ISSN. 1363-6650

MARCH 1998
Issue 15

International Journal of FORENSIC COMPUTING™

Contents

International Journal of Forensic Computing

Third Floor, Colonnade House,
High Street, Worthing,
West Sussex, UK
BN11 1NZ

Tel: +44 (0) 1903 209226
Fax: +44 (0) 1903 233545
e-mail:ijfc@pavilion.co.uk
http://www.forensic-computing.com

Comment

If you deposited £10,000 in your bank, would you expect the staff to leave it in an unlocked safe? Of course not – no one can be that idiotic.

Yet firms, organisations and government groups across the world are doing just that, often with much more than just money at stake. They seem oblivious of the risks they run by leaving their sophisticated computer networks unprotected, the technological equivalent of leaving the vault door wide open.

We are only now beginning to see the real threat that hackers pose to modern society, and the future could be a scary place unless we take action now.

Cyber criminals can wreak havoc using easily available and often quite basic equipment to illegally break into computers holding just about anything. With just a few mouse clicks and keystrokes almost any type of data can be accessed if the security is not up to scratch, from company databases to military secrets.

At a recent conference on computers and privacy (see page 14) delegates heard how one hacker had easily gained entry to a wide range of systems, ranging from remote air conditioning systems to the local fire department.

While altering the temperature in an office building miles away could seem like a schoolboy prank, dispatching fire engines on a fake call out could end up costing lives. The hacker in this case reported the gaping security holes to the relevant authorities in the hope they would be patched up, but many others would only too gleefully take advantage.

While most people would regard any form of hacking as malicious and irresponsible, many of those behind the computer attacks see themselves as renegade cyber warriors waging a high-tech war of minds with officialdom. They brea into systems not necessarily to perpetrat another crime, such as stealing mone or fraud, but merely because they see th target as a challenge to crack. These type of hackers far outnumber those wh make the headlines by transferring mi lions in electronic accounts, but the could also be far more dangerous.

Hacking is no longer just the preserv of the "techno nerd" stereotype belove of the media. Using a £1,000 compute a modem and software and instruction pulled off the Internet, just about any one can embark on a life of crime.

The US military has revealed tha even its supposedly secure computer sys tems were breached, and so far the sus pects appear to be schoolboys flexin their fledgling computer know-how. people like these can achieve such dev astating results, the threat of hardene and experience hackers is immense.

The good news is that police force and law enforcement across the glob have finally woken up to the possibil ties, and are slowly getting up to scratc Investigative equipment and technique are continually improving as is the ex perience and abilities of the officer themselves, and criminals are being pu behind bars.

It's important that the authoritie don't rest on their laurels – by their ver nature hackers will often be one ste ahead of those tracing them – but at leas the equation is rather less one sided tha before. The only way hacking can be e fectively tackled is by a two-pronged a tack of education and investigation.

Hacking is a unique crime in our so ciety, and one which could potentiall cause immense damage. If we take it se riously we may well turn the tide.

Articles are published on the understanding that publication is not taken to imply endorsement of the views therein by t Publisher or Editorial Team or members of the Advisory Board of the Journal. Courses of action described in the Journal relation to one set of circumstances will not necessarily be appropriate for a different set of circumstances.

Accordingly, readers should take their own independent specialist advice before proceeding on any project or course action and any failure to do so is at their own risk. No responsibility is assumed by the Publisher or Editorial Team members of the Advisory Board for any loss or damage to persons or property as a matter of contract, negligence (save respect of liability for death or personal injury arising out of any negligence) or otherwise, or from any use or operation any methods, products, instructions or ideas contained in the material herein. Whilst all reasonable care is taken, neither t Publisher, nor the Editorial Team, nor members of the Advisory Board can be held legally responsible for any errors articles or listings. Upon submission of an article, the author will be requested to transfer copyright of the article to t Publisher.

News

New hacker busting unit to be set up

The Justice Department in the US wants to set up a government centre to clamp down on computer crime.

US Attorney General Janet Reno has unveiled plans to form a unit, called the National Infrastructure Protection Center. Reno said growth and development in technology, computer systems and the national information infrastructure are more vulnerable than ever to cyber attack.

Law enforcers, she said, "are used to robbers and guns. There are now new criminals out there that don't have guns. They have computers and many have other weapons of mass destruction."

She emphasised that the unit would focus on everything from attacks by individuals on specific computers to terrorists both domestically and internationally who aim to bring down entire systems, such as power or telephone grids.

The centre will be run mainly by the FBI and will work together with other federal, state, and local law enforcement agencies. It will also aim to pull in the private and commercial sector.

The lab will also develop international co-operation in the fight against cyber attacks, a message that was brought home in the recent G8 International Summit on computer crime.

Developing technology "brings us a new world of incredible opportunity and of daunting challenges," Reno said.

"The government, including the Department of Justice, is facing these problems head on but we know full well we cannot do it alone.

"It must be based on the idea that infrastructure protection requires we work together like never before."

The centre will seek to act as a national clearinghouse for computer crime, and perhaps be directly linked to various Computer Emergency Response Teams throughout the country to monitor and assess potential threats.

Reno said: "Through partnerships among federal agencies and private industry, the NIPC will be able to achieve the broadest possible sharing of information and comprehensive analyses of potential threats and vulnerabilities."

It also will provide training for local law enforcement officials. Reno stressed that stepped-up enforcement will not violate the rights of individual. She said: "We must not and cannot sacrifice any Constitutional protections."

While the unit was planned before news about an apparent break-in to Pentagon computers, (see page ?) the fact that it's being announced is not being seen as coincidental.

The Pentagon incident "is a perfect example as to why this is such an important issue at this building," a Justice Department official said.

"The attorney general recognised that that's the new frontier of crime, and if we don't set up a structure for it, we're never going to be able to deal with it."

Reno will ask Congress for $64 million in increased funding to help pay for the centre and staff it with 125 people, including six investigative squads and more federal prosecutors specialising in cybercrime. Regardless of whether the centre gets all the requested funding, it will go ahead, said a DOJ official.

The centre will be an outgrowth of the FBI's Computer Investigations and Infrastructure Threat Assessment Center, which was developed after a report was issued by President Clinton's Commission on Critical Infrastructure Protection.

It will not only focus on government break-ins but also those in the private sector and will cover any crimes perpetrated over the wires, including those involving telephones.

Hacker broke into business computers

A former Kennedy Space Center worker has agreed to plead guilty to using his computer to hack into several businesses.

Shawn Hillis, 26, of Orlando, is charged with one count of computer fraud. According to court documents, Hillis is charged with unlawfully accessing a computer in July 1997 at the Institute for Simulation and Training at the University of Central Florida.

An institute spokesman said a file containing passwords was downloaded during the incident, but the institute lost no critical or sensitive information. Hillis worked for NASA subcontractor Lockheed Martin at the time.

Under sentencing guidelines, Hillis faces six to 12 months of prison, home confinement or probation. He can also receive a lower sentence in exchange for co-operating with investigators.

The document states that Hillis must make restitution to other victims. They include DiamondStar Network of Orlando, a Time Warner Communications office in Maitland, Internet Access Group of Altamonte Springs and Junto Net Press of Winter Park.

Hillis' attorney, Mark Blechman, said the Orlando man had no malicious or criminal intent when he broke into other companies' computers.

Blechman said Hillis was studying NASA's computer security when he tried to test the security of several one-time employers. Hillis formerly worked for the institute and Time Warner.

Blechman said the investigation began after NASA computer security officials found several large data files stored in Hillis' working folder.

"He didn't disclose what he found to anyone. When he was confronted, he gave a full confession," Blechman said. "This is just a young guy who made a mistake."

Programmer charged with sabotage

A computer programmer has been charged with allegedly costing a company up to $12 million by deleting important files.

In a computer sabotage case that the US Secret Service sees as one of the most costly in history, a disgruntled computer programmer faces up to 15 years in prison. He is charged with permanently deleting a production system critical to the operations of Omega Engineering Corp and of stealing $50,000 in computer equipment to commit the act.

Timothy Lloyd, 30, of Wilmington, Delaware, has been arraigned on the two-count indictment in federal district court, with a trial date set for April 20.

Danny Spriggs, the Secret Service

agent who headed up the investigation in the case, said that the damage from a "computer time bomb" allegedly unleashed by Lloyd has cost Omega up to $10 to $12 million in lost contracts.

Al DiFransecso, director of human resources for Omega, alleged that Lloyd intentionally deleted Omega's CNC (Computer Numerical Control) program files about 20 days after leaving Omega on July 10, 1996.

On the first count in the two-count indictment, Lloyd is charged with using a computer command to delete "all the design and production programs that Omega needed to operate."

On the second count, he is charged with stealing $50,000 in equipment from Omega, and with transporting the equipment across state lines from Omega's headquarters office in Bridgeport, New Jersey.

Omega produces instruments and control systems used worldwide and customers include NASA and the US Navy.

Spriggs said that the Secret Service was called in to investigate the case mainly for two reasons. Omega is a federal contractor; and Lloyd's alleged criminal activities crossed state lines.

During the course of the investigation, Spriggs said the Secret Service narrowed down the list of alleged perpetrators to individuals possessing access codes to Omega's CNC program files.

Following a finding of "probable cause," the Secret Service searched Lloyd's home in Delaware, retrieving evidence that included a computer hard drive, in addition to a back-up tape.

"If the back-up tape had not been deleted (prior to its retrieval), it could have been used to (restore) the system," he said.

DiFransesco acknowledged that Omega did not change the access codes to the CNC files following Lloyd's departure from the company.

"Hindsight is 20/20. There was no reason at the time to think that something like this would happen," he said. But, he added, Omega has since "completely replaced the system," dealing with the issue of access codes during the process.

If convicted, Lloyd faces a sentence of up to five years in prison on the first count, and ten years in prison on the second count. Each count also carries a maximum fine of from $250,000 to "twice the loss or gain from the crime." In addition, if Lloyd is convicted, he could be ordered by the court to make restitution to Omega Corp.

DES 56-bit encryption cracked

A team of university students, programmers, and scientists used loosely networked computers to crack a message protected by the 56-bit US Data Encryption Standard in a record 36 days.

The massive effort smashed a 90-day DES-cracking benchmark set in 1997 and the decoded message read "Many hands make light work".

Cutting the DES-cracking record to less than half last year's time took 22,000 participants, who made the idle time of more than 50,000 central processing units (CPUs) available to the project until the key was found.

The team, running as a group named distributed.net, used a cryptographic massive attack to crunch away at approximately 72 quadrillion possible keys.

Before hitting the right one, the team had searched 61 quadrillion, 254 trillion keys at a peak rate of 26 trillion keys per second.

"We're very appreciative of all the volunteers who offered their time and their computer's idle processing time to help crack the code," said David McNett, distributed.net co-founder and logistics co-ordinator.

It was a machine in the US running an Alpha CPU (central processing unit) that finally hit the right key. By then the team had muscled its way through 85 per cent of the possible total.

The distributed.net team started seeking a solution right after DES Challenge II was announced at RSA's Data Security Conference in San Francisco, January 13. The challenge seems now to have become an annual affair.

US company RSA Data Security, a subsidiary of Security Dynamics Technologies Inc, says DES encryption is inadequate, despite US government assurances it is good enough for most purposes. When the firm announced DES Challenge II it said the aim was no longer just to prove DES could be beaten by hackers, it was to set a new speed record.

Jim Bidzos, president of RSA, said that the firm would continue sponsoring the challenge as long as it takes for the US government to "rethink our current encryption export policies and standards for use in commercial applications."

RSA's Web site is at http://www.rsa.com

China to police viruses to cut crime

In a bid to stem the tide of computer viruses, the Chinese government will put the nation's police force in charge of virus research.

Businesses that want to study viruses or develop anti virus software must register with the Ministry of Public Security, according to the Xinhua News Agency.

Individuals and companies that have a record of computer-related crimes will be prohibited from collecting or storing viruses for two years, Xinhua said.

The announcement comes at a time when the Chinese government is still discussing how to control Internet users from "subversive material" and pornography while still promoting the medium for commerce and research.

The government released a range of rules to prevent the spread of "harmful information" on the Net and says it will impose fines and other penalties on those who violate them.

The Internet is continuing to grow in China, with 620,000 subscriptions, a figure likely to double within six months.

Delegating authority over virus research to the police force will be a daunting task, and controlling viruses may prove to be harder than controlling the Internet. Even the ministry itself has addressed this difficulty.

"It is difficult to detect and crack down on computer crimes, which can seriously harm social security and cause big economic losses," Zhu Entao of the MPS said in the Xinhua report.

