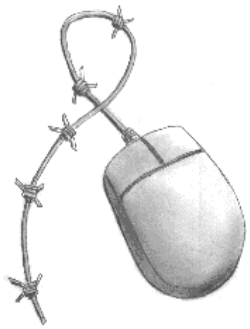
Participating With Safety Briefing no. 3

Passwords and Access Controls



Written by Paul Mobbs for the
Association for Progressive Communications, March 2002.

This briefing is one of a series on Information Security. It looks at:

- Access control and classifying data
- Passwords and authentication
- Using passwords
- Using passwords to improve security

A summary of access control

Access control

'Access control' is all about ensuring that information is accessible to those who need it, but not to those who do not. This is not always as straightforward as it seems; being too strict about access can deny information to those need it.

To control access effectively and efficiently you need to think in terms of layers:

- Do not rely on just one or two levels of access which may effectively bar everyone;
- In general, do not prevent access to information or resources unless there is a good reason to. Creating unnecessary barriers will just make additional work and wasted effort.

So, for example, if your computer can dial in to the Internet, it is a good idea to control who uses it - otherwise someone could use your computer to do things on the Internet in your name. But rather than close the whole computer, all you need to do is set up your Internet services for manual connection, rather than leaving your password on the computer and allowing automatic connections. This way other people can use the computer, but you can control who gets access to the Internet through it.

Classifying data

You should seek to classify data according to its *sensitivity*; you can then manage access on the basis of the sensitivity of the resources or information concerned, and not solely on the basis of whoever has clearance use the computer.

When considering how to protect the information you hold, remember that *access can be controlled by a number of means, but you must always assume that any data held on a computer is vulnerable to disclosure*:

- Physical locks, and passwords on the hardware and operating system can be circumvented;
- File locks can be easily circumvented if you have the programs to do this;
- Any machines or networks that are connected to the Internet, especially those machines that are always connected, are vulnerable to having the operating system hacked by others to gain access remotely;
- Any machine connected to a network, is vulnerable to attack by other machines on the network, and especially by any machine used to monitor the traffic sent over the network;
- Encrypted data held on the computer it was encrypted on is not fully secure if you have the encryption keys stored on the same computer; and
- Once a person has access to the hard disk inside your machine, they can copy it, and use other systems to recover data from it.

You can minimise the likelihood of sensitive information being disclosed, but you cannot, in the face of a determined effort to get access to the information you hold prevent access. For example, a raid by the state will result in you computer, with its encrypted data, being seized, and in many states the failure to turn over the encryption key and password can result in imprisonment. In these circumstances you would have to chose between your liberty and disclosing your most secret information.

In terms of controlling access, this leads to three simple rules:

- If information is not in any way sensitive, you only need to control access minimally - this saves the effort of protecting information that does not require control;
- If information is sensitive, but you need to use it regularly, should be stored on computers that have additional barriers to access - for example using password locks on individual files; and
- If information is extremely sensitive, you shouldn't keep it on the computer at all - there are various options, from keeping the data encrypted on a floppy disk, on a secure server, to using a removable hard disk on the computer and swapping it with a hard disk containing your most sensitive information that keep securely hidden (the latter is quite technical to set up, but is easy to use for most people).

Passwords and Authentication

Many people do not bother using passwords because the range of passwords can eventually get confusing, and if you make mistakes you are denied access.

Passwords are a means of authenticating access - of proving a permission to undertake some sort of action. There are various forms of authentication in use today:

- Passwords - widely used, from the PIN number on a cash card to long, complex passwords on encryption programs, but the idea is that you have a unique identification based upon a string of letters and/or numbers that grant access to a system;
- Keys or tokens - physical keys, swipe or smart cards, that uniquely validate identity by the possession of them, and grant access to the areas permitted by those keys;
- Biometrics - the automated reading of physical features about you, such as fingerprints, iris scans or facial features, that uniquely identify you, and hence your conditions of your access.

Computers can use all of these methods. Most non-corporate computers use only passwords, although the technology to allow other forms of authentication can be purchased.

In practice, authentication is only of use where the systems are able to effectively implement controls over access. Under the Windows operating system (Windows 95/98/ME etc.) the evolved standard is that only one password is used to log on to the system, but even then this password can be easily circumvented and full access to the system granted. In this sort of environment the strength of your passwords, or the regularity with which you change them, makes very little difference. You can build in security by other means, but even these additional methods can be circumvented by skilled computer users and computer security experts.

There are other options to improve the security of Windows system; for example, using the password protection for word processor files and the files created by many other office-based applications.

But because Windows does not prohibit the running of new software by any user, people may run programs that can use you own computer's resources to 'crack' (break the security of) your Windows passwords, as well as the passwords used to protect the most popular word processor and other files.

You can buy additional security features for Windows, using a variety of authentication systems, but as this is not standard, and it is designed for the corporate environment, it is expensive.

There are also other proprietary products you can by that provide some extra protection for systems by preventing software being installed, or preventing access to certain areas of the system without a password. But these products have been developed for the business world by computer security companies, and so are expensive.

The most secure, easily available option available for use with a Windows system is *encrypting* files, or setting up an encrypted area on the hard disk. Programs such as *PGP Free* can do this (see briefing no.4 on PGP Free), and program like this are available free from a number of sources. Using encryption requires the use of a password to access or decrypt files, so providing an additional layer of security.

