

The Application of Intrusion Detection Systems in a Forensic Environment

(Extended Abstract)

Peter Stephenson

Netigy Corporation, San Jose, CA

And

Oxford Brookes University,

School of Computing and Mathematical Sciences, Oxford, UK

ABSTRACT: Over the past three or four years there has been some controversy regarding the applicability of intrusion detection systems (IDS) to the forensic evidence collection process. Two points of view, essentially, have emerged. One perspective views forensic evidence collection and preservation in the case of a computer or network security incident to be inappropriate for an intrusion detection system. Another perspective submits that the IDS is the most likely candidate for collecting forensically pristine evidentiary data in real or near real time.

This extended abstract describes, briefly, the framework for a research project intended to explore the applicability of intrusion detection systems to the evidence collection and management process. The project will review the performance and forensic acceptability of several types of intrusion detection systems in a laboratory environment.

1.0 Background and Problem Statement

Intrusion detection, as a discipline, is fairly immature. Most of the serious work in intrusion detection is being carried on in the academic, commercial and government research communities. Commercially available examples of successful intrusion detection systems are limited, although the state of the art is progressing rapidly. However, as new approaches to intrusion detection are introduced, there is one question that seems to emerge continuously: should we be using intrusion detection systems to gather forensic evidence in the case of a detected penetration or abuse attempt.

The whole concept of mixing investigation with detection of intrusion or abuse attempts begs a number of questions. First, can an IDS perform adequately if it also has to manage evidentiary data appropriately to meet legal standards? Second, what is required to automate the management of data from an evidentiary perspective? Third, what measures need to be added to an IDS to ensure that it not only can perform as an IDS (including performance requirements for the type of system in which it is implemented), but that it can manage evidence appropriately? It is not appropriate to ask any system to do double duty, performing additional tasks which may or may not be related to its primary function, at the expense of the results of its primary mission.

This idea – that of combining evidence gathering with system protection – has generated considerable discussion over recent years. There is reasonable conjecture as to whether the presence of an IDS during an

attack provides an appropriate evidence gathering mechanism. There appears to be general agreement, informed or otherwise, in the courts that such is the case. Today, in the absence of an alternative, the IDS probably is the best source of information about an attack. Whether that information is forensically pristine or not is an entirely different question.

Sommer [SO98], however, reports that the NSTAC Network Group Intrusion Detection Subgroup found in December 1997 that:

- “Current intrusion detection systems are not designed to collect and protect the integrity of the type of information required to conduct law enforcement investigations.”
- “There is a lack of guidance to employees as to how to respond to intrusions and capture the information required to conduct a law enforcement investigation. The subgroup discussed the need to develop guidelines and training materials for end users that will make them aware of what information law enforcement requires and what procedures they use to collect evidence on an intrusion.”

This finding implies strongly that there is a disconnect between the use of intrusion detection systems and the collection of forensically appropriate evidence during an intrusion attempt.

On the other hand, Yuill et al [YU99] propose that an intrusion detection system can collect enough information during an on-going attack to profile, if not identify, the attacker. The ability of an IDS to gather significant information about an attack in progress without materially affecting the primary mission of the intrusion detection system suggests that an IDS could be deployed that would provide both detection/response and forensically pristine evidence in the case of a security incident.

1.1 Problem Statement

Fundamentally, this project seeks to answer the question: “Is it practical and appropriate to combine intrusion detection and response with forensic management of collected data within a single IDS in today’s networks?”. The issue we will address in this research is three-fold. First, can an IDS gather useful forensic evidence during an attack without impacting its primary mission of detect and respond? Second, what is required to provide an acceptable case file of forensic information? And, finally, in a practical implementation, can an IDS be implemented that will accomplish both its primary mission and, at the same time, collect and manage forensically pure evidence that can be used in a legal setting?

