Trends in Computer Crime

Richard E. Overill

INTRODUCTION
In this article the historical development of computer crime is traced and analysed. Some major examples of the phenomenon are examined with particular reference to financial and commercial information systems and institutions. The varied motivations of computer criminals are also considered. Finally, some lessons for today's financial and commercial IT communities are offered.

SCOPE AND DEFINITIONS
It is convenient to define computer crime as any criminal act which involves one or more computers either as the object of the crime or as accessories in its commission. Computer crime may then be subdivided into computer related crime (CRC) and computer assisted crime (CAC). In the former, the computer or its contents is the subject of the criminal act (eg hacking or denial of service attacks), while in the latter, the computer is merely an accessory in the commission of a crime which could at least in principle have been committed by other means (eg financial fraud or embezzlement). In this article, those areas of CRC and CAC covered by the UK Computer Misuse Act 1990 (CMA90) will be broadly surveyed; essentially, the Basic Hacking offence and the Unauthorised Modification offence of CMA90 relate to CRC, while the Ulterior Intent offence relates to CAC.

EARLY DAYS
The 1970s and early 1980s saw a number of seminal developments in the USA which laid the conceptual and practical foundations for future tools for computer crime. Around 1972, National Security Agency (NSA) spook Dan Edwards coined the term Trojan Horse, after the Greeks' ingenious scheme to end the siege of Troy. It denotes an apparently benign macro or utility with undocumented side-effects which may be security violating or palpably destructive. Trojans were occasionally referred to as Trapdoors because their effect can be similar, but the term 'trapdoor' properly denotes a back door or security loophole left in a system which can be exploited for access purposes.

By the early 1970s, in the context of the Cold War, the US military was sufficiently concerned about the security of sensitive information held in computer systems to mount a number of intrusion experiments. During late 1973 and early 1974, David Stryker, John Shore and Stanley Wilson of the Naval Research Laboratory subverted the Exec VIII operating system of a Sperry Rand Univac 1108 computer using security violating Trojan Horse techniques to obtain unauthorised and surreptitious access to classified information. Meanwhile, between 1972 and 1975, in a series of experiments for the US Air Force, Steven Lipner and Roger Schell used both trapdoors and Trojans to subvert the MIT-Honeywell Multics operating system into yielding up confidential information without leaving a trace.

In 1982, John Shoch and Jon Hupp from the Rank Xerox Palo Alto Research Center (RX-PARC) reported the first experiments with Worm programs. The aim of their work was to 'mop up' the idle time on a network of computers with useful computations in a manner transparent to the users. The worm program replicates itself in each node of the network and activates a portion of the desired computation if the node is quiescent; if a node becomes busy its computation is suspended and withdrawn.

The first computer virus was written as an experiment by Fred Cohen in November 1983 while a graduate student in Len Adelman's computer security class at the University of Southern California. As distinct from worms, viruses are parasitic replicators which must attach themselves to other machine instructions in order to be executed by the processor. The first virus infection 'in the wild', by the BRAIN virus from Pakistan, was recorded in 1986.

DEVELOPMENTS IN CRC
Basic hacking, or unauthorised access, has been practised by students, computer technophiles, commercial spies and counter-intelligence services, among others. Their motivations include recrea-
tion, intellectual curiosity, technical challenge, freedom of information, demonstrating security flaws, gaining commercial advantage and national security. Hacking may also be the logical precursor to other acts of CRC or CAC described below. Statistical profiles show that hackers are most likely to be male, aged 14-30, middle class and technically competent individuals. Some operate solitarily, others in groups (eg Chaos Computer Club, Legion of Doom, Masters of Deception, Vaxbusters, 8LG). To enter a system, either an existing trapdoor must be exploited or a valid password must be found. Passwords may be obtained remotely by 'social engineering' or locally by 'shoulder surfing' or 'trashing'; they may be guessed or systematically 'cracked'; they may be discovered locally using a 'password grabber' Trojan or remotely using a 'packet sniffer' program.

In the UK, there have been several examples of 'compulsive hacking'. Edward Austin Singh was arrested in October 1988 for hacking into 250 Prime and Vax computers world-wide from Surrey University and elsewhere during the previous eight years, using a sophisticated form of password grabber operating at the dial-up node. Although questioned by UK police and the US Secret Service, in the absence of CMA90 he was not prosecuted.

In the UK the courts have not always dealt severely with convicted logic bombers, despite the provisions of CMA90. For example, in November 1992 Gareth Hardy was convicted of planting a logic bomb at Chilworth Communications prior to his resignation in September 1990. One month later the logic bomb was triggered, damaging business critical files at a cost of over £30,000 to the company. Yet in December 1992 Hardy was sentenced to 140 hours community service and ordered to pay £3,000 compensation.

Unlike software bombs which are concealed, Trojan Horses need to be explicitly run by an unwitting user in order to perpetrate their hidden side-effects. They can be subdivided into those that dupe the user by offering something interesting and those that masquerade as an everyday utility. An example of the former type is the Aids Trojan (sometimes incorrectly referred to as a virus) which was concealed on diskettes labelled 'Aids Introductory Information Diskette' offering information on the human AIDS virus. The diskettes were mailed world-wide from London in December 1989, and when installed displayed a licence agreement and printed invoices for $189 or $378. Users were instructed to send money to a fictitious PC Cyborg Corporation at an actual PO Box number in Panama, otherwise their PC would cease to function. This was no empty threat; after a variable number of power-ups since its installation the Trojan rendered the PC inoperable. At the end of January 1990, Joseph Popp was arrested by the FBI in Ohio, extradited to London and charged with 11 counts of blackmail, but was found to be mentally unfit to stand trial. With over 20,000 Aids diskettes in the UK alone, it was estimated that this Trojan was intended to extort at least £6m.

Worm programs are replicators which do not necessarily damage information, but instead of performing useful computation as originally envis-
aged, they may simply consume system and network resources (processor cycles, memory capacity and communications bandwidth) by increasing exponentially in numbers until they render the system incapable of performing any useful work. This state of ‘electronic gridlock’ represents one form of ‘denial of service’ attack which, if launched at military Command and Control, National Information Infrastructure (NII), or commercial online transaction processing (OLTP) systems, could cause major disruption. A classic example occurred in November 1988 when Robert Morris Jr, a student at Cornell University, released a worm program which exploited trapdoors in the Unix system to spread itself through 6,200 computers on the Internet, bringing them to a standstill for up to a week at an estimated cost of over $100m.

Worm programs thus have the potential for sabotage, extortion or blackmail. So also do two recently described line-of-sight devices, the high intensity radiofrequency (HIRF) gun which can disrupt electronic circuits at close range, and the electromagnetic pulse (EMP) canon which can permanently damage computer circuits. Over 50 ‘electronic siege attacks’ are reported to have been launched on financial institutions and other organisations world-wide since January 1993, with an average extortion demand of £10m. While a HIRF gun has been cited as a possible tool in such attacks, an automated synchronised flood attack on the modem or PABX used for handling incoming transactions could be equally effective.

Being parasitic replacers, unlike worms, computer viruses must attach themselves to executable or command files, bootstrap sectors of disks, or macros within documents. Six generations of virus are now generally recognised: benign, self-encrypting, stealth, armoured, polymorphic and macro. By March 1997 over 12,000 individual viral strains were known, but only about a dozen were active ‘in the wild’ of which 49 per cent of infections were due to the Word Macro Concept virus first seen in summer 1995. As with software bombs, the trigger can be a date (eg Michelangelo’s birthday) or a condition (eg the 32nd power-up since infection), and the payload can vary from the irritating (eg playing a tune) to the devastating (eg formatting the hard disk). Different infection and concealment strategies have also been recorded, including ‘slow’ viruses which infect only files that are being legitimately modified (eg Starship), ‘fast’ infectors which infect every file that is opened (eg Dark Avenger), and multipartite or ‘tunneling’ viruses which exhibit a three-stage life cycle moving between executable file, hard disk bootstrap partition and main memory (eg Tequila).

The first virus author to be convicted under CMA90 was Christopher Pile (aka the Black Baron) who was sentenced to 18 months’ imprisonment in November 1996 on 11 counts, including the damage done by his Pathogen and Queeg polymorphic viruses at Microprose, Apricot Computers and Map Line Engineering which totalled almost £1m. Although the motivation in this case was apparently vandalism, the potential of viruses and related malicious codes for information warfare is also evident.

