ISSN. 1363-6650

MAY 1998
Issue 17

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

Politicians hoping to capture votes and win approval are jumping on the moral majority bandwagon in the US.

The local and federal legislation in the States has always erred more to the conservative than cosmopolitan, with strict controls on what can and cannot be shown on television or published in newspapers and magazines.

And now that the full scope and impact of the Internet has been seen, lawmakers are gearing up to impose similar restrictions and controls.

These vary greatly in what they do, who they affect and how they are implemented. For instance, in this issue of the Journal we report how many states are bringing in legislation to filter out undesirable material from Net access computers in libraries and schools.

This is fine up to a point; the thought of children downloading hardcore porn with impunity is certainly unattractive. But the issues of taste and decency are not set in stone and a lot of the middle ground can be argued either way.

There is a real danger that baby will go with the bath water and much of the good, albeit controversial, material on the Net will also be inaccessible. When does censorship end and freedom of speech begin?

Unfortunately this issue, while extremely important, has taken centre stage over pieces of legislation which aim to harness or at least curb the real crimes being committed in cyberspace.

These very real and altogether terrifying offences include fraud costing millions, hacking for profit or revenge and those evil enough to use the Net to prey on children, either sexually or otherwise.

Law enforcement agencies have very limited budgets and these need to be prioritised to achieve the maximum impact in tackling serious crime.

In this month's Journal we also cover a news story about the dangers of treating online communications too lightly – in the US colleges and universities are already taking action following cyberspace attacks. While abhorrent and extremely offensive, these Net outbursts are usually just the product of immature and excitable imaginations and lack any real substance.

People, including most of the adult workforce using e-mail, feel they can say what they want online, no matter how abusive or libellous. They send messages they would never dream of speaking out loud or putting in a letter.

But it's important to put this sort of behaviour into perspective rather than using a sledgehammer to crack a nut. Action should be taken, but it should be in proportion to the offence and not used as a political vehicle for furthering any politician or prosecutor's own agenda.

The Internet is a medium like any other form of communication, and has to conform to the rules and regulations that are imposed if it is to flourish within a democratic and creative framework.

But we have to see where the real dangers lurk, and find the right way to ferret the culprits out and punish them without stifling the unique aspects of online communication that make the Net so important.

The Journal would welcome article submissions from anyone working or studying in the field of computer forensics and law, including case studies, technical pieces, product reviews and news updates. For further information contact the Journal editorial team.

News

NASA hacker arrested

A 22-year-old Canadian man suspected of breaking into a NASA Web site and causing tens of thousands of dollars in damage has been arrested by Canadian Mounties.

The Royal Canadian Mounted Police in the northern Ontario city of Sudbury charged Jason Mewhiney with mischief, illegal entry, and wilfully obstructing, interrupting, and interfering with the lawful use of data, Corporal Alain Charbot said.

Charbot said the unemployed former part-time computer science student was "very knowledgeable" when it came to computer systems.

Canadian police were tipped off 14 months ago by FBI agents in Washington, who were investigating security breaches into computer systems at NASA.

More than $70,000 worth of damage was caused at the NASA Web site and officials were forced to rebuild the site and change security, Charbot said.

The FBI tracked the hacker by tracing telephone numbers to the Sudbury area. The Mounties raided the homes of Mewhiney's divorced parents and seized an old computer, a second basic computer, a high-speed modem, diskettes, and documents.

Charbot said police were still investigating breaks at several Canadian college and university sites.

The number of charges has not yet been released, but for each count there is a maximum penalty of one year in jail and fines of thousands of dollars.

Canadians condone software piracy

Nearly half of those Canadians questioned in a survey said that pirating software for personal use is an acceptable practice, according to the Canadian Alliance Against Software Theft.

The study found that only 20 per cent of respondents would report someone for unlawfully copying software, yet 70 per cent say that software piracy has a negative impact.

Norm Dubois, Microsoft Canada's anti-piracy marketing manager, and a CAAST spokesman, said that the piracy rate in Canada is 42 per cent, compared to 27 per cent in the US," he said.

Dubois said that the relative newness of computers in Canadian society is a factor in creating this attitude. He added that of software pirates, most were either new users or young users who did fully understand the potential consequences of piracy.

The study was conducted by Toronto-based Decima Research. Among the respondents, 70 per cent were computer users, either at work or at home.

CAAST and software piracy can be found at CAAST's web page at http://www.bsa.org/canadadocs

Child porn arrests

In one of the first cases of its type in Denmark, a 40 year-old man has been charged with distributing child pornography across the Internet.

Although police have not named the man, they have confirmed that he has also been charged with abusing his seven-year-old daughter.

Police sources have indicated that the man was arrested as part of an ongoing pan-European investigation into Internet pornography, with its roots in Belgium and France.

If found guilty, the man could get up to six months in jail for the Internet porn charges, but would also be hit by a 10-year sentence for the physical sexual abuse of the child.

Police have said that the man was arrested due to his online activities with a pan-European child sex ring on the Internet that spans 19 countries.

According to Preben Andersen, the Danish Deputy Criminal Inspector, investigations into the ring are ongoing in Belgium, France, Germany, and Italy, as well as in the US and Canada.

During the raids on the unnamed man's house, police found more than 20,000 images of children on the man's PC, while reports suggest that videos of him abusing his daughter were found when the raids took place late last year.

French police swooped in across France in mid-March to make more than 30 arrests as part of an ongoing project to stamp out Internet pornography.

In that case, police have said nothing, although the French media has reported that the 30-plus people are suspected of being members of an online network exchanging paedophile images across the Internet.

French TV stations reported that, as well as exchanging pornography across the Net, the group was also busy organising "sexual encounters" between adults and children, and that police are interested in talking to their counterparts elsewhere in Europe, where the groups' activities are known to have spread.

Unconfirmed reports on French TV last month suggested that the mid- March clampdown was the direct result of an arrest late last year of a known paedophile, who had details of the group's activities on his PC.

The files containing the information were encrypted, but the file system was easily cracked by the police's computer staff, reports suggest.

Last November, French police announced a massive clampdown on Internet using paedophiles across the length and breadth of the country, resulting in 50 people being detained and five people subsequently being arrested.

According to senior police at the time, the roundup of 50 suspects was the culmination of an eight- month investigation by the paramilitary division of the Gendarmes, the French police force.

More arrests in Net gambling probe

The case against offshore Internet gambling operations is growing, with charges filed against the operators of five Internet sports betting companies in the Caribbean.

Recently the US government filed charges against 14 owners and managers of six online betting companies in the first cases of federal prosecutions for gambling on sports over the Internet.

"We will continue to monitor and vigorously prosecute offshore sports betting operations that engage in this blatantly illegal activity," Mary Jo White, US Attorney for the Southern District of

New York, said.

The five separate complaints charge the seven new defendants, all US citizens, with "owning and/or operating sports betting businesses that illegally accept wagers on sporting events over the Internet and telephones."

All of the companies advertise and promote their sports betting operations to US customers on Web sites, the complaint stated.

White said: "Such blatant and widespread efforts to evade gambling laws cannot and will not be tolerated.

"These cases send an important message that we will vigorously prosecute any use of the Internet to conduct criminal activity."

The cases are likely to become the testbed for laws against Internet gambling. The separate complaints charge the defendants with running Internet sports betting operations headquartered in the Caribbean and Central America.

According to the complaint, the seven new defendants are affiliated with Galaxy Sports and Grand Holiday Casino both located in Curacao; World Sports Exchange and World Wide Tele-Sports, both located in Antigua; and Global Sports Network, located in the Dominican Republic.

Each of the defendants faces a maximum sentence of five years in prison and a fine of up to $250,000 if convicted.

UK security breaches

According to a report on security titled the Business Information Security Survey 98, British firms are ignoring IT security issues to the point where it is causing major problems.

The survey said that nearly half of all respondents have suffered from an information technology security breach, 48 per cent of which were considered serious. Developed by the National Computing Centre, in conjunction with AT&T, DTI, the UK ITSEC (information technology security) scheme and Sysdeco, it concludes that IT security breaches are a major threat to business.

According to the NCC, the cost to business could run into billions of pounds. The survey found that the average cost per breach was £7,146 and that this cost actually increases to more than £20,000 for sites with more than 500 employees.

The NCC says the research has shown that the true cost to business is likely to have been substantially under reported by the respondents and the real figures are likely to be as much as three times higher.

Despite these startling figures, only 39 per cent of companies have some form of IT security policy in place. With 72 per cent of respondents rating security at least four out of five in importance, this highlights a large gap between awareness and IT security practice, the report notes.

The report suggests this may often be caused by companies failing to inform employees of their security policy and outlining what action should be taken to prevent breaches from occurring. Revealingly, 53 per cent of companies who had suffered a breach said that it could have been prevented.

While almost all respondents were aware of the Data Protection Act and the Copyright Act, less than half were aware of the Computer Misuse Act 1990.

The report notes that the frequently predicted security threat from the Internet does not yet seem to have materialised.

While a fifth of the organisations expected all employees to have Internet access within 12 months, a quarter have suffered from a breach arising from a virus. The NCC's Web site is at http://www.nnc.co.uk

Sex offenders online

The state of North Carolina in the US has begun making information about convicted sex offenders available online.

A 1996 statute requires state residents to be registered with the local police, and that information is what makes up the database of more than 2,000 people.

Users visiting the database, at http://sbi.jus.state.nc.us/sor need just supply a zip or postcode, city name or county name to get a list of registered sex offenders in a desired area. The list is also searchable by name and age.

The North Carolina Sex Offender and Public Protection Registry was established in January 1996 and the law requires all North Carolina residents who have a reportable conviction to maintain registration with the sheriff of the county where they reside.

Gearing up against spam

Internet Service Providers in Washington state in the US are being told to take those behind junk e-mail to court.

Assistant Attorney General Paula Selis of the Washington State Attorney spoke about the problem at the Washington Association of Internet service providers held in Seattle.

Selis told WAISP members how they can use new anti-spam law that takes effect June 11, 1998. Selis said the Attorney General's office received some 1,000 complaints about spam in just one portion of 1997 alone, up from nearly zero just two years ago.

The law makes it illegal to falsify the point of origin of the message, provide misleading or false information in the subject line, or use a third party's Internet domain name without permission.

It applies to electronic mail sent from computers in Washington State or sent to e-mail addresses of Washington State residents. ISPs can go after spammers at the rate of $1,000 per message and attorney fees. The law also allows recipients action at $500 per message.

The Attorney General's office is also authorised to file lawsuits and spammers could be sued by all three parties simultaneously.

Under the provisions of the law, a person cannot send illegal spam to a Washington resident if the spammer knows, or has reason to know, that the recipient's e-mail address is held by a Washington state resident.

Consequently, said Selis, "The law creates an obligation for the spammer to determine if an email address belongs to a Washington state resident. In order for this law to work, this information has to be available to the spammer."

A method defined in the law, but not restricted to that method, is for the ISP to make the information available to spammers upon request. Selis added that

there is no prohibition for charging a reasonable fee for this Washington State residency verification.

Washington State customers of America Online, however, may find it difficult to use the law. The latest word from America Online via AOL spokesperson Tricia Primrose is that the service will not provide residency verification, citing privacy concerns.

Should a spammer contact AOL, ask for verification, and be denied that verification, the law may not apply. ISP Earthlink reported the same position.

Even though customers may run into some barriers, Selis said "Our office will be looking to file lawsuits this year."

Text of the anti-spam law can be found at http://www.eskimo.com/~brucem/tugsplaw.htm

Investigation into online fraud ring

Authorities in Canada are investigating an online investment service after complaints from European investors.

The British Columbia Securities Commission is looking into the activities of a firm called Turner Phillips.

The company falsely claimed on its Web site that it was a member of official financial regulation bodies, and the Commission said the firm was not registered under the Securities Act in any capacity.