Virus researchers elsewhere in the world are sceptical of the effectiveness of the move. Trying to prevent a new virus from a network would be like trying to prevent the flu, said Gregory Sorkin of IBM's Watson Research Center.

"Since virus technology changes so rapidly, it's unlikely that any specific governmental requirements would stay relevant for long," added Sorkin.

"It is hard to control virus writers, since once it spreads, a computer virus - just like a flu virus - is hard to trace back to a source."

Net security risk

The Internet could be the major security challenge of the next millennium, according to a new watchdog report which also warns that computer fraud is on the increase.

New dangers are posed by connecting company networks to the Net and by modern digital telephone systems, which are the latest potential target for fraudsters according to the Audit Commission in the UK.

The independent public spending watchdog says that 45 per cent of organisations are affected and that people in management posts commit a quarter of computer fraud.

According to the report, the key risks facing businesses are computer viruses, fraud by employees and attacks by computer hackers. It says viruses cost an average £1,700 per computer to put right.

The report says that businesses are getting better at setting up their defence but adds that "the overall position shows little improvement", suggesting that fraudsters are also becoming more sophisticated.

With businesses and governments increasingly more dependent on computers and digital technology, security should be a top priority for those wanting to minimise risks, says the report.

Paul Vevers, director of audit support at the Commission, said it was not always the stereotyped "computer geeks" who caused the problems.

He accused some big businesses of not taking the problem as seriously as they should. "We have seen examples where people make use of a computer system to get themselves total control of a firm's financial process," he said.

"They become responsible for making orders and invoices and signing cheques and it's easy for them to make false ones and send the money to a bank account.

"We last did a survey like this three years ago and we are not seeing the signs of activity that we ought to be. A large number of organisations are not taking it as seriously as they should.

"There is this attitude among senior managers that it is a complicated issue, but once you have done a proper risk assessment, implementing action is not particularly difficult."

Microsoft warn of piracy scam

Computer giant Microsoft has revealed what it says is the latest software piracy technique.

A limited number of resellers who participate in Microsoft Easy Fulfilment program are selling what Microsoft calls "components" which are ordered after a volume licensing agreement.

Customers are charged for the component, but Microsoft does not receive a percentage, the company said.

Through MEF, resellers ordering supplemental components receive a full version of a product such as the Windows operating system or a version of Microsoft Office.

However, the programs are called components because they ship without documentation, registration forms or standard packaging.

Components are not meant for retail distribution, but Microsoft said some resellers illegally sell MEF components into the retail channel at full or discounted prices and that the software is also being copied and then distributed into retail channels. Microsoft said any of its software that does not have standard labelling, packaging, registration forms or manuals should return it and ask for an explanation.

Year 2000 could mean law suits

A summit in the US on the millennium bug problem has heard that agencies are worried about being sued in the event of problems.

The first-ever California Statewide Intergovernmental Summit on Y2K, sponsored by the California Department of Information Technology and Government Technology magazine, examined a wide-range of issues.

California Chief Information Officer John Thomas Flynn addressed a crowd of nearly 600, including local and federal government employees and representatives from technology companies.

"Success will be the silence we hear on Jan. 1, 2000," Flynn said. "To get there, co-operation will be more important than ever."

The fear of litigation against government agencies for problems caused by systems that malfunction occupied many of the discussions during the summit.

Russ Bohart, director of the California Health and Welfare Agency Data Center, said litigation is the "most significant risk" surrounding the Y2K problem. "Although some states, like Nevada and Washington, have used legislation to protect them from Y2K liability - and California has some similar bills moving around the legislature - we in government can still expect to be sued - there are no ifs, ands or buts about it."

"Ultimately, this is going to become a legal issue," said Shirley Malia, deputy chief information officer for the US Department of Labor.

Fewer virus cases

The Australian corporate virus infection rate appears to be dropping, according to a survey.

The survey, by Computer Associates/Cheyenne Australia, polled 171 Australian and New Zealand organisations with 100 or more networked PCs.

In 1996, the Cheyenne anti-virus survey found that 90 per cent of its survey base had a virus attack. The 1997 survey found that 60 per cent of respondents had a virus attack in the first 11 months of the year, while 17 per cent reported "previous virus experience."

The most virulent digital viruses were Word macro viruses styled on the infamous Word.Concept virus, while the A-CAP virus came in second, and Junkie was third.

The growth area for virus transmission is by e-mail attachments - this method of attack rose from 15 per cent in 1996 to 35 per cent in 1997.

Transmission by floppy disk remained stable at 35 per cent of infections.

But almost 40 per cent of respondents with external network connections had no firewall in place. Of the 60 per cent that had a data barricade, 67 per cent regarded their firewalls as "very good or good." However, 40 per cent said they were unhappy with their data barricades in some way.

The top complaint was that firewalls are too complex. Respondents also said their equipment was missing features, hard to manage and too expensive.

AOL settles class action law suit

Internet service provider America Online has settled a class-action lawsuit filled against it by angry subscribers.

A judge in Illinois gave the go ahead for the firm to come to an agreement with members who found it difficult to access AOL's network in early 1997.

The class-action suits, one among several filed last year against the world's largest ISP, were brought by AOL members angry with the company over the inability to log on. AOL's system became overloaded after it switched its main membership-billing plan from a monthly fee plus-hourly subscription model to an unlimited usage plan.

Cook County Circuit Court Judge Stephen Schiller wrote that AOL subscribers who experienced that difficulty in February and March of last year were entitled to refunds or credits.

AOL spokesperson Tricia Primrose said that the Chicago-based suit overtook the other suits filed against it, and "became the certified class on suits related to access." She also said AOL views the settlement as a "fair and reasonable resolution" to the legal difficulty.

AOL's access problems also got it into trouble with most US states' attorney generals. After AOL members from their respective states could not get through to AOL last year, the attorney generals reached a settlement, where AOL would refund customers up to two months worth of fees.

The settlement avoided a consumer fraud suit that the attorney generals threatened to file, and called for a graduated scale of refunds. AOL also agreed to disclose in its advertising that access to its service might be unintentionally restricted, especially during peak hours.

Clinton wants more Internet spending

President Clinton is asking Congress for £110 million funding for an Internet project that promises greatly increased network speeds.

The "Next Generation Internet," to cost $500 million or more over five years, will operate at speeds up to 1,000 times faster than today's Internet.

But some lawmakers complained last year that the project lacked focus and might improperly spend US funds on computer networking infrastructures that should be paid for by the private sector.

To build support on Capitol Hill, the White House has planned to rally universities and research centres that stand to benefit from the program.

After last year's funding request ran into difficulty, the administration prepared a 75-page outline of the program's goals.

"While there have been some bumpy roads these last couple of years, I think we have convergence now on what the role of the federal government is in making these advances," presidential Science adviser John Gibbons said.

Last year's proposal included provisions to encourage development of an encryption scheme allowing covert monitoring of all communications by law enforcement officials - an approach strongly opposed by some in Congress.

EU set to launch charter plan

The European Commission has launched a proposal aimed at strengthening global co-operation on the legal and technical issues surrounding the Internet.

The European Union's executive will formally propose an "international communications charter," to be drawn up by the end of 1999, that would provide a blueprint for the treatment of questions ranging from data protection and copyright to taxation and pornography.

"This proposal argues that an international framework is necessary which can foster the development of the global electronic marketplace by removing obstacles and uncertainties for businesses and consumers," the draft text says.

The proposals will attempt to define a number of issues, including jurisdiction, copyright, data protection and the protocols for Web commerce. As a principle, the legal frameworks of the "off-line world" should apply to the "on-line world," the Commission said.

"However, the technical possibilities of open networks like the Internet are already beginning to put legal structures to the test in various fields of existing law."

"This is a global and fast changing business and the regulatory response must be rapid in order to be effective," said EU Trade Commissioner Sir Leon Brittan. "Otherwise we'll end up dealing with yesterday's issues."

The initiative has been closely watched by the computer and communications industries, which feared a new level of government intervention, since Bangemann suggested it in September.

EU Telecommunications Commissioner Martin Bangemann said, "If we don't agree to terms globally, each of us will try to set our own regulations, which will lead to over regulation."

The commission proposes to discuss the charter idea with other countries and to organise a meeting with industry later this year.

Net threat down under meeting hears

Australia's national security is at risk from Internet attacks according to an air force expert on information warfare.

Squadron Leader Nigel Thompson, officer-in-charge of the RAAF's information assurance centre, said that criminals and cyber terrorists could use the Internet as a devastating weapon.

He told an Australian Institute of Criminology conference on Internet crime the classic method of attacking the Internet was to shut it down.

But other forms of disruption could include penetrating a user's equipment to harm its performance and saturating it with unwanted traffic such as e-mail.

Non-lethal terrorism through the Internet, such as denying basic services or sabotage of manufacturing, were a real threat, Thompson said.

"For Australia the Sydney 2000 Olympics could provide a period of heightened sensitivity to cyber-terrorism and any of the numerous issues of discontent in the domestic, regional or global communities could provide a motive," he said.

He added that the world's military forces were making greater use of the Internet, making them vulnerable to attacks on their data and intelligence.

"Military services should remain capable of operating effectively without access to the Internet and should be capable of protecting their military capabilities from damage from Internet attacks," Thompson said.

And he warned that non-military targets, such as transport and communications industries, were at risk as well.

But an attacker bypassing the military altogether in an attack known as Iwar or Infrastructure Warfare was perhaps most dangerous.

"Possibly the greatest danger to a nation is where it exposes itself widely to attack via the Internet - exposed in such a way that the nation's interests can be attacked directly via the Internet where defences may be totally inadequate," Thompson said.

"While the ADF (Australian Defence Forces), the Australian Federal Police, customs and immigration are defending our coast, ports of entry and territories, who is protecting the data highways into and within Australia?"

He said the military were not practised at dealing with those operating through the "virtual realm" and could not readily counter objects defying physical detection or description.

"Via the Internet all elements of our national power are exposed and hence our national security is vulnerable to attack from the Internet."

He said the key to countering such attacks and cyber-terrorism was to curtail dependency on the Internet, to respect the problem and plan for it and to adequately protect information networks, Mr Thompson said.

Other delegates warned of the threat of computer crime. Security researchers Russell Smith and Peter Grabosky said in a study released at the conference that the potential for computer terrorism includes hijacking air traffic control systems to crash planes and cutting power supplies.

They said in the report: "Techniques of 'information warfare' may be employed by terrorist organisations with no less effect than the traditional bomb. Widespread death or injury has yet to occur as a result of hacking."

"Some people regard their information systems with a degree of nonchalance," Grabosky said. "It's the contemporary equivalent of leaving your home with the door unlocked.

"We're at the dawn of an age of electronic commerce, and ensuring it can flourish while minimising the risks of illicit exploitation...is a real challenge."

Law banning workers from porn is axed

A federal judge in the US has struck down a law that barred state employees from using state-owned computers to look at explicit Internet sites.

District Judge Leonie M. Brinkema issued the ruling in a lawsuit filed by six college professors and the American Civil Liberties Union.

The professors filed the suit in May, saying they needed access to explicit sites for research and that the law took away their free speech rights.

"I'm obviously delighted," said plaintiff Terry Meyers, an English professor at the College of William & Mary.

"I've felt all along that it wasn't appropriate for the government to dictate to citizens what they can read and can't read and what medium they can use to do it."

Under the law, professors and other state employees who wanted to download, post, transmit or store sexually explicit material on their computers had to first ask for approval in writing from agency heads, such as a university official. Such requests would be made available to the general public.

The law, which took effect in July 1996, was intended to prevent state workers from wasting time and state money on inappropriate Internet use; it was not aimed at professors doing research, backers of the law say.

But because the law defined nudity as sexually explicit material, it could affect material professors use in such courses as art history, human sexuality, English literature and psychology, Virginia American Civil Liberties Union director Kent Willis said.

The six professors argued that under the law, it was technically illegal for them to do Internet research on nude portraits or classic literature that uses erotic language, even though the same material is readily available in the library.

"We have now heard from 18 federal judges in four separate cases that these kinds of restrictions of online speech are unconstitutional," said Ann Beeson, ACLU attorney.

"How many more challenges do we have to bring before lawmakers stop trying to impose unconstitutional restrictions on virtual speech?"

Beeson noted that the US Senate recently held hearings on two pieces of legislation seeking to censor "indecent" speech from the Internet.

One bill, introduced by Sen. Dan Coats (R-Indiana), would punish commercial; online distributors of material deemed "harmful to minors" with up to six months in jail and a $50,000 fine.

Another, introduced by Sen. John McCain, would require schools and libraries to block "indecent" Internet sites or lose federal funds for online programs.

Hacker admits stealing millions

A Russian hacker who broke into a bank's computers and transferred millions of dollars to accounts all over the globe has pleaded guilty.

Vladimir Levin admitted taking

money from Citibank using the computer network and now faces up to five years in prison.

Levin's, 26 at the time, got into the bank's computer system from St. Petersburg four years ago. He used identification codes and passwords belonging to Citibank corporate customers to transfer $3.7 million to accounts in banks in Finland, the United States, Germany, Israel and the Netherlands. Citibank recovered all but about $400,000.

After the Levin break-in, Citibank upgraded security on the cash management system that allowed corporate customers to move money around the world. Now, all customers must use a calculator-sized card that gives them a new password each time they use the system.

A spokesman for Citibank said: "We are grateful to the Federal Bureau of Investigation, international law enforcement officials and the U.S. Attorney's Office for their work on our behalf.

"Citibank is proud of the technical skills and ingenuity of a number of Citibankers who were instrumental in detecting, tracking and stopping this criminal and his accomplices.

"Since this incident occurred Citibank has enhanced security on the system compromised and has experienced no other such incidents. No customers lost any money due to this fraud.

"Citibank takes fraud attempts of any kind seriously and will aggressively use all resources to pursue and prosecute anyone who attempts unauthorised entry into its systems.

Net policy forum

The Internet may draw increasing levels of government scrutiny if the industry does not regulate itself, said a speaker at the Internet Law and Policy Forum.

Governments throughout the world are becoming more interested in regulating the Internet, said Alec Szibo, a partner at the Vancouver law firm of Gowling, Strathy & Henderson. Szibo told delegates that while the industry's attempts at self-regulation have staved off government intervention in the US, the possibility of government regulation still remains at the international level.

"If the industry does not move fairly quickly to establish international self-regulation it may find itself facing the prospect of intergovernmental regulation and ordered codes of practice," he said.

Numerous countries took an increased interest in regulating content on the Internet in the past year, driven by a desire to protect children from objectionable content. The public concerns that fuelled government interest in the Net also spurred the industry to look at regulating itself, he said.

For instance, Internet service providers in the United Kingdom banded together to form a watchdog organisation and establish a hotline that people could call to report illegal activities, said Janet Henderson, rights strategy manager at British Telecom.

The group also set up a code of conduct that will be updated later this year.

"It was an initial symbolic gesture that was welcomed by the government as a sign that we were willing to move forward," she said. "It bought us a window of time to go at the issue."

While ISPs have a strong self-interest in keeping government regulation to a minimum - specifically, protecting themselves from liability - the issues goes beyond that, Szibo said.

Arrests in phone cloning scam

Two men and a woman have been arrested after police in Canada investigated claims that electronic serial numbers of cellular telephones were being used to create cloned phones.

The Royal Canadian Mounted Police took action after a worker from communications firm Bell Mobility allegedly supplied the numbers to a distributor who passed phones on to customers.

Cloning cellular telephones means copying the electronic serial number from one telephone into another so calls made on the second phone are charged to the first.

In this case, the numbers were coming from within the cellular carrier Bell Mobility, said Sgt. Bob Davis of the RCMP's Commercial Crime Unit.

After investigators at Bell Mobility alerted the RCMP in December, Davis said, the force carried out an investigation and searched a home in the Toronto suburb of Etobicoke, finding a number of cloned cellphones.

A 23-year-old man, a female Bell Mobility employee and another man, were arrested and will appear in court.

Davis said it is difficult to know exactly how much cellphone cloning goes on in Canada, but in a city the size of Toronto "my best guess is probably one or two cloners are active at any one time." Some cloners profit from cloned phones by offering low-priced calls on the street.

In this case, Davis said, the cloner had a regular roster of customers who would use their cloned phones for about a month and then return them to have new electronic serial numbers put in, in an effort to avoid detection.

Russian hacker sentenced

The first convicted computer hacker in Russia, a teenage college student, has been given three-year's probation.

A local court in Yuzhno Sakhalinsk on Russia's Far Eastern borders sentenced him and ordered him to pay the equivalent of $US 3000 - 200 times the region's average monthly wage - and also told to pay the equivalent of $US300 to firms affected by his hacking.

According to local police, an investigation into unauthorised access to computer systems of local companies and law enforcement offices was launched last May. After some considerable investigations, police were able to track the hacker down to his college, where he was arrested late last year.

Although the teenager admitted he had gained unauthorised access to various computer systems, court officials were unable to prove that he had downloaded commercial and confidential information.

Despite this, the judge in the case handed down the stiff probation and massive fine, with the clear intention of it sending a warning signal to other would-be hackers in the Russian Federation.

Product news

SurfWatch reports on child exploitation

A new web site has been launched so Internet surfers can report child pornography or other forms of exploitation.

The National Center for Missing and Exploited Children in the US has a special spot on SurfWatch Software's Web site for users to give details of offences to NCMEC's Exploited Child unit.

"We will work with federal, state, and local law enforcement to find out who is behind the site, then either prosecute or have the site taken off the net," said Todd Mitchell, from NCMEC's exploited child unit. Information left at the SurfWatch site gets added to the Internet filter-maker's database after it is checked against the firm's established filtering criteria for inappropriate sites, said SurfWatch.

The new SurfWatch site is at http://www.surfwatch.com/submit and NCMEC will launch a new site called CyberTipline at http://www.missingkids.com/cybertip

A US FBI spokesperson said the San Francisco office had "neither the time or resources to surf the Net looking for child pornography," but the agency does respond aggressively when sites are submitted from outside sources or developed during the course of other investigations.

For more information contact SurfWatch Software, on +1 650-917-2247 or the NCMEC on +1 703-516-6128

Internet scanner software

UK firm Internet Security Systems has launched a major update to its Internet Scanner that it claims now allows Windows NT and Unix users to assess their network security vulnerabilities.

David Bridson, a spokesperson for the company, said that Internet Scanner 5.0 features a range of unique security reporting capabilities, performance enhancements, and a significant number of new Windows NT and Unix features.

The package helps users reap the benefits of open systems while actively protecting their information from hacker attacks. Internet Scanner 5.0 is claimed to use unique security engine containing a comprehensive database of attacker methods and security vulnerabilities to scan a network and identify security holes automatically.

Bridson claims that Internet Scanner is the only software available that thoroughly evaluates the security of an entire enterprise network and intranet - including all Unix, Windows NT, and Windows 95 machines, as well as firewalls, Web servers, routers, and applications..

According to Kevin Black, ISS' UK general manager, new checks incorporated into Internet Scanner also include Windows NT host vulnerabilities such as misconfigurations and weak passwords.

"Each new month brings to light new Windows NT and Unix vulnerabilities, so Internet Scanner's comprehensive detection of a wide range of security weaknesses is becoming an increasingly critical weapon in the network manager's defences," he said.

Using Internet Scanner, the company claims that organisations can quickly and easily generate reports - including a technical security policy and a security "report card" - or a comprehensive summary of their actual security practice.

ISS is offering users an evaluation copy of the software for free download from its Web site at http://www.iss.net

For more details contact the firm on (UK) +44 1923 266023 or (US) +1 770-395-0150)

Secret messages for drug busting agents

A firm in the US has announced it is helping drugs agents in California by setting up a secure communications network.

Cylink Corporation, a provider of network security and management solution, is securing the highly classified wide area network of the California Department of Justice State wide Integrated Narcotics System.

Cylink's Hardware Link Encryptors will encrypt and protect confidential information gathered on narcotics trafficking and stored in SINS.

"SINS is a crucial weapon in the war against drugs. Without Cylink's critical encryption technology to protect investigation data from increasingly tech-savvy criminals, SINS could be compromised," said Gail Overhouse, SINS Project Director for the California Department of Justice.

SINS allows law enforcement organisations to rapidly share and exchange information, track and geographically display information about criminal activity, and provides a sophisticated system for managing and tracking complex case information.

"Information is a precious resource. When it is compromised, companies and, at times, entire industries are placed at risk," said Fernand Sarrat, president and CEO of Cylink.

"Law enforcement agencies rely heavily on information as they plan and execute operations. It is critical that they be able to securely access and share covert information without fear of it being accessed by the very criminals they are investigating."

It is estimated that narcotics enforcement agents spend about 40 per cent of their time locating and acquiring suspect information and SINS' major role is to make this task easier and quicker.

The objective is to bring together, through a single computer entry, all existing information held by various agencies on many computer systems that could affect narcotics information gathering and enforcement operations.

Originally developed for the State of California, SINS has evolved into a nationwide system, providing information to 1,050 statewide and 50,000 nationwide personnel, and more than 5,000 law enforcement agencies.

Organisations using SINS include the FBI, IRS, U.S. Customs, US Attorney General, Drug Enforcement Agency, Border Patrol, and local police and sheriff's departments. Other countries are now evaluating the SINS architecture for similar uses.

"SINS is light years ahead of how we previously operated. It gives our officers an advantage in capturing and arresting criminals," said Karen Aumond, administrator of the Western States Information Network.

SINS combines relational databases, a geographic information system, computer imaging, remote access, state-of-the-art security, and other advanced technologies in a single, integrated network system.

SINS uses relational database technology to store and organise complex information related to a criminal investigation. This database technology allows data to be regionally organised and distributed so that maximum performance and accessibility is achieved.

the system uses biometric fingerprint technology to ensure that only those who are authorised gain access to the system. Cylink's encryption technology protects the transmission of information across the network.

For more information contact Cylink on +1 408 328-5175 or visit the firm's home page at http://www.cylink.com.

Anti-slamming report on Web

A comprehensive site on the Internet has been set up to list each US state's rules regarding the tempering of telephone services, known as slamming.

VoiceLog LLC, a provider of automated third party verification, has announced the release of its "Anti-Slamming Rules Report".

"The 'Anti-Slamming Rules Report' has become the standard guide for the industry", said Jim Veilleux, President of VoiceLog. "With so many people using it, including law firms, carriers, resellers and agents, we wanted to make it as current and easily accessible as possible. Publishing it on the Web allows us to keep it updated between paper editions and to provide alerts to state activities which the industry may have an interest in."

The rules report lists each state, whether that state has "slamming" rules, the acceptance of third party verification and letters of agency, and other aspects of the state's rules.

Where possible, the report also notes potential future actions regarding slamming. With the release of the report on the Web, VoiceLog will also be adding alerts regarding current proceedings.

The report can be found at "http://www.voicelog.com/vl—rules.htm".

To get more information or get on the "Anti-Slamming Rules Report" mailing list, call Larry Leikin +1 703-356-1325 or send an e-mail to info@voicelog.com.

Palm scanner a world's first

Identix Inc, a supplier of scan systems and biometric identity verification systems, has introduced its TouchPrint 600 Palm Scanner.

Together with the TP-600's fingerprint capture and ID/verification capability, the US firm says it provides the first complete such electronic solution widely available to law-enforcement agencies. According to San Bernardino Sheriff's Department Cal-ID Administrator Sergeant Gary Eisenbeisz, at least 20 per cent of latent prints taken at crime scenes are palmprints.

"There are probably thousands of cases on file around the country that could have been linked to a perpetrator by now if palmprint databases were available," he said.

"The new Identix technology will enable us, and other agencies, to build such databases. From now on, we're routinely taking both finger and palm prints from every suspect."

Sergeant Eisenbeisz said that the Identix system also enables palmprint capture and transmission "much more accurately, faster and without the considerable messiness inked palmprints present. We can additionally make multiple copies for broader dissemination."

Identix chairman, president and chief executive officer Randall Fowler said the system features a curved platen, or scanning surface, which conforms to the shape of the hand and eliminates pockets, creating a superior image for identification purposes.

File viewing utility updated

Canyon Software has released version 4.0 of its popular Windows 95 file viewing utility, Drag And View.

The new release adds a multiple document interface, or MDI, plus screen capture capabilities, and support for more file types.

Drag and View lets users quickly view files of different formats without having to invoke, or even own, the original applications. The new MDI adds the ability to open multiple files as a series of "windows within a window," after the fashion of Microsoft Office applications like Word and Excel. The windows can then be tiled, cascaded, or manually resized.

The screen capture function can grab a full screen, full windows, child windows, or selected rectangles and will save images in most formats.

Additional viewable file types include various Internet and graphic file formats. The program also can show World Wide Web HTML (hypertext markup language) files on computers using Microsoft's Internet Explorer.

