MASTERING COMPUTER FORENSICS

Colin J. Armstrong
Curtin University of Technology, School of Information Systems, Perth, Western Australia, email ArmstrongC@cbs.curtin.edu.au

Abstract: This paper discusses the importance of computer forensics to both business and law enforcement environments and describes the passage along the path from act of crime to the court. It highlights the need for computer forensic training and education and gives an overview of the computer forensic course taught in a Masters degree at Curtin University.

Key words: Computer forensics, Masters Program, security education, system administrators, law enforcement, crime investigation.

1. INTRODUCTION

Police are responsible for upholding the law and investigating, apprehending and prosecuting breaches of the law. The successful prosecution of computer based crime is reliant upon the investigator being able to prove beyond a reasonable doubt who, what, how and when a criminal event occurred within the stringent principles of forensic examination of evidence. Computer crime is of such a nature that it is often difficult for the general public to perceive or to understand that a crime has actually occurred. Criminals are using computers to store records regarding drug deals, money laundering, embezzlement, mail fraud, telemarketing fraud, prostitution, gambling matters, extortion, and a myriad of other criminal activities (Icove et al, 1995). The victim may be a large corporation, may be far away, or may be considered an unfriendly nation, competitor or even an enemy.

The nature of the Internet provides a borderless environment, easy anonymity, concealment of activities and new low cost tools with which to perpetrate crime (Vatis, 2000). Evidence that computer and Internet crime

C. Irvine et al. (eds.), *Security Education and Critical Infrastructures*

incidences continue to in increase is confirmed in publications such as the annual Computer Security Institute report. (Powers, 2002) Computer crime is on the increase but there are indications that some public perception of malicious abuse may be inflated. Furnell, (2002) discusses how some figures relate to reported incidents from one particular set of surveys and that the true level of computer crime may be much higher because much is not reported due to risk of undesirable consequences; bad publicity, legal liability, loss of custom. Also financial loss is only one type of impact. Others include; disruption of service, loss of data, damage of reputation and these are difficult to quantify and could be more significant (Furnell, 2002).

An investigation of computer crime may use tools, procedures and methods not readily be available to the public and therefore not be readily understood and accepted. For these investigative findings to be accepted they must be recognised by other experts within the field and conform to national and international standards of practice. The risks facing a computer forensic investigator include loss of credibility if another expert witness can demonstrate that proper or appropriate courses of action were mismanaged. It is the role of the independent expert to explain technical issues in layman's terms so that the judge, jury, accused, barrister and solicitor alike can understand the evidence put before them (Armstrong, 2002).

This paper discusses the needs of law enforcement and IT professional in computer forensic training and education. An overview of a course in Computer Forensics in a Masters program at Curtin University is also presented.

2. THE CRIME TO COURT PATH

Kruse and Heiser (2002) suggest that cyber lawyers are constantly facing a changing legal environment and need to be flexible and learning continually. There are two particular participants in the battle against computer crime that would benefit from education and training in computer forensics. They are the systems administrators of corporate computer systems and the law enforcement investigators. Both may be required to present prosecution evidence in a court of law either as an expert witness or a prosecuting officer of the law. If the representatives for the defence can reduce the credibility of the prosecution case the prosecution may fail.

Law enforcement offices investigating computer related crime are often introduced to the case well after a criminal act has been discovered. The offices carrying out computer forensic investigators most frequently commence their activities part way along the crime to court path. The path shown in Figure 1 commences when the criminal act is committed and

continues through to prosecuting the case in court. Figure 1 also shows the points along the path where the involvement of systems administration and law enforcement personnel start, overlap and fade into the background.

After a computer related criminal act is committed, it may be some time before anyone notices. The act may be first noticed by friends or family at home but as many acts are committed on networked computer systems in the work place, educational institutes, or public facilities such as Internet cafes, it is the systems administration staff that will probably have their curiosity attracted when they notice unusual activity. To satisfy this curiosity a period of observation would clarify whether further action is justified. Assuming that an act justifies further action it is reasonable to expect evidence to be sought to confirm something untoward is in progress. This leads to the suspicion being confirmed and at this point one could state that the criminal act has been discovered. It is at this point that someone will decide to either ignore and forget the matter, or to continue along the path and to collect evidence to support a response to the situation.

This is another critical point along the path because now the decision required is to either deal with the matter privately or to advise law enforcement authorities. Until this stage the responsibility for action resides with computer systems administration personnel and no law enforcement office is involved. Once a law enforcement agency is advised of the situation and they commence a crime investigation the situation changes dramatically. It is now imperative that activities comply with accepted practices and nothing is done to jeopardise a successful prosecution. Law enforcement offices may now seize digital data and identify and preserve evidence. From about this point along the path the systems administration staff fade into the background and law enforcement offices take control and responsibility for the case. They will copy, analyse, and interpret the data before presenting the prosecution report in court.

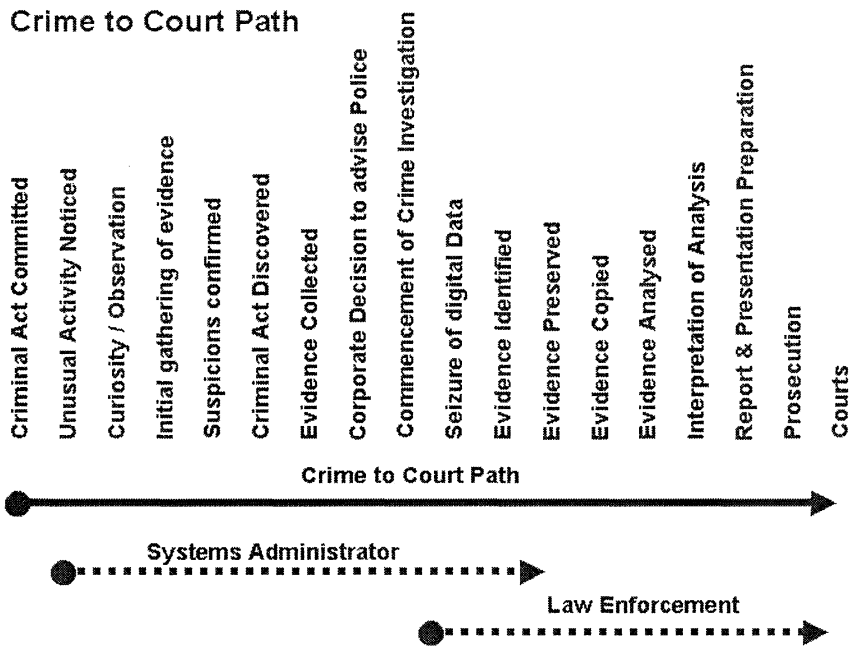

Figure 1. Crime to Court Path

Figure 1 shows that the systems administrator may be critical to the success of a prosecution case because their early recognition of a situation and their subsequent actions may either greatly assist or hinder the work done by law enforcement offices. Although they have distinctly separate and vastly different roles and responsibilities, by working in concert they may dramatically improve the chances of bringing about a successful result to a prosecution case.

The danger of criminal activity not being successfully prosecuted due to the failing of a computer forensic process is very real. This is further exasperated by the provision of advice that works against the objectives of computer forensic investigators. Advice given by Bologna and Lindquist (1995) discusses how to use a computer, modem, communication software, procomm, tymnet and databases such as TRW and D&B. They then state that, "You are now ready to dig into files. The procedure is to (1) turn on the PC; (2) insert the communications software diskette in the A: drive; (3) when the program is loaded, dial up the database provider; (4) when connection is made, sign on with your user ID and then your code name; (5) when the menu is displayed, select an area of interest and follow instructions." (Bologna and Lindquist, 1995). Further, in discussions on

forensic accounting of large computerised account systems Bologna fails to acknowledge computer forensic science in any way (Bologna and Lindquist, 1995). Anyone following this advice will seriously compromise any prospective computer forensic investigation because the very search for evidence will intrude and alter critical files. A primary principle of computer forensic investigation is to conduct any analysis of digital evidence on a replication of the original data after it has been gathered in such a manner that the original data is not contaminated or altered.

While an investigation may be considered successful because a conviction was gained many convictions result from the suspected criminal confessing to an accusation and the need to prepare and present conclusive evidence is not demanded. In some cases the computer evidence is collaborating or circumstantial evidence that supports, but is not essential to, a case. In a recent Perth murder case, the female suspect admitted killing her husband after evidence showed that she had visited two Web sites. One site was on how to hire a hit man and the other on how to dispose of a body. In other situations the perpetrator of the crime may be a professional and much respected computing expert familiar with how evidence may be obtained and too clever to be easily incriminated. In this type of case a more in-depth investigation may be required to produce evidence for prosecution and the evidence presented may include very technical concepts relating to sophisticated tools and systems that requires to be explained in non-technical terms so that members of the court will comprehend the issues.

The credibility of an expert witness may be crucial to the outcome of a case and where the volume of work and the increasing number of investigations demand quick results there may be a tendency to select new automated examination and analysis tools. Government agencies within the USA have approximately 1400 active cases of cyber crime being investigated and this number does not include the myriad of cases where computers have been seized and evidence gathered and analysed to support other crime cases (Hatcher, 2001). Under these circumstances there is a potential to discredit expert witnesses because as "point & click" wizards they may be perceived to have little or no expertise and not understand what they have done, nor why (Barbin and Patzakis, 2002).

3. THE ROLE OF ACADEMIA

Academia has an important role in meeting the needs raised by this increase in computer related crime and the subsequent investigations.

The aim of teaching computer forensics is primarily to meet industry demands by addressing the needs of law enforcement personnel and those

that manage and operate computer systems. Academic research, teaching and training to support industry and law enforcement should improve confidence and credibility of investigators that result in better success rates of litigation which in turn may lead to crime reduction.

By comparing law enforcement requirements with existing solutions, the gaps in existing technology can be determined. By working together, researchers in academia, industry, and government can give our public servants the tools they need to address one of the critical public security and national security issues of the 21st century." (Vatis, 2002). This statement promotes the need by both law enforcement personnel and corporate system administrators to undertake training and education programs. Training in individual tools to improve competency skills and further education to enhance a broad understanding of concepts and processes related to subject that leads to gaining an academically recognised qualification. Together these help to improve the perception of being a creditable expert.

4. CONTENT OF A COMPUTER FORENSICS COURSE

In order to meet this demand from industry a computer forensic course has been designed to suit both law enforcement offices and IT professionals. The objectives of the course include developing an understanding of the principles and practices of computer forensics. By the end of the course students are expected to be able to understand and to practically demonstrate how to correctly access digital data equipment, obtain an exact working image, analyse the image and recognise evidence, then report their finding in an adversarial environment. The students are expected to maintain and document investigation notes, follow chain of evidence practices and have a thorough overview of computer forensic tools and the appropriateness of their use.

This computer forensics course is a core unit in the Masters of Internet Security Management. It is undertaken in the final semester of full-time study. This is to ensure that students have a knowledge base of Masters level units that includes network and communication security, operating systems and software security, business intelligence and cyberwarfare, encryption, and Internet security.

The course addresses the points along the crime to court path. Students from law enforcement agencies backgrounds will be able to extend their skills by engaging in the concepts on which the practices they apply in the field are based. Students employed in systems administration areas will gain a perspective of law enforcement issues and the practical application of

policing investigation practices. Students from these backgrounds would normally be expected to share their work place and field experiences for the benefit of the other students.

The content of the computer forensic course offered at Curtin University assumes a prior knowledge and understanding of network and communications security. Areas to be covered in the course include;

- computer forensic technology tools and concepts
- computer and Internet architecture
- isolation and seizing of equipment and files
- computer image verification and authentication
- data recovery
- investigation processes
- discovery of evidence
- chain of evidence
- national and international legal issues, rights and responsibilities

The course will be conducted over 12 weeks with each week consisting of three hours split between lectures and laboratory exercises. Students engage in practical exercises where computer forensic tools are used to capture, copy and analyses digital data so that the students gain an appreciation of the physical requirements of undertaking a computer forensic investigation. This is seen as a vital ingredient to the course. Currently, Curtin University academic staff are working closely with a number of law enforcement agencies on joint research projects and teaching programs. Students will investigate criminal cases taken from the public domain supported by evidence from enforcement agencies. Students are expected to take digital media and progress along the crime to court path to the extent where they will be expected to present their findings in a simulated adversarial environment.

The course will run for the first time in the second semester of 2003.

5. CONCLUSION

Law enforcement agencies are responsible for investigating and prosecuting breaches of the law. Computer related crime is increasing and the workload of investigators is growing.

New automated examination and analysis tools assist investigations but there is an established need to provide additional training and education

programs plus a need for University research to support computer forensic education.

The crime to court path shows points along the way from the time that an act of crime is committed through to when it is dealt with by the courts. It shows where IT professionals may assist law enforcement offices and at which point crime investigators take up a case.

An explanation of the Curtin University Master of Internet Security program put into perspective how the computer forensic course relates to and addresses the needs of industry and law enforcement officers.

The computer forensic course offered at Curtin University is designed to meet industry needs by adopting a practical application of knowledge approach.

REFERENCES

Armstrong, I. (August 2002) *Now in Session. The Judiciary and the Digital World,* SC Info Security Magazine. p19.

Barbin, D. and Patzakis, J. (2002) Computer Forensics Emerges as an Integral Component of an Enterprise Information Assurance Program, Information Systems Control Journal, Volume 3, p25.

Bologna, G. J. and Lindquist, R. J. (1995) *Fraud Auditing and Forensic Accounting (Second Edition),* John Wiley & Sons, Inc., New York.

Furnell, S. (2002).. *Cybercrime : Vandalizing the Information Society*, Addison-Wesley, London

Hatcher, T. (2001). *Survey: Costs of Computer Security Breaches Soar* . CNN.com, . Available on-line at : http://www.cnn.com/2001/TECH/internet/-3/12/csi.fbi.hacking.report/index.html . (12 March 2001)

Icove, D., Seger, K. and VonStorch, W. (1995) *Computer Crime. A Crimefighter's Handbook,* O'Reilly & Associates, Inc, Sebastopol CA.

Kruse, W. G. and Heiser, J. G. (2001) *Computer Forensics. Incident Response Essentials,* Addison-Wesley, Boston.

Powers, R. (2002) Computer Security Issues & Trends : *2002 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute. Available on-line at : http://www.gocsi.com . (9 November 2002)

Vatis. (2000) . Statement of the Director, National Infrastructure Protection Center, Federal Bureau of Investigation on Cybercrime before the Senate Judiciary Committee Criminal Justice Oversight subcommittee and House Judiciary Committee, Crime Subcommittee, Washington, D.C. February 29, 2000 . Available on-line at : http://www.usdoj.gov/criminal/cybercrime/vatis.htm . (14 December 2001)

Vatis, Michael. A. (June 2002). *Law Enforcement Tools and Technologies for Investigating Cyber Attacks. A National Needs Assessment.* Institute for Security Technology Studies, at Dartmouth College, Hanover, NH.