Commission spokesman Lang Evans said that the complaint originated with six alleged victims in Sweden.

He added, "We don't yet know the scope of the operation...usually we hear from a small fraction of the overall victims."

The scheme consists of an initial sale of suspect securities to investors. After the initial purchase, investors are re-approached by a firm such as Turner Phillips and are offered the opportunity to sell their original securities for a significant profit.

The catch is that in order to sell the securities, the investor must post with Turner Phillips an advance cash fee as an insurance bond. Investors caught in this scheme will usually end up losing their original investment and the advance cash fee since the repurchase offer is never concluded.

Evans said the operation looks like a duplicate of an operation known as Bathgate Dryfus Pierce, which was uncovered in the UK last year.

The British Columbia Securities Commission has issued a free Investor Protection Kit on its Web site at http://www.bcse.gov.ba.ca

Microsoft guns for pirates after victory

Microsoft Australia is claiming a major victory in its war against piracy. The company says an award of damages of $197,389, plus costs, should "illustrate to illegal software dealers that they face stiff penalties for violating intellectual property rights".

The Federal Court penalties followed the long-running campaign it fought with KT Technology (Aust) Pty. Ltd., a Melbourne software and hardware supplier.

KT's admission of liability for breach of Microsoft's trademarks and copyright by importing and selling counterfeit Microsoft mice and Microsoft Multimedia packs, and selling counterfeit Windows 95 product.

After an incident in 1996 when a shipment of counterfeit mice was seized, KT Technology consented to restraining orders. But only a few months later, Microsoft was tipped off that more counterfeit Windows 95 software had entered the market. An Anton Pillar raid followed, then the Federal Court issued its restraining order.

However, after counterfeit product was later purchased from its store, Microsoft claimed KT had breached the order and was in contempt of court. The statement says KT admitted contempt and was ordered to pay costs.

Code cracked on digital phone

Cryptographers have "cloned'' a digital cellular phone, until now considered impossible.

Cloning, or copying the codes in a cell phone so that an unauthorised user can use them to make calls on another phone, costs the industry millions of dollars every year.

Thieves use specially configured analogue phones to steal codes out of the airwaves, then sell cheap, illegal calls.

The Global System for Mobile Communications (GSM) digital standard is the most widely used in the world, with more than 79 million phones in use. The cryptographers used a GSM phone, which is still relatively rare in the US.

David Wagner, who with fellow University of California-Berkeley graduate student Ian Goldberg broke the encryption algorithm in about five hours.

The cryptographers' feat is the first public cracking of any digital phone code. Encryption uses an algorithm to scramble data to make them secure. Fellow researcher Marc Briceno of the Smartcard Developers Association provided the digital phone's algorithm after two months of tinkering with the phone's chip on nights and weekends, he says, with only "a home-built smart card reader and a laptop."

The trio did the research purely as a challenge. Wagner and Goldberg also found a security flaw in Netscape's Web browser in 1995 and broke analogue phone codes last year.

One reason they wanted to test the chip's code was that it was designed in secret. "Security through obscurity doesn't work," says Wagner, who urged the industry to make security designs public as many code creators do so cryptographers can test them.

But industry experts say that to clone a GSM phone, hackers would need to have it for six to eight hours to extract the code key from the chip inside the phone.

That single copy wouldn't be of much use because digital networks don't allow the same account to be used by more than one phone at a time.

BSA on Net piracy

With its confidence boosted by a series of well-publicised successes against Asian software piracy, the Business Software Alliance is turning its attention to the perils of the Internet.

The issue is the popularity of "warez," or pirate software and serial numbers distributed over the Internet.

Robert Kruger, the BSA's vice president for enforcement, admits his organisation has failed to find evidence of a problem in Asia, but said: "It belongs on everyone's radar screen. Internet piracy really is a new frontier for us."

Kruger said that, although there were no reliable figures for the size of the problem, there was evidence of its rapid growth in the US, where the BSA is closing down warez sites "almost every day."

In the Net's early days, users often exchanged pirate software by way of local bulletin board services and newsgroups. But the death of the local BBS scene and the size of today's commercial software have seen both of these avenues dry up.

Pirate newsgroups such as alt.binaries.warez.ibm.pc are now mainly a source of serial codes, as posting and retrieving software has become "very inefficient," he said.

E-mail is another cause for concern for the BSA. Kruger used the example of someone e-mailing a copy of Norton Anti Virus to a friend.

But it's the Web, and the dawn of e-commerce that have got the BSA worried. "The most chilling thing of all is Web sites, where you can download the software direct," said Kruger.

Although most pirate Web sites are run on an amateur basis, Kruger said the use of advertising and mail-order CD sites were an indication of the commercial viability of online piracy.

But he added: "From the victim's point of view it doesn't make a heck of a lot of difference to us whether a person is making a lot of money doing this or whether they're some eccentric philanthropist."

Kruger said the exponential growth of the Web means the arrival of widespread Web piracy is inevitable.

To keep track of the problem, the BSA employs reformed warez distributors, who spend time in Internet Relay Chat rooms and scan File Transfer Protocol sites for evidence of illegal software.

"We use these people. They show us how these things are done. We'd rather have them working for us than working against us," said Kruger.

Kruger, a former Assistant US Attorney in Washington, said he had encouraging discussions in Hong Kong with a number of officials, including those from the Customs, Judiciary, Trade Department, Trade Development Council, and the Consumer Council.

Kruger said the BSA hoped to increase international co-operation between governments to aid prosecutions.

However, he admitted that co-operation would have to be on an information and legislative level, as governments would be unlikely to consider the issue serious enough to warrant extraditions.

AOL not liable for libel says judge

America Online and other Internet service providers are carriers, not producers, of information online, and therefore cannot be sued for providing information developed by third parties, a federal judge has ruled.

The immediate effect of the ruling, by US District Judge Paul Friedman, releases AOL from a $30 million defamation lawsuit filed against the online giant and Internet gossip columnist Matt Drudge.

In his 28-page ruling, Friedman said that Section 230 of the Telecommunications Act of 1996 specifically exempted ISPs from such lawsuits.

The original suit, which named both AOL and Drudge as defendants, was filed by White House adviser Sidney Blumenthal and his wife, Jacqueline, after Drudge alleged in his August 10, 1997 Drudge Report that Blumenthal "has a spousal abuse past that has been effectively covered up."

"Whether wisely or not," Friedman wrote in his ruling, Congress "made the legislative judgement to effectively immunise providers of interactive computer services from civil liability ... with respect to material disseminated by them but created by others."

"In recognition of the speed with which information may be disseminated and the near impossibility of regulation information content" on the Internet, Friedman wrote that "Congress decided no to treat providers of interactive computer services like other information providers such as newspapers, magazines or television and radio stations, all of which may be held liable for publishing or distributing obscene or defamatory material written or prepared by others."

The case against Drudge, whom Friedman called "simply a purveyor of gossip," and not a journalist, will continue, however.

Although Drudge retracted his statement and issued an apology a day after the original report was published, Blumenthal and his wife sued both Drudge and AOL for $30 million.

Drudge's gossip column is available on his own Web site and several ISPs, including America Online, which pays Drudge $3,000 a month to run his report.

Blumenthal attorney Jo Bennett Marsh said the couple will appeal Friedman's ruling, and will continue the suit directly against Drudge.

Student's e-mail slur

Law enforcement officials are cracking down on illegal activities on the Internet although the perpetrators call these offences mere "student pranks".

Police in the US have investigated a series of separate incidents, including online death threats, racial slurs, and offensive jokes.

A 19-year-old student at the University of Maine sent a message to a fellow student saying "I'm gonna shoot you in the back of the head." Inadvertently, he sent the message onto campus computer bulletin boards, including one run by a gay-lesbian group.

The state attorney general started a hate crime lawsuit, accusing the student of violating the civil rights of homosexuals. The university ordered him to serve 30 hours of community service and suspended his computer account. The state waived a $5,000 fine when Belanger signed an agreement promising not to harass or threaten others.

On the Internet and via e-mail, offensive material travels through cyberspace between anonymous users, often without repercussions.

But when such expressions appear on college and university computer networks, they can trigger complaints or even criminal investigations. They can

also set off a debate pitting First Amendment rights against campus administrators' authority and responsibilities.

In another case, an Internet site that listed the names of high school students and how they should die was shut down and the police called in.

Despite the offensive nature of the site, titled "People deserving to die and how," most students considered the publication little more than a joke, said Joe Crowder, superintendent of schools in the Washington state town of Cashmere.

Other recent cases include:

- Four students at Cornell University in New York state who sent a derogatory joke about women to their friends through e-mail. The message was sent on via e-mail prompting angry responses from across the country.
- At the University of North Carolina, officials closed an e-mail account belonging to a former student after a racist message from that account was posted on at least 10 Internet news groups. Anyone reading the joke about "why all blacks should go back to Africa" could see that it originated at the university.
- At Virginia Tech, a student was punished for posting a note on the World Wide Web page of a gay organisation that suggested gay men be castrated and killed.
- At Bates College in Lewiston, Maine, a student used the computer network to type an obscenity-laced message saying she hated white people. Bates officials called the message "offensive and divisive."

High tech forgers

Federal investigators in the US are warning that just about anyone with a computer can begin counterfeiting money.

Treasury officials estimate that 43 per cent of domestic counterfeits are produced on personal computers, compared to less than one per cent just three years ago. But federal law remains rooted in the days of illicit printing presses and large stashes of counterfeit bills.

Today, when law enforcement officials raid a counterfeiting operation, all they may recover is common office equipment and a computer disk. Counterfeiters' punishment is often based on the number of fake bills found at the scene, which can lead to lighter sentences for computer fraudsters, who often just print out a few bills at a time.

Dennis Lynch, special agent in charge of the Secret Service's Counterfeit Division, asked the US House subcommittee on Domestic and International Monetary Policy to craft tougher penalties for computer counterfeiters.

He said would-be counterfeiters could download dollar bill images from Internet sites, or use a scanner to create an even sharper image. Some criminals even use high-resolution copy machines to run off pages of low-quality bills.

Lynch said computer-generated, ink-jet counterfeiting accounted for 19 per cent of all currency seized in fiscal year 1997, an 805 per cent increase from 1995. For the first five months of 1998, ink-jet printers were used to make 43 per cent of the fake currency seized

"When using the technology currently available these devices are capable of producing high-quality counterfeit currency," Lynch said.

The Treasury Department is in the process of putting more anti-counterfeiting measures into the currency.

Already new $100 and $50 bills are in circulation, and later this year a $20 bill will incorporate watermarks, holographic strips and other improvements.

Subcommittee chairman Rep Michael Castle said measures that could tag laser printers to make it easier to identify the origin of computer fakes will be considered. The technology is already in use in colour copiers.

Castle said: "Personal computer counterfeiting has become a print-to-order crime and previous sentencing guidelines based on total amounts of notes seized should not apply."

New computer laws

Law makers in the US state of Illinois have voted to crack down on cybercriminals by creating two new high-tech offences.

The creation of the crimes of theft of on-line services and harassment by computer were unanimously approved. Harassment by computer would include transmitting obscene comments with the intent to offend; interrupting Internet service use with the intent to harass; transmitting anything that would prevent a person from using their computer with intent to harass; threatening injury by computer.

"This will be the crime of the new millennium," predicted the bill's sponsor, state Rep. Elizabeth Coulson.

Judge strikes down ruling

A federal judge in the US has struck down part of a child pornography law that targets computer technology used to alter images to make them sexually explicit.

District Judge Gene Carter said that language in the 1996 law that defines child pornography was unconstitutionally vague.

Previously, prosecutors had to prove that children actually were used in the pornographic images that were shipped, including by computer, across state lines.

Kathy Fondacaro, spokeswoman for the National Coalition Against Pornography, criticised the ruling, saying paedophiles will use the materials to arouse themselves and then seek out children.

