ISSN. 1363-6650

DECEMBER 1997
Issue 12

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

The usual arguments have once again been drudged up over the future of the Internet. Is it safe for kids? Do thousands of predators lie in wait in cyberspace for the next innocent victim? Can there ever be any control?

After an important part of the US's Communications Decency Act was overruled earlier in the year, the American moral majority has been ever more perturbed by the ever increasing use of computers, particularly by children.

This culminated in the recent summit (full report on page 12) attended by leading politicians, government and law enforcement figures and the major industry representatives. Predictably, the gathering attracted intense controversy.

Before the conference had even begun, some conservative groups blasted the effort as little more than a public-relations gimmick, while others fear self-regulation will wind up stifling free speech on-line.

Because of the commercial nature of the Internet, business interests will more often than not come out on top. This is not necessarily a bad thing as it guarantees a fast technological expansion fuelled by the need to stay ahead of the field and make a profit.

Manufacturers and Internet service providers are constantly looking to increase the level of services offered and up the speed at which they are delivered, all to the consumer's benefit. But it's all too easy to just lose perspective and confuse the medium with the message.

There's a lot of rubbish on the Net, as anyone who has spent half an hour surfing it will know. Most of it, while inane, is completely harmless. But there is a tiny percentage of material in cyberspace which is truly revolting and offensive to all but the most debased in society.

The danger is that anyone with suitable equipment can access this if they persevere long enough - computers and telephone lines don't know or care if the user is eight or 80.

And most youngsters are actually more computer literate than their parents. What chance has a mother of guarding her son from the worst elements of the Web if she doesn't even know how to turn a computer on?

This is the context in which the Washington summit was set, and the general consensus and direction has to be applauded. The Internet was recognised as a serious media capable of many things, both good and bad, and was given the serious attention it deserves. True, little in the way of concrete policy was created, but at least the main message was strong and clear.

Perhaps the most positive outcome of the meeting was the call to set up local education groups where everyone, including teachers, parents and children, can learn more about what the Web can offer as well as how to avoid the pitfalls.

And it finally looks like law enforcement agencies are beginning to wake up and start addressing the problem of Net crimes with a little more concern - policeman need educating about computers and their potential for abuse just as much as anyone else.

Despite its many critics, the summit has achieved a degree of success, if only for putting the issue back on the map and on the legislature maker's agenda. It'll be a long, slow process before society catches up with its creation and manages to harness it, but at least there's light at the end of the tunnel.

News

Croatia tackles crime

Computer criminals in Croatia will become the target of new laws next year as the country gets to grips with global standards.

From January 1, under a new legal code, the country will define as criminal such activities as computer hacking, breaking into databases and falsifying computer information.

Inspector Ognjen Haramina, who heads a small team of hi-tech police at the Interior Ministry's economic crime department said: "We have so far had no legal grounds to prosecute people who used computers to cause material or other damage to other people."

Haramina's team, trained by British officers, has processed some 30 to 40 cases of computer crime this year, but was able to press charges in only one, which involved distributing child pornography on the Internet.

"We are way ahead of any country in our region in terms of the suppression and control of computer-related crime," Haramina added.

Another key aspect of Croatia's new legislation is copyright and the country has upgraded the level of its intellectual property protection.

Experts say the new act makes it obligatory for state authorities to prosecute any copyright violation, rather than await private action by an interested party.

More than 90 per cent of all programs run on personal computers in Croatia are thought to have been obtained illegally, including many of those used in the state administration.

Passwords stolen in hacker break-in

An Internet service provider firm is investigating a security breach that allowed someone to give out internal system passwords to a hacker.

A security official at On-Ramp Technologies Inc., a ISP affiliated with Verio in the US, said the company had fallen victim to a leak.

"We weren't exactly hacked, in terms of our firewalls being compromised," said Joe Bush, chief technical officer at On-Ramp in Houston. But he added that a security breach did result in the release of "some internal administrative passwords that were only meaningful if used from internal, secured machines."

One Verio employee, who had been manipulated by "social engineering" techniques employed by one or more external conspirators, gave out the passwords, according to Hill.

One of On-Ramp's customers came into contact with one of the people involved when he bragged about his exploits in one of On-Ramp's chat areas.

"No customers have been affected so far, to my knowledge," Hill said. He added that Verio is working with the authorities to identify the hacker responsible for the incident and will prosecute all involved parties

Hill said that the same individual or individuals has possibly attempted the same technique against other Internet service providers and that other firms should be on their guard.

EU on digital copyright

The European Commission has published a set of proposals that it claims have been designed to deter pirates from stealing data on the Internet or other electronic networks to make illegal copies of music, films, or text files.

EC officials claim that the lack of inter-country legislation, apart from the Berne convention of copyright, means that there is a need for a pan-European copyright framework.

The proposals build on the outline of two global treaties agreed in the World Intellectual Property Organization last year, which have themselves drawn considerable criticism from a series of experts who claim that the treaties are either unnecessary, or seek to impose draconian restrictions on individuals' rights of access.

EC officials claim that the proposals have gone a long way towards answering the needs of the entertainment and publishing sectors in one corner and the telecoms operators, online service providers, and equipment manufacturers in the other.

They must be approved by Ministers from all 15 EC countries, as well as the European Parliament, before they can be considered for legislation.

The proposals also include provision to outlaw the marketing of electronic devices designed to flout existing protection systems, such as systems to beat software protection mechanisms.

Critics of the proposals say that they are too broad-ranging and fail to take account of issues such as private copying for own consumption and the liability of carriers (i.e. Internet service providers or telecoms companies) for copyright infringements.

Yahoo hacker virus threat a "hoax"

Hackers broke into the systems running Yahoo!, the Internet's most popular web site, and threatened to release a crippling virus into the world.

Calling itself PANTS/HAGIS, the group demanded the release of imprisoned fellow hacker Kevin Mitnick. The hacker's posted message read: "For the past month, anyone who has viewed Yahoo's page & used their search engine, now has a logic bomb/worm implanted deep within their computer.

On Christmas Day, 1998, the logic bomb part of this virus will become active, wreaking havoc upon the entire planet's networks."

The group also issued a statement regarding a possible antidote: "The virus can be stopped. But not by mortals." According to the note, the antidote would only be available upon the release of Mitnick.

But Yahoo! said the threat was a hoax and that no users were at risk.

Spokeswoman for the firm Diane Hunt said: "The main message to our millions of users is that there is no virus, no damage and no corruption of data."

Hunt confirmed Yahoo's service was hacked, but added "all of our safeguards worked. Within ten minutes, built-in electronic warnings went off and in almost the same period our staff of technicians detected the problem and took actions to stop it."

And the entire event lasted about 15

minutes, except where the message was held in data caching systems.

The hacker message, according to Yahoo, could not be read by the majority of Yahoo's 17.2 million users. "We use a table system at Yahoo and the hacker message was not in a table," added Hunt. "Only users accessing Yahoo with a Lynx browser, one capable of reading non-table text, could see this message."

The group is better known in the Internet world for its pranks and members say that the HAGIS part of their name stands for Hackers Against Geeks in Snowsuits.

Missing children tip line to go on Net

The National Centre for Missing and Exploited Children has set up a cyber tipline to report possible Internet child pornography and sex crimes.

It will give families the chance to call a national toll-free hotline to report incidences involving child sexual exploitation, including the online enticement of children for sexual acts and information on child pornography, child prostitution and child-sex tourism.

NCMEC president Ernie Allen said: "Until now, there wasn't a clear place to go if you saw something illegal going on in cyberspace."

The second phase of the launch, which will be operational in early 1998, will allow online users to use the Net to report information, which will be passed on to the FBI and other law enforcement agencies. The toll free tip number is +1-800-843-5678 or on the Net at http://www.missingkids.com/cybertip

Web sites at risk

Government web sites in Australia are vulnerable to cyber attack, the country's Parliament has been told.

The Federal Auditor General, Pat Barratt said: "There are a number of risks faced by Commonwealth agencies using the Internet including unauthorised interception of confidential material, outside hackers gaining access to material and imported computer viruses.

"As Commonwealth agencies expand their use of the Internet they will need to continually review the adequacy of the security."

The auditor's report on Internet security management found that most agencies had not fully planned their security policies and had failed to carry out risk assessment analysis.

Chain letter hoax

A bogus e-mail claiming to be from the office of the chief executive of Microsoft Corp asked users for money to avoid a system failure.

The letter explains that the recipient qualified for a $1,000 prize and asked for a credit card number and its expiration date.

"This hoax is quite well done," said Rob Rosenberger, the Webmaster of the Web site. "The first part of the letter sounds almost believable - well, only to those people not yet justifiably sceptical about Internet chain letters."

Under the title of "Legal Disclaimer," the spoof says the money compensates for an embedded executable virus program, or EEVP, that has been transferred to the reader's hard drive.

The $1,000 includes $257 to cover the user's loss of data, $43 for time and anguish, $93 for pain and suffering, and $9 or $10 for a couple of stiff drinks. And the remainder, $597, was to "buy a mythical future product from Microsoft to prevent a recurrence of this event".

Online gamers bet on loose restrictions

A new group has been formed to put forward the concerns of firms and individuals who use the Internet to gamble.

Members of the International Internet Gaming Association hope that self-regulation will keep the legislators at bay.

Dennis LaRochelle, chairman of the IIGA and an attorney with Donovan Leisure Newton & Irvine in New York City, said: "IIGA's purpose is to assist the Internet gaming industry in tackling the many issues presented by a regulatory framework ill-suited to deal with t gaming and modern technology."

At a recent Internet gambling symposium in Washington DC, several speakers provided estimates of the size of the new industry, with many forecasts ranging beyond $10 billion.

Much of the attention, however, was focused on legislative threats in the United States, particularly S 474, sponsored by Sen John Kyl, which seeks to ban Internet gambling.

The bill also would let federal, state and local officials to halt telephone and Internet service to computer gambling concerns, and provides for criminal penalties for violations, including fines up to $2,500 and a maximum of six months in jail.

Hacker to plead guilty

An Argentine computer hacker who was tracked down with the aid of the first court-ordered wiretap of a computer network has agreed to waive extradition and plead guilty to computer crime charges.

United States Attorney Donald Stern said that Julio Cesar Ardita, of Buenos Aries, Argentina, has agreed to voluntarily return to the US and plead guilty to charges contained in an Information filed in the US District Court.

During the summer of 1995, the Department of Defense detected intrusions into a number of military and university computer systems containing important information about government research on satellites, radiation and energy.

The activity was traced to a changing set of misappropriated accounts on an Internet host computer at Harvard University.

Stern's investigative team put together an electronic profile of the intruder, using key words such as unique names the intruder gave to files and Internet protocol addresses of systems being targeted by him.

This profile was used to apply for the wiretap order, the first ever obtained to search communications over a computer network, and to configure a monitoring computer which had been adapted to conduct the complex, high speed searches needed to isolate his activities.

Under the present treaty with Argentina, Ardita could not be extradited. US Attorney Stern said: "Solving this case required extensive cyber-sleuthing and great work by prosecutors and agents. Complex, international computer crime

cases such as this one will require ever increasing co-operation between countries both to investigate and prosecute."

Ardita has agreed to waive extradition and plead guilty to charges that he unlawfully intercepted electronic communications over a military computer and that he damaged files on a second military computer.

The agreement contains a joint sentence recommendation to the Court of three years probation and a $5,000 fine.

It also acknowledges that Ardita has co-operated completely and truthfully to date and had been debriefed over a two week period in Buenos Aires.

This case was investigated by the Naval Criminal Investigative Service and the Federal Bureau of Investigation. The case is being prosecuted by Assistant US Attorneys Stephen Heymann, Deputy Chief of the Criminal Division of the US Attorney's Office for the District of Massachusetts, and Jacqueline Ross, of the Northern District of Illinois.

