Title: ***Electronic Forensics: A Case for First Responders***

by Dr. Henry B. Wolfe

Abstract

Almost every aspect of our lives is touched or somehow controlled by technology driven processes, procedures and devices. It is therefore important to understand that because of this pervasive electronic influence, there is a high probability that a successful criminal or unacceptable incident will occur within the perimeter of an organization's information and/or computer and network infrastructure. The difference between conducting a successful investigation resulting in a potential prosecution or failing these will often lie squarely in the lap of the electronic forensic investigator. If potential evidence is compromised at any point in the investigation, it will be unacceptable in a court of law. The highest risk of compromise occurs at the point prior to evidentiary acquisition. The first responder's primary responsibility is to protect and preserve potential evidence and to see to it that suspect electronic devices and storage media are not tampered with by anyone until such time as the professional electronic forensics investigator (law enforcement or private) takes full control of the scene. This paper will explore electronic forensics demonstrating the need and making the case for the appointment and training of a first responder to incidents where electronic devices may have been used.

Introduction

More than ten years ago when we first began talking and writing about electronic forensics, there were few purpose built tools to attack the problem. We mostly made use of general purpose utilities and some fundamental knowledge to capture and explore potential evidence. These were used by law enforcement and/or the organization's computer guru to find relevant evidence. Sometimes they were successful and sometimes not. During the intervening period, specialist tools have been created and some accepted procedures and methodologies have also been authored.

Electronic Forensics

Electronic forensics now covers a plethora of electronic devices and methodologies used to capture and authenticate data at its source, analyse that captured data for evidence relevant to the case at hand, produce an understandable report that can be introduced into evidence in a court of law, and testimony as to the authenticity of evidence presented. The sequence of executing this methodology is important to the success of an investigation and may impact potential evidence acceptance in a court of law.

Any company and/or staff may be the subject of various attacks. Some examples are attempts to undermine customer confidence, attempts to extract personal or business-related information to sell, or the redirection of organization funds, or any other activity you deem to be unacceptable to the ongoing success of your organization. Typical sources are disgruntled employees opportunist hackers, criminals, competitors and others. Their motives and purposes may or may not be known but rest assured that their actions can be devastating to an organization.

It is not the intention of this paper to profile attackers or define all the types of intended agendas. Many security references have extensively profiled the would-be intruder from among the internal and external users, as well as defined unacceptable behaviours.

Information in electronic form can be stored in various devices using methods normally unknown in detail to the average user. They don't need to know this to be a good user. In addition, there is also content stored that average users may not be aware of. Modern forensics tools and techniques can extract evidence from properly captured data - if it's there. Some examples are information about sites visited on the Internet, information thought to be deleted by the suspect, improper or illegal images held on the suspect machine, specific timeline information and much more.

The current accepted process requires that care be taken to protect the original source data. A formal chain of evidence record must be created that follows the evidence from capture through to the last appeal in a court of law. There are a number of guidelines for the collection of evidence published by various groups. They provide guidance for front line staff who would be likely to be the first responder to an incident. The US Department of Justice has a number of publications that provide very thorough advice in this area as well. An example is *Electronic Crime Scene Investigation: A Guide for First Responders*.

The chain of evidence referred to above documents possession, access and control of evidence from the instant it is captured until well into the judicial process (to allow for one or more appeals). If the evidence is out of the control of the investigative authority, and can be shown to be so by opposition council, the court is likely to declare it inadmissible. This is done because while it is out of the control of the authority, the evidence may have been altered and therefore, its integrity can no longer be guaranteed. All of the investigative and analytical work invested will be lost and the case may also be adversely affected as a result. Therefore, it becomes an important issue – especially at the very beginning of an investigation to ensure that first responders understand the necessity for protecting potential evidence. The local IT guru may be very talented but is unlikely to have, as a matter of course, a knowledge or understanding of this aspect of evidence acquisition.

Each evidentiary copy of the original data source must be validated - proven to be an exact mirror image of the original. This is accomplished by using a mathematically proven hashing algorithm designed to create a unique fixed length value (a fingerprint) of any given string of data - file, folder, drive, disk or other data group. This fingerprinting process is performed on both the original and evidentiary copy and the two hash values are compared and must be equal in order to authenticate the evidentiary copy. The operating system copy command cannot be used for this function because it will only copy files, folders, drives, etc. There is much more to be captured in addition to those entities. Specialized tools and/or software are, therefore, required to create the mirror image. It is unlikely that the local IT guru will have any of these tools and the required knowledge to use them properly. Analysis can begin after the evidentiary copy is authenticated.

Data encryption has become more commonly used these days. It is therefore encountered by investigators with great regularity. This is not the forum to address issues surrounding how to deal with encryption, however, suffice it to say that there are several successful methods and specialist tools that can be used overcome blockages to analysis presented by encrypted data. It is worth mentioning that we are not successful in all cases where strong encryption has been used.

