ISSN. 1363-6650

AUGUST 1998
Issue 20

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

Computers are a powerful and effective tool for any criminal. At the touch of a button they can steal millions of pounds, destroy companies, and peddle child pornography so evil it defies description.

As a source of evidence they are unrivalled, holding as much information in a tiny hard drive as a stack of filing cabinets brimming with paper.

That is why the science and practice of forensic computing – the investigation of computer crime and the preparation of computer evidence – is becoming recognised worldwide as a vital part of any police or law enforcement unit.

But we have to make sure we get it right at this stage, or risk losing the already considerable momentum.

In this month's Journal we continue our report on a case in which a vast amount of pornography was found on computers at a UK defence research centre. The investigation and subsequent prosecution were riddled with problems, many of them arising from a fundamental lack of understanding about forensic computing.

Well meaning but ill-informed staff made the preliminary examination of the systems and unwittingly contaminated the evidence to an alarming degree. Accurate logs and records of events and actions were not taken and information was misinterpreted leading to false conclusions about who was responsible for the pornography.

But this situation is not as bleak as it sounds. Forensic computing is a science and as such we can learn as much from our mistakes as we can from our successes.

The important thing is to take on board what went wrong, in whatever investigation or prosecution, so we can re-examine our methods and techniques and refine them to avoid encountering the same problems.

This process, involving investigators, law enforcement groups, lawyers, politicians and the judiciary, is a slow and complex one, and there will be many casualties along the way. But if this evolution results in a global acceptance of the basic principles and goals involved in computer investigation, it will have been worth it.

There will be conflicts and arguments as the courts and expert witnesses themselves debate what is and is not acceptable. This is fine, but we have to guard against the risk that the whole profession will be dragged down to the point where credibility and goodwill is lost.

Continuity, communication and co-operation between everyone working in this important sector should lay the keystones for the future and ensure that the best possible methods are employed to catch the criminals.

In the same vein, this month the Journal also covers the Dutch child porn investigation.

What the outcome of this will be, no one knows.One thing looks likely though, and that is that the case will cause shockwaves throughout Europe and the world as the horrific details of a child pornography making business emerge.

If we learn from the lesson, it could result in new laws and greater international co-operation to stamp out this evil trade.

But if we do the minimum and sweep the implications under the carpet it will let other paedophiles flourish, along with the suffering of countless innocent children.

News

US military go on hacking offensive

In what deputy Defence Secretary John Hamre called a radical departure, the Defence Department is creating a new office to defend the United States' infrastructure from cyber attack.

It's radical because the scope of the work is outside DOD's jurisdiction, he said last month at the Defence Special Weapons Agency's Annual International Conference on Controlling Arms.

"The Department of Defence only deals with threats outside of the borders of the United States," Hamre said. "If it's inside of the borders of the United States, it is a law enforcement problem."

With the exception of locks and dams, which fall under the auspices of the Army Corps of Engineers, DOD has not had responsibility for protecting the nation's infrastructure, Hamre said.

But in the digital information age, split-second global computer communications makes internal and external threats harder to define, he added.

"Cyberspace doesn't know geographical boundaries," Hamre said. "We're looking at a future where, frankly, DOD doesn't have any primary responsibility or jurisdiction but almost inevitably will be pulled in very early in any cyber protection role."

The new office, which DOD officials still must name, will be part of the Office of the Assistant Secretary of Defence for Command, Control, Communications and Intelligence and will manage Defence efforts to safeguard the nation's critical infrastructures.

These include telecommunications, banking and finance, energy, transportation and essential government services.

"Because of our constitutional orientation and our history, (the DOD) is not going to be the lead in anything, but we will be the backbone of everything, when you get down to it," he said.

The DOD office will work closely with the Justice Department's National Infrastructure Protection Centre and the multi-agency Critical Infrastructure Assurance Office, Hamre said.

"We have committed ourselves and are supporting the National Infrastructure Protection Centre," Hamre said. "We provide the deputy, and we'll provide, I believe, three of the five heads of the directorates."

The FBI's new National Infrastructure Protection Centre, at FBI headquarters and headed by Michael Vatis, will gather threat and vulnerability data and then disseminate analyses and warnings of threats to both the government and private sector.

"We are actively partnering with the Department of Justice and the FBI," Hamre said. "I meet on a monthly basis with the attorney general and with the director of the FBI as we are laying out our plans on the NIPC."

The Critical Infrastructure Assurance Office, which the Commerce Department spearheads, serves as the planning office for the Clinton administration's Critical Infrastructure Protection Program and works with Richard Clarke, the newly appointed national coordinator for security, infrastructure protection and counter terrorism.

- The US Army is setting up SWAT teams to battle computer hackers, who have made the military a favourite target. "This is the fire brigade," said Lt. Gen. William Campbell, chief of the Army's information systems.

The military is growing increasingly reliant on computers. Once reserved for secret tasks such as nuclear testing, computers are now used to keep personnel records, track inventory and communicate with contractors. Much of that work is done on the Internet, opening the door for mischief.

"The threat is global and ranges in scope from a single, non-malicious intrusion to a potentially organised effort by a foreign adversary," Col. James Gibbons said.

The Army Computer Emergency Response Teams, mirrored in the other services, are the latest layer of defence.

Specialised troops, backed by civilian experts, monitor networks for signs of intrusion, take emergency calls from system operators and, if needed, rush to the site of an afflicted computer. They track the latest hacker techniques.

"For every measure, there's a countermeasure. Every time that you think you have something fixed, you'd better go back and check it again," Campbell said.

Special Agent Jim Christy, of the Air Force Office of Special Investigations, is on a team working to co-ordinate hacker defence in the military and government agencies.

He said the military was ahead while "state and local governments haven't even thought about this."

Much work remains, he said: "We only catch the dumb ones. I'm not sure we have the capability yet, if it were a very sophisticated attack."

ViRii members admit infiltrating computers

Two teenage members of the ViRii group, which over the past year has broken into hundreds of government and university computer systems, have pleaded guilty to juvenile delinquency.

Last February 25, the FBI raided the Californian homes of the two youths, aged 15 and 16, and confiscated computer and related equipment as part of a worldwide round-up of ViRii members.

Also detained at that time were Calidan Levi Coffman, 20, from Washington state, Ehud Tenebaum, 18, of Tel Aviv, Israel, and two other Israeli teenagers. Tenebaum, considered the leader of the ViRii group, is known by his "Analyzer" alias online.

According to US Attorney Michael Yamaguchi, the two Californian teens, who have not been named, admitted to infiltrating a number of federal civilian and military computer networks, as well as university computer systems, and installing wiretaps, or "sniffers," to intercept passwords.

Although no sentencing date was arranged by US District Judge Maxine Chesney, Assistant US Attorney Albert Glenn said the teens probably would be sentenced to a probationary period that could include limited and supervised access to computers and modems, and being banned from computer jobs during their probation.

"Each juvenile will only be able to access a remote computer system under the supervision of a school teacher,

a librarian, an employer, or other person approved by the probation office," Yamaguchi said, and would be forbidden from using a modem at home.

"The government takes very seriously any attacks on the computer systems which have become so much a part of the American infrastructure," Yamaguchi said.

"We all rely heavily on these computers operating properly on a day-to-day basis, and any intrusion can lead to major disruption in important public and private services."

The teenagers, and Coffman, still may also face civil suits from a number of Internet service providers and US universities which are claiming hundreds of thousands of dollars in lost revenues and damage to their systems.

Coffman, who was arrested by special agents from the NASA Computer Crimes Division, was also charged with possession of unauthorised computer passwords. That case is pending prosecution in Portland, Oregon.

NASA Inspector General Roberta L. Gross said the agents' investigation revealed evidence about ViRii breaking into a large number of government, corporate and university Net-based systems. Gross said the NASA investigation into ViRii started in June 1997, when network security officials at the agency's Jet Propulsion Laboratory in Pasadena, California, detected a problem with a network server there.

The investigation established that the NASA server was controlled by intruders, Gross said, and that a number of foreign and US sites were used by the intruders as conduit points of attack to control the JPL server and to launch further attacks against ViRii targets.

In January separate attacks against other government sites, including seven US Air Force sites and four US Navy sites, brought the FBI and the Air Force Office of Special Investigations to focus on the Analyzer.

The nationwide attacks, Hamre said, involved unclassified information, including personnel and payroll records, and were felt by all branches of the military. Although the ViRii group appears to be primarily teenagers and young males in their 20s, Thomas J. Talleur, director of the NASA's Computer Crimes Division, said that many of today's "hackers are not juveniles playing games."

"The serious threats are coming from militias and other fringe groups who seriously want to disrupt and destroy the government, as well as from international terrorists and groups trying to spy by computer," he said.

"Computer security problems will get a lot worse before they get better," Talleur said.

Thai police want to monitor Net

Police in Thailand are asking communication authorities if they can monitor telephone numbers of Internet users.

Police Col. Chalermkiat Srivorakan, an assistant to the director of the Royal Thai Police Department, said the department wants the Telephone Organisation of Thailand to provide caller ID features for all local numbers used to connect to the Internet network.

The department wants to know all Internet users' login name and the phone number they use for Internet access.

Col Srivoraken said this was "to protect against any crimes that may occur on the network".

He said: "All Internet access in Thailand will be monitored by the department."

"Telephone numbers that are used to access the Internet will be displayed at the department's server so we know what every Internet user is doing. The display, which is similar to the caller ID feature used on some mobile phones, will allow police to increase their efficiency in crime prevention and suppression on the network."

He added that the department recently submitted a proposal to TOT and is now waiting for approval.

The department claims that the idea to display the numbers that Internet users are using is a part of the Internet Police project which uses the Internet as a new way to get criminal information from the public.

People are expected to inform the police about sources of crimes and other criminal information through the net work anytime, anywhere. Police say tha as a result, they can get criminal infor mation rapidly, helping them to suppres crimes on time.

Col Chalermkiat said that at thi stage, information on stolen cars an missing persons can be sent to then through the Internet.

However, the department hopes t have citizens informing about compute and Internet crime as well as Interne hacking in the future.

Survey says firms risk Web business

A survey conducted by a securit firm warns that Canadian companies us ing the Net are open to fraud because o a lack of security.

According to security and investiga tion organisation KPMG's 7th annua Canadian Fraud Survey Report, whic polls the chief executives of Canada' top 1,000 companies on fraud and cor porate security, only 11 per cent of re spondents believe that the Internet is secure way to send information.

However, the study shows 43 pe cent stated their company uses the In ternet to transmit sensitive or private in formation, anyway.

"The increase in electronic com merce provides opportunity for fraud i all industries." KPMG Investigation an Security Inc. President Norm Inkste said.

He said that 82 per cent of respond ents think their systems are at risk, bu only half use Net security measures.

Copies of the survey are available b phone from Stephen Schneider at + 416-777-8465 or through KPMG' Web site at http://www.kpmg.ca

Thai cell operators fight phone insecurity

Mobile phone operators in Thailan are using technology to tackle the in creasing problem of fraud.

Cellular phone companies are tryin to tempt new customers with the offer of low charges, but this has proved to b a double edged sword.

Instead of paying the 12 baht to 18 baht ($0.28 to $0.43) per minute for a call to a province like Chiang Mai and Phuket, people find it cheaper to pay just 3 baht ($0.07) a minute by using mobile phones.

This cheap telephone service became popular when "unwanted resellers" stopped buying mobile phones from legal channels to enjoy the discounts, and have instead started tapping signals from registered phones.

The country's largest cellular phone operator, Advanced Info Service Plc has lost about 170 million baht ($4.04 million) in such illegal phone calls and so has decided to install a more secure system, worth 400 million baht ($9.50 million).

