement strong passwords than to go back and re-educate users on this issue.

Assessing the risk of what you are trying to protect vs. the data's worth must be taken into account. Deciding on the reasonableness of the password format required of your users will depend on risk and to a great extent on what the corporate culture will tolerate.

The Internet is an excellent research resource in defining corporate policy regarding implementing password parameters, specifically choosing strong passwords. The Gartner Group was also instrumental in guidance and siting industry standards, when we get too paranoid about security. (They have told me there is such a thing!)

Security experts and professionals have various opinions on the criterion that makes a strong password. There is no definitive list of required elements for strong passwords, but the following are criteria common to nearly all the research I've done:

- Passwords are required for all accounts.
- New users must change password the first time they log on.
- Passwords must be a least 6 characters long.
- Passwords should contain a mixture of upper and lower case letters.
- Passwords should contain a numeric character.
- Passwords should not contain any form of your name or userid.
- Passwords will expire every 90 days.
- Password history is kept preventing reuse of the last 10 used passwords.
- Passwords should not be a word found in a dictionary (even foreign).
- Passwords should not be shared or written down and kept in plain view.
- Passwords will be audited on a regular basis for compliance.

After some internal debate, we reached an agreement on the following parameters (some mandatory, some suggested) for creating strong passwords:

Sample Password Policy

Purpose and Scope:

Define the parameters pertaining to Network, Mainframe and Netscape mail passwords to promote a more secure computing environment.

Detail:

- LAN, Mainframe and Netscape mail passwords will expire every 90 days. *
- New users must change their passwords the first time they log on to the system.
- The minimum password length for these systems will be 6 alphanumeric characters.
- User chosen passwords should be difficult to guess. (link to creating strong password instructions)
- Accounts will be locked out after 5 invalid log on attempts. Locked accounts will remain locked until unlocked by the Help Desk or Security Administration.
- A password history will be kept, remembering the last 10 passwords used, preventing their reuse.
- Passwords should not be shared with others or written down in plain sight.
- Passwords will be audited for compliance on a regular basis

*We actually lengthened our password expiry duration from 60 to 90 days. This was a trade off for users being required to choose strong passwords. This was a Gartner Group recommendation.

See other policy and articles related to passwords: (links to pertinent documents)

How to choose strong passwords
Unattended workstations
Password Resets
Access violations

Auditing Passwords

There are tools available that come standard with operating systems to ensure compliance with password parameter policies. There are also third party software tools that can be installed in addition to the operating systems security modules. We utilize the tools that come with the operating systems combined with a third party software package. This reinforces the organizations' philosophy of defense in depth.

This configuration allows the for the standard compliance settings to be automated. An example of this is the system not allowing a password to be created and used unless one of the characters is an Arabic number.

With this type of check in place, it is easy to be lulled into a false sense of security that security professional's task is complete in regard to strong passwords. This is a very common mistake and should be deemed extremely dangerous to enterprise. There is still a need to manually audit passwords with tools such as L0phtcrack for Windows NT systems and Crack for Unix systems.

The reason is very simple. These tools are widely available on the Internet for crackers and legitimate security professionals alike. The tools are relatively simple to use, inexpensive and the results are a good indication of the health of the password policy that is implemented in the organization. By taking this small extra step, you could save a lot of trouble and time by simple prevention.

Words of warning. Make absolutely certain before beginning that the appropriate authorization to run password cracking tools against your own systems is attained! (Consider including this authorization as part of the organization's policy.)

Conclusion

Passwords are a fundamental part of any organization's security measures. Implementation of strong passwords should be the goal of the security professional. Strong passwords are a direct indication of the organization's security program and a direct reflection of the organization's commitment to security.

Implementation of strong passwords depends on commitment in three key areas. They are: employee education, written policy with management support and the ability to audit passwords for compliance. The lack of support in any one of these critical areas will make the implementation of strong passwords extremely difficult for the security profession, if not impossible.

Successful implementation of strong passwords should be viewed as a major milestone in security and the organization's overall commitment to security.

Sources

Ryan, Daniel J. URL: "Making Passwords Secure."
//http://www.fcw.com/articles/2000/0410/tech-passwd-04-10-00.asp

Csdweb@unb.ca "Passwords – Why yours is important."
http://www.unb.ca/csd/student/unix/passwords.html

"Protecting Your Organization's Passwords." Newsletter Volume 2 Issue 3.
http://www.vaultbase.com/page/NewsletterV2-3.htm

"Guidelines for Strong Passwords." Desktop Systems & Networking Information Technology – UCAR – NCAR. http://www.fin.ucar.edu/it/dsn/userdocs/pswdguide.htm

"Best Practices in Passwords." http://www.more.net/security/password.html

"CERN Security Handbook on Passwords," CERN, November 1998.
http://consult.cern.ch/writeups/security/security_3.html#SEC7