MARK GRIFFITHS, PhD
Psychology Division, Nottingham Trent University

The two articles that follow are both authored by Mark Griffiths

COMPUTER CRIME AND HACKING: A SERIOUS ISSUE FOR THE POLICE?

It is perhaps only very recently that the police have begun to consider computer crime seriously. In May 1999, the Government announced the formation of a 24-hour code breaking centre to help police, customs and the security services tackle IT criminals (Hencke, 1999). The actual extent of computer-related crime remains a somewhat elusive figure. However, some of the most recent investigations have asserted that the extent of computer crime is on the increase and that the majority of such activities are committed by individuals against their employers (Audit Commission, 1994; 1998). Charlesworth (1995) noted that the criminal law and those who enforce it have taken time to come to terms with the implications of change with regards to computer crime. The technical complexity associated, rightly or wrongly, with computer crime combined with the limited number of prosecutions has permitted criminal justice practitioners the luxury of ignorance. However, if we intend to take seriously the findings of these recent investigations then this period of avoidance may well be over.

In the broadest possible sense, computer crime can be divided into two categories: (i) display, downloading and/or the distribution of illegal material, and (ii) hacking. Though "hacking" is a term with which most people are now familiar, the actuality of the process continues to be unclear for many. Generally, such an activity refers to the unauthorized alteration or removal of material and/or the illegal interception of communications. This article examines the case of hacking only.

Is Hacking a Serious Problem?

Hackers caused an estimated $286 million worth of damage in the US in 1998 (Lillington, 1999). Over the last few years, there have been increasing numbers of headlines and articles about the threat of hackers to national security (eg, "US at mercy of cyber terrorists", *The Sunday Times*, May 17, 1998; "How Bevan cracked top secret X-files", *News of the World*, November 27, 1997). Hackers also appear to be switching tactics. Instead of going for big companies (eg, Citibank; see section

below), they appear to be targeting people's individual home computers and their personal accounts. By leaving viruses scattered across the Internet, the hackers have discovered they can seize control of home computers and steal people's identities. This can all be used to gain access to bank accounts, shopping accounts, phone records and private business information.

The Audit Commission (1998) also reported that organizational computer fraud (including hacking) was on the increase. Their latest survey of 900 organizations reported that (i) 45% of companies reported IT fraud in 1997, (ii) the number of organizations reporting hacking incidents had trebled since 1994, (iii) virus infections were the single most prevalent form of abuse, and (iv) telephone systems are the new target for hackers.

In general, it could perhaps be argued as the Home Secretary Jack Straw said "that the police are using 19th century procedures to pursue 21st century criminals" ("Straw seeks to patrol Internet", *The Guardian*, 29/12/97, p.8). Until recently, hacking into government computer systems seemed the preserve of teenage pranksters (Campbell, 1998) portrayed in films such as *War Games*. However, more recently, there have been numerous announcements by NASA, the Pentagon and the US Navy that their computers are under cyber-attack (eg, Graham-Cumming, 1998; Campbell, 1998).

What Exactly is a "Hacker"?

The word "hacker" has had a number of meanings and was originally a positive term for creative programmers. By the late 1970s, the term was used to describe "computer revolutionaries" (ie, entrepreneurial types who ended up founding many of the computer companies around today). In the 1980s, the meaning shifted somewhat and referred to those people who were actively involved in breaking copyright on computer games by copying them and selling them on. Nowadays, a hacker is usually perceived to be a criminal or a "cyberpunk" who is motivated by greed, power, revenge and/or malicious intent (Marc Rogers, cf. Lillington, 1999).

