Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Combating Computer Crime

Computer crime and computer related crimes are growing areas of concern for both law enforcement and businesses alike. Anyone can be a victim of computer crime. Ironically, those who do not own a computer can also be victims of crimes such as identity and credit card theft. However, businesses are much more likely to be victimized in a targeted attack.

Copyright SANS Institute
Author Retains Full Rights

AD

Combating Computer Crime

Jason Upchurch
September 26, 2001

According to the Nevada State Attorney Generals Office, the average bank robbery nets $2,500, the average bank fraud nets $25,000, the average computer crime nets $500,000, and the average theft of technology nets $1.9 million. While these numbers are staggering, high tech crime investigations and prosecutions are still not common endeavors, particularly with local law enforcement agencies. A universal standard surrounding high tech crimes and their investigations has yet to be established and there has yet to be the push from the public to fund programs that would make these investigations mainstream. Questions such as "What constitutes a computer crime?" "How do we investigate it?" "What are the legal concerns?" and "How can businesses help?" need to be addressed in our high tech world, as we are all potential victims.

What is computer crime?

Computer crime and computer related crimes are growing areas of concern for both law enforcement and businesses alike. However, while there is no specified universal definition for these types of incidents, they can be grouped into two categories. Computer crime is the type of criminal activity that can only be perpetrated through the use of a computer. These include:

- Computer intrusions
- Denial of Service attacks
- Damage to data form persons within
- Damage to data from persons outside

Computer related crimes are crimes in which a computer is used as a tool to complete any crime. For example, records can be manipulated on a computer to facilitate crimes such as embezzlement, or kept on the suspect's machine to record financial information of criminal activities.

Anyone can be a victim of computer crime. Ironically, those who do not own a computer can also be victims of crimes such as identity and credit card theft. However, businesses are much more likely to be victimized in a targeted attack.

Businesses offer the greatest temptation for computer criminals. Several factors play into this:

- <u>First, most businesses offer the most reward for the crime.</u>
  They have more money and other resources than most individuals. An attacker looking for a claim to fame may attack large or well know businesses for publicity.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Second, ease of attack.
  Large businesses usually employ large amounts of people, any of whom can potentially attack internal systems.
  Small businesses often contract out for their accounting and computing needs, giving the same opportunities, with even less security measures to deter them.
  Many businesses have little or no security in their systems, thus leaving themselves wide open for attack.
- Third, little fear of the consequences.
  At the present time, many talented computer criminals who remain modest and careful, have little fear of being caught and prosecuted. This is due to the difficulty in detecting and gathering evidence in wrongful computer acts.
  Even if caught, most will not be prosecuted due to many businesses' lack of faith in law enforcement and fear of bad publicity.

What is Computer Forensics?

Forensics is the recovery of evidence through a scientific method. Methodology is the heart of any forensic science, and computer forensics is no exception. A standard procedure for collecting, protecting, and examining digital evidence must be made and adhered to from start to finish, so as to preserve the integrity of the evidence.

COLLECTING

The first phase in the forensic methodology is the collection of evidence. Digital evidence comes in many forms. From personal computers, to web enabled cell phones, from servers, to PDA's, the playing field for a computer forensics specialist is immense. The evidence collection process is as crucial as any other part of the investigation. Following are some tips to aid in this process:

- The scene must be secured:
  Protect the scene from persons outside the investigation as well as from untrained investigators.
- The scene must be thoroughly documented:
  For example, cables must be labeled to match their respective plugs prior to removing systems. Photograph the scene and computer screens prior to handling the systems. Document your observations.
- Decide what will be taken:
  It may not be possible, or advisable to seize the entire system. Consider a company's production server, which was unlawfully used to store suspected evidence. In this case, it is best to work with the company to duplicate the data that is needed for evidence. If a system is to be taken, take all components, peripherals, manuals, cables, software, and any item that could contain data.
- Shutdown the system correctly:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Systems must be shutdown to prevent damage or alteration. The power should be pulled from the back of the computer's case (do not use the computer's shutdown sequence) to preserve the system, as it was when it was found.