**DEVELOPMENTS IN CAC**

In October 1996, Bill Marlow, a security consultant with SAIC (Science Applications International Corporation) noted that in the USA the average bank stick-up nets $1,900 and is prosecuted 82 per cent of the time, whereas the average cybercrime nets $250,000 and less than 2 per cent are prosecuted. Estimates of the annual cost of cybercrime range from $2bn according to the American Bar Association, through $5bn according to the FBI, to $7.8bn according to Europol. The 1998 US CSI/FBI Computer Crime and Security Survey was based on responses from 520 security practitioners in US corporations, government agencies, financial institutions and universities. A major conclusion of this survey was that the frequency of outsider penetrations of these organisations (mainly via Internet connections) has now overtaken the frequency of insider penetrations. The total financial losses for the 241 organisations able to quantify them had grown by 36 per cent since the 1997 survey.

In the UK, four national information security breaches surveys have been published by the National Computing Centre (NCC) in 1992, 1994, 1996 and 1998 respectively. The 1998 survey employed different categories of logical security breaches from the three preceding surveys rendering meaningful comparisons of fraud and hacking incidences impossible. The average reported cost of each security breach was over £7,000 but further investigation revealed that the true cost was as much as three times higher. In the
1996 survey, only 3 per cent of respondents reported incidents of computer fraud, with a fraud of £650,000 being the largest single logical security breach reported, compared with 2.6 per cent in 1994 and 5 per cent in 1992. However, the 1998 Audit Commission report\(^{31}\) found that one-half of public bodies and one-third of companies in the UK had suffered from computer fraud during the previous four years. Furthermore, a survey of the 120 largest organisations in the UK conducted by PA Consulting Group in 1996\(^{25}\) concluded that the cost of fraud to UK businesses alone is some £80m per day, or £20bn per annum (£10bn per annum detected and a similar amount conjectured). Fraud accounted for losses of up to 3.5 per cent of annual turnover and up to 200 per cent of profits. The figures varied little across the different business sectors, but the numbers and relative sizes of the frauds differed: in banking, a small number of large frauds predominates whereas the converse holds in retail, telecommunications and government; in insurance there is a mixture of both types of fraud.

In the 1992 NCC survey, 7 per cent of respondents reported internal access breaches and 4 per cent reported external access breaches. The corresponding figures for 1994 were 4.6 per cent and 2.5 per cent respectively; the 1996 figures were 8 per cent and 3 per cent respectively. In the 1998 NCC survey, the greatest risk of security breaches was found to arise from the activities of personnel within organisations which accounted for nearly 52 per cent of all (physical and logical) security breaches detected. This confirms the findings of the 1996 survey of US corporate security directors by Carter & Katz that 'the primary threat came from full-time employees, followed by part-time and contract employees, with computer crackers (hackers) a close third.'\(^{21}\) It also mirrors one result of the 1998 CSI/FBI survey\(^{26}\) which found that easily the greatest single source of financial loss (almost 37 per cent) was attributable to unauthorised insider access.

The Audit Commission report of 1994\(^{25}\) concluded that over 50 per cent of all detected security breaches were discovered by accident and only 2 per cent of detections were directly attributable to security activities. This parallels the finding of a 1996 Pentagon report in which the US Defense Information Systems Agency (DISA) subjected 30,234 unclassified Department of Defense (DoD) computer systems to cyberattack; 96 per cent of the system managers were unaware that they had suffered an intrusion.\(^{26}\) A similar figure also applies to commercial information systems.\(^{27}\)

The difficulty in arriving at reliable estimates from such surveys is exacerbated by the well-attested belief that over 90 per cent of all detected computer fraud goes unreported\(^{28}\) as institutions seek to preserve at all costs the confidence of their clients in their reputations for secure practice,\(^{29}\) a stance which causes exasperation to both the Department of Trade and Industry (DTI) and the Metropolitan Police Computer Crime Unit (CCU).\(^{30}\)

An early US example of computer-assisted fraud occurred on 25th October, 1978, when Stanley Rifkin, a professor of Social Computing at the University of Southern California and a computer consultant at the Los Angeles HQ of the Security Pacific Bank, transferred $10.2m to an account in New York and thence to Switzerland, where he used it to buy diamonds. He used a combination of insider information and social engineering to accomplish his task; by first obtaining the electronic funds transfer (EFT) password of the day, which was not managed securely by the employees in the money transfer room, and then making an external call from a public telephone posing as a bona fide client branch manager requesting a money transfer. Following an investigation by two FBI special agents, he was finally convicted and sentenced to nine years' imprisonment.\(^{31}\)

An interesting example of UK computer-assisted fraud by an insider was reported in 1985.\(^{32}\) One of the major London clearing banks suffered a £6m loss in July 1984 when an employee programmer managed to divert to his own bank account in Switzerland ten EFT payments destined for other international banks. He did this by gaining unauthorised access to the live transaction files served by the bank's front-end processor and altering the payment codes. Naturally an audit took place when the payments did not arrive at their expected destinations, and when their actual destination was traced, the employee offered to return half the money if the bank would promise not to bring charges against him. As a 'sweetener' he would also explain how he did it so that the security loophole could be closed. The bank agreed.

In the three months between June and September 1994, the world's largest bank, Citibank of
New York, suffered a series of some 40 cyber-raids, totalling $10.7m, on accounts held by, among others, the Philippine National Bank in Hong Kong and the Argentinean stockbrokers InvestCapital SA. The attacks were launched via multi-link international telephone calls which were eventually traced to Russia, to the office of AO Saturn in downtown St Petersburg. Vladimir Levin, a 24-year-old programmer of business accounting systems and a former Red Star graduate of the Leningrad Technical Institute, was later implicated by another worker at the office. While travelling through Stansted Airport allegedly on route to a computer fair in Germany he was arrested and remanded in Brixton prison from where he was extradited to the USA on 5th September, 1997, to await trial in New York.33

It is interesting to note that during two decades the value of a typical electronic funds fraud has remained roughly constant in the region of $10m, despite the manifest changes in technology which have occurred over that period. It is also worth recalling that the average extortion demand in electronic siege attacks on financial institutions is reported to be of a similar magnitude.34 This figure may therefore be useful as a realistic benchmark for performing cost–benefit analyses to determine the levels of digital security required by such an institution.

Today, with turnovers of up to $500bn per day, major banks must realise the enormous temptation faced by an employee who discovers a flaw in either the human security procedures or the computer security controls. Equally, they need to be highly sceptical of their current capabilities to protect themselves from, detect and react to an ever-expanding repertoire of sophisticated external attacks, whose origins and destinations are both global. To quote a representative of the Metropolitan Police: ‘Any medium that presents businesses with opportunities to make money will present criminals with opportunities to take it off them.’35

**CONCLUSIONS**
What lessons can be drawn for today’s financial and commercial IT communities? Both CRC and CAC are continuing to develop apace and ‘the price of freedom is eternal vigilance’, both externally and internally. The existence of CMA90 has not of itself stemmed the tide of computer crime and it has at times proved difficult to operate. The potential weakness of the human component of all security systems is not always adequately recognised or effectively managed. Finally, 25 years after the earliest localised computer security experiments, financial and commercial information systems and their network infrastructures remain disturbingly vulnerable to increasingly globalised, focused and concerted modes of external attack.

**REFERENCES**
(12) Schoch and Hupp, ref. 4.
(16) NCSA 1997 computer virus prevalence survey, at URL: http://www.antivirus.com


(24) 'Ghost in the Machine', ref. 21.


(33) 'Superhighway Robbery', ref. 18.


---

CRIMINAL PROCEDURE

R v Crown Court at Southwark, ex parte Bowles

Rinita L. Sarker

The benefits of accountants seeking prompt independent legal advice to protect both themselves and their clients during criminal investigations has been reinforced by the recent House of Lords case of R v Crown Court at Southwark, ex parte Bowles.¹

The case was possibly every accountant's, not to mention their insurers', worst nightmare. The accountant in question was forced by a court order to produce confidential documents relating to her clients to the police, who were investigating the clients for various offences of dishonesty. The dishonesty also extended to deceiving the accountant with bogus information regarding the company accounts.

In such situations, accountants are torn by conflicting duties — the duty of confidentiality towards their clients with the threat of costly litigation for breaches of confidentiality juxtaposed with the equally important public duty to report fraud to the appropriate authorities and assist the police in the proper prosecution of such cases.

The central issue in R v Crown Court at South-

---

Dr Richard E. Overill FBCS, FIMA, Senior Lecturer in Computer Science, Algorithm Design Group, Department of Computer Science and International Centre for Security Analysis, King's College London.