"Safety is a very sensitive issue. We have spent a lot to make sure our customers are safe," president of the communication company, Somprasong Boonyachai said.

The company has two security systems on offer. Subscriber Identity Security which is used to protect analogue mobile phones from being tapped and the Fraud Management System which monitors the system to tackle heavy usage of mobile phones as done for public phone purposes.

AIS claims it is among the very first in the world to complete the SIS system, which it completed within two years, whereas Sweden, where more mobile phones are used, took a lot longer.

"About 14,000 subscribers, or only two per cent of our 745,000 analogue phones, have not been installed with SIS," Somprasong said.

Its rival, Total Access Communication, has a serious plan to limit airtime for its mobile phone users.

The operator also offers a PIN Security system which prevents handsets from being used for overseas calls.

Cellular phone operators have already declared war on illegal phone providers by shutting down some handsets.

AIS's vice-president for operation support, Arpattra Sringkarrinkul, said the Fraud Management System had already caught more than 1,000 mobile phones used illegally.

The fraud system specifically tracks outgoing calls to different destinations everyday, which shows if handsets are being used for commercial purposes.

"AIS cancels phones, making the owners contact us," Arpattra said.

Cyber chat turns to physical bat

A US man was attacked and beaten unconscious after he had been using an online chatting room.

The 22-year-old man from South Brunswick, New Jersey, was a frequent visitor to a Filipino chat room on America Online.

Seven men from New York allegedly discovered who he was and where he lived through another participant in the chat room.

"There was no history between (the victim and the assailants)," Det. James Kinard of the South Brunswick Police Department said. "They didn't know each other."

Kinard said the victim and his assailants first met anonymously over a year ago while visiting the chat room on America Online.

"Apparently, somebody said something," cyber-words were exchanged, and the online argument continued for more than a year, Kinard said.

A female university student, also of Filipino descent, knew the victim through his girl friend, and also met the group from New York through the same chat line without knowing of the online arguments, Kinard said.

The student unintentionally introduced the victim and his assailants and in a later fight, which went out to the street, the seven assailants knocked the victim unconscious, Kinard said, and later confessed to continuing to beat and kick him after he fell to the ground.

Six men in their late teens and early twenties were arrested and charged with aggravated assault and possession of a weapon, and a 15 year old was charged as a juvenile.

The victim was hospitalised and released, Kinard said, but still suffers from blackouts.

"The meeting between the victim and the assailants was completely coincidental," Kinard said. "But this is the first time we know of people who meet online actively seek out their victim once they find out who he is."

Quick Net access clouds crime

The Communications Authority of Thailand wants to control the way local Internet service providers sell their packages in a bid to cut crime.

Since people buying instant Internet packages to access the Internet currently do not need to provide personal details, CAT thinks that some can abuse the products and commit crime online.

At present customers can buy 20 hours of Internet access off the shelf and can use the service straight after it is installed on their computer.

People can create their own user ID and password and register online without using a real name, and they get instant authorisation to participate in the network.

CAT says that this means there is a loophole allowing some people to abuse the Net and the authority wants online firms to incorporate more security into their products.

A spokesman for CAT said that the organisation was now considering meeting local ISPs who sell instant packages to ask for a copy of the customer's identification card before they buy the product. This would allow ISPs to trace the culprits of any offences.

Vivatvong Vichit-Vadakan, the president of Loxley Information, a local ISP, said making Internet package purchasing more secure could stifle the use of the Net in Thailand.

He said: "I think that in the first stage we should encourage Thai people to use the Internet by helping them to get quick access rather than putting obstacles in their way."

He added that even though ISPs sold instant Internet packages to customers without requiring any user information at the initial stage, when they wanted to renew their subscription they had to send legal documents such as a copy of their ID card to the ISP.

Phone hackers put firms on alert

Many companies are unaware that they're vulnerable to voice-mail hackers who may steal confidential information or clog the system.

The issue is capturing employers' attention in the wake of claims that a reporter from the Cincinnati Enquirer in the US stole internal voice mail from Chiquita Brands International.

The newspaper agreed to pay Chiquita more than $10 million and publish apologies.

Hackers may find a password, break in and listen to messages. They may get into an internal phone system and place personal calls.

ICEE-USA, a manufacturing firm in Ontario, California, was hit by youths in 1996.

The pranksters, who eventually were arrested, entered through an 800 number, made thousands of unauthorised calls and clogged the voice-mail system with messages.

"Those who assume it can never happen to them generally end up having the problem," said Alan Brill at Kroll Associates, a New York-based business intelligence firm.

Hackers can learn a company's litigation strategies, information on mergers and tips that could be used for inside stock trading.

Less than 10 per cent of 407 firms polled had policies for communicating confidential information via telephone, based on a 1998 survey by the American Management Association.

Security experts say avoiding break-ins can be as simple as using long passwords and changing access codes regularly.

For extreme cases, there are voice-recognition systems, which verify voices in addition to passwords, says Bob Bhavnani, president of 2Va Software of Ridgefield, Connecticut.

In the Cincinnati Enquirer case, a reporter allegedly used illegally retrieved voice mail in a story about Chiquita's Central America business practices. The reporter was fired and faces a civil lawsuit by Chiquita.

Hackers attack Air Force computers

A computer system at Elgin Air Force Base in Florida in the US was illegally breached but the break-in was detected before any damage occurred.

According to the US Air Force Office of Special Investigations, the break-in was detected after the intruder was able to enter a Silicon Graphics workstation.

But Dave Sears, a computer scientist with the USAF 96th Communications Group, said automatic security programs detected the break-in and blocked further access to supercomputers and other systems at the base.

Other computer systems, including those belonging to the German Free Democratic Party and Internet service provider ProHost were not as lucky.

According to John Vranesevich, founder of Website AntiOnline, ProHost was broken into "by an unorganised group of hackers" to change the domain http://www.milw0rm.com, the group that recently gained access to an Indian nuclear research facility.

"After we changed the milw0rm page, all sorts of people started attacking ProHosting" the attacked told Vranesevich.

Vranesevich estimated that at the height of the attack, nearly a dozen different hackers had "root," or highest level access to the server, and one individual deleted the entire contents of the server, putting nearly 1,000 separate domains out of commission.

"We tried to stop him," the hacker told Vranesevich. "But he managed to delete everything anyway."

"That guy just crossed the line; what he did isn't cool," said another of the hackers.

Vranesevich said the 16-year-old "mystery hacker" that deleted the accounts is known as "DeathCraze," one of the newest members of the Milw0rm group.

Germany's Free Democratic Party, part of German Chancellor Helmut Kohl's coalition, also was attacked over the weekend, causing "considerable damage."

"While technically extremely proficient, the hacker made rather unimaginative, clumsy and humourless changes," the FDP said. The damage done was considerable."

AntiOnline's Web site is at http://www.antionline.com

Mobile phone firms warn about snoopers

The Cellular Telecommunications Industry Association in the US fears the FBI will try to increase its eavesdropping powers in a new law.

According to the CTIA, the FBI has presented to several key senators a proposal to attach to the Appropriation Measure for Commerce, State and Justice language that would extend the FBI's rights under the existing Communications Assistance for Law Enforcement Act.

What the FBI is seeking includes a requirement that wireless carriers provide information about the location of mobile telephones, simply on the strength of a law enforcement agent's claim that the information could be relevant to the investigation of a felony, CTIA spokesman Tim Ayers said.

The FBI also wants to prevent carriers and equipment manufacturers from petitioning the Federal Communications Commission to rule on whether any FBI demand is reasonable, the CTIA said.

Under the CALEA, the FCC can be asked whether a demand made under the act is too costly, would have a negative impact on competition, or would negatively affect subscriber rates.

The CTIA claimed that eliminating this recourse would in effect mean the FBI could demand "compliance at any cost."

Ayers said the FBI is also seeking the right to listen in on conversations even when neither party involved is the subject of a court order, and to capture certain digital information from calls, such as credit-card numbers entered using the telephone keypad.

According to the CTIA, when the CALEA was passed Congress made clear that its purpose was to extend the FBI's existing surveillance powers to

new communications technology, not to extend those powers, and FBI officials testified that they understood this.

Since then the FBI has stopped industry implementation of CALEA provisions, claiming the authority to require more intrusive surveillance.

The current attempt to have its powers extended by new legislation shows that the FBI did not in fact have that authority all along, Ayers said.

Misusing data

The UK's Data Protection Registrar has successfully prosecuted a son, his father and his father's company, for misuse of personal data.

According to the DPR's office, the investigation was undertaken with help from the National Westminster Bank. After being found guilty, fines totalling £8,000 and costs of £1,214.89 were imposed by Horseferry Magistrates Court in London.

The Registrar was contacted by the National Westminster Bank after the bank became concerned about the searches which one of its employees was making on the bank's databases.

But the employee, Noel Larbey, was providing information to his father, Michael Larbey, a private investigator. Larbey senior was providing the information in response to a request from a solicitor.

Noel Larbey, the son, was convicted on two charges of unlawful disclosure of personal data from the bank's databases and was fined £500 on each count.

His father's company, Kingscliffe Limited, meanwhile, was convicted on one charge of non-registration, two charges of unlawful procuring of personal data and two charges of unlawful sale of the data. The company was fined £1,000 on each charge.

Michael Larbey, the father, as the owner of Kingscliffe, was convicted on four charges of consenting to or conniving with the commission of offences by the company and was fined £500 on each charge.

Elizabeth France, the Data Protection Registrar, said: "It's encouraging that institutions like the NatWest are prepared to come forward and assist us in detecting and investigating such examples of unlawful procuring and disclosure of personal data.

"The level of fines imposed by the court clearly shows how seriously these offences are viewed."

The DPR's Web site is at http://www.open.gov.uk/dpr/dprhome/htm

FTC coalition wants to cut spam

Online consumers should be able to identify all unsolicited e-mail, according to a US Federal Trade Commission report.

The report, developed by a coalition of companies and organisations recommended that senders of junk e-mail, or "spam," should not be allowed to use false, or disguised return addresses which stop the recipient from responding directly.

Most junk e-mailers hide their true online identity to avoid being "spammed" themselves by thousands of complaints from those receiving the unwanted and unsolicited e-mail, generally asking the recipient to respond to a Web site.

"If every business that was sending out unsolicited commercial e-mail had to hear back from all the 300,000 people they angered, and they had to bear the cost of that, folks would realise it's not the most effective means of getting your message out," Deirdre Mulligan of the Centre for Democracy and Technology, said.

"The FTC's report is an excellent policy analysis of a problem that most people on the Internet already know far more about than they would like," Junkbusters President Jason Catlett said.

Catlett, noting the report's major recommendation is to target enforcement action on spammers who use fake return addresses and forge headers misrepresenting the e-mail's origin, said that "once spammers can't hide, they'll have to run from the millions of people they annoy every day.

"The Internet's best hope of containing spam right now is a combination of social pressure, vigilance by ISPs and government action under existing laws," he said.

Junkbusters runs a service called Junkbusters Declare at http://www.junkbusters.com which gives consumers a free option to tell direct marketers what they want, and don't want to receive, Catlett said.

The company's software, the Internet Junkbuster Proxy, also blocks unwanted "cookies" and banner ads, he said.

While the report recommends further restrictions on unsolicited e-mailers, the report, citing First Amendment concerns by the ACLU, the Direct Marketing Association and other groups, declined to press for an outright ban on junk e-mail.

Along with the report, Jodie Bernstein, director of the FTC's Bureau of Consumer Protection, released the bureau's "dirty dozen" list of spam scams, designed to assist consumers in avoiding such consumer rip-offs.

The list, Bernstein said, came from a special e-mail box at uce@ftc.gov the FTC set up for consumers to send spam they received in their own mailboxes.