"Whether it's simulated technologically or it's the real stuff, it arms a paedophile," she said today. "It arms a paedophile so it's easier to find children and molest them."

Carter, who issued his ruling in Portland, is the first judge in the country to attack the constitutionality of the Child Pornography Protection Act of 1996.

Legal observers predicted that the matter is likely to end up before the 1st U.S. Circuit Court of Appeals in Boston.

"If it ends up there is disagreement among the circuit courts, this would be the type of case the Supreme Court takes on," said Jeffrey Douglas, a lawyer with the Free Speech Coalition. "Then this could turn out to be a landmark case."

The Supreme Court has already struck down another law aimed at regulating Internet smut. Last June, the court ruled that the 1996 Communications Decency Act, in attempting to protect children from indecent material on the

Internet, improperly restricted the free-speech rights of adults.

The Child Pornography Protection Act was adopted to combat the use of computer technology that enables a pornographer to alter a picture of a child to make it seem as though the child engaged in an explicit sex act.

FBI and computer crime

Businesses should report hacking to law enforcement authorities, just like any other crime, an FBI official urged.

In a presentation at an event in the US sponsored by technology firm Bull, Richard D. Watson, assistant special agent in charge for the FBI, pointed to several recent examples of serious computer crimes.

In one case, Watson said, a hacker by the name of Carlos Salgado, nicknamed "Smack," was caught by the FBI in an Internet-based "string" after he unwittingly sold stolen credit card numbers to federal agents, for $5 or less apiece.

"Smack" is currently serving a prison term of about 31 months for the deed, according to the FBI agent.

In another case, a systems integrator allegedly deliberately crashed a network server at Forbes Magazine, after he'd been fired from his job.

Watson said that the bureau is witnessing an increase in computer crime among "former employees who have a vendetta." In Texas, a ring of cybercrooks with a high degree of expertise in telecom technology broke into and "re-engineered" systems used by MCI and Sprint, among others, making off with items that included unlisted phone numbers.

But a recent study shows that only about 17 per cent of all computer crimes today are being reported to law enforcement agencies, according to the FBI agent.

This is despite legislation passed by the US Congress such as Title 18, which makes it a federal crime to break into any computer, including a small office's PC, that is used in "interstate commerce."

The main reason why companies are reluctant to report these crimes is fear of exposing the security holes in their systems, Watson contended.

As a result, the names of victimised organisations are not being released by federal authorities until the cases come to trial, giving the companies adequate time to rectify the security problem.

Watson also maintained that law enforcement agencies need access to cryptography keys as a weapon against cybercrime.

As with federal wiretapping, though, use of cryptography keys should require a warrant - and the court should carefully monitor its use, revoking permission if authorities fail to find evidence within a week or so that the alleged perpetrators are "talking about crime" over the Internet, according to the agent.

Not all presenters at the event on Monday agreed with Watson's stance on cryptography.

During a panel presentation at the event, Steve Foote, VP of research strategy for the Hurwitz Group, suggested that it would be impossible for the US government to regulate cryptographic products sold by companies outside the US.

Steven J. Ross, director, Enterprise Risk Services, for Deloitte & Touche, predicted that by demanding key access, federal authorities would be "pushing" the thriving industry of cryptography from the US to other nations.

Web firm carries on fight against spam

A Web company has been awarded $174,000 after it took action against a group of businesses which used its e-mail server to send spam to thousands of its customers.

SimpleNet executive Allen Cocumelli said the aim was not to make money from the legal case but to highlight the need to hit back at those sending junk e-mail.

"The main reason is to show the Internet community that we can respond to these acts and we can win," said Cocumelli. He now intends to pursue a criminal complaint against the spammers with the local district attorney.

SimpleNet, of San Diego in California, is a "Web hosting" company, whose customer e-mail list, amounting to tens of thousands of addresses, was spammed with some 100,000 messages during a four-month period in 1997.

The messages appeared to come from SimpleNet and used SimpleNet's mail server. The content of the e-mail promoted a book titled, "Meet, Attract and Date Gorgeous Women."

The award came when the defendants, which include the firm VNZ Information, failed to appear in court.

Cocumelli said the case of spamming and stealing e-mail addresses is not an uncommon story, but in this case, SimpleNet traced the perpetrators through a private detective.

"Today's technology can make it difficult to trace these types of acts," said Cocumelli. "But in this case they made one mistake.Their e-mail listed a post office box number. We hired a detective to watch the box and then follow whoever opened it.

Since the spamming appeared to come from SimpleNet, several Internet service providers stopped access to Web sites hosted by SimpleNet.

In addition, the load on SimpleNet's mail server caused clients to lose send and receive capabilities. Cocumelli said he chose the federal court because it would bring more attention to the case.

"People need to know these things happen to a lot of companies, not just AOL," he said. "Not only can they happen, but we can find them and take them to court and win."

Now, Cocumelli says he believes he has a case which will stand up in a criminal court. "I think this case has enough evidence to show criminal intent and I am pursuing it now."

Paedophiles caught in Net sting

More than 60 suspected paedophiles, most living in Scandinavia, have been arrested by US police who lured them by posing as children on the Internet.

Police in the state of New Hampshire set up a special unit to crack down on paedophiles using the Web to find vic-

tims, according to detective James McLaughlin.

The New Hampshire police, posing as children, set up meetings with the suspects on the Net. Over the weekend, a 47-year-old British man living in Norway was caught by police when he arrived for a meeting in New Hampshire with an officer who had posed as 14-year-old "Billy" on the Net.

The suspect, whose name was withheld from the newspaper account in accordance with Swedish law, was charged with attempting to have sex with a minor. He is expected to be tried in a US court.

Web of lies rejected

A court in the US has cleared a woman who was sued after calling a man a liar on the Internet.

Stacy McCahan called Ken McCarthy a liar in a public online forum and was challenged with a $5,000 lawsuit. McCarthy won his case in small-claims court in February but has now lost to McCahan's appeal in San Francisco.

McCarthy, a Web consultant and freelance journalist, argued the posting was a personal attack that could damage his reputation because it was archived on the Net.

But in court earlier this month, McCahan's attorney countered that "flame wars" were customary on the Net, where people regularly exchange insults during heated discussions.

The San Francisco Superior Court, which doesn't write detailed opinions in such cases, ruled in favour of McCahan and ordered McCarthy to pay her $221 in attorney's fees and other legal costs.

"I think it is a victory for uninhibited, robust, and wide-open speech on the Internet," said Karl Olson, McCahan's San Francisco attorney.

But McCarthy rejected the claim that the case was about free speech.

"This was someone who was abusing the Net and found a sleazy lawyer to dress up her behaviour as 'protecting the First Amendment,'" he said today. "The key to her attorney's whole strategy in court was to turn me into a public figure - just because I had used the Internet - so I would lose my protection from defamation."

The dispute began last year during a public controversy over San Francisco's Critical Mass bicycle protest, which resulted in multiple arrests during a ride last July. McCarthy said he emailed McCahan, one of the more visible members of the bicycle group, and asked her for details regarding a posting she made to the "sf-critical-mass" mailing list.

McCarthy says he was working on some investigative articles about Critical Mass for his Web site, E-media, and emailed McCahan three times requesting an interview with her. The two then exchanged email and later had an argument on the phone, both say.

Then, on July 30, McCahan posted to the "sf-critical-mass" mailing list a message entitled "Ken McCarthy is a liar—be warned." Her posting accused McCarthy of inaccurately stating the details of their phone conversation in another posting and of harassing her.

Net criminals fight back hack attack

The manager of a small Internet access provider says vandals shut down her site in retaliation after she reported a child pornography site to law enforcement authorities.

Marrya VandeVen, general manager of ISP Stockton Community Wide Web in California, said she came across the pornographic site on March 11. The site, which she had traced to New Mexico, was not hosted by her ISP.

"I've been working with other parents and groups on ways to keep our children safe. When I came across this site, I was really upset - not as the general manager of an ISP, but as a parent.

"How could someone convince a child to do that? This wasn't a young-looking 20-year-old. This was a prepubescent child pornography site."

VandeVen, who has a seven-year-old son, says she brought up her discovery on a mailing list that discusses unsolicited commercial email.

She asked the list's members what to do about the information she had been able to gather about the site's origin and owner.

"I got a lot of criticism. People told me to mind my own business and let it drop," she said, noting that some warned her of the threat of retaliation if she reported it to law enforcement. Still, she added, "I never thought my peers would tell me not to do what was right."

However, Doug Lim, another list member, said, "Since the list's purpose is to defend against and work to prevent spam, and the fact that Ms. VandeVen did not actually receive spam from or promoting the site, a few people felt that her posts were off-topic, but most responses were helpful."

Lim said that because the list is designed to combat spam, often spammers "lurk" on it to learn what is being done to fight their practices.

"If you'll grant the assumption that those who send junk e-mail are sorely lacking in ethics, certainly it's not hard to imagine that some of these spammers also traffic in pirated software and/or child pornography," Lim said.

"Perhaps that is where the threats and harsh criticism and suggestions to 'mind her own business' came from."

On Sunday, March 15, "I got a call at home from an employee at about 7 p.m., telling me the server was locked up. That happens every once in a while," she said.

When the employee rebooted the system, however, "nothing came back up," VandeVen said. "It deleted everything mounted on the system. The hackers were good - they got the backup to launch, and it wiped itself clean."

She explained that the hack was perpetrated using a Unix command to remove the root files, the core operating system files.

"We had to rewrite everything from scratch," she said, noting that some information was saved on an old, "retired" hard drive, which the ISP used in the interim. "We had to re-create an ISP from a blank computer."

Since the ISP has been repaired, VandeVen said she is still feeling the effects. "I've gotten threatening emails from as far away as Australia," she said.

"They feel I've encroached on one of their own. But if I have to be hated by any group, this one I don't mind so much."

Product news

Law online

Two legal databases have been put onto the Web to speed up both research and locating lawyers and their firms.

The online databases, include the West Group's Web-based Westlaw, and a customised version of Martindale-Hubbell's database of more than 900,000 listings of lawyers and law companies developed exclusively for the American Bar Association.

The new site can be accessed on the ABA Network, located www.abanet.org

Martindale-Hubbell's original Lawyer Locator is located at http://www.martindale.com and the Westlaw legal database is at http://www.westlaw.com

The database provides full access to Westlaw's more than 10,000 databases and the hypertext linking capabilities of the site also allow researchers to jump to other sources within and outside of Westlaw documents.

Security certification service

The International Computer Security Association has introduced a service that attempts to plug holes to protect networks from hacking attacks.

ICSA say that Internet protocol configuration details are too complex for most information technology departments to handle them correctly. The firm's system, called TruSecure, is designed to establish and then monitor corporate network security angles.

Pam Zemaitis, ICSA TruSecure program manager, said: "Security products are now so complex and the relationships between parts of the network so dynamic that many companies have discovered they need to put processes in place to evaluate how vulnerable they are.

A study by ICSA found the top problems managers face include inadequate security policies, such as policies for password management, incident response, internal data destruction and physical access, which together accounted for 40 per cent of network security failures. Non-secure services like unsecured NETBIOS, echo, telnet or ftp services accounted for another 25 per cent of problems.

Undocumented devices like dial-up modem lines, test servers and backup Web servers accounted for 20 per cent. Inadequate data backup policies, such as infrequent or non-existent backups, inappropriate backup media, or lack of data recovery planning accounted for 10 per cent, and outdated software accounted for the remaining five per cent.

The TruSecure service costs $39,995 a year per site for up to five devices such as firewalls and e-mail servers and will take a five-step approach to the problem, Zemaitis said.

First, a team will test and analyse current vulnerabilities. Next the organisation will prepare a methodology of best practices to bring the system up to security standards. Once the site has been brought up to scratch with all current security patches, needed hardware and the like, ICSA will conduct on-site audits, provide continuing perimeter certification and then make periodic spot-checks.