Many robust, specialized and all encompassing tools have been created since the early days of electronic forensics. There are now many tools that facilitate the analysis process. This process searches the entire evidentiary data set for information relevant to the case. This selected material is incorporated in the final forensics report. Original evidence is almost never used for anything other than capturing and validating the evidentiary copy.

Evidence that is found must also be recorded and produced in a form that can be easily understood by those considering the case. The forensic investigator must be in a position to present and defend (and if required - reproduce) the processes used to acquire the evidence. There are now plenty of legal precedents in many jurisdictions that validate the use of the various forensic tools and techniques. These precedents strengthen the credibility of evidence presented.

The first hard drive that I investigated (a two gigabyte drive) took ten and a half hours to capture and authenticate. The whole process is time consuming and labour intensive since typical hard drive storage capacities increase regularly. Today's tools can capture at about three gigabytes a minute - twenty-five minutes for a one-hundred gigabyte hard drive. The profile of an electronic forensics investigator is part detective, part technician, part analyst, and part expert witness. These qualities each, on their own, could constitute a person's entire profession. Finding these attributes together in one package is difficult. Universities in the last few years have begun to provide tuition in this profession. Some product vendors are providing specialist training but to put together all of the necessary foundation and specialist knowledge and experience will take a combination of sources. This is expensive. Be prepared to pay a premium to professionals in this discipline.

The way it is

Security will fail if top management does not take an active role in initiating, developing and supporting it. Security will fail if top management, because of their lofty importance, choose to exempt themselves from applying the secure policies and procedures implemented. This is not a new revelation. It has been stated repeatedly by myself and many others in the profession. Management has continued to ignore it repeatedly as well. Because it is often ignored, to the detriment of those who do so, we feel compelled to restate it yet again for this forum.

This is a real life example: a government department has at its head an individual who does not like the idea of being forced to change their password regularly and therefore, is exempt from doing so. This in turn has allowed the number two in command to also be exempt from changing their password regularly. Policies that incorporate password change have been repeatedly proposed as a required security measure. These and other security policies have not been approved by these executives because they will be forced to change their passwords regularly like everyone else. Other employees who are aware of this approach can plainly see that security is not an important issue to these top executives. This filters downward and as a result of this irresponsible attitude and incompetence on the part of top management, the organisation still has no formal password policy. Moreover, since security is not important to those at the top, why should it be important to anyone else in the organisation? The entire information assurance policy regime suffers and is weakened as a result.

The example discussed is not unusual or unique. Individuals like those described above are far more common that we would like to think and found in every country and across both private and public sectors. Everyone believes that they are special and that they alone should be exempt from specific rules and can make convincing arguments (in their own minds), supporting their

contention. However, in order to protect the continuity, integrity and confidentiality of any IT system it is necessary to instil an ethos of security amongst the entire staff of the organization. This especially includes top management since subordinates will follow top management's example. Leadership is born out of example not from command authority. There should be no exceptions and all should be required to abide by agreed on policy. These policies should each be justified by a risk assessment, policed and have consequences for those who choose not to adhere to them. They should be communicated to all staff regularly so that there is no misunderstanding of what acceptable behaviour is and what is not.

Unfortunately for many organizations or industries, this is not always a reality! Government or large organizations may have identified the need for code of conduct and security policy, due to fiduciary, statutory or government regulations, or possibly due to the impact of previous security events. Medium or small organizations may not have the resources, budget, inclination or regulatory requirements to identify or manage a risk management and business continuity plan.

It may take a business-disruption, politically sensitive or public-embarrassment type incident to gain the attention of senior management or the board of directors. Addressing the incident at that point may not be enough to prevent the organization from ceasing to exist. By then it may be too late to recover if properly considered measures have not previously been put in place.

Security Breach – What do we do?

A breach may be defined as a potentially criminal action for purposes of this discussion. A violation can be defined as an infraction of a security policy. Detection of the breach or violation needs to occur. Much of the time crime and inappropriate behaviour is not detected. Measures need to be put in place that will detect patterns of potentially unacceptable action. For example, intruder detection systems (IDS) or intruder prevention systems (IPS), attempt to identify events that occur when someone tries to hack into your system, or a staff member attempts to gain access to part of the network they are not permitted to access. IDS produce logs containing information about network traffic activities. These logs can be used for traffic analysis and enable the network administrator to identify network bottlenecks as well as network performance and capacity indicators to determine whether additional resources (server, memory, storage, network bandwidth, etc.) may be required in order to maintain acceptable performance levels.

Information captured and stored in these logs can also be used for forensic purposes to track individual activities depending on log file configuration parameters. There is a trade off required in the decision to capture everything or selectively capture only data that is desired. When capturing everything, significant overhead in processing power, network performance and disk storage space may be required. Therefore, a balance is usually struck by network administrators to capture a subset of logged data required for general analysis or potential investigative purposes. This subset is usually intended to provide enough data to be able to identify what has happened and how it happened (if an intruder has been successful). This information assists the administrator to reconfigure and introduce measures to protect against a similar event or attack from successfully occurring at a future date.

This is okay for hacking attacks, however, other potentially criminal activities or inappropriate activities may not be so easy to detect. It is possible and practical to use various audit devices that detect fraud, embezzlement, theft and the like. There are filtering tools that prevent access to forbidden Internet sites (porn and other questionable sites). These are important tools to reduce the "opportunity" by making this behaviour difficult or easily detected.

Internal authorised users performing authorised activities often act upon opportunity. Taking advantage of an opportunity may be considered unacceptable behaviour. Security measures may not pick up the immediate actions if the user is authorised to perform like-activities as part of their job description and function. For example, an unauthorised modification to a customer's bank account to redirect funds may only be picked up after the customer queries a missing payment.

It is important to understand that while an organization may identify actions by internal staff or external users as inappropriate or unacceptable, the actions themselves may not be deemed illegal or criminal to a level worth investigating by the law enforcement community. This may be due to the low value of monetary loss, physical disruption or goodwill damage to the organization. Legal advice is recommended in such cases.

An organization can choose a civil action against a staff member, such as dismissal or a formal warning. Management must ensure their evidential facts are clearly defined to counteract any potential employee legal action against their employer for wrongful dismissal. Civil remedy is not necessarily an option where an external person or another organization is responsible for damage. Legal advice may recommend monetary damages be sought in court from the responsible parties.

However, when all of the best security practices have been observed, suitable security controls are in place, and a breach or violation is detected, certain procedures should be followed so that any useful and relevant evidence that may still be in place will not be corrupted or destroyed – either by purpose or by accident.

How do we handle it?

Forensics by its nature is an after the fact discipline. As with traditional forensics, the timing of the incident response, along with defining and securing the potential crime scene is critical. In the electronic world, this involves more intangible evidence and not necessarily easily put into an evidence bag. Evidence may include PC and system logs, local and removable backups, removable media such as diskette and CDs, printouts, flash drives, as well as any other local, removable or remote storage devices or processing systems, etc. PDAs and mobile phones can also contain relevant evidence and there are specialist tools to deal specifically with them.

For example, the suspect equipment and all associated devices should be immediately isolated. If the PC is turned on, it should not be turned off. If it is turned off, it should not be turned on.

Third parties, ISPs, systems administrators and users may also be critical in the data and information discovery process. In the case where information or data may need to be obtained from outside your organization, court orders and warrants may need to be prepared and subpoenas sought. In these cases, the involvement of law enforcement and legal council is critically required. It is recommended that the organization does not attempt to obtain evidential information from external parties without legal or law enforcement advice. This may make the evidence inadmissible in a court of law and seriously jeopardize the likelihood of a successful investigation and prosecution.

It is critical that if a breach or violation is detected, the organization's IT support staff do not compromise or contaminate the evidence. Only suitably trained security staff should attempt to

take evasive action if the perpetrator is identified to still be online and in the process of the potential crime or unacceptable behaviour. Evasive action may include closing off the network around the perpetrator, following at a distance to collect additional information to assist in the subsequent investigation and hopefully identify the culprit.

Whether there are in-house forensics staff or not these and other procedures should be followed until the forensics professional takes control and begins the investigation and data capture process if required.

What do you do?

Incidents may vary in structure and substance. Where an activity is deemed criminal, local law enforcement should be immediately contacted and the case investigated by them. If management decides the incident will be handled internally, as a civil remedy matter without law enforcement assistance, there are several recommended approaches.

One approach is to contact a private forensics professional to handle the investigation. This is a fairly new profession with varying levels of skill available in the market place so shopping around is definitely an important task. It makes sense to do this before there is an incident so that on the day, you can call in an appropriate expert without delay. These cases are most often time critical. In various jurisdictions, there are professional groups, like Vogon for example, that have excellent reputations thus providing confidence that the best job that can be done will be done.

The organization, if economically feasible, can set up an in-house forensics group trained to perform such activities. This would require highly technical professionals, a laboratory and a good deal of specialized hardware and software – probably not warranted in small organizations. Another approach is to contact a local Computer Emergency Response Team (CERT) for their advice and possible assistance.

No matter which path is chosen by your organization, someone needs to be trained and responsible for this kind of activity. They need to know what measures to take to ensure that potential evidence is not destroyed or corrupted either deliberately or inadvertently before the forensics investigator arrives to begin the investigation. They need to know who to call to perform the investigation and who to report the incident to.

Strategic Importance of Forensics

When a breach or violation is suspected, the organization's most likely intent is to first recover - if appropriate, then to seek a prosecution or discipline internal staff and if losses have been sustained as a result of the breach, recover those losses. Even after a successful prosecution, there is no guarantee that the organization will remain operational. The impact and subsequent damage from the security incident may in fact put the organization out of business, or affect its position in the marketplace such that it no longer has a viable business model.

The organization's Business Continuity Plan is critical at this point. Recovery is vital from the immediate incident, whether this is installing a replacement server from backups or finding new premises during the incident's period of investigation. Resumption of normal business activities is also important after the recovery period back to the same business operational level with hopefully enhanced security controls, as before the incident.

After the event, it is recommended that a full investigation around the handling of the incident is included to identify potential risks and create mitigation plans designed to minimize the impact of a similar event in the future.

First Responders

The handling success of an incident will be determined by how an overall incident response plan will be managed. It must be defined by senior and technical management, prior to the actual need arising, including forensics investigation. At the time an incident arises, as with traditional forensics, timing and evidence handling are critical. Electronic evidence may be deliberately or accidentally contaminated or corrupted and therefore must be protected from the very beginning of the investigation. External partners may need to be contacted and court orders prepared in order to gather evidence from their systems or staff.

The approach to managing the incident internally has several critical focuses. First and foremost is protecting and preserving the scene and potential evidence. The gathering and analysis of evidence requires specialist expertise. This is needed for identifying and extracting the electronic information from all of the sources that can provide potential evidence, and to ensure that all due process is followed for the purposes of protecting the chain of evidence.

The non-technical aspect of managing internal communications and external public relations type information is one consideration, which may not be immediately apparent. This includes an authorised forum for staff, management, customers or external parties or media to be advised of the situation. Early release, incorrect, or unauthorised disclosure of information may not only affect the hope for a successful investigation and possibly identifying the culprit, but equally critical is the financial and continued stability and viability of the organization staying in business, including political, statutory, board, management, staff, customer, partner and public confidence.

Conclusions

This paper has addressed in broad non-technical terms the role of electronic forensics within an overall security policy and strategy. It is but one part of an all encompassing holistic view of information assurance: protecting the assets, integrity, reputation, continuity and operation of any given organization.

When and if an incident occurs, policy should dictate what steps are to be taken. If the possibility of a prosecution exists, it is necessary to transfer control to one or more “first responders” who are trained to protect and preserve potential electronic evidence until such time as the professional forensics investigator law enforcement or private) arrives to take control of the scene. The necessary training is not onerous or otherwise expensive but rather money well spent.

Security begins with policy and ends with a continuity plan that will facilitate recovery when all else fails. It also entails everything in between such as physical security, internal audit measures, anti-virus and malware protection, firewalls and intruder detection and protection capabilities to detect and thwart intruders into your network, strong proven encryption to protect the privacy or confidentiality of organizational information (both at rest and in transit). It is not one dimensional but holistic in its nature. Adding first responder capabilities serves to make your security stronger and enhances the likelihood of successful prosecution when required.

Bibliography:

Bace, Rebecca Gurley & Smith, Fred Chris; *A Guide to Forensic Testimony*, Boston, Massachusetts, Pearson Education, Inc., 2003,ISBN: 0-201-75279-4.

Casey, Eoghen; *Digital Evidence and Computer Crime*, Academic Press, London, 2000, ISBN: 0-12-162885-X.

Kruse, Warren G., Heiser, Jay G.; *Computer Forensics: Incident Response Essentials*, Addison Wesley, Boston, Massachusetts, September 2001, ISBN: 0-201-70719-5.

Mandia, Kevin, Prosise, Chris; Incident Response: Investigating Computer Crime, New York, 2001, ISBN: 0-07-213182-9.

Nelson, Bill; Phillips, Amelia; Enfinger, Frank & Steuart, Chris; *Guide to Computer Forensics and Investigations*, Boston, Massachusetts, Course Technology, 2004, ISBN: 0-619-13120-9.

Stephenson, Peter; *Investigating Computer-Related Crime*, Boca Raton, Florida, CRC Press, 1999, ISBN: 0-8493-2218-9.

US Department of Justice; *Electronic Crime Scene Investigation: A Guide for First Responders*, Washington D.C., July 2001, NCJ-187736.
http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm.

Electronic Reference Sources:

International Journal of Digital Evidence - http://www.ijde.org/

Computer Crime Research Center; *Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* - http://www.crime-research.org/eng/

High Technology Crime Investigation Association - http://htcia.org/

The International Association of Computer Investigative Specialists - http://www.cops.org/

US Department of Justice; Cybercrime Page - http://www.usdoj.gov/criminal/cybercrime/index.htm/