"We invited consumers to forward their unwanted UCE (unsolicited commercial e-mail)," Bernstein said, "and consumers had forwarded well over 250,000 pieces of spam, and they continue to do so at a rate of between 1,000 and 1,500 spams per day."

Bernstein said the Commission put that e-mail into a searchable database "so that we could study the spam and identify possible targets for law enforcement actions." To date, the Commission has brought five such actions, she said.

Senate approves Net control laws

Amid controversy, the US Congress has tacked a number of amendments on to two bills in an attempt to limit access to undesirable material.

Two of the amendments require schools and libraries to install Internet access filtering software, the other revisits the Communications Decency Act.

The amendments were tacked on to

appropriations bills for the Departments of Commerce, Justice and State in the Senate, and appropriations bills for the Departments of Education, Health and Human Services and Labor in the US House of Representatives.

S. 1619, the Internet School Filtering Act of 1998, would require schools and libraries to block "explicit" material on the Internet, or lose billions in federal funding.

Under the act, libraries would only have to certify they are using a filtering or blocking system, such as CyberPatrol, CYBERsitter, NetNanny or SurfWatch, for one or more of their computers so that at least one computer "will be suitable for minors' use."

But allowing different communities to set their own standards, and requiring only one computer in a library to have filtering capabilities, appear to be a way around constitutional issues of banning free speech, critics of the amendment said.

"This is nothing less than Big Brother in the classroom," American Civil Liberties Union (ACLU) national staff attorney Ann Beeson said.

"We believe that educators, not Congress, should be the ones making decisions about what students can learn on the Internet."

She added: "You can no more create a computer program to block out one community's views of `indecency' than you can devise a filtering program to block out unconstitutional proposals by members of Congress."

The second amendment added to the appropriations bill, is still being debated in Congress, would amend section 223 of the Communications Act of 1934 "to establish a prohibition on commercial distribution on the World Wide Web of material that is harmful to minors, and for other purposes."

The amendment, S. 1482, introduced by Sen. Dan Coats (R-Ind.), is an attempt to "find a constitutional way to...help families protect young minds, hearts and eyes from the rawest, most degrading forms of pornography," Coats said.

Coats was an original sponsor of the Communications Decency Act, struck down by the US Supreme Court last June 26 as unconstitutional.

Unlike the CDA, however, Coats' bill would apply only to Web sites, and not to chat rooms, e-mail or newsgroups.

Coats' bill states that "whoever in interstate or foreign commerce in or through the World Wide Web is engaged in the business of the commercial distribution of material that is harmful to minors shall restrict access to such material by persons under 17 years of age."

Violations of the proposed language would be subject to fines up to $50,000 and up to six months in jail.

The bill also requires Web sites to use a verified credit card, debit account, adult access code, or adult personal identification number to determine if a person accessing the site is over 17.

But the ACLU also is fighting Coats' amendment.

"By claiming that the bill address only Web sites involved in commercial distribution, Sen. Coats says he is `hunting with a rifle,' but in fact has lobbed another virtual grenade attack into the heart of the Internet," Beeson said.

The amendments still have a long way to travel before becoming law, however, since both the House and Senate must reconcile the appropriations bills before sending them to the White House.

Fight over names of scrap critics

A large Canadian scrap metal company, has won a court battle allowing it access to the names and addresses of people who criticised it online.

An Ontario court judge ordered Internet service providers America Online, iStar and Weslink Datalink to give Philips Services Co the names, addresses, e-mail addresses and phone numbers of people who posted messages about the company on a Yahoo board from April through June of 1998.

Several of the messages apparently allege that Philip executives committed criminal activities.

Other missives reportedly express concern about the safety of a person who reveals the firm's activities.

Philip's stock price has come under pressure after the disclosure that it apparently hid unauthorised trading losses in its copper division.

Philips says it will sue a copper trader or traders who are blamed for the losses and the company faces several lawsuits in the wake of the revelations.

The judge's decision could mean the end of privacy and secrecy on the Internet for Canadian citizens because people who used anonymity in posting their opinions can now be held liable.

Police guide to find computer porn

Detectives in the UK investigating the trade in hard-core pornography on the Internet have been issued with a new guide to help them trace paedophiles across the Web.

"The Internet Detective", published by the Home Office, was written by West Midlands Detective Inspector David Davis to help officers. DI Davis saw the need for the guide while head of the force's Paedophile Investigation Unit.

Officers discovered child porn was being downloaded from the Internet, but at the time few in the British police knew how to deal with it.

During investigations it became clear paedophiles were exploiting what was then new technology.

"They could talk about things, swap things, almost with impunity in the early days," said DI Davis.

The guide shows the techniques used by paedophiles to hide their identity on the web and stop police identifying them, although DI Davis admits that if encryption programs are used correctly, they are uncrackable.

As well as pornography trafficking, the Internet is being used by organised crime to communicate using email.

"They know normal phones can be tapped, they know mobile analogue phones can be tapped, and there's a lot of talk about digital mobile phones being tapped, so they're moving to using this."

Anonymous emails have also been used by staff to threaten their bosses.

New investigative techniques are vi-

tal to crack Internet crime, but sometimes old-fashioned police work can pay dividends, said DI Davis. Recently his team raided the office of a man suspected of child abuse to check his computer for pornography.

They found the PC on his desktop was clean - but an officer noticed a strange dust pattern on another desk. Questioning a secretary, he found another computer had been moved to another office the day before the raid. "On the second one, we found the pornography," DI Davis said.

Hackers create havoc in South Africa

Cyber criminals could cost South African companies millions as the problem reaches crisis levels, according to security experts.

Ian Melamed, a Johannesburg computer crime expert working with Interpol to control the problem in Africa, said break-ins on the continent's computer systems had reached crisis levels and were getting worse.

Most developing countries, like South Africa, have inadequate legislation in this field, making it difficult to prosecute computer crime.

Mr Melamed is working with the SA Law Commission to draft new laws which will outlaw hacking (defined as illegally breaking into private computer networks) and cracking (stealing money or tampering with and damaging digital information).

In the first case of its kind in South Africa, a computer hacker is to be tried in the Pretoria High Court for snooping in private files in an off-limits area of one of the country's big Internet service provider networks.

The hacker scaled the "firewall" used to protect private areas of the company's network, but left "footprints". Computer fraud experts were able to trace the location of the computer where the crime was committed. A court date is yet to be set.

Mr Melamed, who is consulted by police regularly to help in computer investigations, said the absence of anti-hacking laws meant the case would be tough to prosecute.

Companies where security had been breached were reluctant to go public because they immediately became targets of hackers and crackers who, knowing someone else had found a way in, also tried to break through their security.

Africa was especially vulnerable now because Internet technology was available, but companies were ignorant about protecting themselves and client information.

The worst local culprits were often juvenile "cyber boffins", some as young as 11, who were fast mastering ways to dodge computer police patrolling networks for rogue visitors.

"Ask a computer-literate child for a tour of the Internet and you will be staggered by what he knows.

"I can only say I hope their knowledge is used for the benefit of the economy one day, because it's formidable," said Mr Melamed.

Police spokesman John Sterrenberg said the school holidays could soon become a nightmare time for computer police as bored youngsters logged on to the Internet and hacked their way into no-go areas.

"There might be no law against hacking or cracking, but stealing is still stealing," he warned.

In the Western Cape police have investigated 40 cases of computer fraud involving 2 million rand over the past two years.

Hackers, often working from overseas, will usually go through second computer networks to cover their tracks. This means police are often sent on the wrong trail - and the wrong continent.

FTC wants laws to protect privacy

The Federal Trade Commission plans to recommend that the online industry be regulated by the government unless it protects consumers' Internet privacy by January next year.

FTC Chairman Robert Pitofsky wants legislators to give Internet firms one last chance to regulate themselves, but if this fails he will urge lawmakers to pass a privacy in cyberspace bill.

Any such law should give an agency like the FTC the authority to establish minimum privacy standards for different industries, Pitofsky said.

Web sites should reveal what information they collect, allow consumers to control dissemination of data and offer consumers a way to check and correct data for inaccuracies.

"Unless industry can demonstrate that it has developed and implemented broad-based and effective self-regulatory programs by the end of this year, additional government authority in this area would be appropriate and necessary," Pitofsky told lawmakers at a House Commerce Committee subcommittee hearing.

The FTC recently called for a law to limit the collection of information about children surfing the Internet after a survey of 1,400 sites on the World Wide Web found rampant abuses.

At the time, the FTC stopped short of calling for legislation to protect the privacy of adult Internet users, but in his testimony Pitofsky will outline a law that would include a requirement that merchandisers inform consumers about the use of their personal data.

A group of leading companies doing business on the Internet asked lawmakers for more time, however. The Online Privacy Alliance, a group of Net companies including Microsoft, AT&T and America Online, suggested a scheme based on third-party validation of privacy practices.

Under the plan, an outside group would allow Web sites that met certain privacy protection policies to carry a seal or label alerting consumers.

Senate passes Internet gambling ban

The US Senate overwhelmingly voted to ban most forms of gambling on the Internet, even though questions remain about enforcement.

The full Senate voted 90-10 on an amendment by Sen. Jon Kyl (R-Ariz.) to extend the current federal ban on interstate gambling on sports by phone or wire to almost all other forms of gambling, including Net-based "interactive

casinos."

Kyl's bill broadens the current phone/wire ban to cover new and upcoming technologies like microwave transmission and fibre optics.

The bill is also the first to prosecute people placing bets with such operations.

Under the provision, individual gamblers could face prison sentences of 3 months and fines of $500.

Those running businesses that run the gambling sites could be imprisoned for 4 years and fined $20,000 or three times the amount of bets accepted.

But the Senate rejected an amendment by Sen. Larry Craig (R-Idaho) that would have excepted the ban from Indian tribes. The vote on that piece of legislation was 82-18.

Even though the bill promises to prosecute Net-based casino operators, those opposed to the legislation say it cannot be enforced since almost all of the Web gambling sites are located outside of the US.

An essentially similar bill regarding Net-based gambling is awaiting a vote in the House of Representatives.

Kyl said: "More than a billion dollars will be gambled over the Internet this year. Internet gambling is unregulated, accessible by minors, addictive, subject to abuse for fraudulent purposes like money laundering, evasive of state gambling laws - and already illegal at the federal level in many cases."

The Senate amendment would require Internet service providers to "pull the plug" on those sites, Kyl said, saying a ban would "likely be enforced by law enforcement identifying a Web site that provides illegal gambling and seeking a court order enjoining the activity."

During two days of debate on the Senate floor, the gambling amendment's supporters contended a ban is needed since there is no way to regulate virtual casinos.

Unscrupulous operators are free to rig their games to cheat customers or accept bets from children who get their hands on parents' credit cards, they said.

But Internet gambling spokeswoman Sue Schneider, chairwoman of the 55-member Interactive Gaming Counci, said: "All prohibition does is build up a criminal infrastructure."

Net user charged with subversion in China

China has arrested and charged a software engineer with subversion after supplying e-mail addresses to an American-based pro-reform magazine, said a human rights group.

Lin Hai, a 30-year old manager of a Shanghai based software company, was arrested in April after providing a list of 30,000 Chinese e-mail addresses to a US-based pro-democracy magazine and Web site called Big Reference.

A spokesman for the Hong Kong based Information Centre of Human Rights and Democratic Movement in China said he is expected to stand trial in Shanghai in the near future.

If convicted, he faces a penalty ranging from 10 years in prison to the death sentence.

The spokesman said a 150-member strong police squad in the Chinese city are monitoring Internet usage and blocking access of some users while confiscating the computers of others.

Internet use in China is rising fast. According to recent reports in the Chinese media, the nation had 1.175 million Internet users at the end of June.

The figures, from the China National Network Information Centre (CNNIC), represent a rise of 115,000 during June and a large rise on the 670,000 users at the beginning of the year.

NASA's tackles crime using Beowulf

Analysing computer crime evidence and tracking cyber criminals has gone from taking weeks to mere minutes, now that the NASA Computer Crimes Division has employed Beowulf

NASA's Beowulf is a low-cost, high-performance computing cluster that helps identify computer criminals.

Previously used by such organisations as NASA and the Department of Energy for high performance scientific modelling and simulation, the Beowulf technology, coupled with additional software tools developed by the CCD, now could benefit law enforcement, network security and other areas that need a low-cost, high-performance computing system for non-scientific applications.

"This is the first time Beowulf is being used for law enforcement," Thomas Talleur, advanced technology programs executive for NASA's CCD, said.

According to Talleur, Beowulf is a low-cost alternative to supercomputers. "What NASA did was to parallelize the Linux operating system, making it so it would run as a parallel operating system."

"We built a modest cluster that features a sustained throughput rate of 2.4 Gb per second for under $60,000," Talleur said, adding that the project "is another great example of NASA's better, faster, cheaper philosophy at work."

Talleur noted that the Beowulf Linux operating system "is great for organisations that have intensive computational demands and small operating budgets."

Because Linux source code is available free, Talleur said "now we have the control and computational power that we need without being dependent upon specific vendors."

As an example of Beowulf's power, Talleur said that while the recent investigation into break-ins into NASA and other government computer systems by the ViRii group took seven weeks for evidence to be analysed, Beowulf could perform that same task in less than an hour.

"We have gone from weeks to minutes in our ability to analyse and process computer crime evidence," he said.

NASA originally pioneered the Beowulf concept at its Centre of Excellence in Space Data and Information Sciences in 1994, by adapting the free Unix-like operating system, called Linux, to work in a massively parallel and distributed computing environment using commodity off-the-shelf hardware.

The Beowulf distribution used by the CCD is called Extreme Linux, and is distributed by Red Hat Software for $29.

Additional information on the Beowulf project is available at http://beoserv.hg.nasa.gov

Product news

Voice security

A new system could cut fraud by processing customer requests by using voice verification.

US firm Periphonics has joined up with T-Netix to enhance its automated transaction processing services by using T-Netix's SpeakEZ Voice Print technology.

According to the company, the SpeakEZ Voice Print technology significantly reduces an institution's risk of fraud by requiring callers to pre-record a spoken password, as well as identify themselves by speaking the same password each time they wish to access secure information and services.

The plan is now for Periphonics to work with T-Netix to port SpeakEZ voice print technology to OSCAR (Open Signal Computing and Analysis Resource), Periphonics' advanced platform designed specifically for leading-edge speech processing algorithms.

The IVR applications, the company says, will prompt the caller to "voice verify" their identity. The spoken reply is then packaged and sent to an OSCAR running SpeakEZ, where it is compared against the caller's previously enrolled voice print stored on the Periphonics system.

The verification engine will then send a message back to the IVR application, indicating whether access should be approved or denied.

"As the frequency and value of telephone-based commercial transactions increase, call centre operators are more concerned than ever with fraud security," said Ron Beyner, T-Netix's vice president of commercial services

"Touch-tone based passwords and PINs can be copied or hacked. With SpeakEZ voice print technology, an account will be protected from unauthorised access, even if the `fraudster' knows the account holder's voice print password," he said.

Cellular fraud control

Mobile phone firm BellSouth Cellular Corp is installing a profiling system to help spot fraud.

The company, a division of BellSouth, will use Corsair Communications Inc's FraudWatch Pro product.

The system profiles individual cellular subscribers by noting their patterns of telephone usage and spotting deviations from normal calling patterns.

Corsair spokeswoman Corey Caldwell said carriers could spot signs of cellphone "cloning" and subscriber frauds that involve using the identity of a legitimate subscriber to create a separate account.

Caldwell said BellSouth Cellular is among the first major carriers to install FraudWatch Pro, although several carriers - mostly international ones - are currently deploying it.

BellSouth Cellular is at http://www.bscc.com and Corsair Communications is at http://www.corsair.com

Next generation credit card security scheme

MasterCard International has announced it is working with HNC Software on a next generation anti-fraud system.

The aim of the project is to allow MasterCard-issuing financial institutions to better detect fraudulent debit and credit card transactions.

Most fraud detection systems currently deployed on the networks of financial institutions rely on a neural network or fuzzy logic approach to fraud, allowing the software to adapt to rapidly changing spending pattern changes, but applying a rules based approach to capture suspicious transactions.

MasterCard's new fraud detection service is based on HNC Software's advanced neural network modelling technology.

According to company officials, by leveraging the MasterCard BankNet global transaction processing network, the system combines cardholder, merchant, and geographical data to give MasterCard members a fraud prediction model that is unique in the industry.

The first module of the new risk predictive service will be available in the fourth quarter of this year and will be exclusive to MasterCard and its member institutions.

According to HNC, the product can be integrated with an issuer's existing system or used as a standalone fraud detection service.

According to HNC, the new anti-fraud system being developed for MasterCard is a new application of HNC's proprietary profiling technology, allowing the fraud predictive system to constantly update information with each new transaction, building a detailed profile of each merchant and cardholder.

This exclusive use of dynamic merchant profiles to supplement the transaction-based account profiles, the company says, provides a boost to the predictive precision of the model.

By using a variety of models of behaviour for each global region, the system will ultimately allow members to examine similar patterns in a given set of countries.

Currently, 12 MasterCard members are participating in the association's pilot program for the credit card fraud detection module. Firstar Bank, based in Wisconsin, has used the system to catch previously undetected fraudulent activity that could have resulted in an average loss of $5,100 per account identified.

MasterCard's Web site is at http://www.mastercard.com

Software to cut harrassment

To help protect companies against a rising wave of e-mail-related harassment lawsuits, a program has been launched to automatically remove offensive words.

Content Technologies has announced an "anti-harassment and profanity" module for configuring its Mimesweeper filtering software to screen out messages containing certain words.

Victor Woodward, spokesman for the firm, said that many types of online activities could easily meet the definition of "harassing conduct," stipulated by the Equal Employment Opportunity Commission in the US. In one recent sexual harassment case, the courts awarded $2.2 million to four female

employees of Chevron Corp., who alleged that they had received sexually offensive e-mail, according to Woodward.

E-mail is also being used as evidence in a number of cases now pending in the US court system, including suits against Microsoft, Nationwide Mutual Insurance, King County in the state of Washington, and the Minneapolis (Minnesota) Community Development Agency, Woodward observed.

Content Technologies' Mimesweeper site is located at http://www.mimesweeper.com on the Web.

Online research tools

Online information provider Lexis-Nexis has announced improvements to its services to streamline the process of retrieving case law.

The new features automatically provide an at-a-glance overview of the major legal terms appearing within a particular case or agency opinion and enable a researcher to highlight important passages and automatically launch a search to find related materials.

"These new features provide attorneys with a superior alternative for scanning and filtering legal materials quickly to find applicable cases and agency decisions vital to their legal research," said Paul Brown, chief operating officer of Lexis. Researchers can also retrieve the full text of legislation referenced in a newspaper or legal publication article as the result of an enhanced linking feature also recently launched by Lexis-Nexis.

The new features are available on the Web-based legal research service at www.lexis.com.

Strong encryption

Jaws Technologies says it is launching the world's strongest security encryption software to address the increasing frequency of unauthorised access to digital information.

Jaws L5 Data Encryption is the industry's first encryption software product with 4096-bit key encryption strength. Claimed to be the most advanced encryption software currently on the market, the firm says it is statistically unbreakable.

The program encrypts files as a means to control access to confidential information stored on desktop PCs, handheld devices and networks and to ensure security of Internet transactions and remote file access.

The application employs recursive mathematics to make backward analysis impossible, and takes advantage of a complex algorithm utilising a random number generator to create a unique encryption "key," meaning no two encryption codes are the same.

Jaws L5 is available for $49.95 online and directly from the company. For more information, visit the company's Web site at www.jawstech.com

Risky Net business

A study into the habits of UK companies has revealed that many have still to come to terms with IT security.

The report was jointly commissioned by Integralis, City law firm Theodore Goddard, and corporate insurer Nelson Hurst, and was conducted by QA Research. The study says that an increasing number of companies are using e-mail or the Internet, but in many cases there is little done to combat the potential security threats through network security, necessary insurance and legal measures.

"This research has uncovered a massive gap that needs to be bridged by corporate Britain, between the current use of e-mail and the Internet by organisations, and what is actually required to ensure they are doing business via electronic methods in a secure manner," said Steve Webb, Integralis Network Systems' European marketing director.

"This research demonstrates that British companies are not generally aware of the extent to which employee access to e-mail and the Internet can expose them to legal liability," said David Engel of Theodore Goddard.

According to Engel, even where there is some awareness of the problem, companies do not appear to be doing a great deal to manage that risk.

"Only last year, we acted for private medical health insurer Western Provident Association which successfully sued Norwich Union for libel as a result of e-mail messages circulated on Norwich Union's internal e-mail system.

"Norwich Union paid our client £450,000 ($700,000) in damages and costs; that case is a salutary lesson for any employer whose staff have access to an internal e-mail system and, even more so, to the Internet," he said.

And the study showed that those responsible for purchasing and setting corporate insurance policies (typically finance directors) were unaware of the need to insure against corporate risks associated with e-business.

Integralis, Theodore Goddard and Nelson Hurst have launched a range of complimentary services to address the IT legal and insurance issues relating to corporate liability through e-business.

For more information see the Web site at http://www.cyberliability.com and there is a hotline on +44-(0)118-930-6060.

Security consulting

Computer security firm Network Associates demonstrated that it's beginning to rationalise its multiple acquisitions of Internet and network management firms.

The company announced a new professional services organisation largely made up of consultants acquired with firewall company Trusted Information Systems in March 1997, Network General last October, and network scanning firm Secure Networks this May.

The company also will offer custom consulting on network security, including full-scale outsourcing and penetration testing.

The news follows announcements of enhancements to Network Associates' firewall software offerings.

The company, which began as an antivirus software vendor called McAfee Associates, has launched WebShield for Firewalls, which builds network antivirus protection into firewalls to keep viruses from entering corporate networks via the Internet.

WebShield for Firewalls is the first product to result from TIS acquisition, and it uses the content vectoring protocol to scan for viruses at the firewall. The product also works with firewalls from other vendors that support CVP.

Dutch child porn scandal

The discovery and investigation of a global child porn ring has resonated through police forces and politicians alike. **Paul Johnson** looks at events surrounding the case and the implications for the future.

The Dutch police have launched an investigation into a suspected international child abuse ring after thousands of pornographic computer and video images were found.

Detectives have been sorting through thousands of porn computer images in the search for evidence that toddlers and young infants were among those allegedly exploited over the Internet.

However, Dutch police themselves stand accused of initially bungling the investigation into the paedophile ring, which is accused of abusing children, some as young as two, and selling the pictures on the Net.

The case was set in motion with the murder in Italy of convicted German paedophile Gerrie Ulrich, 49, who had been living in the Dutch seaside town of Zandvoort.

Ulrich ran a computer shop in Haarlem near Amsterdam and is thought to have been a central figure in an international network, using his shop as a cover for the distribution of child pornography. It is thought that his murder, in Pisa in June, was at the hands of another suspected paedophile.

And it was reported that the dead man's family, who wanted to disassociate themselves from Ulrich, first went to the police with evidence of the paedophile's activities.