For more information contact ICSA on +1 717-241-3233, e-mail brose@icsa.net or visit the Web site at http://www.icsa.net

Fears over accuracy of virus scanners

At the recent InfoSecurity '98 show in London, Reflex Magnetics announced that it has undertaken a series of tests that have revealed the unreliability of most commercial virus scanners.

UK data security specialist Reflex says the tests, conducted over the last two years by independent consultancy BrownWright Security, showed that some products missed hundreds of potentially crippling viruses.

Reflex says that BrownWright used a test library of 6,301 "viruses" acquired by courtesy of around 20-or-so easily accessible Internet Web sites. The company has recently published the results of its testing in a paper entitled "The Great Scanner Mystery."

"BrownWright's report lays bare the bankruptcy of the anti-virus vendors' product hype," said Phillip Benge, Reflex's sales and marketing director.

He added that claims by anti-virus companies offering 100 per cent detection rates were absurd.

"The BrownWright tests clearly demonstrate that there is no such thing as complete protection against computer viruses and no chance of 100 per cent detection," he said.

"Whatever their vendors claim, virus scanners alone just cannot provide adequate protection for business critical systems," he claimed, adding that the trouble is that many users have been lulled into a false sense of security by the scanner vendors' hype.

Reflex Magnetics' Web site is at http://www.reflex-magnetics.co.uk

Live hacking at show

IBM's team of "ethical hackers" successfully broke into an unnamed company's computer network in a demonstration of a live attack at a computer industry conference.

IBM's team of hackers, who work at its research division in Yorktown Heights, New York, are paid security professionals who are hired by corporate customers to detect security flaws.

A "large transportation" company, which would not be identified for security reasons, agreed to let IBM try to penetrate its network in a demonstration and discussion of hacking at the PC Forum conference.

The IBM researchers successfully penetrated one of the company's file transfer protocol servers through the root directory and had access to employee telephone numbers, social security numbers, payroll data, and other sensitive information. They broke into three different Unix machines on the network.

"Most people think hacks are random attacks," said Charles Palmer, head of IBM Research's Global Security Analysis Lab. "They are very organised probes."

The IBM team, which has an 80 per cent success rate in electronic break-ins, is not a team of reformed hackers and Palmer warned the audience that hiring former hackers can be very dangerous and not worth the risk.

He said that there are currently about 100,000 hackers worldwide, but about

only 9.99 per cent of those hackers are potential professional hired hackers who may be involved in corporate espionage, and .01 per cent are world-class cyber criminals. Ninety per cent are amateurs who "cyberjoyride."

"There are about 100 people in the world I would not want touching my computer," Palmer said, adding that hack attacks are on the rise.

Tool for analysing data

A new program is claimed to be able to sift through information quickly to find segments, build profiles and discover patterns.

AnswerTree, developed by SPSS Inc, automatically produces a tree diagram from its findings to provide a visual snapshot of patterns.

"With AnswerTree, users can make the most of their data," said SPSS CEO and President Jack Noonan. "No other classification tool has as many tree-based algorithms, enabling users to make more informed decisions and get the best model for their data."

Its makers say AnswerTree is ideal for those who need to identify key groups in their data, such as credit risk scoring, database marketing, institutional research and crime analysis. The program requires Windows 95 or Windows NT 3.51/4.0 and is priced at $995 in the US.

For more information contact SPSS on US 800/525-4980, e-mail pr@spss.com or visit the web site http://www.spss.com

Cyberlaw library covers computers

Those involved in the legal profession can now get access to the latest developments in information technology law with the launch of a new electronic library.

Online information service Lexis-Nexis now covers computer issues, from domain name disputes to electronic commerce tax considerations, as well as US federal and state case law, statutes, and regulations covering computer and Internet issues.

The library also includes a comprehensive collection of computer and technology law reviews and computer news sources key to conducting cyberlaw research, such as the Journal of Law & Technology, The Computer Lawyer and PC World.

Customers can contact Lexis-Nexis for more information on +1 800 543-6862 or visit the Web site at www.lexis-nexis.com.

E-mail screening to boost security

An automated system which screens a firm's incoming and outgoing e-mail for certain words or phrases has been launched.

US firm SRA has developed the Assentor system as a compliance tool to allow brokers to communicate with their clients via e-mail while conforming to regulatory guidelines.

Its makers say that Assentor mimics a human compliance reviewer and checks all e-mail messages at financial firms. Using a linguistics-based natural language pattern matching engine and compliance patterns developed closely with the securities industry, Assentor flags messages that could expose firms to Securities and Exchange Commission violations.

The flagged messages are forwarded to the firm's compliance reviewer for further scrutiny. Assentor also enables the securities industry to comply with requirements set by the SEC regarding archiving of business-related communications.

For more information visit the firm's Web sites at http://www.sra.com or http://www.assentor.com/

Video analysis

A system for examining and analysing video could greatly speed up law enforcement investigations, according to its maker.

Excalibur Technologies has launched its Video Analysis Engine, a software developer's kit that the firm says will transform the way video can be searched.

The company says that using the system, applications can be built that automatically analyse any video content to discover crucial events, such as scene changes, as they occur.

Excalibur claims its new technology is expected to become the de facto standard for analysing video content for event and scene changes, and be used to create video "storyboards" representative of the content.

Available internationally in two versions, Excalibur VAE costs $49.95 per user/developer for the Windows 95/NT Microsoft DirectShow Filter version and $495 for Windows NT Servers; or as the Excalibur VAE C Library Developer's Kit, priced at $249 per developer.

A pre-release version is available to qualified developers in a 60-day free trial on the Excalibur web site.

For more information contact the firm on +44 (0) 1344 893444 or e-mail: infoexcalib.co.uk

First biometric units get certification

The first six biometric devices designed to positively identify humans have been certified reliable for real-world use, the International Computer Security Association.

Participants in a teleconference forecasted an explosion of use in 1998 and predicted the face, voice, and fingerprint recognition devices will quickly become pervasive, now that problems of cost and reliability are largely solved.

"We're here today to announce that biometrics is real," said Dr Peter Tippett, ICSA president. "It is here and now."

He cited fingerprints, voice, face, body odour, and the eye's iris and retinal patterns as examples of identifying properties.

ICSA tested more than 100 products, said Tippett, before certifying six that he said perform as advertised with real humans in real-world environments.

Certifications went to Hi-Key Technologies, Mytec Technologies, National Registry, and SAC Technologies for fingerprint recognition systems. In addition, Intelitrak Technologies was certified for voiceprint recognition and a Miros product was certified as able to recognise faces.

Court reports

NASA e-mail bomb hacker is guilty

A hacker in the US admitted launching an e-mail bomb attack at NASA which devastated network services.

The Alabama-based hacker pleaded guilty in United States District Court for the Northern District of Alabama, to sending damaging transmissions to a NASA electronic-mail server system, in violation of The Computer Fraud and Abuse Act.

The court withheld the identity of the juvenile offender, and ordered him to comply with probationary conditions for 12 months.

An investigation by special agents from the Computer Crimes Division in NASA's Office of Inspector General found that the offender launched an e-mail bomb attack last August 4 consisting of 14,000 e-mail messages across a NASA network against another person using network systems in a commercial domain.

The use of NASA's network bandwidth caused a simultaneous attack against the agency's electronic-mail network server at the Marshall Space Flight Centre in Huntsville, Alabama resulting in a loss of network services, CCD Director Thomas J. Talleur said.

Although the juvenile's attack was intended against another individual, and not directly against NASA, other recent cases were more direct.

Recently, a former Kennedy Space Centre contractor employee pleaded guilty in Federal District Court at Orlando, Florida, to a charge that he used his workstation to hack into the computers of several Orlando businesses.

Shawn Hillis, 26, of Orlando, Florida, a former employee of a NASA contractor Lockheed Martin Corp, used a NASA workstation at the Kennedy Space Centre to gain unauthorised access to a computer network domain at the University of Central Florida in Orlando, and downloaded password files to his NASA workstation.

The unauthorised access was discovered by NASA systems operations employees at Kennedy Space Centre.

As part of the plea agreement, the court ordered Hillis to make restitution to other victims in Florida, including: Time Warner Cable; Full Service Network, formerly of Maitland; Diamond Star Network, Orlando; Internet Access Group, Altamonte Springs; and Junto Net Press, Winter Park, Florida.

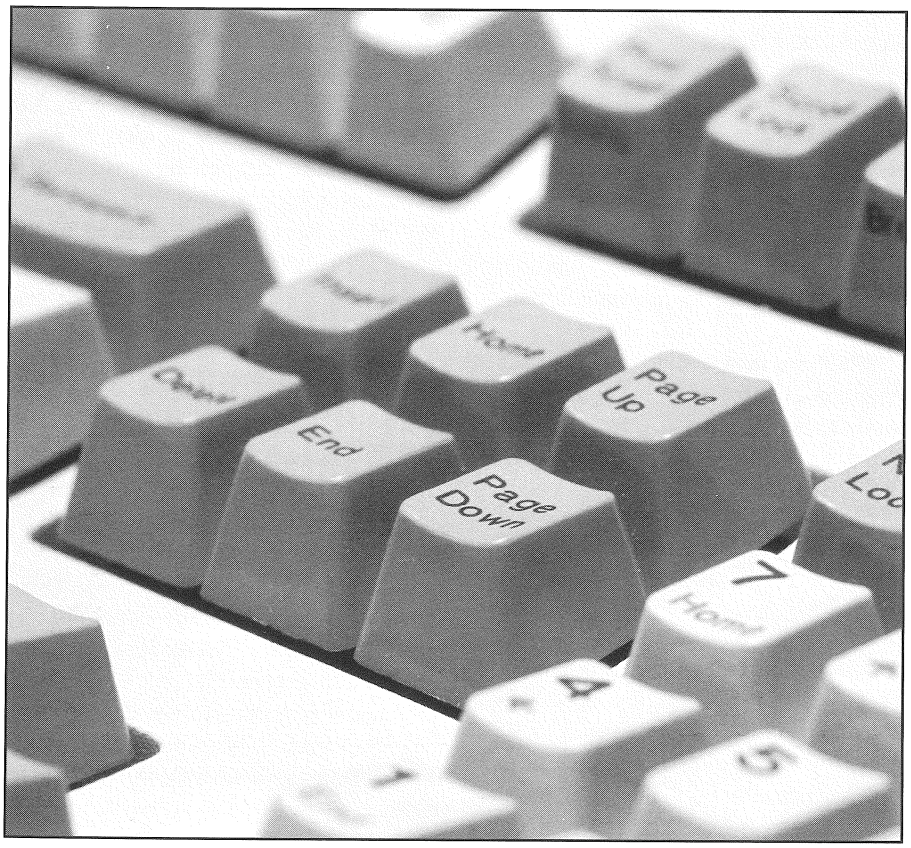
Hillis' case is set for sentencing on July 14.

"Both government and private industry sources cite the Internet, inside offenders, and certain foreign countries as the biggest threats to the national security of the United States," Talleur said. "This is just another example of an inside offender."

Two other inside offenders also recently pleaded guilty to using a NASA computer to download pornographic images from various Internet Web sites during duty hours.

Nicholas Catalano and Jeffery Miller, former employees of the security contractor at Goddard Space Flight Centre, Greenbelt, Maryland, pleaded guilty to a charge of violating NASA regulations in US District Court in Maryland, and were each sentenced to one year probation, 40 and 30 hours of community service, respectively, and a $175 fine.

Talleur cautioned that most computer hackers today fall into more serious categories than the four recent cases NASA successfully prosecuted.



FTC closes Internet auction house scam

A federal judge in the US has stopped an online auction scheme which tried to dupe those who bought goods.

Judge Daniel Hurley issued a temporary restraining order in a case filed against a firm in Lake Worth,

Florida by the US Federal Trade Commission and the company's assets were also frozen.