Drag And View requires a 486-based PC or higher with 8MB of RAM and 8MB of hard disk space. Sixty day time-limited versions can be downloaded free of charge at http://www.canyonsw.com and full registration costs $35.

HP to strong cryptography technology

Hewlett-Packard has announced it has received approval from the US government to export VerSecure, the company's most advanced technology for managing and providing strong encryption services.

The license granted to HP gives end users in approved non-US countries access to strong 128-bit and triple-DES encryption.

Users can choose from limited to very strong cryptography and select whether or not to activate a key recovery capability. HP was granted approval to export VerSecure technology to the UK, Germany, France, Denmark and Australia. More countries are expected to implement the VerSecure technology in the coming months.

Lewis Platt, HP chairman, president and chief executive officer said: "By addressing the security issues that have hampered international e-commerce in the past, HP's cryptography infrastructure - applied globally - will help ensure privacy and help stop piracy of Internet-based communications and transactions worldwide."

VerSecure technology allows secured electronic transfer of such sensitive data as financial transactions, blueprints, digital signatures, medical and legal records, telecommunications billing, business-to-business communication, consumer credit information and private messages.

Users of the system can also choose when to use key recovery, a data-backup technology that allows users and law enforcement, when necessary and within the context of local government policies, to recover encrypted data.

For more information visit HP's web site at http://www.hp.com.

Watching the net surfers

A network monitoring and auditing software server has been launched which lets users capture information sent across the Internet.

Network Flight Recorder, Inc. announced that its system, also called the NFR, is now commercially available.

More than 700 companies worldwide took part in the open Beta program in December, which was conducted completely over the Internet.

The NFR is a general-purpose tool that lets network managers capture a broad array of information from the IP packets travelling across their network. The NFR analyses all of the IP packets then sends selected information from each packet into a "decision engine."

Filters are applied to the collected data, which sends the data to an alerting system. A Java interface allows administrators to perform real-time queries on the available data and presents the results in both text and graphic formats.

Marcus J. Ranum, President and CEO of NFR said: "We believe it is important to provide a general-purpose window into network activity.

"When we developed NFR, we made the most flexible possible network traffic monitoring and analysis system, which is already being put to good use for a wide variety of purposes. I see the NFR as an essential step toward merging capabilities for network management, audit, and security."

Among its uses, the firm says that NFR Version 1.5 allows users to recover or monitor on-line transactions, log how their network services are being used and by whom, watch for patterns of abuse of network resources and identify the culprit in real-time, set burglar alarms that alert them to security violations, replay attackers' sessions and learn what they did and filter their e-mail for sensitive words or phrases.

"Network managers are vulnerable, they don't know they are vulnerable, and if they get hit, they won't have any way of telling through which backdoor the attack came, where it went, or how to prevent it from happening again," said Mr. Ranum.

"For lack of a better term, we've been referring to this as 'network forensics' - instead of mapping blood patterns and DNA samples, we're looking at how to analyse packet traces and network connectivity graphs.

Just like forensic scientists at a crime scene, we'd rather be able to re-construct events using a closed-circuit video camera's recording than to have to use scuff marks on the floor. Especially since network 'scuff marks' are much, much easier to conceal."

The product is available for a variety of UNIX platforms, including Solaris, BSD/OS, FreeBSD, and Linux. A version for Windows NT is planned for release in first quarter 1998.

And both the product and source code are available for download from the firm's Web site at http://www.nfr.net.

The software is free for non-commercial use or research, and to universities. While NFR says it expects users will create their own proprietary backend modules, the company is encouraging the exchange of information.

NFR says it also provides space on their Web site for users to post their filters for use by other NFR users.

Virus catching lab

Viruses attached to Usenet newsgroup messages on the Internet have become an increasing problem, and keeping up with new viruses has always been a challenge for software vendors in the lucrative anti-virus market.

McAfee Labs, the AV research arm of Network Associates, is now going to the source and filtering every known public newsgroup, using the firm's NewsSniffer AV program.

It is thought that there are about 27,426 public newsgroups, though the actual number of groups with messages in the feed rises and falls constantly.

The highly automated operation taps into public groups at the Hurricane Electric news server, which McAfee Labs Manager Shannon Talbott described as "one of the fastest news feeds in the world".

She said that 98 per cent of all groups go through that server, the remainder being very local topics.

To catch viruses, all postings through the Hurricane Electric server are also sent to a Network Associates system, which filters out binary and heavily formatted files and sends them on to McAfee Labs in Santa Clara for processing.

"Anytime we find something, we post back a message to the newsgroup and the person who sent the message, if we can get the name, telling them we found the virus," Talbott said.

"The users generally don't know they've posted a virus until we tell them. Telling the newsgroup and the poster about the virus gives them a chance to do something about the infection before it causes any damage."

She added: "Of course, there are sites for hacker groups, where virus writers go to post their creations, and we don't bother to tell them what we found.

Talbott said when a new virus is found, it is added to the company's virus database at http://www.beta.mcafee.com, where the data file is updated hourly between the regularly scheduled, monthly data file updates at http://www.mcafee.com

"We find a lot of new viruses that way," said Talbott. "We're especially proud of our latency now, the period from when messages are posted to the time we reply with a warning. It's down to under six hours.

"It really helps limit the spread of those things, cuts the risk by a lot."

US Defence hacking attack

US Defence Department officials and the FBI are investigating a series of breaches in military computers. Paul Johnson reports.

In what can only be seen as another indictment of US national computer security, hackers gained access to sensitive data in a prolonged two-week assault.

Deputy Defence Secretary John Hamre said it was probably the most intense break-in effort to date, and that this was the latest "wake-up call" on the vulnerability of government and corporate computers to sophisticated search software used by professionals and amateurs.

The break-ins occurred at more than eleven military sites, including seven Air Force sites and four Navy sites

Hamre stressed that ultra sensitive classified systems had not been breached.

He added: "During the last two weeks, the Defence Department has experienced a fairly heavy-duty cyber attack. In this case, we have been working very closely with the attorney general and the FBI.

"We did not have any penetration of our classified networks, the unclassified networks, however, were penetrated."

Hamre noted the incidents had intensified attempts by the defence agency to more quickly spot break-in attempts and catch persons responsible.

"It has dramatically accelerated the Pentagon's and federal government's plans to get on top of this problem," he said, underscoring that sensitive data on personnel, payrolls, and other information from Wall Street to the armed forces often is not adequately guarded by software firewalls.

Hamre said it was not known whether the attempts, which were nationwide, involved one or more persons in the United States or overseas who used computers to get into Pentagon information systems.

But he suggested the moves might be by amateurs in response to "contests" among hackers.

"There are hackers that enjoy just breaking into people's computers to see what they can see. And, of course, there is always a mystique about the Defence Department," he said.

"There are actually hacker clubs and there are hacker contests. In that sense, the department is vulnerable."

Hamre declined to discuss details of the latest efforts or to reveal what information had been obtained. But he said the incidents appeared to be similar to previous attempts by hackers to show that they could get into protected systems.

He said the recent incidents included attempts to set up electronic "trap doors" in software systems through which information could be siphoned.

FBI agents investigating the systematic attack may have uncovered the culprits, according to reports.

But instead of the sophisticated criminal first thought to be behind the incidents, two schoolchildren have been linked with computer break-ins.

FBI agents descended on Cloverdale, a town of 5,500 about 75 miles north of San Francisco, and searched the homes of the teenage boys, seizing computers, software and printers

FBI spokesman George Grotz declined to reveal specifics of the search conducted by the FBI computer crime squad. "It was part of a computer intrusion investigation," Grotz said. "It is an on-going case."

In one of the houses searched, agents caught one boy in the act of hacking into a non-classified Pentagon computer. The boys, who are about 15 years old, were not arrested.

The Cloverdale hackers apparently used a local Internet company, Netdex Internet Services, as a base, and left a clear "electronic path" pointing to a series of federal and military computers.

Netdex owner Bill Zane said that administrators began noticing hacker activity in their system in mid-January and immediately notified law enforcement agencies and the Computer Emergency Response Team at Carnegie-Mellon University in Pittsburgh.

Zane said Netdex began tracking the activities of the hackers as they leap frogged into other systems, including the University of California at Berkeley, the Massachusetts Institute of Technology, national laboratories, numerous military sites and two sites in Mexico.

"We actually had online battles with the hackers," Zane said. "We were watching them and they knew we were watching them. They were trying to reinstall their software files as fast as we could destroy them."

He also said there were "clear indications" that the hackers were communicating with other hackers and getting software tools from others.

"The sheer volume of it differentiates it from some hobbyist amateur," Zane said, "These people were doing it in a methodical, organised way."

"I would be very surprised if this were just kids," Zane said. "It's not beyond conception that there's a group of people, and kids are being used by someone else."

He said one of the most interesting aspects of the case was that it appeared to combine both surprisingly sophisticated hacking techniques with amateurish errors.

He said: "We've had mail spammers before, but this is a horse of a completely different colour.

"It was massive. The two kids that they got, I don't believe is the extent of it. There are other hackers out there, and they are communicating with each other."

Zane said his analysts had noticed several different hacking "styles" or signatures in the system, which could indicate that more advanced experts were feeding hacking programs to the teenagers.

"The hacker really isn't somebody at a keyboard trying to guess your password. They are writing and using programs that they hope can bust your machine," he added.

● The Journal reported last year that a US presidential commission warned major computer networks in the country were vulnerable to attacks.

At about the same time it was revealed that hackers had broken into more than 250 US Defence Department computers. Air Force Lt Gen Kenneth Minihan, director of the National Security Agency, said that the US would eventually pay for building its information infrastructure on a poor foundation unless security protection was increased.

Court reports

BBS posting

In an important case, a US court has heard arguments concerning the legal implications of a bulletin board message.

In the case of Mallinckrodt Medical Inc. v Sonus Pharmaceuticals Inc., decided recently in Washington DC, the District Court had to consider the jurisdictional issues arising out of the BBS posting.

Sonus Pharmaceuticals, in the course of a patent dispute, sent a message from Seattle to Virginia over America Online, which was posted on AOL's bulletin boards.

Mallinckrodt argued that, as there were approximately 200,000 District of Columbia residents who were subscribers to AOL and that as they all would have had access to the posting, Sonus had been carrying on business in the District Columbia for the purpose of the long-arm (jurisdiction) statute.

In addition, the Plaintiffs argued that the transmission of the message, which they claimed was defamatory, provided jurisdiction in DC in terms of another provision of that statute which provided personal jurisdiction over a person who "cause[s] tortious injury in the District of Columbia by an act or omission outwith the District of Columbia if he regularly engages in any persistent course of conduct in the District of Columbia."

The Court rejected both these arguments. In a detailed analysis of the position, Judge Paul Friedman stated said: "The AOL transmission from Seattle to Virginia which was subsequently posted on an AOL electronic bulletin board and may have been accessed by AOL subscribers in the District of Columbia, cannot be construed as 'doing business' in the District of Columbia.

"The message was not sent to or from the District of Columbia, the subject matter had nothing to do with the District of Columbia, and neither plaintiffs nor Sonus reside in, have their headquarters in or are incorporated in the District.

"Other than the fact that some people may have visited the electronic bulletin board and read the message from here, the AOL posting has no connection to this jurisdiction. The act of posting a message on an electronic bulletin board - which certain AOL subscribers may or may not choose to access, according to each individual's tastes and interests - is not an act purposefully or foreseeably aimed at the District of Columbia. Therefore it does not... constitute transacting business within the District of Columbia for the purposes of the long arm statute."

Dealing with the question of jurisdiction on the grounds of defamation within the District of Columbia arising out of the AOL posting, the Court found that there was no evidence that the Plaintiffs had suffered any injury that they had not suffered in any other State.

Accordingly the mere fact of the Internet and of Internet service providers such as AOL did not change the normal legal position that there is no nationwide jurisdiction for defamation actions.

David Flint, partner in the IP & Technology Law Group of MacRoberts, Solicitors, said: "If the District Court is correct, it would appear that - unless a message is deliberately targeted at a jurisdiction - legal jurisdiction will only lie where the sender, and possibly the recipient resides."

Net copyright row

In another Internet jurisdiction debate, a court ruled over a trademark infringement argument. Two firms with the same name, Cybersell, clashed over a website.

In Cybersell Inc (Arizona) v Cybersell Inc (Florida), the Ninth Circuit ruled that a passive website was insufficient to found jurisdiction in Arizona over a Florida company and that some form of targeting was required.