Marc Rogers, a Canadian forensic psychologist who works with the Winnepeg police department, has claimed that hackers fall into three main sub-types on what he calls the "hacker continuum". He claims that the term "hacker" is no more use than the word "criminal"' for law enforcers, ie, in the same way that police want to know whether the criminal is a burglar, embezzler, shop-lifter, forger or blackmailer, police should also know what type of hacker they are dealing with. Rogers' research indicates that hackers conform to popular stereotypes. They are socially inept "geeks", white, middle-class males aged 12 to 28 years of age, have limited social skills and who have good computer skills but perform poorly in schools. Basically these people are what Rogers describes as "sad loners" who crave membership and tend to participate in online discussion groups. Many of them get caught

because they like to brag about their hacking attacks online. Rogers further distinguishes between:

> " '*Newbies*', '*Cyberpunks*' and '*Script Kiddies*' – these hackers are inexperienced and have little skill. They tend to use other hackers' programs, and cause malicious damage such as defacing web sites
> '*Insiders*' and '*Coders*' – these hackers are more experienced and usually write their own hacking programs. They also mentor 'newbies' and 'script kiddies'.
> '*Professionals*', '*Hacktivists*' and '*Cyberterrorists*'' – these hackers are élite, highly motivated, and are often former security experts from the former eastern Bloc. They also use all the latest state-of-the-art equipment."

What Methods do Hackers Use?

There are a number of tried and tested techniques at the hacker's disposal. Some of these are of a technical nature whereas some are more psychological, although hacking into a private system often requires inside knowledge. The methods used by hackers go by such names as brute force, war-dialling, denial of service, sniffing, social engineering, buffer overflow, trashing, spoofing and Trojan horses (see Grey and Warren, 1997; McClellan, 1997; Graham-Cumming, 1998). These are briefly described below.

Trashing – One popular method is to look through dustbins for old computer manuals, printouts and password lists. Companies routinely throw away out-of-date information without shredding it. The hacker can use some of this old information to their advantage.

Social engineering – This method involves the hacker phoning an organization pretending to be an IT worker. During a single telephone call, a hacker can usually extract vital information about the computer system including login names and passwords.

Brute force – This method is where a hacker will use password-cracking programs. As many computer users choose easy-to-guess passwords, a program will often yield good results by trying every word in the dictionary.

War-dialling – This method gets its name from the 1983 film *War Games*. This is where a simple program is directed to dial all the phone numbers with a specific STD code or region and note the tones that would identify a computer answering.

Data sniffing – This method involves special software called "packet sniffers". This can be connected to a computer network and will extract all the packets of information used to pass data between computers (ie, a package which eavesdrops on communication between computers). Computer systems connected to networks (such as the Internet) are particularly vulnerable to sniffing. Data sniffers collect any information that might be useful including confidential passwords and account

information. These secrets are then sent back by electronic mail to the hacker's master computer.

Buffer overflow – This method is one of the hacker's more technical attacks. Many computer operating systems store data and programs interleaved in the same part of the memory. When one part of the data is a buffer (ie, a location used to store data being transmitted to the computer), it is often possible to send more data than will fit in the allocated space. When this happens, the data overflows and may override the program that is running. A hacker can then send a series of commands that gets written into the computer's memory and allows the hacker to take control of the computer.

Denial of service – This method is where specific machines or specific regions of the Internet are disrupted to prevent legitimate users from getting access to their own machine. The hacker then takes advantage of this during the blocked period.

"Trojan horse" viruses – This method is one of the newer threats created by hackers. The method works by concealing a virus within an attractive page of information on the Internet. The page appears harmless but unfortunately conceals deadly functions. In essence, the viruses proceed to take over the computer like an invisible man. The simplest Trojan horse viruses replace the messages shown when a login is requested. Users think they are logging into the system and unwittingly provide their user names and passwords to a program that records the information for later use by the hacker. Other Trojan horses perform destructive activities like deleting hard discs. There are also other viruses such as *'identity thieves'* and *'worms'*. 'Identity thief' viruses leave instructions inside sensitive software. When the computer owner logs on, the hacker's hidden instructions are carried out. 'Worms' (created by infamous hacker Robert Morris back in 1988) are viruses which creep inside security barriers (known as firewalls) set up by companies to protect their confidential information. The worm moves around the company network causing damage or mailing secrets back to the hacker.

Hacking: The Case of Cybertheft

It is a commonly held belief that crime always follows money (Griffiths, 1999). Given this general rule of thumb, the Internet is no different. New technology and virtual money brings with it new problems as hackers use their skills to engage in cybertheft. It is often joked that the only safe computer is one that is unplugged! The reality is that technological advancement and increased Internet availability has provided for new innovations in, and an expansion of, the field of criminality. There is also the problem of defining at what point is something deemed criminal. In cyberspace, many Internet users make the distinction between "hackers" and "crackers" (the latter of which are criminals, the former of which claim they are not and argue they are merely leaving their digital calling card). Well-known hackers (such as

the Russian "Megazoid") claim they are not in it for the money but for the intellectual challenge (Sweeting, 1997). No one really knows for sure how big the problem is. The US legal system estimates the problem to be $2 billion, the FBI estimates it to be $5 billion and Europol estimates it to be $7.8 billion (Equinoxe, 1997).

Stanley Rifkin and Angelo Lamberti were probably the first notable cyber-bankrobbers when they stole $10.2 million and $8 million respectively from large corporations (Security Pacific in the US; Prudential Bache in the UK) (Equinoxe, 1997). Both were inside jobs and both received long jail sentences. A more recent infamous case has involved Citibank in New York (which is the largest bank in the world). The bank was defrauded of $10.7 million dollars by an anonymous hacker who took the money in 40 separate "break-ins" over a three-month period. Citibank took the decision to keep the problem internal as they presumed there would have been a severe loss of customer confidence.

Thanks to a 200-strong worldwide team they identified a Russian couple (Mr and Mrs Korolkov) living in San Francisco who were withdrawing the money from a bank account in Argentina. Catching these two individuals led them to Vladimir Veronin who was laundering the money in Holland. Voronin's calls were then traced to an office in St. Petersburg where Vladimir Levin, a 21-year-old software writer (now 27) was arrested in connection with this fraud (Sweeting, 1997). He was originally put in Brixton Prison but since September 5, 1997 he has been held in New York's Metropolitan Correction Centre and he is currently awaiting trial. One of the major problems with Levin is deciding on where the trial will be since the cybercrimes he is alleged to have committed are in a number of countries including Russia and the US! Even if Levin is successfully tried, there are so many other hackers to tap into unsafe security systems.

Hacking on the Internet: Kevin Poulsen and Paul Bedworth

Criminal hacking cases get a lot of publicity if (and when) they reach court. Two of the most high profile cases (first outlined in Sparrow and Griffiths, 1997) involve Kevin Poulsen (brought to trial in the US) and Paul Bedworth (brought to trial in the UK).

Case 1

Kevin Poulsen, a former computer programmer in Silicon Valley, was recently released from an American prison after spending five years behind bars after being convicted of computer hacking. He is now out on probation and has been told he must repay about £40,000 in damages. He has been told that he is too dangerous to be allowed behind a keyboard again. His crime was hacking telephone systems where he blocked the telephone phone lines of radio stations so that he himself could ring through unchallenged and win the on-air competitions for him and his associates – Ron Austin and Justin Petersen (McClellan,

1997). He was also alleged to have stolen sensitive Government documents although these charges were later dropped. He even appeared on the infamous US TV show *America's Most Wanted*.[1]

Case 2
Paul Bedworth gained illegal access to a number of mainframe computers and managed to cause over £500,000 worth of damage. He also caused panic among systems managers whose machines began to behave strangely, running up mysterious telephone bills. After a 16-day trial in March 1993, he was eventually acquitted on three counts of hacking because the jury accepted his claim that he was "addicted" to computers.

As you will have noticed, the verdicts given were highly discrepant. These two cases were chosen because they are at extreme ends of the sentencing spectrum. In the first case we have a man who appears to have caused little external damage and serves more time in prison than someone convicted of (say) manslaughter. In the second case we have a man who appears to have caused major damage but is acquitted due to his mitigating circumstances (ie, he was allegedly "addicted" to computers). It is not the intention to point out the "rights" and "wrongs" of each of these cases but merely point out that with such "new" crimes, the precedents are ever changing and can be highly contradictory.

