Cyber Forensics: A Military Operations Perspective

Joseph Giordano, Technical Advisor, AFRL Information Warfare Branch
Chester Maciag, Program Manager, AFRL Digital Forensics Program

Abstract

This paper discusses some of the unique military requirements and challenges in Cyber Forensics. A definition of Cyber Forensics is presented in a military context. Capabilities needed to perform cyber forensic analysis in a networked environment are discussed, along with a list of current shortcomings in providing these capabilities and a technology needs list. Finally, it is shown how these technologies and capabilities are transferable to civilian law enforcement, critical infrastructure protection, and industry.

Introduction

In the common vernacular, cyber forensics has been best understood to be a discipline belonging to the Law Enforcement community. In fact, most academic research and commercial tool development in this field have focused on assisting the police investigator in a post facto evidence-gathering process to meet the perceived minimal evidentiary requirements. The investigative process and its requisite tools require the physical seizing and imaging of the suspect's storage media and related hardware with emphasis placed on completeness and data integrity favored over timeliness of analysis in recovering and presenting the digital information, which routinely takes months to complete. Furthermore, many automated data recovery and analysis tools assume most crimes committed with computers are to enhance

conventional crimes and are so oriented so as to provide piecemeal recovery and analysis of standalone hardware such as desktop computers, personal digital assistants, and cellular telephones.

In contrast, while the term cyber forensics is a relative newcomer to the U.S. Military vocabulary, the concept of forensic computer analysis had its roots in the earlier days of computer intrusion detection (Anderson, 1980; Denning, 1988). Protecting the military's information infrastructures requires real-time assessment and analysis of perceived and actual cyber attacks, without the benefit of quarantining the victim computer or taking it off-line as in the law enforcement model. In the military environment it is almost certain that the information system is itself the target, and the information system and its connective elements are the primary sources of corroborative evidence used to timeline or piece together the sequence of events. This requires the preservation, recovery and analysis of digital information from broadly distributed network appliances and devices to determine how the information system was subverted to meet an adversary's objectives. It is this assessment that plays a pivotal role in the military's tactical decision-making process, otherwise known as the OODA Loop[1] (Boyd, 1987). The goal is to "get inside of the adversary's OODA cycle" by continually reducing the amount of time it takes for our military to observe and respond to the enemy's actions so that the adversary's ability to react is outpaced by our military actions. The forensic process is what drives the military's cyber attack recovery, reaction, and response functions. The military must provide timely post-attack and trans-attack cyber analysis, and if possible, prior indications and warnings of a cyber attack if it is to keep pace with the adversary's actions and OODA cycle.

A Military Cyber Forensics Definition

Given the above considerations, we offer the following definition for cyber forensics.

"*The exploration and application of scientifically proven methods to gather, process, interpret, and utilize digital evidence in order to:*

- ***Provide a conclusive description of all cyber-attack activities for the purpose of complete post-attack enterprise and critical infrastructure information restoration***
- *Correlate, interpret, and predict adversarial actions and their impact on planned military operations*
- *Make digital data suitable and persuasive for introduction into a criminal investigative process"*

While the last goal of the definition directly addresses law enforcement needs in cyber forensics, it is also required for the military commander who will be making decisions on how to engage aggressors in cyberspace, who may be civilian enemy combatants rather than state-sponsored attackers. The commander will need to know for sure who is attacking prior to taking any action that would be viewed as a violation of a Treaty or other international agreement. Forensic results that meet criminal investigative criteria can help justify a commander's actions in retaliation.

Current Cyber Forensics Challenges

Now that we have defined the criteria for a scientific pursuit of cyber forensics, let us look at some of the current challenges in making this pursuit viable:

[1] Observe, Orient, Decide, and Act

- There are no universal processes or scientific underpinnings in the methods used to recover or interpret digital information. There are a number of best practices in the field, some of which vary from agency to agency. With these varied processes and techniques in place today, there are no metrics established for comparison of process error rates or experiment repeatability to measure the merit between competing processes or best practices that are in use.
- There is a lack of standards to guide or drive commercial or military development of digital forensic tools and technology (NIJ, 2002):
    - A small number of vendors have built proprietary forensic tools that require expensive support. The vendors are often subpoenaed to describe their tools' theory of operation, again costing time and expense.
    - A large number of individuals from academia and law enforcement have built ad hoc tools for cyber forensic purposes, without good programming techniques that ensure some minimal standard for data integrity.
    - Given these disparate tools, a toolbox cannot be easily assembled because there is no data interoperability standard that allows the output of one tool to be used as input to another.
- There is a lack of adequate community information sharing for developed tools and technologies. As a result, there are many duplicative efforts trying to address the same problems, forfeiting the potential gains that could be made in researching and developed leading-edge capabilities (NIJ-CIAO, 2002).
- Commercial and private tool offerings are limited to post-attack analyses. Again, this is a result of the law enforcement model that precludes data collection on individuals

without a warrant. However, a trans-attack model could be applied to developing a new generation of tools for Industry and Government, both of whom own their networks and generally have strong "right to monitor" employment provisions. In addition, these analyses are:

  - Time-intensive and require on the order of months to analyze large media. By the time the analysis is complete, other electronic leads usually go cold.
  - The analysis is human-intensive due to a lack of sophisticated, automated recovery and analysis techniques. Success or failure in the courtroom currently depends on the strength of the expert witness called in to analyze the data and recovery processes, and not necessarily the recovered data itself.

- Currently offered tools or analysis concepts do not scale properly to the networked environment. Most tools and concepts assume the analysis or imaging of a single computer, offline from the network environment. The military will require the on-line analysis of its own compromised systems, whether on-site or at some geographically distant locale. Tools will need to address the impact of data integrity and transport issues when collecting information across the network.
- The law enforcement community currently drives the development of digital forensics tools. We need to bring a military operations perspective to include:
  - "Quick-looks" at digital information, while preserving its integrity.
  - Confidence factors provided to the commander when only a partial analysis of the dataset has been accomplished.

Required Military Operations Capabilities

The following required capabilities have been adapted from the 2002 Cyberterrorism Summit at Princeton University (NIJ, 2002):

- Data protection – When a candidate digital information source is identified, measures must be put in place to prevent the information from being destroyed or becoming unavailable.
- Data Acquisition – The general practice of transferring data from a venue out of physical or administrative control of the investigator, into a controlled location.
- Imaging – The creation of a bit-for-bit copy of seized data for the purposes of providing an indelible facsimile upon which multiple analyses may be performed, without fear of corrupting the original dataset.
- Extraction – The identification and separating of potentially useful data from the imaged dataset. This encompasses the recovery of damaged, corrupted, or destroyed data, or data that has been manipulated algorithmically to prevent its detection (e.g. encryption or steganography.)
- Interrogation – The querying of extracted data to determine if a priori indicators or relationships exist in the data. Examples include looking for known telephone numbers, IP addresses, and names of individuals.
- Ingestion/Normalization – The storage and transfer of extracted data in a format or nomenclature that is easily or commonly understood by investigators. This could include the conversion of hexadecimal or binary information into readable characters,

conversion of data to another ASCII[2] language set, or conversion to a format that can be input into another data analysis tool.

- Analysis – The fusion, correlation, graphing, mapping, or timelining of data to determine possible relationships within the data, and to developing investigative hypotheses.
- Reporting – The presentation of analyzed data in a persuasive and evident form to a human investigator or military commander.

Proposed Research Agenda

In this section we describe the work that needs to be carried out in order for forensics to be useful in a military operations environment. First, we need to begin R&D in the area of network forensic awareness. This is the overall concept of identifying, collecting, protecting, fusing, and analyzing distributed network information in order to scientifically understand the sequence of digital events and their impact on the enterprise. A major issue in this area is how to rapidly collect and normalize digital evidence from a variety of sources including firewalls, hosts, network management systems, and routers. The information that is collected could then be used to predict or anticipate adversarial actions, understand the current state of affairs, and help in determining appropriate courses-of-action.

