ISSN. 1363-6650

FEBRUARY 1998
Issue 14

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

On the face of it, it's a minor transgression. Internet service provider America Online gave out some personal details of a customer, a sailor, to an investigator from the US Navy, causing red faces and a civil law suit.

The story hit the headlines mainly because of the suggestion that the sailor had written that he was gay in a personal profile, but the real issues are far more wide reaching than this superficial level.

In most modern societies, just about every part of our lives is documented, recorded and cross-referenced using computers. There are databases storing everything from our medical records and educational achievements to our driving licence details and bank accounts.

A large part of our daily lives, both private and public, is collected on a computer somewhere. Most of us accept this with alacrity and assume that once more technology is making our lives easier. This is fine, and certainly the days of paper records, which easily lost or altered, are certainly over.

In the business world, information is a currency in its own right – many firms will pay handsomely for details about where we live, what we earn, what we like and so on.

Using the Internet has a similar effect. Logging onto a web page can tell a computer somewhere a whole host of details about you, such as what computer you are using, what software you've got and sometimes what sites you've visited. This can reveal an awful lot about an individual and, argue those collecting the information, help provide a better service to the customer.

Many of us will happily fill in online questionnaires that some sites require to access them, thinking that information will be locked away or used in some anonymous market research project.

Maybe. The trouble is there is an awful lot of information floating around, much of it highly personal. Would you tell a complete stranger in the pub what your salary was, where you lived and that you had a powerful computer in your living room? No? There are almost certainly a considerable number of databases in private hands that have that information.

Despite the promises and guarantees of those who hold this data, it can and does leak out, as Timothy McVeigh found out to his cost (see page 12). AOL said this was a "human error".

There are laws which aim to protect privacy, such as the Electronic Communications Privacy Act in the US and the Data Protection Act in the UK, which are fine in theory but still can't stop serious transgressions in the real world.

The tide of personal information available through online networks is rising fast, and such breaches as McVeigh's will become more commonplace.

The only way of stopping it is to take data security seriously. That means prosecuting those firms, online companies and government or local agencies that flout the law and let information leak out.

There is a place for officials to see personal details as part of a bona fide police or law enforcement investigation, and this will be accompanied by the correct authorisation such as a subpoena or warrant. But computer databases should not be considered as a repository for just anyone to dip in and out of at will.

There is too much at stake to be lax and those acting as the guardians of information have to get their house in order or risk losing both their status and the public's confidence.

News

Reject spam ban, say lobbyists

Politicians in the US have been urged to carefully think about the implications of a bill aimed at banning most forms of junk e-mail.

At a Washington State Senate hearing on Senate Bill 6434, which would prohibit most forms of unsolicited commercial e-mail, Jerry Sheehan, legislative director for the American Civil Liberties Union in Washington State, spoke against the proposals.

Sheehan said: "This bill is not about junk e-mail. This bill is about controlling the Internet."

During the hour-long hearing, Sheehan and associates were the only speakers against the bill. A long line of users, Internet Service providers, an assistant attorney general, and an attorney, supported the bill.

One proponent of the bill urged the lawmakers to not only pass it, but to implement it as emergency legislation, providing several hundred pages of spam to illustrate the problem.

Edward J. McNichol, owner and operator of McNichol.com, defended the bill, saying "The First Amendment guarantees no person the right to hijack my private business tool and subvert it into a public forum for their financial gain, in my home and at my expense."

Senate Bill SB6434 and the identical House Bill HB2752 would amend the State's consumer protection act.

Under the new provisions, Washington State residents could claim actual damages or $500 per message, whichever is greater.

A Washington State Internet service provider could claim actual damages or $1,000 per message, whichever is greater and the bill would also stop unsolicited e-mail from being sent from computers within the state.

The legislation does allow for some unsolicited messages to be sent legally, although under the rules it must contain the word "Advertisement" as the first characters in the subject field and it must contain the legal name, mailing address, true e-mail address and telephone number of the firm involved.

The bill is currently in the Washington State Senate's Energy and Utilities Committee. The text of the bill can be found through the Washington State Legislative Web Pages at http://leginfo.leg.wa.gov

AOL steps up fight against junk e-mailers

Internet service provider America Online is continuing its tough policy on unwanted junk e-mail by suing two US firms.

AOL says the Michigan companies, LCGM Inc. and Web Promo Inc, were responsible for the transmission of thousands of unsolicited messages advertising pornographic sites on Web.

The suit, filed January 22 in the US District Court for the Eastern District of Virginia, asks for an injunction to prevent the companies from sending junk e-mail to AOL subscribers.

The suit also seeks damages from both companies, which it says are owned and operated by the same individuals.

AOL claims that both of the firms forged references to its domain name, aol.com, in their junk e-mail messages.

The use of such forged references, a practice that has become increasingly common among junk e-mailers, is designed to hinder AOL's ability to detect and filter such unwanted e-mail, AOL spokeswoman Tricia Primrose said.

She added that the unauthorised use of aol.com by spammers is designed to mislead AOL members into believing that the junk e-mail originates from AOL.

Although AOL demanded that both companies stop sending unsolicited bulk e-mail, the companies persisted in using deceptive techniques to circumvent AOL's e-mail filtering technology, the suit said.

Recently AOL also filed suit against three other alleged junk e-mail firms, IMS of Knoxville, Tennessee; Gulf Coast Marketing of Baton Rouge, Louisiana; and TSF Marketing and TSF Industries of Riverside, California.

According to the suit, the three companies have sent AOL and its members "tens of thousands of unsolicited and unwanted e-mail messages."

Despite demands by AOL that the companies stop sending unsolicited bulk e-mail, "each company not only refused to stop their mailings, but used a number of deceptive techniques designed to evade AOL's junk e-mail detection and filtering mechanisms, including forging aol.com within their e-mail messages," Primrose said.

AOL is also charging in this suit that TSF Marketing and TSF Industries violated the Computer Fraud and Abuse Act in their harvesting of AOL screen names.

The suit against IMS, Gulf Coast and TSF followed a federal court ruling in favour of AOL against junk e-mail firm Over the Air Equipment, Inc.

In that case, AOL won a court order barring Over the Air Equipment from sending unsolicited e-mail to AOL members. Later, Over the Air Equipment dropped its challenge to the order barring it from spamming and agreed to pay AOL a substantial sum of money in damages.

EU gives go ahead on Internet police

The European Commission is looking at ways of using computers to combat organised crime and examining the issue of tapping suspect e-mail. While general sweeps of the Web and the Usenet are currently allowed under EC law and member country legislation, tapping specific e-mail messages is prohibited.

In the UK, for example, e-mail is classed in the same category as voice telecommunications and, as such, is protected under the Interception of Communications Act, a law that is paralleled in all EC countries.

There has been growing concern that criminals - from organised crime gangs to paedophile rings - can use modern encryption techniques to flash encoded messages around the globe.

At a meeting held in the UK, and hosted by British Home Secretary Jack Straw, EC officials agreed to look at the possibility of removing e-mail from the same category as voice communications.

They stressed however, that any tapping of e-mails would have to be very

carefully controlled to prevent damaging the rapidly growing computer and Internet industry.

"There could only be such access under strictly controlled conditions and on the basis of demonstrable need," said an official.

Police access to e-mail would almost certainly require the use of a court order, a situation that currently applies to voice and data (including e-mail) taps in all EC member countries.

Having the EC approve such methods, however, would put the official stamp of approval on an otherwise grey area of police procedures, and would almost certainly increase the number of court orders issued by legal officials.

Mr Straw is also seeking to secure greater EU co-operation in policing criminal activity on the Internet - with round-the-clock contacts in each country to enable forces to respond rapidly to any threat.

New police computer training lab

A new training laboratory, claimed to be the first of its kind in the US, has been opened for law enforcement agencies in Pennsylvania.

State Governor Mark Schweiker and Police Commissioner Paul Evanko officially launched the Municipal Police Officers Education and Training Commission's computer laboratory training centre in Hershey.

The new 23-station lab offers free computer training to all employees of criminal justice agencies in the state, from court clerks through police officers to prosecuting attorneys. The training centre was created with funds from a $300,000 federal grant awarded to the Pennsylvania Chiefs of Police Association with the approval of the Pennsylvania Commission on Crime and Delinquency.

Evanko said the lab is equipped with 23 personal computers plus an instructor's station and all the machines are connected to the Internet.

The facility also features a 35mm slide projector and a special projector that can display the instructor's computer screen, VHS tapes and other materials.

Major Richard C. Mooney, executive director of MPOETC, said the training facility initially is focusing on the basics, such as introductory courses on personal computers, Windows '95 and the Internet.

He said the centre would offer advanced classes on topics such as how computers are used to commit crimes and how investigators can seize evidence of crimes stored in computers.

"We have to keep up with the criminals who are storing information about drug deals and other illegal activities in their own computers," Evanko said.

The computer lab expects to train between 100 and 200 students a month, with single and five-day courses.

Man found guilty of hate mail in test case

A 21-year old former student has been convicted in the first successful federal prosecution of a hate-mail crime.

A jury in the US convicted Richard Machado of Irvine, California, for civil rights violation after he used the Internet to send threatening "hate" e-mail.

Machado, a former student at the University of California, Irvine campus, faces up to one year in federal prison and a fine of up to $100,000 for sending the threatening e-mail to other Irvine students.

He was charged with the 1996 distribution of two separate batches of "racially derogatory messages" to Asian students. The 59 e-mail messages threatened to "find and kill everyone of you personally."

As Machado testified last week, he also sent messages to the campus newspaper staff in November 1995, because they favoured eliminating affirmative action programs on the campus.

The prosecutor told jury members the messages told the newspaper staff they would die in four days.

US Attorney Michael Gennaco said: "We feel that this (conviction) sends an important message to high-tech hate mongers who choose to use the Internet to threaten people's lives."

Douglas Mirell, a Southern California attorney, specialising in first amendment law is on the board of directors of the American Civil Liberties Union.

Mirell said that this is the second Machado prosecution. The first trial last November deadlocked 9-3 in favour of acquittal.

In this trial, the former student was found guilty only of interfering with students' rights to attend a public university. The second count was deadlocked.

"That's two counts, one conviction one hung jury," Mirell said.

"I would be very surprised if there wasn't an appeal and I would expect that the constitutionality of this conviction would be a significant issue in that appeal," he said.

He cautioned he has not looked at the actual evidence presented at trial but said he has read as many published reports as he could find.

Mirell talked about one of the flaws in the prosecution's case: "This threat was not filed against any one individual, but was a threat directed against a group of people.

"I'm concerned that this conviction flies in the face of three decades of contrary US Supreme Court authority," he said.

He specifically cited the 1969 case of Brandenburg vs. Ohio, when the court declared it unconstitutional to "forbid or proscribe advocacy of the use of force or of law violation, except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."

Workers' data sold on Net

A temp service in Japan is planning to sue a computer programmer for allegedly stealing data on about 90,000 women and putting it on the Internet.

Officials at Temp Staff Co, a major Tokyo-based temp firm, said the stolen data was shown on the Internet for three weeks.

Now the company is preparing to file a complaint against the 28-year-old man who is believed to have stolen the data last August.

The man, who was employed by

Temp Staff from March 1996 to October 1997, worked on computerising data on 90,000 women registered with the agency.

He is believed to have offered the data to an Internet home page company in exchange for not paying a 10,000 yen fee for his own Net page. The company then posted the information for sale on the Internet. Temp Staff first became aware of the situation earlier this month after receiving queries from publishers of weekly magazines who had seen the data posted on the Internet.

Prisons with pirate problem

Prison staff have been told to check their computers for pirate software after a UK jail was forced to pay out thousands for illegally copying programs.

The unnamed prison was forced to pay out £37,600 after an investigation by the Federation Against Software Theft found that 30 per cent of its software broke the law.

Jails in England and Wales now have until March 30 to check their systems and buy licences for programs which may have been illegally copied.

A prison service spokesman said: "The service treats this issue very seriously and measures to eradicate the use of unlicensed software have been devised and communicated to all heads of prison establishments."

"A mandatory Prison Service instruction on this matter has been issued for immediate action requiring prisons to carry out an audit of all computer software and obtain appropriate licences by 30 March.

"The Prison Service subscribes to the Federation Against Software Theft and is committed to ensuring that it correctly purchases all software before it is installed and that software is only installed in accordance with the licence conditions."

Officials also said there was a "common assumption" in the service that all software was covered by site licences, which would allow staff to make unlimited copies free of charge.

Digital signature talks in Congress

Politicians are warning that electronic commerce will be hampered unless a standard to confirm document authenticity is found.

Richard Baker, David Drier, and Bill McCollum, are cosponsoring HR 2937, the Electronic Financial Services Efficiency Act of 1997, which aims to establish common principles to govern e-business.

Baker said: "Although technologies currently exist to authenticate the identities of the parties using computers to affect transactions, the problem is that no national consensus has emerged over the development of laws governing the certification, validation, and use of such signatures.

"In particular, state efforts have been haphazard and unfocused, leading to laws ranging from the comprehensive to the limited to the non-existent."

He added: "To ensure that governments, businesses, and consumers can be confident that the transactions we engage in electronically are safe and secure, we must have a nationally uniform legal system governing the use of digital signatures and their authentication."

Stressing that H.R. 2937 promotes industry self-regulation, Drier said that "it is critically important...that the federal government encourage the private sector development of uniform standards for electronic authentication while not imposing rigid rules that may stifle innovation. It is equally important that any effort to pre-empt state digital signature laws does not accord such a pre-emption solely to one particular provider of authentication services."

According to Drier, under HR 2937, any person or entity seeking to offer electronic authentication services must be a registered member of the National Association of Certification Authorities, the self-regulatory body set up by the bill.

The purpose of the NACA, he said, "is to provide confidence to people using such services that the certification authority is trustworthy. It's like a notary's stamp of approval."

Noting that there is some concern that a single technology could dominate the certification authority, Drier added that he would support modifying HR 2937 to insure that non-NACA-certified providers of authentication services can also compete in the marketplace.

He said: "NACA will maintain a market-oriented approach to the regulation of electronic commerce by promoting a clear and predictable legal environment to insure that competition and consumer choice are the hallmark of the emerging global digital marketplace.

"HR 2937 places the responsibility for setting the rules governing the authentication and security of electronic commerce in the hands of the people most knowledgeable about that technology," he said.

"Only as that technology becomes more standardised and widely understood, and as problems arise that cannot be adequately addressed by a set of voluntary rules, should we begin to consider the need for direct government oversight or regulatory intervention.

FTC warns junk e-mailers

As far as the Federal Trade Commission (FTC) and the US Postal Service are concerned, junk e-mailers can spam, but they can't scam.

After examining over 60,000 dubious e-mail offers of get rich quick schemes, weight loss programs, easy credit and loans, and pyramid investments, the FTC and USPS put more than 1,000 junk e-mailers on notice that the agencies are monitoring and keeping track of unsolicited e-mail for fraudulent schemes.

"Fraud promoters should think twice before plying their trade on the Internet," Jodie Bernstein, director of the FTC's Bureau of Consumer Protection, said.

"First, the FTC is on the Internet beat and will follow up with spam artists who don't clean up their correspondence. Second, many consumers are already on to them - they know better than to believe promises from strangers."

Bernstein said the largest category of junk e-mail targeted by the FTC was chain letters.

"Pyramid schemes and chain letters make money only for the first few on the list," Bernstein said. "All the others lose their money. That's why pyramids and chain letters deceive consumers and are illegal under state and federal laws."

Chain letter schemes urge e-mail recipients to send a small amount of money to a list of several people, remove one name, add their own and forward the e-mail in bulk to others, she said.

"Theoretically, the participants will start to receive money as other 'downstream' recipients receive the e-mail and participate," Bernstein said, noting that economists estimate that about 95 per cent of pyramid participants lose their money.

Although a number of junk e-mail claims of quick riches claim they are legal, and cite federal regulations to prove their point, the USPS's Larry Maxwell said "don't be fooled by claims the US Postal Service has given approval for these schemes.

"Many letters provide the correct legal citation, Title 18, Section 1302, which negates rather than supports the legality of the scheme, Maxwell, who is manager of the Fraud, Prohibited Mailings, and Asset Forfeiture Group of the US Postal Inspection Service, said.

"We, as an agency never approve a solicitation, and recommend consulting an attorney if you contemplate such mailings."

Maxwell said that other categories of e-mail that received the warning message were business opportunity offers that appeared to be fraudulent cash grant schemes, deceptive diet and medical offers, credit repair scams, and suspect guaranteed credit card solicitations.

Both the FTC and USPS have kept copies of the warning letters for possible use in future law enforcement actions if the violations continue, Bernstein said.

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

The FTC recently published a new consumer publication about unsolicited commercial e-mail called "Trouble @ the In-Box," which offers examples of some common scams and provides tips on how to avoid them, Bernstein said.

The FTC also publishes a number of other consumer education publications, including publications on advance fee loans, credit repair, virtual health treatments, pyramid schemes, and investment scams available at http://www.ftc.gov

Bernstein added that if you've been the target of a junk e-mail scam, "contact your Internet service provider, your local consumer protection agency, your state Attorney General's office, or The National Fraud Information Center http://www.fraud.org

E C unveils net charter

The European Commission has announced proposals to create its own Internet charter, with the aim of clarifying the complex legal and technical issues relating to its use.

Unusually for the EC, however, the pan-European state government wants to discuss the details of the charter with other world powers, before laying down the charter's foundations towards the end of next year.

According to EC officials, the aim of the charter is to establish a framework under which EC member governments, as well as governments of non EC nations, can tie down legally grey areas, such as Internet pornography and spamming.

In its outline the EC claims that an internationally agreed framework is necessary to foster the development of the global electronic marketplace "by removing obstacles and uncertainties for businesses and consumers."

The EC claims that it is not looking to create yet another industry body with supervisory powers. Instead, the aim of the charter is to create a steering environment that will assist the entire Internet industry.

Last August, to support the discussions, the EC published a paper that called for a five-month public debate on how the EC must update EC and national legislation to take account of the growing "convergence" between the telecoms, broadcasting and computer sectors.

"One thing is definite, with the existing legal regulations, we won't be able to keep up," said Martin Bangemann, the EC telecoms minister, at the time.

The discussion paper, which was the forerunner to what is now becoming an EC Internet charter, highlighted the way that once distinct services such as TV, telephone, and online services, are now often carried on the same networks as each other.

The discussion paper noted that technology is already making it possible to watch TV or make phone calls over the Internet, to hook up to the Internet over TV sets, or to receive electronic-mail using mobile phones.

It now appears that new rules will be drawn up to add to current regulations to cover the latest technology.

South Africa hit by computer crime

South Africa lost an estimated R326 million to computer crime last year, more money than in robberies or heists, according to police statistics released this week.

The police's technical support unit, which investigates computer crime, is expecting an increase in offences,

And one national bank, which on average has one hold up a day at one of its branches, says it is losing more money through white-collar crime and hackers gaining access to accounts.

A report by the director of the technical support unit, Tiens Steyn, lists the assistance given by his unit to other police units to investigate crime involving computers.

Fraud and corruption investigated for the Cape Town branch of the Office of Serious Economic Offences amounted to an estimated R310 million. Its Pretoria office investigated an estimated $3.7 billion worth of international computer crime and fraud, committed by a South African-based organised crime syndicate.

The Organised Crime Unit in Cape Town investigated fraud estimated at R6 million and the Internal Security Branch's Pretoria office investigated one case involving an estimated R10-million.

A further loss of R204,000 was investigated in two cases in Pretoria and Nelspruit.

"Crime via computer is difficult to prosecute, because offenders sometimes know a great deal more about computer technology than do prosecutors, judges and even members of the police," Steyn says.

"As dependence on computer technology grows in South Africa and around the globe, it will be crucial to ensure that the rate of technological dependence does not outstrip the rate at which the corresponding social, legal and political frameworks are developing," he says.

"It is important to plan for security and crime prevention at the same time that computer technology is being implemented."

South Africa's computer systems are extremely vulnerable to computer crime for the simple reason that there is no law to deal with it.

A report commissioned by the Gauteng legislature to look into information technology and biotechnology was completed last year, and the South African Law Commission is currently looking at legislation to cover computer crime, which should be on the books by next year.

The new laws would make hacking into somebody else's computer or network without permission a crime.

Internet debate

Politicians appeared to be locked in a stalemate after discussing freedom of speech versus fear of online pornography.

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

"We can put a brown paper wrapper around Internet porn, while still protecting our First Amendment rights," Sernovitz said. "It takes a partnership between technology developers, government, and communities to solve this problem."

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

American Civil Liberties Union legislative counsel Gregory Nojeim, however, said that the ACLU recognises the "deeply felt concerns of many parents about the potential abuse of information on the Internet". But he added that the organisation "strongly believes" that individual Internet users must be given the right to access information, "and parents should not abdicate responsibility to the government for determining which information their children can see."

Both Sernovitz and Nojeim, however, found common ground in criticising Sen Daniel Coats' legislation, introduced last November, which would punish commercial online distributors of material deemed "harmful to minors."

Coats' legislation would impose criminal penalties of up to six months in jail and a $50,000 fine.

Sernovitz opposed Coats' bill "as being ineffective and highly destructive to the American principle of free speech," while the ACLU said the criminal penalties, which could be levelled against "distributors," could include such groups as the Amazon.com virtual bookstore or a promotional site for a Hollywood movie.

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

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

But trying to find a middle ground, Seth Warshavsky, CEO of Internet Entertainment Group, Inc., proposed that Congress mandate the creation of a new "adult" segment of the Web to help cordon off sexually explicit material and keep it away from juveniles.

Warshavsky's company recently made headlines after it won the legal right to air on the Internet a notorious "honeymoon video" featuring television actress Pamela Anderson and her husband, drummer Tommy Lee.

The video has been receiving upwards of 12 million hits per day, Warshavsky said.

The company also is currently engaged in a legal struggle to air another sexually explicit video of Anderson and former boyfriend, rock singer Bret Michaels.

Under Warshavsky's proposal, all current federal and state regulations governing sexually oriented content on the Internet and other interactive computer expression would be pre-empted by a new "adult act".

Anyone wishing to transmit erotic content, Warshavsky told Committee Chairman John McCain (R-Arizona), would be required to use an Internet address ending in ".adult," and bar entry to adult sites by minors.

Warshavsky said such barriers could include mandatory credit card usage, a pre-arranged personal identification number issued only to adults, or a pre-subscription agreement validated by an electronic signature.

In addition, Warshavsky's proposal would mean that every new computer sold in the US would require a V-chip capable of screening out any adult material. Parents would have control over whether the V-chip was enabled or not through a password or similar device.

The "adult act," Warshavsky said, would provide a legal "safe harbour" exempting individuals and companies who abided by the "adult" provisions from prosecution.

Warshavsky said the act was drafted with the assistance of John H. Weston, a prominent Los Angeles attorney who is considered an expert on Constitutional and legal issues surrounding erotic material.

"Our company provides sexually oriented content and Web services to adult subscribers who usually pay a fee," Warshavsky said. "I am here today to express my commitment, as a socially conscious American citizen and as the head of a responsible company, to comply with the law.

"I am passionately committed to the principles of the First Amendment, that adults should be able to make their own

decisions about what they want to see, read and view. But that commitment doesn't mean that my company or any other should permit a minor to have access to sexually oriented content which our society deems inappropriate for that minor without parental consent."

"Irresponsible people flood the Internet with sexual material without adequate barriers to stop minors from access to these sites," Warshavsky said.

"We must find ways to stop juvenile access which are sufficiently effective so parents feel comfortable with adult access. I want to be able to provide adults with erotic content, but only in ways that will be unavailable to minors."

Data mining combats fraud

Data mining technology helped insurance investigators ferret out a scheme in which fictitious companies billed for services that were never provided using the names of real doctors and patients. Data mining is an increasingly important weapon for insurance companies trying to fight all sorts of fraud.

The recent scam is just one form of medical insurance fraud. Fictitious companies got hold of the names of real doctors and patients, and submitted bills for services that were never performed.

These might include medical procedures, tests, ambulance rides, and the like. They keep the amount of each claim small enough that it does not trigger careful scrutiny.

In other cases, it is clinics, ambulance operators, labs, and doctors themselves who submit fake bills, said Ben Barnes, general manager of global business intelligence solutions at IBM, whose Fraud and Abuse Management System helped uncover the latest racket.

Joyce Hansen, vice-president of Integrity Plus Services Inc. in Minneapolis, said that Integrity Plus, an insurance fraud detection company, has been using the IBM system for four years and has caught many forms of fraud.

Integrity Plus has caught bills for services supposedly provided on Sundays and holidays, for clinics claiming to serve patients who live far away, and so on, Hansen said.

While it is difficult to say exactly how much the system saves, Hansen said that in the first year of its use, the claims savings from catching fraudulent billing increased 20 per cent.

Barnes said that the IBM system, designed in consultation with several customers in the insurance industry, looks at about 100 different characteristics of claims to spot patterns of abnormalities that might suggest fraud.

It might spot, for instance, the fact that a particular ambulance operator consistently claims longer runs than others in the same area. When something suspicious turns up, investigators can take a closer look.

Barnes admitted that the system cannot usually work fast enough to prescreen claims, so when a fraud is caught the insurer may have to take legal action to recover money already paid. However, the service provider who has been caught once will be watched more closely.

The fact that the technology exists to analyse claims looking for fraud will deter some would-be fraudsters.

Others will try to outsmart the system, and Hansen said that is already happening as the perpetrators of fraud change their behaviour in attempts to avoid detection. "They're learning those controls, and so they can bypass them," she said.

She added that she believes the detection technology can keep improving to stay ahead of the fraud attempts.

Most wanted fugitives on web sites

A new site on the Internet has been launched to try to catch fugitive criminals in the US.

Online publisher E-Ticket is running "America's Most Wanted Online" (http://www.amw.com) in conjunction with the Fox television series. The site fully integrates with the TV program, which airs Saturday nights in the US.

Features on the new site include the current week's cases, unsolved crimes, an APB system, an interactive crime map of the US and late breaking news.

"We're excited about the new Web site becoming a strong component of the show," says E-Ticket president Rick Gibson. "E-Ticket's goal has always been to bring existing and important communities online, and America's Most Wanted Online will be one of the few places where we can all truly make a difference."

- The Internet dragnet's most recent success in the US came when the mug of a man wanted in connection with a bank robbery on Dec 26 at a grocery store popped up on the Provo Police Department's fledgling web site (www.provo.org).

It didn't take long for the police hotline to ring with calls from the suspect's parole officer, a former employer and other acquaintances.

"We got a hit and scored the first time up," Lt. Greg Du Val said.

Police tracked the man to Las Vegas, where a suspect with a similar description had hit three banks. The FBI was able to get the man's photo from the Provo heist and positively identify the man, who remains in custody.

Provo has also posted photos of unidentified homicide victims in San Juan and Washington counties on its page and posted a composite drawing of a suspect in a December rape.

Provo information systems analyst Steve Bulkley was able to load video taken from the Provo bank robbery into the computer and e-mail copies to other police departments. Images can go from videotape to a home computer thousands of miles away in about 10 minutes, Bulkley said.

"It's a great tool. It's so immediate and so quick," said Provo Police Capt. Keith Teuscher.

The Utah County Sheriff launched a similar web site (www.co.utah.ut.us) last summer and Salt Lake City and Ogden police have expressed interest in using their web sites in the same way.

Jennifer Kibbie-Hiatt, a Salt Lake police information specialist said: "It's definitely a law enforcement tool."

The Salt Lake City police web site (www.ci.slc.ut.us) does have a photo gallery of the city's most wanted criminals - mostly suspected murderers - and brief descriptions of the crimes.

Product news

Hardware storage of encrypted keys

Two firms specialising in secure electronic commerce have teamed up to launch a hardware and software system to boost trade on the Net. US company CertCo has signed an agreement with SPYRUS, a provider of hardware cryptographic solutions, to incorporate the Spyrus Lynks Privacy Card into its CertCo CertAuthority Solution package.

The CertAuthority product suite incorporates hardware and software safeguards to protect the integrity of certificates. It uses sophisticated cryptographic solutions for the management of the root key and its certificate, certificate issuance and certificate revocation.

Tamper-evident hardware devices are used to provide protection of private key fragments, ensure a secure processing environment for trusted signatures, and support distributed control of the certification process.

The package uses the Spyrus Lynks privacy card, a PC card-based cryptographic module that can be inserted into the elements of CertAuthority(TM), to enforce secure operational staff access to critical certification functions such as certificate approval and certificate revocation.

This card features a number of high assurance capabilities, including on-card private key and random number generation, private key backup, and reader-based PIN entry.

"CertCo and SPYRUS have pioneered innovations in information security through distributed private key systems, which eliminate single points of vulnerability and failure," said Charles S. Walton, Jr., CertCo Chief Operating Officer. "This agreement allows CertCo to provide solutions that combine the cryptographic and technological innovations of both companies with the trust infrastructure provided by traditional banking transactions. These solutions can foster the rapid growth of global commerce, while enabling financial institutions to offer a new line of secure, high-value certification services to their customers."

"We are pleased to be providing CertCo with hardware-based cryptography that forms a critical element of the CertAuthority(TM) security architecture," said Sue Pontius, Spyrus CEO. "The combination of the Spyrus cryptographic products with the CertCo Certification Authority application creates a strong solution, as evidenced by its adoption by Visa/MasterCard for the SET Root CA and by the State of Utah's PKI with Digital Signature Trust Company."

For more information contact CertCo on +1 617 267 0042, ext. 331, e-mail tfrederickson@rourke.com or visit the web site: http://www.certco.com/

New firm to focus on digital commerce

PostLinear Entertainment, a network content developer, has launched a new company that will focus on technologies for the buying and selling of "digital objects" — products and services that exist only in cyberspace.

Transactor Networks Inc says it has developed Java-based products and services for multiple platforms that enable a marketplace in digital objects, such as commerce-ready business applications, component software, Java applets and services, digital coupon, and music, networked games and other media.

Ron Martinez, CEO of the US firm said: "Much of the industry's work in electronic commerce has so far focused on developing various pieces of technology to enable commerce in physical goods via the Net.

"Each of these technologies, such as SSL, SET, shopping carts and online catalogues, does a good job at its specific task. But until now, no one's adequately addressed the rapidly growing need for a programmable, e-commerce platform that enables a marketplace for digital products and services existing only in the digital realm. Transactor is that solution."

"We see the value of Transactor as a secure software transaction and distribution platform," said Mr. Toshio Nakanishi, General Manager, Solutions Division for ASCII Corporation, a leading Japanese publisher and distributor of CD-ROMs, books and magazines.

He added: "Safeguarding ownership of digital objects and preventing piracy on Internet communications are the next important steps in electronic commerce."

For more details contact the firm on +1 415 487 1100, or visit the web site at http://www.rsa.com/

Fraud busting system

UK firm Applied IT has taken the wraps off an enhanced version of its Fraud Management System for wireline and wireless telecom networks.

The company has already signed up four companies - Sita, Equant, Scottish Telecom, and Diamond Cable - to install FMS 1.3 on their networks.

Mike Jennings, a spokesperson for the company, said that the software is suitable for both wireline and wireless networks, mainly because the parameters relating to fraud are broadly similar on either network environment.

He said: "Our software looks for changes in the user profile of a subscriber, which may suggest a fraud is taking place. The software also looks for large numbers of short calls, which suggests that a hack is taking place, a number of very long calls, which suggests fraudulent calls may be taking place, or a series of high value calls."

According to Jennings, if a call or series of calls meeting the criteria are found on one or more accounts, the software takes appropriate action.

"Fraud is a major problem on telecoms lines. Industry estimates suggest that between five and 15 per cent of calls on networks are fraudulent in some way or another, but our figures suggest that the problem is nearer three percent," he said, adding that even three percent, of lost revenue is still a major problem.

"Many telcos dress up fraud as a different problem, preferring to call it bad debt or something similar, but it is a problem none-the-less," he said, adding that FMS has been designed to spot fraudulent telecoms activity.

According to Applied IT, FMS 1.3 processes and analyses high volumes of network traffic up to 60 per cent faster than version 1.0 and in much greater detail.

This means, the company claims, that new, sophisticated methods of fraud, which have previously gone undetected, can now be identified.

One of the key features of the new system is its Usage Variation Analysis facility, whereby accounts profiles are generated and analysed on a daily basis.

This enables the systems to detect irregular patterns, thus generating alarms indicating potential fraud.

With the development of its Usage Variation Module, Applied IT claims to have introduced an implementation of ideas taken from research into neural networks.

FMS 1.3 has been enhanced to cover cellular fraud problems, as well as virtual private networks, another fast-growing target market for the fraudster community, the company claims.

As the cellular phone market is one of the fastest growing targets for fraudsters, the company claims to have enhanced the software to allow customers to target cellular fraud faster and more efficiently.

As an example, the new version is now able to tackle the growing problem of SIM (subscriber identity module) cards being stolen and used in different mobile frauds.

According to Jennings, FMS 1.3 comes with an improved, more Windows- like graphical user interface, presenting data for administrators in a user friendly format. The package now runs under most versions of Posix compliant Unix systems and currently runs on IBM, DEC, HP, and Sun Microsystems.

For more information contact Applied IT +44-1628-890412, visit the web site at http://www.appliedit.co.uk

Better e-mail security

Worldtalk Corp has announced the availability of its WorldSecure Server 2.0.2, the latest version of its flagship e-mail security product.

WorldSecure Server features an e-mail security management engine designed to give customers greater control over security policies throughout their organisation.

The new features in WorldSecure Server extend key benefits to customers in the legal and healthcare industries enabling them to meet statutory requirements, facilitate secure communication and minimise liability exposure.

"Organisations are choosing WorldSecure Server to ensure compliance and privacy of their e-mail communication over the Internet," said Reynold Wong, WorldSecure product manager.

"WorldSecure Server is ideal for a number of industries that are looking to secure their messaging systems while enabling users to exchange sensitive information, such as legal contracts and patient records.

"The policy management engine is a powerful tool to enforce and manage e-mail security policies that are transparent to the end user."

WorldSecure Server, for Windows NT, is an e-mail firewall that protects corporate messaging systems and includes server-based S/MIME encryption and digital signature, virus scanning, Internet access control, content filtering, SPAM prevention, and security policy management.

For more information contact Worldtalk on 800 454 4674 or +1 408 567 5168 or visit the Worldtalk web site at http://www.worldtalk.com

Litigation support software for lawyers

US firm Executive Technologies Inc has introduced version 2.0 of SearchExpress Legal software.

SearchExpress Legal is a scanning and full-text retrieval system designed for litigation support at law firms and corporate legal departments. Its makers say SearchExpress Legal has the capability to search across hundreds of cases.

The new version includes the capability to search the database over the Internet or an intranet using an Internet browser.

And it also offers a CD-ROM publishing module, so the scanned images and data can be sent to co-counsel on CD-ROM, or taken into court on a portable PC with a CD-ROM drive.

One of the "secret" features, which the manufacturer says some lawyers using the product would prefer to remain secret for competitive reasons, allows one to stamp lines of text such as "Produced for Smith Case Subject to Protective Order", diagonally across each page in large grey-scale letters.

The image is still readable by the opposing counsel, but cannot be scanned in and read by computer successfully.

Another of the "secret" features allows one to re-sequence the bates numbers of produced documents, so the opposing counsel will not see gaps in the bates numbers and know there are additional documents they could request.

Other features include redacting, OCR Proofing, and private and public notes. Redacting allows attorneys to "white-out" portions of a page before the image is printed or placed on CD-ROM and given to opposing counsel or retained counsel.

The system allows complex searching techniques and will index and retrieve documents or objects in a wide variety of different file formats, including HTML, Acrobat, word processing, image, audio, or video format.

The program works on Windows NT and Windows 95 platforms. For more information contact the firm on +1 205 933 5494, e-mail eti@searchexpress.com or visit the web site at www.searchexpress.com.

Security for lawyers

A supplier of legal information in the US has teamed up with a digital certificate specialist firm to offer secure communications for law firms.

West Group announced an agreement with VeriSign, Inc, so lawyers can ensure client confidentiality while conducting business online.

Digital certificates allow lawyers to send encrypted messages and authenticate the identification of the parties conducting business.

Michael Baum, vice president, practices and external affairs at VeriSign, and chair of the American Bar Association's Information Security Committee, said: "Law firms can now begin to take full advantage of the opportunities the Internet has to offer, safe in the knowledge that their systems and information are secure.

"West Group is providing a critical service for the legal community, moving secure records, documentation and communication into the 21st Century."

He added: "This launch is particularly timely as digital signatures are increasingly being recognised by judicial systems both domestically and globally."

West's Legal Directory, West Group's online directory of legal professionals, will serve as the registration authority for issuing certificates and will maintain an online certificate repository for the entire legal profession.

Kevin Ritchey, director of West's Legal Directory, said: "Lawyers who have held off taking their practice online will now have the tools offering the security they need to send secure e-mail and documents across the Internet. "With digital certificates lawyers can identify themselves to the world as lawyers, and conduct business as usual, online."

Digital certificates serve as electronic credentials over the Internet for businesses and individuals and authenticate the sender of messages, encrypt messages, ensure message integrity and protect privacy on the Web.

For more information contact West Group on (US) 800 455 4565, e-mail ruven.schwartz@westgroup.com or visit the web site at http://www.westgroup.com

Law web site a hit with users

The Martindale-Hubble Lawyer Locator, at http://www.martindale.com, has surpassed four million searches on its database for information about lawyers and law firms since its initial launch.

Publisher of the system, Louis Andreozzi, said: "The Martindale-Hubbell Lawyer Locator is the definitive Internet resource for finding information about lawyers and is now averaging more than 25,000 searches per day.

"Crossing the important milestone of four million searches illustrates that we are providing a valuable resource on the Internet for people both inside and outside the legal community."

The web site is linked with some of the other leading Internet sites for legal professionals, such as LEXIS-NEXIS Exchange (http://www.lexis.com), Law Journal EXTRA! (http://www.ljx.com), FindLaw (http://www.findlaw.com) and America Online (keyword: legal).

"Based on the feedback we've received, users have been equally impressed with the Lawyer Locator's speed, efficiency and reliability for retrieving lawyer and law-firm profiles from the Martindale-Hubbell database," said Andreozzi.

The pages are a reference source consulted by corporate legal staff and lawyers for information about the professional qualifications and expertise of attorneys and law firms around the world.

For more information contact the firm on (US) 800 526 4902.

Surf in safety, says phone company

Pacific Bell Internet Services has launched a new public service campaign to provide parents with an informed look at safety issues surrounding the Internet.

Safety Net will provide advice and information that enables parents tackle issues such as access to inappropriate materials, online crime, chat room interactions and secure business transactions.

"Our goal is to make it easy for every Internet user or potential user to access the information they need to safely use the information superhighway," said Steven Hubbard, president and CEO of Pacific Bell Internet Services.

To get the free Safety Net brochure, write to Pacific Bell Internet services, c/o Fleishman-Hillard, 595 Market Street, Suite 2700, San Francisco, CA 94105. The information can also be accessed online at http://www.pacbell.net.

New telecom fraud detector

International provider of billing systems Amdocs has unveiled a fraud detection and control package for the cellular and landline telecommunications industry.

Norman Rafalowitz, Amdocs' senior vice president, said that telecoms fraud is one of the fastest growing industries in the world, mainly since it is one of the most profitable of illegal activities, yet is relatively risk free.

He said: "With current estimates that the problem is costing the world's telcos – telephone companies - about three percent of their total revenue and increasing, every telco will have to become actively involved in combating fraud in order to control losses and protect the corporate bottom line."

According to Rafalowitz, Amdocs has joined the fight against telecom fraud by providing cellcos and telcos with tools to fight fraud and to control fraud related losses.

The software is claimed to use artificial intelligence capabilities to detect abnormal usage behaviour that indicates that fraud is being committed.

The system creates a profile of each individual subscriber's "normal" usage behaviour. This profile is based on an analysis of call detail records (CDRs) received from the switch.

These individual usage profiles, the company claims, are continuously updated and analysed on a call-by-call basis. Behavioural deviations fall into different patterns which are indicative of specific types of fraudulent activity. Any deviation from the normal usage behaviour of an individual subscriber is closely monitored.

When a problem occurs, a prioritised fraud alert is generated for review by telco fraud investigators.

In addition to individual subscriber behaviour monitoring, the system has the ability to monitor the behaviour of any network-related entity, such as lines and switches. This "network entity" monitoring capability significantly expands the scope of fraudulent activities that can be detected by the system.

According to Amdocs, the software features a comprehensive set of pre-defined fraud discovery rules. These rules are used to automatically detect every type of known fraudulent activity such as subscription fraud, cloning, tumbler phones, hacking, calling card, call selling, 900/800 number fraud, and dealer fraud.

Amdocs' Web site is at http://www.amdocs.com or phone +1 314 821 3242, e-mail info@amdocs.com

Electronic privacy

A row erupted after Internet service provider America Online gave out personal details of one of its customers, resulting in a sailor being threatened with discharge from the US Navy. **Paul Johnson** looks at the case and its implications for confidentiality and the right of law enforcement and government agencies to gather such details.

Timothy McVeigh was an anonymous senior chief petty officer in the Navy before the story broke. Now he has become one of the centrepieces in the row over just how far the state can go in gathering personal and sensitive information.

The saga started when Navy officials decided to discharge McVeigh, a 17-year naval veteran serving aboard a submarine, under the guidelines of the military's controversial "don't ask, don't tell" policy over homosexuality.

The Navy said it plans to discharge McVeigh because it learned that a biographical profile connected to an alias screen name he used on his AOL e-mail account listed "gay" under marital status. Military policy allows homosexuals to serve in the military as long as they don't publicly state their sexual preference.

McVeigh, 36, no relation to the Oklahoma bomber of the same name, had used his AOL account to e-mail the wife of another sailor about a children's holiday gift drive. His AOL screen name, Boysrch, prompted her to check the profile he had posted. Under the name ''Tim,'' it listed marital status as ''gay.''

She notified the Navy and an investigator contacted AOL and learned the profile was McVeigh's.

Infuriated and shocked, the sailor filed a lawsuit charging the government with violating an electronic privacy law. After he filed suit, his discharge was postponed.

His suit charged that Naval investigators violated the federal Electronic Communications Privacy Act (ECPA), when they requested and received confidential subscriber information from AOL without a court order. ECPA, which became law in 1986, bars Internet service providers from knowingly releasing personal information on subscribers to law enforcement officials without a court order.

After several hearings, US District Court Judge Stanley Sporkin made a landmark decision in the case when he told the Navy McVeigh could not be barred from the Navy until the court case was over.

Judge Sporkin issued the permanent injunction preventing the discharge of McVeigh, three days after issuing a preliminary injunction pending the hearing.

The US Navy, however, reserved the right to appeal the injunction in the DC Circuit Court of Appeals.

Sporkin said: "this court finds that the Navy has gone too far. In these days of 'big brother,' where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalised, it is imperative that statutes explicitly protecting these rights be strictly observed."

In a statement Sporkin wrote: "The government knew, or should have known, that by turning over the information without a warrant, AOL was breaking the law."

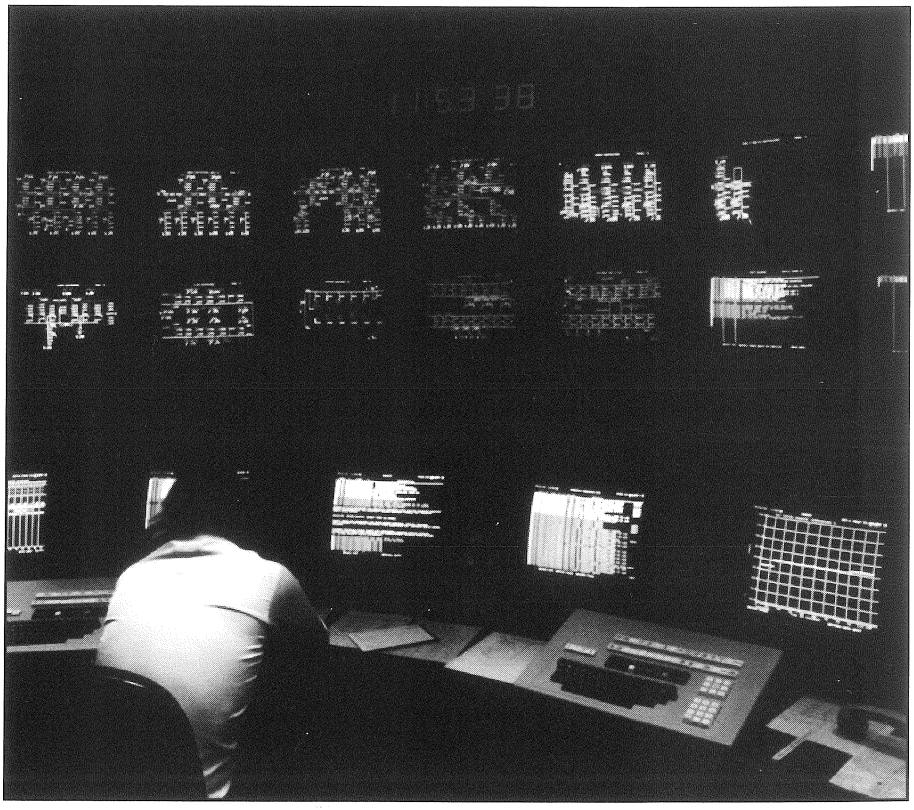
"Yet the Navy, in this case, directly solicited the information anyway. What is most telling is that the Naval investigator did not identify himself when he made his request."

"Suggestions of sexual orientation in a private, anonymous e-mail account did not give the Navy a sufficient reason to investigate to determine whether to commence discharge proceedings," Sporkin wrote.

Sporkin also was critical of AOL, saying the online service also broke the law.

He said: "The government knew, or should have known, that by turning over the information without a warrant, AOL was breaking the law,"

Sporkin wrote. "Yet the Navy, in this case, directly solicited the information anyway. What is most telling is that the Naval investigator did not identify himself when he made his request."



McVeigh declined to say whether he would pursue legal action against AOL, saying he first wanted to resolve his discharge suit against the Navy.

Judge Sporkin, however, remarked to McVeigh in court that "it seems you certainly have a good case against AOL."

The permanent injunction "is a huge victory for McVeigh," Dixon Osborn, co-executive director of the Service Members Legal Defence Network said.

"What Judge Sporkin's ruling means is that after reviewing the merits of the case, he determined that the Navy violated the Electronic Communications Privacy Act (ECPA), as well as the limits on investigations under the Navy's 'don't ask, don't tell, don't pursue' policy."

"This is the first time a federal court judge has said that the Navy has failed to follow its own rules and regulations under that policy," Osborn said.

McVeigh's lawyer, Christopher Wolf, said the case had implications for every other Internet user.

He said: "It raises the issue of the government's right to obtain information from Internet service providers like AOL without a warrant and without a court order as required by federal law.''

'Online services promise privacy to their subscribers, and a contract is a law."

He added: "It was only the government calling AOL and getting information which linked him to the profile which allowed them to conclude he was gay. The Navy shouldn't have asked for the information and AOL shouldn't have given it out.''

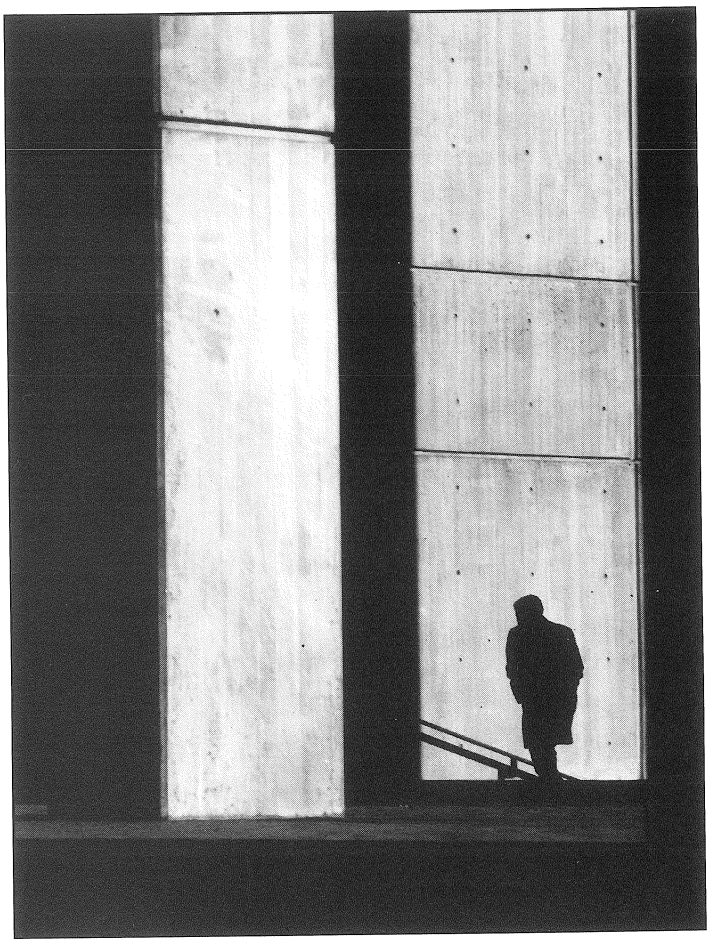
The case is "significant for anybody concerned about the ability of the government to obtain personal information from online services without a court order," he said.

"He (McVeigh) is delighted that what the Navy did has been recognised to be unjust," he added.

AOL, which promises users it will not disclose personal information unless compelled to by law, admitted a customer service representative had violated company privacy policy by revealing to Navy investigators McVeigh's true identity.

"Our member services representative did confirm information presented to him by the Navy," AOL officials said in a statement. "This clearly should not have happened and we regret it."

The statement came at the end of AOL's investigation into the company's role in the affair.



AOL is attempting to deflect criticism in the case, saying that government investigators did not follow customary procedure of obtaining a court order or subpoena that AOL typically requires before it releases account information.

"We have a clear policy in place to protect private information," said AOL spokeswoman Tricia Primrose. "We're disturbed that the government may have circumvented customary channels in acquiring this information."

AOL admitted "human error" on its part, but accused the Navy of misleading its customer service representative "both by failing to disclose his identity and purpose and by portraying himself as a friend or acquaintance of Senior Chief McVeigh's."

At a discharge hearing last November, naval investigator Joseph Kaiser testified he spoke with a "gentleman named Owen" in America Online's technical services, and asked to confirm the ownership of the profile.

AOL said the company plans to institute "additional measures" to enforce the company's privacy policies and procedures.

And it has also sent a letter to the Department of the Navy, expressing its concern that "the Navy deliberately ignored both federal law and well-established procedures for handling government inquiries about AOL members."

"In light of this situation, we are instituting additional measures that will reinforce our privacy policies and procedures to our member services representatives," AOL officials said in the statement. "This was a case of human error under very unusual circumstances. We want our members to know that privacy is of paramount importance to AOL and we take our responsibility to protect it very seriously. We will do everything we can to maintain that commitment."

According to AOL, the customer service representative who handled the phone call voluntarily left the company several months ago.

McVeigh's case is a hugely important test of electronic privacy laws, said David Sobel, legal counsel to the Electronic Privacy Information Center.

He said that the outcome of the case could become a precedent for government use of e-mail and other potentially damaging personal documents. Whistleblowers and others who want

anonymity would be at risk.

"A lot of people assume that only people who are doing something wrong or illegal want the ability to remain anonymous. That is a real misconception,'' said Sobel.

"The information was received from AOL in clear violation of ECPA, which prohibits the government from obtaining `information pertaining to a subscriber,' without a court order or subpoena."

"And in addition to the privacy protections contained in ECPA, AOL's contractual `Terms of Service' prohibit the company from disclosing such information to any third party `unless required to do so by law or legal process,'" he said.

"This case is an important test of federal privacy law," Sobel said. "It will determine whether government agents can violate the law with impunity, or whether they will be held accountable for illegal conduct in cyberspace.

"All the industry sees is the upside of collecting private information," Sobel said. "But this is a wake-up call that in the rush to collect this information, there also must be safeguards in place to secure that information."

Sobel added that the incident also raises serious questions concerning the adequacy of contractual privacy protections like those contained in the AOL subscriber agreement.

John Aravosis, an Internet expert helping McVeigh, sent e-mails to news reporters with the return address Navysex1. It was a spoof.

The point, Aravosis said, was that AOL e-mail addresses and member profiles ''are not always what they appear. For the Navy to assume so in the McVeigh case, and use such an assumption to destroy a man's career is criminally negligent.''

The Navy, whose response to the case has been muted, said that it had gathered enough evidence to begin McVeigh's discharge on homosexuality grounds even without the AOL-provided information.

"There was no intentional violation of any federal laws or regulations by Department of the Navy personnel," a Navy statement said.

After the Navy discovered McVeigh's identity, it removed him from his position as the senior enlisted man aboard the USS Chicago, a nuclear-powered attack submarine based at Pearl Harbour.

The Navy spokesman said McVeigh, a highly decorated enlistee, was moved to a submarine squadron where he is now in charge of developing a "comprehensive naval publication warfare library."

McVeigh said he holds "no animosity" toward the Navy and looks forward to continuing his Naval service.

Net community feels effects

Although the Electronic Communications Privacy Act, or ECPA, does make the disclosure of information illegal, there are no immediate punishments or deterrents for transgressors.

The ECPA, passed in 1986 to guarantee privacy of electronic communications, was updated in 1995 to address the explosion in popularity of the Internet.

Victims can file a lawsuit, following in McVeigh's footsteps. But that takes both time and money.

And the law doesn't in any way provide a mechanism to exclude from criminal or civil proceedings information obtained in violation of the act.

"I think everyone is learning. The courts are learning. Users are learning. We are learning how to deal with it," said Tim Brady, executive producer and vice president of production for Yahoo! Inc. "Everyone is concerned, and at some point a balance will be struck."

Other Internet companies contend that law-enforcement officials, private investigators and other information seekers have tried similar ploys to get data about customers.

"We've had the police try and schmooze us or get in good with our security guards. But we are careful when they ask us for certain stuff," said Steve Dougherty, director of Internet operations for Earthlink Network Inc. "We have all watched 'The Rockford Files.' We know that is how things use to work. We have to be careful that doesn't happen."

Henry Smoak at Net service provider Mindspring Enterprises Inc said the situation should never arise.

"This really could have happened to anyone," said Smoak, a manager for Mindspring, in Atlanta.

"So we just notified all of our staff about our privacy policies, just as a reminder that this is one of the reasons we don't give out that information."

If only it were that simple.

Despite assurances from ISP's that every effort is made to protect personal information, people are still concerned about on-line privacy. Internet legal experts question the effectiveness of corporate policies and federal privacy laws in the age of cyberspace.

With the Internet constantly changing in size and scope, on-line companies are still learning how to handle the volumes of information left in their keep. Meanwhile, federal privacy laws are riddled with loopholes that offer victims few remedies.

"It is a substantial problem and one of the reasons why so many people are resistant to the Internet," said Jane Hughes, professor of law at the University of Indiana.

"What we have to do is either create a body of laws or an enforceable set of contracts with the company for consumers regarding privacy policies."

"This case highlights many things," said Deidre Mulligan, staff counsel for the Center for Democracy and Technology, a civil rights organisation based in Washington DC.

She said: "It highlights that if appropriate steps are not taken to ensure that federal agencies and on-line service providers comply with federal laws, then once information is released, people don't have too many effective remedies."

RSA conference

A record number of people attended the four-day RSA Data Security Conference in San Francisco in a comprehensive review of the state the industry.

The conference, which drew about 3,000 participants from around the world, more than 150 speakers and 68 exhibitors, is one of the keystone events of the data security calendar.

As businesses seek to take advantage of the global spread of the Internet and other public and private networks, their security needs for both commerce and communications offer significant opportunities for the data security field.

From online banking to global export controls, from the future of smart cards to encryption during the Renaissance, cryptographers, executives, customers, software developers and analysts looked at their businesses from different angles.

A number of key themes evolved as central to the data security industry:

- Calls for intensifying the battle against export controls and domestic restrictions on encryption technology.
- Public education about data security as a tool for crime prevention.
- Moves within the industry towards offering interoperable, standards-based products, based on APIs, to enable plug-and-play security solutions.
- Growth in the number of new security products and technologies entering the marketplace, including digital certificate technology, encryption tools and new firewall programs.

The long-running battle in Washington over federal restrictions on the export of encryption technology and products promises to heat up in 1998, which various conference speakers called the most important legislative year yet for encryption technology.

Congress is expected to be the battlefield as opponents of export controls, led by the computer and software industries and civil liberties groups, continue the war against control supporters - primarily federal law enforcement agencies and the Clinton Administration.

Jerry Berman, a panellist and executive director of the Center for Democracy and Technology in Washington, said that despite early Congressional successes, the once-growing tide to remove export controls and ensure that controls are not imposed may be waning.

He pleaded for more active lobbying, noting that without a "door-to- door" fight in the halls of Congress, America will find itself with domestic controls on encryption, as well as on export.

"You can't pass this legislation without help from the industry," said U.S. Rep. Bob Goodlatte who along with Sen. John Ashcroft spoke to the assembled cryptographers and security experts, while Rep. Zoe Lofgren was also present.

They discussed the Security and Freedom through Encryption (SAFE) Act. The bill was originally drafted to expand the industry's and individual's right to manufacture and export software with encryption to customers outside the US. "Americans must be free to communicate privately, without the government listening in," Ashcroft, chairman of the Senate Judiciary Committee's constitution, federalism and property rights subcommittee, said.

"For government agencies to have the keys to computer communication is like mandating that house keys be left on deposit with Uncle Sam."

The computer industry must get involved if it wants Congress to pass encryption reform, delegates at the RSA meeting were told. At present, companies have to apply for a license on a case-by-case basis, and often licenses are not granted for the more secure methods of encryption.

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.

The speeches from the members of Congress were half progress report and half reverse lobbying. "We are going to push hard to educate those not up to speed on this issue," said Ashcroft, "but we need industry support."

Encryption is a technology for scrambling data so that only the user with the proper "key" can access it. The technology enables secure financial transactions in E-commerce and enhanced privacy for individuals, with applications ranging from securing cell phone lines to personal-computer data.

Unfortunately for the government, encrypted data is secure from even its prying eyes - a problem for law enforcement and intelligence organisations.

At nearly every keynote, Q&A and panel discussion on the conference's first day, fear and disdain toward government policy on encryption – particularly export limits on strong encryption and FBI director Louis Freeh's call for a system of mandatory key escrow in the US – boiled over with heated debate.

While the FBI has been criticised for its support of encryption controls, one of its agents, computer crime specialist Dan Nielsen, made a special plea that the audience regard his agency as an ally. While he acknowledged mistrust among the industry for the FBI, he vowed that in the case of criminal incidents, companies could count on him for help.

He also warned that the sources of much data crime can be found inside the companies themselves, among disgruntled staff or temporary workers with unrestricted access to sensitive data.

"This has been a truly exciting and fast-paced week," said Charles R. Stuckey, Jr., chairman, president and CEO of Security Dynamics Technologies, Inc. "This conference continues to be the crossroads where members of the security industry meet. The explosive growth of the conference is additional proof that computer security is becoming mainstream."

Next year's event will be held at the San Jose Convention Center, Silicon Valley, from January 18-21, 1999.

RSA Data Security Inc, is a supplier of security components and related developer kits and provides comprehensive cryptographic consulting services.

RSA can be reached at http://www.rsa.com.

Product - first impressions

Disksearch MK II – Data Investigation Software

Here two investigators working day to day with computer evidence give their impressions of this piece of software. The Journal will be examining the program further in a future issue, with an in-depth review along with investigative software from other manufacturers.

By Paul Gillen and Noel Wade

Introduction

Disksearch MKII is a search utility that quickly and accurately searches any IBM PC compatible floppy disk or hard disk (up to 8GB). It is very useful on a search site where a large number of computers are located as it will quickly identify which computers contain information relevant to the investigation.

It was developed in early 1992 in co-operation with US and Canadian law enforcement agencies.Among those already using DiskSearch are the FBI, the US Attorney General's office, and the Royal Canadian Mounted Police. The product is marketed solely by its author William A Haynes.

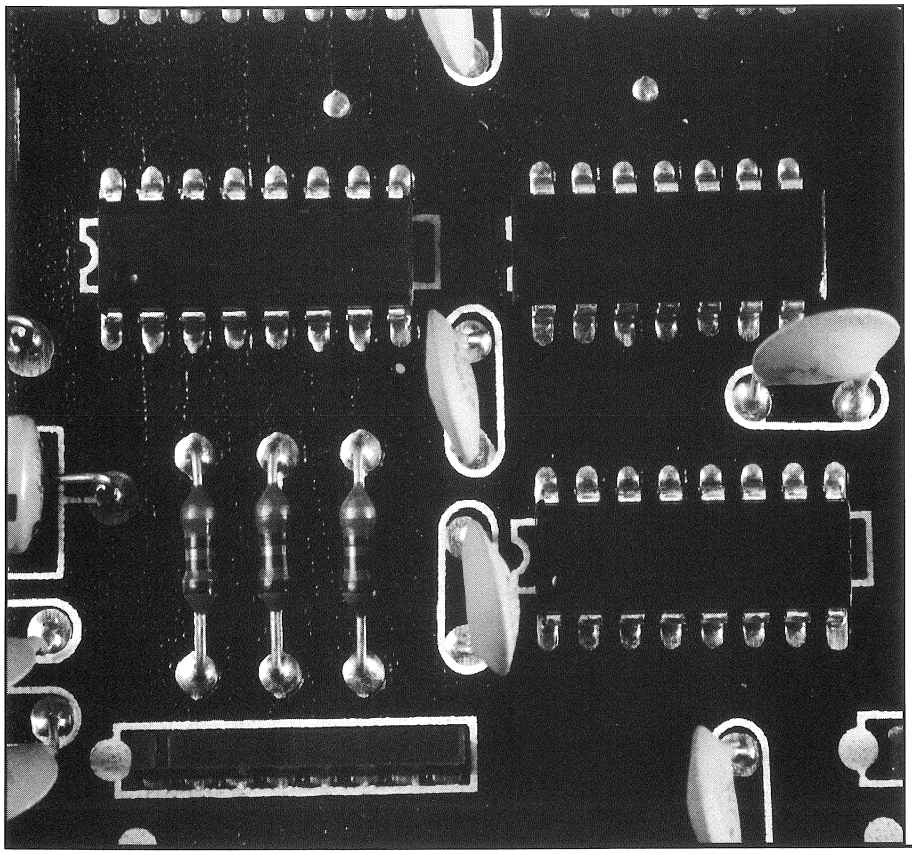
Requirements and compatibility

DiskSearch MKII is compatible with all PC/DOS versions 3.1 and above. On most systems 380K of available RAM should be sufficient memory.

How DiskSearch MKII works

DiskSearch MKII is a menu driven DOS program. The main menu consists of the following selections: Drive, Source, Options, Begin, View, Help, About and Quit. The Drive selection opens a submenu used to designate which disk drive will be searched. It contains selections for physical hard drives, floppy drives and DOS volumes (logical drive e.g. C:).

The Source selection allows you to specify that search strings will be either entered from the keyboard or read in from a text file.



The Options selection allows you to decide whether output from the search will be sent to the screen, the printer or a file. If output to the screen is turned on, the search will be suspended each time a match is found and open a window showing the match's physical location (e.g. logical sector 63, offset 32) and its logical location (file name or system area, e.g. C:\Notes\src-code.doc).

Reports sent to a file or printer are identical except for page headers containing a copyright notice and the name of the device being searched.

The Begin selection commences a search. If you select a file as the Data Source you will be asked to enter the name of the file. DiskSearch will read the file and display the serach strings allowing you to review, edit or add to them.

If the keyboard was specified as the data soruce you can enter up to 256 search strings and specify the percentage of accuracy at which to search for each.

Using "fuzzy logic technology" prevents mis-spellings and typos from causing data to be missed. It also allows data to be located when the correct spelling of a key word is not known, e.g. McGuire vs McGuire. To minimise time spent reading disk data DiskSearch MKII searches for multiple items in a single pass.

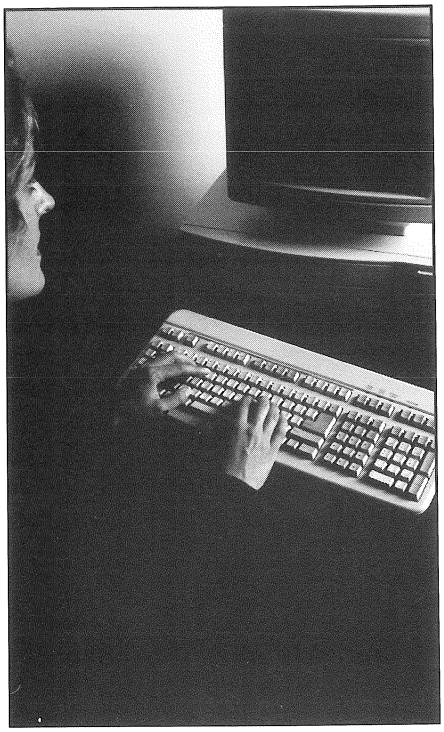
The View selection opens a Sector viewing window providing a quick and easy way to view any sector on the target device. It also allows the previous or next adjacent sector to be viewed.

The Help selection contains information on using DiskSearch.

The About selection provides information about DiskSearch including the version being used.

Features

- To preserve the evidence, absolute protection of data on the target disk is provided by special, system wide, write protection installed automatically each time DiskSearch runs.
- It is case insensitive, seeing and displaying all letters as uppercase.
- According to literature provided, hit locations are now explicitly identified in the following areas: DOS Volume



search mode – boot area, primary and secondary FATs, root directory, partition slack, file slack, unused clusters, bad clusters and lost chains.

Hard disk search mode – master boot record, MBR slack, unpartitioned space, DOS, Xenix, Disk Manager, Novell, CP/M partitions, DOS extended partition tables and extended partition header slack.

- Accompanying program called PARTNTBL, which reads partition table data (including extended partition tables) and prepares a list of all partition table entries for the entire system.

Limitation

A limitation of DiskSearch II is that it does not provide 100 per cent system wide write protection on a target machine operating under Windows 95. However, software for this purpose known as Writeblock for Windows 95 is currently being developed by New Technologies Inc. Contact NTI at 2075 North East Division Greshan, Oregon 97030, US.

Thanks to Paul Gillen and Noel Wade at the Computer Crime Investigation Unit, Garda Bureau of Fraud Investigation in Dublin.

By Tom Galligan

Forensic analysis with DiskSearch MKII

Forensic computer specialists should consider adding the latest version of DiskSearch MKII to their software library. This powerful investigation program will locate information lurking in the darkest reaches of any DOS-compatible disk.

DiskSearch MKII probes disk locations that don't typically contain data files, setting it apart from more typical search programs. This thoroughness, combined with the program's speed and flexibility, make it an essential tool for forensic computer specialists. The latest release, version, 2.4, simplifies the task of examining large numbers of floppy disks.

How it works

DiskSearch MKII locates any occurences of your search strings on the targeted disk without regard to the normal restriction of the operating system. It examines numerous disk locations that are off-limits to most search utilites, including file and partition slack space, unused and bad clusters, and Netware, Xenix, and other non-DOS partitions.

The hits resulting from a search can be displayed on the screen, spooled to a printer, or captured in a file for later analysis. Directing the results to a printer or a file allows the search to proceed unattended, freeing the user to attend to other tasks.

The program's character-based interface is fairly straightforward, though most users will find it helpful to use a mouse and spend a few minutes with the manual before going to work.

Program highlights

DiskSearch MKII is enhanced by its ability to search for as many as 256 strings at one time, with each string as long as 68 characters.

This is a great time saver, since it minimises the lengthy process of reading the information on the targeted disk. The collection of search phrases can be re-used in later searches, allowing you to scan multiple disks for the same strings.

This feature also facilitates investigations of similar cases by allowing you to save a library of strings that may commonly appear in particular types of cases.

DiskSearch MKII includes a "fuzzy logic" feature, which is critical for a thorough examination. This feature allows you to expand the scope of your search to locate words that are similar but not necessarily precise matches of the specified search strings.

This feature is intended to help locate names when you are unsure of the proper spelling, or to locate key words that may be mis-spelled or abbreviated. DiskSearch MKII can accommodate even your most particular requirements, allowing you to specify just how accurate a hit must be in percentage terms. Careless use of this feature will yield unintended results, so review the manual and experiment on a test disk before forging ahead.

DiskSearch MKII helps preserve the evidence by automatically write-protecting the targeted disks. This ensures that you cannot alter the data under examination, regardless of the requirements of any software that may be running. The program also supports analysis of removable media, such as the popular Zip or Jaz drives.

The various versions of Windows, OS/2 and other operating systems have introduced increasingly complex file systems in recent years. DiskSearch MKII can be used on these systems, but the program will correctly report only the physical location of any hits. Any file name reported in such a search may not be correct. Supplement DiskSearch MKII with a disk utility program designed for the operating system in question to locate the appropriate file.

Disksearch MKII is distributed solely by WA Haynes and Associates. Government and law enforcement agencies may purchase the program for £245 US plus shipping, with a discount for eleven or more copies.

For more information, contact the company on +1 541 688 0499, or by e-mail at wah@efn.org

The Internet for cybercops

Identifying Internet activity and looking at Net security

By
Michael R. Anderson

The Internet...friend or enemy? The popularity of the Internet has grown at incredible rates and today it reaches into the hearts of many corporations and households worldwide.

The Internet gives computer users access to a wealth of information. It is also a wonderful mechanism for the exchange of e-mail communications and file attachments globally. International boundaries no longer exist when it comes to the exchange of information over the Internet.

This new technology has proven to be ideal for international commerce and it has the potential to be a valuable communications tool for exchange of law enforcement and government information. However, the Internet also provides the 'crooks' with communication capabilities that did not exist previously. Through the use of a modem and with just a few clicks of a mouse, criminals can share information worldwide.

Sad but very true. Cyber crime has become a reality in our modern world.

More and more, law enforcement agencies are encountering computers at crime scenes. These computers are used to store the secrets of criminals and they are also used in the commission of crimes.

Internet related crimes are clearly on the rise and abuses of corporate and government Internet accounts by employees are becoming common place.

I know of one recent case involving the employee of a large corporation. He was using his corporate Internet account, on company time, to run his side business. What a deal...thanks to the Internet he had two day jobs.

To make matters worse though, he was also using the corporate computers on company time to view and download pornographic images from the Internet. In another case a law enforcement management official destroyed his 15-year law enforcement career when he was caught using a law enforcement computer to download pornography from the Internet.

Recently I received a call from a deputy sheriff who was requesting help in the investigation of the rape of a young girl. The girl had been lured from an Internet chat room to meet the rapist at a shopping mall and the rapist's computer contained crucial evidence in the case.

The law enforcement community is starting to effectively deal with computer related criminal investigations. Funding is finally being focused on the creation of local and state computer crime units.

Law enforcement training organisations like the National White Collar Crime Center, Search Group, International Association of Computer Investigation Specialists and the Federal Law Enforcement Training Center are training hundreds of law enforcement computer specialists each year.

Some of these training efforts are being directed at Internet-related crimes and you will see more training emphasis placed on this important technology issue in the future. Things are looking up on the training front for law enforcement.

Law enforcement successes in computer related investigations are directly tied to the availability and quality of forensic software utilities.

Until recently, law enforcement computer specialists were without specialised forensic tools to deal with Internet related computer evidence.

New Technologies, Inc. recognised this deficiency and created a forensic tool to deal with it. One of these new forensic tools is IPFILTER which was specifically created to help law enforcement computer specialists identify Internet E-mail and browsing activity.

Because of the increase in Internet related crimes, this program has been made available free of charge to law enforcement agencies by New Technologies, Inc. It was created primarily to help investigate cases involving child pornography but it has proven to be a powerful tool for use in the identification of any Internet misuses.

From a computer investigator's standpoint, the Microsoft Windows operating system is a dream come true. After all, DOS and Windows were never designed to be secure.

This is particularly true concerning Internet related evidence stored on computer hard disk drives in the form of ambient data. E-mail addresses, content and a history of Internet browsing activity potentially pass through the Windows swap file.

Much of this information remains behind waiting for discovery and documentation by the computer investigator. This is essentially true of all versions of Windows and the same information becomes a potential source of computer security leakage for corporations and government agencies.

Computer investigators are fortunate that data fragments remain behind in the Windows swap file. That is the good news. The bad news is that these swap files can be huge and picking out the various URLs can be a time consuming and tedious task.

That is where the IPFILTER program comes to the rescue of the computer investigator. It relies upon fuzzy logic concepts to automatically identify patterns of e-mail addresses and URLs.

The process takes just a few minutes and the output is a data base file that can be reviewed or analysed using any popular spread sheet or database application.

A copy of the public domain program DM, is provided with the program and it can be used to quickly sort through the database created by IPFILTER and provide meaningful statistical information about prior Internet activity on a specific computer.

As a point of clarification, the Internet activity is identified from remnants of data stored on the computer hard disk drive and not from an analysis of web traffic or with electronic sniffers.

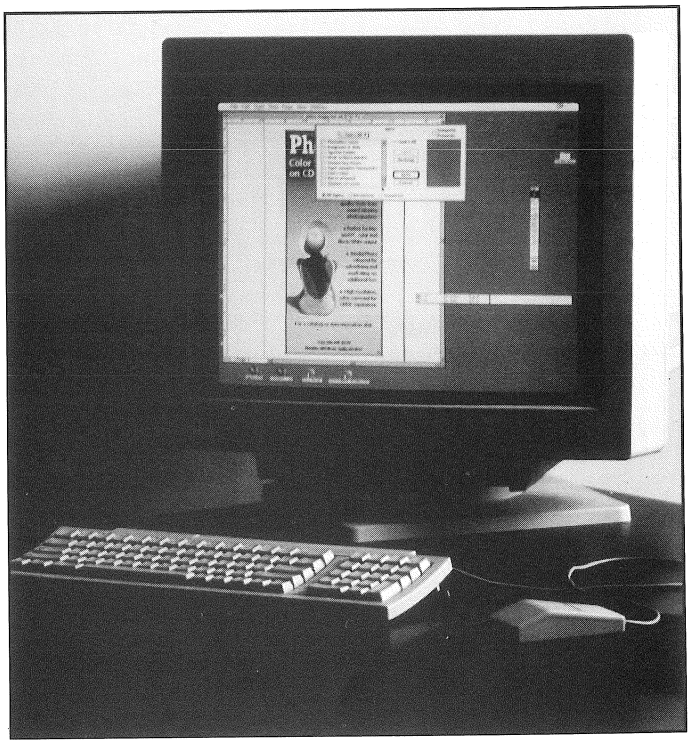
In those cases where Windows swap files are dynamically created during the work session and then erased, the same information is left behind as a large erased file in unallocated space. Such information can be recovered and easily processed by the IPFILTER program.

The Internet and related computer evidence issues are here to stay! Because of the common belief that Internet use cannot easily be monitored by law enforcement and corporate internal auditors, it is likely that misuses of the Internet will continue in the future.

Training and the availability of automated computer evidence processing utilities will be the key to success for law enforcement and corporations in the coming months and years.

IPFILTER Hints & Tips:

The IPFILTER program was created by New Technologies, Inc to quickly and easily process binary data from Windows swap files, accumulated files slack and/or unallocated space.



It relies upon fuzzy logic concepts to identify valid patterns of e-mail activity and URLs. The output from the program is in the form of a dBASE III file that can be viewed or analysed by almost any spreadsheet applications and/or database application.

The IPFILTER program (version 2.1) was tested with a 20MB Windows swap file.

Within five minutes it had identified over 455 valid e-mail addresses and URLs.

The file slack on the same computer was captured with GetSlack software, by New Technologies, Inc. and the resulting binary file was just over 600MB. IPFILTER processed the file within 20 minutes and it identified over 30,000 valid e-mail addresses and URLs.

The resulting output from both runs was statistically evaluated and the results of a frequency distribution analysis revealed that the output from both runs tied with known Internet activity of the user of the test computer.

However, the larger sample obtained from an accumulation of file slack proved to be the most accurate. Our tests of the IPFILTER program suggest the following:

Quick reviews of Internet activity on a specific computer can be done within ten minutes if Windows swap files are copied to external storage devices for processing. Such an analysis may be ideal for law enforcement intelligence gathering or corporate spot checks by internal auditors or security specialists.

More valid evaluations of Internet activity on a specific computer result when file slack is dumped and analysed.

This process is more time consuming but it tends to provide more valid results and thus better leads.

The process can be performed through the use of Iomega Zip Disks or Jazz Disks and the entire process of capturing the data and processing it can be accomplished within 30 minutes on most computers.

Final decisions regarding Internet activity and possible misuses of corporate accounts should not be solely based on the output from the IPFILTER program.

It is suggested that suspicious URLs be traced using a forensic text search program.

Conclusions should be based on the content of e-mail documents, fragments of e-mail documents and/or graphic files actually found on the computer and as identified by the text search program.

More specific information about IPFILTER is available on this site. It is available free to law enforcement agencies and it can be purchased by government agencies and corporations.

Internet security - firewalls and encryption - the cyber cop's perspective

It has been an interesting transition. A few years ago I was a federal law enforcement agent breaking the 'crooks' computer security and teaching other cops how to do it.

Now, I find myself in the reverse role of helping computer users protect their secrets. Interestingly, I also find myself helping corporations and government agencies in finding computer 'secrets'.

They want to identify their security risks and need the capability of conducting their own internal computer investigations. You see... it is not good for corporate public relations when law enforcement agencies are called in concerning computer breaches or employee Internet misuses.

For this article though, let's limit the discussion to protecting corporate and government secrets.

Due to the current popularity of international commerce on the Internet, the topic of computer security has moved quickly from being a low priority for corporations and government agencies to a high priority. This interest has been heightened by computer break-ins at places like Los Alamos National Laboratories and NASA.

Admissions by the United States government that many attempted military computer break-ins were successful has only added fuel to the fire.

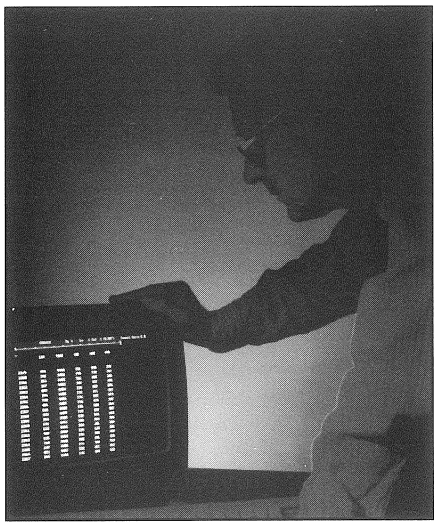
A retired director of the FBI's computer crime squad, was quoted in USA Today as saying, "You bring me a select group of hackers and within 90 days I'll bring this country to its knees." He was talking about the United States.

Is there any truth to this claim? I don't know if I fully agree with it, but it makes a good point. Our computer systems are at risk, but the good news is that we can do something about it.

The creators of the Internet never envisioned that it would become the hub of international commerce. They designed the Internet for the open and free exchange of research information between universities and government.

They did not design it to be secure and Internet firewalls were an afterthought. Some firewalls are good and others are not. Are proxy firewalls better than filtering firewalls? Nobody really knows and both may be necessary depending on the risks involved.

However, firewalls may not be enough protection. Secure network routers are coming on line, but they have yet to prove themselves. From my perspective, potential security problems exist anytime a government or a corporate computer is connected to the Internet. Furthermore, fragments of previously deleted e-mail and files may linger for years in the heart of computer hard disk drives and discarded floppy diskettes. Trust me on this one... computer secrets never go away.



Many crooks have learned this lesson the hard way. However, things may not be as bad as they appear from a computer security standpoint.

Through the implementation of proper computer security policies and strategies, network connections to the Internet can be made more secure and sensitive data can be secured by using file encryption.

Also, computer storage media can be effectively cleansed of sensitive information. Knowing the risks up front makes the job much easier for computer users and security policy makers. Firewalls and secure network routers haven't come of age yet and security tied to them may not be adequate protection for trade secrets and sensitive computer data.

However, these technologies have their place and only a fool would connect a computer network to the Internet without some sort of firewall.

Given enough time, desire and resources, it is a safe bet that almost any computer security system can be broken.

The only totally secure computer system is one locked in a room, without people and without connections to other computers. Since such a security strategy is impractical, other security strategies and policies must be implemented. Government and corporate management cannot ignore the Internet just because of potential Internet security problems.

The wealth of 'free' information available on the Internet and inexpensive worldwide e-mail access can result in significant cost savings and increased productivity.

Don't forget. We do live in the information age. A corporation cannot remain competitive if it doesn't take advantage of all available technologies. Internet firewalls serve a very good purpose. Much like the perimeter fence at a military base, firewalls act as the first important line of defence.

However, they are not the total answer. Encryption should be wisely used to protect sensitive information from 'unauthorised eyes'. It is no secret that foreign competitors of large US corporations gainfully employ former Eastern Block intelligence agents.

You see, it is more cost effective to steal the secrets of your competition than it is to spend millions of dollars for research and development. Unless good encryption is employed, they can make copies of the computer 'secrets' without leaving any trace or clue that they even compromised such secrets.

Most written communications today are created on computers. Most of these computers are not secure and to make matters worse many computers involved are portable notebook computers. File encryption helps here also.

An Internet firewall is essentially one or more systems that control access between computer networks. In this regard, the Internet is nothing more than a very large computer network.

An installed firewall on a computer network serves two basic purposes: it

controls access to the network from outside servers, and it also controls the transfer of information from the network to outside servers.

It is not enough to just install an Internet firewall. The type of firewall(s) needed is usually dictated by the needs of the organisation and the level of risk involved.

The most important thing to remember about a firewall is that it creates an access control policy for the organisation. Executive management and the computer security staff must be involved in defining what the access policy will be prior to purchase and installation. If such planning is absent, the organisation will set its security policy based on the on the whim of the installer, or worse, the default configuration of the manufacturer. Let's not forget that... hackers love default security settings.

In my career as a 'cyber cop', not much difficulty was ever created by network or system security systems used by the criminal element, e.g., in my work helping other agencies, we easily accessed computers used by criminals.

However, breaking good file encryption schemes proved to be a difficult, and sometimes impossible task. Yes, we did have our successes thanks to private sector help from experts like Eric Thompson. The encryption used by a CIA spy 'gone bad' was broken.

The encryption used by a federal agent to secure child pornography files stolen from the evidence room locker was broken. Now they have more time to think about better computer security strategies...and you think I'm kidding. Some prisoners have more access to computer systems for training purposes than federal employees in government agencies. Sad but true.

Once the mysterious focus of spy stories and movies, encryption is really nothing more than the scrambling of data to make it unreadable. There is strong encryption and weak encryption.

Most word processing, spreadsheet and database applications that provide encryption as an option, are not secure. In fact, commercial applications exist which can be used to quickly defeat the security afforded by these applications. For our purposes of this article, I am talking about standalone file encryption products.

To keep things simple, let's just say that the longer the encryption key the stronger the security. This assumes, of course, that a solid encryption algorithm has been employed. Unfortunately there are several algorithms to choose from.

The most secure encryption algorithms, implemented by software, have a key length of 128 bits or more. These include IDEA, Triple DES, 128 bit RC4 and 128 bit SEAL.

A relatively new algorithm that seems secure is Blow Fish. The "lesser strength" but still relatively secure algorithms include 80 bit RC5 and 64 bit

RC5 encryption schemes. The Data Encryption Standard (DES), developed back in the 70's is currently the standard used by the US federal government regarding the encryption of sensitive but unclassified data.

It deals with a 56 bit key length and is on the edge of what is breakable using today's technology and about $250,000 worth of computer hardware. We had one criminal case which involved the use of DES encryption and fortunately we were able to break the encryption scheme used by the 'bad guys'.

Currently, the US government restricts the export of most encryption software that relies on strong encryption algorithms. However, there is heated controversy regarding this issue between government and software companies.

Because of the potential loss of international technology trade by US companies, Congress will probably support the export of more powerful encryption products in the future.

If they don't, this country could lose billions of dollars in foreign trade, over the next few years.

If they do, it could create more problems for the government's law enforcement and intelligence agencies. There are good arguments in both directions.

How difficult is it to break encryption? The answer involves the speed of the computer used to perform the task, the length of the key involved and how much money you have to throw at the problem.

Calculating how much time it takes to break a specific key length is simple. Given current technology, approximately 90 million DES key combinations or five million RC4 key combinations can be processed per second.

The cost of the computer hardware to accomplish this is approximately $50,000 - $75,000. In other words, for about $50,000, given current technology, it would take only a second or so to break encryption tied to a key length of 26 bits. It would take approximately one hour to break a key length of 38 bits.

A 40-bit key could be broken in about four hours, a 48-bit key in about one month, and a 56-bit key (Full DES) in 30 years or so. Up the price to about $1 million and DES can be broken in approximately 10 days. I think you get the idea.

Security tied to a 128-bit encryption algorithm is very secure, given the state of technology today and the expected state of technology for the next 30 years.

My message to you is this... fear of the Internet is unfounded if proper security measures are implemented as part of a well-designed security strategy.

Firewalls have their place in the security design, but corporate trade secrets and sensitive government data need to be encrypted at a high level of security.

To avoid the threat of destruction of data by hackers, make regular and periodic backups and store copies off site.

That might sound pretty basic, but I know of several major agencies and large corporations that don't backup critical data files on a regular basis. To put it mildly, they are playing with 'cyber' fire.

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

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

The firm can be contacted on +1 503 666 6599 or by e-mail to info@forensics-intl.com

Forensic Q&A

Q ***If I receive an image of a computer where the user has been deleting both files and directories can I still retrieve the data?***

A The recovery of files is a very simple business, especially with an application such as Microsoft Undelete. It is good forensic practice for the files to be recovered to a different drive to ensure that when the recovered version is written to the disk the clusters of other deleted files are not over written. Deleted directories are slightly more complex. These cannot be recovered to a different drive; they must be recovered from and written to the same drive that they were deleted on. If deleted directories are present the best method for recovery of them is to recover the directories one at a time; after each directory has been recovered analyse the contents and copy the data to a different drive. The drive image should then be recreated from the original copy and the next directory should be recovered. The reason for this is that when the directory is recovered many clusters, and thus potential data, on the target drive are over written and so the drive needs to be recreated from the original best evidence copy.

Q ***When I run a search engine across a hard disk hits are often reported in slack space. What is this and how can I access this information?***

A The physical storage space on a computer's hard disk is divided up into separate storage areas called Clusters. When a file is saved on the disk it occupies one or more clusters depending upon the size of the file. When the file is deleted the clusters are regarded by the operating system as available for use for another file. When a second file, which is not large enough to completely fill a cluster, is saved into a cluster that had previously contained data belonging to a deleted file, the new data does not completely overwrite the data from the original file. The area of the cluster between the end of the new data and the end of the cluster is referred to as Slack Space. Your hits have been occurring in this area and there are several utilities available to access any data stored in slack space.

Q ***Why does DOS restrict the number of clusters? Is there anyway of creating smaller clusters?***

A At the core of the 16 bit FAT system is the File Allocation Table itself. This is an area of the disk specially set aside for the storage of what is essentially a map of the usage of the disk. As the name implies, a 16 bit FAT is made up of a series of numbers, each of which occupies 16 bits (2 bytes for one word). The position of each of these word entries represents a block of space on the disk - the 20th word represents the 20th block (or cluster). The number stored in this 20th position represents the state of the cluster. If the 20th word contains a zero then the 20th cluster is available for use. If the 20th word contains any other number it indicates that cluster 20 is currently in use and the number (with some special exceptions) indicates the next cluster in the allocation sequence (or chain) where information subsequent to the 20th cluster is stored. The special exceptions include a value of 65535 (HEX FFFF) which indicates that this cluster is the last in a chain. The other numbers between 65520 and 65534 indicate various conditions including marking the relevant cluster as unusable or reserved. This system has proven its usefulnes, but it has some serious limitations. One of these is that it cannot address more than 65520 blocks. Since the original size of clusters was fixed at 1 sector (512 bytes), this meant that a single FAT could address around 32 Mb of data. As hard disk capacities increased, arrangements were made to increase the size of each cluster up to a maximum of 64 sectors (32 KBs, with a maximum addressable capacity of 2GB. This solved the capacity problem at the expense of creating an inefficient space usage system because the larger the clusters, the larger is the slack area associated with each file. A very simple approximation of the amount of slack space on a disk is given by the equation:

$$S = F*(C/2)$$

where S is slack space in bytes, F is the total number of files and C is the cluster size in bytes. Thus if you double the cluster size you double the amount of slack space. There is a way to reduce cluster size and that is to reduce the disk size by partitioning. Since the cluster size is determined by the FORMAT program as it checks the size of the partition, if the partition size is reduced then FORMAT can reduced the cluster size accordingly. Assume you have 8000 files on a 2 Gbyte partition with 32Kbyte clusters - from the above equation this will have around 131 Mbytes of slack space. Now assume the same 2 Gbytes but this time in four partitions (each of 500 Mbytes with a cluster size of 8Kbytes). Now the 8000 files will only give rise to around 32 Mbytes of slack space. This saving more than makes up for the slight overhead associated with each partition. A recent development with Windows 95 OEM service release 2, is the introduction of the 32 bit FAT system which attempts to address the problem and increase the addressable number of clusters without increasing the cluster size. This system cannot be accessed by earlier versions of DOS.

Thanks to Guest Analyst, Craig Earnshaw, Forensic Analyst, Computer Forensic Investigations Ltd., Hulton House, 166 Fleet Street, London EC4A 2DY. Tel: +44(0)171 353 3777.

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

Notice Board

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

Events

NetLaw 98

28-29 April
Howard Hotel, London WC2, UK

A forum dealing with the risks and opportunities of using the Internet.

Contact: +44 (0)171 878 6888

Tools for Tackling Telecoms Crime

11-15 May 1998
Manila, Philippines

Global Intensive Programme said to be the first of its kind will include high profile industry speakers who will expostulate the problems.

To be followed each day by intensive training to equip delegates with the solutions.

Topics include: Customer &Distribution Fraud plus an introduction to technical fraud;

Technical Attacks and Network Security, Internal Crime, Intelligence Management; Investigative Deterrent plus Building a Fraud and Security Department.

Contact: Praesidium Services Ltd
Tel: +44(0)1249 467800
Fax: +440)1249 467809

Frauds on the Internet

21 May 1998, Milan

Advanced strategies and techniques for preventing online frauds.

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

Fraud and Security in Telecommunications

21 May 1998, Milan

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

Colossus: How We Cracked the Codes

21 May, Guildford, Surrey, UK

Programme details state: "This was probably the birth of electronic computers. Cracking codes set up in mechanical machines was just not fast enough. One could argue that the V2 rocket technology brought us jet airliners. Do we have to thank the second WW for the WWW?"

Contact: T. Dashwood, British Computer Society
Tel: +44(0)1252 392796

Securing and Auditing Internet Connections

21 May 1998, Bristol, UK

The International Police & Security Expo '98

14-16 July 1998

Birmingham, UK

Contact: Labelex Exhibitions Ltd
Tel: +44(0)181 313 3535
Fax: +44(0)181 468 7472

Forensic Computing Course

A forensic computing course is being run by Professor Tony Sammes at the Royal Military College at Shrivenham, UK, from March 9 to 20 1998.

The cost of the course is in the region of £2,200 Contact Prof Sammes, on +44 (0)1793 785270, or Det Insp Brian Jenkinson of Cambridge Fraud Squad on +44 (0)1480 437766 for

Dibs User Group

The Dibs User Group held its first meeting in Worthing, UK, recently, attended by police and civil investigators from across the country.

The latest developments from Computer Forensics Ltd, which supplies hardware and software for those working in retrieving computer evidence, were discussed, including the latest technological developments.

Members of the group discussed their own working practices, investigation problems and pooled their extensive experience of working in the field.

Topics covered included:

1) Standardisation of procedures – the Association of Chief Police Officers group paper being prepared on the principles of forensic evidence recovery, the essential use of standardised logs and the latest developments in training. Members of the group were asked to submit their own statements and logs so the committee could find the best way of recording forensic information.

2) Presentation of evidence in court – the group felt that many problems were being encountered in court to the detriment of the prosecution of a case.

The meeting also agreed to draw up a 'help list' of people in the computer industry to help investigators who need a specific piece of hardware or software.

Chairman of the group, Dave Lattimore, of Thames Valley Police, said: "The aim of the group is to find the best working practices in our field, sharing problems and assisting each other to achieve the correct result.

"The Dibs User Group will only succeed if all the members take an active part in promoting and contributing to it."

The next Dibs User Group meeting is scheduled for April 30 and May 1 in Newcastle, and the planned theme is Courts and the Presentation of Evidence.

Submitted logs and statements will be discussed to find a common and best practice for all users. Subjects to be covered in the meeting include evidence, warrants and legal privilege.

For more information contact Dave Lattimore on +44 (0)1189 504611.

International Journal of
FORENSIC COMPUTING™

Mike Anderson

IJFC is tied to
Computer Forensics Ltd
and tied to DIBBS system
(black box)

sold
~~$3~~ $25,000 per user
DIBBS = Authentec

Published by
Computer Forensic Services Ltd