ISSN. 1363-6650

JULY 1998
Issue 19

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

It is only now that we are truly beginning to see the full implications of the computer, and this is no where more true than in the field of crime fighting and law enforcement.

Technology can be used as a tool to commit crime at the click of a mouse, whether it is multi-million pound fraud or Net porn. And by a similar token, computers can contain the vital evidence to secure a conviction – the classic smoking gun brought up to speed.

It's taken a while for police forces across the world to get to grips with the implications. Just a few years ago the concept of computer forensics was just that – a theoretical concept for most people. Now it is a burgeoning industry and computer crime cases are being prosecuted in courts across the globe.

But we've still got a long way to go. While computer crime is being tackled, it is being done in a haphazard and unpredictable way. Just about every law enforcement group has a different way of approaching the subject and the result is that many cases are either lost or hugely compromised.

In the UK, police forces are gradually finding common ground and learning from each other, but there are still many forces in the country which are going their own way, possibly with disastrous consequences. The same story is true for the rest of Europe, which still has a lot of catching up to do, and the US, where the problem of computer crime has been recognised for many years but a comprehensive strategy to tackle it has not been put in place.

That's why the article on page 19 of this month's Journal is so important. It is about the guidelines produced by the UK Association of Chief Police Officers to create a framework for the application of computer forensic skills.

This builds on the conclusions of the G8 international meeting of ministers last year and sets up the parameters for just about all the work done within forensic computing, from evidence retrieval to investigation and prosecution of computer crime.

It is not a "how to do it" guide to computer forensics, nor does it try to be. Instead it is an attempt to create a common set of rules that will hopefully mean an end to embarrassing and costly prosecution failures. Of course, like every science, those involved in forensic computing will learn from their mistakes and put them to constructive use – without setbacks there is no evolution.

But the ACPO document will provide a level playingfield for everyone in the industry, a common set of standards that will hopefully be the cornerstone of tackling computer crime.

Police, law enforcement and government agencies across the world should look closely at the ACPO guidelines to see how it could be incorporated into their own local or national strategy. And the British police would welcome international input in a bid to come up with the best working practises possible.

Computers are not limited to geographical or political boundaries and it's important that crime investigation isn't either. The field of forensic computing will grow at a faster and faster rate, potentially into a ragbag mix of conflicting ideas, methods and laws.

But with development of documents like the ACPO guidelines, politicians and law enforcement groups across the world have a real chance of pooling their resources to become truly effective.

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

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

News

Bid to cut spam

The British government has announced that it is planning a series of tough new laws to clamp down on e-mail and fax spammers.

While e-mail spamming is well known in the online world, a number of UK firms, notably the British Fax Directory, have progressively built up-to-date indexes of virtually all PSTN (public switched telephone service) accessible fax machines in the UK.

These are said to have been built up by the laborious procedure of calling all phone numbers in specific sequences in the UK and letting the line ring out for a few ring cycles. If a fax machine or modem tone answers, the number is logged.

Such calling patterns are, according to Oftel, the government regulator, illegal under current telecoms legislation, but the databases used by these junk fax firms now appears to be complete.

The junk fax firms buy telephone time by the millions of minutes at deep discount rates, with no call minimum, and send out faxes urging recipients to call up its fax servers to receive faxes on topics ranging from repossessed houses going cheap to details of outlets for cut price designer clothing.

The numbers for these services are premium rate, meaning that callers pay up to a £1.50 ($2.50) a minute, and then often receive a fax at just 2,400 bits per second - a quarter of the normal fax speed. Pages often take a minute or more to download.

It is this problem that the legislation aims to resolve. Earlier this year, ECTIS, an Oftel telecommunications watchdog subsidiary, noted in a report that unwanted faxes had overtaken chatlines to become the most common cause for complaints to its helplines.

Now the Department of Trade and Industry has started a consultation period aimed at drawing up means of controlling "cowboys" in the direct marketing industry. The move is being made in advance of a European Commission data directive, which comes into force this coming October.

Although precise details of the DTI initiative are still up in the air, sources close to the DTI suggest that new legislation will make it a criminal offence, punishable by a fine or even imprisonment, to send unwanted faxes, e-mails and phone calls offering goods and services, to businesses and consumers.

Man admits porn

A man admitted possessing pornographic computer pictures of children in the US after prosecutors agreed to drop distribution charges. According to US Attorney Faith S. Hochberg, Eugene Byrnes, from New Jersey, pleaded guilty to one count of possession of child pornography.

The defendant waived the right to have his case presented to a grand jury and pleaded guilty to charges presented by the government, Hochberg said.

In court, Byrnes admitted that in September of 1996 he possessed more than 20 child pornographic computer images on the hard drive of his computer and on at least two computer disks.

Byrnes allegedly used America Online on September 4, 1996, to transport eight child pornographic pictures, and allegedly used AOL to receive a total of 16 child pornographic photographs between September 4 and 17, 1996, according to an earlier indictment.

The earlier indictment also showed that by December 11, 1996, Byrnes possessed more than 180 child pornographic photographs.

Authorities say Byrnes had possessed at least 180 graphic image files containing visual depictions of minors engaging in sexually explicit conduct.

Under the terms of the plea agreement, Hochberg said the government agreed to dismiss the September 12, 1997, six-count indictment returned against Byrnes, charging him with receipt and transportation of the child pornography, in addition to the possession.

Byrnes, a self-employed risk management consultant, faces a maximum of five years in federal prison and a $250,000 fine when he is sentenced on August 31 by US District Judge John C. Lifland. Byrnes currently remains free on an unsecured bond until sentencing.

- Another man from New Jersey in the US has been arrested for allegedly possessing three computer disks containing child pornography.

US Attorney Faith S. Hochberg said that Alfred Ciolino, 43, was arrested by US Customs Service Special Agents and New Jersey Police Department officers on a three-count indictment.

According to the indictment, Ciolino was charged with the possession of three computer disks, one containing five images, another with three images and a third with eight images of child pornography. If convicted, Ciolino faces a maximum of five years in prison and a $250,000 fine on each count.

FTC blasts industry's online privacy efforts

The US Federal Trade Commission has attacked the online industry's efforts to protect consumer privacy through self-regulation.

The Commission's online privacy report, delivered to Congress, found that consumers have little privacy protection on the Internet, with only 14 per cent of commercial Web sites disclosing their information collection practices.

The Commission's survey of over 1,400 Web sites also found that only about two per cent of the sites currently provide a comprehensive privacy policy.

And when it came to children's Web sites, 89 per cent of the 212 children's sites surveyed collect personally identifiable information directly from children, and only 54 per cent of the children's sites disclose their information collection practices.

The Commission said, is that fewer than 10 per cent of the sites directed to children provide for some form of parental control over the collection of information from their youngsters.

The Web site survey "tells us that industry efforts to encourage voluntary adoption of these principles have not met with great success," FTC Chairman Robert Pitofsky said.

Pitofsky said that "more incentives are necessary to encourage self-regulation and to ensure consumers that their personal information will be protected online."

In examining current online industry self-regulatory policies, the Commission concluded that these guidelines generally encourage "members to provide notice of their information practices and some choice...but fail to provide for access and security or for enforcement mechanisms."

The study examined Web sites in six categories, including commercial sites; children's sites; health, retail and financial sites; retail; financial; and "most popular" sites.

Of the commercial sites, the FTC found that, while 92 per cent collect personal information, 89 per cent of the children's sites took information and some 88 per cent of the 404 health, retail and financial sites surveyed collected personal information.

Financial Web sites rank the worst in disclosure statements, the FTC study found, with 97 per cent collecting personal and only 16 per cent disclosing information practices.

Although the online industry has initiated a new set of self-regulatory guidelines regarding online privacy, the Commission's report recommends legislation, particularly in the area of children's online privacy "that would place parents in control of the online collection and use of personal identifying information from their children," Pitofsky said.

"To date we are not satisfied with the implementation of fair information practices by the online industry," he said.

● If the private sector won't ensure consumers their privacy is protected online, then the federal government will step in and try, Commerce Secretary William M. Daley warned.

Daley, opening a two-day online privacy summit in the US, challenged the private sector to "implement enforceable privacy protections to ensure that consumers can feel confident that their personal information is safe online.

"Articulating principles isn't adequate," he said, warning that "there has to be some meaningful consequences to companies that don't comply."

He added: "I sincerely hope industry steps up to the plate first," Daley said. "But if it doesn't, we will have to consider all the options we have for protecting the American consumer."

The Clinton administration is closely examining a private sector proposal to protect privacy in business transactions on the Internet, Daley said, but noted that "industry must move swiftly to draft an effective plan to enforce privacy or face inevitable government regulation of electronic commerce."

Daley told the summit his first impressions of a proposal by the Online Privacy Alliance, a group of 50 companies and business associations to self-regulate online privacy was positive, but expressed disappointment over the group's request for additional time until September 15 to come up with a proposal to enforce privacy on the Internet.

"There has to be a way to enforce this that the consumer can trust, or this won't work." Daley said public concern over Internet privacy is so high that government will "have no choice" but to intervene unless industry "puts its teeth" in its self-regulatory plan.

Online industry bets on gambling

Internet companies and organisations fear a US bill designed to curb online gambling will make criminals out of them overnight.

The bill, S 474, is otherwise known as the Online Gambling Prohibition Act. The legislation, introduced by Sen. John Kyl (R-Arizona), seeks to ban Internet gambling, and would let federal, state and local officials halt telephone and Net service to computer gambling concerns.

The Online Gambling Prohibition Act also provides for criminal penalties for violations, including fines up to $2,500 and a maximum of six months in jail, and would allow the president to seek agreements with foreign governments to allow US law enforcement officials to prosecute operators of offshore gambling concerns that enter the US through the Internet.

The online industry, however, is lobbying that the bill would make every Internet service provider, every online service and every telephone company criminally liable for "knowingly" transmitting gambling information.

The bill would also subject ISPs and online services to court actions that would require them to engage in the virtually impossible task of trying to monitor, identify and block access to Web sites overseas, members of the International Internet Gaming Association said.

But Kyl said: "The law must keep pace with technology," he said. "Gambling is either heavily regulated or expressly prohibited in the states. In the Internet, it is neither."

Kyl, chairman of the technology, terrorism and government information subcommittee of the Senate Judiciary Committee, added that "given the tremendous potential for abuse, addiction and access by minors, online gambling should be prohibited."

Kyl's bill would amend sections 1081 and 1084 of title 18 of the US Code to outlaw gambling on the Internet. The bill also would require the US Attorney General to report on the extent of computer gambling and the problems associated with enforcing laws against it.

"My bill will protect children from logging on to the family computer, borrowing the family credit card, and losing the family home, all before their parents get home from work," Kyl said.

The Internet Gambling Prohibition Act "dispels any ambiguity by making it clear that all online betting, including sports betting, is illegal," Kyl said. He noted that non-sports online betting currently is being interpreted as legal.

The bill also would make gambling on the Internet or other interstate computer networks a criminal offence, and would provide a mechanism for law enforcement to stop illegal gambling. And it also makes it clear that Internet access providers are covered by the pending legislation.

But in a letter to the Senate Judiciary Committee's ranking Democrat, Sen. Patrick Leahy (Vt.), Acting Assistant Attorney General I. Anthony Sutin said the legislation would not only be unenforceable, it would adversely affect the way people look at and conduct business on the Internet.

In his letter, Sutin expressed serious reservations about the bill's attempt to criminalize office pools, fantasy sports games, and "casual" bets conducted using e-mail or the Internet.

Because the National Gambling Impact Study Commission is reviewing the issue of Internet gambling, Sutin suggested that Congress wait for the NGISC report before further work on the bill.

Hong Kong looks at gambling firm

An online sports betting service targeting Chinese gamblers has come under scrutiny of Hong Kong Police.

The Easybets service, based in the Dominican Republic, went online last September and has just launched its Chinese language interface.

Following a series of high-profile raids on illegal gambling operations in the territory, the Hong Kong Police have stated they are "looking into" the Easybets service.

Principal information officer, Li Sung-ming said although Hong Kong legislation did not address Internet gambling, any bet that was not specifically sanctioned by law was illegal. "We are targeting the act itself rather than the means," he said.

"The Internet is just like a telephone. You place a bet by electronic means. It is no different than if you use a telephone to call a bookmaker to place a bet."

Easybets spokesman Robby Ho said that the online gambling trade was not prohibited in Hong Kong, "We're not an illegal company. If we were an illegal company, we wouldn't be here. At this moment, we don't have any area that's against the law, because we're a licensed company, we hold a license that says we can accept bets. Our bookie is licensed to accept bets anywhere in the world."

However, according to the Hong Kong Police, the issue is almost certainly illegal although a case precedent is yet to be established. "In Hong Kong some kinds of betting are legal, just like betting on the horse races," Li said.

"Apart from these legal gambling activities, all gambling is illegal in Hong Kong. So betting on the Internet is illegal in Hong Kong."

Because of uncertainty over its legal status, Easybets has no plans to market the service in China, but will concentrate instead on Hong Kong, Singapore and Taiwan.

Easybets was set up as an online companion to a small chain of Dublin-based bookmakers called PM Racing. The company, which was founded in 1972, is now owned by Hong Kong interests.

It claims to have around 2,000 active customers, around 30 per cent of who are based in the Asia-Pacific region.

The average wager is around US$200 to $500, with minimum bets of $10; a big contrast to the US 30 cents that some Irish punters would bet in PM Racing. Ho said that on a good day the site takes around $410,000 in soccer bets, with $245,000 on basketball, though this includes telebets.

High-tech leaders ask for looser encryption

The Clinton Administration's current encryption policy is killing the US software industry in the international markets, and proposals to introduce key escrow policies would cost billions, high-tech executives said today.

The White House's encryption policy "is turning out to be a real crisis," Novell Inc. chairman Eric Schmidt said at a Business Software Alliance conference. "It's killing the American industry."

The US government today restricts companies from exporting encryption technology above a 40-bit key length without meeting some special conditions.

Over the next two-year period, US companies will be allowed to export up to a 56-bit key length if certain conditions are met related to investments and plans to incorporate key recovery technology into future products.

At the end of the two-year period, US export controls are scheduled to revert back to a maximum 40-bit key length - without going through a formal approval process for individual licenses, as is the situation today.

Citing two studies released today on electronic commerce and encryption, the high tech execs, including Schmidt, Adobe Systems Inc. chairman and chief executive officer John Warnock and Microsoft Chairman and CEO Bill Gates said that business-to-business Internet commerce for the year 2000 is estimated in the $66 billion to $171 billion range.

By 2002, electronic commerce is expected to reach $300 billion, the electronic commerce study said.

The second study on the cost of key escrow encryption showed that the total direct cost of the "back-door" system of gaining access to consumers' encrypted computer files envisioned by the White House will cost at least $7.7 billion per year and $38.5 billion over five years.

"As we've said in the past, encryption policy must be guided by the digital Hippocratic Oath — first, do no harm," Schmidt said. "The high cost of the key escrow system documented in this study does not pass this test."

And US software companies have a lot to lose, according to the first report, "E-Commerce: Policy Principles Developed by Members of the BSA on Critical Issues Facing the Future of Electronic Commerce."

According to the e-commerce report, traffic on the Internet doubles every 100 days, with some 8.2 per cent of the US economy already devoted to Internet technology.

The study also found that advertising spending on the Internet reached $1 billion in 1997, triple the amount spent in 1996, and that by the year 2000, at least 46 million Americans will purchase products or services online, spending an average of $350 per person per year.

According to the study, "The Cost of Government-Driven Key Escrow Encryption," conducted by Nathan Associates, the cost for users to comply with such a key escrow system is at least $1.7 billion per year, while payments that users would have to make to escrow agents to comply with this system is $6 billion per year.

The high tech execs met with Attorney General Janet Reno and FBI Director Louis Freeh to discuss the impact of key escrow on the industry and the US economy. Both Reno and Freeh want the back door keys to encryption programs to assist law enforcement.

But "encryption with a back door is widely available," Microsoft's Gates said. "That's a change in the world of spying and law enforcement that we cannot affect. "Having all of us deliver breakable encryption isn't going to change that."

The bill, "Encryption Promotes the Rights of Individuals in the Virtual Arena Using Computers (E-PRIVACY) Act," would allow US companies to export products with strong encryption without key-recovery requirements, provided that a competing fore gn product is already or imminently available.

The bill also provides for a National Electronic Technologies Centre, which would assist law enforcement at all levels with expertise in encryption technology. The bill subjects all encryption products to a technical review of their capabilities prior to export.

While the bill prohibits the mandatory escrow of decryption keys, it allows law enforcement access to decryption keys under existing wiretap authority and allows them to obtain keys or third-party assistance for remotely stored data with a court order or subpoena.

US computers still being attacked

More than a half dozen serious attacks on the US government's computer networks have occurred in the past five months, according to the head of the FBI's National Information Protection Centre.

And NIPC head Michael Vatis warned that that more attacks are on the way. Testifying before the US Senate Judiciary Committee's subcommittee on technology, terrorism and government information, Vatis said that "somewhere in the vicinity of a half dozen of what I would consider substantial" attacks were launched against US government computer networks since February."

Vatis declined to give specifics on the attacks, telling the hearing that investigations into the attacks were under way. But Vatis did acknowledged that Defence Department computer systems were always a prime target.

Attempted intrusions into Defence Department computers make up "a good percentage of the incidents we see," Vatis said, because the Defence Department "is such a prime target for even individual hackers who want to test their skills."

"They see the Department of Defence as the big banana," he said, "the ultimate challenge to test their skills."

Vatis' testimony before the Senate subcommittee came less than a week after Stanford University reported that its Stanford Linear Accelerator Centre research laboratory was attacked.

The lab, which runs under a Department of Energy contract, had to stop outside access to prevent further intrusions, according to a newspaper report.

The paper reported that more than 30 of the centre's file servers were accessed illegally, and could have been used as jumping off points to other government and research centre networks.

The MilW0rm and other groups also continued their forays into India's computer networks. **(See page 15)**. One group, which calls itself Armageddon, claims to have gained access to an Indian biomedical research facility.

The group says it has accessed and retrieved test results and internal memos on the effects India's recent nuclear tests have had on India's environment and civilian population.

The group claims to have broken into the facility's servers on June 5, a claim that is just now going public, AntiOnline founder John Vranesevich said.

"The hackers apparently used crit1.univ-montp2.fr as a bounce point to hack the Indian server bioinfo.ernet.in among others," Vranesevich said.

Although the facility denied the group's claims of accessing the facility's servers, an e-mail message retrieved by Armageddon from a Prof. A.S. Kolaskar, director of the Bioinformatics Centre, saying that "our Web page was tampered by using your machinie (sic) crit1.univ-montp2.fr," appears to support Armageddon's claims.

"They have logged in as `root' into our machine and changed the files," the e-mail said. "The hackers have played with our log files. We lost information from 3rd June to 6th June."

"It amazes me that this organisation would flat out deny being hacked," Vranesevich said. The letter, he said, was "sent from the Director of the Bioinformatics Centre to the administrator of one of the computers that the hackers used as a jump point. I think this clearly shows that yes, they were indeed hacked."

Washington anti spam law kicks in

Washington State's new anti-spam law is now up and running, although it is still at the centre of controversy.

The law forbids the transmission of certain types of junk e-mail from computers in Washington or to e-mail accounts held by Washington State residents. Many characterise the law as a "truth in spamming" law, because e-mail that does not contain forged header information or misleading subject lines, or has not used a mail server without permission, are not forbidden.

Each message that violates the law entitles minimum damages of $500 to individuals and $1,000 to Internet service providers. The law also allows the Attorney General's Office to take legal action.

Generating more controversy and confusion from the law is not the "truth in spamming" aspect, but the issue of how spammers know an e-mail address is held by a Washington State resident.

The law states, "For purposes of this section, a person, corporation, partnership, or association knows that the intended recipient of a commercial electronic mail message is a Washington resident if that information is available, upon request, from the registrant of the Internet domain name contained in the recipient's electronic mail address."

Some Internet service providers, such as America Online and IBM.NET, have stated they will not respond to such requests, potentially leaving many Washington State residents without the protection of the law.

Attorney David H. Kramer, of Silicon Valley's largest law firm, Wilson Sonsini Goodrich & Rosati said: "The portion of the statute dealing with information being available from the domain name registrant is not exclusive. It merely provides one sure fire way of establishing the spammers knowledge."

Nevertheless, anticipating a problem over this section of the law, the Attorney General of Washington State entered into an agreement with the Washington Association of Internet Service Providers for the WAISP to create an e-mail registry for Washington State residents.

The registry allows Washington residents to add their e-mail addresses to the registry. Would-be spammers can check one address at a time to determine if an address is held by a Washington State resident.

The registry, for use by any Washington State resident with an e-mail address, is at http://registry.waisp.org. The e-mail addresses can only be released to the Attorney General or any other party by court order.

The Attorney General's Office has set up a Web site specifically about the new law, including information on ways to submit complaints electronically.

The site is at http://www.wa.gov/wwweb/AGO/junkemail. The Washington anti-spam law can be found on the Web at http://leginfo.leg.wa.gov/pub/billinfo/house/2750-2774/2752-s_sl_032798

Blue Ribbon for online freedom

The Electronic Frontier Foundation in the US has announced that it is re-launching its Blue Ribbon Campaign for Online Freedom of Expression. It says the move is in opposition to new Congressional attempts to impose censorship controls on the Internet.

The original campaign in 1995 raised awareness of and opposition to the Communications Decency Act (CDA), which was eventually ruled unconstitutional by a unanimous Supreme Court decision.

"When the U.S. Supreme Court struck down the CDA exactly one year ago this month and declared that speech on the Internet is entitled to the highest Constitutional protection, we had hoped that Congress would have given up on its foolish crusade to restrict protected speech on the Internet," said EFF President Barry Steinhardt.

"Sadly, we were mistaken and the struggle isn't over yet. The Blue Ribbon campaign is just as urgent today as it was a year ago."

For more information visit the Web site at http://www.eff.org/blueribbon.

US law tackles Net paedophiles

The US Congress is taking a tough route to ensure the safety of children from sexual predators.

By a unanimous vote, the House passed H.R. 3494, the Child Protection and Sexual Predator Punishment Act of 1998. The bill, which has the support of the Clinton Administration, now moves to the Senate.

The bill would amend the federal criminal code to subject to a fine and five years' imprisonment anyone who knowingly contacts, or attempts to contact, an individual under the age of 18 for purposes of engaging in criminal sexual activity, or who knowingly transfers obscene matter to such an individual.

The bill also sets a three-year minimum term of imprisonment for enticing or coercing within US jurisdiction, or for using a computer or any facility of interstate or foreign commerce to entice or coerce, any individual under age 18 to engage in prostitution or a criminal sexual act, and doubles penalties for abusive sexual contact where the victim is under the age of 12.

"The technology of computers and the Internet have got ahead of the law," co-sponsor Rep. Tony Hall (D-Ohio) said. "This bill is an attempt to catch up."

The legislation, which is expected to pass the Senate by the same margin, would require mandatory life prison sentences for serial rapists, and a minimum of a life sentence for a person convicted of a sexual offence that causes the death of a person under age 14.

- New York State Attorney General Dennis Vacco's "Operation Rip Cord" nabbed another three men, this time from Long Island, for distributing child pornography on the Internet.

The three men, Joseph Greco, 44, of Great Neck, Irving Winick, 51, of Roslyn Heights and Curtis Elder, 38, of Westbury were charged with transmitting pictures of young girls engaged in sexual acts.

"These arrests should be taken as a loud and clear signal that I have zero tolerance for the dissemination of vile child pornography and that I will seek jail time for those snared by Operation Rip Cord," Vacco said.

"Children are being raped and molested in order to produce this smut, which is then zapped into our homes with the click of a mouse," he said.

Irish phone card fraud arrests

Police in Ireland arrested eight people after investigating the country's biggest ever telecommunications fraud.

The phone fraud against Telecom Eireann resulted in the arrest of six men and two women while 14 premises were raided in the Dublin area.

The raids were the biggest of their type in Ireland and involved 38 officers from the Garda (police) Bureau of Fraud Investigation.

The fraud is alleged to have centred around the use of cloned Telecom Eireann phone cards, which were used from payphones to call premium rate phone lines, which cost 150 Irish pence ($2.20) a minute to call.

After deductions, the premium rate phone line operator gets slightly more than 60 per cent of the proceeds from the call. The fraudsters using the cloned phone cards may have been in league with the operators of the premium rate lines, meaning they were effectively being paid for revenue that Telecom Eireann was not collecting.

According to Telecom Eireann, its monitoring system picked up on the potential for a fraud when lengthy duration calls were spotted going to the three premium rate lines in question.

Unfortunately for the former state telecommunications firm, around

100,000 punts ($150,000) was paid into the bank accounts of the premium rate line operators before the cloned cards were traced.

The premium rate lines apparently offered computer problem assistance to callers and requested that a PIN was entered. Because the lines were not advertised anywhere, and the fact that callers actually ended up listening to a silent line - only talking down the line from the payphone when someone else wanted to use the phone - it is thought that the bulk of the call revenue originated from the clonec cards.

Cyber warfare threat

Potential enemies of the US are working on ways to disrupt the nation's cyber networks, CIA Director George Tenet warned Congress.

"These countries recognise that cyber attacks against civilian computer systems in the United States represent the kind of asymmetric option they will need to `level the playing field' during an armed crisis against the United States," Tenet told a US Senate Governmental Affairs Committee hearing here.

"We know with specificity of several nations that are working on developing an information warfare capability," he said. Although Tenet declined to name any countries, Committee Chairman Fred Thompson (R-Tenn.) cited China, Russia, Libya, Iran and Iraq by name, and alluded to at least seven other countries developing information warfare strategies.

"We cannot wait for an electronic Pearl Harbour or Oklahoma City to recognise there is a problem," Thompson said. "At risk are the systems that control the nation's national security, air traffic, finances, power and communications."

Thompson added that "while most Americans know about the benefits of computers, they may not be aware of the darker side of the information age that could leave us vulnerable to attack."

US Air Force Lt. Gen. and National Security Agency (NSA) head Kenneth Minihan agreed with Thompson's warning of an "electronic Pearl Harbour," telling the hearing that attacks on US computer networks were happening "every day."

"We are only seeing the tip of the iceberg," Minihan told the hearing. "Even when attacks are detected and reported, we rarely know who the attacker was."

According to Tenet, attacks on US computer networks would include "our electric power grids and our telecommunications networks" as "targets of the first order."

"An adversary capable of implanting the right virus or accessing the right terminal can cause massive damage," Tenet said.

Such adversaries could include foreign intelligence and military organisations, terrorists and guerrilla groups, criminals, industrial competitors, hackers and disgruntled employees, he said.

"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," Tom Talleur, director of NASA's Computer Crimes Division said.

"Today's hackers are not juveniles playing games," Talleur said. "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 the growing sophistication, age and motives behind hacking, accurately known as "cracking."

"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 government security."

Virus causes red faces

A new virus has been identified which can send copies of the victim's Word documents to dozens of different Usenet newsgroups.

Antivirus and security software firm Data Fellows has warned that the macro virus tricks Net users into reading it by using subject lines like "New Virus Alert!," "Important Princess Diana Info" and "How to find child pornography."

The bug is formally designated the WM/PolyPoster virus, for Word Macro/ Polyposter. When it posts, the messages look like they came from a machine's real user and include the user's real name and signature, says Data Fellows.

To work, the virus, activated by opening a MS Word DOC file, must find a copy of the popular Forte Agent newsgroup reader program and there must be an active Internet connection.

Data Fellow's manager of antivirus research Mikko Hermanni Hypponen said that Word versions 6.0 through Word 97 are vulnerable to the bug and that there was no real way for users to tell if their copy of Word is infected.

Hypponen said that antivirus program F-Prot, developed by Forte and Data Fellows, would tackle the problem and the program is available on the Web at http://www.DataFellows.com

Hypponen said the virus was only discovered recently and that he does not know whether it is widespread yet. The virus infects all documents it posts so users who view them in Word also get infected. This allows the virus to spread.

Some Newsgroups where it posts attract thousands of users while others are more specialised. The bug's internal list includes several groups with erotic material, others aimed at both traditional hackers and crackers.

The documents go out as message attachments because Word uses binary formatting codes. In the body of the message, the virus sends "JZ/Ntrag ol Ybeq Angnf," identified by Data Fellows as a ROT-13 system encryption of the plain text, "WM/Agent by Lord Natas."

Hypponen says traditional security methods like firewalls and Windows NT security settings do not evade this kind of virus, which Data Fellows considers to be a completely new type.

"Viruses like WM/PolyPoster will arrive to users through normal e-mail document attachments, and will further spread from the company's network with e-mail or standard Usenet newsgroup postings. Most firewalls won't prevent this from happening."

postings. Most firewalls won't prevent this from happening."

He added: "This is something we've been expecting for quite some time. Viruses which activate by simply deleting data are easy to recover from by using back-ups. However, there is no way to recover from an incident where a virus posts confidential documents publicly to the Internet."

More information on Data Fellows is on the Web at http://www.DataFellows.com, which information specific to the WM/PolyPoster virus is in the site at http://www.DataFellows.com/v-descs/agent.htm

Spam undermines e-commerce

The problems of junk e-mail and online fraud could undermine consumer confidence and slow the growth of Internet commerce, according to the Federal Trade Commission.

FTC Commissioner Sheila F. Anthony, testifying before the US Senate Commerce, Science and Transportation Committee's communications subcommittee, spoke of the dangers.

She said that, while the Commission "steadfastly called for self-regulation as the most desirable approach to Internet governance...for problems involving deception and fraud, however, the Commission is committed to law enforcement as a necessary response."

Subcommittee chairman Sen. Conrad Burns (R-Mont.) called spam "a threat to computer networks across the nation". "Spamming is truly the scourge of the Information Age," he said.

While not all unsolicited commercial e-mail is fraudulent, Anthony said the "Internet's capacity to reach literally millions of consumers quickly and at a low cost through UCE has been seized on by fraud operators, who are often among the first and most effective at exploiting any technological innovation.

"UCE has become the fraud artist's calling card on the Internet," she said.

Of over 100,000 pieces of UCE the FTC staff has reviewed, Anthony said, "much of it contains false information about the sender, misleading subject lines, and extravagant earnings or performance claims about goods and services. These types of claims are the stock in trade of fraudulent schemes."

Although most bulk UCE burdens Internet service providers and frustrates recipients, Anthony said the FTC's main concern with UCE "is its widespread use to disseminate false and misleading claims about products and services offered for sale on the Internet.

"The Commission believes the proliferation of deceptive bulk UCE on the Internet poses a threat to consumer confidence in online commerce," Anthony said. He added that the FTC earlier this year worked with the United States Postal Inspection Service, putting more than 1,000 junk e-mailers on notice that the agencies are monitoring and keeping track of unsolicited e-mail for fraudulent schemes.

Eileen Harrington associate director of the FTC's Bureau of Consumer Protection, said the Commission has brought more than 35 federal law enforcement actions to stop fraud and deception on the Internet, most involving "old-fashioned scams".

As part of its weaponry to combat online fraud, Harrington said the FTC recently launched Consumer Sentinel, the first bi-national, multi-state computerised consumer fraud database that uses the Internet to provide secure access to consumer complaints for over 150 law enforcement organisations across the US and Canada.

Consumer Sentinel contains over 110,000 complaints, including 23,000 complaints added just since March 1998, concerning telemarketing and direct mail problems, as well as Internet fraud, Harrington said.

The FTC also maintains an e-mail box at uce@ftc.gov which receives more than 1,500 e-mails a day where consumers can forward unsolicited commercial e-mail they believe may be fraudulent or deceptive, she said.

The FTC recently published three new consumer publications about unsolicited commercial e-mail, online fraud scams and safe Net browsing. These are available from the FTC Website at http://www.ftc.gov

New name for Net lobby

The Internet trade and lobby group Interactive Services Association has been renamed the Internet Alliance.

"This name change reflects our evolution towards building an alliance of innovators, political and industry leaders," ISA Executive Director Jeff Richards said. "We're advancing our mandate to undertake the public policy, advocacy and leadership tasks that shape the industry landscape."

Richards said the association's membership, consisting of about 85 per cent of the consumer-focused online services industry, including America Online, AT&T, Bell Atlantic, IBM, Microsoft, Netcom, Netscape and Prodigy, will speak for the industry in such areas as online privacy, unwanted e-mail, taxation, encryption, content regulation, children's marketing online, Internet security, fraud and law enforcement.

"The emergence of the Internet Alliance signifies that the fastest growing industry on the globe is poised to act upon its promises and obligations to policy makers and constituents," ISA Chairman Bill Burrington said.

Censorship law put on hold for talks

A federal judge in the US has granted a civil liberties group a preliminary injunction against a New Mexico Internet censorship law.

The law, Senate Bill 127, was signed by New Mexico Gov. Gary Johnson on March 9, and would have gone into effect July 1. It carries penalties of up to one year in jail, a $1,000 fine, or both, 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 American Civil Liberties Union said it would not challenge the "child luring" portion of the law, however, which targets paedophiles who use the Internet to "knowingly and intentionally induce a child under 16 years of age" to engage in sexual contact.

Although New Mexico Assistant Attorney General Steven Bunch told US District Court Judge LeRoy Hansen that the law was specific in that it applies only to direct online communication between a minor and an adult, Hansen said he was concerned over the effect of the law on interstate communications.

The law, however, while in many respects is similar to laws already struck down as unconstitutional in three states and in the US Supreme Court, is one of the most restrictive passed so far in any state, ACLU national staff attorney Ann Beeson said.

Wiretapping deadline extended

The US House of Representatives has extended a deadline requiring telecommunications companies to give the FBI access to the nation's developing digital telephone system.

As part of the Justice Department's appropriations bill, the House adopted a provision to extend by two years the deadline for telecommunications firms to comply with the 1994 Communications Assistance for Law Enforcement Act. The deadline now is October 1, 2000.

The FBI's wiretapping scheme grew out of the CALEA, which allows the FBI to participate in the process of setting technical standards for the development of the US telecommunications system. CALEA also requires telecommunications carriers and manufacturers to build wiretapping capabilities into the nation's telecom infrastructure.

Under the law, the federal government would have reimbursed the telcos up to $500 million to develop the technological infrastructure and implement the plan by October 24, 1998.

E-commerce software flaw found

A flaw in a type of e-commerce software protocol could be the key for crooks to decode Internet-based transactions under certain circumstances.

A researcher at Lucent Technologies' Bell Labs unit has discovered that a well-equipped hacker can decode "the contents of an Internet session protected by the standard encryption scheme used in most World Wide Web commerce."

Bell Labs' Daniel Bleichenbacher found the problem in secure sockets layer (SSL), which is based on technology developed by RSA Data Security Inc.

E-commerce software companies like Netscape Communications, Microsoft, and RSA, have written and are now distributing a patch for the problem.

RSA said that the cracking of the code has so far happened only in a lab and not in the outside world. In addition, "Due to the large number of messages needed, the potential attack is detectable by network administrators," RSA said.

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

Customs tackle abuse

A bill has been launched in the US to help Customs officers catch those who get involved in online child exploitation.

U.S. Rep. Nick Lampson announced the move, warning of the threat that can lurk within the Internet.

Lampson said his measure would give an additional $2 million to the Customs Service's International Child Pornography Investigation and Co-ordination Centre, which seeks potential paedophiles and child smut traffickers.

During a news conference at the Customs Service's north Houston office, a computer displayed a sexually explicit "chat room," one of thousands that allows users to communicate anonymously or trade software.

Customs Special Agent John MacKinnon said about three per cent of the rooms cater to illegal activity, such as luring children into sexual rendezvous or the trading of child sex pictures. The criminals often use software allowing them to lurk in such rooms without their identity appearing on screen.

"Not only do they not want to be seen by law enforcement, they remain in rooms and avoid conversation while they look to identify a child of the age and gender they prefer," MacKinnon said. "Then they reach out and try to seduce that child."

MacKinnon said Customs agents have arrested 670 people on related charges since 1991.

He said at least one Customs agent in each of the service's 20 main offices is proficient in computer sleuthing, but most of the effort is conducted at his office in Washington.

Because so much child pornography flowed into the United States from abroad by more traditional smuggling means, MacKinnon said Customs has been the lead federal agency for decades. The service was a natural fit to address the move of such material to computers, he said.

Doc admits child porn

A doctor in the US accused of using a medical computer to look at child pornography on the Internet pleaded guilty and agreed to undergo therapy.

Gary Beehler, 37, pleaded guilty to modifying the Providence Newberg Hospital computer system by installing a modem and Internet software without permission.

In exchange, prosecutors agreed to drop all other charges against him — while limiting Beehler's access to children through his medical practice.

"The process has been painful, but I think it has helped me better understand myself and the underlying reasons for my sexual disorder," Beehler said at his court appearance.

Judge John L. Collins sentenced Beehler to 20 days in the Yamhill County Jail. Beehler also must serve five years on probation, not use the Internet, and complete a treatment program with a clinical psychologist.

Oregon State Police searched the hospital computer and discovered more than 400 sexually explicit images, many involving pre-pubescent boys and pubescent girls, according to court documents.

During a search of the doctor's home, police also discovered a two-way mirror that had been installed between an office and a child's bedroom and bathroom.

But it did not appear that the hidden camera behind the two-way mirror was ever used, prosecutor Cal Tichenor said.

Product news

HP tackles global telecoms fraud

Hewlett-Packard has created a global fraud management-consulting program to help fixed and mobile phone operators tackle crime.

The new operation will provide fraud audits, business case development, and fraud centre consultation and training.

Mary Chacanias, former director of fraud prevention for Bell Atlantic and an expert in fraud centre management, has joined HP to lead the effort.

"The formation of HP's fraud management consulting program will help service providers worldwide take a proactive approach to reducing losses due to telephone fraud," said Tom White, HP's vice president.

"The program will benefit significantly from the talent and experience of Mary Chacanias, who is recognised internationally as an expert in communications fraud," he explained.

The new program will build on HP's experience in providing network monitoring systems, he said, including the capability to detect fraud on a real-time basis, which enables service providers to take swift action to prevent losses, reduce bad debt and catch those who misuse the networks.

Plans call for the program to centre on HP's acceSS7 system, which offers real time network monitoring and data collection services to telecommunications service providers.

Under the program, Chacanias and a team of trained consultants will analyse service providers' current practices, recommend process changes, and outline measurable results to strive for in maintaining a proactive approach to fraud management.

HP's test and measurement operations' Web site is located at http://www.tmo.hp.com

Network Associates buys Dr Solomon's

US firm Network Associates is buying UK-based Dr. Solomon's Software in a stock-trade deal the two firms valued at more than $640 million.

The deal is expected to close within the third quarter of this year and is subject to approval by Dr. Solomon shareholders, the High Court in London, and various regulatory reviews.

Dr. Solomon's holds the top market position for antivirus software in the UK and several northern European countries, while NAI is strong in network security and antivirus markets in the US and Europe. The company still considers McAfee VirusScan its flagship.

Bill Larson, chairman of Network Associates, said the two firms have been in talks on and off for the past four years about combining their businesses.

Larson said the keys to finally making a deal was the growing opportunity to up-sell corporate owners of Dr. Solomon's antivirus software into an integrated NAI network security suite while combining customer bases.

"In a year or two we won't be talking about antivirus or intrusion detection or firewalls as point products," Larson remarked. "We'll be talking about integrated network security suites as a core component of the enterprise."

Larson said he expects the acquisition, which will involve NAI's issuing 15.4 million new shares, will let NAI go head-to-head globally with such huge network software vendors as Computer Associates and Tivoli.

Dr. Solomon's anti-virus toolkit will continue to be heavily marketed but will also become part of Network Associates' enterprise security suites, the Total Virus Defence suite, and Net Tools Secure.

Larson said that, by the end of 1999, the two firms' antivirus products would be folded together into one.

- Meanwhile Network Associates has announced big expansion plans for the Asia-Pacific market.

"From a minimal presence in the region four months ago, we have increased our infrastructure, manpower and sales," said James LaLonde, Network Associates' director for the Asia-Pacific region. "Our newly launched Network Associates partner program, under which we have appointed some of the region's best and strongest networking channels, gives us added confidence in our ability to take market share in the region rapidly."

The new company has established offices in Japan, Australia, Singapore and Hong Kong over the last four months and has recently opened its first office in China, in Beijing.

Encryption key recovery

US firm Entrust Technologies says it has found a solution for businesses and groups which need to recover encryption keys without third-party key escrow.

The company has announced its ability to deliver an Enterprise Key Recovery solution that allows firms to retain full control of their encryption keys to protecting valuable information.

Businesses understand the importance of key backup as they must be able to retrieve encrypted data when users lose their decryption keys, forget their passwords or leave the organisation.

If users forget their passwords, Entrust's Enterprise Key Recovery feature provides system administrators with the ability to allow users to recover their keys and regain access to encrypted data. And Entrust says the Enterprise Key Recovery gives corporations the ability to deliver only the relevant decrypted data to law enforcement officials or other third parties.

"While the debate over the relevant merits of key escrow continues, we continue to see strong business requirements for Entrust's Enterprise Key Recovery feature," said John Ryan, president and chief executive officer, Entrust Technologies, Inc.

"Organisations want to retain control of their sensitive information and our system meets this requirement while providing the ability to surrender decrypted data to law enforcement officials when necessary."

Entrust says the system addresses a critical business problem while maintaining protection for documents signed with digital signatures. Entrust software provides separate keys for encryption and digital signatures, but only includes the encryption keys in the key recovery system. This is designed to ensure that users' digital signatures are not compromised by the key recovery system.

For more information contact Entrust on +1 613 247-3455, e-mail carrie.bendzsa@entrust.com or visit the Website at www.entrust.com

Cellular calls can be tracked

SigmaOne Communications Corporation announced the first prototype demonstration of its E-911 system for locating and tracking cellular calls.

The demonstration is the first system to be deployed in the Southern California area in the US to successfully prove that a cellular caller can be located and continuously tracked while in motion.

"We are extremely pleased to report results that prove the accuracy and effectiveness of our E-911 location system," said Mark Licht, president of SigmaOne.

"By locating stationary and mobile calls, this is an extremely important step in offering law enforcement agencies and emergency personnel the best tools for locating and responding to emergencies as they happen. Cellular subscribers are now armed with a communication device they can rely on at the most critical times."

Its makers say that the demonstration of the Southern California network-based system shows accuracy results of 105 meters (345 feet), 67 per cent of the time, in both stationary and continuous tracking tests.

SigmaOne says this exceeds the FCC Phase 2 mandate of 125 meters (410 feet). The capability to successfully track a moving vehicle on the voice channel means SigmaOne's technology can locate cellular callers in a variety of environments.

Tested in the San Fernando Valley area, the demonstration was conducted with a mixture of residential and commercial settings, including two, three and four-story buildings. The continuous, extensive testing of the system includes 350,000-location test points performed to-date with 10,000 new locations tested daily.

And the makers say that as an example of the system's capabilities, the results from a sample mobile test run demonstrated accuracy of 50 meters over 1,000 test locations and that 99.1 percent of all test points exceeded the FCC's accuracy mandate.

The company is currently in development of its second generation integrated AMPS/TDMA system expected to be available for testing in the fourth quarter of 1998 and a CDMA system in the first quarter of 1999.

SigmaOne's second generation correlative location technology is a networked-based system that it is claimed will reliably and accurately measure the bearing angle of arrival and time difference of arrival of incoming cellular phone 911 calls.

Features will include a fully-integrated base station that will support either AMPS only or AMPS and TDMA IS-136 and a capacity to handle 500 locations per second per cell.

For more information contact SigmaOne on +1 818 348-3300 or e-mail mlicht@pacbell.net

Green light for scrambling export

Computer Sentry Software in the US has announced that it has been granted approval to export advanced encryption software to virtually any company in any country in the world.

The US Department of Commerce recently authorised the company to export its new product, the CyberAngel EXR, which offers encryption strengths ranging from 56-bit DES to the ultra-powerful 448-bit Blowfish.

"The CyberAngel EXR will allow global organisations - anywhere, in any industry - to adopt world-wide data encryption standards," said Dyrk Halstead, CEO of Computer Sentry Software.

"The vast majority of export authorisations granted to US encryption companies so far have been limited to specific countries or industries such as financial services."

The CyberAngel EXR protects stored data - such as files on a laptop or PC - and was designed to allow the legitimate access to that data in the event that "keys" or passwords are forgotten or unavailable.

As such, EXR met the requirements for exportation under the KMI, Key Management Infrastructure, and export license exception.

"The Department of Commerce has found a win-win solution for the government and the US software industry with Computer Sentry Software's encryption product," said William Reinsch, Undersecretary of Bureau of Export Administration, US Department of Commerce.

Barry C. Collin, Senior Research Fellow, The Institute for Security and Intelligence said, "We believe that the responsibility for finding a security system that serves the global needs of corporations and that satisfies public safety is the responsibility of the private sector.

"Computer Sentry Software has neatly solved this problem by providing plain text data recovery while ensuring individual privacy for corporations around the world. CyberAngel EXR offers an impressive breadth of security functionality, enabling corporations to recover data on specific PCs and laptops - without compromising the security of the entire enterprise."

The CyberAngel EXR offers three powerful encryption algorithms: 448-bit "Blowfish," 128-bit EMD-2 and 56-bit DES, the US government's Data Encryption Standard.

Its makers say the CyberAngel EXR actively detects unauthorised users on both mobile and networked computers preventing access to information stored on the hard drive as well as on the corporate network.

In the event of an unauthorised access attempt, the CyberAngel silently alerts either Computer Sentry Software's monitoring headquarters or a corporation's network administrator, via modem or network TCP/IP connection.

Following an access alarm, registered computer owners are notified by CSS of the attempted breach within two minutes via e-mail or fax.

For more information contact Computer Sentry Software on +1 615 790-

8821 ext. 103, e-mail brian@sentryinc.com or visit the Website at www.sentryinc.com

New name and new security systems

Cycomm International Inc. has announced that its secure computing subsidiary has a new name and has also launched 12 new products.

Cycomm Secure Solutions Inc, formerly XL Computing Corporation, says the new products provide protection against the increasing number of cyber attacks being made on government and business information networks.

"The risk of information loss due to intrusion of the computing infrastructure is a grave and growing one," stated G.T. Gangemi, President and CEO, Cycomm Secure Solutions.

"The threats range from sabotage of data to financial fraud to theft of proprietary information. Our product introductions broaden the arsenal of security tools available to organisations such as the military, government agencies, and financial institutions.

"In fact, any corporation that relies on computers to run their business needs to analyse this facet of their company's information security program.

Cycomm Secure Solutions says that its line of EMI (ElectroMagnetic Interference) and Tempest (the classified standard for securing computer equipment and peripherals products) will appeal to firms and government agencies which rely on top-level security.

Computers, monitors, keyboards, printers and related peripherals produce emissions that can be intercepted with relatively inexpensive equipment through the building structure from various distances. In this regard, it is possible to obtain the content being inputted or transmitted.

The new EMI products are commercial grade and include a 260E Pentium II Personal Computer, a 4525E Colour Monitor, and a 430E ruggedized portable laptop. As exportable EMI products, they are designed for use by business and governments internationally.

"The military is concerned, too, about protection of the armed forces communications," said Jules Rutstein, Vice President of Business Development for Cycomm Secure Solutions.

"Late last year, a Presidential commission questioned how prepared the United States is against electronic warfare. Cycomm Secure Solutions is expanding our Tempest-approved computer line to help address that.

"We have the only Tempest version of a Compaq DeskPro computer and a Tempest version of a Hewlett-Packard laser jet printer. This will allow users to buy industry standard products for use in a classified environment."

The 3512T and 3522T laser printers expand Cycomm Secure Solutions' line of Tempest printers. Based on the Hewlett-Packard 4000 LaserJet, these printers meet the specifications for Level I (3512T) and Level II (3522T) NSA Tempest criteria.

Cycomm Secure Solutions is releasing another model of the only commercially available NSA-endorsed Tempest laptop. The new 425LT has a 200 MHz MMX processor with optional upgrade to a 233MHz processor and memory expandable to 128MB. The 425LT simultaneously supports 1.44MB floppy and 20X CD-ROM drives and has 2 serial ports.

Other products being announced by Cycomm Secure Solutions include the 430E, a secure, ruggedized laptop. Based on a Panasonic CF25, the 430E is for tactical secure computing. Additionally, two new Zone desktop computers, the 215MXA and 215MXB, are being introduced.

For further information, contact Laurie Rice, Director of Corporate Communications, Cycomm International, at +1 800-884-8544 or visit the Cycomm Website at www.cycomm.com

Internet filtering and monitoring solution

A system to manage Internet content at the workplace has been launched by US firm Content Advisor in a bid to cut down on system abuse.

Content Advisor's tool uses trained editors to systematically categorise URLs and is tightly integrated with the leading firewall product from Check Point Software Technologies, Ltd.

The system lets network managers to effectively monitor Internet usage deemed inappropriate in the workplace, control valuable network bandwidth and protect against potential legal issues.

"Now that Internet access is essential to business, employers need a reliable and flexible solution to filter and monitor Internet usage," comments Steve Shannon, president and founder of Content Advisor.

"Our patent pending technology produces the best corporate solution by offering the largest database of categorised URLs and the most accurate and rigorous standard for categorisation to be customised according to the specific needs of the corporate user."

For more information contact Lynne Christos Taylor on +1 617 520-9116

· A software company that monitors Internet usage says sexually explicit web sites are being accessed by employees during work hours at nearly two-thirds of responding companies.

Kelly Haggerty, spokesman for Elron Software Inc., says the Internet Manager program can pinpoint exactly which inappropriate sites have been selected, "It goes down to the specific user or work station, depending on how the computer is configured."

Haggerty said that almost one-third of companies polled have taken punitive action against employees who abuse web surfing privileges.

She said: "We mainly focus on reporting to enforce a particular Internet-acceptable usage policy that the company or organisation has put into place."

Rita Risser, an attorney specialising in employment law issues, says an employee disciplined for viewing sexually explicit sites while at work would have little recourse.

She said: "Under the Federal Electronic Communications Privacy Act, employers have the absolute right to monitor employees' Internet and e-mail type uses. There is no right to privacy."

The program is available on the Web at http://www.mailjail.com for $19.95, or on a CD for $29.95 plus shipping.

Fake software ring smashed

A software theft ring involving almost $20 million worth of Microsoft computer software disks is almost closed after seven people were charged in the US.

The five men and two women, all residents of Massachusetts, were indicted in federal court with conspiring to transport stolen computer disks and computer software in interstate commerce from December, 1995, until December, 1997.

All of the defendants except one also are charged with 16 counts of transporting specific shipments of stolen computer disks in interstate commerce.

The disks originally had been stolen from Kao Infosystems Co., a computer disk manufacturer and distributor located in Plymouth, Massachusetts, by three warehouse employees.

Two of the warehouse employees - Scott J. Dooley, 29, of Hyannis, Massachusetts, and Kelly Downing, 27, of Plymouth, Massachusetts - pleaded guilty to a one-count indictment charging they conspired to steal more than $25 million worth of computer disks and software from Kao Infosystems.

The indictment also charged them with conspiracy to transport millions of dollars worth of stolen computer disks and related merchandise in interstate commerce, US Attorney Donald K. Stern said.

The third employee - John J. Costello, 36, of Marshfield, Massachusetts - pled guilty to one count of conspiracy to transport the disks.

In the most recent round of indictments, Robert S. Simons, 61, of Peabody, Maxine S. Simons, 58, of Peabody, William A. Simons, 34, of Salem, Sherri L. Craig, 35, of Malden, David F. LaPointe, 34, of Hyannis, Marc L. Rosengard, 44, of Salem and Dover, New Hampshire, and Gerald P. Coviello, 61, of Woburn, appeared in US District Court to answer charges contained in a 33-count second superseding indictment, Special Agent in Charge of the FBI Barry W. Mawn said.

Three of the defendants - Robert and Maxine Simons, and Craig - were charged with a separate conspiracy to launder the proceeds of the various sales of stolen property, and with eleven counts of money laundering.

LaPointe and Maxine Simons also were charged in three counts with structuring various transactions in order to conceal the sale and purchase of the stolen property, and Maxine Simons also was charged with making false statements to the FBI during the investigation of the case.

US Attorney spokeswoman Amy Rindskopf said the indictment charged LaPointe with selling the stolen computer products to Crazy Bob's, a discount computer software and hardware store in Wakefield and operated by Robert and Maxine Simons.

The stolen property included "substantial amounts" of the Microsoft CD-ROMs stolen from Kao Infosystems.

After receiving a number of shipments of stolen property, the indictment charged that Crazy Bob's sold the disks to various CD-ROM outlets in California and the UK.

Robert Simons and Coviello also tried to sell 8,000 stolen Microsoft Office 97 Professional disks last fall to a buyer from North Carolina for $245,000, the indictment charged.

As Coviello attempted to transfer the disks and collect the money from the North Carolina buyer, he was placed under arrest by the FBI, Mawn said, while Simons was arrested at Crazy Bob's office in Wakefield.

Rindskopf said that, if convicted, each of the defendants face penalties of up to five years in jail and a $250,000 fine on the conspiracy count.

Robert, Maxine and William Simons, as well as Craig, LaPointe and Rosengard also each face additional penalties of up to ten years in prison on each of the 16 counts charging interstate transportation of stolen property.

Robert and Maxine Simons and Craig each face additional penalties of up to 20 years in prison and a $500,000 fine, on each of the 11 counts.

The indictment also seeks forfeiture of the defendants' bank accounts and of $462,000, due to money laundering charges.

The Kao warehouse employees - Dooley, Downing and Costello - have stolen "tens of thousands" of recordable compact disks, computer disks containing Microsoft software, and other computer merchandise, Rindskopf said, while Dooley and Downing also stole more than 23,000 Microsoft Office 97 Professional software disks, which they later sold for profit.

According to the charges against Dooley and Downing, they also tried to sell a second shipment of the stolen disks, worth over $10 million, including an additional 18,000 Microsoft Office 97 Professional disks, to a buyer from New York.

Unknown to the defendants, however, the buyer from New York was an undercover agent with the FBI, who had been introduced to the defendants by one of their co-workers at Kao, Mawn, said.

On March 22, 1997, after final arrangements had been made for the sale of the $10 million shipment to the New York buyer, the three defendants were arrested on a federal warrant, Mawn said, and the $10 million shipment was recovered from a storage facility in Plymouth.

- The FBI and the US Attorney's Office for Indiana arrested a number of alleged software pirates in a series of fast-paced raids at a computer fair.

The raids came after a five-month investigation into individuals accused of illegally making and selling CD-ROM compilations and counterfeits of a number of software packages, worth millions at real prices.

During the raid at the MarketPro Computer Show at the Indianapolis fairgrounds, which was co-ordinated with a parallel raid in Radcliff, Kentucky, FBI agents seized counterfeit software, unbundled software and computer hardware, including CD-ROM duplicating equipment, and financial records.

California-based software firm Autodesk initially alerted the FBI to the alleged counterfeit operation as a result of its own investigation following a call to its anti-piracy hotline.

The suspects allegedly sold counterfeit copies of AutoCad Release 14, normally a $3,750 product, on CDs without documentation for $75, as well as a CD compilation with more than $3,500 worth of Adobe software for $60.

The Software Publishes Association has a hotline on +1 800-388-7478.

Nuclear hackers

Members of the Milw0rm hacking group claim to have broken into the computer network of a nuclear research facility in India.

The group, which calls itself Milw0rm, said it accessed e-mail messages sent between nuclear scientists and Israeli government officials, as well as a list of planned nuclear projects and other files related to India's nuclear research program.

Members of the group, who use the online aliases of "JF," "Hamstor," "Keystroke," "savecore," "Venomous" and "ExtreemUK," said some of the files they copied belonged to a group of experiments called the Neutron-Gamma Coincidence Studies.

They said they broke into the Bhadha Atomic Research Centre (BARC) to protest about the Indian nuclear testing.

"It seems the Indians don't have the (security) technology to protect the (nuclear) technology they have," a source close to the Milw0rm group said.

"It's ironic that India has weapons capable of destroying the world, but they can't secure a little web server which is connected to their networks," one of the hackers, called Keystroke, said in an Internet relay chat with John Vranesevich, founder of the Anti Online Web site at http://www.antionline.org.

"We have information on their weapons, their test projectories (sic), everything, and we are doing this from all over the world," another Milw0rm hacker, JF, said. "They are not secure, Milw0rm are beating them, this shouldn't be happening."

The group broke into BARC's local area network through its Web site at http://www.barc.ernet.in which was connected to the LAN, Vranesevich said. "There was a firewall, but it wasn't configured properly and Milw0rm managed to bypass it," he said.

The group was able to access e-mail between the BARC scientists, as well as a list of planned nuclear projects and other files related to India's nuclear research program.

One piece of e-mail retrieved by the group detailed a conversation about increasing the yield of gamma rays in Pm141, an isotope of the rare earth element Promethium.

"The slight increase in the yield of 882 (keV gamma ray) in our alpha data could be accepted because at lower energy, the population of the isomer may be more which stabilises after some threshold energy of the projectile," the e-mail said.

After being shown the information, scientists of the University of Tokyo's Institute for Nuclear Studies said it had nothing to do with weapons but that it did contain "pretty advanced nuclear physics."

The group said it is "still contemplating" what to do with the information they hacked, "but we securely have it locked away and we will be keeping this position until further events unfold."

"We could use it in a very serious case of international terrorism and sell the information," they said, "but as we are not interested in causing world trouble (he he) we will hold onto it."

Milw0rm also changed BARC's Web page into an anti-nuclear tirade.

"It just goes to show that `No' information is safe, the group said. This is a highly classified and highly sensitive issue, the recent tests show that it is no laughing matter."

Officials at BARC confirmed their computer network was infiltrated and that e-mail was accessed, but denied the breach had been serious.

"It's all taken care of, there's nothing to worry about," an official said. He confirmed the claims of the group of hackers calling themselves "Milw0rm" who said they managed to breach network security at BARC, change the Web home page and download five megabytes worth of e-mail and data.

"It's a very normal loophole in sendmail," the official said. Sendmail is defacto Internet standard software for running electronic mail systems.

"Definitely, there was some problem with sendmail, they were using an old version," he added before refusing to comment any further.

Sendmail has been the object of many security attacks in the past and most security-conscious users have addressed the loopholes uncovered and

documented over the years.

It is unlikely that the sendmail software at BARC had been updated with the latest security measures.

A second group of hackers also attacked the BARC Web site. As opposed to the Milw0rm group, which attacked the network and accessed files, the second group replaced the home page with a simple message under the title "Just Say No."

"Nuclear Tests in India. This page has been hacked in protest of a nuclear race between India, Pakistan and China. It is the world's concern that such actions must be put to end since, nobody wants yet another world war.

"I hope you understand that our intentions were good, thus no damage has been done to this system. No files have been copied or deleted, and main file has been just renamed," the Web page read.

Chairman of the Atomic Energy Commission, R Chidambaram, has denied that any of the hackers had gained access to sensitive information of any kind from the classified servers.

Chidambaram said that the hackers could access only the BARC home page, which was in the public domain, and some of the e-mail messages.

"The computers used for these are isolated from all other computers being used at the BARC and obviously did not contain any sensitive information," he said.

Dr. Dekne, senior scientist at the BARC confirmed that there was no critical data that was wiped out from the BARC computer server simply because the centre physically isolates sensitive data from the Web and e-mail servers which are prone to such attacks.

He said: "We have several levels of isolation before reaching our internal network." He added that formulas and cascading mathematical equations are usual in e-mails among nuclear scientists.

While the incident may have involved only non-sensitive information, it may have helped to alert India's network managers about the importance of security, said Dr. S. Ramakrishnan, director of ERNET (Education & Research Network), India's first Internet service provider to which BARC is connected.

"Recent access by hackers has been only to e-mail messages of scientists and BARC home page information, and the connections for these are isolated from all other computers used at BARC and obviously do not contain any sensitive information," said S. Narendra, principal spokesman for the Indian government.

Meanwhile, the MilW0rm group, made up of of about a half dozen teens, aged 15 to 18, from around the world, says it has gained access to servers in a Turkish nuclear research facility.

According to John Vranesevich, founder of antionline.org, the teenage intruders gained access to the Cekmece Nuclear Research and Training Centre in Istanbul and retrieved hundreds of pages of memos and e-mail from scientists, including conversations between Turkish nuclear scientists and the International Atomic Energy Agency (IAEA).

The MilW0rm group, Vranesevich said, also apparently had assistance in accessing the Turkish facility from a second "hackgroup," which also has turned over "proof" that they also gained access to servers in Iran, Israel and Latvia.

But like the information retrieved from BARC, none of the information stolen from the Turkish research centre appears to be directly related to nuclear weapons research.

There do appear to be several encrypted documents downloaded from the Turkish facility, Vranesevich said.

Since the story first broke about MilW0rm's penetration into the Indian nuclear research centre, the group, with members from the US, the UK, Israel and New Zealand, have also claimed they are attempting to infiltrate nuclear research sites in Pakistan as well.

But according to one Pakistani source, it would be difficult for any group to infiltrate the Pakistani centres.

"Neither Pakistan Atomic Energy Commission, nor Kahuta Research Laboratories (Uranium enrichment plant site and research centre) have loopholes for external Internet hackers to log in," Rashida Shaikh said.

"Computer systems installed there for nuclear computation and information systems purpose are disconnected from Internet service.

"Even different remote computer centres are not on WAN (wide area network), except a few. So hackers who log in planning to log in using Internet connectivity are just wasting their time."

Hacking across the world in seconds

The MilW0rm group said they accessed the BARC computers through a series of "hacks," starting by a telnet out of their individual computers to a Wingate.

The Wingate software is used by hackers as jump points without fear of being logged, they said.

The group then did a telnet to a NASA Jet Propulsion Laboratory (JPL) server at tartarus.jpl.nasa.gov, which served as the "dead end" point, or the last place someone can retrace the hackers tracks.

From the JPL server, the group then went to a US Navy server via telnet at yokipc.navy.mil, then to the US Dental Command Centre at dencom.army.mil.

MilW0rm then reportedly used the Dental Command Centre site as a jump point to India and the BARC system. The group was then able to access e-mail between the BARC scientists, as well as a list of planned nuclear projects and other files related to India's nuclear research program.

A US Army spokesman confirmed that unauthorised sources did break into a US Army computer system last week, but declined to speculate whether that was the route MilW0rm took to gain access to the Indian facility.

The incident, however, is being investigated by both the US Army and FBI Army spokesman Gerry Gilmore said. He added that the dencom site was immediately shut down, and has since been secured.

UK DERA porn scandal

The Journal has helped uncover one of the biggest Internet pornography scandals in the UK. Paul Johnson reports.

Workers at a Ministry of Defence research laboratory downloaded more than 170,000 pornographic images in just three weeks. Many of the pictures involved young children or animals.

Details of explicit and illegal images were revealed during the trial of a computer engineer who worked at the Defence Evaluation Research Agency in Malvern, Worcestershire.

Paul Roper, 35, was acquitted at Droitwich magistrates court on all eight counts of possessing indecent computer photographs after a five-day hearing.

MoD investigators were astonished at the sheer amount of pornography at the Malvern DERA site - an agency responsible for developing battlefield technology for Britain's armed forces.

The investigators found that a key computer server, which was intended to help scientists swap information or conduct Internet research, had spent most of its time downloading and distributing the pornography images.

Although Mr Roper, a network engineer, was found not guilty, evidence given during the hearing showed the extent and scale of computer misuse by workers at the DERA.

The court was told that any of 3,500 users of a sophisticated government computer system, mostly civil servants, could log on and access vast quantities of pornographic material without restrictions. And the trial heard that a special program called Sucker had been used, which automatically retrieves thousands of pictures from the Internet while the operator is left free to carry on with other day-to-day computer work.

Records show that during the course of just three weeks in January and February last year, one user alone downloaded more than 30,000 pictures from Internet newsgroups – areas in cyberspace where people can swap information, computer programs or pictures with each other.

In one case, 10,045 images were taken from a newsgroup called "erotica.teen.female" and another 2,868 pictures were retrieved from one called "erotica.young". Other newsgroups where pictures were downloaded include those entitled "lolita", "schoolgirls", "pre-teen" "rape", "pedophilia" "torture", "bestiality" and "incest".

Although the computer system is based in Malvern, it is linked to dozens of other military and government sites across the country using high-speed connections and ISDN lines.

Forensic computer expert Jim Bates, technical director of Computer Forensics Ltd, gave evidence in court for the defence and had made an independent investigation of the material stored on the DERA computers, including the central server system which acted as a hub to other satellite computers.

He told the court that he found thousands of suspect files on the computer server and said that a large amount of the system's time was spent on distributing pornography.

Mr Bates said: "A preliminary analysis of the log indicates that around 60 per cent of callers were accessing the pornographic newsgroups and around 90 per cent of the active server time was spent on transferring pornographic articles.

"The concept of an unrestricted network available to anyone, from any computer sounds fine in theory. However, given that such provocative material and intriguing material was available at the push of a button it is not surprising that this problem developed to such alarming proportions."

He added: "The configuration of the network at Malvern and its associated sites was apparently self-designed and self-administered and it seems that little attention was paid to access security."

And Mr Bates said that even when MoD investigators moved in after the allegations came to light, computer pornography was still being retrieved.

He said: "Even after the 24th of January, when presumably most personnel either knew directly or had heard that an inquiry was being made, pornographic material was still being downloaded from the server in large quantities.

"Thus in spite of the seriousness of the situation, no attempt was apparently made to cut off the supply of this material at the source."

The court heard that Mr Roper had even brought the huge amount of pornography to the attention of managers, but with little consequence.

Paul Roper, from Malvern, was cleared of the pornography charges after the court heard that evidence had been accidentally corrupted by DERA managers and MoD police during initial investigations and that the correct forensic procedures had not been followed.

Mr Bates told the court: "The actions of management and security personnel has compromised and contaminated the evidence that I have seen in this case.

"These people should certainly have realised that the best course of action was to isolate and switch of the relevant machines pending expert attention. They should have known better and the result of their activity has been to obscure an already complex case."

Mr Bates added that although a large quantity of computer pornography had been found, it could not be directly linked with Roper as his machine could be used by anyone who entered the room.

He said: "Access could be gained through the computer by simply switching it on and pressing the enter key when asked for a password. Thereafter, access to the server and the whole of the Internet was just as free."

After the case, a spokesman for the Defence Evaluation Research Agency, part of the Ministry of Defence, said action was taken when employees were found to be misusing the computers.

He said: "It's a disciplinary offence to download material from the Internet that is not related to work on a work computer in work time. We take it very seriously. We have made it quite clear that accessing this sort of material in government time and on government property is not allowed."

He added: "Ninety per cent of our work is military science and technology based. There is a lot of material on the Internet and our scientists need to use it on a regular basis."

Next month the Journal examines the problems in the forensic investigation of the Roper case.

UK evidence guidelines

ACPO Good Practice Guide - computer based evidence

By
DS Nigel Jones

The Association of Chief Police Officers in the United Kingdom (ACPO) has recently issued guidelines to police officers dealing with the correct procedures to be used when encountering computer equipment which is believed to contain evidence of criminal activity.

Background

The background to the production of this document which is believed to be the first giving such guidance on a national basis is that the involvement of the police in computer crime can be divided into two distinct areas, namely computer crime investigation and computer forensics.

There has been and still remains much confusion amongst those not involved on a daily basis with either or both of these disciplines, of the differences and the relevance of the distinction between the two.

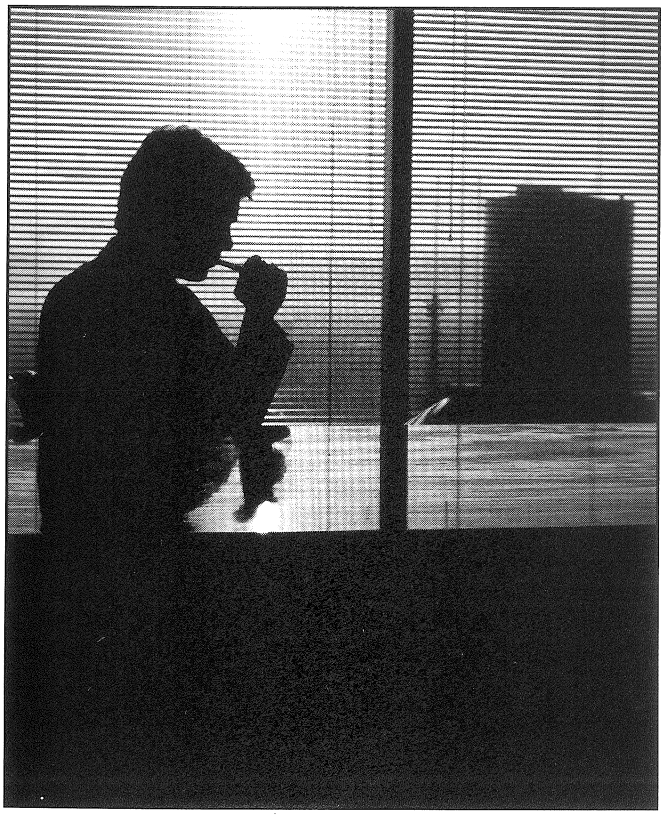
The police service as a whole, historically did not comprehend the nature of computer-based evidence and the difficulties created by the international nature of computer crime.

The Association of Chief Police Officers in 1996 identified a need to be advised on matters relating to computer crime and computer forensics. They instructed that a working group be formed to carry out this function.

As a result of this need, the policing regions of England and Wales made nominations and appointments were made to the group. There have been additions since then and there are now some 19 members.

The current chairman is Detective Chief Superintendent Keith Akerman, the head of Hampshire CID.

It is fair to say that the group is made up of practitioners rather than managers and most if not all of the members have experience in computer crime investigation, computer forensics or both.



Membership of the group is made up of the following organisations:

- All ACPO Regions Including N Ireland
- ACPO (Scotland)
- National Police Training
- National Crime Faculty
- Home Office Police Information Technology Office (PITO)
- Forensic Science Service
- National Crime Squad
- MOD Police
- Police members of the Joint-Agency Forensic Computing Group

The Group first met in August 1996 with the following terms of reference:

To provide advice and guidance to ACPO Crime Committee on the following subjects:

The Investigation of Computer Misuse Act Offences

Generally the hacking type of offences that the Metropolitan Police Computer Crime Unit (CCU) have traditionally dealt with on behalf of the rest of the country

Crimes on the Internet

The main publicity about crime on the Internet relates to the distribution of paedophile material but as we know, there are many other crimes that may be committed using the Internet as a vehicle and we have recognised that co-operation with the Internet Service Provider (ISP) industry is essential.

To this end a combined ACPO/ISP forum has been created to work towards a memorandum of understanding between the parties.

Computer Based Pornography

Work has been carried out into the role of the Internet Watch Foundation (IWF). A further area of concern is the effect on staff of continually viewing pornographic and paedophile images and an examination of scientific selective sampling is taking place

Technology relating to Theft of Hardware

This area was included in our remit but realistically is a different type of crime than the others included in the responsibilities of the group.

Computer Based Evidence

This is the area of responsibility that has resulted in the production of the

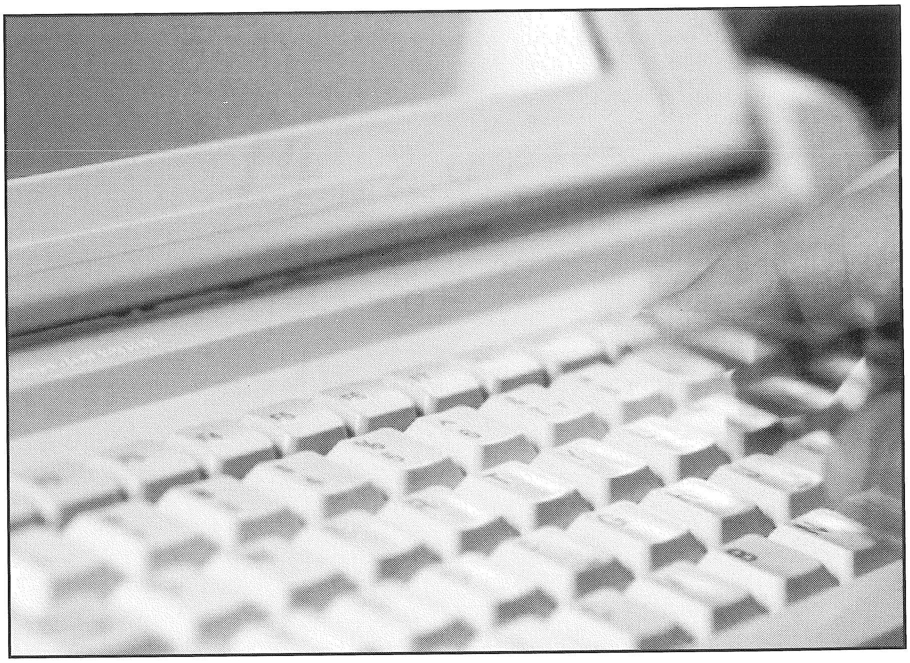
ACPO guide.

Counterfeit and Pirate Software

We are charged with looking at the relationship between the police and industry organisations and establishing what the police response should be to software piracy. Work is proceeding towards a memorandum of understanding between the parties.

Training Implications

A very important aspect of our work is to identify any training issues that arise from our other work. To date all work carried out has identified areas of training need and a recently formed training sub group is addressing these.



ACPO Good Practice Guide Computer Based Evidence

Background

A survey of police forces revealed there were various practices used in relation to the recovery of evidence from computers.

Concern had been expressed that some of these were bad practice and liable to lead to the acquittal of criminals if not rectified.

It was also acknowledged that a great deal of good work had been carried out by some police forces. In an attempt to harness this and ensure that everyone benefited, a sub group of 4 people was set up in July 1997 with a remit to produce a good practice guide for computer based evidence which as an ACPO document would encourage standardisation of procedures in UK police forces.

Consultation with other agencies and industry took place as appropriate. Views and contributions were invited from interested parties and a number of meetings were held.

We decided that it would be impossible to deal with all of the issues involved in computer forensics in one document. It was our view that the reasons for the failure of others to produce a good practice guide in the past was that other publications have sought to do too much and have ended up not achieving their aim.

A draft document was tested in December 1997 by visiting officers involved in computer forensics and allowing them as practitioners to follow the guide through.

Other groups were invited to comment upon the content of the guide. These included the two main suppliers of equipment to the police to see if the guide created difficulties for those products.

Some minor amendments were made and the document was presented to the Computer Crime Group on 8th January 1998 and submitted for approval to ACPO.

The document was placed before the ACPO Crime Committee meeting in Cardiff on 26th March 1998 and was approved for circulation to all Chief Constables in England and Wales.

The Principles

There are five basic principles which underpin the message given in the guide and these are based on the requirement to ensure that any evidence recovered from computers is as admissible in a court of law as would be documentary evidence.

The Doctrine of Documentary evidence may be explained as:-

"The onus is on the prosecution to show to the Court that the evidence produced is no more and no less now than when it was first taken into the possession of police."

Data held on a computer is no different to information or text contained on a document. For this reason evidence that is based on a computer or on computer media is subject to the same rules and laws that apply to documentary evidence.

The principles set out in the document are given as guidance for all police forces when dealing with computer based evidence and are as follows:

1. **No action taken by Police or their agents should change data held on a computer or other media which may subsequently be relied upon in Court.**

The fundamental issue is one of integrity and acceptability of data stored on a computer or associated media. The first principle is therefore deliberately specific.

2. **In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions.**

In a minority of cases it may not be possible to obtain an exact copy of the entire target device. In these circumstances it may become necessary for the original machine to be accessed to recover the evidence. With this in mind it is essential that any such access is made by a person who is competent to carry out the function and give evidence explaining the effect of what they have done to a Court of Law. The second principle acknowledges this.

3. An audit trail or other record of all processes applied to computer based evidence should be created and preserved. An independent third party should be able to repeat those processes and achieve the same result.

There are a number of reasons why an audit trail is important to ensure that the recovered data stands the best chance of being accepted in evidence.

As we know operating systems and other programs frequently alter and add to the contents of the computer's storage space. This can happen automatically without the user necessarily being aware that the data has been changed.

An audit trail of the processes will assist and is considered essential. In order to comply with the principles of computer based evidence a copy should be made of the entire target device.

Partial or selective file copying should not be readily considered as an alternative. The copy or copies should be made onto media, which should be retained for examination and subsequent Court use.

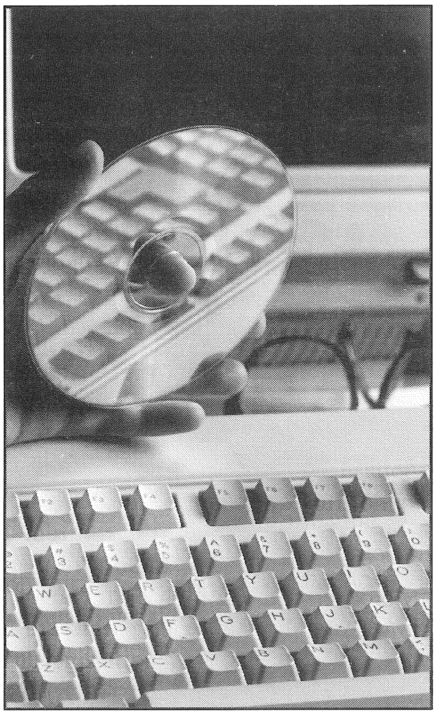
It is essential to objectively show to a Court that the continuity and integrity of the evidence has been preserved. It is necessary to demonstrate to the Court how evidence has been recovered showing each process through which the evidence was obtained. Evidence should be preserved to an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a Court.

4. The onus rests with the Officer in charge of the case to ensure compliance with any law pertaining to the possession of, or access to, information contained on a computer.

The officer must be satisfied that the use of any copying device or actions of any person having access to the computer complies with these laws.

5. The onus of ensuring that these principles are adhered to and that the evidence is admissible rests with the Officer in charge of the case.

The officer must be satisfied that the use of any copying device or actions of any person having access to the computer complies with these principles.



Both principles 4 and 5 are included to remind colleagues that responsibility for ensuring that the law and the principles set out in this guide are complied with lies firmly with the Investigating Officer.

He or she cannot abdicate responsibility for their own investigations by leaving either in house specialised staff or external consulting witnesses to make decisions on their own, without the investigator considering the implications.

Compliance with the principles will ensure that the continuity and integrity of the evidence will be preserved. We do not believe that it is to difficult to comply with these principles, even for forces who have not set up specific units to deal with computer based evidence.

Purpose of the guide

The document is intended for use by the Police Service as a guide for good practice when dealing with computers in the possession of a suspect. It is not intended as a guide for Officers dealing with evidence produced by witnesses from third party computer systems. It is intended for use by personnel in specific circumstances, namely:

Officers discovering computer equipment

Advice is given on securing, seizing and transportation of computer equipment from search scenes, with a view to recovering computer based evidence. These are simply described as:

- What to do
- What not to do
- What should be taken?
- How to take it
- How to pack it
- How to transport it
- Where and how to store it

The advice given to persons discovering equipment to be seized is very simple and relates to the subjects above. There is no attempt to reinvent the wheel and many of the things that are seen in the guide are already accepted practice in most police forces. In fact the more of the practices that are recognised by readers of the guide as being practice in their organisation the better.

Investigating Officers

Advice is given in relation to the planning and management by investigating officers of the recovery, identification, production in court and storage of computer based evidence. Again the advice falls into the following simple categories:

- Pre search considerations
- Identification of equipment
- What should you take?
- Who should you take?
- Ensure adequate briefing of staff

- Detail records to be kept
- Interview strategy
- Retention of equipment

This section of the guide is not intended to be seen as teaching experienced investigators to suck eggs.

It is an attempt to encourage them to realise that the issue of obtaining and using evidence from computers requires as much planning as any other part of their enquiries.

The subjects here are dealt with in the guide and it is, I would suggest, far better for an investigator to be in possession of the knowledge to consider these as part of his investigative strategy rather than deal with them on the hoof.

Computer evidence recovery personnel

Copying and reproduction of seized computer based evidence, by personnel who are trained to carry out the function and have the relevant experience to give evidence in court of their actions.

Persons who have not received the appropriate training and are not able to comply with the principles must not carry out this category of activity.

The areas covered by the section are:

- IBM compatibles
- Non IBM compatibles
- Hard Disks
- Floppy Disks
- Magnetic Tapes
- Removable Media

I will stress again that this section of the guide is aimed at experienced and trained personnel and is not to be seen by keen amateurs as authorising them to undertake computer forensic work.

The guide gives general advice on how the listed items may be dealt with effectively.

One of the things we have recognised as a group is that there is a need for a manual for evidence recovery personnel and a sub group has been formed to produce this.

External consulting witnesses

Advice is given on the selection and management of persons who may be required by investigating officers to assist in the seizure, recovery, identification and interpretation of computer based evidence. Specific guidance is necessary in this area in order to ensure that investigators who have little technical knowledge do not use inappropriate people.

The following areas are included for consideration by investigators:

Specialist Expertise

This is the skill or competence to do a particular job

- What are the relevant qualifications?
- How skilful is the person at this particular job?
- What is the specific skill?
- Is it based on technical qualifications or length of experience?

Specialist Experience

- What experience of this type of work has the individual?
- How many cases?
- What type of cases?
- How long has the individual been working in this area?
- What proof is there of this experience?

Investigative Knowledge

Understanding the nature of investigations in terms of PACE, confidentiality, relevance and the distinction between:

- Information
- Intelligence
- Evidence

Contextual Knowledge

Understanding the different approaches, language, philosophies, practices and roles of:

- Police
- Law
- Science

Fundamental to this is the understanding of probability in its broadest sense and differences between scientific proof and legal proof.

Legal Knowledge

Understanding of relevant aspects of law, legal concepts and procedures in relation to:

- Statements
- Continuity
- Court Procedures

Clear understanding of the roles and responsibilities of expert witnesses is essential.

Communication Skills

The ability to express and explain in layman's terms, both orally and in writing:

- Nature of specialism.
- Techniques and equipment used
- Methods of interpretation
- Strengths and weaknesses of evidence
- Alternative explanations

It is considered that all external consulting witnesses should be provided with a contract to ensure that they receive the protection afforded by Section 10 of the Computer Misuse Act 1990 to police officers.

It is recognised that the guide is not a definitive manual. It is intended to address the most common circumstances that will be encountered with evidence retrieved from computers.

Conclusions

The challenges facing the police in the areas of computer crime and computer forensics are beginning to be met now that there is national and international pressure for positive action to be taken.

The following principles were set out by the G8 Government Ministers meeting on 12th December and are therefore considered as a standard for countries to aim to meet. I have highlighted one of the principles that is particularly relevant when considering the ACPO guide.

Forensic Q&A

G8 Ministers Principles:

- No safe havens for IT criminals
- Co-ordination of IT crime investigation and prosecution
- Properly trained & equipped personnel to address IT crime
- Legal systems must protect systems from serious abuse
- Legal systems must allow preservation of & access to data
- Mutual assistance regimes to allow exchange of evidence
- Trans-border electronic access to open source information without authorisation
- Development of standardised forensic techniques for retrieving and authenticating electronic data in investigations
- Design of systems to prevent and detect hi-tech crime

The time to standardise procedures for the recovery of computer based evidence is now and the issue of the ACPO guide is perhaps the first step to ensuring that evidence will be admissible in whichever country it is needed, regardless of the country in which the computer is located.

Interpol has already decided to include the guide in its computer crime manual to be circulated to all member countries.

The guide is available to any law enforcement agency and may be obtained from Detective Sergeant Nigel Jones, Computer Crime Unit, Police Headquarters, Sutton Road, Maidstone, Kent, England ME15 9BZ. Telephone +44 (0)1622 654925.
E-mail nigel@ccscrops.demon.co.uk.

The ACPO computer crime group is also interested in hearing from anyone who has developed good practice in this area in their own country in order that this may be shared on a mutual basis.

Kind thanks to DS Nigel Jones, the author of this article. DS Jones, from Kent Police, is currently an ACPO representative and has just been appointed as Secretary of the group.

Q What does the term 'Hex Dump' mean?

A First of all the word 'hex' is short for hexadecimal. Hexadecimal notation is the representation of numbers in the positional number system with base 16. The sixteen hexadecimal digits are usually represented by 0-9, A-F. Decimal notation works to a based of 10 and binary notation to a base of 2. Any hex number can be converted into its decimal or binary equivalent, and vice versa.

Computer code is written in programming languages that conform to hexadecimal notation. This is because at the most basic level computers work by setting a series of switches to either on or off (1 or 0). Information is encoded by noting the settings of groups of 8 switches. If information stored on a computer is examined in the coded form it will appear in hexadecimal notation.

Normally this is not the way in which it will appear to the user because the computer 'converts' the hexadecimal to more readily readable text output form. This is sufficient for most purposes but in forensic analysis it is sometimes necessary to present the information in it raw, or hexadecimal, form. To do this one uses a program called HXD.EXE which copies the hexadecimal code contained in defined clusters to a second file. This can then be printed and is used to show the contents of a file in their entirety.

On task that will often be performed by a hex dump is to show the contents of slack space. However, hex dumps are now less frequently used. This is because specialist forensic software is increasingly available to automatically perform the function previously performed by a hex dump.

Q Whilst investigating a number of 3.5" floppy disks I was unable to read them using a standard 1.4Mb floppy disk drive in a PC. Why?

A The most likely reason is that the disks were not of the same format as that supported on the machine on which they were being read. This happens most frequently when a DOS based computer attempts to read Amiga or Macintosh disks.

Another possible reason is that you have encountered some floppy disks with a capacity exceeding that of the hardware with which you are trying to read them. Some program floppy disks have a formatted capacity of 2.8Mb and may not be readable on a 1.44Mb floppy disk drive. There are also floppy disks with a formatted capacity of 120Mb which need a special floppy disk drive in order to be accessed.

These larger capacity floppy disk drives are backward compatible, so if you can get one you should be able to use it to examine all capacities. If this is not possible then you may be able to read the disks by using the machine upon which they were created. But be very careful if doing this. Always boot the machine with a forensically sound boot disk and you may consider disconnecting the hard drive to ensure that evidential integrity is not compromised.

Two final points to bear in mind. Always set the write protect tag on floppy disks before any read attempt is made. And consider obtaining specialist forensic floppy disk copying software. This will read a wider range of formats without risk to the integrity of the information on the media.

Q I've heard the term 'logic bomb' used when referring to computer viruses. Is a 'logic bomb' a virus?

A The term logic bomb is used to describe a type of computer virus. It is defined as any program which initiates an action when triggered by a condition, such as the date, or the absence of an event performed on a computer.

For example, a logic bomb may be programmed to destroy valuable data should the programmer's name ever be deleted from a companies employee database. However, the action performed by a logic bomb does not have to be malicious in intent. It may just be that program's operation is altered by a change in the environment in which it operates.

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

Notice Board

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

Events

21st International Conference on Research and Development in Information Retrieval

24-28 August 1998
Melbourne, Australia

Contact: Keith van Rijsbergen
Email: keith@dcs.gla.ac.uk

IFIP World Congress

31 August-4 September 1998
Vienna and Budapest

URL:http://www.ocg.or.at/ifip98.html

Securing the future

The annual conference of the International Institute of Security.

26 and 27 September 1998
Basingstoke, Hampshire, UK

Contact Paula Tarr
Tel: +44 (0)1803 663275
Fax +44 (0) 1803 663251

California Association of Criminalists Fall 1998 Seminar

14-17 October 1998
San Diego, California

Contact: Jennifer Shen or Tanya Dulaney of San Diego Police Department
Tel: +1 619 531 2577

Forensic Science Society Autumn Meeting and AGM Interpretation of Evidence

30 October-1 November 1998
Sheffield, UK

Contact: Anne Holdsworth, FSS
Tel: +44(0)1423 506068
Email: Anne@fscisoc.demon.co.uk

Training

DIBS®Training in Forensic Computing

Over the past four years Computer Forensics Ltd, the originator and pioneer of the science of computer forensics and image copying technology, has progressively developed and run unique and comprehensive training courses in computer forensic procedures and techniques. Hundreds of candidates have participated in the courses.

Many are now skilled computer forensic practitioners in both government and commercial sectors; some now undertake training in forensic computing.

The success of the training methods used, in conjunction with the evolving nature of computer forensic science, has led to the expansion of the range of courses on offer:

Fundamental Computer Forensics, Applied Computer Forensics, Advanced Computer Forensics, Legal and Procedural Computer Forensics, Specialist Courses.

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

University Diploma of Criminal Investigation

Teaching carried out by the American University of Washington DC, the Paris International Centre of Forensic Sciences, and the University of Bordeaux.

Location: Bordeaux and Washington DC.

Contact: Prof. Doutremepuich,
Universite V. Segelen - Bordeaux 2,
146 rue Leo Saignat, F-33076 Bordeaux,
France.

Tel: (33) 5 57 57 12 68
Fax: (33) 5 56 98 76 70

National Training Centre for Scientific Support to Crime Investigation

Specialist training courses tailored to customer needs, delivered in the UK and overseas.

Accredited by ACPO, National Police Training, Durham University and the Open University (UK)

Contact: NTCSSCI, Co Durham, UK
Tel: +44(0)1388 762191
Fax: +44(0)1325 742509

Subscription Form

Send completed form to **International Journal of Forensic Computing, Colonnade House, High Street, Worthing, West Sussex BN11 1NZ, UK.**

Please enter my subscription to International Journal of Forensic Computing at the rate of:

□ UK £186.00 □ Europe £216 □ International £236.00

Name..
Position..
Company..
Address..
....

□ Cheque attached (make payable to International Journal of Forensic Computing)

□ Please invoice my company quoting purchase order no..

□ Please debit my credit card: VISA/ Mastercard/AMEX

Cardholder's name....................
Card No. ....
Expiry date..............................
Signature.................................
Date..

International Journal of
FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd.