the computer is situated, then the technique used by the protagonist in *War Games* could be used: he programmed his micro to dial every possible telephone number in his town. If a computer answered — identified by the tell-tale carrier tone whistle — then the machine took a note of the number; but if a person answered, the modem hung up and went on to the next number. With an auto-dial modem this can be done automatically; dialling manually would get very tedious!

Once connected with the computer, you are invariably asked for a password. Some networks allow limited access if you type in 'GUEST' or 'NEWUSER', or if you just press RETURN. But the true hacker will try and crack the password. Often this is not particularly difficult, as users tend to be rather unimaginative and use names, such as 'SMITH', or obvious words, like 'SECRET', or even, simply, 'PASSWORD'. Similarly, with passwords made up from numbers, people tend to choose easy-to-remember sequences: for example, their date of birth, like '090560'. Many computers are very forgiving and will allow several attempts at the password before disconnecting you. Even then, you can normally dial back and continue where you left off, without the host computer becoming suspicious.

Once into a system, most hackers are content to just look at everyone's files, find the games pages (if any) and 'talk' to other hackers who have also broken in. Some of the more destructive ones delete files, leave obscene messages and try to 'crash' the whole system. A system crash can have a disastrous effect on legitimate users.

Even on the more sophisticated mainframe machines, programmers often leave 'back doors' in the system so that in an emergency they can bypass all the protection measures and quickly get into the program. More often than not, the people who operate the system will not know that such back doors exist.

You will notice that most of the cases we have outlined involve university computers. This is because such computers, apart from having external dial-up access, usually operate an open access policy. With thousands of users and many remote sites this is the most practical way to run such a system. Unfortunately, they are also very easy for hackers to get into, and once in they can 'leap-frog' from one computer to another by posing as legitimate users. One student at San Jose State campus found a loop-hole in the university computer's Talk program, which allows students to 'talk' to the other campuses in the California State University. The student managed to overcome the local restriction and succeeded in talking to computers in Sweden, Iran and China, as well as all over the United States. The telephone bill came to over £7,000.

Why do hackers do it? Usually just for the thrill of 'beating the system'. Many have an unofficial code of conduct, and claim not to delete files or leave obscene messages. For them, the excitement is simply in breaking the codes. Nevertheless, by using computer time and not paying for it they are committing fraud.

Banks have long suffered from computer crime, but until recently it was all done 'in house' — by dishonest employees transferring money to bogus accounts, for example. Estimates for computer fraud vary from £30 million to over £2,500 million per year — and that's in Britain alone. Understandably, banks and companies seldom publicly acknowledge that they have been victims of computer fraud and hence it is difficult to put an exact figure on it.

With the growth in ownership of home computers, and with more and more computer networks using the telephone lines, the problems of computer crime can only increase. Whether it be mischievous teenage hackers deleting files and stealing computer time or professional criminals siphoning money into their own accounts, the methods used are exactly the same.

Trial And Error

IAN McKINNELL

The process a hacker uses involves a great deal of trial and error, which on very rare occasions leads to successful unauthorised entry into a system. Even if a hacker is able to locate a particular system, he is often met with a dialogue like this when he tries to log on to the system:

```
CONNECT QX001001 14.32
     12/7/84
>                          Press return: prompts for user ID
USER?
>HELP                      No help: not user friendly
USER?
>£$OFF                     First attempt at a valid ID
USER?                      ID not valid for entry
>UK001                     Second attempt at a valid ID
PASSWORD?                  ID accepted: prompts for password
>GUEST                     First guess
PASSWORD?                  Not accepted: second request
>NEWUSER                   Second guess
PASSWORD?                  Not accepted: third request
>QWERTY                    Desperation guess
LOGOFF 15.13 CONNECT       The user is disconnected after
     TIME = 0.13 MINS      the third failed attempt to find a
                           password
```

In some cases, whether by intrigue or pure luck, a person is able to find a valid high-priority password and enter a system. The following imaginary dialogue describes how such a user could learn confidential information about a legal user:

```
CONNECT BYF990
     15.14.02 12/07/84
>                          Press return
USER?
>UK001                     Valid ID: prompts for password
PASSWORD?                  First attempt: system operator
>SYSOP
LOGON 15.15.07 12/07/84
HOST: BYF990/SPYLOM        Serial number of software
USER: UK001                Full clearance to files
SERIAL NO: ZA180-7         Users can be made inactive if
PRIORITY: SUPERUSER        they don't use the system
STATUS: ACTIVE             regularly
YOU ARE SYSOP              Confirmation
7 USER(S)
APP01 APP02 BYF7 BTY04     Lists all users
     BZX88 BZX02 SYSOP
>REMOVE ARP01              Command reserved for system
USERS(S) ARP01             operator
     DISCONNECTED          Valid user removed
>WHO IS BTY04
BTY04      CAREY DIMMIT,
     BTY LOPP, 742
     SILICON DV
HERTS 07662-093164
```