Craig Lee Hare, also known as Danny Hare, and doing business as Experienced Designed Computers and C&H Computer Services, used online "auction houses" to offer new and used computers for sale, but never delivered the goods to the consumers, the FTC said.

After "successful bidders" paid as much as $1,450 per computer, the FTC

complaint alleged, Hare provided them neither the computer nor a refund.

According to the FTC complaint, Hare offered computers and computer hard drives for sale at auction houses with claims such as "Brand New in their Original Boxes," and "Refurbished, and Carry a one year Warranty from Toshiba."

The FTC alleges that Hare accepted offers from the highest bidders, but failed to provide the promised merchandise or a refund to consumers.

In its complaint, the FTC asked the court to order Hare to provide refunds to consumers who lost their money and to issue an injunction permanently barring Hare from violating the FTC Act and the Mail or Telephone Order Merchandise Rule.

Stephanie Herter, also known as Stephanie Branham, also was named in the FTC complaint as a relief defendant because checks received from consumers were deposited in her account.

The FTC noted that a number of legitimate Internet auction houses "facilitate communications between would-be buyers and sellers."

Sellers list their goods, and auctions are conducted using e-mail to send and receive bids. When the last bid is accepted, the buyer and seller negotiate terms of payment and delivery via e-mail and complete the transaction through US mail.

The FTC's Web site at http://www.ftc.gov has advice on how to avoid falling foul of Internet scams.

Playboy wins millions in copyright test case

A Web publisher in the UK has been told to stop using images belonging to Playboy Enterprises Inc. and hand over more than $3.74 million.

The $3.74 million award, plus attorneys' fees and court costs, was assessed against Five Senses Productions and its owner, Francesco Sanfilippo by a federal judge in the US for the unauthorised use of almost 7,500 Playboy-owned images.

In issuing her order, US District Court Judge Irma Gonzalez ruled that each of the Playboy images had an "independent economic value" and was worthy of protection.

"This judgement is a significant victory in our efforts to combat copyright infringement on the Internet," Michelle Kaiser, intellectual property counsel for Playboy Enterprises, said.

Five Senses' Web site, which went online in May 1996, included thousands of Playboy images scanned from issues of Playboy magazine and its newsstand special issues, Playboy spokesperson Rebecca Theim said.

The site included a free "teaser" page, which advertised the Playboy and other images on Five Senses' paid subscription area.

Theim said that after numerous warnings to remove Playboy's copyrighted images from the site, federal marshals raided Five Senses' San Diego offices and seized computer hard-drives and CD-ROMs containing Playboy images.

The raid on April 15 of last year is believed to have been the first of its kind in the field of Internet copyright law, Theim said.

A week later, Playboy Enterprises and Sanfilippo agreed on a preliminary injunction that prevented Five Senses from using Playboy images until the suit was resolved.

Theim said that the judgement was "a landmark legal victory" for Playboy, which spends millions of dollars annually on photography and design.

"Because of the value associated with our copyrighted images and trademarks, Playboy Enterprises is extremely aggressive in tracking and stopping trademark and copyright infringement on the Web," Theim said.

"Just because people have the ability to post material on the Web doesn't mean it's all right to publish other people's material without authorisation," she said.

The $3.74 million judgement considered to be the largest such award for online copyright and trademark infringement, "is especially notable" from a legal standpoint, Theim said.

She said it treated each use of the 7,475 Playboy images on Five Senses' Web site as an individual copyright infringement, rather than limiting the violations to the number of magazine editions in which the images appeared.

Cyber attacks

Once again, hackers have broken into US defence computers. But this time it could be a lot more serious. Paul Johnson reports.

A group of computer hackers successfully penetrated a US Department of Defence computer network and it claims it stole classified software.

The group, who call themselves the "Masters of Downloading" managed to steal software from the Defence Information System Network (DISN) during their intrusion and may now be offering it to the highest bidder.

The hack took place about six months ago and was centred on the DISN, operated by the Defence Information Systems Agency. During the break in, the group downloaded an application called the Defence Equipment Manager. The software can be used to monitor and control the DISN, the group claimed.

Hacker Web site AntiOnline, (http://www.antionline.com) has published what it says is an interview conducted on Internet Relay Chat with someone claiming to be a member of MOD.

In the interview, the group member says the group targeted the DoD systems because they presented more of a challenge than conventional systems. On how the group cracked the network, the interviewee said, "It was a case of finding weak links in networked environments, using many techniques."

"We wanted to make absolutely sure that the DISA hadn't busted anyone," said the group member on why they were talking now, six months after the original break-in. "The DISA shut down a few of the FTP sites it was stored on days after. I am perfectly sure the coast is clear."

The group says they have examined the DEM and now understand its use. "It was used by the DISA to routinely check and maintain the DISN hardware from a remote location that hardware being routers, multiplexers, IDNX networks, repeaters and GPS satellites and receivers."

The MOD has no plans to use it, the interviewee said, but, "It is always nice to have such power over a network as big and valuable as the DISN."

But the destination for the application and information obtained in the break-in is still in doubt after a second hacker, claiming to be a member of the same group, suggested it might be up for sale. The second interviewee was asked the same question about what the group will do with the data. He replied, "Release it, or sell it."

"I think international terrorist groups would be interested in the data we could gain access to ... governments would buy it for intelligence purposes ... we're not your normal hacker kids," he said.

AntiOnline says it was supplied with a copy of the DEM software, which it tested on a computer disconnected from the Internet. Screenshots from the 18Mb large application are posted on its Web site. The Department of Defence has now admitted that its networks had been breached by hackers, but denied that any classified material had been involved.

Some of the classified software taken is thought to monitor and manage global position system satellites.

And it has also emerged that the same group of hackers may also have compromised networks across Asia.

A person claiming to be a member of the group told Web site AntiOnline that they had scanned computers in Japan and Thailand for security holes

"We have infiltrated many systems based in Eastern Europe and Asia," the member told AntiOnline editor John Vranesevich.

More critically, the spokesman claimed to have targeted China's military networks for future action. "We have already proven our point purely by stealing classified material from the DoD over the Internet.

"We have a lot more pressing projects to undertake now, regarding China and other countries...as they also have defence networks."

Even if the group does attempt to break into Chinese military computers, there is some scepticism as to what they could achieve.

"In China, not a lot of computers that contain sensitive information are connected to the Internet," said Samuel Chanson, director of the Hong Kong University of Science and Technology's Cyberspace Centre.

"The Internet is not very well developed in China, so I don't think the Chinese government is concerned yet."

Chanson added that, while low security made China a potential target, he was unaware of any incidents involving gov-

ernment servers.

A New China News Agency spokesperson said she was aware of the issue, but declined to comment.

A second MoD member told AntiOnline that the group had already begun "major work" in Asia. "We are looking into information warfare exercises against more network-dependent countries, like Singapore and Japan."

Chanson agreed that the region's better-developed states make far more enticing targets for intruders.

"It's very logical that you can only attack those systems that are connected," he said, adding that Japan, Singapore, and Hong Kong would be most susceptible to attacks.

He said that it usually takes a well-publicised security breach before providers begin to take the issue seriously. Online security in Hong Kong was given very low priority until two years ago, when an unemployed graduate was caught having broken into computers around Hong Kong.

Military warn of growing threat

The US is facing a growing threat from cyberspace, Deputy Defence Secretary John Hamre warned after the latest attacks.

"I think everybody has to realise that we are now entering a period where we have to worry about defending the homeland again," Hamre said. "As computers are becoming interconnected, it is possible for people to come in and disrupt our lives through computers."

Last year, and again earlier this year, the Pentagon and other US government agencies experienced such attacks against government sites, including seven US Air Force Web sites and four US Navy sites.

Alluding to the computer penetration, Hamre said that it now is possible "for people from other countries to attack the United States with computer connections."

Recently, the Pentagon announced exercises in which a US national security team secretly attempted to break into government computers to test the system's vulnerability to such attacks.

The virtual war games, codenamed "Eligible Receiver," "succeeded beyond its planners' wildest dreams in elevating the awareness of threats to our computer systems," Pentagon spokesman Ken Bacon said.

The games, held last June, targeted unclassified computers in the Defence Department, including the US Pacific Command in Hawaii.

Bacon said the National Security Agency team also gained access to a US electric power grid.

The DISN Web page is at http://www.disa.mil

A number of Internet service providers and US universities are planning to file civil suits against members of the ViRii computer hacking group, claiming hundreds of thousands of dollars in lost revenues and damage to their systems.

The ViRii group, allegedly headed by Ehud Tenebaum, an Israeli teenager, and Calidan Levi Coffman, 20, of Carson, Washington, has been accused of breaking into US and Israeli government, university and business computers.

The ISPs and universities, including the Massachusetts Institute of Technology and Harvard, and ISP NetDecks, claim Tenebaum and other members of ViRii used their computer networks to gain access to other computer systems.

No charges have yet been filed against Tenebaum, but he has been drafted into the Israeli army.

ViRii "crew members," meanwhile, posted a statement on the Internet at the AntiOnline site saying: "Our activities as a group do not represent dangerous actions against the federal government. Our goals are to learn and enhance our views on computer security. Without us there would be lackluster advances in that field."

"Today's hackers are not juveniles playing games," Thomas Talleur, director of the NASA Computer Crimes Division. "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.

"Computer security problems will get a lot worse before they get better," Talleur said, noting thegrowing sophistication and motives behind hacking.

"Many computer hacking cases now involve individuals in their mid-20s to mid-30s," Talleur said, "and they're involved with a number of fringe groups who either perceive the government as the enemy, or are trying to obtain information to destabilise security."

Gross said the NASA investigation into ViRii started last June,when network security officials at the agency's Jet Propulsion Laboratory in Pasadena, California, detected a problem with anetwork 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.

And FBI Deputy Assistant Director Michael Vatis told the Congressional Joint Economic Committeethat advances in information technology "go well beyond the potential loss to the individual victim," affecting "our national economy and, indeed, our national security."

Vatis, who also is chief of the FBI's recently established National Infrastructure Protection Centre, said that a 1996 Defense Information Systems Agency (DISA) study estimated that as many as 250,000 attacks may have occurred on Defense Department systems in 1995 alone.

Vatis said the "problem is exacerbated by our continued romanticization of hackers as technical whizzes who are really not doing anything wrong but are actually providing a service by pointing out the vulnerabilities in an individual's or a company's or a government agency's system."

"But do we praise a burglar for demonstrating the vulnerability of our home security by breaking in and stealing?" Vatis asked. "Of course not."

Free speech vs online law

Lawmakers in the US want to curb the worst excesses of the medium to protect children and help law enforcement groups. But civil liberties groups say that freedom of speech is paramount. Paul Johnson reports on the moral battle that looks to have no clear winners.

The state of New Mexico in the US has passed a law making it a crime to have online communications about sex, but opposition groups are determined to get it struck off.

Similar laws have already been struck down as unconstitutional in three states and in the US Supreme Court.

New Mexico's law, Senate Bill 127, makes it a crime to disseminate by computer material "harmful to minors," when that material, "in whole or in part, depicts actual or simulated nudity, sexual intercourse, or any other sexual conduct.

The law, which carries penalties of up to one year in jail, a $1,000 fine, or both, was signed by Gov. Gary Johnson and goes into effect July 1.

Following its challenges to similar laws around the country, the American Civil Liberties Union has filed a complaint that says the New Mexico statute affects Internet speakers nationwide, and as a result violates the Commerce Clause, which bars states from regulating activity outside its borders.

The ACLU said it would not challenge the "child luring" portion of the law, which targets paedophiles who use the Internet to "knowingly and intentionally induce a child under 16 years of age" to engage in sexual contact.

According to ACLU national staff attorney Ann Beeson, the law is an unconstitutional content-based restriction on free speech that would reduce adult communication to levels acceptable for a six-year old.

"Taxpayers ought to be furious at their representatives, who continue to pass laws that are clearly unconstitutional," Beeson said.

"Politicians may enjoy jumping on the censorship bandwagon, but their constituents are the ones who will ultimately pay the price for the ride."

New Mexico is the sixth state - the others being Tennessee, Illinois, Rhode Island, Kansas, and Arizona - that have introduced Net laws since January 1. In the last three years, 25 states have considered or passed Net censorship laws.

The ACLU has successfully challenged three state Internet censorship laws in New York, Georgia, and Virginia, as well as the landmark Reno vs ACLU case last June, in which the US Supreme Court struck down parts of the federal Communications Decency Act as unconstitutional.

The New Mexico law is even broader, and more restrictive, than the state and federal statutes that have been found unconstitutional, Beeson said.

As a result, anything from an image of Michelangelo's David to speech about prison rape, abortion, safer sex practices, and other sexually related topics would be criminalized.

"It's sad that the state of New Mexico, known for its wide-ranging free speech traditions and dedication to the arts, has passed a law criminalizing online discussion about safer sex or displays of classic nudes and other artistic images," Jennie Lusk, executive director of the ACLU of New Mexico said.

Beeson said the ACLU is likely to repeat its argument that the Commerce Clause of the US Constitution bars state regulation of the Internet because it is an interstate commerce medium.

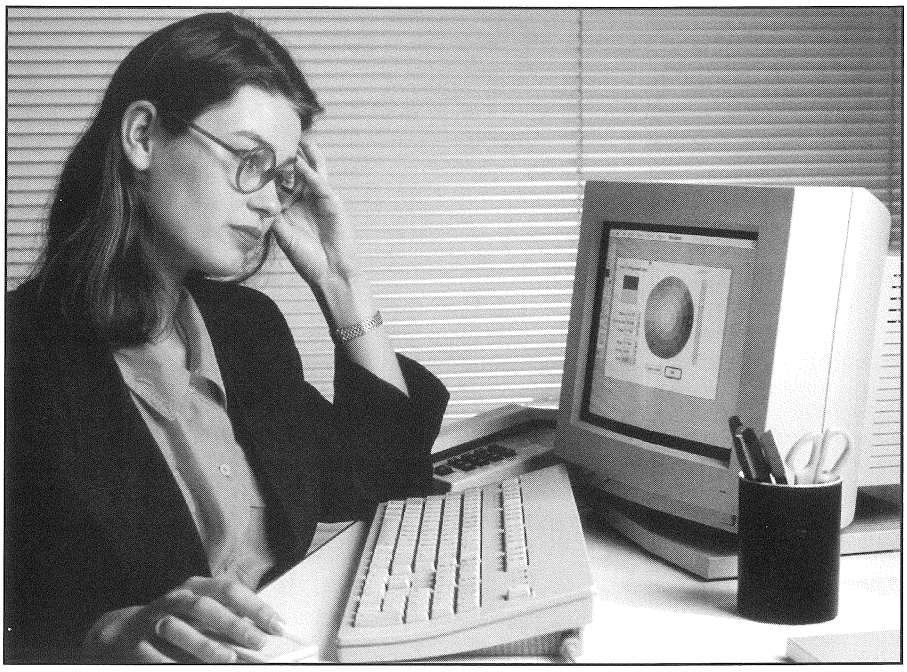
In New York case, American Library Association vs Pataki, Federal District Judge Loretta A. Preska last June blocked New York State from enforcing its version of the federal Communications Decency Act.

Judge Preska issued a preliminary injunction against the New York law, calling the Internet an area of commerce that should be marked off as a "national preserve" protect online speakers from inconsistent laws that could "paralyse development of the Internet altogether."

While "the protection of children from paedophilia is an entirely valid and laudable goal of state legislation, the New York act's attempts to effectuate that goal, however, fall afoul of the (federal) Commerce Clause," Judge Preska wrote in her decision.

Judge Preska's 62-page decision warned of the extreme danger that state regulation would pose to the Internet, rejecting the state's argument that the statute would even be effective in preventing so-called "indecency" from reaching minors. Judge Preska also noted that the state could already protect children through the vigorous enforcement of existing criminal laws.

Lusk said the ACLU is putting together a coalition of plaintiffs who fear prosecution under the new law, and that because of the global nature of the Internet, plaintiffs would not necessarily have to be based in New Mexico.



The 20 plaintiffs named in the suit all feared that the law would prohibit them, at risk of jail or fines, from communicating valuable information on a wide range of topics, including art, literature and health.

In its complaint, the ACLU asserts that the Act "will reduce the adult population in cyberspace to reading and communicating only material that is suitable for young children."

The law will not even accomplish its aim of shielding minors from inappropriate content, the ACLU said, because at least 40 per cent of Internet content originates outside the United States.

Beeson noted that in the last three years, at least 25 states in the US have considered or passed Internet censorship laws. But however popular the laws may seem, they do not hold up well to constitutional scrutiny, she said.

In addition to New York, courts in Georgia and Virginia have found Internet censorship laws unconstitutional in challenges brought by the ACLU.

And in its June 1997 landmark ruling in Reno v. ACLU, the US Supreme Court struck down the federal version of these laws, saying that it placed an "unacceptably heavy burden on protected speech" that "threatens to torch a large segment of the Internet community."

The ACLU also is fighting Internet censorship bills pending in a number of other states, including: California, Illinois, Kansas, Kentucky, Missouri, New York, Ohio, Rhode Island and Tennessee. The laws range from stopping minors from accessing obscene Internet material in libraries and schools to criminalizing sexually explicit conversation with children over the Net. Tennessee's House Bill 3353 holds Internet service providers strictly liable for the dissemination of "obscene material, child pornography, or pornographic materials harmful to youth."

The battle in Virginia

A federal judge in Virginia has decided to allow a trial in a high-profile lawsuit against state libraries that use software to try to block out Internet smut.

In what is the first major ruling on the use of Internet blocking software in public libraries, Judge Leonie Brinkema rejected a government motion to dismiss a lawsuit challenging the use of filtering software in the libraries.

In her 36-page decision, Judge Brinkema of the US District Court for the Eastern District of Virginia said the government "misconstrued the nature of the Internet" and held that the Loudon County Library Board "may not adopt and enforce content-based restrictions on access to protected Internet speech" unless it meets the highest level of constitutional scrutiny.

Calling public libraries places of "freewheeling and independent inquiry," and quoting from the landmark Reno v. American Civil Liberties Union (ACLU) Supreme Court decision on Internet free speech, Judge Brinkema called the Internet a "vast library including millions of readily available and indexed publications, the content of which is as diverse as human thought."

Brinkema also rejected the government's notion that the use of blocking software can be considered similar to a librarian choosing books. Internet publications "exist only in cyberspace," Brinkema, a former librarian said, and do not "take up shelf space or require physical maintenance of any kind."

The ACLU, and the ACLU of Virginia, hailed the ruling as one of the strongest ever defences of online free speech. "We're thrilled that the judge in this case recognised the Internet as the ultimate library resource," Ann Beeson, an ACLU staff attorney who appeared before the court, said.

"Every member of every library board considering an Internet-blocking policy ought to read the judge's ruling," Kent Willis, executive director of the ACLU of Virginia, said." It will remind them of why we have libraries and why an unfettered Internet serves the fundamental purpose of libraries better than any invention since the printing press."

Beeson added that although the case will still go forward, the unequivocal language of the ruling gave the government a very high burden to meet in its defence of the blocking policy.

According to the ACLU, the Loudon County, Virginia, library's Internet policy purports to block access to materials that are "pornographic" or "harmful to juveniles." But the ACLU's complaint charges that by using blocking software to implement the policy, the library board is in fact "removing books from the shelves" of the Internet with value to both adults and minors in violation of the US Constitution.

In objecting to the block on their clients' speech, the ACLU's complaint before the US District Court for the Eastern District of Virginia noted that Web sites offering opposing views are not blocked.

"A library by definition is a place where people have access to all types of information, from photos to essays," Willis said. "Restricting the use of this valuable research tool erodes the whole notion of a library"

In its complaint, the ACLU said that the library's Internet policy purports to block access to materials that are "pornographic" or "harmful to juveniles." But the ACLU's complaint charges that by using blocking software to implement the policy, the library board is in fact "removing books from the shelves" of the Internet with value to both adults and minors in violation of the Constitution.

In objecting to the block on their clients' speech, the ACLU's complaint noted that Web sites offering opposing views are not blocked. "Blocking software is nothing more than CDA (Communications Decency Act) in a box," Beeson said. "With today's ruling, the court correctly applied the same level of First Amendment scrutiny that the Supreme Court used in rejecting the CDA."

Beeson also said that the ruling should serve as a strong deterrent to recent efforts in Congress to mandate the use of blocking software in public schools and libraries.

Whatever the outcome of the legal battle in Virginia, the war between the moralists and the free speech advocates is sure to continue unabated, both in the US and shortly in Europe and elsewhere in the world. It is a fight that leaves the law enforcement groups and prosecuting agencies caught and confused in the struggle and a situation which only case law and judicious legislation can begin to untangle.

Evidence processing steps

Computer evidence - guidelines

Michael Anderson, president of US forensic computing firm New Technologies Inc gives a step by step guide to the procedures and guidelines in retrieving and examining computer evidence. He also gives an overview of some of the firm's products and explains how they can help the investigator or law enforcement officer.

By Michael Anderson

Computer evidence is fragile by its very nature and the problem is compounded with the introduction of destructive programs and hidden data.

Even the normal operation of the computer can destroy computer evidence that might be lurking in unallocated space, file slack or in the Windows swap file.

We work hard to give our students a solid foundation of technical knowledge so that they will understand the technical issues involved and they will make the right decisions. There really are no strict rules that must be followed regarding the processing of computer evidence.

Every case is different, and flexibility on the part of the computer investigator is important. However, in the interest of law enforcement, the following general guidelines have been provided.

Please remember that these do not represent the only true way of processing computer evidence. They are general guidelines provided as food for thought for use by individuals that are trained in computer forensics.

1. Shut down the computer

Depending upon the computer operating system, this usually involves pulling the plug or shutting down a network computer using relevant commands required by the network involved.

At the option of the computer investigator, pictures of the screen image can be taken. However, consideration should be given to possible destructive processes that may be operating in the background.

These can be in memory or available through a connected modem. Depending on the operating system involved, a password protected screen saver may also kick in at any moment.

This can complicate the shutdown of the computer. Generally, time is of the essence and the computer system should be shut down as quickly as possible.

2. Document the hardware configuration of the system

It is assumed that the computer system will be moved to a secure location where a proper chain of custody can be maintained and evidence processing can begin.

Before dismantling the computer, it is important that pictures are taken of the computer from all angles to document the system hardware components and how they are connected.

Labelling each wire is also important so that it can easily be reconnected when the system configuration is restored to its original condition at a secure location.

3. Transport the computer system to a secure location

This may seem basic but all too often seized computers are stored in less than secure locations. We can tell war stories on this one that relate to both law enforcement agencies and corporations.

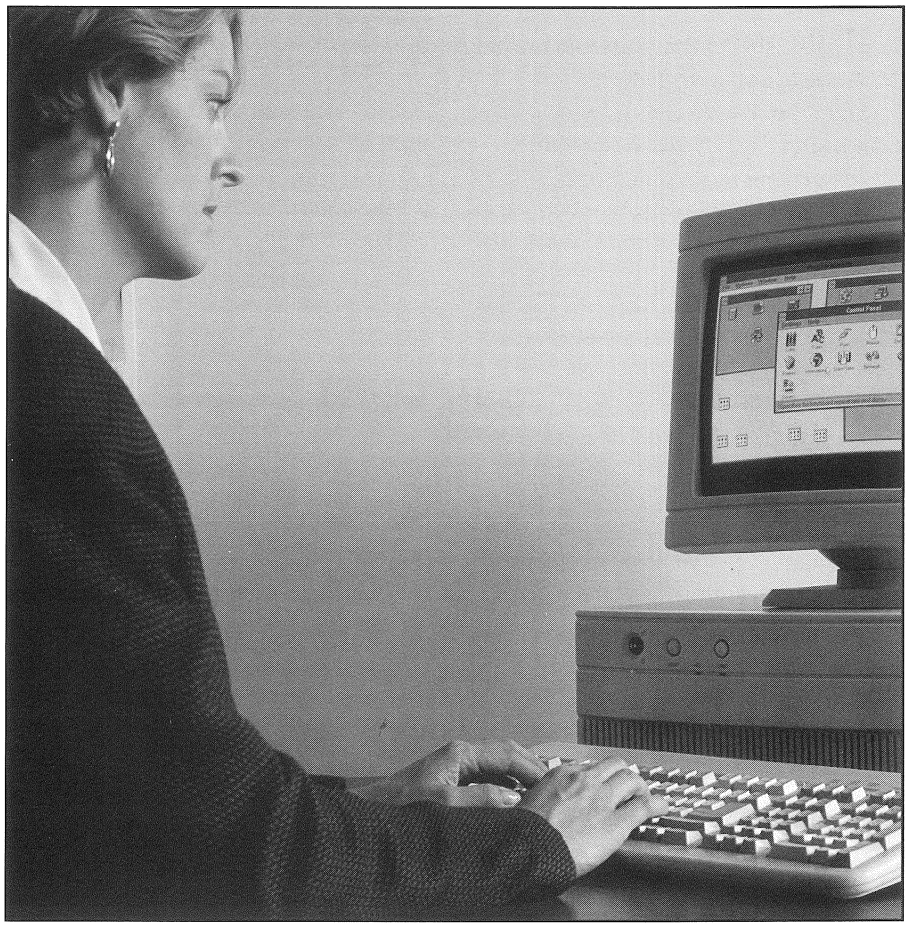
It is imperative that the subject computer is treated as evidence and it should be stored out of reach of curious computer users.

All too often, individuals access seized computers without knowing that they are destroying potential evidence and the chain of custody.

Furthermore, a seized computer left unattended can easily be compromised.

Evidence can be planted on it and crucial evidence can be intentionally destroyed.

A lack of a proper chain of custody can make the day for a savvy defence lawyer. Lacking a proper chain of custody, how can you say that relevant evi-



dence was not planted on the computer after the seizure? The answer is that you cannot. Don't leave the computer unattended unless it is locked up in a secure location!

4. Make bit stream backups of hard disks and floppy disks

The computer should not be operated and computer evidence should not be processed until bit stream backups have been made of all hard disk drives and floppy disks.

All evidence processing should be done on a restored copy of the bit stream backup rather than on the original computer. The original evidence should be left untouched unless compelling circumstances exist.

Preservation of computer evidence is vitally important. It is fragile and it can easily be altered or destroyed.

Often such alteration or destruction of data is irreversible. Bit stream backups are much like an insurance policy and they are essential for any serious computer evidence processing.

5. Mathematically authenticate data on all storage devices

You want to be able to prove that you did not alter any of the evidence after the computer came into your possession. Such proof will help you rebut allegations that you changed or altered the original evidence.

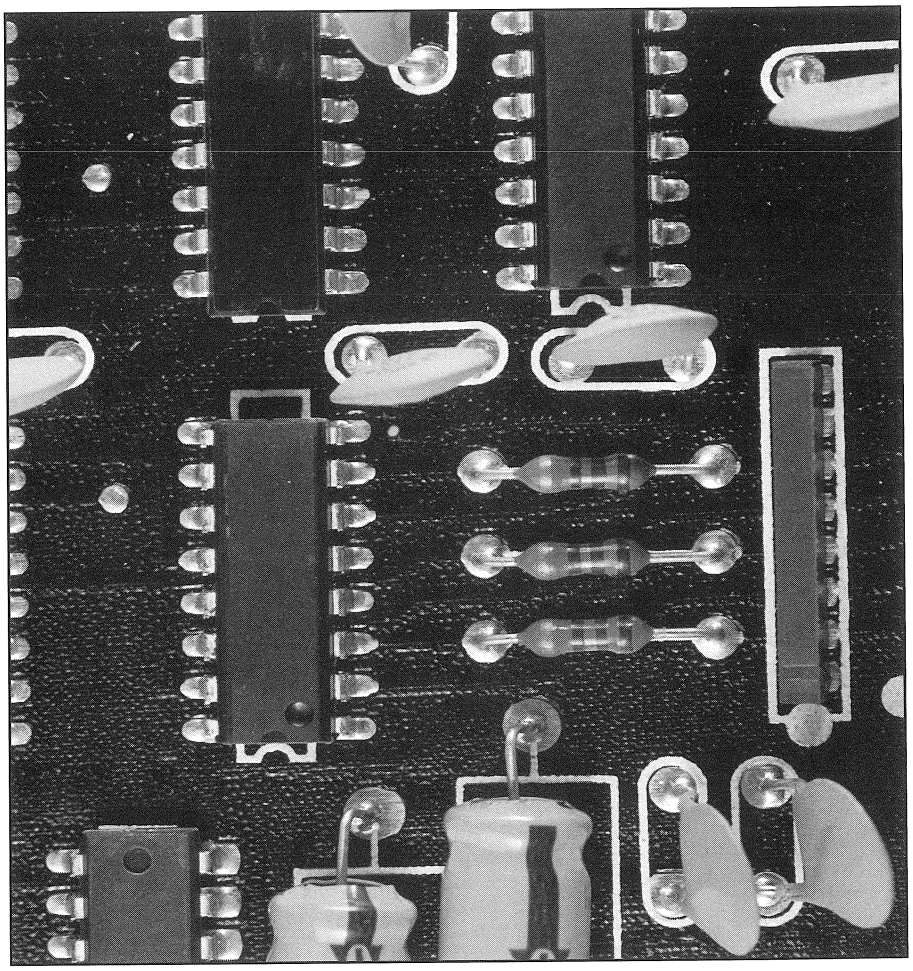
Since 1989, law enforcement and military agencies have used a 32-bit mathematical process to do the authentication process. Mathematically, a 32-bit validation is accurate to approximately one in 4.3 billion.

However, given the speed of today's computers and the vast amount of storage capacity on today's computer hard disk drives, this level of accuracy is no longer accurate enough.

A 32 bit CRC can be compromised. Therefore, NTI includes two programs in its forensic suite of tools that mathematically authenticate data using a 128-bit level of accuracy.

Such a huge number provides a mathematical level of accuracy that is beyond question.

These programs are used to authenticate data at both a physical level and a logical level.



6. Begin to make a list of key words

Because modern hard disk drives are so voluminous, it is all but impossible for a computer specialist to manually view and evaluate every file on a computer hard disk drive.

Therefore, state-of-the-art automated forensic text search tools are needed to help find the relevant evidence.

Usually, some information is known about the allegations, the computer user and the alleged associates that may be involved.

Gathering information from individuals familiar with the case to help compile a list of relevant key words is important. Such key words can be used in the search of all computer hard disk drives and floppy diskettes using automated software.

Keeping the list as short as possible is important and you should avoid using common words or words that make up part of other words. In such cases, the words should be surrounded with spaces.

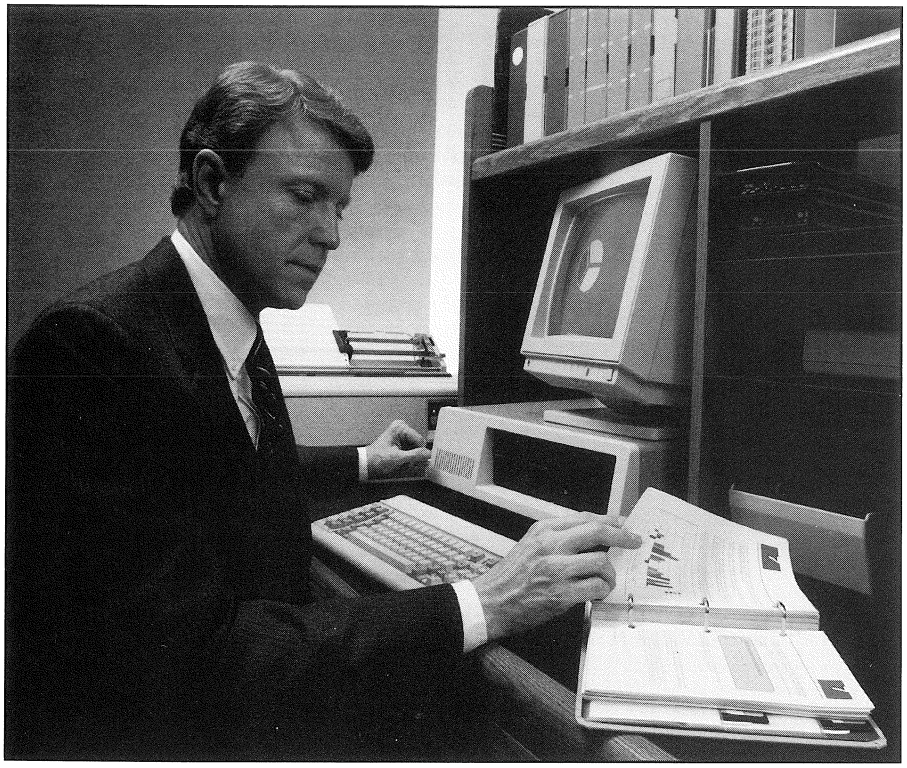
7. Evaluate the Windows swap file

The Windows swap file is potentially a valuable source of evidence and leads. The evaluation of the swap file can be automated with NTI's IPFILTER and/or the FILTER_I forensic tools.

In the past this tedious task was done with hex editors and the process took days to evaluate just one Windows swap file. By using automated tools, that process now takes just a few minutes.

The IPFILTER program relies upon artificial intelligence fuzzy logic to identify patterns of text associated with prior Internet activities. This program is made available to law enforcement agencies free of charge by NTI to aid in the investigation of cases involving the distribution of child pornography and other Internet related cases.

IPFILTER is also sold to corporations and government agencies for use in the



identification of corporate and government Internet account abuses. All too often, corporate Internet accounts are used to download pornography or to transmit corporate trade secrets.

The FILTER_I program is also an NTI program that relies on artificial intelligence fuzzy logic. It automatically identifies patterns of English language text, phone numbers, social security numbers, credit card numbers, network logons and passwords that may have passed through the Windows swap file during a Windows work session.

The output from this program can be used to identify fragments of e-mail or word processing documents that may have been previously erased or never saved to disk at all by the computer user.

The output from both the IPFILTER and FILTER_I programs can be successfully used to identify 'unknown key words' that can supplement the key word list created in step six above.

The automated review of the swap file takes just a few minutes with these automated tools.A manual review can take days or even weeks if the process is done manually using programs like the Norton utilities.

8. Evaluate file slack

File slack is a data storage area that most computer users are unaware of. It is a source of significant 'security leakage' and consists of raw memory dumps that occur during the work session as files are closed.

The data dumped from memory ends up being stored at the end of allocated files, beyond the reach or the view of the computer user. Specialised forensic tools are required to view and evaluate file slack and it can prove to provide a wealth of information and investigative leads.

Like the Windows swap file, this source of ambient data can help provide relevant key words and leads that may have previously been unknown.

On a well-used hard disk drive, as much as 900 million bytes of storage space may be occupied by file slack. File slack should be evaluated for relevant key words to supplement the keywords identified in steps six and seven above. Such keywords should be added to the computer investigator's list of key words for use later.

Because of the nature of file slack, specialised and automated forensic tools are required for evaluation. NTI has created a forensic utility called GETSLACK that captures file slack from hard disk drives and floppy disks.

The output from the GETSLACK program can be evaluated in the same fashion as a Windows swap file using the IPFILTER and FILTER_I programs mentioned previously.

File slack is typically a good source of Internet leads. Tests conducted by NTI suggest that file slack provides approximately 80 times more Internet leads than the Windows swap file.