Microsoft tackles software pirates

Microsoft Corp has filed a record eight law suits against suspected software pirates.

The company said the action stems from a single investigative sweep of Southern California computer resellers suspected of installing unlicensed software and illegally distributing counterfeit products at computer swap meets.

The products involved included Microsoft's Windows 95 operating system and Office 97 Professional Edition.

According to Microsoft spokesperson Sarah Alexander, the lawsuits are part of a programme the firm has launched in several key North American regions aimed at stopping the practice known as "hard disk loading, which is when pirated software is installed on computers that are in turn sold to customers.

Microsoft corporate attorney Jim Lowe said: "Microsoft has never before filed so many lawsuits resulting from a single hard disk loading sweep.

"This confirms that consumers need to be aware of how much illegal product is distributed at swap meets."

Lowe said the illegal activities were discovered over a three-month period by undercover investigators at various computer trade shows throughout Southern California.

Investigators posing as customers canvassed swap meets, contacting vendors of software and computer systems for counterfeit product and illegally preloaded software.

Man charged with porn possession

A 35 year-old man from Massachusetts in the US has been arrested on suspicion of storing child pornography on his laptop computer.

Domenico Mauro, of Watertown, was investigated by both the US Customs Service and US Attorney Donald Stern, and he is suspected of using America Online to receive the material.

Stern said: "Computer transmission of child pornography, particularly via online services and the Internet, has revitalised a very troubling means of victimising children, both those who are depicted in the pornography and those who are preyed upon using such images to break down inhibitions.

"The ease with which this crime is committed is no defence. The federal sentencing guidelines treat child pornography in general very seriously, and computer transmission even more so."

If convicted, Mauro faces a maximum penalty of five years in prison, as well as a fine of $250,000.

Quebec lawsuit seeks closure of site

The struggle for Quebec independence from Canada has entered cyberspace, prompting a Montreal-based party to seek removal of a controversial Web page from the Internet.

The pro-Canada Equality Party said it is launching a civil suit against a former Quebec terrorist who they accuse of issuing death threats and maintaining an inflammatory Web site.

And the party, which advocates unity between Quebec and Canada, says convicted Front de la Liberation du Quebec terrorist Raymond Villeneuve has threatened party members and others who support Canadian unity.

His Web site, at http://www3.sympatico.ca/scamire/presentation.html promotes separation from Canada and identifies prominent Canadian unity supporters.

Villeneuve, who now heads the radical separatist Mouvement de Liberation Nationale du Quebec, is accused by party members of inciting violence.

In 1970 Villeneuve was found guilty of manslaughter while a member of the now-outlawed FLQ. He served 12 years in prison for his role in a bombing that killed a maintenance worker in Montreal.

World's largest anti-virus library

Symantec has launched what it claims to be the world's largest online encyclopaedia of computer viruses. The database, which includes details on 10,000 computer viruses is complete with descriptions, a detailed overview of computer viruses in general, the different types of computer viruses, virus threats specific to the Macintosh platform and various virus hoaxes.

It can be reached at http://www.symantec.com/avcenter/vinfodb.html

Jail for Net abusers

Internet service providers who knowingly allowed child pornography to be transmitted to clients should face prison, an Australian minister claimed.

The West Australian minister responsible for censorship, Cheryl Edwardes, said she was disappointed to learn the federal government was not considering imprisonment for such offences and called for it to get tough on those transmitting child pornography.

Although the WA government, in its Censorship Act of 1995, was the first Australian administration to outlaw the knowing transmission of child pornography on the Internet or through other computer services, there are fears the federal government could change this.

Mrs Edwardes said: "Those who break the law face fines of up to $15,000

for individuals and $75,000 for companies or imprisonment for 18 months.

"Planned changes to Commonwealth legislation could potentially over-ride these provisions, meaning that service providers could only face imprisonment if they were actively involved in the distribution of the material.

"The federal government should send a clear message that any transmission of child pornography on the Internet is not acceptable and could result in jail."

School staff find porn on the Internet

Staff at a US school have been disciplined after they were found to have used education computers to visit pornography sites on the Web.

David Banis, deputy superintendent of the Pasadena Unified School District said staff were given passwords to use their home computers for Internet access and to send electronic messages for the purpose of school business.

A routine monitoring of Internet logs showed several visits to pornographic sites, but records did not show which staff had dialled them up.

France gets tough with paedophiles

French police have announced that a massive clampdown on paedophiles who use the Internet to swap illegal material.

Out of 50 people detained as part of the enquiry recently, five have been arrested and will be charged shortly. The roundups were the culmination of an eight-month investigation by the paramilitary division of the Gendarmes, the French police force.

The five people who have been arrested so far are those suspected of either taking, exchanging, stocking, or selling explicit photos of children via the Net.

Although all of the 50 questioned so far were French, investigations into several foreigners are now under way, and details are being passed to the relevant foreign government agencies.

This latest clampdown follows on from a series of arrests in the spring of last year, which culminated in the arrest of two directors at two French Internet service providers (ISPs) as part of an investigation into pornography.

At the time, the arrests were understood to be connected with the carrying by the companies of a network newsgroup containing child pornography.

The men arrested last year were directors at Francenet and WorldNet, two Paris-based ISPs. Although the two men were never prosecuted, the investigations into the Usenet newsgroup continued throughout the year, with police tracing anyone who left messages on the newsgroup.

- The French Government is expected to announce plans to create a high-technology fraud buster unit within its police operations.

The new unit would operate on a similar basis to the existing computer crime division, but with the remit to tackle the rising problem of white collar information technology-related fraud.

Although government officials have refused to comment, it is thought letters have been written to senior officials within the French judiciary saying that a new high-tech crimes division will be in operation by the end of 1998. It is thought the new, as-yet unnamed, division will have at least 200 staff.

FBI overstepping the mark?

An FBI wiretapping plan goes beyond the intent of the law and should be put on hold, civil liberties groups told the Federal Communications Commission in the US.

The FBI's wiretapping scheme grew out of the 1994 Communications Assistance for Law Enforcement Act (CALEA), which requires telecommunications carriers and manufacturers to build wiretapping capabilities into the nation's telecom infrastructure.

Under the law, the telecom industry must implement the plan by October 24, 1998. But according to the American Civil Liberties Union (ACLU) and other groups, the FBI's "wish list" of surveillance needs is an attempt to "strong arm the telecommunications industry into adopting surveillance capabilities well beyond what the law allows."

According to comments filed with the FCC by the ACLU, the Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation (EFF), the FBI is pushing the limits of the law, in calling for such standards as requiring every cellular phone to provide location information of users to police.

The FBI should not be in the business of drawing up the blueprints for our nation's telecommunications system," ACLU associate director Barry Steinhardt said. "That's like getting a Peeping Tom to design window shades."

Steinhardt said the civil and electronic liberties groups are urging the FCC to delay implementation of the act until October 24, 2000, giving industry time to adopt technical standards."

He added: "At present, neither the public nor the telecommunications industry are in a position to comprehend the scope of the capacity and surveillance requirements sought by the FBI."

According to the FBI, capacity requirements will be released in a final notice this January.

Sex offenders online

New York state attorney general Dennis Vacco has proposed that the names of sex offenders required to register under Megan's Law be posted on the Internet.

Vacco was talking at a Megan's Law task force meeting in Manhattan and under his plan, concerned people could submit the names of neighbours or teachers into a computer to check if they have been convicted of a sex offence.

He said: "It is indeed ironic that paedophiles can use the Internet to flood our homes with vile images of abused children, such as through the proliferation of child pornography, yet parents cannot use this medium to safeguard their children."

Vacco said posting names on the Internet, a practice already followed in five other states, would make information about convicted sex offenders more readily available.

Megan's Law was named for 7-year-old Megan Kanka, who was raped and murdered by a convicted sex offender who lived in her neighbourhood.

Product News

Net credit card fraud to "explode"

A company specialising in Internet security and commerce software has warned that business on the Web will be hit by a massive credit card fraud explosion unless action is taken now.

British firm JCP, a developer of Java-based Internet encryption technology, claims that e-commerce companies need to start taking direct action to counteract the problem of credit card fraud if electronic transactions are to succeed.

Narda Shirley, a spokeswoman for the firm, said that credit card fraud on the Internet is a growth industry that already costs millions of pounds a year.

JCP claims that an organised attacker prepared to spend around £36,000 on dedicated hardware can break the 56 bit DES technology on a magnetic stripe card in an average of 12 minutes.

"That means five cards an hour, 120 cards a day. If the attacker steals as little as £100 from each card, he can regain his investment overnight," Shirley said.

JCP claims that its Secure Internet Transactions Protocol (SIT) can solve a lot of the e-commerce industry's problems as regards card security. SIT is billed as the world's first protocol which addresses the issue of non-repudiation of Internet e-commerce transactions.

Non-repudiation means that transactions can be made legally binding because neither party can deny that a transaction took place.

JCP claims that, to be fully secure, an Internet e-commerce transaction needs to be not only confidential, tamper proof, and between parties who are who they claim to be (authenticated), but must also be non-repudiable, with an audit trail which provides evidence that a transaction occurred.

SIT is billed as an open standard. According to Shirley, the aim with the technology is to allow third-party companies to license SIT for inclusion in their own software applications.

Further details of the SIT software technology can be found on the Web at http://www.jcp.co.uk Contact JCP by phone on +44-7010-700527.

Internet watermark to beat theft

US firm Digimarc Corp says it has developed a security system to protect online images being stolen on the Net.

Currently pictures posted on the Net can be downloaded by anyone and used illegally without copyright permission.

But the Digimarc PictureMarc product embeds an indelible "watermark" into electronic images and files and its associated MarcSpider software follows every computer that downloads the image and reports back.

The company says that the technology can be applied to photographs, printed material, graphics, video and security products When a computer user tries to download a protected image, a warning sign appears telling them the picture is copyrighted.

Anthony Lupo, a Washington DC based attorney who specialises in Internet Law, said: "It's an incredible way to protect way to protect yourself on the Internet. The hardest thing is finding out where infringements are. MarcSpider takes care of that."

Keeping tabs on Net surfing

US firm Watchsoft has released a program to follow and record where users go on the Internet.

Called Disk Tracy, the CD-ROM software is aimed at parents to keep tabs on their children's activities, but could equally be used in business to investigate a worker's records.

Bill Holbert, the firm's president and program designer, said: "If your child, or even an employee, has downloaded computer hacking tools or bomb plans, for example, it will tell you about it as well."

Holbert added: "Disk Tracy has a URL (uniform resource locator) tracker that thwarts a child who attempts to enter a forbidden site through a back door, like Telnet or FTP.

"What we're doing with our program is following them around and counting the number of times a site is visited."

Results are printed out, complete with pictures and URLs.

Holdbert said: "Disk Tracy even identifies and lists files that have tried to disguise with incorrect extensions."

"Anyone can take a graphics file with a GIF or JPG extension and embed it into the body of a text file, or give it an EXE extension. Disk Tracy scans the system and reports back that a file was found with one extension, but was stored on the disk under a different extension."

"Even if the all the relevant information is erased from the computer, the master disk can be used to pull up the erased information."

To view a demo or get more information about Disk Tracy, go to the Web site at http://www.disktracy.com

Smut scanning

Demon Internet, which claims to be Europe's largest Internet service provider, has begun testing an automated scanning system for Usenet pornography.

The system relies on data from the Internet Watch Foundation a UK association of ISPs, which has set up telephone and online hotlines for members of the public to advise on suspect Usenet newsgroups and Web addresses.

Although many ISPs use feeder systems that delete offending messages, it's still possible for pornographic material to be re-posted to the same and even different Usenet newsgroups.

And since there are 26,000 Usenet newsgroups, it is almost impossible for anyone to keep track of them all.