More importantly, the Court stated that: "We decline to go further solely on the footing that Cybersell (AZ) has alleged trademark infringement over the Internet by Cybersell (FL)'s use of the registered name Cybersell on an essentially passive web page advertisement.

"Otherwise, every complaint arising out of alleged trademark infringement on the Internet would automatically result in personal jurisdiction wherever the plaintiff's principal place of business is located. That would not comport with traditional notion of what qualifies as, purposeful activity invoking the benefits and protections of the Forum State."

David Flint, Head of the IP & Technology Law Group at MacRoberts, Solicitors, said: "For the UK business, the possibility that its legitimate use of a trademark or trade name on a Website will be seized upon by a litigious US Corporation must be coming much less. Indeed, even for US businesses, the fact that inter-state infringement cases are less likely must be good news for commerce as a whole."

Case sets Net domain name precedent

An interesting legal case over similar domain names, passing through the Scottish legal system, has set a precedent.

A court has ruled that an interim order can be issued that blocks an organisation from using a disputed domain name while the case awaits a full civil trial.

The Scottish case centres on the use of the domain name menu.co.uk, which is used at http://www.menu.co.uk by Alan Brooks, a Scottish businessman.

He uses the Web site to publicise menus from UK restaurants that pay Brooks a small fee to display their menus on the Internet.

Recently Brooks noticed that a third party had registered a second domain name of menus.co.uk , and had established a Web page noting that the Web site "was under construction."

According to Brooks, while the domain name was different from his own, it clearly intended to cover the same subject matter, including as it did the words "sometimes it's good to see the menu before you book" to introduce the new Web site.

Brooks subsequently made an application to the Glasgow Sheriff court to stop further use of the name www.menus.co.uk on the basis that the harmful event of passing off, occurring through the viewing of that site, occurred in Glasgow.

As a result of this application, the Sheriff at Glasgow has now granted an interim interdict against the continuing use of www.menus.co.uk .

Cyberspace intrusion

The latest issues and arguments in computer law and privacy were debated at a major meeting.

Law experts, privacy advocates, hackers and law enforcement agencies members discussed the latest issues at the annual Conference on Computers, Freedom and Privacy.

Topics included free speech on the Net and inappropriate material on the Web, as well as the regulatory laws surrounding them.

Brian Kahin of the White House Office of Science and Technology Policy reiterated President Clinton's philosophy of keeping federal regulation of the Net to a minimum.

But new issues have been emerging, the conference was told, such as the proliferation of junk e-mail and concerns related to online privacy and the use of personally identifiable information on line. These may require government regulation, he says. "Obviously we're not going to martyr ourselves to our principles."

Hackers, computer consultants and network administrators called on colleagues to grapple with the "real issues" of computer security, rather than relying on firewalls and other security programs.

Computer security consultant and former hacker Peter Shipley said he had spent the past two years researching the vulnerability of networks to something as simple as a phone call.

Shipley, who makes his living doing security audits, rigged his computers to do what's called "war dialling", continuously and systematically calling local phone numbers in the San Francisco Bay area, identifying which had modems attached.

Out of 2.6 million calls, he found hundreds of vulnerable systems, including the dispatch centre of the Oakland Fire Department, a paediatric medical practice's scheduling and billing information system and one of the Bay Area's biggest bookstores, which had left its ordering database unprotected.

He also got access to a large number of air conditioning systems, which were connected to the network to allow them to report faults and be remotely operated. He said: "You could turn up the heat, turn down the water pressure, anything you wanted."

He said that using Strobe, a popular software program, intruders could scan for open ports on networks, which provide easy entry to networks once they are identified.

Once connected to such a network, other software can be used to scan for known vulnerabilities and unpatched security holes, which are common with operating system and security software products.

Shipley, founder of Network Security Associates in California, said during the debate that companies are more afraid of the Net than they should be, but then fall into the trap of being too confident about the level of security they have set up.

"The old-fashioned modem dial-ups are still there, and they still leave people open," he said.

Shipley said that malicious hacks can be classified into four categories: disclosure of information, such as theft of credit card numbers; destruction of data, which can be an act of economic terrorism; alteration of data, such as grade fixing; and denial-of-service attacks.

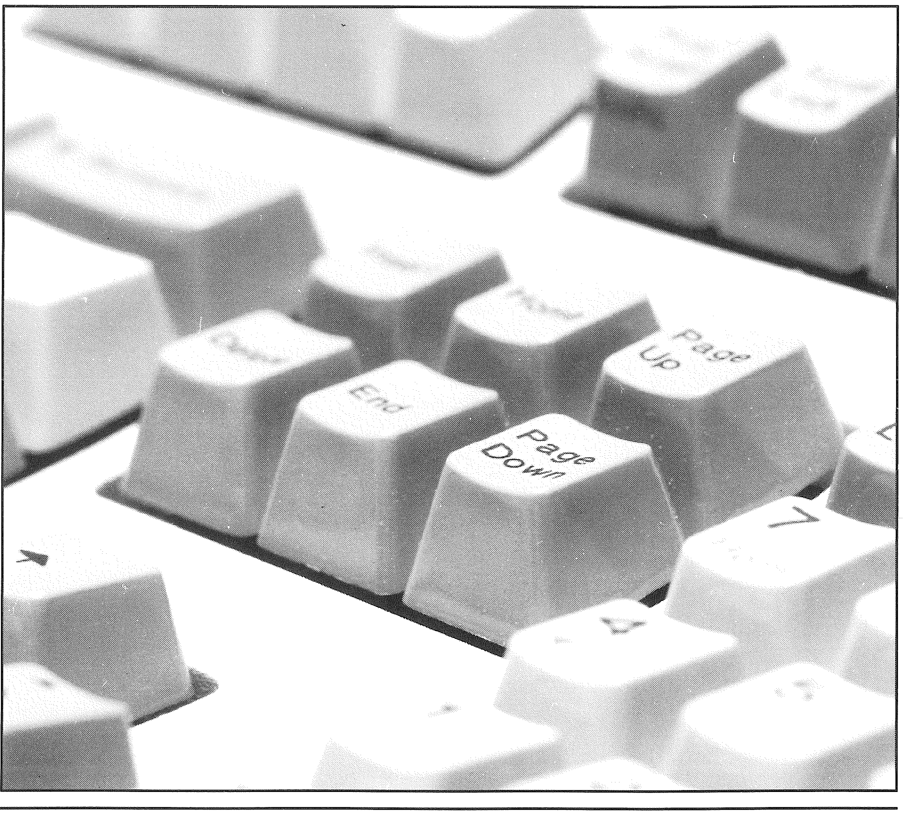
The motivation for such attacks ranges from financial to revenge to peer respect, he added.

Shipley and the other panellists for the "Net Hacks and Defences" discussion attributed the lack of security in computer networks to disbelief, laziness, and overconfidence. Free Web-based email services are a classic example of network vulnerability, he said.

"All of your Hotmail is readable by the world," said Shipley, introducing the topic of sniffers, one of the fundamental tools used to monitor and intercept data over a network. He then presented a list of protocols that can be exploited using hacking tools: telnet, http, SNMP, SNTP, POP, FTP, and many other baseline standards used to send email, files, and other communications over the Net and computer networks.

"It really works too well," Shipley said, pointing to the fact that hackers routinely take advantage of the same tried-and-true techniques that have brought them so much success in the past.

A good hacker will normally do some research first, to discover anything useful about the nature of the target network. Information can include the type of firewall, networking software, and oper-



ating systems in use, as well as host lists, usernames, network connections, and sibling domains.

"Look at all your inbound connectivity and co-developers," Shipley said, explaining that even if a network itself is well protected, there are often peer network connections, such as those at business partners, ISPs, or home modems, that can be used as back doors into a network.

"If you want to hack NASA, go to Lockheed and get in through their connections," he suggested.

But some methods are even more straightforward and bold, Shipley said, such as entering an office building to steal something as benign as an employee phone list, or something as guarded as the map of a network's computers and software implementations.

Even easier, he said, are social engineering techniques, where a would-be intruder calls up a network engineer - or someone else with pertinent information - and simply asks what types of software and configurations, or port assignments, are being used in a network.

Dave Del Torto, a software designer with Pretty Good Privacy, said: "People are absolutely pathetic about maintaining security policies, and social engineering is the easiest way in.

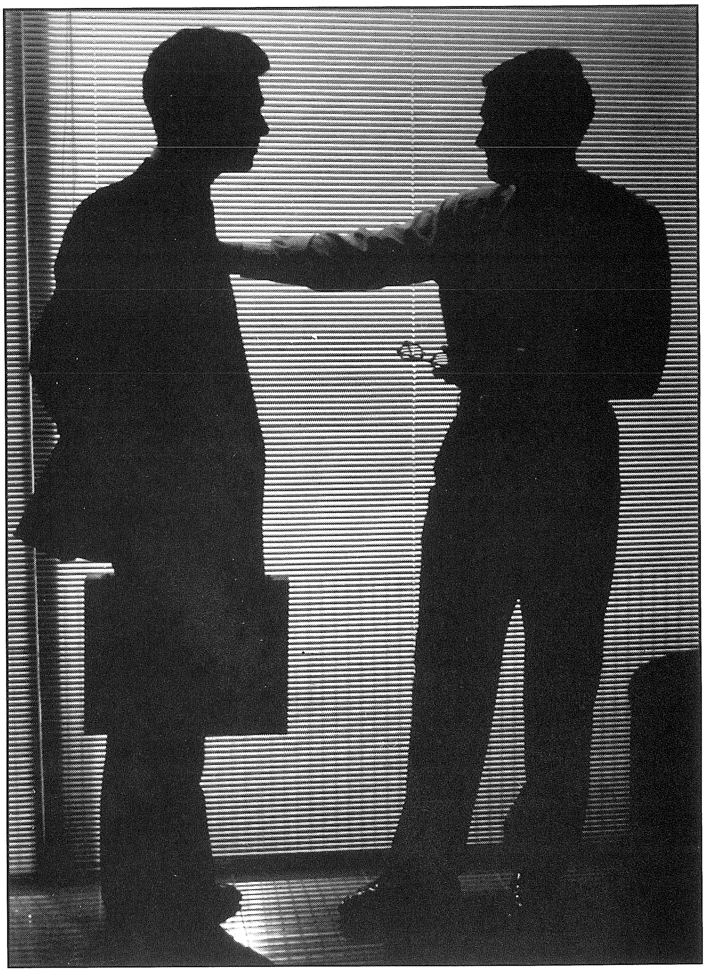
"Don't underestimate the value of educating your staff," said Del Torto.

Some operating systems, Shipley said, are easier to compromise than others, and "[Windows] NT is not capable of being anything nearly like a reliable system for the Internet." He recommended that "multiple firewalls" be used if a Windows NT machine is to be used on networks with Internet connections.

But even firewalls have their problems. "Seventy percent of packet filter firewalls are misconfigured," said Castagnoli. "You don't just set them up and walk away. You need to constantly monitor and update them."

In general, the panellists were sceptical about the value of mainstream network security software products. One reason cited was that nobody, aside from the vendors, knows what's behind the GUI.

"You can't trust a system unless you can see the entire inside of it," said PGP's Del Torto. "As a trend, patronise companies that open source code," he advised, and complimented Netscape for doing so with its Navigator browser code.



The panellists recommended several strategies to improve individual user security.

First, a randomised, mixed character-number password kept in a wallet is much more effective than an English word or name committed to memory, panellists said. Several software programs, including Crack, are available for quickly cracking passwords that are dictionary words and common names.

The panellists also recommended cautious users buy a cross-shredding paper shredder and use it on anything that contains personal data. Dumpster-diving is popular sport for data thieves, and a woman in Oakland was recently caught with files on 300 people in the area, with enough information about them to get credit cards and driver's licenses.

Finally, the panel recommended encryption software is used on any sensitive communications or files that a user wouldn't want someone else reading.

The panel also advised that companies allow employees to use company email for personal use, because at least a firewall stands between their email and the open Internet. They estimated that 30,000 people are signing up for free email services every day, and most of those are open to packet sniffers and other monitoring tools that turn such emails into postcards on the Net.

The conference also discussed privacy issues in Europe. In October, the European Union will implement new privacy standards for all 360 million of its citizens.

While protecting Europeans against having information collected and used without consent, the directives also prohibit the shipment of data to or through any "non-adequate privacy state", one of which is very likely to be the US.

In March, the Federal Trade Commission will audit Web sites to see what privacy policies they have in place and then report to Congress. This isn't just because of the European Union, said former FTC commissioner Christine Varney, now a lawyer in private practice.

"We need to engage in this because there are massive amounts of information being collected. And that may or may not be OK."

US Government debates

Online pornography argument

The issue of freedom of speech versus fear of pornography has divided members of a US Senate committee.

"It is bad for business when the fear of pornography keeps families off the Net," Andy Sernovitz, president of the Association for Interactive Media told the Senate Commerce, Science and Transportation Committee hearing.

"We can put a brown paper wrapper around Internet porn, while still protecting our First Amendment rights," Sernovitz said.

"AIM believes that there are technologies that can effectively deal with adult content," Sernovitz said, noting that many filtering systems have been developed that can screen out adult content on a voluntary basis while still protecting adults' rights to publish and view such material.

American Civil Liberties Union legislative counsel Gregory Nojeim said that while the ACLU recognises the concerns, the organisation "strongly believes" in the individual's right to access information. He added: "Parents should not abdicate responsibility to the government for determining which information their children can see."

Both Sernovitz and Nojeim criticised Senator Daniel Coats' legislation, introduced last November, which would punish commercial online distributors of material deemed "harmful to minors".

The law would impose criminal penalties of up to six months in jail and a $50,000 fine. Sernovitz opposed Coats' bill "as being ineffective and highly destructive to the American principle of free speech".

And the ACLU said the criminal penalties, which could be levelled against "distributors," could include such groups as the Amazon.com virtual bookstore or a movie promotional site.

Sernovitz quickly parted company with the ACLU, however, denouncing the ACLU's campaign to sue any library that attempts to install a filtering system as having "a chilling effect on every good-faith effort to solve this problem."

"The ACLU's actions virtually guarantee that hard-core pornography is available in every classroom, to every child," Sernovitz said.

But trying to find a middle ground, Seth Warshavsky, CEO of Internet Entertainment Group, Inc, proposed that Congress create a new ".adult" segment of the World Wide Web to help cordon off sexually explicit material.

Under Warshavsky's proposal, all current federal and state regulations governing sexual content on the Internet would be pre-empted by a new ".adult Act." In addition, Warshavsky's proposal would mandate that every new computer sold in the US would require a V-chip capable of screening out any ".adult" material. The ".adult Act," Warshavsky said, would provide a legal "safe harbour" exempting individuals and companies who abide by the ".adult" provisions from prosecution.

"Our company provides sexually oriented content and Web services to adult subscribers who usually pay a fee," Warshavsky said.

"I am passionately committed to the principles of the First Amendment, that adults should be able to make their own decisions about what they want to see, read and view. But that commitment doesn't mean that my company or any other should permit a minor to have access to sexually oriented content which our society deems inappropriate for that minor without parental consent."

"Irresponsible people flood the Internet with sexually oriented material without adequate barriers to stop minors from access to these sites. We must find ways to stop juvenile access which are sufficiently effective so parents feel comfortable with adult access."

Law to protect online copyright

Legislation in the US could help identify and prosecute those who steal other people's work on the Internet.

Seeking a consensus on who should be liable for copyright infringement online, Rep Bob Goodlatte has introduced a law designed to protect both the content and service provider, while targeting the parties directly responsible.

According to Goodlatte, his bill, the Online Copyright Infringement Liability Limitation Act, codifies the decision in Religious Technology Center v. Netcom, 907 F. Supp. 1361 (N.D. Cal. 1995), in which the court held that an Internet access provider was not directly liable for copyright infringement committed by a bulletin board subscriber.

Goodlatte is a member of the House Judiciary Committee's subcommittee on Courts and Intellectual Property, which has jurisdiction over all issues involving copyright law.

"While I do not yet have a proposal that I can say is supported by both sides of this debate, I am not currently aware of any opposition to the principles adopted by the court in Netcom," Goodlate said. The Virginia congressman acknowledged that while the bill "will not solve every problem posed by the content and service provider communities, it is a good first step toward reaching consensus on the issue, which is critical to the development of the Internet."

Net trade hit by fraud

The chairman of the Federal Trade Commission has told a Senate panel that business on the Internet could skyrocket from $2.6 billion in 1996 to $220 billion in 2001. But chairman Robert Pitofsky warned "Consumers must feel confident that the Internet is safe from fraud."

Pitofsky was one of a number of witnesses testifying about the Internet to the investigations subcommittee of the Senate Governmental Affairs Committee.

The FTC chairman told the panel that the commission first held public hearings about the problem in 1995. It concluded that consumer protection must be coordinated, private and public officials must act in "partnership," and consumers need to be educated "through the combined efforts of government, business and consumer groups."

Pitofsky said the FTC has filed more than 25 law enforcement actions against alleged fraud on the Internet.

Though the alleged frauds are dressed up in high-tech garb, he said most were just old-fashioned scams. He cited pyramid schemes, business opportunity schemes and credit repair scams.

Examining computers

Seizure of computers

Personal computers have become an inexpensive yet powerful tool that can be used in the furtherance of almost any criminal activity.

Criminal acts can easily be coordinated worldwide using the Internet, and criminal communications can easily be encrypted and thus secreted from law enforcement officials.

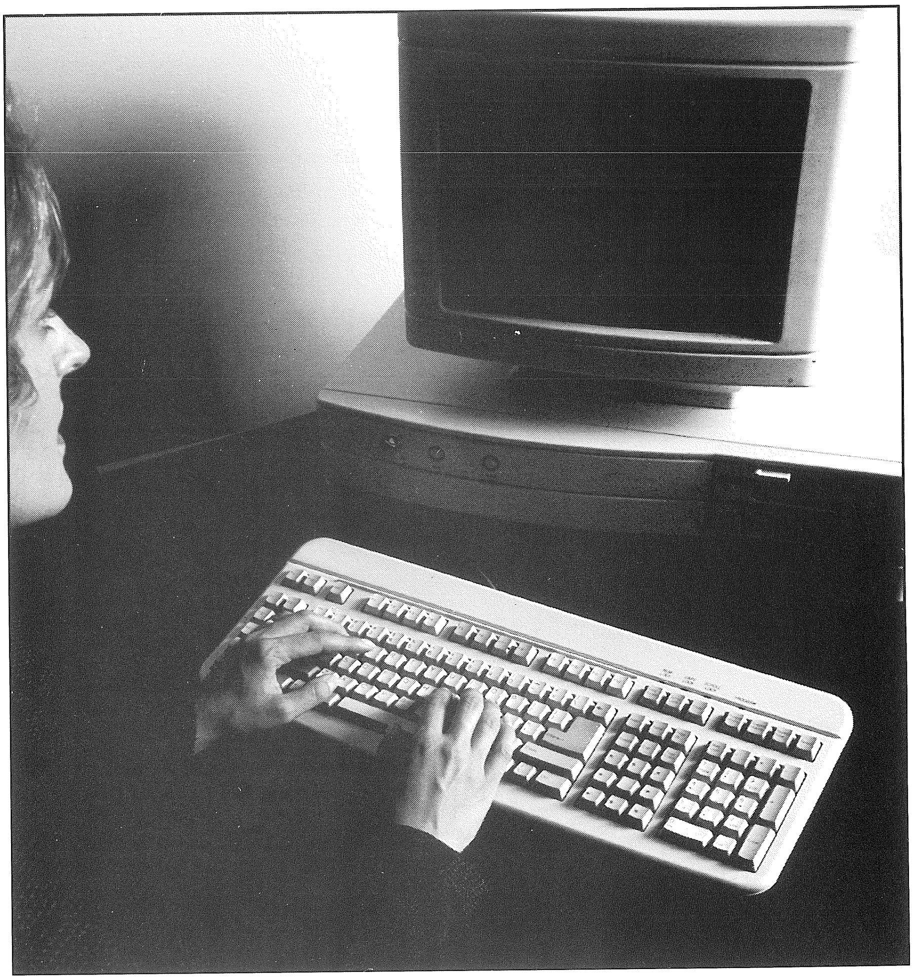
Bomb-making recipes and other tools of terror can be shared worldwide over the Internet. The fruits of a crime can be recorded and tracked with computer spreadsheets and the particulars regarding criminal associates can be easily managed using computer databases.

While this could present a bleak picture for law enforcement, the use of personal computers by the criminal element can create a wealth of unique and valuable evidence that might not otherwise be available to investigators.

Fortunately for law enforcement computer evidence specialists, personal computers were never designed to be secure.

As a result, sensitive data, passwords, time and date stamps and other potentially valuable information are written to bizarre locations on computer hard disk drives and floppy diskettes as part of the normal operating process. To the corporate, government or individual computer user this can be the source of serious computer security concerns.

To an experienced "cybercop," it can be a dream come true.



Progress

Back in "the good old days," we knew very little about computers and attorneys and judges knew even less. But computer evidence is very fragile and can easily be altered, and the processing of such evidence for use in trial by an individual without proper training is like performing brain surgery with a pocketknife.

It is important that only properly trained computer evidence specialists process computer evidence.

The first computer evidence courses were offered at the Federal Law Enforcement Training Centre (FLETC) back in 1989. We've come a long way since then. Specialised software utilities to automate the search of large computer hard disk drives have been developed by folks like Steve Choy and Bill Haynes.

The "electronic crime scene" can now be preserved with programs like SafeBack from Sydex Corp.

Obscure data segments containing binary (nonreadable) data can now be filtered, making the contents easily printed or displayed using simple word processing software.

Most importantly, additional training courses have been spawned to deal with the demand for law enforcement and military forensic computer science training.

The University of New Haven, in West Haven, Conn., created a Forensic Technology Institute which is dedicated to such training.

This is probably the first university to offer college credit and certification tied to computer evidence processing.

A Training and Research Institute was created at the National White Collar Crime Center to deal with law enforcement computer evidence training issues.

Because of the demand, these much-needed institutions are welcomed and supplement the training courses already offered at FLETC and by SEARCH and The International Assn. of Computer Investigative Specialists (http://www.cops.org).

Common Mistakes

Obviously, a complete training course in forensic computer science is outside the scope of this article. However, following are some of the common mistakes that are made and some tips that may be helpful in the processing of computer evidence tied to DOS/Windows-based computer systems.

Mistake 1 — Running the Computer

The first rule is to never run any programs on the computer in question without taking precautions — e.g., write protection or by making a backup. Also, you should not boot or run the computer using the operating system on the computer in question.

It is relatively easy for criminals to rig their computers to destroy hard disk drive content or specific files by planting decoy programs or through the modification of the operating system.

For example, the simple DIR instruction, which is used to display the directory of a disk, can easily be rigged to reformat the hard disk drive.

After the data and destructive program has been destroyed, who is to say whether the computer was rigged or if you were negligent in processing the computer evidence?

Mistake 2 — Getting help from the computer owner

It is a serious mistake to allow the owner of the computer to help you operate the computer in question. It's like asking some thug to help you unload the 9mm pistol you just found under his car seat. Don't do it.

In one case a few years ago, the defendant was asked to answer questions about the computer evidence and was allowed access to the seized computer.

He later bragged to his buddies that he had encrypted relevant files "right under the noses of the cops" without their knowledge.

The good news is that the computer specialists had made a bit-stream backup of the computer before giving the defendant access to it. As a result, his destructive act became another nail in the coffin at his trial.

Mistake 3 — Not checking for computer viruses

You can imagine how credible your testimony might be as the expert witness for the government if you were the one that infected the computer evidence with a computer virus.

It might get even worse, if you carry that a step further and infect several of the computers in the police department in the process. Always use fresh diskettes and check all diskettes and hard disk drives with good quality virus-scanning software.

Mistake 4 — Not taking precautions in the transport of computer evidence

Computer evidence is very fragile. Heat and magnetic fields can destroy or alter it in a very short period of time. The heat of summer in a car trunk or the magnetic field created by an operating police radio in the trunk of a squad car can ruin computer evidence.

If a good defence attorney can show that you were negligent in storing or transporting the computer equipment, your case may be in jeopardy and you may spend some time in civil court defending your agency against a lawsuit.

Helpful tips

Tip 1 — Perform bit-stream backups

Normally, computer evidence is preserved by making an exact copy of the original evidence before any analysis is performed. It is not enough to just make copies of computer files using a conventional backup program.

Valuable evidence may exist in the form of erased files and the data associated with these files can only be preserved through a bit-stream backup.

Specialised software is available to law enforcement agencies that perform this task, e.g., SafeBack. For floppy diskettes, the DOS Diskcopy program will suffice.

Tip 2 — Check temporary files

Word processing programs and database programs create temporary files as a by-product of the normal operation of the software. Most computer users are unaware of the creation of these files because they are usually erased by the program at the end of the work session.

