How to use passwords securely

Author: Panda Software

Published: Friday, 15 October 2004 09:13 GMT

Passwords have become, without doubt, users' ID cards in the Internet. Thanks to passwords, you can prove who you are and unauthorized access can be blocked. However, by the same token, should a malicious user steal or discover this data, they can take on your digital identity.

The most widely used attacks to find out passwords in authentication systems are 'dictionary' or 'brute force' attacks. In order to have any chance of success, the attacker must know the user name of the account, which is not as difficult as it sounds, as many people leave default passwords unchanged (such as root, administrator or admin).

Dictionary attacks involve, once a correct user name is obtained, trying out a series of passwords from a set list to see if they match. This kind of operation is often carried out using a purpose-built application, with a dictionary as the source of the passwords to try, as many users simply use common words as passwords.

A brute force attack is similar to the one mentioned above, although instead of using a set list, it uses all possible combinations of characters. This kind of attack is most effective with short passwords, as the number of combinations needed is obviously related to the length of the password.

Many of these attacks are aimed at accounts with maximum privileges, exploiting the fact that a system has a default user name. In Windows platforms for example, the "administrator" user account is a frequent target. One sound security tip is to change the user name of this account for one less well known or less obvious. Similarly, you can leave a decoy account with the name "administrator" with minimal privileges and a complicated password. This means that the real administrator account will be protected and you will also be able to detect when there is an intrusion attempt, using the auditing options on Windows accounts that will inform you about failed authentication attempts.

How to create and use secure passwords

One of the basic rules for choosing a password is to ensure it is both long and complex in terms of characters. As a rule of thumb, a good password is a least eight characters long and combines letters, numbers and special symbols (example: "ke8_JW.@").

Although creating a good password is not difficult, with so many services requiring password authentication, remembering them can be a problem, especially as the objective is to avoid having a series of numbers and letters that are easy to guess or remember.

To prevent having to remember a variety of different complex passwords, many users have same password for different applications, services, etc. Unfortunately, this increases the risk of an attacker stealing users' digital identities, as the password could be stored in applications and potentially accessible to others. If you use the same password for using your computer, accessing web mail and electronic banking, an attacker who cracked one of the passwords would be able to read your mail and make transactions under your name. For this reason, it is important to use different passwords, especially when it comes to services with confidential information (such as online banking services), and only use simple passwords for less important services (for example subscription to online newspapers, etc.).

However, there are also other means of authentication, including digital certificates. The best known of these are those used on secure web servers -such as electronic banking- and are used to establish encrypted connections through the HTTPS protocol. Digital certificates for clients are similar but, in this case, they can be used to verify the identity of the user, adding an additional security layer to systems based exclusively on passwords.

Several banks are already issuing digital certificates to clients. They provide them with a certificate which can be installed on their PC, preventing an attacker from accessing from another computer, even if they have stolen the user's password. For users that don't always connect from the same PC, digital certificates can be issued in USB keys, the size of a normal key- which can be used on any computer.