Demon say this is where its automated scanning system comes into play, using data fed from the IWF. According to company officials, the new system has been designed specifically with the aim of eradicating child pornography from Usenet newsgroups.

The system works by scanning material as it is sent and automatically recognising material that has previously been deleted.

Cliff Stanford, Demon's founder and managing director, said that out of the few postings of illegal material into Usenet Newsgroups, such as child pornography, a significant proportion are repeats of previously removed material being posted to either the same or a seemingly

innocuous newsgroup, such as alt.disney.

He said: "The aim of this new system is to help streamline the process of finding duplicated illegal material on the Internet and reduce the number of abusers of the Internet by reporting and removing the material that has been sent."

James Gardiner, a spokesperson for Demon Internet, said that once the software has been tested, it will be made available through the IWF.

"The software takes an MD5 format fingerprint of each sexually explicit image that has been posted to the Usenet and has been removed for legal reasons," he said, adding that when the software spots the same fingerprint anywhere else on the Internet, it alerts staff at the ISP, so they can take appropriate action.

Plans call for the new software to be used in conjunction with the IWF's program of identifying, reporting, and removing illegal material from newsgroups.

The IWF was set up in September of last year as an independent body to address the problem of illegal material on the Internet, with particular reference to child pornography. The group's web site is at http://www.internetwatch.org.uk and Demon Internet can be contacted on +44 (0)181 371 1234 or E-mail: sales@demon.net

Blow to bank fraudsters

Banks in the UK are fighting back against fraud with the launch of an expanded electronic database to check on suspect credit cards.

Card Clear, which already distributes the system to 8,500 retailers, has been awarded two contracts which will give it sole responsibility for collecting and distributing information on lost and stolen credit, debit and cheque guarantee cards.

The firm, which merged last year with Cardcast, its main rival in the UK, collects stolen card information from more than 20 banks, including Barclaycard, the UK's biggest card issuer.

And the new contracts with the Association for Payment Clearing Services, which represents the main banks and financial institutions, will enable Card Clear to gather data from 73 issuers, creating a much more comprehensive file.

The databases have been one of the most important weapons in the fight against fraud in the UK, helping banks to cut the total losses from a peak of £165 million in 1991 to £83 million in 1995, although levels are now up to about £97 million.

European law archive

All aspects of European law together with supplementary material will be available on a new CD-ROM.

Technical Indexes, a UK supplier of specialist information services, says the software database draws from three key European information sources: CELEX, DTI Spearhead, and the Spicers Centre for Europe database and contains the full texts of all European Union treaties, agreements, legislation and case law.

The service is updated every 60 days to give users the latest information.

Further information is available from the Customer Support Department at Technical Indexes, Willoughby Road, Bracknell, Berks, RG12 8DW. Telephone: 01344 404409. Fax: 01344 404421. Email: c.supporttechindex.co.uk

Online law search

Legal professionals can now use standard Internet World Wide Web browsers to access the LEXIS-NEXIS information database with the launch of a new service.

The US firm says the Xchange facility at www.lexis.com offers a single location on the Web for legal professionals to get legal and general news, access practice-specific information search the legal archives.

Current summaries of high profile cases and significant legislation from Congress, as well as news updates from CNN are available on the service. Legal professionals can individually tailor LEXIS-NEXIS Xchange to their practices by automatically creating links to the specific types of information on the service.

For more information, customers can contact LEXIS-NEXIS at +1-800 528-1891.

Legal research system

A new breed of electronic legal discovery system was used to perform research supporting a $9.5 billion dollar company acquisition.

Lawyers from across the US used a private internet network and document retrieval system created by Thunderstone EPI Inc, based in California.

The firm set up a web interface to the massive database and lawyers connected to the system to perform queries and generate reports.

CEO of Thunderstone Bart Richards said: "This was an amazing process. We had less than two weeks to deploy a system that would import, catalogue and search more than 500 gigabytes worth of JAZ and ZIP disks.

"The disks contained every conceivable data type, from mainframe to ancient DOS-based word processor files."

For more information about Thunderstone's suite of software programs that search, manage, filter and retrieve information, contact the firm at +1 216 631 8544, e-mail info@thunderstone.com, or on the web at http://www.thunderstone.com

Fingerprint technology

US firm NEC Technologies has launched a system for the electronic capture, storage and transmission of fingerprints.

The firm says that its LS-21 live scan system performs more reliably than other systems which work by scanning inked fingerprint cards and that the images can be sent electronically within seconds to other law enforcement groups.

Vice president of NEC AFIS division Bill Wells said: "Unlike traditional fingerprinting methods, the LS-21 system captures and monitors prints electronically, creating the most accurate fingerprint records available.

"It's easy to use advanced digital technology make sit the most sophisticated fingerprint capture system in the world."

For more information contact NEC at +1 888 AFIS NEC or by e-mail at chen@necafis.com

Court reports

Pair banned from Net name trading

Two men have been banned from trading Internet domain names in the London High Court, following several months of legal wrangling that culminated in multiple lawsuits being taken against them.

The affair started earlier this year when Richard Conway and Julian Nicholson formed several companies, including One in a Million Limited, to register domain names that were similar to the trademarks of well-known companies, and then offered them for sale or hire to potential users.

Two of the plaintiffs in the case, Burger King and Ladbrokes, were advised by Virtual Internet, which claims to be the largest domain name issuer in the UK. The case centred around the allegations that all of the domain names were apparently registered without the consent of the owners.

Matters came to a head when lawsuits from BT and Orange were served on the pair. Now the London High Court has banned the pair from "domain name trading," with the judge in the case warning that the practice would not be tolerated.

The case has set a major legal precedent for the UK Internet world. Jason Drummond, the managing director of Virtual Internet, said that he was happy that the plaintiffs had won their case.

He said: "Domain name registration relies on the integrity and good faith of the applicant. Companies that abuse that system and register domain names that are clearly trespassing on another organisation's intellectual property, purely for personal profit, should be stopped, as in this case." He said that names need to be made available to their rightful owners.

According to Drummond, one of the defendants, Richard Conway, wrote to Burger King offering to sell it the name "burgerking.co.uk." for £25,000 (US$40,000) plus sales tax. He claims that Conway informed the firm that, unless it bought the domain name from One in a Million, it would be available for sale to any other interested party.

In court, Deputy Judge Jonathan Sumption QC said that the Internet had no central regulating authority and was almost entirely governed by convention. He stressed that the mere registration of a name was not, in itself, passing off or infringement of a trademark, but the obvious threat was there and injunctions should be granted to prevent it.

As a result of Judge Sumption's comments, injunctions have now been granted against the pair and their businesses, One in a Million Limited, Global Media Communications, and Junic. The pair have also been ordered to pay £65,000 (US$110,000) in legal costs.

Judge Sumption also directed the two men to have the disputed names assigned to the complaining companies.

But the dispute is not yet over as the pair have now been given leave to appeal by the High Court.

After the hearings Conway said: "They (the plaintiffs) could ask for the domain names to be handed over, but, if the appeal is successful, we could ask for them back. We don't think it's likely that they will ask for them to be passed over until the case is decided."

He said that when he and Nicholson formed One in a Million Limited, they were both students. "We registered these names and, far from us approaching these companies, we waited for them to contact us. When the IT director of Burger King phoned us to say that he had been asked to obtain the name, he asked us how much we wanted for the domain names. We came up with the £25,000 price tag as a price out the air."

The pair had registered the domain names of virgin.org, bt.org, sainsburys.com, ladbrokes.com, marksandspencer.com, and cellnet.net, all large UK companies.

According to Conway and Nicholson, despite the apparently conclusive nature of the original judgement, which has been widely reported, they still feel that their actions do not justify the order made against them. "It's most certainly not over yet," said Nicholson.

"It needn't have even got to the first Court hearing, but now the matter will not be closed for many more months, possibly years," Conway added.

One in a Million's Web site is at http://www.million.com

Stolen parts probe nets 16 convictions

An investigation into stolen computer equipment and parts has resulted in 16 people being jailed and $4 million worth of equipment being forfeited.

According to United States Attorney for the Eastern District of New York Zachary Carter, the Oliver-Allen Corp, of Larkspur, California, was convicted on money laundering charges following a corporate guilty plea before Senior US District Judge Leo Glaser.

The company was sentenced to a $100,000 fine and a one year probation.

Following a guilty plea to a criminal forfeiture count based on the money laundering conviction, Oliver-Allen also forfeited $780,000 to the US. At the same time, Mark Taylor, an Oliver-Allen salesperson, forfeited around $77,000 in a civil proceeding before Judge Glaser.

These funds represented the commissions Taylor earned in 1992 from his sales transactions with Computer Science Corp. of New York, Carter said. Along with pleading guilty to the charge of criminal possession of stolen property in the fifth degree in Criminal Court in Richmond County, New York, before Judge William Garnett, Taylor and John Howe, an Oliver-Allen vice president, were sentenced to an unconditional discharge and ordered to pay court costs.

Carter said the convictions and sentencing end a case that started on August 14, 1992, when two Staten Island, New York residents, Joseph Lentine, then an unemployed 23 year old, and Joseph J. Terrano, then an IBM account customer engineer, "established and controlled" two Staten Island-based computer companies, Compu-Tech and Computer Science Corp of New York.

According to court documents and proceedings, the two companies were used to defraud IBM of approximately $35 million in computer parts.

Through Compu-Tech, Lentine and Terrano placed orders for IBM AS/400 computer parts from IBM's West Orange, New Jersey office by manipulating IBM's internal computer system, court records show. With assistance provided by a corrupt IBM customer engineer, IBM's

Thailand's Net

standard delivery and payment procedures were bypassed, and the Compu-Tech account was opened without a credit check or COD requirement.

Lentine and Terrano then retrieved the equipment and resold it to Computer Science Corp to five reseller or computer brokerage companies nationwide at approximately 20 per cent to 80 per cent of its secondary market value to the tune of about $5.8 million.

One of these companies was Oliver-Allen, which in late 1992 bought about $2.1 million worth of AS/400 parts.

Lentine and Terrano fled to the Cayman Islands, where they were arrested and, after waiving extradition, they pleaded guilty in federal court in Brooklyn to wire fraud.

The FBI investigation, which ran from September 1993 through May 1995, operated through an undercover company in Brooklyn, and then in Staten Island, which engaged in the nationwide sale of what were purported to be millions of dollars worth of stolen IBM computer equipment.

As a result of the undercover investigation, two computer brokers were arrested on stolen property charges from July 1994 through December 1996.

Twelve defendants pleaded guilty to conspiracy to transport stolen IBM equipment in interstate commerce in US District Court in Brooklyn; 11 defendants are awaiting sentencing, where they each face a maximum sentence of five years in prison, a $250,000 fine and restitution to IBM.

And in October, a federal grand jury in Brooklyn returned an indictment charging Michael Knutson, president and CEO of US Data Inc, an Atlanta computer dealer, and Julian Harper, vice president and CFO of US Data, with conspiracy to transport stolen IBM computer parts in interstate commerce.

If convicted, they each face a maximum sentence of five years imprisonment, a $250,000 fine and restitution to IBM.

The the trial on these charges, which are based on the defendants' dealings with the FBI undercover company, is scheduled for May 11, 1998.

Finding a consensus on how the Internet should be regulated in Thailand is proving to be a difficult task, experts say.

Attorney General Office Prosecutor Shinnawat Thongpakdee said the law defines and protects human rights and duties and inevitably involves itself with human behaviour.

As the Internet is a phenomenon related with human behaviour as well, it would "unavoidably" be involved with the law as well.

Thongpakdee said that there are several "rights" involved with Internet information: the right to control access to information, right of information use, the right of copying information, and the right to publicise information and that these rights cannot be separated.

The rights come from several laws - "without laws, there are no rights," the prosecutor said.