Next, we desperately need to perform work that allows us to detect data hidden within network traffic. The hidden data problem is especially insidious. The art of hiding data is called steganography, which means "covered writing". In steganography one can embed data of interest inside of a carrier. The carrier is a piece of data that looks

[2] American Standard Code for Information Interchange

legitimate or harmless but hidden within the bits of the carrier is another message which is the true message. The carrier can be used by insiders smuggling sensitive information through a firewall or it can be used by a malicious outsider who wants to push malicious code or messages into a trusted domain. We need to perform R&D that allows us to detect and extract data hidden with transactions or streaming media. We need to look at the hidden data area from the perspective of covert channels within standard protocols.

Another area of importance and one that thus far has received no attention is database forensic analysis. We need to be able to reconstruct past events and trace evidence to indicate data destruction, reconstitution of damaged or destroyed databases or their schemas, and direct attacks on the DBMS's[3] security mechanism to gain privileges to a database or the operating system. Although there are a few vendor-provided analysis tools to assist in forensic reconstruction of databases, these tools rely upon system auditing and logging which are frequently turned off in favor of performance. Best practices, processes, algorithms, and tools need to be developed to provide these indicators without the benefit of the system-provided auditing.

A fourth area that holds great promise for forensic analysis in a military operations environment is distributed intelligent forensic agents. Distributed intelligent forensic agents would be small, lightweight programs that are launched from an agent control center whenever a suspicious event is identified. These agents would then gather the appropriate digital evidence and return the evidence to central control for further analysis by other tools. Due to legal considerations, use would be limited to monitoring and reconstruction of military-owned networks. Use of these agents could be similarly

[3] DataBase Management Systems

extended to the corporate environment in company-owned Intranets where company right-to-monitoring has been established in the acceptable use policy.

Trusted Timestamps are a fifth area of research to be considered when performing network-based cyber forensics (Hosmer, 2001). In order to properly timeline events over a distributed network system, events collected at each appliance or node need to be properly time-synchronized. Due to the natural drift errors in computer clocks, combined with the ease in which system clocks can be changed by the attacker and the ease in which the NTP[4] can be subverted, a method needs to be developed that relies upon a trusted third party to corroborate the time that an event occurred. This could also be used in forensic analysis facilities to prove when certain data was retrieved and analyzed, to provide irrefutable proof of the time when a transaction occurred on a digital system.

Sixth, the proliferation of cellular and wireless hand-held devices presents a unique challenge to the forensic examiner. Unlike a wired network in which investigation of a cyber attack eventually leads to tracing the attack back to a physical location, a wireless information attack does not require physical access to the medium being exploited. Furthermore, it is not difficult to envision a scenario in which malicious software could be inserted into military or commercial wireless devices in order to obtain classified or proprietary information from those devices in a covert manner. This may be a concern now that these devices possess sufficient configurability and processing power to run a range of capable programs. Similarly, the analysis of seized wireless and cellular equipment, while preserving data integrity, will be a required capability as well to determine adversary intent and intelligence collection strategies.

[4] Network Time Protocol

"Quick views" of seized media is the seventh major area to be researched. Current approaches to analyze the entire hard drive can take many months. For the purpose of quickly restoring operations, an Operating System Hash Library could be constructed to fingerprint hash values of operating system files of properly configured software. A quick comparison of this hash list to the fingerprint obtained from a suspect system could yield important information regarding the severity or intent of a cyber attack, while the digital "leads" are still hot.

An eighth area of pursuit is the multi-lingual analysis of storage media. No longer is the cyber world one which is utilized primarily by English-speaking citizens. Each day a greater percentage of Asians, South Americans, and Africans are able to obtain access to the Internet and pose a threat to the U.S. Military and law enforcement. The investigations of these attacks in the past have involved processing deleted and damaged files and media through North American ASCII character sets. We now realize that information may be innocuously present through a mapping to alternate ASCII character sets. An automated means that can translate the recovered data or at least indicate a probable language set is vital to the timely processing of cyber attacks posed by non-English speaking citizens and foreign nationals.

Finally, there needs to be a uniform standard for the development and testing of forensic tools. There need to be metrics established that help determine the extent that a software or hardware tool performs a particular forensic function, and the associated error rate with that process. This will help expedite the analysis of comparable tools, with an understanding of how failed tests will impact advertised capability.

Conclusion

While this paper presented the challenges and projected needs for military operations, these capabilities will soon have direct applicability to the problems faced by local and Federal law enforcement. The paradigm of using computers as a enabler for traditional crimes is constantly shifting toward one in which the information system itself is exploited. As a result, Government, Industry, and Academia are faced with new challenges in scaling current capabilities toward a network-based cyber attack scenario. The analysis in the network environment engenders the same needs for data preservation, recovery, etc., as in the standalone environment, yet presents some unique additional challenges in scalability, data integrity, and timeliness of analysis.

The next steps in pursuit of a cyber forensics program that meets current and future military operations needs are:

- The Initiation and sustainment of a community of researchers with expertise in Digital Forensics.
- Increased awareness of existing tools and ongoing research efforts.
- New tools and capabilities that address:
    - Unique forensic challenges presented by a networked and wireless environment.
    - Post-attack cyber attack damage assessment and awareness of impact to infrastructure.
    - Military and Critical Infrastructure Protection requirements for Indications and Warnings prior to a cyber attack.

  - Development of better prosecutorial requirements for submission and use of digital evidence in the courts.

- Improved Industry investment in Digital Forensics area through establishment of standards and guidelines for tool development. The military has been challenged to obtain commercial solutions for its forensic requirements. It is incumbent upon the military community to articulate its needs so that partnerships can form between Industry and DoD to provide the required capabilities off the shelf.

Bibliography

Anderson, James P. (1980). *Computer Security Threat Monitoring and Surveillance*, Retrieved from UC-Davis Web site October 17, 2002, http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf

Boyd, John R. (1987). A Discourse on Winning and Losing, Unpublished set of briefing slides available at Air University Library, Maxwell AFB, AL, Report No: mu43947

Denning, Dorothy. (1987). An Intrusion Detection Model. IEEE Transactions On Software Engineering, Vol. SE-13, No. 2

Hosmer, Chet. (1998). Time-Lining Computer Evidence, Retrieved from WetStone Technologies Web Site 4 Jun 2002, http://www.wetstonetech.com/timelining.pdf

National Institute of Justice. (2002). Results from Tools and Technology Working Group, Governors Summit on Cybercrime and Cyberterrorism, Princeton NJ

About the Authors

Joseph Giordano

Joe Giordano is the technical advisor for the Defensive Information Warfare branch at the Air Force Research Laboratory's Rome Research Site located in Rome, New York. He has worked at AFRL for 21 years in the areas of Database Security, Computer Security, Information Assurance, and Information Warfare. Currently, he is responsible for the R&D and technical planning in the area of Information Assurance.

Chet J. Maciag

Mr. Maciag is a serves as a full-time civilian employee of the Air Force Research Lab's Information Directorate, Rome NY. In this capacity, he leads research and development of computer forensics tools and technologies for military operations and law enforcement. He routinely interacts with the Office of the Secretary of Defense, the NY Electronic Crimes Task Force, the National Institute of Justice, the National Institute of Standards and Technology, the DoD Computer Forensics Lab, and the NYSP Computer Crimes Unit. He has helped formulate AFRL's Information Warfare Vision and has been a contributing author in over eleven papers in the areas of information assurance and information operations. His expertise is in the areas of network management, firewalls, guards, intrusion detection, and enterprise protection planning.

Mr. Maciag serves as adjunct professor of Economic Crime Management at Utica College where he teaches *Internet and Network Security* and *Information Security*. He is also a graduate of the master's program in Economic Crime Management program. He is a mentor for Utica College, SUNY-IT, and Scholarship for Service students each summer.