But it is claimed that police indifference led them to take the potentially crucial evidence, including disks and CD-ROMs containing pornographic files, to the Belgian anti-porn group Morkhoven, which in turn released parts to the Dutch current affairs programme Nova.

More seriously, police are accused of failing to discover the dead man's extensive links with the shadowy world of child pornography after receiving several tip-offs about his alleged activities a year ago.

Dutch police said they had first been tipped about Ulrich's suspected involvement in child pornography in early 1997.

"The tips that came in were hearsay," police said. "The police did mount an investigation... (which) did show Ulrich had pornographic images in his possession, but nothing indicated that child pornography was in play."

Consequently no crime was uncovered, as possession of pornography is not punishable under Dutch law, police said.

The Dutch newspaper Algemeen Dagblad blamed management costs and personal egos for bogging down police procedures, saying money and manpower for an investigation was made available only after the affair hit the international headlines.

And the NRC Handelsblad paper said: "That unspeakable practices can occur in the Netherlands means that the Netherlands has a serious problem. The Zandvoort case proves that the Netherlands is a major production and distribution centre for child porn, as has been repeatedly claimed by US and German authorities - a claim that has always been denied here."

The Morkhoven group finally handed over dossiers believed to contain names and addresses of those involved in the child pornography ring to Belgian authorities which passed them on to Dutch justice officials.

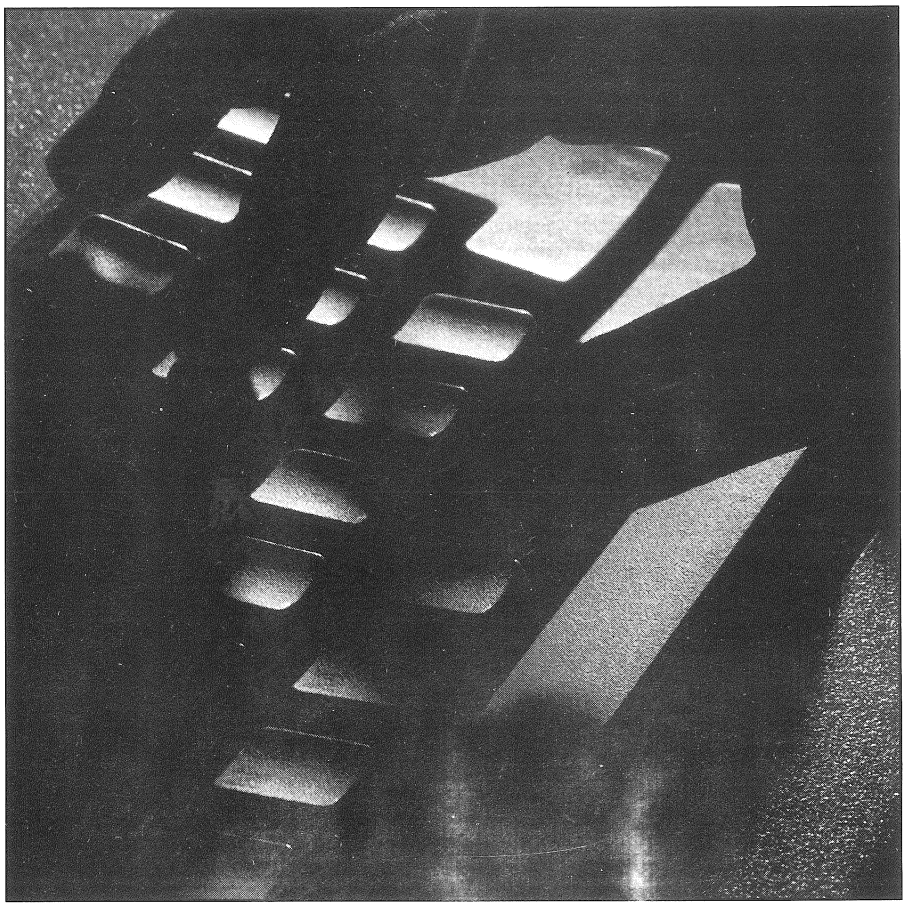
In a response to the mounting criticism, a police statement said they had to wait until the end of June to examine the computer material because there was no legal basis to do so earlier.

The statement also said police had launched an investigation last year into the man's alleged links with paedophiles based on "hearsay" tips, which revealed he possessed pornography, but not child pornography.

A Justice Ministry spokesman said the problem of Internet pornography was not as easily handled as child abuse, adding that the problem required an overall EU response.

"Child abuse has a very high priority in the Netherlands and then there's the relatively new problem of Internet images," the spokesman said.

"An added problem is that of the



power of jurisdiction. This Internet crime has to be tackled on an international level," he said.

Now the Dutch Justice Ministry, stung by criticism over its handling of child pornography on the Internet, is to increase the number of investigators working on it and boost co-operation between Dutch authorities.

"More detailed agreements have been made on how to handle reports of child porn on the Net...the Central Research and Information service will put more people on the matter," Wijnand Stevens, ministry spokesman said.

In a statement, the Justice Ministry said: "The minister wants to take away the impression that police and justice in all areas give insufficient priority to the fighting of sexual offences against minors."

In a letter to parliament the same day, Justice Minister Benk Korthals said those investigating cyberspace child pornography faced new technical complexities. But police and justice officials were catching up on the knowledge backlog.

He also said the need to fit international co-operation with national policies also complicated the battle.

"There's a legal problem. Legislation has been established along the lines of territorially organised states in the past centuries. The creation of the necessary international law is still in a tender stage," Korthals said.

Enhanced international exchange of information between investigation bodies should be improved, he added.

The Netherlands, Germany and Sweden recently started a pilot project to exchange digital information on Internet child porn, intended to help create a European Union network of databanks.

Dutch officials said the search for and prosecution of commercial production and distribution of child porn on the Net would remain a priority, and that methods to battle against the abuse had been refined.

The Central Research and Information service will refer cases that fall under Dutch law to a special office of the public prosecutor, which will co-ordi nate national investigations. Up to nov the public prosecutor's office has bee entrusted with five cases, Stevens said

Catalogue of horrors

Morkhoven chairman Jan Boeyken said the group held thousands of horrifi photos.

Morkhoven says it has uncovered mountain of videotapes, CD-ROMs an encrypted computer diskettes showin children as young as 18 months bein sexually abused by adults.

The group also said it had hundrec of names and addresses in various cour tries of suspected users and manufac turers of child pornography.

Among the films is one titled "O Daddy," in which balding, middle-age men have intercourse with five-year-ol and eight-year-old girls, one of whoi appears to have been so heavily drugge that some experts fear she may hav been dead.

Bank statements recovered b

Shadowy vigilante group wage war on child porn

Jan Boeykens leads a group called Morkhoven that is waging its own private war against child porn.

These vigilantes, founded in 1988, are determined to put an end to a business that has spread to the Internet, and their actions - including a fight with police about handing over evidence - have earned them a mixed reputation.

Boeykens, a human rights campaigner who long has fought child abuse and police brutality, says he has no faith in Belgian authorities. He doesn't have much confidence in Dutch police either. And like many vigilante groups, his has had occasional brushes with the law.

On July 20, Belgian police arrested Morkhoven member Marcel Vervloesem for refusal to hand over diskettes and files on the child-sex ring. He eventually complied and was released.

"I think some people in the justice system are involved," said Boeykens, explaining why Morkhoven was reluctant to relinquish the material. "Some policemen are involved. They are not angels. And I think some political people are involved."

Belgian officialdom is suspicious of Morkhoven. An investigation of the group is under way, but it is not know whether charges have been filed.

Morkhoven is a close-knit group of 20 to 25 people, most of them part-time volunteers from Belgium, the Netherlands and Germany with the shared goal of exposing mistreatment of children.

They began fighting the use of isolation cells for children in a psychiatric clinic and eventually to other issues involving young people.

"From the beginning we've had a lot of problems with the authorities," said Boeykens. "When we started with actions against the isolation cells, it was a taboo. They denied these problems existed. It's the same now with the pornographic network. They are criminalizing us.

"We are not connected to a political party, we are not subsidised. We are completely free."

One sympathiser is Austrian Foreign Minister Wolfgang Schuessel, president of the European Union Council of Ministers, who thanked Vervloesem for his "courageous and exemplary action" in helping to expose the pornography ring in the Netherlands.

The publicity generated from the Netherlands case has shed light on the previously little known organisation, increasing its support and funding. But there are no plans to increase its size. "It's best to work small," says Boeykens. "We have been infiltrated in the past. And I think our telephone conversations are monitored."

Morkhoven and shown on Dutch television's NOVA programme indicate Ulrich marketed a bulletin board called Apollo.

For a fee deposited to his account, subscribers could dial direct into the Apollo site and view more than 30,000 images of sexual abuse of minors.

Morkhoven says it has evidence linking the computer porn network to a sinister child smuggling racket that stretches from Russia to the United States, Portugal, France and Belgium.

A spokesman for the group said: "The size is so enormous - the police will need several weeks to plough through it.

"There are people from England involved who founded (pornography) businesses in the Netherlands which are active in the Czech Republic and in Berlin."

The group said it gathered its evidence during its search for a Berlin boy who disappeared in 1993 aged 12, then resurfaced in the child pornography world of Amsterdam.

Dutch police said they had met with the boy's father and that they would look at his disappearance as part of the investigation.

Some of the child-pornography pictures similar to those retrieved at the Zandvoort flat are reportedly still available on the Internet.

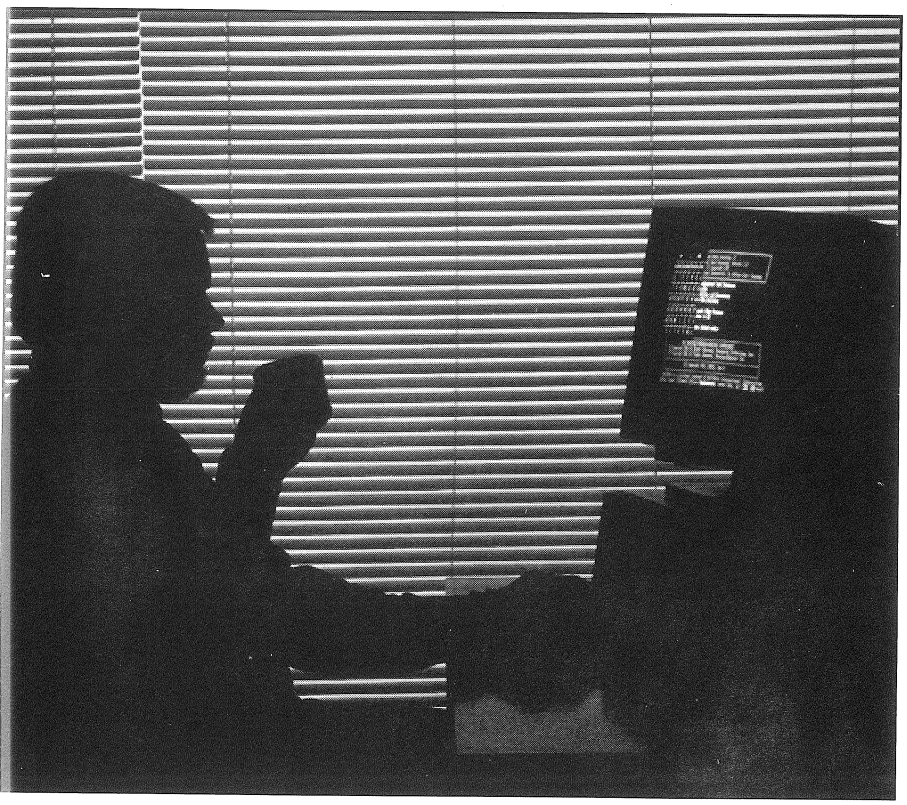
A spokesman for the Dutch Public Prosecution's anti-pornography work group said he understood the pictures were on a US Internet site, and so beyond the reach of Dutch law.

