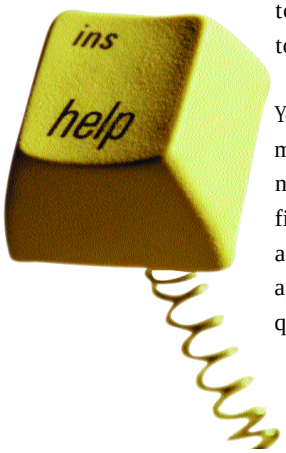
Computer (in)security,

In this issue's V&V, Bob McDowall discusses the essential features of network and application security.



Let's be very clear from the start: there are no secure computers. All we are talking about are degrees of acceptable insecurity. What is defined as 'acceptable' will vary from individual to individual and organization to organization.

For instance, consider your own PC. Your programs and data are stored on a magnetic medium, the hard disk. This is not very robust, as shock and magnetic fields can affect the operation of the PC and the availability of the data and application programs. Consider these questions further.

- Can anyone access the PC and your data?
- Is it password protected?
- Is your PC a portable?
- Can anyone steal your PC?
- Do you regularly back-up your data onto other magnetic media? (sometimes is not the acceptable answer here)
- Do you hold any intellectual property on your PC?
- Do you archive onto an optical disk?
- Do you transfer files from one PC to another?
- Do you use the Internet either for e-mail or transferring files?
- Do you use a virus-checking program AND regularly update the virus signatures from the vendor?

I can go on and develop a long shopping list of questions around computer security.

Now consider your organization, what do they do about the security of their programs, the associated data and their intellectual property? Take the questions above and apply them to your organization, which could employ 10, 100, 1000 or more staff.

Of course, we also have security problems resulting from unhappy employees and hackers. One of the latter group's most recently publicized events was breaking the security of all the users' e-mail records in Microsoft's Hotmail e-mail system. Anyone could read your e-mail. Personally, I think this is a two-edged sword as some of the e-mail I receive is more soporific than Valium. However, breaches of computer security can be very serious, especially as e-mail can be used as evidence in court cases.

What I want to discuss in an occasional series of articles in this V&V column are the aspects that constitute computer security. This has many subject areas:

- physical security
- logical security
- data integrity and availability
- appropriate access to data
- audit trails
- back-up and recovery
- fault-tolerant systems
- system and network reliability
- disaster recovery
- archive and restore of data
- communications.

R.D. McDowall

part I: logical security

As you'll agree, this is a wide range of topics too great to fit into one column, hence the split into various subsets.

However, there is a balance to be achieved in each of these areas so that all users can work effectively without corrupting data or compromising the overall security of the whole operation. Risks must be managed effectively in these areas to determine the best approaches. For instance, if the physical security of the computer room is greater than Fort Knox then does this add up to a good place to work? If the security of an application is too tight how much effective work can be undertaken?

Logical security

In this V&V column I want to cover logical security. This deals with the security that is provided by either an application and/or the operating system (OS) software, which enables a user to gain access to the application or computer system respectively. Within logical security, there is also the issue of access by an individual to some or all functions of an application and the associated data.

Therefore, we'll be concentrating on the following areas in this column:

- access to individual systems and/or networks
- access to individual functions
- access to data.

Most logical security is traditionally a user name and password. Then the security of the network and/or application provides access control to the functions and data. We'll discuss these issues first. However, there are also the common themes such as the role of management and the training of users in logical computer security, which we'll discuss at the end of this column.

User registration

Before you can obtain access to a network or application a user usually needs to register with an administrator. This should be a formal process, usually when an individual first joins an organization. However, how many organizations perform checks on potential employees before they join the company? Normally the references asked for concern the applicant's ability to fulfil the new role; it would be useful to ask one or two questions on computer security at the same time. This will be especially important if the individual is to have access to sensitive information in their new position or will be running a major application or network as the administrator. Commercial information is valuable to the organization that owns it; unfortunately it is just as valuable to unscrupulous competitors.

Assuming that any security and background checks are OK, a new user will usually complete a form that is countersigned by a line manager, before an account and password is issued by a network administrator. Some managers consider this a waste of time and think of it as just pushing paper around an organization. Think again. What you are doing is allowing a new user access to your network: do you have a policy whereby everyone has access to all the information on a networ
or works on a need to k
Tailoring the access to an individual is the best approach to use.

Most users may need training before access to the system can be allowed. This may include the security policies of the organization and password policies. It may also cover the use of floppy disks for working at home and the process of increasing or decreasing the access to applications, functions and data. When an upgrade is installed that causes the network OS to undergo a major change, follow-up training is usually required as there may be an impact on security and usability.

A network administrator will need to have a list of current and retired registered users and their levels of security clearance. When an employee leaves or retires their old account must be removed and retired as well. Similarly, if a user changes or moves positions within the organization should the access levels be changed as well?

Some organizations reuse old account numbers after a certain time. Best practice should ensure that old account identities are re-issued. For example, some organizations use the employee number as the account number, others input a user's name providing that it is unique, and others use the official company initials of an individual. This is a good and logical approach for the user name, but someone from outside the company who wants to gain access to the organization's

files can easily understand it. Thus, this places more importance on a user's password and the measures necessary to keep it confidential and secure. We'll discuss passwords and their role in logical computer (in)security now.

Passwords and their management

Currently passwords are the main way of checking that you are who you say you are when you log on to a computer system. However, there are a number of issues that make this difficult to operate in some environments.

Passwords in practice: Let's introduce ourselves to the 'password paradox'. This states that a short name used as a password is easier to remember and use but can be guessed by others. A long nonsensical word, especially computer generated, is easily forgotten; this can lead to a user writing it down to avoid forgetting it, where it can be compromised.

So what can we do about using passwords? Individuals must each have their own password. The corollary to this is that passwords must not be shared, as this compromises security immediately. Passwords must be kept confidential: no record must be made of the password outside of the computer. The classic story of the password written down on a post-it-note placed next to the PC was exceeded in one organization I have visited where the screen had a printed label on top of it which said PASSWORD = XXXXXX.

Passwords must be changed regularly, and an OS or application can enforce this every 30, 60 or 90 days if required. Whenever security has been compromised, this should trigger a password change as well. The disadvantage of this approach is that infrequent users will have the problem of remembering the current password and all users will have problems remembering a new password in the first few days after a change.

I was standing next to a user logging onto a computerized system during one audit I was involved with; out of the corner of my eye I saw that one key was depressed three times to log on to the software. After discussion it turned out that the password entered was AAA; this was the default password delivered with the system over 10 years previously.

Ideally, a good OS should remember the passwords issued to a user and prevent them reusing them. Personally, I used to have two passwords that I alternated until the OS decided that this was a bad idea.

So now we turn to the password itself: the length of it should be a minimum of 6 characters. The next advice is very sound and will probably be ignored by many readers, but you should NOT use the following as passwords:

- days of the week
- months or any other aspect of dates
- family or pet names
- car registration numbers
- birthdays
- telephone numbers.

The rationale for this is that if you know a person you'll be able to access their account by reasoned deduction. Investigations of password security can be depressing reading: in one instance a password-breaking program obtained access to over 60% of accounts in one organization. To help the situation, some OSs will have a function that prevents a user from entering some of the common words such as days of the week etc.

A password consisting of either all numbers or all letters should not be used: one covering both letters and numbers increases the permutations that could be available, making it harder to enter a system.

To help increase the number of combinations possible for a password, the alphabet can be made case sensitive thus increasing the number of characters from 26 to 52 with an increase in several orders of magnitude for the number of different combinations. Adding numbers and special characters can further increase the number of keys used for a password. More complexity can be added by concatenating words to make them longer and therefore more difficult to identify.

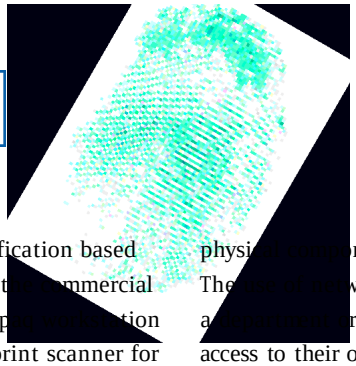
This is counterbalanced by the ease of remembering the password as human nature now snatches defeat out of the jaws of victory: we are lazy. Having devised a reasonable password that we can remember, we now concatenate 1 for January, 2 for February etc. to make it easy to remember. Of course, this never happens in your organization does it?

Further password protection: Once you have entered the password into the workstation, that is not the end of the work needed to protect your password. The weak link with passwords and any security system is that the password must be stored in the computer for comparison with the entered string. Therefore, the password must never be displayed in human readable format either on the screen or within the system, otherwise the password will be compromised. Thus, the password must be encrypted if stored and hidden carefully within the system, but the encryption algorithm will still be stored on the computer.

You may think that this is basic, common stuff but during qualification of a computer-controlled spectrometer, a colleague found that the password was stored as a text string in the WIN.INI file of the PC. The manufacturer expressed surprise that this was an unacceptable practice.

Application designers must use echo inhibition when entering the password at a terminal or workstation. This is where a keystroke is entered into the PC but not echoed back to the workstation. This must extend to remote access, especially via the Internet, to ensure the password is protected as securely as a normal network.

Putting your finger on it: Will the password continue to remain with us forever? Yes, but



not as we know it. Identification based on biometrics is entering the commercial arena — witness the Compaq workstation that comes with a fingerprint scanner for identification. What is biometrics? It is the identification of individuals based on their biological characteristics, in the example above it is the fingerprint. It is harder to forget your hand than forget your password on the simple premise that your hand is attached to your body. We'll look at biometrics in a few V&V columns early next year, providing the printing presses survive Y2K.

Network access control

So you've entered your account identification and you've remembered and typed in your password; now you are in. Welcome to Windows or UNIX or whatever OS you use. Can you do anything and everything or is there access control to various functions? Here's where the network administrator and the information technology department can help by tailoring the access control.

Limited network access: Increasingly, administrators are restricting the access rights of users to all the functions available in a network. For example, one organization eliminates the Microsoft games from its employee's portable PCs. Another organization only allows users to have access to common office applications and those business functions directly needed to perform their job function; moreover, the use of the Windows Explorer function is restricted for common users and their application drives.

As a user gains access to the network, there is an enforced path that reflects the privileges requested during the user registration process. This approach means that there is a lower risk associated with a user having unrestricted access to all functions, it also avoids the situation in which an authorized user may blunder into an area and cause disruption to applications and/or data.

At a lower level in the network design this approach may be enforced by the physical components of the network. The use of network segmentation, where a department or user community only has access to their own resources and, as a corollary, denies others access to them, is one way to enforce limited network access.

Other approaches to logical security of the network are listed below.

- Identification of terminals — when a function has to be performed in a specific place, the terminal has a network address that confirms whether the task is completed in the correct location.
- Use of time-outs for logging users off their workstation — if no activity has been detected for a predefined period the user then has to log in again to continue their work.
- User reauthentication — where, at key stages of work, a user is prompted to re-enter their password (see below).

Reauthentication of user ID: Part of making computer environments secure is the reauthentication of user identity, where the user is prompted to re-enter their password to confirm their identity. Typical situations where this may be appropriate is when a user attempts actions such as:

- attempting to use a function not usually privileged to all users
- requesting access to a highly classified program or file
- requesting a service deemed excessive in a particular environment (e.g., heavy download of files from an intranet over a long period of time).

This feature would be used in addition to some of the other logical security features discussed above.

Monitoring unauthorized access: Usually an OS will allow a user three attempts to gain access, three being a balance between a non-tolerant (one attempt only) and a hacker's paradise (unlimited attempts) system. To be effective the system should log the person off the system after three attempts. There is then a delay before the user can log on. If the user fails again there will be a longer delay before a new attempt can be made. If this happens to a specific user several times, it may be because more training is required or a possible security breach has occurred.

Most OSs have the ability to monitor and record all log-in attempts as well as the failures. Thus, the attempts described above will be monitored and recorded in a log. These logs, ideally permanent ones made on CD write-only disks to prevent unauthorized tampering, should be monitored regularly to see whether discontinued accounts and user identities have been used or unusual events have occurred on the network. Unusual events on a network are typified as

- abnormal termination of an application
- abnormal system failure
- failure of software security mechanism
- unsuccessful attempts to log on to the system or network
- attempts at unauthorized access to files or applications
- attempts to use privileged instructions improperly.

Again these events need to be investigated to see whether there is any potential breach of security, and the appropriate changes made.

Application security

OK, you have got into the network and can now access the application you want (at last!); this may require a second user identification and password, or the enforced path from the network will direct you to the appropriate application and you'll enter directly. Within the application you'll find another level of access control features that will allow the application administrator to define the access of classes of users or individuals to different functions. Access to all systems, but especially business critical ones, must be defined in writing.

There are three main areas of security regarding applications that will be discussed below:

- access privileges
- access by function
- security models.

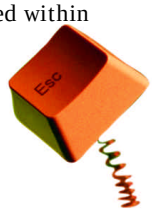
However, the principles described are also applicable to network security. This is intended to provide a rational introduction to logical security within an application.

User privileges: Any discussion of the logical security in an application should first consider what each user could do when they use any function. These are the privileges associated with the user of a function within an application. This has a continuum that ranges from the ability to undertake any function to being denied access. These privileges are shown in Table 1 and are intended to be general. This continuum may need to be tailored to any application in practice. For instance, you may decide that an execute-only function and a read-and-write function are so similar that combining them makes sense. Alternatively, the privilege may not be implemented in the application you have purchased or developed.

Mapping user privilege to application function: Once the user privilege continuum has been decided, the next stage is to map the levels to job functions. In this example we'll use just four levels:

- zero-level (denied)
- read only
- read–write
- administrator (create, read, write, copy and delete).

Also in our example we'll have four jobs that will be considered within the application:



- trainee
- user
- supervisor
- system administrator.

The approach taken here is that the minimal privileges required, consistent with the user being able to perform their job effectively, will be implemented. In our application there are four functions: it's a simple application!

The mapping of user privilege to application function is shown in Table 2. The trainee has only read access to three functions, as the impact that an untrained user could have, including corrupting the data, is then limited until they are competent. As any user becomes more experienced they have access to more functions together with greater access privileges. However, if you look at Function 1, only the system administrator has full access to this function as it may be associated with data security or access rights.

The system administrator should review the access rights of individuals regularly, especially if they are trained or are promoted. This should be reflected in a change of user privilege. However, this may be difficult to implement in some applications, as the security system may not allow this approach.

Security models: There are two main types of security models possible in applications: legacy systems tend to have a hierarchical security model and newer applications have a class model. Regardless of approach, the security profiles of each user will be kept by the system but best practice is also to document this outside of the system.

The hierarchical security approach is based on a tier of users whereby a user can see everything that their peers can see and the functions in the tiers below but not above them. Thus, the system administrator can see everything. This is shown in Figure 1 and is similar to an organizational chart. Each user will be able to see what the other users may be doing and have access to their data as well as their own. From this perspective, it is not ideal but is better than no application security.

The class approach is more flexible and can be tailored to individual users. You'll have the same user types but each profile can be different. Again refer to Figure 1 and consider the two trainees, both will have the same profile as shown in Table 2. However, during their training one user is seen to be more proficient compared with the second. Under a class security system the access profile of the more proficient trainee can be updated so that he or she can have read/write access to Function 2 but the second trainee cannot. This approach allows a dynamic modification of a user profile to be made relatively easily.

Role of management

Although this topic has been left to last, it is essential that the role of management in computer security be discussed because of its importance.

In short, managers must take the lead for computer security. They are responsible for running the business and thus must also be responsible for ensuring the business is protected from loss of confidential or important data and computer services. This is not just an information technology issue; it affects everyone in the organization. Unfortunately, when you mention the word 'computers' to many managers you can see their eyes glaze over and they pretend not to understand. 'It's not my

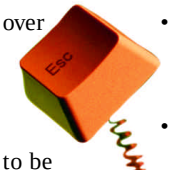
Access privilege	Access rights
Zero-level	No access rights or access denied
Execute only	User can execute functions accessed but nothing else
Read only	User can only read the data accessed but cannot write or append anything
Write only	User can overwrite data
Read–write	User can read or write as required
Append only	User cannot change any data but can add additional information
Administrator	Full access rights to create, read, write, copy and delete data

Table 1 Continuum of user privileges.

responsibility, go and see IT' is the common response. This is an appalling viewpoint and a total abrogation of responsibility.

The responsibilities that management should undertake with respect to computer security are

- understanding the problems associated with computer security, as this provides the basis for the other roles of management
- providing visible and vocal support for computer security. This provides the environment in which computer security can be sold to the user community and guidance given effectively. Without this there is little point in IT personnel trying to provide security, as local management will override their efforts
- planning for appropriate computer security responses based on business drivers and an evaluation of risks facing the business. For instance, if you are responsible for a stand-alone computer application that is not networked and is not linked to other applications in the organization, then the security requirements are a lot less stringent compared with an application that runs partly over the Internet.



Training of users

For computer security measures to be effective, the users involved in implementing them must be trained. This training will need to cover full-time, temporary, part-time and contract staff that use computers in your organization. It may also need to cover service and maintenance engineers performing repairs to computerized equipment or applications. Furthermore, as technology provides the means to access applications remotely via modem, special arrangements may be necessary to minimize the impact that they can have, especially in a regulated environment.

The training will involve using the security measures (e.g., passwords and their maintenance), but also general awareness of computer security issues. For example,

- user's authorization to access systems and networks
- the need to report problems with software, including bugs, errors and possible breaches of security
- documented ways of working.

Summary

We've looked at a variety of logical security issues such as user registration, passwords and their maintenance, and access control associated with applications and networks. These are fundamental to ensuring the integrity and confidentiality of data and the smooth operation of applications.

Bob McDowall is Principal of McDowall Consulting, involved in the design and validation of LIMS systems and software applications. He is also Visiting Research Fellow in the Department of Chemistry, University of Surrey, UK, and a member of the Editorial Advisory Board of Scientific Data Management.

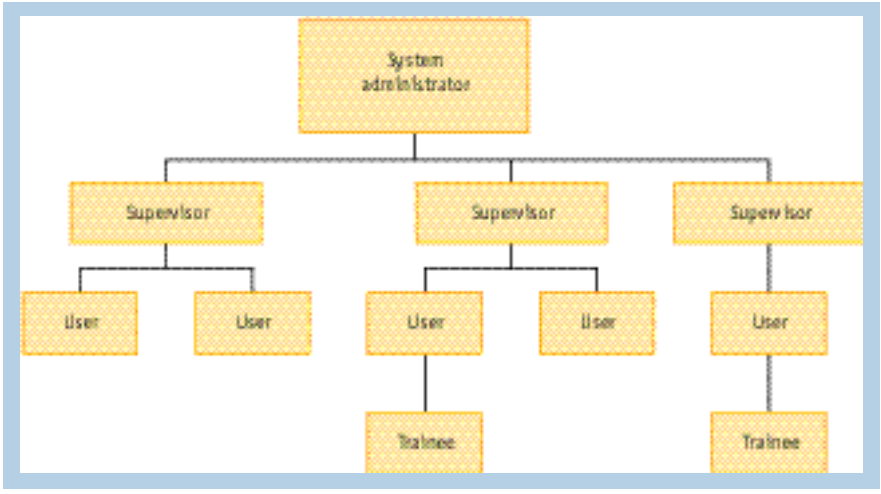
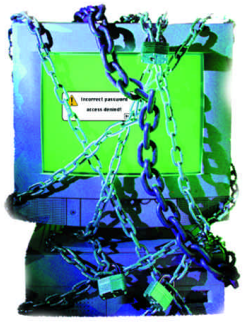


Figure 1 Hierarchical and class security.



User type	Function 1	Function 2	Function 3	Function 4
Trainee	Denied	Read	Read	Read
User	Denied	Read/write	Read/write	Read/write
Supervisor	Read only	Read/write	Create/read/copy write/delete	Read/write
System administrator	Create/read/copy write/delete	Create/read/copy write/delete	Create/read/copy write/delete	Create/read/copy write/delete

Table 2 Access by user types to individual functions within an application.