In the Internet world, the producers of information own the copyright to their work, and consequently, any law regarding the Internet should also go hand in hand with copyright laws.

There is no solution at the moment as to whether there should be compulsory laws regarding the Internet because it's difficult to use legal means to enforce such laws, and they would also vary greatly from one country to the next.

One practical approach would be drawing up of a worldwide conventional agreement regarding Internet regulation, allowing each country to sign off of their own choosing.

At the very least, he said, we should accumulate information concerning the Internet in order to consider what should be allowed or prohibited - this information would be useful in the future.

Mr Shinnawat added that Internet technology is very new for the legal sector and other societies, and it was difficult to make any conclusions in legal term about the Internet at the moment.

According to Internet Thailand Service Centre President Trin Tantsetthi, infringement on the Internet has increased greatly during the last year, and laws regarding the Internet would be very hard to enforce.

For example, there were already 30,000 documents on the Internet in Thailand already.

Copyright infringements on the works of others was wrong in both moral and legal terms, he said, but using legal means to deal with it would prove difficult. Social pressures might be an alternative.

Wanchai Kanti, of Thammasat University, said people should have freedom of speech and freedom to express opinions, and that the flow of information "should not be closed", especially to academic institutes. There should not be laws to control Internet content, although opinions expressed should be done in a responsible manner.

By Sasiwimon Boonruang

New court to cover intellectual property issues

Thailand's Intellectual Property and International Trade Court officially began operating Monday. It has been four and a half years since the Justice Ministry proposed the establishment of the court to the cabinet on March 22, 1993, approved in principle May 4, 1993.

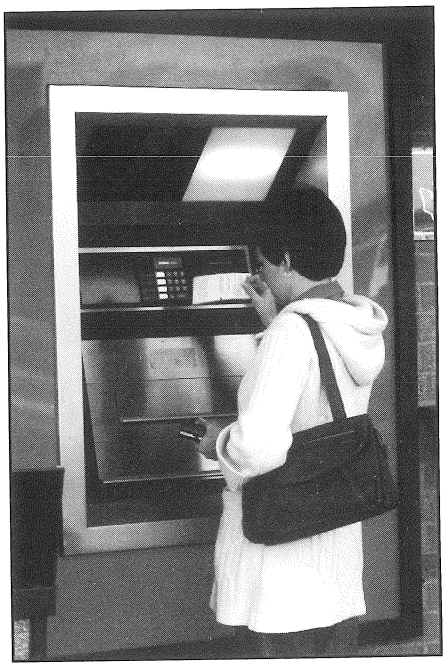
As a "special court", differing from civil or criminal cases, the IP and International Trade has been set up under the Intellectual Property and International Trade Law to judge all cases involved with IP and international trade issues. Consideration of the cases will be undertaken by the judges appointed by the judicial officers as well as co-judges, who are IP and international trade experts, selected by the Judicial Committee, holding their positions for five-years. The Court has the power to judge both civil and criminal cases involving intellectual property and international trade, covering some aspects of computer crime and technology disputes.

Cases considered under the IP Court will be decided more quickly and effectively than before since they will be taken care of by both legal and IT and international trade experts.

The cases to be considered must be submitted through a decision of the Supreme Court President.

Chaos Club hackers

A notorious group of computer hackers claim to have exposed a major flaw in the technology used by automatic teller cash machines. Paul Johnson examines the issue.



The Chaos Computer Club in Germany says that its members have found security loopholes in the way the machines read magnetic card stripes to confirm personal identification numbers.

In a recent "proof of concept" demonstration to security experts, Chaos club members showed how easy it was to clone a magnetic stripe from a legitimate Eurocheque debit/ATM card and clone the data onto a blank second card.

By running this data through a statistical analysis package that the club has developed, members generated around 200 "probable" four digit PIN codes for the card.

They explained that, by creating around 70 clone cards and progressing through all 200 sets of PIN codes, allowing the ATM to invalidate each clone card after three PIN attempts, they could eventually draw cash, as they did in the demonstration.

The whole process, using extra PC hardware costing under US $100, took an hour, and "generated" the equivalent of around US $350 in cash, a "profitable" concern in most people's books, once the minor legal issues are taken into account.

Christian Wolff, a Chaos club member said: "This card fraud is possible, despite the statement of the ZKA (the Germany banking authority), because at off-line ATMs and ATMs not in Germany, no central storage of failures is possible. The possibility of statistical analysis has been known to the banks for at least eight years."

After the demonstration, the German Central Card Authority, the ZKA, said that its system is still secure. It claims that cracking the PIN code is not just a matter of scanning through all the possible 9,999 combinations.

Wolff, however, said that ATM card four digit PINs can be derived from statistical analysis software. On the German Eurocheque system, for example, one out of every four PINs begin with a one, while the chance of a PIN starting with zero or a five is twice as likely as any other number, excluding one.

These factors, together with other PIN patterns, he claimed, allowed the club to crack the card PIN in well under an hour.

Wolff said that the club's purpose is to point out long-time flaws in the German banking system. "The club is showing the technical feasibility of computer fraud, which is otherwise not known to the public, which has meant the customer has to assume the responsibility of fraud rather than the companies," he said.

The Journal notes that the Eurocheque PIN crack by the Chaos Computer Club is likely to not to work for much longer. Most banks in the US, as well as in the UK, with the exception of some Plus/Link, MasterCard/Cirrus, and Visa ATM-accessible networked machines, store the PINs online, rather than on the card, a trend that is increasing.

Of the card issuers that store the PIN on the card (such as Eurocheque card issuers), the PIN is encrypted using 56 bit DES (data encryption system). As an additional security measure, the ATM does not decode the PIN code off the card, but encrypts the PIN entered by the user and compares the resultant code with the data read window on the magnetic stripe.

The Chaos Club - saints or sinners?

The Chaos Computer Club has achieved considerable notoriety both inside and outside Germany for its members' ability to perform major acts of unauthorised access to computer systems.

Like the Hacktic organisation in the Netherlands, the Chaos club says it exists to exchange IT (information technology) security knowledge, and publicise security flaws in supposed secure IT systems.

Others have accused the club of being little more than an IT anarchist's association, exchanging hacker information. However, since the club sprang into the public view in 1989, it has established a charter among its 200-plus members.

The charter is that members will not undertake hacking for commercial gain. In addition, club members will publicise loopholes and security gaps that have been found in sensitive systems and nets, and agreed not to alter any data in systems they enter.

Club members also agreed to help the IT industry to achieve a high level of security only for the most sensitive information (i.e. that relating to private individuals and research results). They will also help to avoid hacks by persuading the public and the influential to make as much information as possible generally available.

In February of this year, the club again entered the news when it demonstrated an ActiveX hacking program on Germany TV that allowed them to access copies of Quicken, the accounting software package from Intuit, and transfer money between bank accounts, without needing to enter the normal password security systems of Quicken.

Internet summit

An important conference in the US took the plunge into the issues of Internet crime, control and punishment. Although steeped in controversy, the meeting is seen by many as a positive step in fighting computer misuse. Paul Johnson reports.

Lead by former Federal Trade Commission member Christine Varney, Vice President Al Gore, and Attorney General Janet Reno, more than 400 business and government officials met in Washington DC last month for a three-day "Internet Online Summit: Focus on Children."

The summit was called by President Clinton last June after the US Supreme Court struck down sections of the Communications Decency Act as unconstitutional, and so provoking an intense debate over the issue of computer rights and wrongs.

While many groups criticised the meeting as a talking shop that lacked any real teeth, several important initiatives aimed at educating and training both the public and police were announced.

And firms working in all aspects of the industry were encouraged to take an active role in making sure they were acting as responsibly as possible.

"Never before have so many people from so many groups gathered to address issues faced by children and American families in the digital age," said Christine Varney, chairwoman of the meeting.

"This Summit is the first step toward addressing a full range of issues of concern to parents such as advertising and marketing on-line, privacy, the development of high quality content and equitable access," Varney said.

"We are committed to holding future meetings and are encouraged by the success in working together so far."

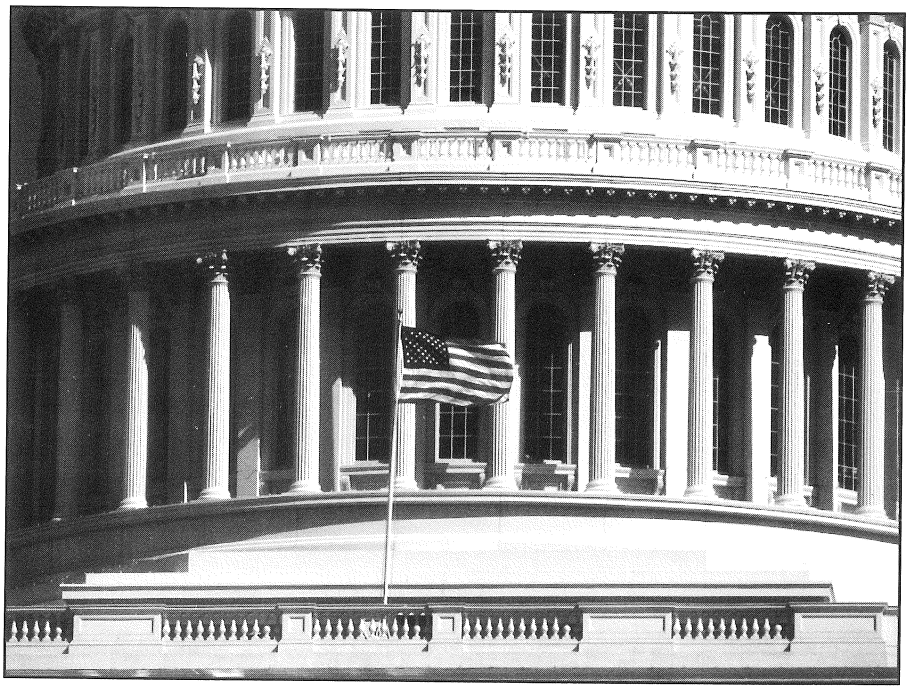
Attorney General Janet Reno praised private sector plans to protect children using the Internet from predators and promised more measures by law enforcement agencies.

Companies doing business on the Internet pledged to work closely with law enforcers in tracking down and reporting child predators and child pornographers. They sponsored a toll-free number for Internet users to report suspicious activity.

"These new initiatives are important steps in protecting our children from the hazards of the Internet. But these measures are only our first steps," Reno said.

"The Department of Justice is currently working with state and local law enforcement and with industry to identify additional measures designed both to identify predators who lure children away from homes as well as purge the Internet of child pornography.

"The rapid and global growth of the Internet raises a host of complex issues involving criminal law enforcement that expand beyond national boundaries."



Rep. Bob Franks, Republican of New Jersey, told the Washington meeting he favoured extending some anti-child abuse laws to companies providing Internet or online access.

Summit organisers are touting a new era of co-operation between online companies and government. "There's been tremendous progress as a result of work leading up to this summit over the past six months," says America Online attorney John Ryan.

The online industry and law enforcement officials, led by Reno, agreed to a program of "Internet alerts." The alerts are designed to allow the public to report illegal activity online, officials said.

Also proposed were public/private law enforcement partnerships, under which the online industry will cooperage with law enforcement by exchanging information on suspected online child pornography with the FBI, the US Customs Service, the Secret Service, State Attorneys General, and local law enforcement agencies.

The online industry also agreed to remove child pornography from their services and online bulletin boards.

The partnership, however, is far from the first time ISPs and other online companies have worked with law enforcement on child pornography issues.

In her address, Reno said police investigators have made amazing strides in the fight against online child pornography and those who stalk youngsters in chat rooms by deploying the same technology used by the criminals. However, the progress came from an ongoing, aggressive effort to keep on top of rapid-fire technological advances.

