Subject:	Password Security
Date:	August 2005
Reference:	TA0155

PASSWORD SECURITY

Password Recommendations

Choosing a good password is probably the single most important thing you can do to keep your site secure. Any passwords can be guessed or "cracked" - but a good choice will minimize that possibility, forcing an attacker to take extraordinary means to gain access to you account. (during which time we'll probably find out about them and prevent them from doing anything destructive) There are some general rules for passwords:

Length

Longer passwords are more difficult to compromise. The minimum acceptable length for a password is six characters. Eight or longer is preferable.

Syntax:

A diverse character set is important. At a minimum, passwords should contain at least one capital letter (A-Z) and one numeric digit (0-9). Some punctuation characters may also be used.

Context:

Even if a password is long and has acceptable syntax, it can still be guessed if the attacker is lucky or insightful. For instance, if you have a church website using the password "Jesus1" would be acceptable, but a bad idea. Using any part of your account or domain name, or email address is a terrible idea. A name, date, or personal number (phone, credit-card, address, etc.) is equally bad. Any un-obfuscated dictionary word is also a poor choice. Ideally passwords would be completely random.

Lifespan:

Changing passwords frequently helps security. The higher the value of what the password protects, the more often it should be changed. A minimum of once every six months is recommended. Weekly is probably more than adequate for all but the most extremely sensitive sites.

Duplication:

Using the same password for different accounts or services is a bad idea. If an attacker obtains the password for one, the others can easily be compromised as well. Each password should be unique.

Distribution:

The more people who know a password, the less secure that system is. Giving passwords out on a "need to know" basis helps keep things under control. In combination with frequent changes, limiting the number of people who know the password at any given time will greatly reduce unauthorized or unexpected changes from being made in group environments.

Storage

Writing passwords down reduces their level of security, and should be avoided if at all possible. Since human memories are finite and fallible, and a forgotten password is both a hassle and a security problem, writing down access information in a secure place should be avoided but is acceptable for most sites if alternatives are not available.

Encryption

If at all possible, passwords should never be sent "in the clear" - meaning without being encrypted. Sending a password to someone via email is probably fine, but there is a chance it could be intercepted, so that should be avoided when possible.

Those rules are more or less in order of importance. If you ignore any of the items in the first half you're asking for trouble. The second half isn't vital for most people, but they are extremely good habits to build and will serve you well in the future. If you're storing nuclear secrets or billions of dollars worth of financial data, all of these steps (and more) should be followed thoroughly and religiously- but in that case you probability shouldn't host your site here or on any virtual server!

Guidelines for passwords

Recommended by The University of Oklahoma

http://www.ou.edu/committees/itc/policy/Password_Recommendations.html

You password should be easy for you to remember, but difficult for someone else to guess. Here are some general guidelines for passwords:

- Passwords should be at least eight characters long;
- Passwords should contain a combinations of letters, numbers, and special characters;
- The numbers and special characters should not be only the first or last character;
- Passwords should not contain your login name, your first or last name, your spouse's or child's name, or any other information that is easy to find out about you, like your license plate number, address, etc.
- Passwords should not be a word contained in a dictionary, spelling list, or other lists of words;
- Passwords should not be formed by appending a digit to a word;
- Passwords should not be common keyboard sequences such as qwerty1 or abc123.

Some methods to choose secure and easy to remember passwords

- Choose a favorite quote, phrase, saying, song, habit, title, or make one up. Use the first letter or syllable from each word of the quote to start your password. Mix uppercase and lowercase letters any way you like. Then, choose relevant special characters and numbers. Examples:

  Last Christmas, I got a big diamond ring = LC1gabd@
  I like to play basketball at 6:00 = iltpB@6:00
  I shot an elephant once in my pajamas = iSae1Imp
  I have come to depend on the kindness of strangers = ihC2dotKfs

- Choose two short words and concatenate them together with a punctuation character between them. Examples:

  dog;rain, book+mug, kid?goat

UNIX SECURITY

Once a password is compromised even at the lowest level then it gives opportunity for more damage to occur.

For example…

Unix systems keep the passwords to their accounts in a file in an encrypted form -- but on many simple systems this file is publicly available. The encryption on these passwords is virtually unbreakable. However, the **crack** program (which is available on the internet and can be run "in the background" for weeks on end on any Unix system) takes each encrypted password and, using a special key (also provided with each password) encrypts every word in an electronic dictionary, and compares them to the encrypted password to see if they match. It also tries the words backwards, with digits in front or behind, capitalized, as well as all the numbers between, say, 1 and a million. It will use any dictionary supplied to it -- whatever the language.

This painstaking process can take a lot of time, but **crack** has a lot of time, and eventually it will wind up with all the weak passwords on a system.