- Packaging:
  Package items carefully for their protection, and logically according to the way they were found. Ensure you seal the computer in a way that will make it impossible to alter data without breaking seals. (Seal the power connection, the case, all drives, and keyboard connections with evidence tape, and sign and/or initial the tape.)

PROTECTING

After the evidence has been identified and collected, it must be protected. Digital evidence, like any other evidence, must be presented in court in its original form. It must not be damaged, destroyed, or even altered, from the time that it is recognized as possible evidence, to the time it is presented in court. Investigators are faced with many new challenges while protecting the integrity of digital evidence throughout the examination process. For example, paper records that are collected as evidence are difficult to unintentionally alter. While they could be damaged or destroyed through gross negligence and mishandling or disaster, the data they contain remains static as long as the media (paper) is intact. They can be reviewed in their original form without worry of the data being altered. They can be casually photocopied, transferred to other investigators, and stored easily without fear of damage. As long as the chain of custody (documentation of all individuals who have maintained control over the evidence) is intact, the defense is hard pressed to bar their admission as evidence. However, digitally stored data, particularly magnetically stored data is extremely easy to alter without proper care and precautions. These alterations can be intentional or accidental. Some of the potential threats to the integrity of digital evidence to avoid include:

- **Intentional (suspect covering his tracks)**
- Altered shutdown sequence:
  The suspect alters the shutdown sequence of the operating system to activate a disk wiping utility to erase the hard drive, or just certain files and the cache that may incriminate him/her.
- Altered startup sequence:
  The same as above, but executed on startup.
- Viruses:
  The suspect intentionally plants a malicious but temping file on the hard drive. (I.e. '*stolen money.xls.'* It would be tough to resist opening a file by this name in an embezzlement investigation!)
- Bombs:
  The real thing!!! Open the case of a suspect's computer to a nasty surprise.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Magnetic fields:
  A degaussing loop/ring around a doorway or a strong electromagnet that is activated upon loss of power to the computer's power supply will erase magnetic data.

- **Unintentional (Investigator mistakes)**
- Storage environment:
  Digital evidence is stored or transported in an area not well suited for computer components, such as areas with extreme temperatures or near electromagnetic fields. (A special note here: police vehicles are equipped with very high wattage radios, which produce strong magnetic fields, usually located in the trunk.)
- Poor scene security:
  Suspects allowed access to their computers during collection provides opportunity for alteration. Untrained personnel "looking around" in a suspect's computer may accidentally alter evidence such as date stamps by simply viewing a file.
- Static Electricity:
  Great care should be used to remove components from a system. Touching components without proper grounding can destroy the system.

EXAMING

The most extensive phase of computer forensics is the examination of evidence. There is no set procedure that is universally accepted when it comes to examining a computer for evidence. There are, however, a number of computer forensic software packages available as well as organizations that can train personnel in data recovery. However, it may be more advantageous for small organizations to contract specialized companies for the examination. Although there are no step by step instructions for data recovery, there are criteria and steps that should be followed in most cases.

- Locate personnel with the ability/desire to grasp both technical and legal subjects:
  This may be more difficult than it first seems. Persons with a strong technical background are not as likely to be interested in criminal laws, and vise versa.
- Diversify:
  It is highly unlikely to find any one person capable of knowing all there is to know about computer forensics. Personnel must be recruited and encouraged to develop different interests in the areas related to computers and evidence.
- Maintain up to date training:
  Very little case law has been established in the area of computer forensics. As a result, expect legal battles at most hearings and trials

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

attacking the examiner's knowledge and abilities. Professional training in the area of computer forensics can help alleviate this problem.