"If the pictures were on a Dutch site, we could put it out of action. Our normal powers would apply and we could conduct a house search and confiscate material," Jurriaan Simonis said.

"If the pictures are in America...all the police can do is tip off their US colleagues."

Authorities say little if any of the material seized in Zandvoort was actually produced in the Netherlands; they think much of it came from central and eastern Europe and originally was posted on the World Wide Web in the US.

Though possession of child pornography carries a maximum sentence of six years' imprisonment in the Netherlands, traffickers are difficult to catch. Paedophiles who once posted illicit images openly on Web home pages now shelter in Internet chat rooms, hiding behind fake names and bogus e-mail addresses.



Call for EU action

Austrian foreign minister Wolfgang Schuessel has rebuked some of his European Union partners for their "lukewarm" response to calls to increase action against crimes against children.

Schuessel, whose country holds the rotating EU presidency, told the European Parliament's foreign affairs committee that he hoped the discovery in the Netherlands of the alleged child pornography ring would jolt them into action.

"To be honest...it was a pretty lukewarm reception," Schuessel said of EU foreign ministers' reaction to his announcement that the fight against such crimes would be a central plank of Austria's six-month presidency.

He said he hoped EU member states would take advantage of events in the Netherlands to broach "this awful problem."

The affair has prompted calls for tightened control of the Internet, but the 15-nation EU is at odds as to how to do it.

Tom Spencer, chairman of the European Parliament committee, told Schuessel that, while the Assembly would look at ways to combat use of the Internet for such ends, previous attempts had come up against legal obstacles.

Maurice Wessling, a spokesman for Internet provider Xs4all, said his company filtered out information intended for child pornography sites.

Removing the sites altogether could lead to the migration of porn elsewhere.

But the industry's approach to tackling unwanted material on the Internet is piecemeal, as is the approach of national governments.

"In the Netherlands it's a crime to say the Holocaust did not happen. In the US it falls under freedom of speech and is okay. But something posted in the US is visible to someone in the Netherlands," Wessling said.

Forensic lessons - case study

In last month's Journal, we reported how workers at a UK Ministry of Defence agency had downloaded thousands of illegal pornographic pictures. A subsequent trial threw up a variety of problems and issues surrounding the case. This month forensic analyst Jim Bates, who acted as an expert defence witness in the proceedings, looks at what happened and what lessons need to be learnt.

The Roper case, involving large numbers of pornographic images on a network based at the Defence Research Evaluation Agency.in Malvern, Worcestershire, was the largest - in terms of quantity - that I have been involved in and possibly the largest that has yet been seen within the U.K.

When investigating such cases, there may occasionally be areas where a professional opinion is required concerning the interpretation of the evidential material. However, the main work of an expert is simply to quantify, analyse and report upon the facts.

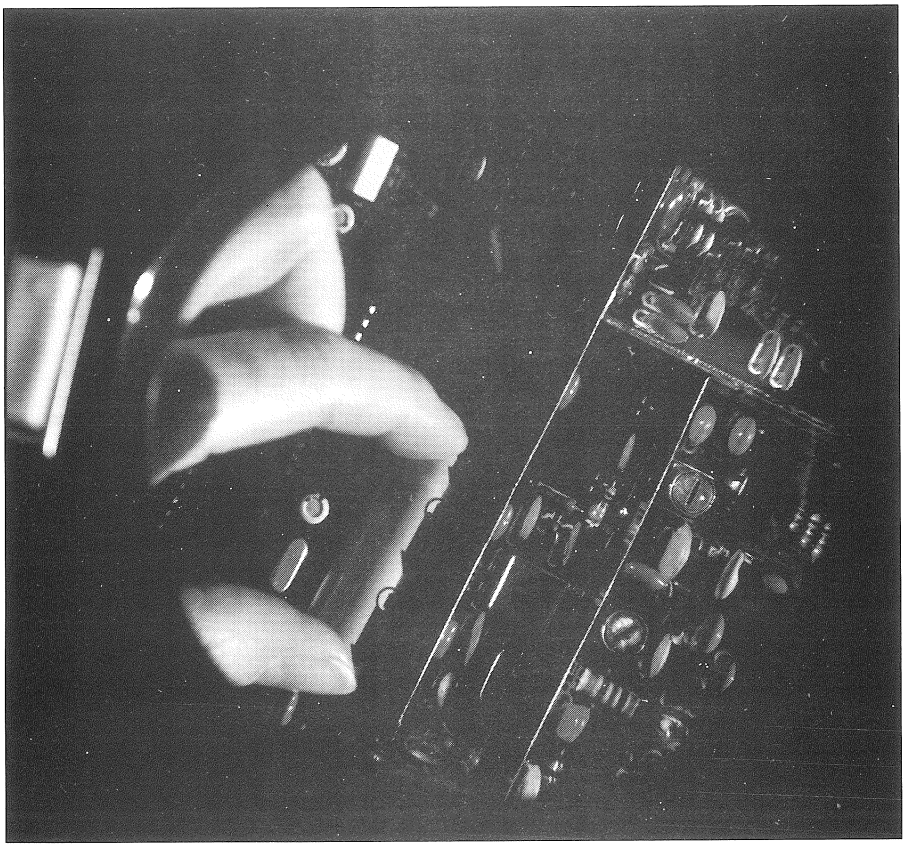
In this case, as with most cases, the facts were not in dispute. The computer used by the defendant Paul Roper at his workplace did contain quantities of pornographic image files.

Some of them undoubtedly involved children and some of them had been deleted. However, these facts had to be seen and interpreted within the greater framework of the circumstances surrounding the use of the machine.

At the beginning of my investigation, from the various statements the story emerged as follows:

In the early hours of a Monday morning, a security guard on night duty was on his normal patrol through buildings within the Malvern site. His route to exit one of the buildings was through the open-plan computer room and out via the fire escape.

As he crossed the computer room he noticed, "a particularly eye-catching screen saver", on one of the computer screens. He sat down at the computer and moved the mouse, thus clearing the screen saver.



Among the various desktop pro grams then displayed he noticed, "a unusual icon on the screen which caugl my eye". Clicking this icon produced picture of, "two very young girls in state of undress lying on a bed ...".

A number of other icons were als displayed and clicking these reveale various other images of a similar int mate and even pornographic nature. No ing that the files were stored under heading called "STUFF", the guard r turned the screen to its original state ar left the building.

On returning to his office the guai informed his immediate supervisor ar was advised to report the matter to tl senior security manager on his (tl guard's) next tour of duty.

It happened that the guard was not c duty again until the following Friday ar at that time he duly reported the matt to the senior security manager. Tl guard was then asked to return to du and report back to the manager at 18:(hrs that afternoon.

During the day that manager reporte the incident to various other manag ment personnel and a meeting was co vened at around 18:00 hrs.

At around 18:15 hrs, the group managers with the guard, went to tl computer room and told the supervis why they were there. The supervis asked all the staff still present to finis their work and leave the building.

The statements describing the ne sequence of events varied in a numb of small details since it appeared that r one had thought to make accurate note

Once the room had been cleared, tl managers asked the guard to show the what he had done the previous Monda The guard accordingly went to the re evant computer (which was switche off), sat down, switched it on and beg trying to find the pictures he had seer

After some searching he managed find some pictures of young girls b none of the child pornography he h seen earlier. Other members of tl group then began examining other cor puters, looking for any pornograph material.

After a period of time, some adı pornographic movie clip files were l cated on one machine but seemed to l

on a network drive and there was some confusion concerning the physical location of this drive.

More searching and the drive was eventually located in yet another computer. One of the managers then attempted to copy some of the files to floppy disks "for evidence", but found that they had "disappeared".

It later transpired that at least one of the people cleared from the room had gone home, logged on to the network from his home machine and had then deleted some files from some of the network drives.

Another manager, attempting to view a number of images on a computer found that the files were being deleted virtually as he watched, "from an external source". Some files were eventually copied to floppy disks and at around 22:00 hrs the system was shut down and Roper's computer and a quantity of removable hard disks were taken to secure storage within the site guardroom.

The following Monday morning, the computer and hard disks were taken to the Ministry of Defence Police where they were connected up and switched on. Some images were examined and discussions were held.

Eventually the machines were switched off and prepared for transport to the MoD forensic division. They were eventually booked into the Computer Examination Store the following day (Tuesday) and were subsequently examined and reported upon by the forensic investigation team.

The report that the team eventually produced was a model of detail and accuracy, and correctly concluded that large quantities of pornographic material had been downloaded to the various hard disks from the Internet.

In the meantime, a series of internal inquiries had begun which culminated in several people (including Roper) being suspended on full pay while investigations continued.

The case took something over a year to come to court, by which time all but two of the suspended personnel had found other jobs (some still at the Malvern site).

Charges of possession were eventually preferred against Paul Roper and I

was instructed to examine the evidence on behalf of the defence. With some small but interesting differences, what I found agreed broadly with the case as I have stated it so far.

The main difference concerned traces of activity noted on Roper's machine in the early hours of the Monday morning when the guard noticed the "eye-catching screen saver".

I should note in passing that the accuracy of the computer clock had been verified by the MoD forensic team. The sequence of events as it appeared from the dates and time of files was that someone accessed a game called MechWars at around 03:12 hrs, at around 04:12 hrs access was made to a program called SUCKER and at 04:18 hrs an attempt (probably abortive) was made to run a movie display program.

Various periods of activity throughout the week were noted until the time (around 18:00 hrs) on Friday afternoon when the room was cleared.

On just one of the drives, a total of 37 files were found to have been altered, created or deleted during this period, totalling somewhere around 3Mb. Further activity on the following Monday compromised, contaminated or destroyed a further 2Mb.

More detailed analysis indicated that quantities of image files had been downloaded over a period of time - specifically at times when Paul Roper had been at different locations around the country.

A complicating factor was the network configuration. It seemed that virtually any machine on the network had read/write privileges to virtually any other drive on the network and my report noted: "A detailed analysis of the position of the computer on the network is impossible without detailed information on how the server was configured and precisely what access was available between participating workstations."

It is possible for example, to connect to the Internet from a networked machine and specify a network drive (rather than a local one) to receive downloaded material. Obviously a networked drive exists on another computer and will thus gain files without any

activity on the part of its operator and probably without the operator even being aware of it".

It also became apparent that not only was there no access security on most of the computers in the computer room, it was also common practice for anyone to sit at any machine and use it.

Roper's machine was popular because it was generally known that it contained a number of games programs and was situated conveniently close to a terminal connected to a different network.

This put a whole new complexion on the case and introduced new levels of complexity which needed to be taken into account when considering the provenance of files.

The picture was complicated even further when I then discovered that most of the image files had been downloaded not from the Internet proper but from the newsgroups area of an internal server named TROG.

This server, maintained and housed at Malvern, mirrored most of the newsgroup services (apparently without filtering) including those specifically concerned with various types of pornography.

Thus it was possible for a user on the Malvern network to switch on a machine, be connected to the network without any password requirement and then access the newsgroups directly.

The Internet Protocol (IP) address normally used in conjunction with a password to control and monitor access to the Internet (including newsgroups) was available without password control on TROG.

This meant that a reasonably experienced user who wished to conceal his machine's access to TROG could simply ping a known IP address and if the return showed that the number was not in use he could then configure his machine to that number and gain immediate, untraceable access.

Within the computer department, IP addresses were issued in quantity to various personnel as part of their function in the installation and maintenance of the network around the country.

