ISSN. 1363-6650

JUNE 1997
Issue 6

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

Almost everyone uses computers these days, either for work or play. The silicon chip is as much a part of our lives as the car, washing machine or television and is taken for granted in a similar way.

Computers are now vastly more powerful and capable than even five years ago and the processing and storage capabilities of a £1,500 system can make a business fly, create a home office, or become a state of the art video games machine.

But the same computers in the wrong hands can be turned into frightening weapons of destruction and hate. The number of crimes which directly involve computers are soaring, including fraud, paedophilia and hacking.

Computers can also be used in just about any other crime, from murder and theft to blackmail and libel. Evidence found on them can be crucial in any police or civil investigation. A 1GB hard disk, which is now on the low end of available data storage, can easily hold as much information as a whole filing cabinet stuffed full with documents. Computer crime is big business and will only get bigger.

Yet the criminal justice system has yet to wake up to the full implications and potential that a comprehensive approach to computer investigation can bring. The police in countries across the world are loathe to invest in the technology and expertise necessary and there is still an amateurish approach to the subject in many law enforcement agencies.

As with much in the computer world, computer investigation is seen as a black art and often handed over to those who profess technical ability. But an investigation is still an investigation, whether it involves computer data or paper, and the same police skills and experience are involved.

The other side of the equation, the legal system, has similarly yet to grasp the full extent of computer crime. Few solicitors, barristers, prosecutors or judges have an in-depth knowledge of what computer investigation involves or how the law can be interpreted to cover such activities. The issues of admissibility and disclosure of computer evidence have yet to be fully put to the test, with the very real risk that cases can be won or lost because lawyers do not fully understand what is involved.

But there is plenty to be optimistic about. The British legal system, that bastion of tradition, is being dragged kicking and screaming into the 21st century. Master of the Rolls Lord Woolf says IT is central to his goal of making justice faster, cheaper and fairer.

Already compuer aided transcription systems are saving hundreds of hours of court time. Lawyers and judges have access to a scrolling, searchable, stored record of everything that is said. This is much more efficient than paper documents and has the advantage of reducing the risk of injustice.

But many in the legal system think they will benefit from keeping to the old system because time is money and a longer court case is therefore more lucrative.

As Lord Woolf says: "This progress has to happen, and the sooner the better."

Everyone in the legal and criminal system needs to understand computers and be prepared to work with them. Failure to do so could seriously jeopardise the course of justice. ■

News

Crime threat posed by new technology

The Director General of the National Criminal Intelligence Service told delegates at a conference that a new style of policing is necessary to fight computer criminals.

Albert Pacey was speaking at the NCIS's third international organised crime conference in London on the opportunities and threats that the Internet and associated technology represents.

He said: "A new police beat is emerging not that of the streets of our cities, but that of the information highways which are creating criminal opportunities that ultimately affect every citizen.

"In many cases the Internet is merely being used as a new form of committing old style crime. Fraud and software piracy are common enough, it is the speed and extent open to Internet users that increases the scale of the problem.

"However, there are areas such as hacking, which are new methods of exploiting the new technology for criminal gain.

"The Internet brings many benefits in terms of worldwide, free communication and possible new markets for commerce. We as law enforcement are not suggesting for a moment a need for draconian powers to in some way censor the medium.

"We realise this is not an option. Rather we are trying to develop mutual aid systems across national boundaries which will speed the exchange of information and evidence among investigators."

Already criminals have woken up to the potential computer crime offers and the conference was told one offender claimed he could make three times as much from software as selling drugs and was confident he would not go to jail if caught.

And in an attempt to combat the problem, the NCIS has begun a study of criminal use of technology called Project Trawler, which is looking at hacking and its use in economic espionage, fraud, electronic payment systems and security, paedophile use of the Net and software and audio piracy.

Mr Pacey told the conference: "We believe this is the first ever in-depth study of the subject attempted from a law enforcement perspective. It remains a work in progress, but we are using this conference as opportunity to share some of our initial findings. This cross-fertilisation of ideas is essential to keep ahead of the criminal.

"What Project Trawler is showing is the need to change our methods of policing to fit the new technological age. Instead of following up reported crimes, it will benefit us far more to be ahead of the game and intelligence driven.

"We need specialist officers with technical knowledge and expert support. This, coupled with mutual support between law enforcement and industry will meet the new policing challenge of the next millennium."

It is hoped that the findings of Project Trawler will be sent in full to law enforcement officers this summer, with a summary document publicly available.

Call to fight Web filth

Australia's deputy Prime Minister has urged countries across the world to take part in a crackdown on paedophile material carried on the Internet.

Tim Fischer told a meeting of the 27-country Organisation for Economic Co-operation and Development that everyone had to work together closely to combat the problem.

There have been calls for a formal treaty on the issue, especially after the shocking revelations surrounding a paedophile ring in Belgium, but officials say a greater communication and closer ties between law enforcement agencies is more likely.

Missing children Web site wins top prize

A service which gives instant access to information on missing children has been cited for best use of Internet Technology in the Service of Humanity.

The site was produced by Computer Associate International Inc in California for its client the National Centre for Missing and Exploited Children in the US and was acclaimed for its effectiveness and ease of use.

Data on missing children, including pictures, case information and a detailed database of each person, can be accessed using a search facility in the site.

President of the NCMEC Ernie Allen said: "Working on the premise that for each missing child there is at least one person who knows the whereabouts of that child, technology is taking the search for missing children into the 21st century.

"With an average of 20,000 hits a day on the Web site, we're hopeful that technology will aid in the efforts to reunite more missing children with their families and educate countless parents and children about ways to stay safe."

The NCMEC site is at www.missingkids.com

Man arrested over Internet porn show

A Japanese computer engineer was arrested after the weather charts on a Web site were replaced with pornographic images.

The suspect claims he altered the weather charts on the Asahi Broadcasting Company's public Internet pages as a bit of fun, but if convicted he could face a fine of Y1 million and a prison sentence of up to five years.

Osaka police say that it is the first arrest they have made in connection with violations of a 1987 anti-hacker law.

Law targets Net paedophiles

New legislation in Alabama in the US has been passed in an attempt to stop paedophiles using computers to lure children.

The law makes it a crime for someone aged 19 or older to use a computer to advise or entice someone under 16 to commit a sex act for the adult's benefit.

Violators could face up to 20 years in prison and Alabama is the sixth state in the US to crack down on those who use technology for immoral purposes.

Senator Bill Armistead, who guided the bill through, said that adults posing as ▶

teenagers used Internet chat rooms to contact children. He added: "The paedophiles are finding this a better way to meet children than going to a ball park or restroom."

Money launderers come clean with e-cash

Organised crime groups could soon be using the Internet to cover their tracks and dispose of money from illegal activities, a conference in Portugal was warned.

A two-day meeting in Lisbon, Portugal, called Cyberlaundering and Fraud, heard how electronic banking and the online transferring of funds could make criminals' lives much easier because it did away with a paper trail for investigators to follow.

Gareth Maclachlan, of the British National Criminal Intelligence Service told the conference: "With most criminal enterprises, notably the distribution of illegal drugs, the proceeds are in cash and law-enforcement tactics for countering money-laundering depend upon identifying the movement and placement of cash."

He added that crime groups could even set up their own web-based companies offering products and services to help wash their ill-gotten gains, and that law enforcement agencies would find it hard to control or police because of the question of territorial jurisdiction.

Teenager hacks into NASA computer

US federal officials are investigating after a teenager hacked his way into NASA's Web site and left a message attacking the space agency as having lax security.

The youngster, who has not been named, gained access to the Internet site running from NASA's Marshall Space Flight Centre in Huntsville, Alabama, and wrote: "Oh, what a tangled web we weave, when we practice to deceive. This page is here to express many people's feelings towards the release of Kevin Mitnick. You guys have to learn security before you can punish people for it." He was seeking support for Mitnick, a computer hacker who was charged last year in connection with a computer crime wave.

NASA Inspector General Robert Gross said the incident showed how vulnerable the agency was to intrusion via the Internet. He said: "We live in an information environment vastly different than 20 years ago. Hackers are increasing in number and in frequency of attack. Although the progress of information technology has been remarkable, in many ways NASA is facing more serious threats than ever before."

Thai police online to fight crime

People in Thailand will be able to report crimes and send tip offs to the police by using a confidential e-mail service. The program will be in full operation in 1999 and will also include information about the Bangkok Metropolitan Police Bureau, details of stolen vehicles and warrants for wanted criminals.

Police say an ever increasing number of people are now using the Internet and that the move will have a serious effect on the country's crime rate.

Computer giants in talks with Clinton

The heads of ten leading computer companies met with President Clinton and with Congress in an attempt to change US laws. Members of the software industry say current legislation on security technology is outdated and that issues such as piracy, intellectual property rights and encryption have to be addressed if firms are to remain competitive overseas.

The software industry employs about 620,000 people in the US and the market for software is now worth $100 billion, but annual losses from piracy are reported to be more than $10 billion.

Technology solves skeleton mystery

Police in Australia used a computer imaging and matching program to formally identify the body of a fisherman found near a dirt track.

The skeleton remains of Trevor John, 36, were discovered on a roadside near Mackay Harbour, Newcastle on September 15 last year.

Using computers, the skull was matched with pictures of Mr Lauder and a human face was reconstructed from the results. A coroner accepted the legal identification, but the cause and circumstances of death are still unknown.

Hong Kong officer posted child porn

A senior correctional services officer posted hardcore pornographic pictures of underage girls on the Internet, a Hong Kong court heard.

Most of the girls appeared to be aged under 14 and the accused man, a 32 year-old denies a charge of publishing obscene articles.

The court was told that 19 pictures were discovered by an Inspector in the Commercial Crime Bureau's computer unit last year and a search at the defendant's Internet service provider found that seven files containing the images had been posted to newsgroups.

German Internet test case

A Berlin court trial could redefine Net law if a left-wing politician accused of aiding guerrilla acts is found guilty.

Angela Marquardt, 25, from the reformed communist Party of Democratic Socialism, is alleged to have used hypertext links on her Web home page to take users to an extremist publication that is banned in Germany. In the past Radikal Internet magazine has carried information on how to sabotage railway lines and is based on a computer in the Netherlands.

The court's decision is likely to set a precedent on the issue of whether it is legal for someone to use a hypertext signpost to lead Internet browsers to suspect sites. The public prosecutor said: "It has nothing to do with censorship."

Experts on the Internet have been called and the case will proceed again on June 30. ■

Product News

New company to combat corporate fraud

Two firms have come together to offer security and investigation services to businesses across the world.

Computer Forensic Investigations Ltd aims to offer a full solution for companies who suspect they could be at risk or have suffered from computer crime or misuse.

The joint venture, by UK firms Computer Forensics Ltd and forensic accountants Lee and Allen is launched this month and will target all types of technology fraud as well as conducting security audits.

Services include data copying, analysing and, if needed, presentation of evidence in a court of law if a case goes to prosecution.

The new company says it has specialised forensic accounting skills and experience and can save businesses a great deal of time and money.

Mark Taylor, one of the directors of Computer Forensic Investigations Ltd, said: "By combining the technical and analytical techniques with the investigating and accounting capabilities, the parties have the skills to investigate corporate fraud at the level demanded by the increasingly sophisticated nature of such fraud.

"We believe that the hardware and software used and the technical support provided are unique worldwide. We will work closely with our clients, keeping them informed and providing support at every step of the operation."

Computer Forensic Investigations Ltd has offices in London, New York and Hong Kong. *Contact telephone +44 (0) 171 353 3777 or fax +44 (0) 171 353 3747.*

Crime report writing

Police will be able to halve the time spent filling in crime reports using a new computer program, according to its makers.

US firms RomTech and ImageWare are collaborating on the FormEZ project, which uses electronic forms rather than the conventional and time-consuming paper equivalents.

The system is part of a suite of programs which includes applications for suspect vehicle identification, booking criminals, image enhancement and facial recognition. *Contact RomTech at Jafalset@romt.com*

Forensic team fights Internet lawbreakers

US firm Infringatek is launching a computer forensics service to combat the growing number of crimes and illegal activities on the Internet.

The company, which specialises in intellectual property protection and information security, will help in investigations within corporate networks and to track suspect information on the Net.

Services on offer include detecting trade secrets leaked through networks, investigating hacking and sabotage, authenticating electronic correspondence and investigating online distribution channels of counterfeit goods.

Infringatek's vice president for IT said: "We have a team of professionals who understand the latest issues, tools and technologies. We are ready to investigate everything from instances of online fraud to counterfeit goods distribution channels. As Internet commerce grows, our services will truly be in demand."

The company, which is based in Vienna, Virginia, can be contacted at www.infringatek.com on the Internet or by calling (US) 703 847-3639.

Music industry fights cyber piracy

Los Angeles firm Intersect Inc will sell its MusicReport software to music and movie studios in a bid to crackdown on bootleggers who cost millions of pounds in lost sales.

The program searches the World Wide Web looking for music files, and once found music companies will be able to notify Internet service providers of the law breakers.

Some people have been known to copy their entire record collections and post them on the Internet for anyone to download.

Advances in technology mean music over the Net can be almost up to CD quality, with the new MPEG Audio Layer 3 format (Motion Picture Experts Group) allowing songs that take up 60MB of space to be compressed to about 5MB.

Meanwhile the Recording Industry Association of America has filed three separate civil actions against Internet music sites which break the law by allowing users to download full-length songs.

RIAA director of anti-piracy Steven D'Onofrio said: "These music archive sites are a blatant infringement of copyright law. Without the law to protect and stimulate creativity, the Internet will never truly see its full potential."

Secure document delivery on Internet

Tumbleweed Software Inc in the US has launched a document delivery program designed to send formatted and encoded material over the Net.

The firm says the software also lets documents be sent to fax machines and other devices and allows the sender to track the material's delivery and confirm receipt.

Jeff Smith, president of Tumbleweed, said: "This is a new market. We're the first ones that are shipping a product for this market."

A kit with network computer software and licences for 20 users or accounts costs $3,999 (additional users costing $189 each).

Free data loss disk

Data recovery firm Ontrack has launched new software to let users perform diagnostic functions themselves. The free program, Data Advisor, performs a range of tests and future products are planned by Ontrack to allow users to link up problem computers to its offices over a modem and have data recovered remotely.

Data Advisor is available from the Ontrack web site at www.ontrack.com or call (UK) 0800 243996 for a free disk. ■

Unix

Introduction

The science of computer forensics on PC based systems is now well established. The necessary methodology, hardware and software has been developed, has stood the test of time and been proven in the most challenging environment, the court of law. PC systems by their very nature are fairly standard. There may be some areas where they differ in set-up, but the operating system and disk format are largely the same. This fact has greatly simplified the process of being able to produce forensic evidence from these computer systems.

There is however another over-riding reason why they are simple to analyse and investigate and that is because they are `single user' systems.

But in terms of the corporate environment PCs present a risk. This is particularly so in today's open client-server environment. Data can be simply copied from corporate systems and databases and removed from site either via floppy disk or electronically via e-mail. These risks though, are fairly well understood by management.

It is however, the large multi-user systems that present the biggest security challenge to large companies. It is on these systems that the company holds its data assets and it is on these systems that the risk of fraud, espionage, data destruction and so on is at its greatest.

The trend over recent years for companies to move away from the traditional mainframe computer, where security tended to be in-built and under control, onto client-server based UNIX systems has dramatically increased the risk to companies' business.

This article examines some of the issues with UNIX, particularly with respect to the difficulties of retrieval and analysis of data needed to assist in forensic investigations.

PCs vs UNIX

Let's start by examining some of the fundamental differences between UNIX and PCs (MS-DOS variety) before we start looking at UNIX in more detail. *(see Figure 1)*

When you start examining a PC you can be reasonably sure what you are up against, with a few exceptions. However with UNIX, there are many variables.

So What is UNIX?

A simple question but a difficult answer! UNIX originated in the early 1960's from the Bell Laboratories in the United States. It derived from a mainframe multi-user operating system known as MULTICS. UNIX was built as a cut-down version of MULTICS primarily to run a game!

Over the years it has been developed in different ways by just about every single computer manufacturer until it has reached the point where there is no such thing as single UNIX implementation. Currently though, moves are afoot to standardise UNIX interfaces in the near future on what is known as Spec 1170.

The system has evolved rather than being designed. It was once described to me (rather unkindly) as 'a system written by hackers for hackers'. However, there is some justification in this remark. UNIX has been exploited for many years by the hacking community and there are many known vulnerabilities both in the operating system and utilities all of which can make security on UNIX something of a nightmare.

Its roots are primarily within the academic community, where the requirements are for openness and sharing of data and information. Today it has been increasingly adopted as the operating system for companies and organisations where the requirements for security are much more rigorous.

UNIX is not an insecure operating system as such. However although UNIX incorporates many security features, on delivery many of these features are either switched off, or are configured incorrectly. Many systems administrators do not have the knowledge or the time to configure their systems securely and many may not even be aware of the options available to them.

All of which brings me to the problem of undertaking forensic investigations on UNIX systems.

Investigating UNIX Systems

When called in to investigate a user's actions on a UNIX system certain questions need to be raised before the investigation can begin. The following needs to be established:

- What is the system manufacturer?
- What is the operating system and version?
- What is the suspected nature of the offence?
- When it is thought the offence took place?
- Is it possible to close down the system & ▶

Figure 1

PC	UNIX
Single User	Multi-User
Disk Capacity <= 2GB	Disk Capacity Unlimited
Operating System MS-DOS	Operating System - various
File system - FAT	File system - various
Security features - few	Security features - many & various
Number of Processors - 1	Number of Processors - various

re-start in single-user mode?

As I mentioned previously, all implementations of UNIX differ. For example, a command which executes on an IBM RS6000 running AIX, either might not work or produce different results if executed on a Sun system running Solaris. This means that:

a) It is impossible to write a generic system for retrieving data for analysis, and
b) Specific expertise is required which can cope with all the different types of UNIX.

In terms of the suspected nature of the offence under investigation, it is important to limit the scope of any data retrieval. It is simply not practical, nor desirable in most cases to image an entire UNIX system (unless it is a stand-alone workstation).

The time-frame under investigation is another important aspect and this again will vary from case to case. The offence could have happened anything from a day to six months ago. On the other hand, it could be currently going on. Once again, each scenario will result in different actions being taken.

For a system currently under attack, there are two options:

- Take the system down until the attack has been neutralised or,
- Leave the system up in the hope of capturing more evidence.

Each option involves its own risks, and these need to be assessed at the time.

Many companies run 24 hour, seven day a week operations and it may not be feasible to close down a system. This though may depend on the seriousness of the suspected offence.

For an investigation which is historic, then it may be that the investigator is not only concerned with the data still on the system, but also data which has been archived during normal back-up procedures.

Some Other Considerations

Advice given to police officers attending a scene of crime is to switch off any computer equipment before making an image copy. Most implementations of UNIX do not like 'just being switched off'. Indeed many of them will 'sulk' for a long time afterwards as switching them off without first synchronising the disks may result in disk corruption and thereafter the inability to boot.

The second issue is that when UNIX is shut down cleanly data which is cached in buffers, which may be of importance to the investigation, will be flushed and thereafter unavailable to the investigator.

UNIX is a wonderful networking computer. This too leads to its own set of problems. For example:

- A user on a system may be accessing files on a network mounted drive on another system.
- Commands can be executed on a UNIX system remotely, i.e. without logging in.
- Electronic mail can be spoofed, i.e. appear to have come from a user when in fact it didn't.
- If the company uses NIS (Network Information Service), it can be ambiguous who actually has access to the system.
- Various utilities exist such as File Transfer and UNIX to UNIX copying (UUCP) which if incorrectly configured will allow files to be removed from or placed on the system without requiring an account.

Users access UNIX with a username and password. There are more sophisticated methods (smart cards, retina scanners etc.) but these are rare. The primary method of authenticating users is via a password.

Passwords are notoriously insecure. When investigating a user's actions, how can you be sure that it was actually that user who created a particular file for example? The answer is that you can't, unless they are either caught in the act, or are captured on closed circuit television. Users are notorious for sharing accounts and passwords and many companies are lax in imposing good password discipline.

A user who is undertaking corporate fraud is unlikely (unless careless) to be using their own account to do so. Instead they will gain access to another user's account in order to hide their identity and possibly their actions.

One of the biggest risks comes from the 'superusers' or 'root' users. These are the systems administrators who have full access with full privilege on the system. They have not only the ability to circumvent most security on the system, but they also have the ability to use any users' account. More worryingly, they have also got access to all the log files and journals so they are able to cover their tracks.

Sometimes it is necessary to undertake covert surveillance on users' actions in order to get evidence. Such operations can be easily compromised by rogue systems administrators as it is impossible to hide such operations from them.

Information Retrieval

Having decided what areas of the computer need to be imaged, it is a fairly straight-forward process to copy the data onto an optical drive. The only problem with ▶

Figure 2

On DOS it would look like:

23-09-96	05:40p	2049	testfile
Date	Time	Size	Name

On UNIX the equivalent file may look something like:

	No. Links				
-rw-r--r--	1 root	sys	2049	Sep 23 17:40	testfile
Permissions	Owner	Group	Size	Date/Time last updated	Name

information retrieval is that normally it will have to be undertaken over the network. The hardware involved needs to be configurable to support the main networking protocols.

UNIX files have more information associated with them than DOS files. For example consider the file 'testfile' as shown in *Figure 2*.

Because UNIX is a multi-user system it is important that the owner, the group and the permissions are set correctly in order to control access to the file. Permissions though, as demonstrated later, are rarely straightforward and need to be considered carefully.

Some files may have been hidden by being created with an unprintable character (e.g. backspace) in the filename. The effect of this is that they will not appear in a directory listing. This can also apply to directories and indeed a common way of hiding files on a UNIX system is to place them in directories that themselves are hidden.

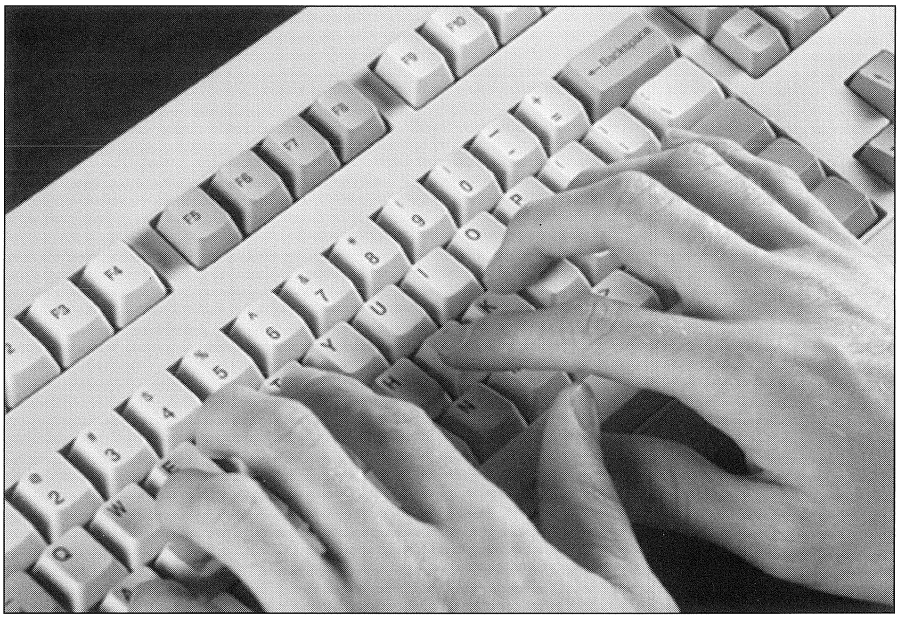
Information Analysis

If a direct file copy has taken place, there will be no scope for doing the normal DOS activities of searching for deleted files and browsing slack space. UNIX in general is a lot tidier than DOS and a deleted file tends to mean deleted! A block by block disk transfer would provide more information but would be more difficult to analyse.

The files themselves may be of many types. There can be ASCII files, executables, shell scripts, encrypted files, compressed files, character special files, data files, links and so on. It is important to understand the file type before trying to examine the contents.

It is also necessary to take account of the permissions on the file. In the example above, the file has read/write permissions for the owner, and read permissions for everyone else. In theory therefore it is not possible for anyone other than the owner to write to it.

Not so! There is also a dependency on the permissions set on the owning directory. If the directory permissions are lax, then although direct write access to a file may be not possible, the file could be replaced or over-written by anyone.



As with DOS, date/time stamps are unreliable. The touch command is normally available on UNIX which can be used by users to set the date/time stamp to any desired value.

Log files may prove a good source of information, but once again, their existence and location will depend upon a) whether they have been set-up and b) the variant of UNIX in question. On 'standard' UNIX there are no tools for undertaking analysis of log files.

The system under investigation may also be running database applications such as Oracle. This again will introduce a further level of complication, as any investigation will need to examine and interpret the audit log files. Users indeed may have no direct shell access (i.e. access to operating system commands and utilities), all their actions being undertaken via a user-interface. The investigation will need to determine what level of application auditing is implemented and how much is available for investigation. It will also need to determine whether 'shell escape' is possible.

The Feasibility of UNIX Forensics

Capturing data for forensic analysis from UNIX systems is of course entirely possible. However, it will never be as simple as the current methods on PCs for the reasons given above. The concept of a 'fool-proof' method for undertaking the capture of data from UNIX for subsequent analysis is unlikely to come about in the near future.

The sheer number of variables, and the complexity of some of these systems means that a different methodology and different tools are required from those currently available in order to undertake such work. It is almost certain that an investigator will require detailed input from a UNIX systems/security specialist in order to maximise the chances of a successful investigation.

A further reason for this is that if a system has been compromised, it is important to ascertain the overall security of the system (or lack of it). Products are available to highlight security problems on systems and will unearth problems on the system which may seem, on first inspection, to have nothing to do with the offence but subsequently may prove conclusive in determining how an attack was carried out.

Furthermore, hackers' tools are widely available on the Internet and these tools can be used to hide or mask a large range of illicit activities. It is difficult, though not impossible, to uncover these tools manually.

Much will depend on the overall security culture of the company. If the culture is strict, there will be a much greater chance of ▶

uncovering evidence from an investigation. However, if the culture is lax there may not be much benefit in undertaking a lengthy and what could be expensive investigation.

Prevention is always better than cure. For many companies who move their business onto computers without understanding the risks and taking appropriate defensive measures, the question is not so much if they are going to be attacked but when. There are also sobering statistics that 94 per cent of all computer attacks go completely unnoticed, while 80 per cent of all computer related crime is carried out by organisations' own staff. ■

About the author

Craig Cameron is a principal consultant with March Information Systems Ltd. Craig is a specialist in information security and has been involved in a large number of investigations into suspected and actual computer related crime on both PCs and large multi-user systems.

March Information Systems Ltd. is a consultancy and software business which was established in 1990. The company is focused on open systems and provides services in systems integration, systems management and security.

Author's note

This article is not intended as a guide to undertaking forensic investigations on UNIX systems. It is written from a point of view of understanding UNIX security issues and vulnerabilities and aims to highlight some of the issues investigators may face, as well as demonstrating the need for expert assistance and software when investigating suspected computer related crime on large multi-user systems.

The author does not claim to have any prior experience of undertaking formal forensic investigations on UNIX based systems.

March Information Systems Ltd. has developed Security Manager, a UNIX and Windows NT security and integrity management system. Security Manager highlights security problems on systems and advises administrators how to fix them. It also has the ability to parse system log files looking for specific events which may indicate activity which requires investigation.

Water Damage

Water can cause extreme damage to computers and storage media, with the very real risk of losing stored data. But according to information retrieval firm Ontrack, all is not lost for the forensic investigator, as Paul Johnson finds out.

Recent floods in the US and Canada caused havoc for thousands of innocent victims, who have found their businesses and homes wrecked. Apart from the cost of damaged property, there was also the hidden loss of damaged computers and lost data.

Recovery firm Ontrack Data International specialises in all areas of data recovery and stepped in to help with the offer of free help for public organisations.

Chief Executive Officer of the firm Michael Rogers said: "We recognise the often priceless value of the data that is stored on the computers of flood victims. The hard drives found in the flooded computers may contain vital information needed to restart a business, continue corporate operations or maintain personal finances. When handled properly by an expert, this valuable data has the potential to be recovered."

But while flooded drives pose problems following accidents and natural disasters, they can also pose huge problems for the forensic computer investigator faced with the task of retrieving valuable, incriminating evidence.

In one case, a gang of credit card fraudsters thought they had taken precautions against any police raids by leaving a window open. If they were surprised suddenly, they intended to throw their external hard drives out into a swimming pool below, in the hope of destroying all the data.

In this case the police were wise to the tactics and pre-empted the gang by actually entering the room through the escape-route window.

A second example occured after the liner the Estonia sank several years ago. The only complete passenger log was stored on the purser's computer onboard the ship, which was lying in hundreds of meters of water.

As criminals begin to realise that merely deleting files will not cover their tracks, they will look at different ways of getting rid of evidence, with disposal in water being an obvious choice.

Being able to retrieve and analyse drives found in water, be it fresh or salt water, could easily make all the difference in an investigation and prosecution.

Water harms the data stored on disks in two main ways. First, it causes electrical damage which makes the information inaccessible to the user. Second, when media is submerged, the water may leak through the seals spreading dirt and contaminants onto the storage area.

Indeed, storage media affected by water suffers not as much from the water itself, but from the impurities found in the water.

Ontrack has put together a lab guide to help investigators increase the chance of preserving data.

- Never assume that data is unrecoverable, no matter what it has been through.
- Send the media to a professional data recovery service as soon as possible.
- Do not shake the media or, in the case of hard disk drives, remove the cover of the assembly.
- Do not attempt to dry water-damaged media by opening it or exposing it to heat and never freeze dry the media.
- Do not attempt to operate visibly damaged media. Waiting for it to dry out and then operating it on your own is the worst thing you could do.
- Do not attempt to clean the media without using proper solutions applied in a clean room environment. Contaminated media requires immediate and thorough cleaning.
- Do not try to recover data with commonly available software utility programs.

Hard drives flooded in salt water require special treatment. Because data can be damaged quicker due to salt oxidising on the media, the drive should be express shipped in an airtight container to a professional data recovery service facility. To reduce the risk even further, drives can be bathed in distilled or fresh water, although they should not be agitated. ■

The Singapore Police Force

Computer Crime Branch

In last month's Journal, we gave an overview of the Singapore Computer Crime Branch. Here, in the second part of the article, Assistant Superintendent of Police, Mr Tan Swee Wan, discusses the laws and working methods as well as providing two case studies.

The Computer Crime Branch of the Singapore Police Force was set up in January 1997. It is made up of four senior officers and five junior police officers. The roles and responsibilities of this branch include:

1) Computer crime investigations.
2) Telecommunication fraud investigations.
3) Computer forensic examinations.
4) Development of computer crime and computer-related crime investigation and training doctrines.

This branch of the TechnoCrime Team is under the Financial Fraud Branch of the Commercial Crime Division, Criminal Investigation Department. This team was formed in 1995 with two senior police officers to conduct computer crime investigations, telecommunication fraud investigations and computer forensic examinations.

The team slowly grew from two men to four men and in 1996 it recommended to the management to form a computer crime branch. This was approved and the Computer Crime Branch was set up.

Computer Misuse Act

The Computer Misuse Act, enacted in August 1993, is the main piece of legislation defining the parameters of investigations into computer crime in Singapore. It created four major offences:

1) Unauthorised access to computer material.
2) Unauthorised access with intent to commit or facilitate commission of further offence such as offences involving property, fraud, dishonesty or which causes bodily harm punishable on conviction with imprisonment for a term of two years or more (Section 4).
3) Unauthorised modification of computer material (Section 5).
4) Unauthorised use or interception of computer services. (Section 6(1)(a/b).

All offences, except for Section 4, carry punishment of imprisonment not exceeding two years and/or a fine not exceeding S$10,000. The enhanced punishment is imprisonment not exceeding five years, fine not exceeding S$20,000 or both. As for Section 4, the punishment is imprisonment not exceeding ten years and/or a fine not exceeding S$ 50,000.

The common ingredient in all these offences is unauthorised access, which is defined under Section 2 (5) of the Act that if a person:

a) Is not himself entitled to control access to the program or data, eg hacking.
b) Does not have consent from an authorised person to access to the program or data, eg using passwords of others.

Section 14 of the Act states that an officer investigating an offence shall be entitled to access, inspect and check the operation of any suspect computer, device or material. He can also require the user or person having charge of the computer to provide him with reasonable assistance for such a purpose.

Computer related crime

The Computer Crime Branch does not investigate computer-related crimes as these are handled by other police investigative units. However, in the event that computer forensic examinations need to be carried out to retrieve incriminating evidence, the Computer Crime Branch will be called in to assist.

Recent cases that investigators have been involved in as forensic examiners have included illegal gambling, paedophilia, and an investigation relating to forged government documents.

Case studies

In a recent crackdown on an illegal lottery collection in Singapore, the Gambling Suppression Branch of CID sought the help of officers from the Computer Crime Branch. The lottery, called 4-D, is a system where people place bets on a four-digit number and the results are dependent on horse races. It was suspected computers were used in the commission of the offence by the syndicate.

Investigations revealed the computers were connected together via a network over telephone lines. Bets were received on various outlets and keyed into the computers (dummy terminals) and then transmitted over the network to a remote computer.

In other cases, information on betting was captured electronically on disks at the outlets. The files were then zipped, encrypted and sent to another site where the information was retrieved and stored in a database.

The computers were seized and sent to the Computer Crime Branch lab for examination and analysis. The officers retrieved the betting information and they also decrypted some of the compressed files. This information was then sent back to the Gambling Suppression Branch for analysis.

The information retrieved was instrumental in the on-going investigations and provided incriminating evidence against the suspects.

Distribution of pornography

In one particular case, police received information that someone was distributing pornographic material. The police set up a trap-purchase which led to the arrest of two male persons. Investigations revealed that the accused distributed pornographic material on floppy disks for sale. A raid was conducted and a computer system and numerous floppy disks were seized. They were then sent to the Computer Crime Branch for forensic examination.

With the use of specialised examination tools, which were not available previously, the examination officer was able to search through a large volume of files in a systematic way, and retrieved all the evidence required for efficient prosecution. ■

Images - Virtual or Real

The definition of a computer data image has important consequences for the investigator and in any subsequent proceedings in a court of law. Here Jim Bates looks at the practical and theoretical meanings.

Some time after I originally coined the concept of "imaging" a fixed disk drive, the term came into general use to indicate the collection of all stored data rather than just the content. It now seems to be used quite freely in ways which diverge from the original idea and it may be useful to clarify some of the misconceptions which have arisen.

It is generally accepted that information on computers is media independent and its correct interpretation depends upon content, location and condition. A simple file copy of the contents of a fixed disk would certainly reveal the content and a little of the condition (active, date/time/attributes etc.) but only of active files. The unallocated space, slack space, directory clusters, system areas and non-system areas are not collected by just copying files.

However, in general terms if the fixed disk is addressed directly by the firmware (i.e. ROM) then all of the stored data becomes available. Information copied in this manner may then be rebuilt into a reasonably accurate facsimile of the original drive and use of the relevant operating system should enable meaningful access to the active, deleted, unallocated, slack, directory and system areas. The process of rebuilding can be done physically by copying each sector from the original drive to its corresponding sector on a forensic drive and the forensic drive can then be called a "real image".

It is also possible to access a sector by sector copy of the original drive (usually in file form) using specially written software which "understands" the various operating system formats. When this is done, the structures produced by the special software may be called a "virtual image".

While I am delighted that my original simple conception has gained such widespread acceptance it is important that forensic investigators should appreciate the vital differences between real and virtual images.

Although a similar level of access is generally available with either system, there are compelling reasons why a real image is easier to examine than a virtual image. A major advantage is that a real image can be treated exactly like the original drive and a boot cycle into the resident operating system can be initiated. Thus the software environment matches the original to a very high degree and it is usually possible to directly execute software on the real image to

gain meaningful access to the data files.

It may also be desirable to implement access control devices in order to reveal their secrets - this may be difficult or impossible when using a virtual image. The usual implementation of the virtual image idea creates sector copy files on CD-ROM media because they are considered secure and inexpensive.

The limitations here are that CD-ROM capacity has fallen far behind fixed disk capacity and it is usual for the sector copy file to be fragmented across two or more CD-ROM disks. This adds complexity to the virtual imaging process and requires additional expensive hardware capable of multiple CD-ROM access. Thus a fragmented sector copy of a 2 GB drive will require at least three CD-ROM drives or a juke box disk changer to provide a directly accessible virtual image.

With this system there is no possibility of even virtual execution of copied software unless additional complex procedures are implemented to handle the fragmentation of the virtual image and the inability of the suspect software to complete any write functions. Another problem here is that CD-ROM writing requires a consistent stream of data at a guaranteed transfer rate and it is not possible to accomplish this from an unknown drive.

The solution is to either copy the data to an intermediate drive before writing it to CD-ROM or to profile the unknown drive to determine transfer rate and error mapping. Either of these processes increases the complexity (and thus the possibility for error) facing the operator during the copying process.

There are a number of alternative copying systems using various combinations of the techniques noted above but all of them can eventually be resolved into either a real image system or a virtual image system by determining their final method of accessing the data during investigation.

Since it is this investigative access method which addresses the image, it is misleading to call the intermediate sector copy files "images" or "image files". One final distinction is worthy of note: a true real image copy would be that created by copying sector by sector from one fixed disk to a similar fixed disk. Thus the copy would be directly and immediately accessible in a meaningful manner.

A sector by sector copy taken first to some intermediate media (whether fragmented or not) and then rebuilt onto a suitable fixed drive may still be called a real image but is one stage removed from the "true" real image. The advantage of course is that if the process is correctly implemented, exactly the same hardware that was used to make the copy can be used to rebuild it. ■

Jim Bates is President of the Institution of Analysts and Programmers in the UK

Cluster Analysis

Computer investigators have many tools at their disposal to copy and analyse information taken from a suspect's machine. One recent development is the ability to examine and collate evidence on the data's physical attributes to try to find something about its history on the computer.

Data stored on computer fixed disks must be considered as comprising content, location and condition. The content is self-explanatory, even though it may require appropriate interpretation before its textual intelligence becomes clear.

The location however, is another matter. Where MSDOS is concerned space on the disk is allocated in clusters where in a specific configuration on a particular drive the cluster is a fixed size. The 16 bit FAT system allows up to 65520 clusters on a single logical drive and these are numbered from two up to the maximum available on that particular drive.

The actual process of allocating space varies slightly with different versions of MSDOS but the internal system remains the same. Thus if a cluster is allocated for use by a file, its existing content is only overwritten by data written to the file (i.e. it is not zeroed before use). It is this peculiarity which gives rise to the phenomenon of slack space

However, if a cluster is allocated for use by a subdirectory it wil be zeroed before use and initialised with two 32 byte entries at the beginning of the cluster. These entries are referred to as the parent and subparent entries and are characterised by a single and double dot in the filename area of the respective entries. Each of these entries will contain the date and time extant on the system at the time the directory was created and these will usually match the date/time details in the original directory entry.

Thus if a directory called WINDOWS is created on 1st January 1997 at exactly midday, the first cluster containing the file entries within the WINDOWS directory will begin with parent and subparent entries also dated 1st January 1997 at 12:00:00. From a forensic point of view this can be extremely important.

Consider first a machine where the owner knew that the machine was going to be seized and copied. For reasons of his own he decides to defragment and wipe the disk to remove all traces of deleted files. The defrag process will copy cluster contents from one cluster to another as it executes, finally resulting in all active data being tidily located at the beginning of the disk. Depending upon the options selected, files and or directories may be reorganised into alphabetical order or matched within directory/file groups. However, the dates and times on directories will not have been altered and the resulting inconsistencies may be a valuable indication that defragmentation has taken place (even after some time when further processing activity may have taken place). Consider now another situation where the computer owner has decided to first delete all incriminating material, then backup all the active files onto some form of external media. He then wipes the disk and finally restores the backed up data to the disk. In this instance, each directory will have been "created" (rather than simply relocated as with defragmentation) during the restore process and the dates and times will reflect this. A recent case where this had happened became immediately obvious when a map was drawn of cluster allocation and coloured according to date/time markings.

The downloading of files via communication channels (such as the Internet) can also leave tell-tale signs of a particular sequence of events where a number of files may often occupy consecutive contiguous clusters within the chosen download directory.

Another fruitful area of investigation can be the presence of deleted file entries and/or deleted or redundant directory entries. For example, a deleted file entry specifying a ZIP file of some length was found within an active directory but the first cluster had been re-used by a later file. Under normal circumstances this would render the recovery of the file virtually impossible. However, the later file was only a few bytes in length and the

slack space of that cluster together with the contents of subsequent clusters (up to the length of the ZIP file) were extracted and concatenated to produce a damaged ZIP file.

The header area was partially repaired and the PKZIPFIX program was invoked to complete the repair. The result was a number of evidentially valuable image files recovered from the ZIP file.

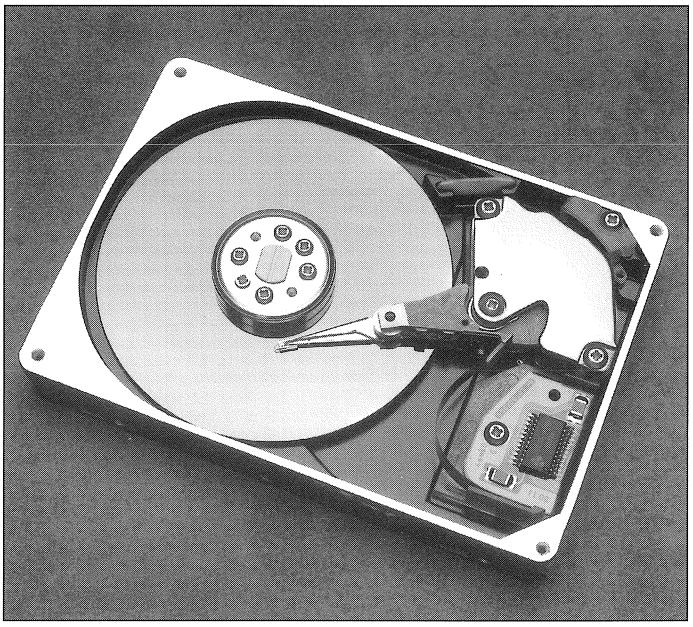
The examination of unallocated and slack space which contain fragments of previously deleted directory entries can also be extremely valuable in determining previous activity or directory structures on the system. These may remain "linked" in that existing deleted entries point to them or they may have become redundant when the original entry was overwritten. Whatever their antecedents, the recognisable MSDOS file entry structures can be interpreted and displayed to show their various dates, times and pointers. The whole business of examining and analysing the highly specific contents of directory entries both in isolation and as part of a coherent whole has blossomed into a process known as cluster analysis.

Some quite spectacular results have been achieved on cases to date and additional techniques may come to light as the process is expanded. However it is achieved, it is a powerful technique which the computer forensic investigator cannot afford to ignore.

Interpreting the Results

Great care must be exercised when interpreting the results of cluster analysis. The first thing to remember is that clusters are preorganised blocks of space which are allocated and deallocated as required by the operating system. It is this allocation and de-allocation which can be so important in determining a possible sequence of events leading to the observed patterns of cluster allocation. For example, consider a new machine with only the system software on the fixed disk. Installation of additional software will gradually fill the available space from the lower clusters to the higher ones. Most installation routines will automatically create one or more sub-directories and copy the files into them.

Once installed these files will rarely be moved. Such a process will show up during cluster analysis when virtually complete directory trees occupy a single block of clusters and each directory cluster is followed by its contained files.



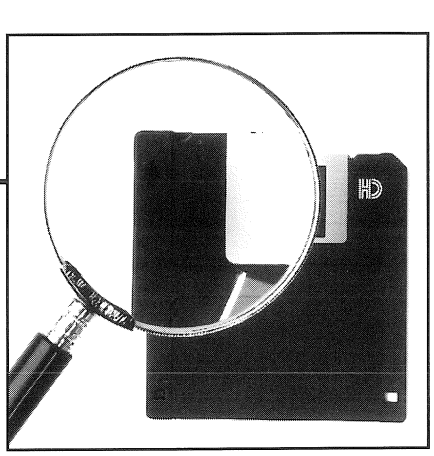
Other events, particularly defragmentation or restoration, may show distinctive signs. Unfortunately there is no substitute for experience when attempting to identify these signs. For example, normal use of a computer is extremely unlikely to create a directory occupying more than one cluster which is NOT fragmented. If you find a directory occupying two (or more) contiguous clusters the chances are that the machine has been defragmented at some time.

In another example, virtually every directory on a machine was dated the same day and timed within a few minutes of each other. Directories were followed by files in a repeating sequence across a large portion of the disk. Unused and slack space was all zeroes. It was known that the suspect had two days notice that the police were coming and the diagnosis (subsequently confirmed) was that the suspect had backed up the illegal disk contents to a tape, then deleted them from the disk. He had then backed up the remainder of the disk to another tape and wiped the disk back to zeroes. Finally he had restored the second tape. Fortunately he had forgotten to delete the tape catalogue file after the first backup and it therefore appeared on the machine. Thus there was at least a list of the illegal files that he had backed up.

Tests of various defrag programs seem to indicate that directory dates and times are not changed during defragging. It is worth remembering that the date and time of a subdirectory are stored in three places - twice in the directory itself and once in the entry which points to it. Thus in the Root directory each entry contains a date and time. In a subdirectory cluster the first two entries are named "." and ".." - referred to as "dot" and "dotdot" or subparent and parent respectively. The dot (subparent) entry points to the cluster occupied by the directory - i.e. it points to itself. The dotdot (parent) entry points to the cluster containing the previous entry in the path - if the cluster number is zero then the pointer is set to zero. In both cases the date and time should match that stored in the parent entry. If it doesn't then there is something suspicious going on and further investigation is warranted. Fairly obviously defraggers need to alter these pointers and so they are quite capable of also changing the date and time. However, this has not been noticed yet.

Note also that the fragmentation condition of a file does not necessarily indicate whether the file was processed in situ or copied there from somewhere else. However, the intervening clusters in a fragmented file might give some indication concerning what was on the disk at the time the file "arrived". ■

Forensic Q&A



Q *Is there a 'work around' for investigating a suspect hard drive that has password protected programs on it?*

A I am not sure what you mean here but I will assume that you need to run a program that is on a suspect hard disk in order to read the data files. This is frequently the case with programs such as accounts packages where the individual data files are only meaningful when run within the creating program.

The first point I must make, of which I am sure you are aware, is that you should never try to run programs on original suspect material. Doing so would alter the contents of the hard disk and invalidate the integrity of any evidence. Always use copied material. If you have only one copy then you must ensure that it is write protected before trying to run the program. Preferably run only copies of copied material. Then, if things go wrong, you can always delete the second copy and start again with a new copy.

The two options you have when faced with accessing password protected programs are:

- to disable the password protection
- to copy the required data files and read them in a non-password protected version of the program

The effectiveness of the first option, disabling the password protection, varies according to the program. Some programs have surprisingly simple password protection that can easily be circumvented. Others are much more secure. In either case you will probably need advice. If your own local or national force is unable to help try the software manufacturer. They may be willing to help once they appreciate that it is a genuine investigation.

The second option is often the most practical. Obtain a copy of the program (an objective of any computer forensic analyst should be to build up a library of programs and any new program acquired is likely to be used again in the future) and install it to a working drive. Then copy over the data files. You may need to experiment to get the right files. Hopefully the information will be accessible. However some password protection works by encrypting the data files. If this is the case then you will have to revert to the first option or contact an organisation that specialises in decryption.

One final point. If you have access to the suspect try asking for the password. It is surprising how often it will be given, once the suspect is aware that withholding the password will not prevent you accessing the information but just cause inconvenience.

Editors Note: If you need advice on who to contact for assistance with passwords we are happy to pass on contact details. Telephone or e-mail us.

Q *Is it acceptable procedure to load other software onto a suspect hard disk in order to view the data?*

A No. Under no circumstances should this be done. If you load other software onto the disk not only will you destroy evidential integrity but you may also write over evidential material which is in unallocated areas of the disk such as deleted files. Only ever work on copied material and examine this with software loaded on another drive. A standard forensic workstation set-up will enable you to do this easily. This has three removable drives. One of these is the forensic drive which is used to examine suspect data. The second is the information to be examined. And the third is the working drive that is used to contain work in progress. Using this type of equipment and following recommended procedures the validity of any evidence produced will be assured.

Q *I have been examining a copy of a hard disk on which I believe there are zipped files which have been renamed. How can I find them? There are over 13,000 files on the computer.*

A Obviously with this number of files it is going to be extremely time consuming and tedious to manually check each and every file. The only practical solution is to use a dedicated search engine that has the ability to identify file types by reading selected header information or looking at the distribution of ASCII characters within the file. The latter technique is currently under development and although some success has been achieved it is still too 'hit and miss' to be used reliably.

Identifying files by selective header information is currently available and is very reliable for certain types of files for which the necessary identification strings have been researched. Some of those currently available are zipped files, common graphics files (JPG, GIF, BMP) and common wordprocessor files. These have proved totally reliable in use and the range of search targets can be expected to increase as more identification strings become available. ■

If you have any tips, advice or cautionary tales you would like to share with readers, please contact the Journal.
e-mail your questions and comments to ijfc@pavilion.co.uk

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

Notice Board

EVENTS

'Who's Watching You? Trust, Security and Privacy on the Internet'

23 June, San Francisco

A half-day workshop to address concerns about trust, security and privacy. Sponsored by CommerceNet, the industry association for promoting and building electronic commerce solutions on the Internet. Launched in April 1994 in Silicon Valley, California, its membership has grown to more than 500 companies and organisations worldwide, including banks, telecommunications companies, VANs, ISPs, online services, software and service companies, as well as end-users.

Contact: CommerceNet
Tel: 415 858 1930
Fax: 415 858 1936

Security - What's New

1 July, Chester, UK
15 July, London
16 July, Heathrow
Contact: Direct Contact Exhibitions
Tel: +44(0)1782 265511
Fax: +44(0)1782 202761

Security Israel '97

1-3 July, Tel-Aviv
Contact: Sigma Team Ltd
Tel: +972 3 629 0055
Fax: +972 3 528 1822

Electronic Commerce Security Conference

4-5 August, Arlington, Virginia
(Pre-conference programme will be held on 2-3 August)

Over 20 educational sessions will be presented including Management Essentials, Legal Issues, Vendor Presentations and an Introduction to Cryptography. Benjamin Wright, author of "The Law of Electronic Commerce" will moderate a panel discussion entitled "Future Directions". Dr Dorothy Denning will speak on the "Use of Encryption by Organised Crime". The pre-conference programme will be offered by Dr Mich Kabay, Director of Education at the National Computer Security Association.

Contact: NCSA
Tel: 717 241 3233
Fax: 717 243 8642

Networks Telecom

23-25 September, Stockholm

Computer networking, telecommunication, connectivity and communication; including practical user education.

Contact: Miller Freeman Scandinavia
Tel: +46 40 24 80 80
Fax: +46 40 24 85 06

UNIX Expo and Banking

10-13 October, St Petersburg

UNIX and open solutions for government ministries, scientific and educational institutions, banking and financial organisations and commercial companies.

Contact: Miller Freeman Inc/WPI
Tel: 201 346 1400
Fax: 212 750 8568

UNIX Security

12-13 November, Maidenhead, UK

The course considers the development of the UNIX operating system from a security point of view. Several currently available UNIX systems are examined and the work under way to develop high security UNIX variants is considered.

Contact: Zergo Ltd
Tel: +44(0)1256 818800
Fax: +44(0)1256 812901

TRAINING

Training in Computer Forensics

Four modules comprising:
Fundamental Computer Forensics
Applied Computer Forensics
Advanced Computer Forensics
Legal and Procedural Computer Forensics
Courses held monthly in West Sussex.

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

Cryptanalysis

A new one-day course covering the latest issues in computer cryptography and cryptanalysis. Aimed at law enforcement officers, military personnel and private companies, the class includes the basics of crypto design, isolating weaknesses in commercial systems, the Internet, electronic commerce and international issues in cryptography. The course, lead by Eric Thompson, Cryptographer at New Technologies Inc., is held in Eugene, Oregon, US. The cost is $995 per person including all materials

Contact: New Technologies Inc.
Tel: 503 661 6912
E-mail: info@secure-data.com

Call for Papers

from The Internet Symposium on Network and Distributed System Security March, 1998, San Diego, California.

The symposium will foster information exchange between hardware and software developers of network and distributed system security services. The intended audience is those who are interested in the practical aspects of network and distributed system security, focusing on actual system design and implementation, rather than theory. Encouraging and enabling the Internet community to apply, deploy, and advance the state of available security technology is the major focus. Symposium proceedings will be published by the Internet Society. The committee invites technical papers (10 to 12 pages in length) and panel proposals, for topics of technical and general interest.

Contact: Matt Bishop, Dept. of Computer Science at University of California.
Tel: 916 752 8060
Fax: 916 752 4767

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

Published by
Computer Forensic Services Ltd.