- Lab set-up:
  The lab needs to be secure, as it will hold evidence where a chain of custody must be maintained. The systems used to examine evidence must also be secure from external manipulation, meaning they must not be networked beyond the lab, or controlled by an outside group. While it may be necessary to go through IT to purchase systems, they must not have any further access to the forensic systems due to chain of custody and validation issues (see below). A large selection of new and dated equipment may be necessary to examine the variety of computers still in use today.
- Test and validate:
  After the test systems are up and running, they must be validated to ensure they do not alter evidence. If a system is changed (i.e. upgrades, patches), it must be revalidated.
- Records:
  Documentation must be kept on all procedures during examinations, and of all hardware and software installations on lab equipment, to protect the integrity of the examination.
- Ensure the right to perform the examination:
  Consent is needed to search or a warrant needs to be issued (though in extreme circumstances other possibilities may give the right to examine). With consent cases, the party giving consent must also have the right to do so. Questions that need to be asked in this situation include:
  - Does the computer belong to the person giving consent?
  - Does anyone else use the computer?
  - Are there disclaimer banners when logging onto the computer?

  The court will ultimately decide if a valid consent was given. The basis for this decision will be the "expectation of privacy" a reasonable USER would expect in the same situation. (An important note here: the decision will be based on the user's expectation of privacy, not the owner's.)
  However, the right to examine is usually granted through a warrant. The warrant's language is very important. It must be specific as to what will be searched for, as well as what will be searched. A warrant that grants the right to seize a computer does not necessarily give the right to examine it. Language must be included in the original warrant specifically granting the right to search hardware for specific data or it must be added in a supplemental warrant.
- Make copies of disks:
  This is the most important aspect of the examination. Using a bit stream-copying program, such as "Safe Back" or the Linux dd command, to make copies of the original media will protect the integrity of the evidence. If the copy is damaged by any of the previously mentioned intentional or

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

unintentional alterations, the copy can be replaced, whereas, the original cannot.

- The suspect's operating system must not be used:
  The suspect's system may contain an altered startup/shutdown sequence and/or altered commands, which can damage evidence without the investigator ever realizing it.
- Disk examination:
  All areas of the disk must be examined. Ensure the reported disk size is the same as the actual size. Slack space, boot records, and cache traces need to be checked for hidden data.
- Examine all files and directories:
  All files must be checked with a viewer capable of opening files regardless of the reported extension type (i.e. Quickview plus). Suspects can intentionally misrepresent files by altering file extensions.
- Stay within the scope of the investigation:
  If evidence is found outside the scope of the search warrant, stop! A supplemental warrant, which includes the new evidence, must be prepared and signed by a judge before proceeding any further.
- Be systematic:
  With the average computer containing tens of thousands of files, one must be systematic in the approach to viewing files in order to avoid missing files.
- Beware of encryption and data hiding:
  Both of these methods raise the expectation of privacy for the user and may necessitate a supplemental warrant.

Legal Concerns

While most of the forensic sciences have been around, and consequently tested in court, for many decades, computer forensics is just becoming a mainstream in today's courtroom. The case laws regarding the validity and admissibility of digital evidence are still being decided upon in today's court. Many earlier decisions are being used as a basis for computer evidence questions. The justices making these decisions are not computer experts and may not even understand the issues at hand. To make this subject even more confusing, several legislative measures have also been passed with regards to electronic communications.

Legislation has been passed on the national level to protect people from government agents and independent individuals that would intrude upon the privacy of those engaging in electronic communications. If violated, some of these federal statutes provide for substantial penalties, as well as excluding valuable evidence needed for investigation. A very useful table has been established by the Center for Democracy & Technology at http://www.cdt.org/privacy/govaccess/accesschart.shtml. It outlines what

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

procedures are necessary to legally gain access to stored communications such as email.

Why should businesses help?

Computer forensics is a growing part of the information security world. It is a unique blend of technology and traditional law enforcement techniques. As the world becomes more and more connected, the role of computers in wrongful acts is also increasing. While it would be nice to believe our local law enforcement agencies have the resources to combat this increasing threat, most do not. All government agencies rely on public funding to support their operations. While system intrusions or other high tech crimes may cost a large organization millions of dollars in losses, there has yet to be the public outcry necessary to demand the funding needed to adequately combat digital criminals. Part of the lack of demand is due to companies focusing their efforts on prevention methods rather than going forward with a public investigation. Although preventive measures are very important, this philosophy leaves little demand for law enforcement intervention, therefore little effort is given to train investigators. As a result, when an incident occurs that deserves law enforcement attention, it is less likely to be reported to law enforcement agencies for fear it will be miss handled. In addition, these incidents will only continue to increase with growing technology. It is imperative for law enforcement to instill intervention/deterrence techniques now, before digital crime becomes to overwhelming. How do we combat this problem?

- Get to know local law enforcement agencies:
  Most large agencies have personnel that have been cross-trained to handle computer-related incidents. Some have actual computer crimes investigators. A meeting can help assess the capabilities and competency of the investigators, thus providing more information to work with when making decisions.
- Lend support:
  Many agencies lack the funding or resources to run a computer crimes unit. However, this lack of funding may not reflect a lack of interest. Agencies frequently have volunteer programs for persons willing to put a little extra time into helping out. People with information security expertise are of great benefit to an agency starting a new computer investigations unit. The volunteer can teach law enforcement officers techniques, while the officers can teach volunteers about evidence handling techniques and legal concerns.
- Voice opinions and concerns:
  The government is responsible for new legislation and public projects. If we are to keep up with these new tech-savvy criminals, action needs to be taken before the problem is out of control. However, this action requires funding and resources, available at the taxpayer's demand. Our democratic government will react to public demands, but only when they are voiced.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Where is our digital future heading?

Criminals, by nature, are opportunist and use what is available to them to commit their various crimes. The vast array of personal computers and workstations are growing at a shocking rate, and with this growth, breeds new tech savvy criminals. Mainstream criminal activity involving computers is in its infancy. How we deal with its growth is dependent upon the public and businesses' involvement.

The Center for Democracy and Technology, "CURRENT LEGAL STANDARDS FOR ACCESS TO PAPERS, RECORDS, AND COMMUNICATIONS."
URL: http://www.cdt.org/privacy/govaccess/accesschart.shtml (2001)

E-Commerce Times Staff interview with Charles Neal, "Exclusive Interview: FBI Computer Crime Squad."
URL: http://www.ecommercetimes.com/news/articles2000/000211-1a.shtml (February 10, 2000)

David T. Lang, "Design and Development of a Distance Education Paradigm for Training Computer Forensic Examiners."
URL: http://www.computerteacher.org/Idea%20Paper(web).htm (January 20, 2000)

Nevada Attorney Generals Office "A strategic Plan to Combat High Technology Crime."
URL: http://ag.state.nv.us/hi_tech/plan1.htm (2000)

Lloyd D. Doney, "The growing threat of computer crime in small businesses."
URL: http://www.findarticles.com/cf_dls/m1038/n3_v41/20825214/p1/article.jhtml (May 1998)

Stanley H. Kremen, "Apprehending The Computer Hacker: The Collection and Use of Evidence."
URL: http://www.shk-dplc.com/cfo/articles/hack.htm (1998)

Bill Clede, "Investigating computer crime is every department's concern."
URL: http://www.clede.com/Articles/Police/compcrim.htm (July 1993)

Judd Robbins, "An Explanation of Computer Forensics."
URL: http://computerforensics.net/forensics.htm (No published date)

Rocky Mountain Information Network, "Computer Crimes 2001 Conference" (classroom)
URL: http://www.utap.org/rmin.htm (August 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The National White Collar Crimes Center, “Basic Data Recovery and Analysis” (classroom)
URL: http://www.cybercrime.org (November 1999)

International Association of Chiefs of Police, “Basic Computer Crimes Investigation” (classroom)
URL: http://www.theiacp.org (June 1999)

© SANS Institute 2001, Author retains full rights

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**