However, the data contained within these erased files can prove to be most valuable from an evidence standpoint. This is particularly true when the source file has been encrypted or the word processing document was printed but never saved to disk. Like magic, these files can be recovered.

Tip 3 — Check the Windows swap file

The popularity of Microsoft Windows has brought with it some added benefits for computer investigators in their quest for new sources of computer evidence. The Windows swap file acts as a huge data buffer, and many times fragments of data or even an entire word processing document may end up in this file.

As a result, careful analysis of the swap file can result in the discovery of valuable evidence when Windows is involved.

Tip 4 — Make document comparisons

Many times duplicate word processing files may be found on computer hard disk drives and/or floppy diskettes. Subtle changes or differences between versions of the same document may have evidentiary value.

These differences can easily be identified through the use of the redline and compare features of most modern word processing programs. This trick alone can save countless hours of time that could be wasted making manual comparisons from one document to another.

Because the resulting file is modified by the word processor, be sure to work from copies.

The popularity of computers in society today has changed the evidence rules a bit, but this technology has provided investigators with potential sources of evidence and information that did not previously exist.

By Michael R. Anderson

Mr Anderson is the President of New Technologies In, based in Oregon in the US.

He has 25 years experience as a Special Agent and computer specialist with the Criminal Investigation Division of the US Internal Revenue Service.

Mr Anderson has written software applications used by law enforcement agencies in 16 countries to process evidence and to aid in the prevention of computer theft.

NTI specialises in the fields of computer forensic science, cryptanalysis, forensic utility software development, computer artificial intelligence and computer security risk identification.

The firm can be contacted on +1 503 6666599or by e-mail to info@forensics-intl.com

Analysis of the UK Police and Criminal Evidence Act, s.69 - Computer Generated Evidence

By
Amanda Hoey

The law of evidence is concerned with the means of proving the facts which are in issue and this necessarily involves the adduction of evidence which is then presented to the court.

At present there are special rules governing the admissibility of computer-generated evidence in criminal proceedings. In this article the issues of when computer output will be considered direct evidence or hearsay and the reliability of computer-generated evidence are discussed.

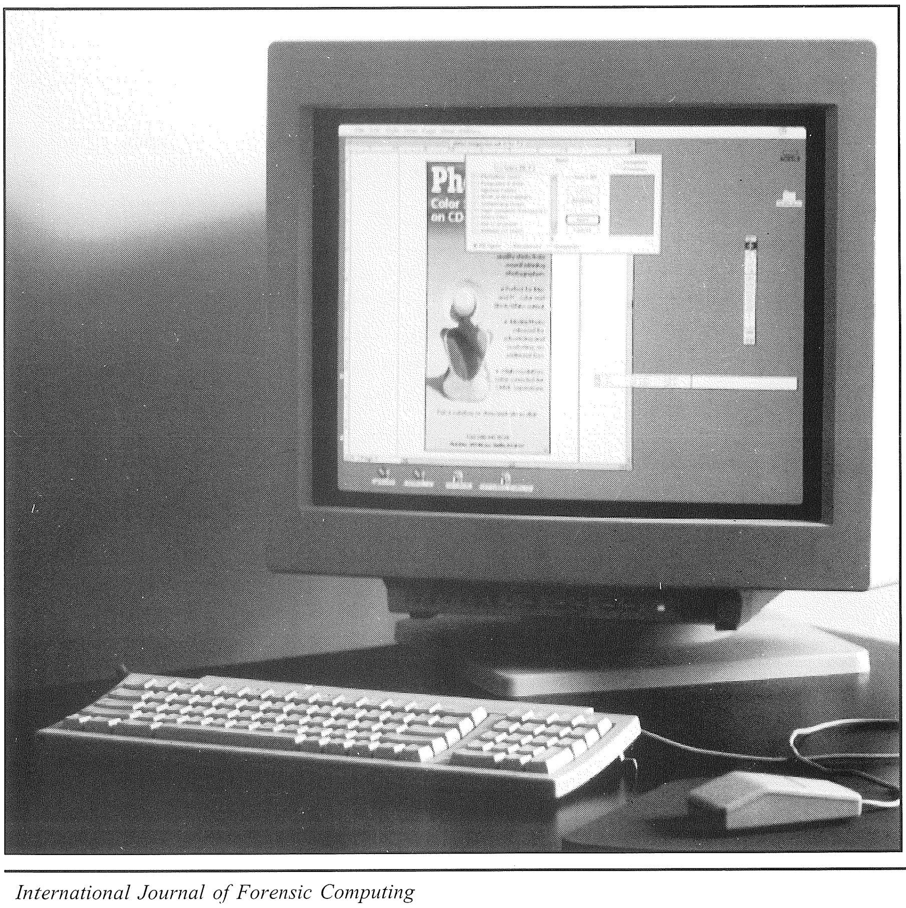
In conclusion the article attempts to ascertain whether these special rules for computer output are necessary and, if so, whether the conditions established by the statutory provisions are appropriate.

Introduction

We are living in what is usually described as an 'information society' and, as the business community makes ever greater use of computers, the courts are going to find that increasingly the disputes before them turn on evidence which has at some stage passed through or been processed by a computer.

In order to keep in step with this practice it is vital that the courts are able to take account of such evidence.

As the Criminal Law Revision Committee recognised, 'the increasing use of computers by the Post Office, local authorities, banks and business firms to store information will make it more difficult to prove certain matters such as cheque card frauds, unless it is possible for this to be done from computers'(CLRC 1972, para 259).



Admissibility

The law of evidence is concerned with the means of proving the facts which are in issue and this necessarily involves the adduction of evidence which is then presented to the court.

The law admits evidence only if it complies with the rules governing admissibility. Computer output is only admissible in evidence where special conditions are satisfied.

These conditions are set out in detail in section 69 of the Police and Criminal Evidence Act (PACE) 1984 (see further Nyssens 1993, Reed 1993 and Tapper 1993).

In general the principles of admissibility are that the evidence must be relevant to the proof of a fact in issue, to the credibility of a witness or to the reliability of other evidence, and the evidence must not be inadmissible by virtue of some particular rule of law (Keane 1994, pp 15-20; Tapper 1990, pp 51-61).

Real evidence usually takes the form of some material object (including computer output) produced for inspection in order that the court may draw an inference from its own observation as to the existence, condition or value of the object in question.

Although real evidence may be extremely valuable as a means of proof, little if any weight attaches to it unless accompanied by testimony which identifies the object in question and explains its connection with, or significance in relation to, the facts in issue or relevant to the issue.

This is illustrated in the case of R v Wood (1982) 76 Cr App R 23 where the appellant was convicted of handling stolen metals. In order to prove that metal found in his possession and metal retained from the stolen consignment had the same chemical composition cross-checking was undertaken and the figures produced were subjected to a laborious mathematical process in order that the percentage of the various metals in the samples could be stated as figures.

This was done by a computer operated by chemists. At the trial, detailed evidence was given as to how the computer had been programmed and used.

The computer printout was not treated as hearsay but rather as real evidence, the actual proof and relevance of which depended upon the evidence of the chemists, computer programmer and other experts involved.

The difficulty in the application of this rule lies in its interaction with the hearsay rule. Evidence is hearsay where a statement in court repeats a statement made out of court in order to prove the truth of the content of the out of court statement (Sparks v R [1964] AC 964).

Similarly evidence contained in a document is hearsay if the document is produced to prove that statements made in court are true (Myers v DPP [1965] AC 1001).

The evidence is excluded because the crucial aspect of the evidence, the truth of the out of court statement (oral or documentary), cannot be tested by cross-examination. (1)

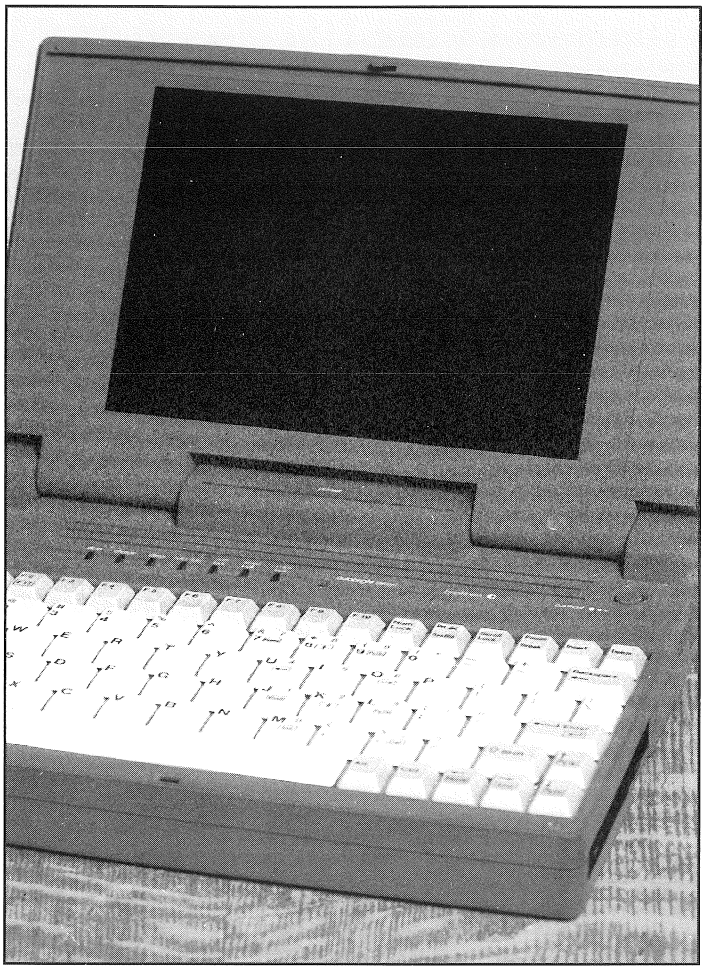
The problem, however, occurs because some statements, although in form assertive and inadmissible if they were to originate in the minds of human beings, in fact originate in some purely mechanical function of a machine and can be used circumstantially to prove what they appear to assert.

The basis for this view was laid down in a case having little to do with computers. In the Statute of Liberty [1968] 2 All ER 195 a collision occurred between two vessels on the Thames estuary.

The estuary was monitored by radar and a film of the radar traces was admitted into evidence. Simon P rejected the argument that the film was hearsay - he held that it constituted real evidence and not hearsay and he placed it on a par with direct oral testimony.

Where machines have replaced human beings, it makes no sense to insist upon rules devised to cater for human beings but rather, as Simon P said 'the law is bound these days to take cognisance of the fact that mechanical means replace human effort' (at p 196).

This useful distinction was apparently overlooked in R v Pettigrew (1980) 71 Cr App R 39, where the prosecution wished to prove that some bank notes found in the possession of the accused were part of a particular consignment despatched by the Bank of England.



A computer printout was used to prove this but the Court of Appeal held that such evidence was inadmissible under the statutory provision concerned (section 1 Criminal Evidence Act 1965 - now repealed).

The Court took the view that the operator did not have the requisite personal knowledge of the numbers of the bank notes rejected from the machine since they were compiled completely automatically by the computer.

This conclusion is quite accurate and a perfect application of the hearsay rule but it failed to consider the use of the print-out as real evidence. This confusion between hearsay and real evidence is unfortunate and it may explain why it was necessary to create special rules for computer evidence.

Criminal Proceedings

It is imperative that computer output should be readily used as evidence in criminal cases since otherwise many cases, particularly those involving dishonesty, would be immune from prosecution.

At the same time one cannot be too complacent about the technology since computers are not infallible. It is widely acknowledged that 'hacking' and 'viruses' may affect information stored on a computer.

These factors were obviously taken into consideration when enacting the provisions governing computer generated evidence in criminal proceedings.

(2) Section 69 of the Police and Criminal Evidence Act 1984 provides that:

"(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact therein unless it is shown- (a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer and; (b) that at all material times the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents."

In addition any rules of court made under section 69(2) must also be satisfied (at the time of writing no such rules have been made).