Therefore, this source of potential leads should not be overlooked in cases involving possible Internet uses or abuses.

9. Evaluate unallocated space (erased files)

The DOS and Windows 'delete' function does not completely erase file names or file content. Many computer users are unaware the storage space associated with such files merely becomes unallocated and available to be overwritten with new files.

Unallocated space is a source of significant 'security leakage' and it potentially contains erased files and file slack associated with the erased files.

Many times the DOS Undelete program can be used to restore the previously erased files. Like the Windows swap file and file slack, this source of ambient data can help provide relevant key words and leads that may have previously been unknown to the computer investigator.

On a well-used hard disk drive, millions of bytes of storage space may contain data associated with previously erased files. Unallocated space should be evaluated for relevant key words to supplement the keywords identified in steps six, seven and eight above.

Such keywords should be added to the computer investigator's list of key words for use in the next processing step. Because of the nature of data contained in unallocated space and its volume, specialised and automated forensic tools are required for evaluation.

NTI has created a forensic utility called GETFREE that quickly captures all unallocated space from hard disk drives and floppy disks. The output from the GETFREE program can be evaluated in the same fashion as the other types of ambient data mentioned previously us-

the GETFREE program can be evaluated in the same fashion as the other types of ambient data mentioned previously using the IPFILTER and FILTER_I programs mentioned previously.

Unallocated space is typically a good source of data that was previously associated with word processing temporary files and other temporary files created by various computer applications.

10. Search files, file slack and unallocated space for key words

The list of relevant key words identified in the previous steps should be used to search all relevant computer hard disk drives and floppy diskettes.

There are several forensic text search utilities available in the marketplace. NTI's utility is called TextSearch Plus and it is included as part of NTI's suite of forensic tools. It was designed to be state-of-the-art and has been validated as a security review tool by one of the federal government intelligence agencies.

This program and several other programs contained in the forensic suite are made available to trained law enforcement computer specialists at a substantial discount.

The entire forensic suite of utilities can be purchased by law enforcement agencies for the price of just a text search program.

It is important to review the output of the text search utility and equally important to document relevant findings. When relevant evidence is identified, the fact should be noted and the identified data should be completely reviewed for additional key words.

When new key words are identified, they should be added to the list and a new search should be conducted using the text search utility.

11. Document file names, dates and times

From an evidence standpoint, file names, creation dates, last modified dates and times can be relevant. Therefore, it is important to catalogue all allocated and 'erased' files.

NTI includes a program called FILELIST in its forensic suite of tools. The FILELIST program generates its output in the form of a database file.

The file can be sorted based on the file name, file size, file content, creation date, last modified date and time.

Such sorted information can provide a time line of computer usage. When FILELIST databases are combined from several computers involved in the same case, the sorted output can provide conspiratorial leads, etc.

NTI also created another forensic documentation tool called NTIDOC. This program is available for free download from NTI's Internet web site and it is used to take electronic snapshots of relevant computer files.

The program automatically records the file name, time and date along with relevant file attributes. The output is in the form of a word processing compatible file that can be used to help document computer evidence issues tied to specific files.

12. Identify file, program and storage anomalies

Encrypted, compressed and graphic files store data in binary format. As a result, text data stored in these file formats cannot be identified by a text search program.

Manual evaluation of these files is required and in the case of encrypted files, much work may be involved. NTI's TextSearch Plus program has built in features that automatically identify the most common compressed and graphic file formats.

The use of this feature will help identify files that require detailed manual evaluation. Depending on the type of file involved, the contents should be viewed and evaluated for its potential as evidence.

Reviewing the partitioning on seized hard disk drives is also important. The potential exists for hidden partitions and/or partitions formatted with other than a DOS compatible operating system.

When this situation exists it is comparable to finding a hidden hard disk drive and volumes of data and potential evidence can be involved. The partitioning can be checked with any number of utilities including the DOS FDISK program or Partition Magic.

When hidden partitions are found, they should be evaluated for evidence and their existence should be documented.

If Windows 95 is involved, it makes sense to evaluate the files contained in the Recycle Bin. The Recycle Bin is the repository of files selected for deletion by the computer user.

The fact that they have been selected for deletion may have some relevance from an evidentiary standpoint. If relevant files are found, the issues involved should be documented thoroughly.

13. Evaluate program functionality

Depending on the application software involved, running programs to learn their purpose may be necessary. NTI's training courses make this point by exposing the students to computer applications that perform more than the anticipated task.

When destructive processes are discovered that are tied to relevant evidence, this can be used to prove wilfulness.

Such destructive processes can be tied to 'hot keys' or the execution of common operating commands tied to the operating system or applications. Before and after comparisons can be made using the FILELIST program and/or mathematical authentication programs.

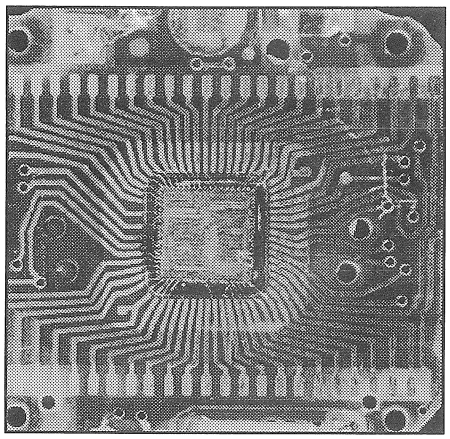
14. Document your findings

As indicated in the preceding steps, it is important to document your findings as issues are identified and as evidence is found. Documenting all of the software used in your forensic evaluation of the evidence including the version numbers of the programs used is also important.

Be sure that you are legally licensed to use the forensic software. Software pirates do not stand up well under the riggers of trial.

When appropriate, mention in your documentation that you are licensed to use the forensic software involved. With NTI's software, a trail of documentation is automatically created for the computer investigator and the name of the licensed user is listed in most output files.

This feature aids in establishing who



did the processing and the exact time and date when the processing was performed. Screen prints of the operating software also help document the version of the software and how it was used to find and/or process the evidence.

As part of your documentation process, we recommend that a copy of the software used be included with the output of the forensic tool involved. Normally this is done on an archive Zip disk, Jazz disk or Syjet disk.

When this documentation methodology is followed, it eliminates confusion at trial time about which version of the software was used to create the output. Often it is necessary to duplicate forensic processing results during or before trial.

Duplication of results can be difficult or impossible to achieve if the software has been upgraded and the original version used was not retained. Please note that there is a high probability that you will encounter this problem because most commercial software is upgraded routinely but it may take years for a case to go to trial.

The author, Michael R Anderson, is the president and primary founder of new Technologies Inc, based in Oregon, US. Mr Anderson's professional background includes 25 years as a Special Agent/Computer Specialist with the Criminal Investigation Division of the Internal Revenue Service.

NTI specialises in the fields of forensic computer science and software development. The firm can be contacted on +1 503 666 6599 or by e-mail to info@forensics-intl.com

Computer Forensic Investigations Limited evidence guidelines

Computer Forensic Investigations Ltd, based in London in the UK, have produced a set of guidelines for securing and investigating evidence.

For assistance in securing or investigating data, contact Mark Taylor at Computer Forensic Investigations Limited on +44 (0)171 353 3777 or e-mail mtaylor@computer-forensic-inv.com

Securing evidence

Do not turn on or attempt to investigate a suspect computer - this could destroy evidence

Identify all computers and storage media that may contain evidence:

- The suspect's desktop or laptop computer
- The suspect's secretary's computer
- The suspect's electronic organiser or palmtop computer
- The server
- Backup tapes
- Voice mail systems
- Floppy disks
- Home computers
- Connected third party computers (e.g. senders and recipients of e-mails or files)

Quarantine the above computers and media

- Do not permit anyone to use the relevant computers
- Disconnect the relevant computers from any network
- Restrict remote access
- Consider the need for court orders to preserve and secure the evidence on third party computers and storage media
- Create evidentially sound copies of the relevant computers and storage media
- Once evidentially sound copies of the computers have been made the computers can go back into circulation

Investigating computer resident data

In order to facilitate the investigation of computer resident data the following facts should be noted:

Hardware

- The type of computer used (e.g. DOS, Mac or Unix based)
- The make and model of the computer (e.g. Toshiba Satellite Pro 430CD laptop)
- The external disk drives in the computer (e.g. 3.5-inch floppy disk or Iomega Zip)
- The capacity of the internal hard disk (e.g. 3.2 GB)
- The current BIOS password
- The way that the computer fits into the network (e.g. linked to server via Ethernet)
- The owner of the computer (e.g. the company, the user etc)

Software

- The operating system (e.g. Windows 95 or Sun Solaris)
- The applications used on the computer (e.g. Microsoft Office Pro)
- Where the applications and user-generated files are stored (e.g. on the server)
- Whether the computer can be run without a network connection
- Any passwords used

The User

- The computer literacy of the user (e.g. highly competent)
- Their knowledge of the situation (e.g. whether they know that they are under suspicion)
- Any other computer to which they have access (e.g. personal laptop)
- Access rights to various parts of any relevant networks (e.g. access only to departmental area on server)
- The existence of a dedicated storage area on the server for the user

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

Financial Frauds on the Internet

Advanced strategies and techniques for preventing on-line frauds

June, Madrid

Contact: D&D Comunication
Tel: 00 39 2 5830 6165
Fax: 00 39 2 5831 5655

IT World Logistics

July 1-2
Excelsior Hotel, Heathrow, Middlesex, UK

Tel: 01494 678000
Fax: 01494 678888

WINDOWS NT security and audit workshop

20-21 August 1998
Bristol, UK

At this workshop delegates will have hands-on access to a Windows NT network; learn everything they need to know about Window NT control systems and security issues; use Windows NT management and auditing facilities; check out the security of Windows NT, stand alone computers, workgroups and domain-based networks. No previous experience of Windows NT is necessary, only a basic knowledge of the Microsoft Windows environment.

Contact: Margaret Mason
System Security Limited

Tel: +44(0)1625 523205
Fax: +44(0)1625 526952

The FCS International Telecommunications Fraud & Crime Conference '98

16-18 September 1988
Queen Mary and Westfield College, London

The conference is specifically designed by the industry for the industry and encourages partnership between law enforcement and the telecoms industry to combat national and international fraud and crime.

Contact: David Harrison
Hospitality Line Limited

Tel: +44(0)181 289 9595
Fax: +44(0)181 289 9696

European Fraud Conference

28-29 September, 1998
Brighton, UK

The organisers state "a fraud case that takes place in Europe has its own special parameters and requirements. This two-day session concentrates on actual cases - from evaluating the initial information to writing the final report, and everything in between.

Contact: Pat Pearce
GartnerGroup

Tel: +44(0)1784 488999
Fax: +44(0)1784 488987

Money Laundering in Banking and Financial Institutions - 3rd edition

October 1988 - venue to be announced

Contact: D&D Comunication

Tel: 00 39 2 5830 6165
Fax: 00 39 2 5831 5655

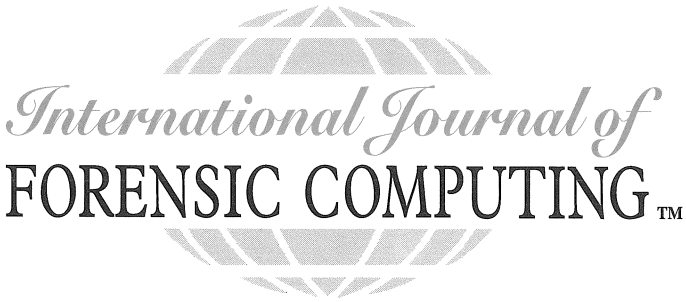
Training

Training in Computer Forensics

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

Contact: Computer Forensics Ltd

Tel: +44(0)1903 823181
Fax: +44(0)1903 233545



Published by
Computer Forensic Services Ltd.