Keeping the same password for a long period need not be risky provided it is appropriate for that use. On many systems you may have one password for the hardware booting up, another for logging onto your system, and a third/fourth for going online and getting email. Adding to this burden with more unique passwords, and expecting them to be changed often, creates problems for many people.

The need to change passwords is in fact only related to the probability that others can discover them. For example, if you have a very secure computer, unused by others, in an office of your own, you will not need to change passwords very often. But certain passwords, such as the passwords used to access a network (including the passwords used over the network, such as those to access email or shared files), will need to be changed more regularly because they can be extracted from the network by those with the skills to do so.

Using passwords

As we have seen, passwords are inherently insecure in protecting systems. To be useful they must be memorable, but their strength lies in the fact they are not so simple that they can be guessed or extracted by accident from the user.

The strength of a password is dependent upon its length, and the number of characters in the character set available to the user. Most passwords allow upper and lowercase letters, the numbers 0 to 9 and the underscore ('_') character. Some passwords limit the length of the password, whilst others enforce a

minimum length. You should try to find out exactly what characters are permitted in the password to ensure you can improve its strength.

The protection given by passwords, particularly on Internet/network connected machines, is reliant on being able to resist mechanised as well as manual cracking attempts and so the greatest number of possible combinations must always be used. Therefore passwords should not be names, dictionary words, or other information that describes publicly available information about you (birth dates, house numbers, friends, partners, etc.).

For example, using only uppercase characters, there are 26 possible options, so a six digit password will have almost 309 million combinations (you can calculate the number of combinations by taking the number of possible characters and raising it to the power of the number of characters in the password). If we use all the possible symbols that can be easily typed on a PC compatible keyboard there are roughly 96 options, making 782 billion 6-letter password combinations. But in practice common words are used as part of the password, reducing the available combinations to only a few tens of thousands, but this can be increased by adding numbers, non-alphabetic characters, or even using words from another language than your native language.

There are many hard and fast rules on passwords, but for most people the work involved in meeting all these rigid rules is too onerous. Most people evolve their own rules, according to the sensitivity of the work they undertake, and the way their computer systems are configured. In general:

- Passwords should ideally be a random sequence of alphanumeric characters not less than six characters long - if not - be sure to insert at least one number or other non-alphabetic character with any words you use as a password.
- Never use sequential passwords (name of saints, months, record titles, etc.)
- Do not reuse passwords - or not within a year or two of their previous usage
- 'Front line' passwords, such as the passwords to boot up a computer or log on to an operating system, should be replaced every few months where they may be discovered by other people. Otherwise replace them when you feel they need replacing.
- Passwords protected behind other passwords are more secure, and need not be changed as often (but on Windows systems, all files are open to all users, so there's no protection).
- If you have reason to believe that someone has accessed your system without permission or supervision, change your passwords immediately.
- If you have reason to believe that information has been downloaded from your system, you may not only have to change passwords, but you should also change any encryption keys kept on your system.
- Never rely on the file encryption provided with word processors and other programs to be secure when you need to protect very sensitive information - use a proper encryption system such as PGP instead.
- Never discuss passwords in public, on phones, or write them in messages posted via email or snail mail
- Do not use any personal information - names, bank account numbers, phone numbers, car registrations, etc.
- Never use the same password more than once on the same system

Using passwords to improve security

For most computer systems you can use the following tips to improve the security of your system:

- **Set the BIOS password** - When you switch on a computer you have the option of using a password to prevent the system booting-up. Newer computers have two BIOS passwords, one for the user that allows the system to boot, and one for the 'supervisor' that protects the BIOS settings from being changed. This is one of the simplest ways of protecting a computer because unless the system boots, nothing on the system can be accessed. It is not fully secure, because expert users may know a backdoor password for the BIOS system, and in any case they can access your data by removing the hard disk and inserting it into another computer. But the BIOS password is a good way to prevent access to the data on the computer by non-experts.
- **Set up user accounts** - On Windows systems the user accounts provide no security, but they are a good way for individual users to segregate their Windows settings, bookmarks, etc.
- **For sensitive files, use password locks** - Many popular office programs have the ability to scramble the content of files using a very weak form of encryption. This is enabled using a specific function, or by specifying the use of a password when saving a file which must then be provided whenever that file is opened. This provides a moderate level of security when combined with other security measures. But there are a number of programs available that are able to easily break the weak encryption on these files for those that are able to locate and use them.
- **For the most sensitive information, use encryption** - encryption systems provide the highest level of protection by encoding the file, or the hard disk, using mathematical problems so complex they cannot be unravelled without a key file and your password. For more information see Briefing no.4 on Using Encryption and Digital Signatures

Passwords and Linux

Linux provides a far higher level of security than Windows. A user name and password are required to gain access to the system, and even then the access granted is only to the areas of the system permitted to that user. The system protects user accounts by denying access between the information owned by different users, unless the user concerned permits this.

The loading of new software is also not permitted on Linux systems unless you have the passwords for the computer's master or 'root' user. Linux is not totally secure, and for the expert Linux users there are means to circumvent the protection given to users and the controls over the operating system. But compared to the way the most popular versions of Windows operate, it is far more secure.

The level of security means that file passwords are not as important compared to Windows systems - but many programs, such as Star Office, allow you to set them.

For those who might have problems with excessive security, such as young children, Linux systems allow the setting-up password-less accounts using the configuration options open to the root users,. This means that on the same computer you can give irregular users access to the system, as well as giving regular users good security for their data (although, be aware, that it is possible for expert users of Linux to abuse the system from a password-less account).