Taxonomy of Anti-Computer Forensics Threats

Joseph C. Sremack, Alexandre V. Antonov

LECG, LLC
Washington, DC USA
jsremack@lecg.com
aantonov@lecg.com

Abstract: Threats to computer forensics are increasingly becoming more prevalent. Attacks against underlying forensic methodologies have come to the forefront during the past five years, in which attacks have become more sophisticated and difficult to prove in a court of law. These threats can negatively affect an investigation, if not completely stymie it. No complete taxonomy of threats to computer forensics posed by anti-forensic techniques currently exists. This paper attempts to construct a comprehensive taxonomy of anti-forensic threats by investigation and threat type.

1 Introduction

Recent developments in several critical areas have drawn attention to the threats facing computer forensics. Advanced anti-forensics techniques are being developed in practice [Gr02] and [PR05], as well as theoretically [Se06]. These anti-forensic techniques can threaten a computer forensic investigation in its entirety. In addition, changing requirements in US and EU case laws are impacting the existing processes and foundations of computer forensics and allow for a new breed of anti-forensics in which case law can be used against the forensic investigator.

Computer forensics, as a whole, is a relatively young field. Compared to traditional forensics, computer forensics is especially young. Traditional forensics has been establishing its body of knowledge and best practices for more than one hundred and thirty years. Compare this to computer forensics, where the practice has largely been performed for only the past two decades.

While traditional forensics is still rapidly developing, little work or examinations are being done with respect to threats. Threats have largely been identified and classified in the areas of security and traditional forensics. Many models and taxonomies have been established to not only identify, but to classify and rank those threats accordingly. Some efforts have been made [Bu06] and [Ha06], but computer forensics has not established these threats in a complete and organized manner. This deficiency can lead to problems in which an investigation can be thwarted by any number of undocumented threats.

The threats facing computer forensics are multi-faceted. Legal, technical, and physical factors must all be considered with respect to the threats. The combination of these factors differs from the mostly technical threats accounted for by security threat models. In addition, threats in computer forensics differ based on the jurisdiction(s) in which an investigation takes place. Differing case law and other jurisprudence factors means that a threat facing a solely US-based investigation may or may not apply to an international investigation.

In addition to the threats differing, the types of investigations can differ. Three major types of investigations are performed: internal, criminal, and civil. Internal investigations are performed outside of a court of law and are typically performed within a single organization to respond to some event. Criminal investigations are performed when prosecuting one or parties for a criminal offense. Civil investigations are performed within the realm of a court of law, but they are conducted in order to settle a civil dispute rather than for prosecution. Threats, for each of these investigation types, differ according to the requirements for proof and what constitutes proper evidence.

In this paper, a taxonomy of threats to computer forensics is developed. To achieve this, threats to computer forensics are defined based on the multitude of factors and types of investigation. Since the threats are specific to each combination, a general taxonomy is developed. Practical considerations for applying this taxonomy are then shown. Section 2 discusses the overall requirements for computer forensic investigations. Section 3 briefly outlines the three types of computer forensic investigations and how they differ. Section 4 discusses the current state of anti-forensics, and how practitioners and theoreticians are developing techniques and approaches to defeating forensic techniques. Section 5 is the taxonomy of anti-forensic threats. Section 6 provides a case study that highlights several of the threats. Section 7 provides concluding remarks and future work on this topic.

2 Computer Forensic Investigation Requirements

Most computer forensic investigations follow a general structure. The first phase of every investigation is preparation. This phase establishes the overall plan for acquisition and analysis to ensure that all data are completely and correctly acquired. The next phase is collection, in which all data are acquired. Analysis is then performed against the collected data. Finally, the presentation phase is performed in order to present the analysis in a clear manner to the adjudicating body (court of law or otherwise). This section outlines the general requirements for each phase and the overall investigation.

2.1 Preparation Phase Requirements

The preparation phase includes all steps necessary to ensure that a complete and correct investigation is performed. This entails accounting for all data that should be acquired, the analysis that is expected to be performed, and how the findings should be presented. This stage is critical and often begins based on nature of the event. For example, a hacked database server would lead an investigator to capture all evidence related to accessing the database server.

There are five requirements for the preparation phase. The first requirement is that the full scope of the investigation be understood. Understanding the scope of the investigation consists of learning the timeline of events leading up to, occurring during, and occurring after the incident or event of interest. This information can arise from system documentation, legal documentation, and/or verbal discussions. The second requirement is the interview process in which all pertinent and accurate information is received relevant stakeholders and witnesses. The number of witnesses and stakeholders varies based on the investigation, where it could be a single person or consist of tens to hundreds of people. From the information gained through interviews and background material, the next requirement is to determine all data points that need to be acquired and how they are to be acquired. Next, the means for analysis must be determined. The analysis may be a simple keyword search across a single hard drive, or it may be complex steganalysis. While the analysis plan may change once the data has been acquired, setting up an analysis plan *a priori* is helpful in organizing and streamlining the analysis. Finally, the venue for presenting the analysis findings must be known. The analysis may need to be presented in court, or it may only be shared internal to a company. Each venue has its own requirements for rigor and presentation, and the analysis should be aligned with those requirements.

2.2 Collection Phase Requirements

The collection phase involves acquiring all data and verifying that the data were properly and fully acquired. There are four main collection phase requirements. The first is that all relevant data be acquired. The second is that the acquired data be verified through some means, such as matching hash values. The third is that the entire process be fully documented. Finally, chain of custody must be maintained and demonstrated through documentation.

The analysis phase is where all data are analyzed based on the investigation plan. The analysis phase consists of six major requirements. The analysis, most importantly, must be performed completely and accurately. The second requirement corresponds to the first; evidence should be cross-verified with other evidence, where appropriate. For example, router log entries should be cross-verified with file server logs. Industry best practices should be employed. Fourth, court-tested tools and techniques should be employed over novel or otherwise untested tools and techniques. The entire process should be documented, and finally, chain of custody must be maintained.

2.4 Presentation Phase Requirements

The presentation phase involves culling the relevant data and assembling in a logical manner to present to the adjudicating body. The presentation phase requires that all relevant information be presented clearly and that the analysis conform to the rules of admissibility of the adjudicating body.

2.5 Overall Investigation Requirements

All phases of an investigation must be performed so that the following requirements are met:

- Follows rules of admissibility
- Findings are convincing and based on court-tested industry best practices
- Full process is documented
- Performed in a reasonable amount of time

3. Types of Computer Forensic Investigations

Three main types of computer forensic investigations exist: internal, criminal, and civil. These types all have different purposes and levels of required rigor. Internal investigations are performed outside of a court of law and are typically performed within a single organization to respond to some event. Criminal investigations are performed when prosecuting one or parties within a court of law. Civil investigations are performed within the realm of a court of law, but they are conducted in order to settle a dispute rather than for prosecution. All three types try to answer the following questions:

1. Who (e.g., who were the sources of the event?)
2. What (e.g., what exactly was the event?)
3. Where (e.g., on what systems and at what locations did the event occur?)
4. When (e.g., what is the timeline of events?)
5. How (e.g., what conditions allowed the event to occur?)

Internal investigations are typically performed in order to resolve an event outside of a court of law. The rigor required for collecting and analyzing evidence for an internal investigation is less, because the requirements for evidence is based solely on the interested party and no other third parties. The first goal is to determine the cause(s) and source(s) of the event. The next goal depends on the event. Containment and remediation may be all that is required of the investigation if the event is small and does not require disclosure. In other instances, determining the exact source of the event is the prime objective. Companies operating in the State of California - online or otherwise - must disclose all hacker incidents that may affect customer information [Ca02]. In cases such as this, which affect customer records or may later require legal intervention, greater care must be given. The full scope of the event must be determined and reported accordingly.

Criminal investigations are presented to a court of law and require that the evidence prove, beyond a shadow of a doubt, the source(s) of the event. A criminal investigation's findings cannot leave any doubts as to who committed the crime and how. These cases are handled by law enforcement professionals.

Civil investigations are also presented to a court of law for adjudication. There are two main differences between civil and criminal investigations. First, criminal cases involve a party(ies) having broken a societal law, whereas civil cases allow citizens to protect their individual rights in court. This difference is telling with respect to the length of the investigation and the types of evidence involved. Second, civil cases only require a preponderance of evidence, instead of the criminal cases' requirement of being proven beyond a shadow of a doubt.

4. Anti-Forensics

Anti-forensics is the practice of thwarting a proper forensic investigation. Any activity that intentionally aims to deceive or impede the forensic analysis is classified as anti-forensics. There are two classes of threats posed by anti-forensics: threats to digital evidence and threats to the legal process.

Anti-forensics is typically considered from a digital evidence perspective. The four main types of threats to digital evidence are data preservation, data counterfeiting, data hiding, and data destruction. There are two main subclasses of threats to digital evidence: physical and technical. From a technical perspective, data hiding and data destruction techniques have existed for some time in the hacker community, e.g. log deletion. In 2002, the first paper was published on intentionally deleting data to avoid detection by a well-known forensics software [1]. Data preservation is the process of ensuring that no forensic evidence is created, be they newly created evidence or the alteration of existing evidence. These techniques have been published recently in which software are loaded into memory for execution and are subsequently wiped from memory upon completion [2]. Data counterfeiting is the process of creating false and/or misleading data. These techniques have been known for many years and include techniques as simple as creating false log entries.

The same four threats to digital evidence exist from a physical perspective. First, media preservation can be achieved through write blocking devices and other means of ensuring that the media are not altered. Media destruction can be performed through the use of chemical, magnetic, and mechanical means. Mechanical threats, such as the use of a hammer or a knife, the use of a magnet or by a chemical solution can all destroy the media. Media replacement is done by replacing the affected system(s) with replicas. The other physical threat is displacement, in which the devices or media are stolen or otherwise moved.

Legal anti-forensics techniques exist as well. Legal doubt can be intentionally created in order to avoid prosecution. If it is not clear who performed an event or how it occurred, prosecution is difficult, especially in criminal cases. Crossing jurisdictions increases the difficulty to bring a matter to court, as well as increasing the difficulty of acquiring all evidence. Additionally, privacy laws, theoretical doubts (e.g., theoretical breakthroughs against MD5), and creating new legal precedents pose threats to investigations.

5. Taxonomy of Threats

Two major categories of threats to computer forensics by the effect they have on the forensic environment exist: threats to digital evidence and threats to the legal process.

5.1 Threats to Digital Evidence

The class of threats to digital evidence includes potential actions that can negatively affect the goals of the investigatory process by compromising digital evidence. There are the following subclasses of technical threats:

- Evidence Preservation: prevention of creation data that later may be used as evidence.
- Evidence Destruction: destruction of data that later may be used as evidence.
- Evidence Hiding: taking special steps to prevent investigators from accessing data.
- Evidence Counterfeiting: creation of misleading digital evidence.

All four subclasses can be divided into technical and physical threats by the way these threats affect the evidence. Technical threats are projected through software, while physical threats are projected through processes outside of the computer logic.

Table 1 provides examples of such threats.

Class	Subclass	Example
Evidence Preservation	Technical	Prevention from writing to hard drive.
Evidence Preservation	Physical	Installation of data gathering equipment that does not communicate with host network, such as a silent sniffer.
Evidence Destruction	Technical	Deletion of log file entries.
Evidence Destruction	Physical	Chemical, magnetic, mechanical destruction of media containing evidence.
Evidence Hiding	Technical	Use of encryption or steganography.
Evidence Hiding	Physical	Use of smart cards or hardware cryptographic modules.
Evidence Counterfeiting	Technical	Creation of misleading log file entries.
Evidence Counterfeiting	Physical	Physical replacement of system hard drive with a ghost image of the original hard drive with non-incriminating digital evidence.

Table 1: Examples of threats by class and subclass.

5.2 Threats to Legal Process

The class of threats to the legal process includes potential actions that can negatively affect the goals of the investigatory process by providing legal obstacles to collection, analysis, or presentation of digital evidence. The following are subclasses of threats to legal process:

- Sufficient Doubt: rules, regulations, and steps taken that ease the process of creation of sufficient doubt regarding the collected digital evidence.
- Privacy: rules, regulations, and steps taken that ease the process of denying the prevention of collection or presentation of digital data due to privacy concerns, which creates problems for the authentication of evidence,
- Cross-Jurisdictional Nature: rules, regulations, steps taken that prevent a forensic investigation started in a given jurisdiction to successfully obtain evidence from another jurisdiction.
- Significant Changes in Scientific Foundation: the threat is posed by scientific research that changes the environment that the proceedings are relied on. Such environmental changes may make the process of collection, preservation, and analysis of digital evidence unacceptable or foundationless.

The following provides examples of threats to the legal process:

Sufficient Doubt: Perform a crime from publicly-accessible or virus-infected computer; use of repudiation techniques such as communication through public forums or "mixed networks;" the creation of legal precedents.

Privacy: European Union laws prohibit transfer of personal data of EU citizens to outside of the EU.

Cross-Jurisdictional Nature: Performing crime from a jurisdiction with no extradition and no working relationship with the law enforcement of the target jurisdiction.

Significant Changes in Scientific Foundation: Recent proofs of weakness in SHA-1 and MD5 algorithms [Sc05].

6. Case Study

While several of the threats are widely known in practice, some are rarely seen in the field. This section presents an example of a case in which some of the less common forensic threats were encountered. The case involved a US-based company who was facing internal intellectual property theft, where evidence destruction and hiding, as well as cross-jurisdictional issues were occurring during the internal investigation.

A US-based medical device company ("A") who had a principal founder leave the company to start a competing company ("B") outside of the US in a country whose extradition and data export laws are known to be difficult for investigations. Because "B" was located in a country that is known to be uncooperative, evidence could not be gathered directly by "A." This legal impediment meant that "A" had to internally handle the intellectual property theft and stop future theft from occurring. This is an example of a legal process threat involving cross-jurisdictional issues.

The initial scope of the investigation was to determine employees who were stealing intellectual property and providing them to "B." The suspected employees consisted of executives, R&D scientists, and IT staff. The first step was to install sniffer devices for email and instant messages. "A" had three locations, one in the US, one in the EU, and one in Latin America. Sniffers were installed at all three locations, and current server email files were acquired.

Initial analysis of the email confirmed the belief that some of the original suspected employees were involved in suspicious emails, though those emails were not themselves smoking guns or sufficient evidence for employment termination. Analysis began on the instant message traffic via keyword searching. Instantly it was noted that data from one of the locations was missing. "A's" Latin American site's IT staff had stolen the device (as well as other equipment) before leaving the company, which prevented traffic analysis via this form of physical evidence destruction. The instant message traffic was surprisingly devoid of any relevant evidence or clues.

Further email analysis was performed – this time focusing on two pieces: the IT staff personnel who may have stolen the sniffer device and any correspondence relating to tipping off other employees of the internal investigation. Keyword searches, such as "investigation" and "instant message," yielded some results that allowed "A" to hone in on a specific set of employees, whereby those employees' hard drives were acquired and analyzed. Although the investigation did yield results, evidence was lost and additional intellectual property was most likely lost due to anti-forensic techniques and issues.

7. Conclusion

Anti-forensics poses a large challenge to each type of forensic investigation. As advancements in anti-forensics are made, the computer forensic body of knowledge and best practices must adapt. In order to do so, an overall taxonomy of threats is required. These threats must then be accounted for and properly classified. This paper provides the overall taxonomy and means for classifying future threats.

There exist two major categories of threats: threats to digital evidence and threats to the legal process. Threats to digital evidence are based on four classes: preservation, destruction, hiding, and counterfeiting. The subclasses for these threats are physical and technical. In addition, threats to the legal process exist. These threats are cross-jurisdictional, creating sufficient doubt, significant changes in scientific foundation, and threats based on privacy.

7.1 Future Work

Future work on this topic includes several steps. First, the development of a full taxonomy of threats, both anti-forensics and unintentional should be created to account for all possible threats. This paper focused on the intentional threats by an adverse party. Outside threats exist in which inherit weaknesses in the process, such as MD5 and chain of custody can prove to be problematic.

The second work is the creation of controls to account for and mitigate the threats posed to computer forensics. As in security, controls can be created for computer forensics. The threats posed to computer forensics are not insurmountable, and as such, they should be controlled through the methodical creation of better software and processes.

The third extension of this work is research into a third subclass of threats, namely "social" anti-forensic threats. Social threats include many of the same threats and themes as social threats to computer security. Collusion, for one, can have a negative impact on a forensic investigation if one person warns others involved in an incident to cover their digital tracks. Incorporating social activities and other non-digital evidence into computer forensic research can provide valuable insights for practitioners.

Bibliography

[BM06] Burmester, M.; Mulholand, J.: The Advent of Trusted Computing: Implications for Digital Forensics. 21st ACM Symposium on Applied Computing, Computer Forensics Track. Dijon, France. April 2006.

[Ca02] California Senate: California Database Breach Act (SB 1386). 2002. Online athttp://info.sen.ca.gov/pub/01-02/bill/sen/sb_13511400/sb_1386_bill_20020926_chaptered.htm

[Gr02] the grugq: Defeating forensic analysis on unix. Phrack 59, July 2002. Online at http://www.phrack.org/archives/59/p59-0x06.txt

[Ha06] Harris, R.: Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. The Proceedings of the 6th Annual Digital Forensic Research Workshop. 2006; pp 44-49.

[PR05] Pluf; Ripe.: Advanced Antiforensics: SELF. Phrack 63, July 2005. Online at http://www.phrack.org/archives/63/p630x0b_Advanced_Antiforensics_and_SELF.txt

[Sc05] Schneier, B.: SHA-1 Broken. Februrary 15, 2005. Online at http://www.schneier.com/blog/archives/2005/02/sha1_broken.html

[Se06] Selinger, P.: MD5 Collision Demo. 2006. Online at http://www.mscs.dal.ca/~selinger/md5collision