"We can't do it alone," Reno added. "Offenders are using the Web in new and ingenious ways, and so that's why I'm excited about the new relationships and initiatives that are being announced as

part of this summit."

One of the main challenges facing investigators into online crimes is tracking down perpetrators. The difficulty is compounded when young victims become unwittingly ensnared by offenders, the attorney general said.

"The youngest may not even know that something wrong has occurred" when a person they encounter online asks for personal information or requests a face-to-face meeting, Reno said.

She cited the Department of Justice's collaborative effort with state and local law enforcement agencies, dubbed Innocent Images, saying the initiative has "created an effective task force aimed at the sellers and chronic users of illegal pornography."

The effort, though relatively new, has helped the agency realise a 162 percent increase in legal filings against child pornographers, and a 263 percent increase in actions against offenders who transport minors with intent to sexually abuse them, Reno said.

She also cited the Child Pornography Prevention Act of 1996, revised earlier this year to specify that computer-generated images of children engaging in sex acts are also illegal.

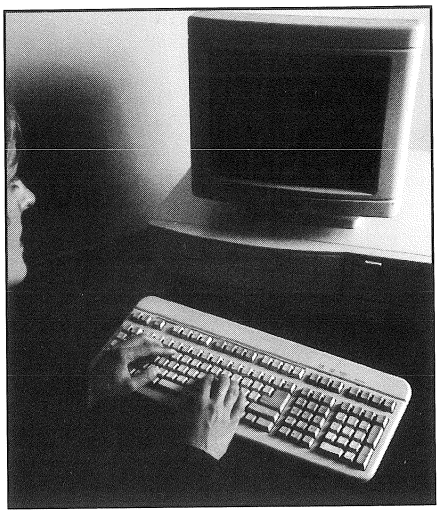
"This offensive against those who pray on and exploit children is making a difference," she said.

"I am proud of the vigorous efforts of our federal, state and local law enforcement officials in their efforts to target and prosecute those who use the Internet to harm children."

Reno said: "One of the greatest challenges we face in this area of law enforcement is to identify online predators in child pornography. Current technology often allows these criminals to mask their location and their identity.

"The rapid and global growth of the Internet raises a host of complex issues involving criminal law enforcement that expand beyond national boundaries.

"Law enforcement needs to know all it can about developments in Internet technology and in the online market industry. More in-depth training will foster co-operation and ensure that all investigations of cybercrime aimed at children are conducted using the most advanced techniques possible."



Reno also asked for continued co-operation in trying to enforce existing laws and to detect abuses against children as well as other criminal activities online.

"Instead of getting frustrated and saying, 'That's just law enforcement. They don't understand our problems,' I would appreciate your picking up the phone and calling me or writing me a letter, identifying problems and suggesting solutions," she said.

She pledged that law enforcement officers across the country would be better trained to appreciate and deal with the phenomenon of computer crime. The training sessions will demonstrate how new technology has created new types of crimes that open the door for new, high-tech ways to steal information or money or disrupt organisations.

The goal will be to close the gap between awareness and arrest by exploring how old-fashioned police work applies to new, electronic crime.

And the training will explore how to identify clues to online crime, identify tools and operations of online criminals, preserve evidence at a "crime scene," determine jurisdictional issues, identify information that might be valuable and its sources, and identify methods to track "e-criminals."

During his address, US Vice President Al Gore spoke to reaffirm his earlier call on the Internet industry to provide effective ways to shield children from the medium's dangers.

"Both the president and I have long been convinced the Internet is not a luxury or a diversion but an essential tool for children. In a short time, more kids will be online than any other demographic group."

He added: "As parents grow increasingly concerned about their children being e-mailed by strangers with questionable intent, and being the targets of unscrupulous advertisers, companies have stepped up to provide ratings systems and filtering tools which, while far from perfect, are an important first step."

Gore took pains to distance the Clinton Administration from earlier attempts at government regulation of the Internet – such as the infamous and ill-fated Communications Decency Act - by saying the administration supports "private-sector-led efforts" at content rating and filtering.

"Some say we should refrain from any action, that to take any steps to shield children from online pornography or hate speech would be censorship," Gore said. "To them I say: Blocking your own children's access to objectionable Internet material is not censorship, it's parenting, and the right of parents to do this is just as important as our First Amendment."

Gore concluded his 40-minute address by calling on law enforcement to aggressively enforce existing stalking, pornography and obscenity laws against virtual offenders.

He said: "It is a warning to criminals and a promise to parents there are Internet police for those activities that are illegal, and they will capture and punish those who abuse the Internet to harm and hurt our children."

"If Internet sites for kids continue to feature advertising blurred into entertainment and targeted directly to children, parents may soon shut off the Internet. If there is not an effective industry-led solution, you might as well prepare yourself for a massive, nationwide backlash that will stunt the growth of this exciting resource."

Others in government and law enforcement told the conference about the latest developments in combating Net abuse.

"The Internet is a faster, cheaper and safer way for child pornographers to move their product so the child pornographers are using it, as are paedophiles

in search of their prey," said Raymond Kelly, an under-secretary at the Treasury Department, which also is involved in enforcing anti-child porn laws.

Federal regulators, prompted by rising incidents reported by watchdog groups, are on the lookout for Web sites with exploitative and manipulative marketing to children.

However, some groups have been critical of the motives for the summit and fear the online/law enforcement partnership doesn't go far enough, attacking the new schemes as too little too late.

"This summit has been co-opted," Cathy Cleaver, legal policy director at the conservative Family Research Council said. "It's an expensive public relations stunt on behalf of the Internet."

The FRC takes a strong view on who is responsible for Internet safety, putting that responsibility directly into the laps of the Internet service providers.

Cleaver said she was pleased that ISPs are committing to the elimination of child pornography from their services, but added that ISPs need to rid the Internet of what she called "all illegal material they carry," not just child porn, but all hard-core material.

FRC President Gary Bauer said "It's a great day in America for online child predators. Law enforcement detectives call the Internet a 'dream come true' for paedophiles because it has taken the playground from the street into their homes. Even adult entertainment dealers say that 'there should be stronger government regulation' and that the Internet is 'a scary place'. It's time for the administration to get tough and hard-core pornographers to feel the heat."

Morality in Media President Robert Peters called the summit, and its emphasis on Internet access blocking software, "one more public relations gimmick intended to saddle parents with an impossible burden and to discourage Congress from putting the primary responsibility on those who create harmful content and those who knowingly profit from its distribution."

Although acknowledging that parental use of screening technology is needed, Peters said, "further legal regulation of indecent content is necessary to provide meaningful protection for children, and the onus should be on the Internet service providers that knowingly permit harmful material, not on parents."

The FRC, joined by the Christian Coalition and other organisations, is supporting a bill introduced by Sen Dan Coats that would require World Wide Web sites carrying material "harmful to minors" to block access by children or face criminal penalties.

The American Civil Liberties Union, on the other hand, said the White House was "trying to achieve by coercion what it could not through the courts."

"In its historic decision striking down the Communications Decency Act, the Supreme Court was clearly influenced by the wide range of socially available speech at risk under the law," ACLU associate director Barry Steinhardt said. "That speech is no less at risk today."

Regarding blocking software, David Sobel, staff counsel at the Electronic Privacy Information Center, said that "the reality is that in the interests of shielding children from a minute amount of inappropriate material, many of these approaches are removing from view a vast amount of valuable information."

See next issue's journal for a full report of the recent International Internet summit

The summit agreed on a package of schemes and initiatives, including:

- A program of "Internet alerts to allow the public to report illegal activity, and public/private law enforcement partnerships, under which the online industry will co-operate with law. The online industry also agreed to remove child pornography from their services.

- Internet companies will help make training videos to turn law enforcement officers into high-tech "cybercops" with the expertise necessary to investigate Net-related crimes.

The program is designed to raise awareness of how traditional financial crimes and street crimes are now committed online, including pyramid schemes, 900-number scams, phony talent searches, beat-the-system scams, harassment, threats, child pornography, child abduction, theft of or unauthorised use of credit card numbers.

- Creation of a national toll-free CyberTipLine for the US (800-843-5678), where parents can report suspicious incidents or online activity. The hot line will be run by the National Center for Missing and Exploited Children, with funding from both the government and industry.

- The government also is announcing a new booklet, The Parents Guide to the Internet, by the Dept. of Education. Parents can get a free copy by calling (US) 800-872-5327, or read the full text on line at www.ed.gov.

- America Online will make access to its parental controls easier. AOL is also launching a new "Neighborhood Watch" program and panic buttons labelled "Notify AOL" to report problems.

- A child-safe e-mail program created by Disney On-Line for members of Disney's Daily Blast (www.disneyblast.com), its online service for kids. Disney also announced plans for a family-oriented Internet directory of thousands of child-safe sites, and a Web-based safety education campaign for kids.

- Teach-ins, to take the form of town hall meetings will be held in schools, libraries and community centers across the nation.

The teach-ins will be preceded by a series of public service announcements starting this spring, providing parents with an 800 number and Web site to obtain a "tool kit" of resources for families.

Retrieving evidence

Frequently a forensic examiner is handed (or shipped) a computer and instructed to "find the evidence on this computer stuff".

When dealing with 20 Megabyte and smaller hard drives, this was a chore, but not impossible. Today, 2 Gigabyte hard drives are the standard minimum, and the quantity of files on a system ranges in the tens of thousands, if not more.

The task of finding the evidence is tedious and time consuming, and might require the case agent work with the forensic examiner for an extended period of time, reviewing the data.

This severely limits the productivity of the forensic examiner, whose time is frequently limited, as well as ties up the investigator for protracted periods of time. One solution to this problem is for the forensic examiner to preserve the computer evidence and provide a copy of it to the case agent in a format suitable for review, which does not require the presence of the computer specialist.

The following method utilizes Optical, CD-R or WORM technology to provide the case agent with a copy of the evidence, without danger of inadvertent alteration or modification of the data.

This method is relatively inexpensive, accelerates evidence processing, and maximises the productivity of the Computer Specialist. The hardware and software requirements are similar to those normally used to examine computer evidence, and also include a CD writable and software to "burn" the CD-Rs, generally bundled with the CD-R hardware.

Since many CD-R software packages require a single session write to the CD-R, the following structure should be created on the processing computer, prior to being written to the CD-R. Alternatively for larger type of media an Optical drive with WORM technology such as the Pinnacle Micro Apex drive will do a great job of handling those drives that cross the 2 GB threshold. As with any forensic processing of a suspect hard drive, create an image copy of the drive and secure the original evidence.

On a clean partition of the processing system (separate from the image copy, create a sub-directory for each logical drive that reflects the drive letter (e.g. C:DRIVE).

From an image copy of the evidence, copy the logical file structure of the corresponding partition to the sub-directory, retaining the original sub-directory structure. Create a sub-directory named DELETED and un-delete deleted files from the image copy into this sub-directory.

This should include files that may not be 100% recoverable. Create a third sub-directory called SLACK, and extract file slack to this sub-directory. Create a final sub-directory, called UNALLOC, and copy the unallocated file space to this sub-directory. If the case agent has provided a key word list, create a sub-directory called SEARCH to contain the results of any key word searches.

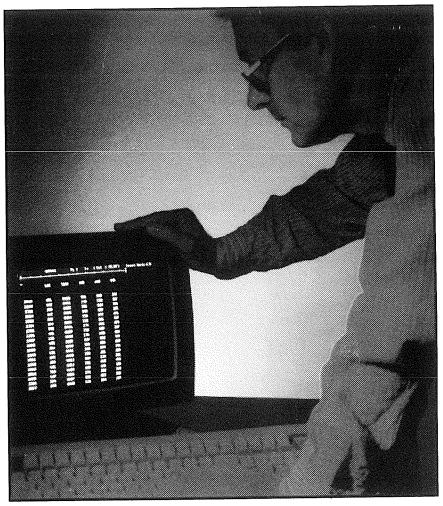
Create a sub-directory called COMPRESS, and as needed, additional sub-directories under COMPRESS, representing the file names of compressed files. These sub-directories should contain the results of restoring the files from the respective compressed archives. Create a sub-directory called ENCRYPTED to contain the decrypted versions of encrypted files, and the passwords used to decrypt the files.

