▲ WHO YOU GONNA CALL? NEIL BARRETT IS YOUR MAN IF YOU SUSPECT FOUL PLAY OF A COMPUTER-BASED NATURE

Neil Barrett, scientist and computer crime fighter, is a leading expert in his field. Organisations including banks, the police, Customs & Excise and others call in Barrett to try hacking their systems or to finger a suspected hacker. Here, he helps George Cole with his enquiries.

Hacker cracker

Neil Barrett spends a good part of his time hacking into computer systems, sneaking into offices, breaking open encrypted files and cracking computer passwords. But before you call the law, you should know Barrett is on the right side of it. At just 36, he's one of Britain's leading computer crime experts and has worked with a range of organisations including the police, customs, banks, the Inland Revenue, telecomms and utilities companies, the NHS, military defence, ISPs and the NCIS (National Criminal Intelligence Service).

photograph by Nick Dawe

As one of three Fellows at Bull Information Systems, his full-time job is looking at the future development of IT (Barrett's Ph.D thesis was on complex computational modelling). "I describe myself as a computer scientist with an interest in computer crime," says Barrett. "It's really a hobby." Some hobby. In addition to his advisory role, Barrett has written many papers, two books on computer crime, and is in much demand on the lecture circuit.

So which computer crime activity makes it to number one? "Dissemination of computer viruses — and it has been for a long time," says Barrett, "The loss of money, per virus incident, is quite low. The problem is the phenomenally high number of incidents."

Insider fraud is "popular", too. It's usually carried out by employees trying to swindle their companies through a variety of scams such as creating false suppliers or contractors and channelling funds to their own accounts. Employees can also cause havoc by leaving logic bombs (electronic time bombs) which can damage a company's IT system.

Says Barrett: "For example, if an employee's work number is registered as 'sacked', the logic bomb goes off. Another is to encrypt important company files, then change the password so only they can access them."

External hacking doesn't rate highly in the computer crime league. "Over 75 percent of hacking is done by insiders and it's easy to see why. The person on the inside is on the right side of the firewall — they know the computer system and have access to the passwords," says Barrett. What lets hackers down is that they either have the computer skills but don't understand the business, or vice-versa. "What's worrying is that we're now getting people who understand computers and how businesses work."

"Pornography on the internet is not as big a problem as some sections of the press make out," claims Barrett. "There's a large number of pornographic images on the internet but not a great deal of the really nasty stuff — dead bodies, bestiality and paedophile material." He adds that there are ways of tracking child porn on the net. "We can get the signature characteristics of files containing this type of material, and if someone downloads it from a newsgroup, we can detect and follow it."

A bigger problem is the dissemination of copyright-protected material such as computer software and PC games from the internet. Barrett complains: "Suckers like me buy software from legitimate sources and end up paying for the losses companies suffer from this type of activity. It's not fashionable to say, but it's theft."

Despite the hysteria over criminals using encryption to protect their computer files, Barrett doesn't believe a Key Escrow system, which would give law enforcement agencies access to decryption keys held by trusted third parties, is either necessary or desirable. "In all the cases I've worked on, encryption has never been a problem as we've always managed to break into the file or get hold of the key. The US ban on exporting hard encryption keys is misguided and foolish because it simply allows others to undercut American business.

With all these skills, it's little wonder that Barrett was ONCE OFFERED £150,000 TO STEAL a file containing a list of high-income customers from a bank

"Protecting your computer system is like locking a car and switching on the alarm. This will stop the 'door rattlers', but if a car thief is really determined, they'll either spend a lot of time cracking the alarm or take it away on the back of a lorry. There's also the 'Black and Decker' hack. If I put a power drill to your knee and ask you to give me the password to your computer system, the chances are you will. The point is that no computer system is completely hacker-proof, but you can go a long way making it hard to crack."

Barrett has a routine when he's asked to help a company to combat computer crime. It begins with a "whiteboard attack" which involves looking at the company's computer system and postulating how it could be attacked. He also considers "the route to reward". "An attack has to be cost-justified," claims Barrett. Then there's a tier analysis, which considers different levels of criminality: from schoolboy hackers to organised gangs, determining which are most likely to attack a company. "We tell the company what action to take to protect themselves, what it will cost, how they can detect it and what their response would have to be."

The second step is a dress rehearsal, showing how the existing company system can be attacked. "It may be as simple as getting hold of passwords or breaking into a web site, or sitting in a darkened room with a PC and attempting to blast open their system. It's demonstrating weaknesses," he says.

Barrett admits that some systems are too difficult to crack, while others are frighteningly easy to break into. "We once obtained some passwords by simply calling up the company and asking for them. We got an employee's name from the company directory and called in, saying that we'd lost our password. We asked for it and they told us!" On another occasion, Barrett and a colleague entered a building by sneaking in with a group of legitimate visitors. "We looked like

part of the crowd, and we could plug into the company's network and bypass the firewall."

With all these skills, it's little wonder that Barrett was once offered £150,000 to steal a file containing a list of high-income customers from a bank. "I never found out who wanted the list, but it looked as if they were planning to set up their own bank and wanted to start with a strong customer base," he recalls. Needless to say, Barrett declined the offer and informed the police, but the mystery caller had covered his tracks.

During his investigative work, Barrett uses a number of tools. The system audit log keeps an electronic record of the system's operations and is a crucial record. The DIBS(R) disk imaging system allows him to make perfect hard-disk copies without affecting the contents. Other tools can detect internet traffic and collect the packets of data for analysis. Profiling tools can tell you whether any traffic looks as though it may be coming from a hacker, or whether someone is trying to edit an audit trail.

In the future, intelligent user-profile systems will automatically build up a picture of legitimate users by analysing the way they use the keyboard: "The way we type is as distinct as the way we sign our signature, and so a computer could detect whether it was really you using the computer," says Barrett. Smartcards will also play a bigger role in IT protection. But who is ahead of the game — the IT criminal or the law? "It's pretty even," says Barrett, "but you've got to remember that the criminal will always have a greater reason for doing it."

☛ *Barrett has used this experience and other events to write a novel, Evil dot Com, which is currently awaiting a publisher. His two other books, Digital Crime — Policing the Cybernatio,n and The State of the Cybernation, are both published by Kogan Page.*

THE ELECTRONIC CRACKER

Psychological profiling is fast becoming a tool in crime detection. The process, made popular by the TV series, Cracker, uses scene-of-crime evidence to create a profile of the individual most likely to have committed the crime. Barrett was recently involved in a case where, for the first time, profiling was used in the investigation of a computer crime. A user profile was created by analysing the way in which the computer had been used. With little more than a series of time stamps and a list of commands, Barrett created a remarkably accurate profile.

The work was part of Barrett's role as a defence witness in a case resulting from a major UK paedophile investigation called Operation Starburst. Caught up in the investigation was a young university student who was found to possess dozens of floppy disks containing around 750 allegedly indecent images of children. The student was charged with possession with intent to distribute.

The evidence suggested that the student had received the images and then copied them onto floppy disks. But more proof was needed: a police error meant that important audit information had been wiped.

"The prosecution and defence had little to go on," says Barrett. The available information consisted of the student's history file, which showed when the student used the computer, the commands he used and the times he was logged-on, plus some backup tapes. "There was some overlap between the history file and the backup tapes — we had information going back six months but no audit logs or email records."

A user profile was created by analysing the command used by the student during each computer session, and the time gap between them. The university has a Unix-based system which uses a "change directory" command followed by a "list directory" command. Some users run the commands together (typing CD;LS), others wait for the LS prompt to appear. "The gap between the two commands isn't thinking time, it's the time it takes for the system to respond," explains Barrett. The student had an internet account with a password known only to him: "He used some shortcut commands, so whenever we saw them, we knew it must be him. He also knew his way around the files, so we expected very few LS commands," says Barrett. But close examination revealed that someone else was accessing the internet account using a different pattern of commands. "This meant the Crown couldn't show that the defendant was the only person with access to the account, thereby casting doubt on whether he had distributed any of the images."

An examination of the commands used by the mystery caller revealed someone trained on an early version of Unix. "Unix machines arrived in universities in the late seventies," explains Barrett. "There are a number of versions of Unix, each with a particular set of commands. The commands used pointed to someone trained to use Unix around 1980-1984, after which the next version was released."

"If he were a systems manager in the early eighties, he'd be aged around 40-45 today, so we were able to tell the court that we had evidence that there was a mystery caller with access to the internet account, what their age was, their job, the date they were in higher education, the type of computer system on which they learnt their skills. We even traced the workstation they'd used to access the account."

It didn't take long for the court to discover the identity of the systems manager, who fitted the electronic profile. Apparently he had been asked by the police to search the student's email account — something the police had omitted to tell the defence. A retrial was ordered.