There is little in the character of these cases that would allow us to claim that they are not the usual province of the criminal justice system. The use of computer technology provides a new slant on a range of offences with which the police service is already familiar and in relation to which it has a good deal of experience. But how are we to regard these new offenders? Is there a depth to their deception which ought to distinguish them from the more traditional criminal? (The criminal of which if we cannot claim understanding that we can at least claim familiarity.) As previously mentioned, attaching a degree of seriousness to an offence is no easy matter. It relies on a range of information and we would suggest at least a rudimentary understanding of the nature and consequences of the behaviour.

Concluding Comments: Issues for Policing
It is the author's contention that those in the criminal justice system (such as the police force) continue to rely on their own familiar scheme of reference when attempting to comprehend criminal behaviour. For the most part, the police have some understanding of the mode of operation, likely benefits to the offender and costs to the victim of the criminal activity presented before them. It is within this scheme of reference that judgments are ultimately made about the offender, the consequences of their offending behaviour and the desirability of a programme of intervention. The unfamiliarity of computer-related crime denies those in the criminal justice system an all-important access

to their own scheme of understanding. Moreover, the hitherto limited attention which such activities have attracted within academic circles have served only to negate the importance which computers are beginning to play in a range of criminal actions.

Despite media representations computer-related crime is not the futuristic indulgence of a corrupt intelligencia. The reality is that advancement in computer technology generally, and the increased availability of the Internet in particular, has provided for new innovations in, and an expansion of, the field of criminality. If computer-related crime is to occupy a position of increasing importance in the range of offending behaviour, then the police must be willing to familiarize themselves with such activities in order to make judgments about the offender and the nature of their offending.

Note

1. See the book by Jonathan Littman (1997) for a comprehensive account of the Kevin Poulsen case. It is also worth pointing out that many journalists appear to get Poulsen confused with another infamous US hacker Kevin Mitnick. These two hackers are not the same person. For a comprehensive account of the Mitnick case, see Littman (1996).

References

Audit Commision (1994) *Opportunity Makes a Thief: An Analysis of Computer Abuse*. London: HMSO.

Audit Commission (1998) *Ghost In The Machine: An Analysis of IT Fraud and Abuse*. London: HMSO.

Campbell, D. (1998) "Police tighten the Net", *The Guardian* (Online Section), September 17, p.2-3.

Campbell, M. (1998) "US at the mercy of cyber terrorists", *The Sunday Times*, May 17, p.26.

Charlesworth, A. (1995) "Never having to say sorry", *The Times Higher Educational Supplement* (Multimedia Section), May 10, p.viii.

Equinoxe (1997) *Superhighway Robbery* (Channel 4 Documentary). October 20, 1997.

Graham-Cumming, J. (1998) "Computing and the Net: Attack of the Trojan Smurfs", *The Guardian* (Online Section), March 12, p.5.

Grey, S. and Warren, P. (1997) "Hackers hit online bank revolution", *The Sunday Times*, May 25, p.5.

Griffiths, M.D. (1999) "Internet gambling and crime", The Police Journal, see article *ante*.

Hencke, D. (1999) "Code experts to crack internet crime", *The Guardian*, May 27, p.6.

Lillington, K. (1999) "Computing and the Net: And what kind of hacker are you?" *The Guardian* (Online Section), January 28, p.5.

Littman, J. (1996) *The Fugitive*. New York: Little, Brown & Co.

Littman, J. (1997) *The Watchman*, New York: Little, Brown & Co.

McClellan, J. (1997) "Hack meets hacker", *The Guardian* (Online Section), June 5, p.15.

Sparrow, P. and Griffiths, M.D. (1997) "Crime and IT: hacking and pornography on the internet", *Probation Journal*, 44, 144-147.

Sweeting, A. (1997) "Cybercops and robbers", *The Guardian* (Section Two). October 21, p.19.