Any attempt to trace who had downloaded what to where and when was thus doomed to failure. For example: user 'X' could sit at a machine, switch on and be connected to the network. He could then ping known IP addresses until he found one that wasn't in use and then use that one to connect to TROG.

The SUCKER program was then available (perhaps on a different machine) to search messages in specified areas of the newsgroups and would automatically extract and download to a previously specified drive/directory, any embedded JPG or GIF image files that it found within the messages.

The activity log from TROG indicated massive use of this program in wide-ranging areas of pornography both in and out of normal working hours. Verbal reports suggested that a common practice was to start one's machine in the morning when work commenced, connect to TROG and start SUCKER, and then leave it running as a background task while continuing normal work in the foreground.

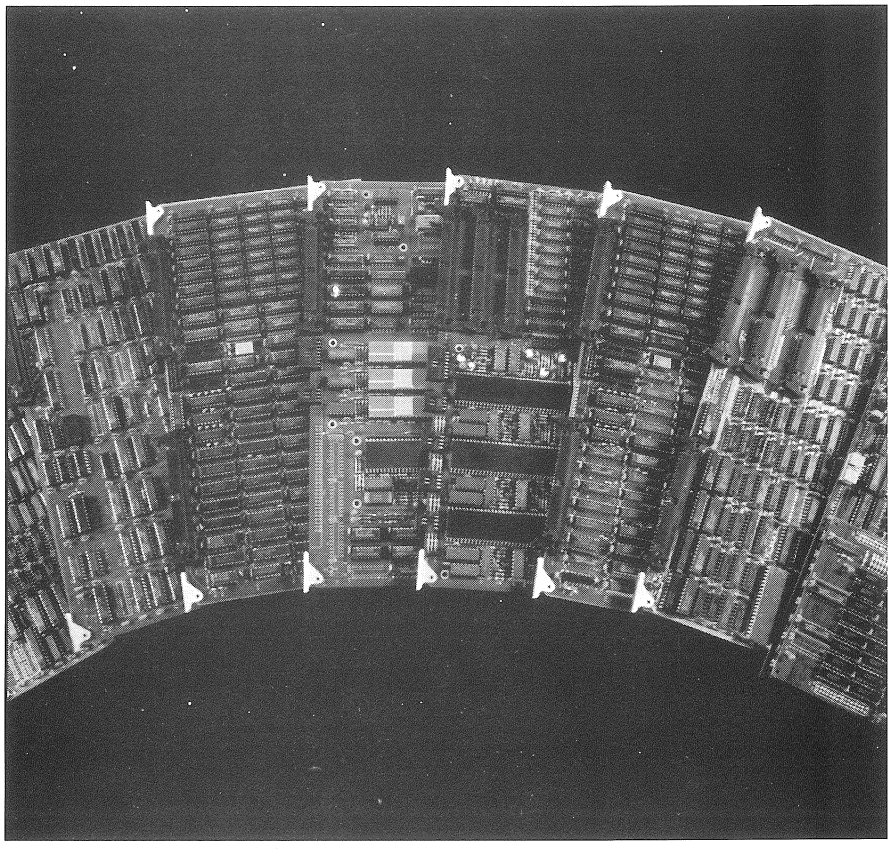
It appeared that personnel were regularly running out of disk space! Other papers in the case indicated that at least some of the management had been aware of this growing problem some months before but nothing had bee done.

In the light of this scenario it seem obvious that there was no way in whic any particular individual could be hel responsible for possessing child poi nography.

However, charges were brought an the case was proceeded with. After a fiv day trial at Droitwich Magistrates Cour Paul Roper was duly acquitted.

It is interesting to speculate upo what would have happened if he had bee found guilty. Since the images had bee downloaded from an internal server (lc cated in fact, in the same room as hi computer), if he was guilty of posse sion then surely so was the owner c TROG, the newsgroup server - Her Ma esty's Ministry of Defence!

Other points of interest which aros during my analysis of the material cor cerned the excellent report prepared b the MoD Computer Investigation Uni No observations had been made cor cerning possible contamination of th material, and no comment was mad about the origin of image files other tha that they were downloaded from the Ir



ernet. I spoke to the senior investigator and she pointed out that her remit was simply that the officers in the case were "looking for porn". She had booked the hardware in on a Tuesday and the indicated seizure date (no time) was given as the previous day. Although she was aware that the computer was a networked machine, she was given no information about the network configuration. So her conclusions and comments were not incorrect but they were incomplete when considered in the wider scheme of things. In fact it must be said that she and her team appeared to be the only ones in this whole sorry saga who had done a proper job.

Looking on the positive side, there are a number of hard-won lessons and vital questions which can be learned from this case. Firstly, when a network is conceived and configured, consideration must be given to possible illegal or unacceptable activity once the network is operating. A number of questions need to be answered at this time - among them (not necessarily in order or priority) are:

- Is there room within the configuration for some form of monitoring which may detect and report any illegal activity?
- Is the configuration such that an individual can be held responsible for the contents or activity of a specific machine?
- Can personnel introduce unknown software? Suckers, defraggers, file shredders, unmonitored passwords and similar devices, may confuse or destroy a forensic analysis and make reconstruction difficult if not impossible.
- Have clearly laid out backup procedures been set up and is there a system for regular testing and monitoring of backups?
- Are personnel properly informed about their rights and responsibilities concerning computer based material?
- Will it be possible to uniquely identify machines responsible for illegal activity?
- In the Roper case, the illegal activity was passive in that there was no attempt to corrupt machine operation.

This is not always the case and it is vital that network architects put in place an effective system of disaster recovery procedures in the event of an active, destructive attack on their systems.

- Are all relevant personnel kept up to date with current security procedures?

Should illegal or unacceptable activity be detected, a course of action will need to be determined and adhered to.

- Before starting any investigation of computers, consider where the worst-case scenario might lead. If it is to criminal action then secure forensic procedures must be implemented right from the start by isolating and securing the data before examination and accurately noting the time and circumstances surrounding it. Even possible civil or disciplinary proceedings would certainly benefit from this approach to avoid needless suspicion or actions for unfair dismissal.
- Once there is any suggestion of illegal activity, act swiftly. Computer evidence can be extremely volatile and what was there today may have melted away by morning.
- Once any in-situ investigation begins it is vital that accurate notes are taken about who does what and when. Copies of these should be passed to the forensic investigator(s).
- Accurate dates and times of equipment seizure are vital to the forensic investigator who needs to consider the possibility of contamination or compromise on the material under examination. Similarly, accurate peripheral information concerning use and access (particularly on networks) is essential if a correct picture of events is to be expected.

One final point, not directly arising from the Roper case, is too often ignored. Consider these questions:

- No matter how technically adept your investigators (at all levels) may be, are they aware of the laws of evidence?
- Having brilliantly recovered and analysed gigabytes of data, can they then produce firm and valid conclusions and observations? More important still, can they present their evidence in a simple, clear and concise report - and are they prepared to face cross-examination in court?

Anti spamming law

A recently introduced law in Washington State in the US has meant people receiving unsolicited commercial e-mail are automatically entitled to compensation payments. The legislation has already had one result and more cases are on the horizon.

The law, which went into effect June on 11, makes it illegal to falsify information about the sender, to use false or misleading information in the subject line, and to use a third party's e-mail address without that party's permission.

The law, however, only covers e-mail originating from a computer located in Washington or sent to a Washington e-mail address, and will not protect e-mail users in other states, unless the message was sent from a Washington computer.

Those breaking the law can be required to pay $500 to individual e-mail recipients and $1,000 to Internet service providers for each proved violation.

Under the legislation, would-be junk e-mail senders are required to find out which of their intended recipients live in Washington.

Bruce Miller, a contributing writer to computer publications, is $200 richer after threatening legal action against Stan Smith, of Salem, Oregon, who solicited buyers for his Tahitian Noni Juice through spam.

Seattle resident Miller, who answered Smith's number listed in the unsolicited e-mail, said that after he received a package of information for ordering the Noni Juice, wrote back to Smith and threatened legal action under the new anti-spam law.

"I'm sure people will be very happy to see somebody claim a victory for the Net," Miller said.

Miller added: "Basically, I have begun to use the law to the extent that I can. When I can track down a spammer, I send a demand-for-damages letter offering to settle out of court for $200, an amount less than the $500 which I am entitled to claim as statutory damages under the law.

"Since the law has gone into effect , I have sent out 30 such demands."

Coming just days after this first case, another firm is under the spotlight for alleged spamming.

WorldTouch Network in the US, the marketers of Bulls Eye Gold spamming software, are being sued under the Washington State law by Adam Engst, his wife, and two co-workers.

All four plaintiffs work for Tidbits, an electronic newsletter about Macintosh computers, and are Washington State residents.

The lawsuit was filed against WorldTouch Network Inc. and the company's California-based owner, Christopher Lee Knight, by Seattle-based attorney Brady Johnson.

The action alleges that the company sells a program called Bull's Eye Gold, designed to collect e-mail addresses and generate unsolicited sales-related e-mail.

According to Johnson, WorldTouch Network's marketing ploys fall under the letter of the law.

"WorldTouch Network advertises Bull's Eye Gold by repeatedly sending unsolicited e-mail advertisements that extol the program's virtues," he said. "They use spam to promote spam."

In their suit, Tidbits owner Adam Engst alleged that WorldTouch uses randomly generated bogus return addresses that claim to originate from large Internet service providers, when in reality the spam is routed through servers in Europe. In most cases, Engst said, the spam contains no actual subject line in the message header, but includes one in the message body where e-mail programs don't recognise it.

Under the suit, Johnson is seeking an injunction or court order to force Knight to stop spamming Washington State residents. In addition, he is seeking statutory damages of $500 per violation for each individual plaintiff and $1,000 per violation for Engst, who is represented as an Internet service provider. Total damages so far are more than $67,000.

"We will continue to seek damages for each new violation while the suit is pending," Johnson said.

"We want to shut down WorldTouch and prove that Washington's anti-spam law has teeth," Engst said.

Spam, said Engst, is on the increase, based on his own counts. From April 1, 1998 Engst said he has received about 1,100 spam messages.

In contrast, the number of spam messages he has received during the previous 12 months numbered only 2,300. Tidbits' lawsuit site is at http://www.tidbits.com/anti-spam.

Washington State Attorney General Christine Gregoire said the new law would act as a major deterrant but would not entirely stop junk e-mail.

"This is not a perfect law, but it will start a process for changing the behaviour of those who use the Internet to market their products and services," Gregoire said.

Nevada is the only other state that has a similar anti-spam law and consumers there who receive spam can ask to be removed from the senders' mailing lists. If the senders do not act, they could face similar financial penalties.

The US federal government is looking at national anti-spam legislation. Earlier this year, Senators Frank Murkowski (R-Alaska) and Robert Torricelli (D-N.J.) included a spam provision in S. 1618, the Telephone Anti-Slamming Act, which passed the Senate last May on a 99-0 vote.

But many Internet service providers are opposed to the proposed law.

"This bill is hardly a way to reduce his constituents' burden because it enables all junk mailers 'one free bite' at virtually no cost to themselves, but potentially huge costs to those who bear the brunt of receiving junk mail," Rachel Luxemburg, owner of America Communications in New York, and a member of the Internet Service Providers' Consortium association ISP/C, said.

Luxemburg said the group supports Rep. Christopher Smith's (R- N.J.) Netizens Protection Act of 1997, H.R 1748, which places the burden of the delivery cost of e-mail advertising on the advertiser, by ensuring that consumers will only get advertising which they actually want and agree to receive.

The spam ban would include all unsolicited commercial e-mail, including get-rich-quick schemes, electronic dating services, offers of unproved medical remedies and any other financial or sales offer.

Shadow group

Hackers have help breaking into government networks. They share their resources and techniques on special mail lists and encrypted chat areas.

By Shawn P. McCarthy

US Government security administrators are taking a similar team approach to combat the intruders.

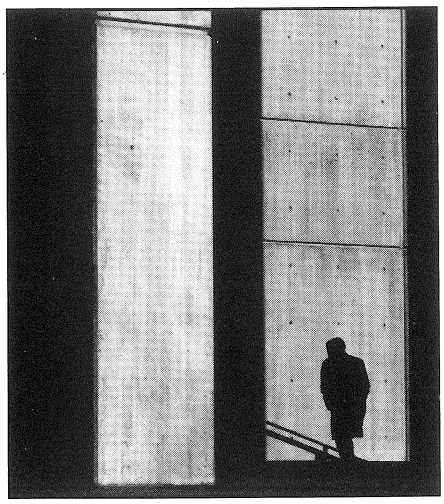
A small group of government network security experts has been using the method with industry counterparts. The exchanges have helped them form a consensus, though not full agreement, on what to do when an intruder penetrates a private network via the Internet.

The Shadow group includes representatives from several US Defence Department sites, the Geological Survey and Energy's Los Alamos National Laboratory. Corporate representatives range from General Dynamics Corp. to Disney Online.

Two big efforts have grown out of these chats. The first is a book: Computer Security Incident Handling Step by Step. Published by the Sans Institute of Bethesda., at http://www.sans.org, the $27 book discusses how to deal with intrusions, denial of service attacks, cybertheft and other security events.

The book's incident handling report lists six stages of response: preparation, detection, containment, eradication, recovery and follow-up. By far the largest section discusses preparation. It stresses yet again the need to be proactive and protect networks before an attack occurs.

The Shadow group found that a good place to start is by justifying the need for investment in a security infrastructure. It also found that many sites don't have a solid security policy or even a philosophy in place, which slows and complicates things when an incident occurs.



"You have to choose which philosophy you will follow and get management approval," Northcutt said, before formulating a response plan.

And the group learned that everyone needs security training.

The group decided that what works for large organisations doesn't always suit small ones.

Large groups have dedicated staffs to handle incidents. Small ones generally press a staff member into an expert role on short notice.

An inadequately trained network administrator, for example, might begin using a privileged account the admin had never used before. That would tell intruders they had been detected, so they would start destroying evidence and cause other damage.

The Shadow group's discussions quickly revealed the flavour of the month in hacker attacks. Members agreed on ways to deal with malicious code attacks (use virus checkers, and scan for inexplicable packets sent automatically from your network out to the Internet).

They also agreed on probes and network mapping (run your own probes to see what can be learned from Simple Network Management Protocol commands and pings). And they talked about denial of service attacks (establish an emergency backup facility), organised espionage (track traffic, point to false documents to throw intruders off), hoaxes (keep employees informed, check the hoax page at http://ciac.llnl.gov, and unauthorised access (restrict IP addresses allowed to connect).

Surprisingly, Northcutt said he's not too concerned about script-driven attacks that pound away at sites.

"The information-gathering probes

Tool to monitor network attacks

Been hacked? Only the Shadow tool may know for sure.

This is the latest weapon in the ongoing war against hackers and the first result of the new co-operative effort between government and private industries to thwart computer break-ins and security breeches.

"The key problem is that hackers win because they co-operate and security people don't," said the SANS Institute, an educational group for systems administrators and network security specialists. "It is time to begin the hard work of co-operating in search of solutions."

The Shadow detection device is already in use monitoring more than 40 known attack profiles in incoming network traffic for more than 14,000 hosts. According to the SANS Institute, analysts using the tool have also found three new types of attacks.

Features of the Shadow include the following:

- **Uses traffic analysis rather than content analysis to assure privacy for users.**
- **Monitors all ports for all protocols instead of just a few.**
- **Combines signature monitoring with statistical assessment which detects events that filters are unable to decode.**
- **Requires computing power that costs less than $10,000, including the large capacity disks needed to store massive amounts of data.**

Details about the Shadow including how to download and install it are available by emailing the institute at info@sans.org with the subject Shadow Description.

give me the greatest concern," he said. "In several cases, we have noted very accurate targeting attack attempts, which indicates someone knows a lot about our structure."

DOD sites turn to their computer incident response teams for fast help. An example appears at http://www.assist.mil.

The second result to come out of the Shadow group is called the Co-operative Intrusion Detection Evaluation and Response project, or CIDER. Also a Sans Institute project, with Navy co-operation, it aims to help organisations build their own network monitoring and analysis capability.

CIDER concentrates on two techniques. The first is TCPdump, a program that monitors and filters TCP activity for matches that indicate a problem. The second is Network Flight Recorder, a set of tools under development to monitor, archive and alert authorities.

CIDER details are available at http://www.nswc.navy.mil/ISSEC/CID. When you visit, you can download intrusion detection shareware. But because huge log files are kept, you may need to add gigabytes of drive space to make it work. The tools come with good user endorsements, however.

Finally, bear in mind that not all emergency recovery scenarios result from hacker attacks. External causes also include natural disasters, backhoe accidents and faulty equipment. Having a response plan and a disaster recovery plan is the first step to control loss of service.

For a list of Web security tools, visit http://www.perl.com/latro.

To monitor UseNet newsgroups dealing with security issues, check out comp.sys.www.security or comp.infosystems.www.cgi .

See the Best of Security list at best-of-security- request@cyber.com.au and Computer Emergency Response Team advisories at cert-advisory-request@cert.org. You can join both sites by e-mail.

Shawn P. McCarthy is a computer journalist, webmaster and Internet programmer for Cahners Business Information Inc.

Q I have encountered a PC which I am told runs under the LINUX operating system. As I have no experience of the Linux operating system can I identify if this is the operating system that is used on the PC or do I need to call in a specialist?

A I will assume that you are working with a copy of the computer hard drive. You need to examine the partition table which is located in the first physical sector of the drive (cylinder 0, side 0, sector 1) at offset 1BE hexadecimal (446 decimal).

Each entry in the partition table is 16 bytes long and there are up to four entries in the table. The fifth byte in each entry specifies the type of partition, therefore the four partition type entries will be at offsets 1C2, 1D2, 1E2 and 1F2 in hexadecimal (450, 466, 482 and 498 decimal).

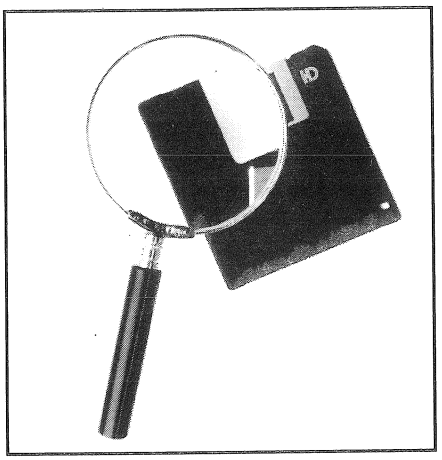
If the hard drive is partitioned for use with LINUX one or more of these locations will contain either 81, 82 or 83 Hex. An unused partition will have a type 00. On a normal DOS system the locations detailed earlier would usually contain either 00, 01, 04 or 06. Some other partition types are 0B and 0C for Windows95 32bit FAT, and 07 for OS/2 HPFS or Windows NT NTFS.

This should enable you to find out if LINUX is installed on the suspect system and from that plan your next step.

Q Following on from the previous question if Linux is the operating system on the PC can the active files on the PC be copied off in order that I can read them in the normal way on my Windows system?

A The simple answer to this is YES but it would require either a knowledge of LINUX or specialist software. The active files could be copied onto a storage device so that you could examine them on your PC in the same way as you would another DOS drive.

By using this method you can keep the cost of specialist help to a minimum and use your knowledge of the case when examining the active files.



Q I have a computer which is suspected stolen. Normally in this type of enquiry I simply boot the computer with a secure DOS disk and search drive C: in an attempt to identify the original owner.

The problem is that when I boot this computer with my secure boot floppy disk there is no drive C:. Can you suggest why this is and is there anything that I can do without going to the expense of calling in an expert?

A This question follows nicely from the first one. It may be that the computer hard drive is configured to use an operating system that is not readable under the version of DOS that you are using or there may be some type of security system installed.

If you refer to the answer to question one you can use the same method to help identify the partition type and perhaps the reason for the drive not appearing as C:. A solution would be to use a physical drive search engine such as Computer Forensics Ltd's - MYCROFT or use the physical drive search in Norton.

Thanks to Chris Magee, analyst at Computer Forensics Ltd, for this month's Q&A.

E-mail questions, comments or suggestions, to the Journal at ijfc@pavilion.co.uk

Notice Board

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

Events

UK - Association of Chief Police Officers, Internet Service Providers & Government Forum

22 September 1998, Edinburgh, Scotland
9 October 1998, London, UK
27 October 1998, Manchester, UK

The ACPO/ISP/Government Forum is to hold three one-day seminars to identify, discuss and address issues relating to policing of the Internet.

These are opportunities for those in the Internet Industry and Law Enforcement to be involved in the partnership process that is developing to ensure that criminal investigations involving the Internet are carried out quickly and efficiently with a minimum impact on the business of the industry.

The Forum is aiming to develop a memorandum of understanding between the Industry and Law Enforcement agencies describing what information may be provided and under what circumstances.

Proposals and communiqués issued by the Council of Europe and the Ministers of the G8 countries, together with events such as the recent Information Warfare Exercise held in England, have demonstrated the importance placed on these issues both nationally and internationally.

These seminars offer unique opportunities for delegates to be involved in the discussion process aimed at addressing these issues.

Details of the seminars are:

Keynote address by a UK Government Minister.

The Victim's Cost chaired by Tony Neate, ACPO Computer Crime Group

A panel of four speakers will study a recent case involving the Internet and Internet Service Providers. This case will demonstrate the cost, effect and implications of this type of crime on those concerned with the Internet industry.

Raids & Regulation chaired by Simon Janes, Admiral Management Services

A panel of four speakers, from the legal and judicial profession, examining criminal and civil liability as it applies to Internet Service Providers. The speakers will outline and seek to address the issues and concerns that Internet Service Providers and Police may have.

Time to Act chaired by Dr Neil Barrett, Bull Information Systems

An interactive panel of eight experts from various aspects of law enforcement, the legal profession and the Internet Service Industry discussing the critical issues that apply to the practicalities of policing the Internet. The speakers will be able to offer practical advice and guidance on handling incidents of computer crime.

Into the Future chaired by Nigel Jones, ACPO Computer Crime Group

A panel of five speakers representing the leading authorities who are promoting various initiatives which address security and integrity on the Internet. Speakers will give a clear indication of the benefits that may be accrued from these initiatives.

Closing Address from Keith Akerman - Chair ACPO Computer Crime Group.

The speaker will summarise the seminar and offer a view as to the manner in which the Internet Service Industry and Law Enforcement may understand each other and work together in partnership to secure their common aims.

Contact: FAS Holdings Plc
Tel: +44(0)1442 828200

IT Expo 98 - The 9th Asian Information Technology Exhibition

Hong Kong Convention and Exhibition Centre, September 16-19,

This event will also focus on the legal implications of information technology procurement, outsourcing, Y2K issues and data protection.

Solicitors, specialising in IT, digital media and telecommunications law, will be available to answer questions and give advice during the first three days of the exhibition.

The **Asia-Pacific Mobile Communications Symposium 98** and the **Professional Mobile Radio Forum 98** are scheduled during the event, and the **Hong Kong International Computer Conference** will take place on September 16 and 17. The exhibition will also focus on corporate messaging, networking systems, Internet access, and multimedia provisions.

Published by
Computer Forensic Services Lt