Real evidence and hearsay

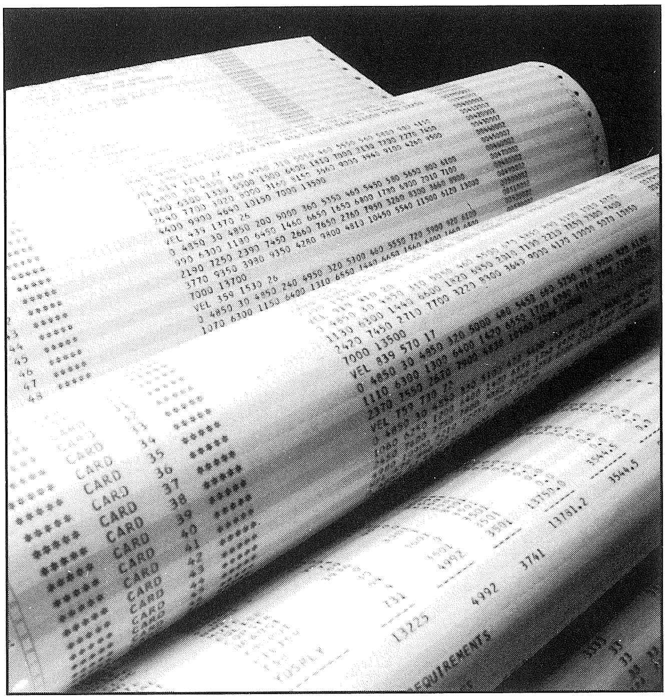
So far the discussion has focused on exceptions to the hearsay rule. However evidence derived from a computer constitutes real or direct evidence when it is used circumstantially rather than testimonially, that is to say when the fact that it takes one form rather than another makes it relevant, rather than the truth of some assertion which it contains. (3)

Direct evidence produced by a computer is not subject to the hearsay rule. As we have already noted, in R v Wood calculations were carried out by a computer specifically for the purpose of the trial to verify whether the composition of stolen metals matched original metals.

Computer output was admissible as real evidence since it did not purport to reproduce any human assertion which had been entered into it.

It was held that the machine was a tool and that in the absence of any evidence that it was defective, the printout, the product of a mechanical device, fell into the category of real evidence.

The court did recognise, however, that the dividing line between admissibility of computer generated evidence as real evidence or hearsay would not always be easy to draw.



The same distinction and result were reached in Castle v Cross [1985] 1 All ER 87 and in R v Spiby (1990) 91 Cr App R 186, CA an automatic telephone logging computer which logged the call details without human intervention was admitted as real evidence.

The Court also held that, in the absence of evidence to the contrary, courts would presume that such a computer was in working order at the material time.

Thus as far as the common law is concerned the status of computer evidence as real or hearsay will depend, in each case, on the content of the computer record, the reason for using it in evidence and the way in which it was compiled.

Cases like R v Wood and R v Spiby, however, must now be read in light of the decisions in R v Shephard [1993] 1 All ER 225, HL and R v Cochrane [1993] Crim LR 48, CA.

In R v Shephard the House of Lords held that section 69 PACE 1984 imposes a duty on anyone who wishes to admit a statement in a document produced by a computer to produce evidence that will establish that it is safe to rely on the document; such a duty cannot be discharged without evidence by the application of the presumption that the computer is working correctly expressed in the maxim omnia praesumuntur rite esse acta; and it makes no difference whether the statement is or is not hearsay.

In R v Cochrane it was held that before the judge can decide whether computer printouts are admissible, whether as real evidence or as hearsay, it is necessary to call appropriate authoritative evidence to describe the function. and operation of the computer.

In that case the prosecution wanted to prove that certain cash withdrawals were made from a particular 'cashpoint'. The machine would only dispense money if the correct Personal Identity Number was entered.

The matching was carried out by a mainframe computer and evidence of its proper functioning was thus required by the court. The prosecution did not adduce this evidence and the conviction was set aside on appeal.

As we have seen, a printout from a computer which has been used as a calculating device, or which records information automatically without human intervention, is admissible as real evidence and involves no question of hearsay. (4)

On the other hand, where the printout contains information supplied to the computer by a person, it is hearsay if tendered for the truth of what is asserted, but may be admissible under either sections 23 or 24 of the Criminal Justice Act 1988.

A statement can only be admitted under sections 23 or 24 if its maker (or the original supplier) had (or may reasonably be supposed to have had) personal knowledge of the matters dealt with.

Furthermore, under section 24 the 'creator' of the document must have been acting in the course of a trade or business etc.

A statement in a computer printout which has satisfied the foundation requirements of sections 23 or 24 can only be admitted on satisfaction of the additional requirements contained in section 69. (5)

Section 69 is couched in negative terms making it clear that evidence which does not satisfy its requirements is inadmissible. The object of section 69 is to impose a duty on anyone who wishes to introduce a document produced by a computer to show that it is safe to rely on that document and it makes no difference whether the computer document has been produced with or without the input of information provided by the human mind and thus may or may not be hearsay (per Lord Griffiths in R v Shephard at p 228).

The operation of section 69, therefore, is not limited to printouts that fall within sections 23 or 24 of the 1988 Act. (6)

Footnotes

(1) R v Blastand [1985] 2 All ER 1095, per Lord Bridge at p 1099 where he stated that "The danger against which this fundamental rule provides a safeguard is that untested hearsay evidence will be treated as having a probative force which it does not deserve".

(2) See Steyn J in R v Minors; R v Harper [1989] 2 All ER 208 at p. 210; see also, to similar effect, Criminal Law Revision Committee, 11th Report, Cmnd 4991, 1972, para 259.

(3) See R v Wood (1982) 76 Cr App R 23; Castle v Cross [1985] 1 All ER 87; R v Spiby (1990) 91 Cr App 186.

(4) See R v Wood (1983) 76 Cr App R 23 and R v Spiby (1990) 91 Cr App R 186 (but cf R v Pettigrew (1980) 71 Cr App R 23). Back to text.

(5) R v Minors; R v Harper [1989] 2 All ER 208 (CA) at pp 212-3. Back to text.

(6) R v Shephard [1993] 1 All ER 225, per Lord Griffiths at p 229, rejecting the construction adopted in R v Minors; R v Harper [1989] 2 All ER 208 and followed in R v Spiby (1990) 91 Cr App R 186.

The author, **Amanda Hoey** LL.M., is a lecturer in law at the University of Ulster at Jordanstown, UK and can be reached on e-mail at a.hoey@ulst.ac.uk

This article was first published in the Web Journal of Current Legal Issues in association with Blackstone Press Ltd.

In the second and concluding part of this article next month, Amanda Hoey takes an in-depth look at the issues of reliability of evidence and asks whether the special provisions in law are necessary.

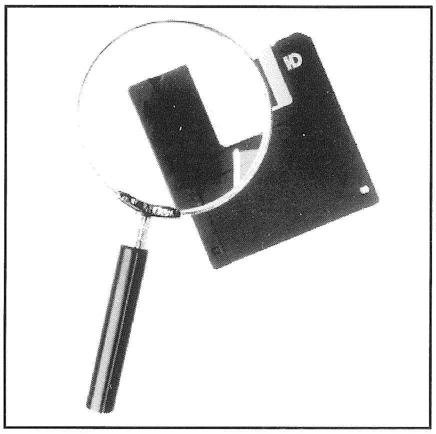
Forensic Q&A

Q **I have copied a computer that appears to have a small partition following the normal DOS partition. What is this and how can I access it?**

A This second partition is a regular feature of laptop computers. It is used to store the contents of the computer's memory and when the Suspend to Disk feature is activated.

The partition is usually about 80Mb large and is usually located at the very end of the physical hard disk. As this partition is not a DOS partition it cannot be accessed in any normal way, for example with file manager. The best way to access its contents is to use a program such as Norton Utilities to examine the very first sector of the computer's hard disk (Side 0; Cylinder 0; Sector 1) to ascertain the Side, Head, Sector reference for the start of the partition

Then view the first sector of the new partition and scroll through the data that is stored there and analyse its content.



Q **I have seized a Psion Organiser. How is the information stored and can it be retrieved?**

A Information on a Psion is stored on silicon based memory similar to RAM found in a PC.

This memory requires batteries to keep the information live inside the Psion, and should the batteries be removed or become discharged then the information will be lost.

A Psion contains both the main batteries and a small lithium backup battery. If the batteries have not been removed or have not become completely discharged, the information contained in memory can be retrieved by linking the organiser to a suitably configured PC by using a proprietary lead, and the information copied from the organiser to the PC where it can then be examined.

Q **How do you know if the batteries contained in the Psion organiser will last after it has been seized as evidence?**

A You don't, therefore it is always advisable to replace the batteries of any organiser as soon as it comes into the hands of the investigator. The person replacing the batteries should ensure that both batteries are not removed from the organiser at the same time, thus losing all stored information, but are replaced one at a time replacing the standby battery last.

Q **I have recovered a number of floppy disks that may have been used in a Canon Starwriter. How can I view and retrieve any information that may be contained on the disks?**

A These disks should be copied using standard disk copy procedures. The copies can then be accessed using any text based viewing engine such as Notepad, Write and Quick View Plus. This will only show you the context of the information contained on the disks. If you require the document to be printed as it was produced this will have to be done using a Canon Starwriter.

If you have any questions, comments or suggestions, e-mail them to the Journal at ijfc@pavilion.co.uk

Notice Board

We will be pleased to receive contributions to this page. Please mark all correspondence 'Notice Board'. We reserve the right to edit if required.

Events

Building an Enterprise Security Architecture

20-21 April 1998, Stockholm
23-24 April 1998, London

This briefing is designed to show information technology, information security, audit, and division managers how to create an enterprise security framework that will promote inter-operability and protect a corporation's network.

Contact: MIS Training Institute
Tel: +44(0)171 779 8944
Fax: +44(0)171 779 8293

Advanced Computer Audit Workshop

27-30 April 1998, Bristol, UK

Hands-on course programme includes auditing communications networks; auditing operating systems and system software; auditing database systems; client/server systems.

Contact: Margaret Mason, System Security Limited
Tel: +44(0)1625 523205
Fax: +44(0)1625 526952

Infosecurity 1998

28-30 April,
London
Contact: Reed Exhibitions
Tel: 01844 262728
www.infosec.co.uk

DIBS© User Group

30 April-1 May, Newcastle
Contact: Dave Lattimore
Tel: +44(0)1189 504611

Tools for Tackling Telecoms Crime

11-15 May
Manilla, Philippines

The event is billed as a comprehensive training program to help operators prevent and combat crime in the global telcoms industry.

Fraud and security experts will take part in the five-day course, and topics covered include customer and distribution fraud, technical fraud, technical attacks and network security, internal crime, intelligence management and the investigative deterrent.

Praesidium commercial director Gary Bernstein said: "The course will provide a clear definition of today's criminal and fraudulent trends while introducing complete effective solutions to meet the problems head on."

Contact: Lisa Williams, Praesidium,
Tel: +44 (0) 1249 467800
Fax: +44 (0) 1249 467809
Email: lisa.williams@praesidium.com

Network Security and Audit Workshop

18-19 May 1998
Bristol, UK

On this two-day workshop participants will have hands-on access to network control systems, and learn about their risks and the security issues; find out how to build secure and stable networks; see how to conduct a thorough audit of network environments, and use some of the available audit software.

Contact: Margaret Mason
System Security Limited
Tel: +44(0)1625 523205
Fax: +44(0)1625 526952

NetSec '98

15-17 June 1998
Hyatt Regency Hotel, San Antonio, Texas

This conference focuses on the security issues, problems and solutions of network systems. Topics covered include Windows NT security, Internet security, e-mail security, LANs and WANs, remote access and telecommuting.

Contact Computer Security
Tel: +1 415 905 2626
Fax: +1 415 905 2218
E-mail: csi@mfi.com

Financial Frauds on the Internet

June 1998, Madrid

Advanced strategies and techniques for preventing on-line frauds.

Contact: D&D Comunication
Tel: +39 2 58 30 61 65
Fax: +39 2 58 31 56 55

Training

Training in Computer Forensics

Four modules comprising: Fundamental Computer Forensics, Applied Computer Forensics Advanced Computer Forensics, Legal and Procedural Computer Forensics

Contact: Computer Forensics Ltd
Tel: +44(0)1903 823181
Fax: +44(0)1903 233545

Appeal for information

Dave Lattimore, from the Thames Valley Police Fraud Squad in the UK, is appealing for information about a hacker who uses the handles "Infamous Crew" and "Toker 999".

Dave writes: "A hacker gets into voice mail boxes belonging to major companies and changes the configuration of that box.

"When the target company closes for the day and switches the mail box on the hacker then controls it obtaining details of people ringing in.

"At present he has hacked into a major software company, a bank and an oil company. If any person has received any complaints regarding this hacker, please let me know so that I can collate these incidents."

Contact Dave Lattimore at Thames Valley Police Fraud Squad, Castle Street, Reading, Berkshire, RG1 7TH, UK.

Tel: +44 (0)1189 504611

International Journal of
FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd.