An overview of computer forensics

Phillip D. Dixon

Predators everywhere look for an opportunity to take advantage of innocent people at any given moment. Computers, in conjunction with the Internet, have given some of these predators a new tool with which to pursue their evil purpose. Due to the steady increase in instances of cyberterrorism, Internet fraud, and constantly evolving viruses, computer forensics has, and will increasingly, become more of a focal point for government and law enforcement. There are several steps and procedures that must be taken to reduce the risk of becoming a victim. There is also a plethora of tools available for use by trained individuals in the field of computer forensics. Some things can also be done to place a great deal of consequential fear in those who may be the culprits.

©2001 PHOTODISC, INC.

What is computer forensics?

The *American Heritage Dictionary* defines the term "forensics" as the use of science and technology to investigate and establish facts in criminal or civil courts of law. However, forensics was initially derived from usage in the medical field. The specialty of forensic medicine was a recognized discipline at the end of the 18th century. An autopsy was one of the most common forensic tasks performed at that time. Through the growth and development of forensic medicine eventually came the evolution of criminal forensics via the examination of fingerprints.

Although the general foundations of forensics is nothing new to us, the concepts and practices surrounding the area of computer, or IT, forensics is a quickly developing area of study. According to Gerhel, the widespread usage of computer forensics has resulted from the convergence of two factors: the increasing dependence of law enforcement on computing and the ubiquity of computers that followed from the microcomputer revolution. For the most part, computer forensics has grown and developed via standards of commonplace investigative theories used by the fields of law enforcement and security.

The core goals of computer forensics are fairly straightforward: the preservation, identification, extraction, documentation, and interpretation of computer data. There are several policies and procedures that need to be outlined and defined with regard to computer forensics. Data must be able to be retrieved and analyzed without it be damaged. At the same time we must be able to ensure the authenticity of the data. Without proper procedures, the forensic data could end up being useless in a court of law.

Current issues, trends, and tools

U.S. federal law is in place that requires federal organizations to report incidents to the Federal Computer Incident Response Center (FedCIRC), which is encompassed within the U.S. Homeland Security Department. The U.S. Federal Information Security Management Act (FISMA) of 2002 requires that federal agencies have set guidelines and tactics for responding to computer incidents. This act states that agencies are required to have an initial and secondary point of contact, report all incidents, and maintain internal documentation regarding corrective actions and any impact.

The capabilities outlined by the FISMA should encompass the following actions:

- Create an incident response policy.
- Develop procedures for performing incident handling and reporting, based on the incident response policy.
- Have set timelines for communication with outside parties regarding incidents.
- Select a team structure and staffing model.
- Establish relationships between the incident response team and other groups internally and externally.
- Determine what services the incident response team should provide.
- Staff and train the incident response team.

Each organization must have a definition of what it considers an "incident" to be. At one time a computer security incident was considered to be any occurrence in which data integrity may have been lost or confidentiality breached. These incidents could consist of any node or network activities that could potentially compromise security within the system or network. An incident could also be in the form of unauthorized usage of systems for storing or accessing data or unauthorized modifications to hardware or software on network or node equipment. In today's environment an incident may be defined as any violation or threat of violation of an organizations security policies, acceptable use policies, or standard security practices. To elaborate, the U.S. Department of Justice assigns cybercrimes incidents to the Computer Crime and Intellectual Property Section (CCIPS), which provides guidance on classifying a cybercrime. These types of crimes are usually targeted towards domestic computer related crimes. These crimes may range from computer-related forgery using falsified information portrayed as though it was authentic or computer related fraud that may cause fraudulent meddling with or exploitation of data

0278-6648/05/$20.00 © 2005 IEEE

to that can cause property loss. Cybercrime can also deal with the areas of e-commerce legal issues, encryption, privacy issues, and intellectual property issues just to mention a few.

Once these forms of crimes begin to infiltrate into the military and international environments, the term cyberterrorism may be more adequate. Dictionary.com defines terrorism as the unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons. In relation, cyberterrorism would be an unlawful attack or threat against computers, networks, or any electronic system with the sole purpose of intimidation or attempted governmental coercion to achieve some terrorist groups' political or social agenda.

The National Institute of Standards and Technology lists what it considers an incident to consist of (see <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>).

• *Denial of service attacks.* An attacker sends malicious packets of data to a Web server that causes it to crash. An attacker may direct hundreds of external compromised computers to send the maximum amount of Internet Control Message Protocol (ICMP) requests to an organization's network. See Fig. 1.

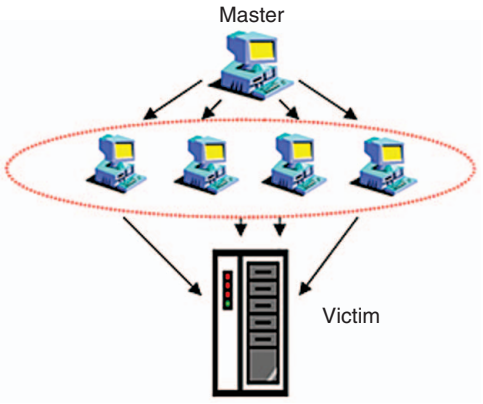

Fig. 1 In a distributed denial of service attacks, the attacking computer hosts are often zombie computers utilizing high-speed connections to the Internet that may have been compromised by virus or Trojan horse programs, permitting the intruder to remotely control the machine and direct the attack. Given enough such slave hosts, the services of even the most robust and well-connected Web sites can be denied.

• *Malicious code.* In this instance a worm may use open file shares to infect hundreds of computers in an organization. An organization may receive a warning from an antivirus vendor that there may be a new virus spreading by way of e-mail and the Internet. Based on previous antivirus incidents, an organization may expect the new virus to infect within a few hours.

• *Unauthorized access.* In this incident the attacker utilizes tools to access a server's password file. An intruder may gain administrator-level privileges to a system and then threaten to release the details of the intrusion to the press if money is not paid to conceal the breach.

• *Inappropriate usage.* This is when a user provides illegal copies of software for other people to use via peer-to-peer file sharing. If a person threatens another person via e-mail is another example.

In 2001, the Information Technology Information Sharing and Analysis Center (IT-ISAC) was formed to help the business world secure its assets. These assets include physical assets such as hardware and network infrastructure as well as logical assets such as software or warehoused data. This came about after several highly publicized attacks on Internet companies at that time. The project was originally conceived in 1998 by then-President Bill Clinton. Clinton urged government agencies to merge resources with various industries to create various information sharing and analysis centers to share information about threats. This has been very useful as the reliance of government services upon private sector resources has steadily increased in recent years. This is apparent in the October 2000 Department of Defense contract awarded to Electronic Data Systems Corporation (EDS). EDS, which provides information technology services and business solutions to its customers, was awarded a US$6.9 billion contract. The contract was to create a central portal for Navy and Marine Corps personnel allowing them to access applications and services electronically from one central Web interface. This contract was the largest ever awarded at that time and utilized hardware and software from various private sector vendors including but not limited to Cisco, Dell, MCI, and of course Microsoft.

Outsourcing of IT-related services oversees has also continually increased the level of risk associated with securing computers. A lack of international laws exists which would govern the legal ramifications of security breaches occurring at outsourced overseas facilities. Outsourced overseas personnel may also not be upheld to the same scrutiny regarding background checks and ethical business practices. The number of application development and analyst positions that are contracted to overseas firms has continued to increase. This has brought about caution when it comes to securing the networks they use. Though many companies would prefer to keep their security administration services as an in-house operation, many companies have grown to the point that the task is too big to maintain internally. Organizations usually know what they are good at and must admit if they do not have the expertise to provide adequate security to its systems. These organizations must ensure that the worst-case scenario is always evaluated before a decision is made to internalize security tasks or outsource security tasks.

Computer forensics tools

There is a plethora of hardware and software tools available to assist with the interpretation of forensic data. One software package, "Forensic Toolkit," is produced by AccessData <http://www.accessdata.com/Product04_Overview.htm?ProductNum=04>. The AccessData Forensic Toolkit can be used by both law enforcement and the private sector to run complete forensic examinations of a computer. It encompasses customizable filters that allow the examiner to weed through thousands of files including e-mail analysis. A few things that this package can do is locate supposedly deleted email on a computer. This feature is compatible with Outlook, AOL, Outlook Express, Netscape, Earthlink, Yahoo, Hotmail, Eudora, and MSN e-mail. The Forensics Toolkit also allows you to access and decrypt protected storage data within the registry.

New Technologies Inc. <http://www.secure-data.com> is a company comprised of private sector computer forensic software developers and retired federal computer specialists. The focus of the company was to compile a suite of tools that could be utilized by the government and business sectors is aid in dealing with malicious computer acts via criminal or corporate abuse.

Computer forensics and its relationship to the Internet

The vast majority of security threats imposed on organizations are possible because of the Internet. This connection of millions of computers all over the world that allows for the exchange of information and data has brought with it many security issues which must continue to be addressed. These issues include virus and worm propagation, spam, e-mail phishing, data theft, and other remotely exploitable threats including denial of service attacks. In today's world of terrorism we must not underestimate our level of dependence on technology and the Internet. This dependence has made the Internet a prime target for espionage and terrorism. The U.S. Department of Homeland Security's Computer Emergency Readiness Team has composed a National Strategy to Secure Cyberspace.

The National Strategy to Secure Cyberspace breaks down the cybersecurity steps and procedures that should be implemented for state and local governments, along with private companies and individuals, to be safe. Before the government could outline recommendations, they first had to identify where the weaknesses were. The initial weaknesses were identified as

- lack of senior management's attention
- lack of performance measurement
- weak security education and awareness programs
- failure of the U.S. government to fully fund and integrate security into capital planning and investment control
- failure to ensure that contractor services are adequately secure
- failure to detect, report, and share information on known or suspected vulnerabilities.

Once the shortcomings were identified, the U.S. government could then begin to analyze what should be done to correct the situation. There are four main points in which the government found the greatest need to address. The first was to strengthen counterintelligence efforts in cyberspace. This meant that the FBI and other members of the intelligence arena assume a more proactive approach in understanding the capabilities and motives of possible threats. Second, the government felt the need to improve attack attribution and preventative capabilities. This meant that not only the intelligence community but the U.S. Department of Defense and other law enforcement agencies needed to be able to quickly pinpoint the cause and source of cybersecurity threats. There should also be in place a process that prevents any attacks from penetrating vital systems and infrastructure. Third, the government felt the need to improve the level of coordination between the United States and the national security community with regard to responding to cyberattacks. This meant that U.S. national security, law enforcement, and defense agencies must all have open means of communication ensuring that criminal matters are referred appropriately. Fourth, the government wanted to reserve the right to respond in an appropriate manner. This meant that the United States did not want to limit retaliatory efforts to criminal prosecution. The United States wanted the right to be able to respond to an attack in a way which they deemed appropriate.

To additionally assist with combating high-tech crime, in April 2004 the FBI launched the National Steering Committee (NSC), a computer forensics advisory board. The goal of this committee is to provide an intergovernmental body that gives guidance and recommendations to the FBI regarding the Regional Computer Forensics Laboratory program. The assistant director of the Investigative Technologies Division said, "Computer forensics is one of the most specialized sciences available to law enforcement, making the RCFL Program one of the most dynamic tools we have to fight crime and terrorism." The main focus of the program is to provide expertise in the area of computer forensics to law enforcement agencies to assist with ongoing criminal investigations and/or prosecutions.

Training and education in computer forensics

The digital front line is where the battle is being fought between infiltrator and security analyst. Having properly trained individuals at the helm of government infrastructure is key in the defense of these systems. There is plenty of industry and government recognized certification programs in existence today. Some of these certifications are for specific platforms, and some are more generalized. Outlined here are some of the more notable programs that may be correlated to the specialty of computer forensics.

One of the most respected security certifications is the Certified Information System Security Professional (CISSP) that was developed by the International Information Systems Security Certification Consortium. The CISSP program certifies that an individual has a mastery of international standards of information security.

The International Association of Computer Investigative Specialists offers training and certifications that were initially only offered to those in the law enforcement community. However, anyone may now pursue these credentials. The key certification that they offer is the Certified Forensic Computer Examiner (CFCE). This certification involves two weeks of training that teaches forensic imaging, examination, reporting, and ethics. Legal issues in the area of computer crimes are also addressed by practicing attorneys. The collection of electronic evidence and search and seizure practices are also addressed. Individuals learn to use the various hardware and software tools available to analyze forensic data. Even case documentation is not overlooked. Instructors know there is a possibility that all work could be useless if it is not documented properly. This is basically an A-to-Z breakdown in the area of computer forensics.

Another respected program is one sponsored by the International Information Systems Forensics Association (IISFA) called the Certified Information Forensics Investigator (CIFI). The IISFA Web site states that the CIFI certification is a designation earned exclusively by the most qualified information forensic professionals in the field. Along with adherence to the highest standards of ethical conduct, the CIFI epitomizes the highest standards in knowledge requirements and expertise. The CIFI encompasses multiple domains of knowledge, practical experience, and a demonstration of expertise and understanding accomplished through a rigorous exam proctored under the most controlled of environments. Unlike many vendor certifications, the CIFI maintains vendor neutrality and is independent of dependency requirements such as sponsored training, purchasing of product, or requirements other than ability. In fact, candidates may choose to sit for the exam without any restrictions other than adherence to the IISFA code of ethics and the exam fee. The CIFI is recognized as the only certification that truly represents the abilities of field information forensics investigators and is the benchmark by which they are measured. Earning the CIFI

designation is a significant accomplishment and identifies the best in the profession of information forensics investigator. The CIFI certification is specifically developed for experienced information forensics investigators who have practical experience in performing investigation for law enforcement or as part of a corporate investigations team. The CIFI certification is designed to demonstrate expertise in all aspects of the information investigative process and is dedicated to bringing a level of consistency to the profession than can be recognized outside the field.

These are just a couple of the credentials available to individuals to prove their proficiency with the area of computer forensics. There exist programs ranging in experience level requirements and cost. It is up to the organization to find individuals and credentials with the correct mixture of skills needed to defend and analyze its data.

Looking toward the future

Our future dependence upon the Internet and technology will continuously increase as years go by. Banks, grocery stores, auto mechanics, and law offices are just a few places that continue to increase the need for pertinent information made accessible via computers. Federal and private sector organizations will continue to face the challenges of keeping pace with countering technological advances that can be used for malicious activities. Coupled with that is the constant evolution of legal issues surrounding the Internet which are incessantly taking years to effectively develop and ultimately maintain. Our U.S. government must continue to increase awareness about this increasing dependence and must continue to plan for worst possible scenarios if something were to happen to our information infrastructure and continue to take the lead role in securing this infrastructure. Legislation that outlines illegal versus legal usage of computer must not only be passed and enforced, but it must also be continually updated and enhanced. This is crucial due to the rapid pace at which technology changes and evolves. The government must fight to stay ahead of those who wish to do nothing but impose damage and terror upon the vital lifeline of bits and bytes we call our information infrastructure. With an estimated loss of approximately US$123,779,000 due to computer crimes, this issue cannot be taken lightly. There is believed to be over 100,000 hackers spread around the globe with approximately 30,000 Web sites devoted to the training and education of new hackers. The government has a responsibility to stop malicious computer activity at its root and make the punishments so severe that individuals will need to think twice before clicking their mouse to perform illegal acts.

Read more about it

- H. Berghel. (2003) Digital Village: The discipline of Internet Forensics, vol. 46, no. 8, pp. 15–20. [Online]. Available: http://doi.acm. org.ezproxy.umuc.edu/10.1145/859670.859687
- T. Grance, K. Kent, and B. Kim . "Computer Security Incident Handling Guide," Special pub. 800-61, 2004 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
- P. Sayer (2001, January). "New center battles computer security threats," *PC World Mag,* Jan. 2001. [Online]. Available: http://www.pcworld.com/news/article.asp?aid=38750
- S. Gaudin, (2004, May). "IT burden forces security outsourcing," *CIO Update*. [Online]. Available: http://www.cioupdate.com/trends/article.php/3348561
- "The national strategy to secure cyberspace." (Feb. 2003). [Online]. Available: http://www.us-cert.gov/ reading_room/cyberspace_strategy.pdf
- CertCities.com. (2005). Certified Information System Security Professional. CertCities.com. [Online]. Available: http://certcities.com/certs/other/cert.asp?ID=59
- U.S. Department of Justice. (2004, April). "FBI announces computer forensics advisory board," [Online]. Available: http:// www.fbi.gov/pressrel/pressrel04/forensic040104.htm
- The International Association of Computer Investigative Specialist. (2004). [Online]. Available: http://cops.org/html/basicinfo.htm
- The United States Internet Crime Task Force. (2004). "Internet crime statistics summary." [Online]. Available: http://64.233.161.104/search?q=cache:jDdqBAzwQ2kJ:www.usict.org/dirmsg.asp+%22internet+crime+statistics+summary%22+usict.org&hl=en
- Carnegie Mellon Software Engineering Institute. (2005) Computer Security Incident Response Team (CSIRT). [Online]. Available: http://www.cert.org/csirts/csirt_faq.html#2
- M. Farmer. (Oct. 2000), News.com. EDS grabs Navy contract worth $6.9 billion. [Onine]. Avialable: http://news.com.com/EDS+grabs+Navy +contract+worth+6.9+billion/2100-1017_3-246720.html
- The EDS NMCI Team|Overview. (Nov. 30, 2005) [Online]. Available: http://www.nmci-isf.com/overview.htm

About the author

Phillip D. Dixon is a Microsoft certified professional and is currently a graduate student at the University of Maryland majoring in computer systems management with a concentration in Information Assurance. In 2004, he received his bachelor's degree in information technology from the American InterContinental University and also has earned two associate degrees in information system technology. Since his departure from the U.S. Army in 1994, he has worked for several DoD contractors and is currently employed as a systems specialist by a U.S. Navy contractor in Virginia.