The final component needed by the case agent is viewing software. Transfer a licensed copy of QuickView Plus (QVP)(INSO CORP.) for use in viewing the data. The QVP program should be installed on the agent computer, for use with multiple CD-Rs or optical drives.

Once this structure is complete, the entire partition can be burned to the CD-R, and transferred to the case agent for review. If relevant information is identified, the case agent can then notify the forensic examiner, who can recover the information from the image copy for inclusion in the forensic report.

For hard drives larger than 650 Megabytes (the size limit on current CDs), it will be necessary to use multiple CDs for storage. This is easily accomplished with this protocol, as individual components can be written to separate CDs.

After all of this is completed give the case agent a quick tutorial on how to use QVP (if needed) and turn over copies of the CDs/Optical disks to them and they can then review all of the data that is available and decide what is relevant to their case and what is not.



One additional aspect of using the CD-R/WORM technology is storage of utilities that you use to extract the data on the hard drive. By storing the utilities on that type of media you have effectively archived the tools for future challenges in court.

How many times have we processed evidence with version 1.1 and later upgraded to 1.2, 1.5, 2.0 etc. without saving somewhere the actual version that was used to examine the evidence. By storing it with the copy that goes into evidence we will have it available later if the use of the tool comes into question.

One caution, due to ISO 9660 standards long paths or long file names will be truncated when storing on a CD ROM so insure you include a list of the complete path/file name for the ones that are truncated.

What's next? With the deployment of DVD (Digital Video Disk or Digital Versatile Disk, depending who you talk to) we soon should have the ability to store up to 17 GB on one disk (both sides) and significantly improve our storage capability albeit increase the time it takes to review the evidence.

By **Howard Schmidt**, Director of Information Security, Microsoft Corp and

Raemarie Szymanski, senior instructor and computer crime specialist with the National White Collar Crime Center, US.

Feature

Hackers, Organised Crime and Security

By
Ian J. Hayward

Abstract

This article examines a number of definitions of what is commonly termed "Hacking", who or what these "hackers" are, the implications of these definitions, the role of the media in propagating the general public's view of these acts, and business managements' attitudes/responsibilities for maintaining these.

Computer crime has been said to be increasing on a global scale and yet management and law enforcement lags behind the criminals in detecting and preventing these acts. An analysis is undertaken of business managements' roles and attitudes toward computer system security in general, and, their apparent lack of appreciation of the extent and implications of unauthorised use of computer systems.

An analysis is also made of the possible uses of Artificial Intelligence in computer security measures to prevent this type of activity, with particular reference to the field of Biometrics.

The role played by 'organised crime' in the proliferation of computer related crime is examined along with its effect on law enforcement. An outline is given of the research being undertaken by the author, and some preliminary results, in this area with regard to common characteristics of `Hackers' and its possible use in the area of computer security preventative measures.

Introduction

The mass media has increasingly given much publicity to the misuse of computer systems by both authorised and unauthorised users, commonly this misuse has been referred to as either 'computer fraud' or 'hacking'.

Unfortunately, these terms have many different and diverse meanings to various groups of people. The term "hacking" means the altering of computer system software to achieve a task for which it was not originally designed, according to the majority of computing professionals. In contrast, the same term has been used by the mass media to cover a vast array of activities from unauthorised use of a computer by employees to intrusion into computer systems used for the control of telephone networks.

The majority of computing professionals prefer to use the term "cracking" to describe unauthorised access to a computer system.

This anomaly in definitions could be argued as one of the causes of the apparent lack of understanding within the general public and business management in particular of the frequency and diversity of unauthorised computer system use.

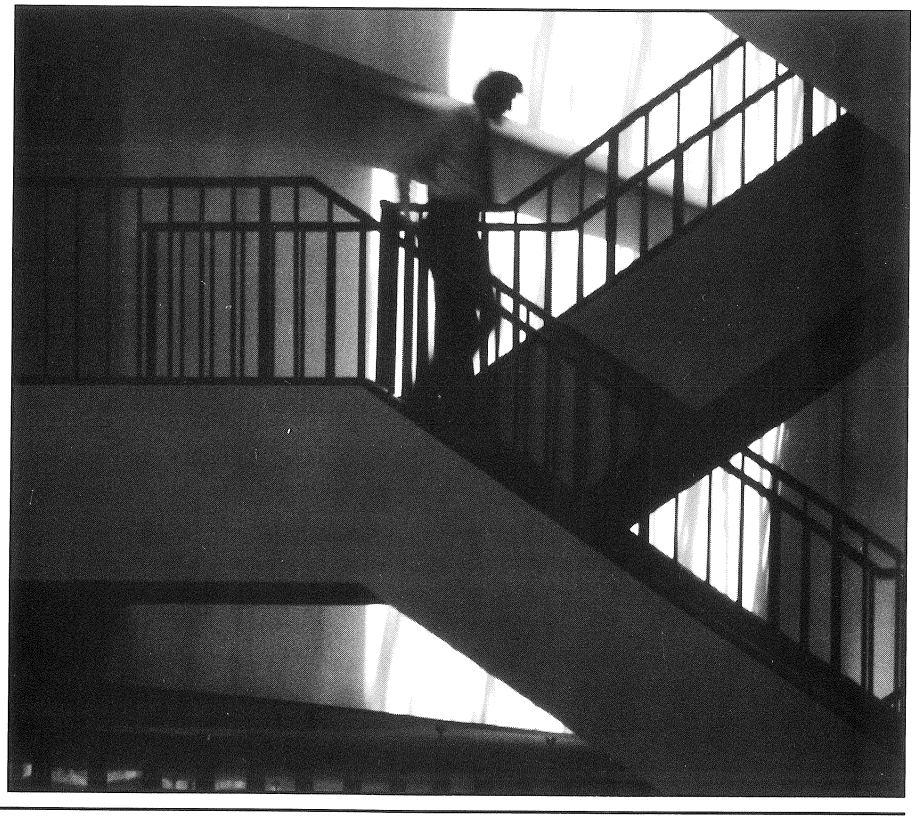
The actual number of "hacking" cases reported by business organisations to various authorities within Australia is relatively low (around 9 per cent of computer abuse incidents) with a correspondingly low monetary loss (under 1% of total loss).

Recent cases and events reported in the media, however, appear to indicate that either it is becoming more significant through the greater connectivity of computer systems, or, that the abuse of computer systems is being both detected and reported to authorities as a result of greater surveillance and co-operation.

This abuse of computer systems should be even more worrying when one acknowledges the ever increasing network of computer Bulletin Board Systems (BBS's) and third party providers of 'Internet' and 'World Wide Web' access.

A growing number of these BBS's etcetera are connected to the 'Internet' thus allowing their members direct access to any other computer system connected to the 'Internet' throughout the world, and access to the International Relay Chat (IRC) system.

This connectivity of computer systems must increase both the ease and therefore the likelihood of casual hacking by an ever increasing number of com-



puter users.

BBS users have the ability to leave messages to each other, download text files and programs, and, depending on the BBS's set up, connect to the Internet in order to utilise any or all of these with another computer system anywhere else in the world.

While the majority of these BBS's telephone numbers are readily available from lists published in various computer magazines (for example PC USER), those of a more dubious nature are generally passed from user to user via messages left on the BBS's or actual listing files contained on the BBS's.

A number of the BBS's have varying levels of access for users with the lower levels being for new users, limiting the amount of time they may be connected for and the areas they may access and use.

In most cases new users are only granted access to a very limited area of a BBS and must send in a subscription and/or further details about themselves, in order to be granted the right to download files or be connected for longer periods.

In order to gain access to the higher levels of the BBS it is quite often necessary for the would-be user to answer a questionnaire about hacking and or 'phreaking'.

One could assume that this method is used to restrict access to those with more advanced knowledge of the methods used to hack/phreak. Quite often the inexperienced hacker/phreaker can obtain a great deal of information by leaving messages, requesting advice on methods of attack, from other hackers/phreakers with more experience and knowledge.

These messages have been known to include general messages to all the users of a BBS giving the telephone numbers for connection to computer systems, along with known account names/passwords, or even giving stolen/forged credit card numbers.

In the 'files area' of BBS's, that users have access to, any number of text files or programs with instructions for carrying out 'hacking', 'phreaking', and 'carding' activities, along with copies of hack/phreak electronic magazines. These files cover a wide variety of operating systems, from VAX through to UNIX, and cover a diverse range of topics, from how to bypass security measures through to obtaining a copy of the password file on a system.

A large number of these BBS's keep files on them which enable users to carry out criminal activities which range from Credit Card fraud through to obtaining free international telephone calls.

As an example, I recently found a program on one BBS which enables the user to generate up to 999 genuine credit card numbers from one legitimate card number, to print a list of the owners details in a range of credit card numbers, to verify a credit card number as being genuine, etcetera.

As a result of all this activity, it is surprising that the reported incidence of hacking/phreaking is such a low figure. Are we to assume that a very small percentage of the perpetrators are ever caught ? Or is it more likely that few incidents are ever reported for various business reasons ?

Whichever is the case, the owners and administrators of computer systems can not afford to be complacent about the security measures they introduce to protect the data stored on their computer systems, particularly if those systems are connected to the Internet.

What is hacking?

The media has used "hacking" to describe virtually any abuse of an organisation or an individual that involves the use of a computer to carry out the action. Anything from embezzlement to computer viruses, have at some time, been attributed to the `hacker' community at large.

In addition to this the media often describes "hackers" as being sociopathic or malicious, thus creating a public image of the computer underground (`hackers' in particular) that most researchers would see as an exaggeration of their ability, and indeed, intent for causing damage.

The criminological definitions that do exist of the computer underground (or 'hackers') from a sociological perspective are less judgemental than those portrayed in the media but are still imprecise. Labels such as 'electronic vandals' (Bequai, 1987) and 'electronic trespassers' (Parker, 1983) have been applied to

'hackers'.

These definitions appear to keep away from labelling them as 'criminal' while still emphasising the fact that the actual act of 'hacking' should be considered a deviant behaviour.

Computer security specialists, in contrast, are often quick to label any computer underground participant as belonging to the criminal element of society. Some would even reject any notion that within the computer underground there are a range of different roles and motivations amongst the participants and would thus refuse to define what a 'hacker' or 'phreaker' or 'carder' actually does.

This reluctance to differentiate between the various roles and activities undertaken by the various groups within the computer underground has created a rather ambiguous definition of a "hacker" with the modern bank robber/fraudster at one end of the scale, and the trespassing teenager at the other end.

As a result, virtually any criminal, or even mischievous act, that in any way involves the use of a computer could be attributed to a 'hacker', regardless of the true nature of the crime committed.

Similarly, 'phreaking' is used to cover a wide variety of activities concerning the abuse of the telephone networks. This term was initially used to describe the illegal use of tone generators or "blue boxes" to gain free use of the telephone network.

It has undergone an expansion in recent years to include such activities as gaining unauthorised access to computer switching equipment which controls the telephone network, again with the intent of obtaining free calls and/or charging the call to another telephone subscriber.

The most recent activity is the altering of the identification code on mobile telephones in order to defraud telephone networks. The term 'phreaking' now encompasses the illegal use of telephone credit cards and tampering with `voice mail' networks.

The term 'carding' can be used for activities involving the illegal use of any type of credit card. While all of these activities involve fraud of one type or another the actual incident may be reported as hacking, phreaking, fraud, or a number of other infringements depending on where it occurs and who is actually defrauded.

This type of crime appears to be on the increase as society in general increases its use of credit cards and the availability of credit cards from businesses of various types becomes easier.

Whereas initially the misuse of credit cards was limited to stolen or forged cards by a relatively small element of the criminal world, with the growing number of BBS's and computer users connected to computer systems this type of crime is being undertaken by an increasingly wide spectrum of society.

In particular, there appears to be a greater number of cases reported in the media involving young high school students obtaining credit card numbers from BBS's and using them to purchase computer equipment via mail order companies. In some instances it has been reported that gangs of juveniles have been recruited by `Fagan' type adults to use stolen and/or forged credit cards to obtain all manner of merchandise.

Business itself appears to have maintained an attitude characterised by its own self-interest, rather than the need for the general public to know of the abuse of computer systems. Quite often, any employee who detects an incident involving computer abuse is quite often told to 'keep it confidential', resulting in a non-reporting of the incident to any outside body or organisation, and therefore there is no likelihood of any prosecution of the offender.

The company may take some action, to patch up the hole or problem, with additional or alternative computer operating or user access procedures. However, the idea of passing the information on to other businesses, is seen as losing the competitive edge they may have gained over their rivals.

Similarly, the majority of businesses are unlikely to report any incident to the various law enforcement agencies for fear of the incident becoming public knowledge.

You can imagine the plethora of reports appearing in the media if a multinational company had an incident of computer related crime taken to the courts.

The business itself may reach a decision not to report or prosecute offenders for fear of the adverse effects that could result through publicity of the incident. These effects may well range from a drop in share prices as investors sell off shares for fear of a drop in profits, through to a loss of business as customers find alternative suppliers for fear that customer details may be compromised.

Business and broader communities will continue to fail in their understanding of the impact of computer crime as long as this attitude of secrecy is maintained by businesses.

It could well be argued that business is playing into the hands of these hackers as long as there is no real deterrent against them committing these crimes.

If there is a minimal likelihood of detection, a lack of reporting to the relevant authorities and little or no chance of being prosecuted, these so called 'hacker attacks' are likely to continue unabated or in fact be on the rise.

Indeed, if one examines the small

number of cases that have actually come to trial, in the majority of cases the actual crimes for which they were sentenced was not for unauthorised use of computer systems but for illegal use of the telephone equipment which is attached to the computer systems, OR, for breaches of confidentiality of the data stored on the computer systems, OR, in many cases for credit card fraud.

Unless business and law enforcement agencies start working together in order to maximise the prosecution rate for these abuses of computer systems they will continue to increase in both number and severity.

Considering the occurrence of computer crime, we would do well to remember that the majority of crimes are actually committed by criminals who succeed to the extent that they are never convicted for them.

Consequently, much of the information gathered by organisations and individuals actually relates to the cases of failed criminals, that is the ones that did get caught.

Indeed, very little research has been undertaken as to who hackers are and/or whether they have anything in common. The majority of cases, which have been reported in the press, involve not an individual but a group of hackers yet we have no information regarding whether this is the norm.

We may well find that it is only when hackers work in a group that they are likely to be caught, and that there are common reasons why they are caught.

Keeping this lack of data in mind, why is there so little co-operation between businesses, authorities, and educational institutions ?

Surely, if this type of computer crime is seen as increasing in terms of both its frequency and its cost, there is a blatant need for more co-operation and data sharing. If data and experiences were shared we would likely see other areas of computer security highlighted, and some or all of these may be solved by a combined effort.

Who commits these crimes?

Having analysed approximately 250 reported cases of computer abuse it would appear that the historical profile of a 'computer hacker' as being `a teenager in a darkened room using a home computer and modem' is seriously in error. I have identified three main age ranges of people committing these computer related crimes :

(a) Those ranging in age from approximately 11 years to 15 years old, in other words High School students. The illegal activities carried out by this age range appear to fall mainly into the "carding" and "phreaking" areas.

The majority of cases involve the use of any hacking to obtain credit information which can then be used to gain free telephone calls and/or computer equipment/software by credit fraud.

The credit fraud has in the majority of cases involved using mail order suppliers and credit card numbers obtained via the computer underground. The other major area of credit fraud involves the use of telephone account numbers again obtained through the computer underground or by hacking into telephone company computer systems.

This limit to activities has been explained by some as a direct result of a thirst for knowledge and the obtaining of more powerful computer equipment as a means of gaining better access to more knowledge and higher social status within the computer underground.

Others, however, explain their activities as causing no harm to any individual because the company defrauded will 'pick up the tab'.

(b) Those within the 18 to 25 years old range, mainly University students or recently employed ex-university students. This age range undertakes activities in all three categories with the majority of cases involving a combination of all three.

The aim of the activities undertaken by this age range does not in general appear to be for financial gain but rather a quest for knowledge and social standing within the computer underground.

Some of the cases reported in the media have been labelled malicious as they resulted in damage to data stored on computer systems but in general the perpetrators have been quoted as stating any damage caused was definitely unintentional. Again, this group has in the main used any credit fraud activity to obtain computer equipment or free telephone connections rather than to gain financial advantage.

It is also this group which appears to be responsible for the majority of the computer viruses which have plagued the computer world. Can we explain these activities in light of their age and position in society ?

(c) The last major age range is from approximately 30 years to 45 years old. The major activities undertaken by this group appears to be that of

hacking for the purpose of espionage and financial gain. Some cases of credit fraud have been reported but in general these have been as a means of obtaining merchandise for resale rather than personal use.

One example would be the alteration of mobile telephone identification numbers and the sale of the use of the phone to other callers at a vastly reduced rate, or, simply reselling the telephone on the blackmarket after obtaining via credit card fraud.

Some would say this group is under more financial pressure as a direct result of mortgages, children, alimony and so on. Others would say they simply have criminal tendencies and would turn to crime of one form or another sooner or later.

Security measures

The physical security of computer systems and the control of access to them are generally regarded by security experts as the first line of defence against intruders (both legal and illegal).

Neither of these measures will completely prevent an inside user from stealing valuable information or using computer time for unauthorised purposes, they will however, significantly deter any attempt by outsiders to access the computer system.

The physical security of a system is generally regarded as the protection of the hardware and facilities from damage and theft. Controlled access is regarded as some means of identification of an individual user along with a privilege level before they are allowed to access various areas of the computer system.

Biometrics (the use of a physical/individual characteristic, which is measurable, to verify an individuals authenticity) has been proposed as one method of reliably verifying a users identification.

The biometric technology currently available deals with both a user's physical characteristics (fingerprints, hand geometry, retinal scan) and their behaviourial characteristics (signature dynamics, voice verification, key stroke dynamics).

All of these methods have been developed through the use of Artificial Intelligence (AI) software. This use of AI software has lead to some weaknesses in using Biometric techniques mainly due to their cost and the present unreliability of the behaviourial systems.

One of the major areas of concern to the computing community as a whole should be the numerous security holes in the various computer operating systems themselves.

Organisations such as CERT in the US regularly place warnings on the Internet News with details of breaches of security which have occurred at various computer installations.

These News items are available to anybody who can access the Internet News, thus the hackers themselves can gain access to this information. The majority of these breaches have been reported as occurring in the US but we cannot assume that the same loopholes have been not been used to hack into computer systems throughout the world.

One of the methods suggested by many security experts is to use what is termed a 'firewall', where access by the outside world is only given to one computer in a network which has been made extremely secure, the firewall has the capacity to test the communications and pass/refuse services of interest to the rest of the computer installation.

Artificial Intelligence has been proposed in some areas as a means of increasing computer security by monitoring the behaviour of computer users.

The basic idea being that, if enough information of users' past behaviour (on the computer), is developed in a knowledgebase, any noticeable change in behaviour can be established and acted upon. In many ways, this is really only a means of detecting a crime after it has been committed, it is not a method of crime prevention unless it is developed into a deterrent - artificially intelligent in itself - regarding software development.

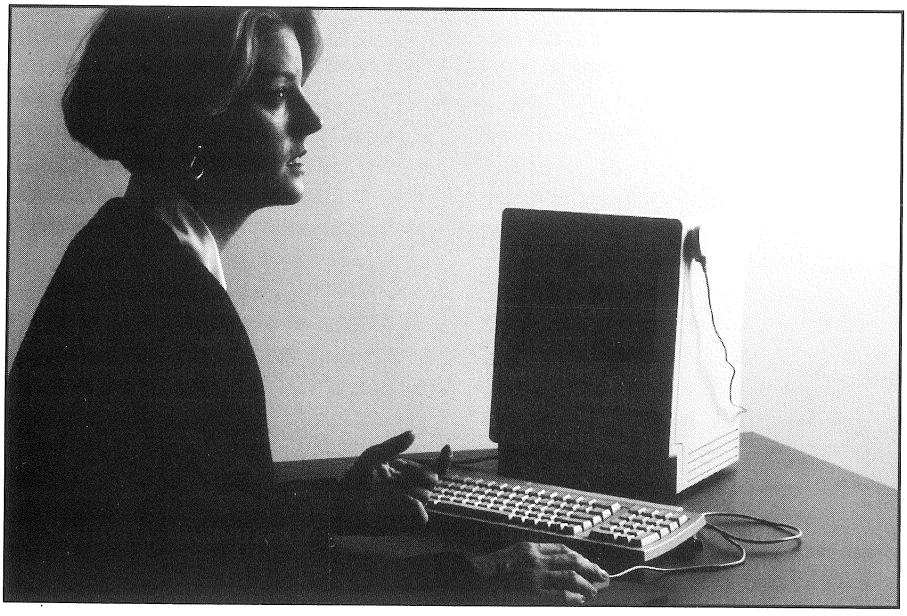
Organised crime

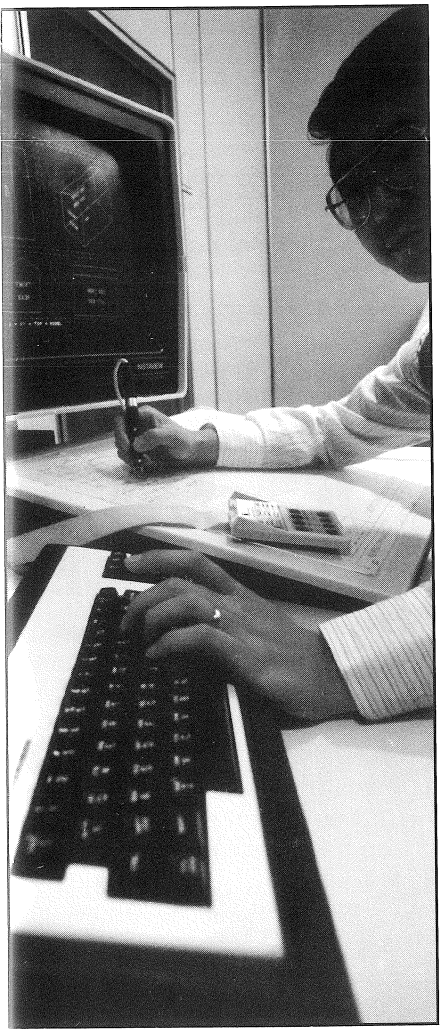
The criminal organisations, which exist in many countries, have always been ready to employ the latest in technology to further their business activities. We have only to look at the way in which they used the telephone to construct national gambling empires.

These criminal organisations have, in the past, shown they are quite capable of corrupting both business and political bodies through the use of various means such as blackmail, bribery, physical violence, extortion, etc.

Using these same methods they can easily gain the expertise required to commit major and minor computer based crimes.

Organised crime poses a real threat in using this computer technology not





only in its traditional crime areas, but also, in the area of white collar crime. Home computers and terminals can readily be used to keep track of thousands of daily drug transactions, to keep track of the inventory and the profits. In this way, organised crime can keep track of its multi-billion dollar empires, while making it more difficult for any of the authorities to investigate its daily operations.

Using facilities such as e-mail, the criminals can communicate throughout the world on a 24 hour basis without the fear of detection. If they were to communicate by means of the telephone or radio they run the risk of law enforcement agencies using bugging devices of one type or another.

One simple example of this is the case reported in the Australian media of the Triad and credit card numbers.

The Triad was reported to have been bribing international hotel staff to provide the credit card numbers of patrons. These credit card numbers were then used internationally to commit credit fraud activities.

To completely eradicate computer crime is a worthwhile, but unfortunately unattainable, goal. The traditional computing environments have been shown to be sadly lacking in security and the only way to make a computer system completely secure would be to lock it away in an impenetrable room and never use it.

Obviously, this is not possible and we can only aim to make any computer system as secure as humanly possible by limiting access both physically and electronically. Unfortunately there is an underlying lack of awareness by management, in general, of the security risks associated with computing environments and the effects of automated development tools and methods on these controls.

To stem the tide of the increase in computer-related crime, and perhaps to even forestall it, there is a need to develop methods for better security education at a management and corporate level and better overall supervision of computer security.

Research

Perhaps, if enough research is undertaken into the background of those people who actually commit computer crime, whether they are convicted or not, we can develop methods of accomplishing these ends. I am presently building a knowledgebase of the characteristics of hackers/crackers to attempt to delineate their common characteristics.

Using such a knowledgebase in conjunction with AI in the form of an expert system, we may be able to pose some factual answers to questions about the characteristics of typical hackers/crackers and the crimes they commit.

To date this type of data has proven very difficult to obtain either from computer underground sources or indeed from any law enforcement agencies.

This type of research should result in the application of AI techniques and/or software packages to the computer crime arena, not only for the education of management in security risks, but as an aid to human resource personnel in conjunction with security personnel to determine the security risks associated with both computer users and computer systems.

Similar use could result in the development of computer software to provide security control measures that are necessary to prevent many of the plethora of computer related crimes.

REFERENCES

Bequai, A. (1987); Technocrimes ; Lexington Books, Lexington Mass.

Coldwell, R.A. (1987); Non Professional Practices in Computing; The Australian Computer Journal 19(4), 215-8.

Coldwell, R.A. (1990a);Computer Crime : A Sociological Perspective in Hughes, G. (Ed) Essays on Computer Law; Longmans, London.

Coldwell, R.A. (1990b); Some Social Parameters of Computer Crime; The Australian Computer Journal 22 (2), 43-46.

Hayward, I.J. (1994a); Looking for the typical hacker trail; The Australian, Computers & High Technology Section, May 24 1994, 34.

Hayward, I.J. (1994b); Hackers, AI and Computer Security; Second Annual Crime Prevention Conference, Brisbane, Australia, August 1994.

Hayward, I.J. (1994c); Avenues open for software to prevent computer-assisted crime; The Australian, Open Systems Supplement, September 6 1994, 8.

James, H. and Coldwell, R.A. (1993); Corporate Computer Security; Information Management and Corporate Security Journal 1(4), 10-13.

Kamay, V. and Adams, T. (1990); The 1990 Profile of Computer Abuse in Australia; Australian Computer Abuse Research Bureau at RMIT, Melbourne, Australia.

Parker, D.B. (1983); Fighting Computer Crime; Charles Scribener's Sons, New York.

Ratledge, E. and Jacoby, J. (1990); Handbook on Artificial Intelligence and Expert Systems in Law Enforcement; Greenwood Press Inc.

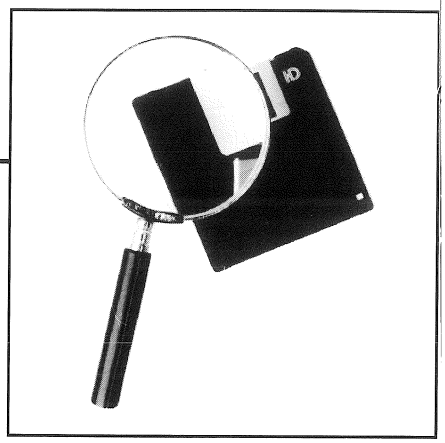
Rauch-Hindin, W. (1986);Artificial Intelligence in Business, Science, and Industry; Prentice-Hall.

Sherman, R.L. (1992);Biometric Futures"; Computers and Security 11, 128-133.

Stotland, E. (1977); White Collar Criminals; Journal of Social Issues, No. 33.

Ian Hayward M.App.Sc. (Computing), B.App.Sc.(Chem.), B.Ed.(Sec.), T.T.T.C.is a former lecturer in Business Computing, Victoria University of Technology, Footscray Campus)

Forensic Q&A

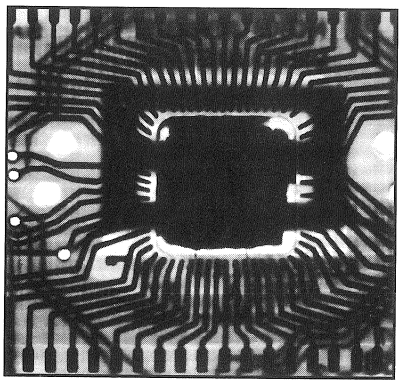


Q: I appreciate the technical arguments in favour of taking a forensic image of a suspect computer but I use a system of file copying to a Syquest drive and have found this to be perfectly adequate for my purposes. The courts don't seem too worried about the technicalities so is this method of copying really justified?

A: A number of correspondents have said similar things. The main point here is just how important are the investigations that you deal with?

It is quite true that done carefully, a file copy can quickly collect the information that you need. However, if the defendant admits the presence of the files on his machine but insists that he didn't put them there - how are you to answer if all you have are the files?

You should consider carefully what file copying actually entails. Firstly it must use the same operating system as that on the suspect machine or be done with specialist software that recognises the structures within that system. We have constantly emphasised the dangers of switching the machine on under its own operating system so a disk with a matching system must be used to boot.



If you work within a corporate environment where the system in use on every machine is known, this is not usually a problem. However, in other cases you would need to try a number of boot disks until you found the right one, remembering that the more sophisticated systems (Windows 95, Windows NT, O/S2 Warp etc) are either too large to fit on a single floppy disk or attempt to find and use software on the hard disk.

Your file copying must therefore be accomplished by a relatively simple system. Assuming that there are no software access protection systems on the machine (in which case you can't even see the disk let alone copy the files), you must then be certain that your copying software will identify and copy hidden files and directories as well as those with quasi-legal characters in their filenames. Many users who download files from web sites will have come across files with strange names, which they cannot copy or delete.

Even if these difficulties are overcome, remember that you are leaving behind a large quantity of material in slack and unallocated space (including the remnants of deleted files) as well as location and timing information which may be evidentially vital to your case.

You should also be aware that simply copying files does not provide a degree of evidential integrity that would withstand an informed attack by a determined defence counsel. The copied information would be too easy to change without trace and even if a second copy is taken, this too is subject to the same objection.

In most current cases, computer evidence consists simply of the contents of certain files and even then it is rare for these to be the only evidence presented. However, there are occasions when the environment that the files are in is of vital importance to determine the truth or otherwise of various witness statements.

The problem is an old one, you have no idea what may be on the suspect machine until you've copied it. You may be fortunate and collect all the evidence you need with a file copy but can you afford to risk it?

The courts in the UK have been well served by the introduction of forensic imaging technology and have displayed a justifiable faith in its reliability. They may not take kindly to a simple copy procedure, particularly if its limitations and weaknesses are explained to them in detail.

Q: Why all this fuss about computer forensics? I was under the impression that an expert's word and expertise was accepted in a court of law. If I say that I copied stuff and did not change it then that should be sufficient.

A: Yes - which is the way that it should be. Unfortunately it is entirely possible that an expert of equal standing but with questionable integrity could stand and call you a liar. The court must then decide between you and if you have nothing other than your word you are no more believable than he is.

If that is the way you wish to work then that is up to you. However, consider the position if you have taken forensic precautions - securing the evidence, maintaining continuity and documenting your investigation, you may then call for an independent expert acceptable to the court to verify your work and this will undoubtedly confirm the accuracy of your original evidence.

Since there are established ways in which you can conduct an investigation so that independent verification is available every step of the way, you risk appearing unprofessional if you do not use them.

Please e-mail your questions and / or comments to ijfc@pavilion.co.uk

Although every effort is made to ensure the accuracy of these answers, they are presented for general information and may not apply in rare specific cases. Readers are advised to seek confirmation from an independent specialists in forensic computing when dealing with evidentially valuable materal.

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

Fraud and Security in Telecommunications

12-15 January 1998
Radisson SAS Portman,
London

This conference offers delegates the opportunity to learn about the current position on Telecomms Fraud. Analyses of the latest trends in fraud will outline where vulnerabilities lie and how to take counter measures.

The conference will explain:

- How to use telecomms and non-telecomms systems to reduce fraud.
- The latest detection techniques and the best methods for prevention.
- The view of the experts, all experienced in Internet fraud.
- The latest fraud detection methods for Internet, Mobile and Calling Cards

Contact: CommEd
Tel: +44(0)171 733 3456
Fax: +44(0)171 733 0226

Securex

20-22 January 1998, London

Contact: Paramount Exhibitions
Tel: +44(0)181 207 5599
Fax: +44(0)181 207 2598

Securex

20-23 January 1998
Poznan, Poland

Contact: Poznan International Fair
Tel: +48 61 692592
Fax: +48 61 665827

Copex USA

9-10 February 1998
Sheraton Hotel, Washington DC

Contact: Copex
Tel: +1 703 451 1444
Fax: +1 703 440 1272

Advanced Computer Audit Workshop

10-13 February 1998
Bristol, UK

At this four-day workshop delegates will have hands-on access to the organiser's communications network and learn how to perform a network audit; experience first hand how operating systems work, and how to harness system features for audit use; learn how to audit database systems and much more.

Contact: System Security Ltd
Tel: +4(0)1625 523205
Fax: +4(0)1625 526952

White Collar Crime Course

24-26 February 1998, London

An interactive, practical course programme for practitioners wishing to acquire a good background knowledge in the area of white collar crime issues.

Contact: International Conference Group Ltd
Tel: +4(0)181 743 8787
Fax: +4(0)181 740 1717

Audit and Security of SAP R/3

25-27 February 1998, London

A three day seminar on: auditing SAP R/3 reports; securing transactions in the SAP R/3 environment; managing security and user access.

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

WebSec '98 The Conference on Web, Internet & Intranet Security

10-12 March 1998, London

This event is designed for all information systems professionals concerned with the security of their Internet, intranet, extranet and Web connections.

Delegates can hear about cryptographic technologies and how to use them to protect Web communications; the real threats of information warfare and how they can be reduced or removed; handling computer security incidents; securing Unix for Internet connectivity; creating secure Extranets; the Intranet as a threat and as a communication tool; the legal challenges of Internet security, including online distribution and defamation; software privacy and audit; controlling and monitoring Internet use within an organisation.

Throughout the conference there will be the opportunity to visit exhibits which feature products that demonstrate real-world solutions to complex security challenges.

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

Asia Pacific Billing '98

16-20 March 1998
Shangri-La Hotel, Singapore

This week long event will include on Monday, 16 March, a full day's module on Fraud Control.

Alongside the conference there will be a full scale exhibition to run from 17-20 March.

Contact: CommEd Ltd
Tel: +44(0)1308 86 7497
Fax: +44(0)1308 86 7499

Police and Public Security

26-27 March 1998
Police Staff College, Bramshill,
UK

Contact: DMA
Tel: +44(0)1428 607788
Fax: +44(0)1428 604567

International Journal of FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd