4.6 Network security

The security problems when using networks such as the internet are well documented. There are various security threats to networks and there are many equally varied ways of combating the threat. Many of these issues are discussed in Chapter 6 but this section will concentrate on four areas:

- user ID
- password
- encryption
- authentication techniques.

User IDs

When logging on to any network system, a user will be asked to type in a **user ID**. This assigns the user privileges once the logon procedure is successful. For example, on a network, top level **privilege** would be for an **administrator**, who is able to set passwords, delete files from the server, etc., whilst a user privilege may only allow access to their own work area.

Passwords

After keying in the user ID, the user will then be requested to type in their **password**. This should be a combination of letters and numbers which would be difficult for somebody else to guess. When the password is typed in it often shows on the screen as ******** so nobody overlooking can see what the user has typed in. If the user's password doesn't match up with the user ID then access will be denied. Many systems ask for the password to be typed in twice as a **verification** check (check on input errors). To help protect the system, users are only allowed to type in their password a finite number of times – three times is usually the maximum number of tries allowed before the system locks the user out. After that, the user will be unable to logon until the system administrator has re-set their password.

When using some internet websites, if a user forgets their password they can request the password to be sent to their email address. The password is never shown on the computer screen for reasons of security.

Encryption

Encryption is the converting of data into a code by scrambling it or **encoding** it. This is done by employing encryption software (or an encryption key). Since the data is all jumbled up it appears meaningless to a hacker or anyone who illegally accesses the data. It should be stressed that this technique *does not* prevent illegal access, it only makes the data useless to somebody if they don't have the necessary decryption software (or decryption key). It is used to protect sensitive data (such as a person's banking details).

The system works like this:

- A user writes a message and the computer sending this message uses an encryption key to encode the data. For example, the message 'THIS IS AN EXAMPLE' (sent on 15 April) is encoded to '43Kr Kr T7 W04887W'.
- At the other end, the receiving computer has a decryption key which it uses to decode the message. Note that the date when the message was sent is important since this formed part of the encryption **algorithm**.

Encryption keys are much more complex than the one above, in order to prevent computers being used to crack the code. Very sophisticated algorithms are used which make the codes almost unbreakable.

Authentication techniques

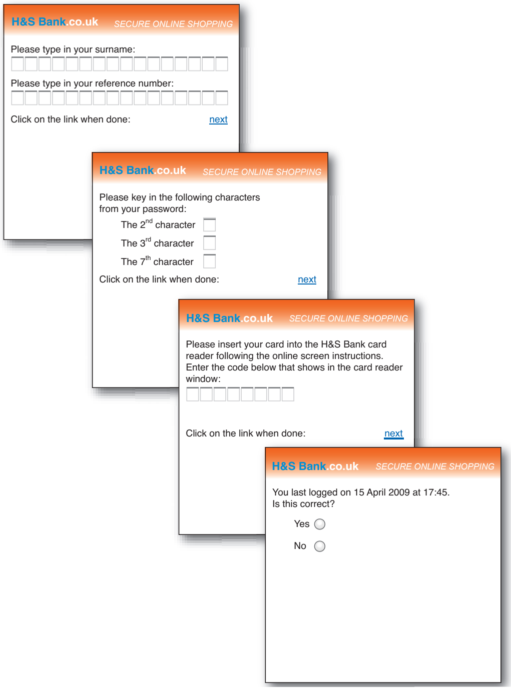
As shown above, there are many ways in which a computer user can prove who they are. This is called **authentication**, and a type of authentication is used in the banking example that follows. Most systems adopt the following authentication logic:

- something you know – e.g. PIN/password
- something belonging to you – e.g. your bank card
- something unique to you – e.g. your fingerprints.

At least two of these are needed at the moment when a user has to prove who they are. For example, the following banking example uses:

- something you know – surname, reference number, PIN, date last logged on
- something belonging to you – card put into card reader to produce the 8-digit code.

In future, the third feature will be introduced (such as a fingerprint scanner attached to a computer to uniquely identify the user).



Please type in your surname:

Please type in your reference number:

Click on the link when done:

Please key in the following characters from your password:

The 2nd character □

The 3rd character □

The 7th character □

Click on the link when done:

Please insert your card into the H&S Bank card reader following the online screen instructions. Enter the code below that shows in the card reader window:

Click on the link when done:

You last logged on 15 April 2009 at 17:45.
Is this correct?

Yes ○

No ○

Figure 4.8 The authentication process

Banking example

A user belongs to H&S Bank. He wants to check the status of his account online. He logs onto the H&S Bank website using his ISP. Figure 4.8 illustrates a sophisticated set of steps taken to prevent unauthorised access.

Only once each page has been successfully navigated will the user have access to his bank account. The last stage is a final check to see if the customer's account has been illegally accessed – if they hadn't logged into the website on 15 April at 17:45 then this would trigger a security check into the customer's account. Note that the last web page makes use of what are called **radio buttons**.