There are several difficulties in addressing these issues. First, the theoretical requirements of an IDS in terms of performing its primary mission may be at odds with the requirements of collecting and preserving forensic evidence. The primary mission of an IDS is to detect and respond to security incidents. The definition of a security incident should be, at least in part, determined by the organization’s security policy. Therefore, the detailed definition of the IDS’ primary mission is partially determined by the security policy, not by some overarching standard or generic procedure. The result is that there can be a wide disparity among requirements for an IDS from organization to organization. That contrasts significantly with the relatively static set of requirements for developing and managing evidence for use in a legal proceeding.

A second difficulty is that the IDS, by design, does not manage its information in the sense that a forensics system does. There is a requirement within a forensic system (automated or not) for, among other things, the maintenance of a chain of custody whereby all evidence can be accounted for and its integrity attested to from the time of its collection to the time of its use in a legal proceeding.

The third difficulty deals with the architecture of the IDS. The ability of a program to perform widely disparate tasks (in this case detection and response as well as forensic management of data) implies an architecture that may or may not be present currently in an IDS. Thus, there develops the need for a standard architecture for intrusion detection systems that also are capable of forensic data management.

2.0 Prior Work

There has been very little prior work done in the area of combining forensics and intrusion detection into a single system. The assumption for the purposes of this project is that we can define both the forensic and detection and response requirements individually. Thus, we look to the literature for examples of both. We are interested in examples of these requirements both in isolation and taken together. Our examination here is not exhaustive, but, we believe, it is representative of significant contributions to the field(s). Please refer to the bibliography at the end of this paper.

Additionally, C.A.R. Hoare has done significant work in mathematical modeling using the CSP (Communicating Sequential Processes) process algebra [CH85]. This work has been extended by William Roscoe [WR97]. In view of prior work with CSP in the security arena, it appears that it may offer possibilities for developing formal models that will be useful in this project.

2.1 Combining Forensics and Intrusion Detection

Contribution to the groundwork in the theoretical area of combining intrusion detection and forensics as well as the roles that both disciplines play in the overall network security picture, has been done by Stephenson in the form of the Intrusion Management Model [ST00]. Yuill et al [YU99] have done significant work on the specifics of the use of the output of an IDS used both as evidence and as an investigative tool. The legal implications of such use, however, are not thoroughly explored. Other work in the area has been done by Gross [GR97] and Monroe [MO99]. We have previously mentioned Sommer [SO98]. Clearly, the work in this combined area is limited and offers fertile ground for further investigation.

3.0 Hypothesis

We hypothesize that evidence exists to suggest that an appropriately designed and implemented intrusion detection system can be used to collect, process and manage forensic evidence of an intrusion or abuse attempt. We believe that existing literature suggests that the barriers to such an implementation are in the areas of the performance and fundamental architecture of the IDS. That being the case, we believe that the barriers can be overcome.

Specifically, the hypotheses we wish to test are as follows:

- The correct implementation of forensic procedures in an intrusion detection system will not materially affect its ability to perform its primary mission: detection and response to intrusion or abuse attempts.
- The requirements for deployment of an automated forensic capability in a network environment can be described and formally modeled and that model can be used in practical application.
- An intrusion detection system can be demonstrated that performs both its primary mission and forensic evidence capture and management, without unacceptable performance degradation, while performing according to the forensic model referred to above. Such characteristics as protection for audit logs, attack and evasion resistance, are, of course, implicit in acceptable forensic, detection and response performance.

4.0 Objectives and Approach

Our general approach consists of three phases:

4.1 Phase 1 – Current State

- Detailed research and cataloging of prior formal work in forensics (both computer and network) and intrusion detection

- Determine the general impact of forensic evidence management on an IDS – devise an appropriate test bed for benchmarking

4.2 Phase 2 – Theoretical Models

- Analyze and model the forensic process both in computers and networks
- Analyze and model (or update existing models) intrusion detection systems of various types
- Theorize a combined model for intrusion detection in a forensic environment – create both operational and formal models – select appropriate IDS type(s)
- Design an appropriate architecture for an IDS in a forensic environment using the SABSA architecture design method traceable to appropriate standards

4.3 Phase 3 – Laboratory Demonstration of Proposed System

- Using the test bed developed in Phase 1, configure and optimize the IDS(s) theorized in Phase 2 for combined IDS and forensic use
- Using metrics developed in Phase 1, measure the impact of forensic analysis on the optimized IDS
- Determine the appropriate architecture for an optimized IDS/forensic tool and reconcile the theoretical model with actual test results

4.4 Overarching Objective

The overarching objective of this research is the development of a theoretical model and architecture for an intrusion detection system that also can perform forensic tasks. Due to the differences in intrusion detection architectures, at least four different types of systems must be explored. Schwartzbard and Ghosh describe the differentiation of intrusion detection systems as falling along two axes: host or network based, and anomaly or misuse detection [SG99]. Stefan Axelsson characterizes the detection axis as containing anomaly based or policy based approaches [SA99]. For our purposes, we prefer Axelsson's description of the detection axis since the concept of the IDS supporting the organization's computer security policy is an important one.

Since the requirements of the various combinations of intrusion detection system deployments (network or host based) and detection types (policy or anomaly based) offer different sets of challenges, both to the IDS and the forensics, we must develop appropriate models, architectures and laboratory instantiations in order to prove our hypotheses completely.

Thus, our overarching objective is to be able to generalize a theory that supports intrusion detection and forensics computer science in the same system, regardless of its specific application. We believe that this overarching objective presents some significant challenges in the case of host based intrusion detection systems. Most of these challenges have to do with defining the lengths to which we wish to extend forensic analysis of the target system. For example, capture of a physical image of a computer disk by the IDS (or an extension of the IDS) presents some significant difficulties.

5.0 Author

Peter Stephenson is the director of technology for the Global Security Practice of Netigy Corporation in San Jose, California. He is the author of several books and numerous articles in computer trade publications. He is a PhD candidate at Oxford Brookes University, Oxford, UK. Prior to joining Netigy in 1999, Mr. Stephenson operated a security consulting practice for 15 years. He is the developer of the Intrusion Management model for information protection and the VAST process for network vulnerability analysis.

- [SO98] “Intrusion Detection Systems as Evidence”, Peter Sommer, Recent Advances in Intrusion Detection – RAID 98.
- [YU99] “Intrusion Detection for an On-Going Attack”, Jim Yuill, S. Felix Wu, Fengmin Gong, Ming-Yuh Huang, 2nd *International Workshop on Recent Advances in Intrusion Detection – RAID 99*
- [RO95] High Technology Crime – Investigating Cases Involving Computers, Kenneth Rosenblatt, KSK Publications, 1995 – ISBN 0-9648171-0-1
- [GR97] “Analyzing Computer Intrusions”, Andrew H. Gross, PhD Thesis, University of California, San Diego, San Diego, CA, 1997
- [MO99] “BlackLab: A Workbench for Forensic Analysts” Area Systems, Exodus Communications, Inc., Columbia, MD, December 1999
- [AM99] Intrusion Detection, Edward Amoroso, Intrusion.net Books, 1999 – ISBN 0-9666-700-7-8
- [NO99] Network Intrusion Detection – An Analyst’s Handbook, Stephen Northcutt, New Riders Publications, 1999 – ISBN 0-7357-0868-1
- [RA97] “Implementing a General Tool for Network Monitoring”, Marcus Ranum, Kent Landfield, Mike Stolarchuck, Mark Sienkiewicz, Andrew Lambeth and Eric Wall, <http://www.nfr.net/publications/LISA-97.htm>
- [DE86] “An Intrusion Detection Model”, Dorothy Denning, *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May, 1986
- [PN97] “EMERALD”, Philip Porras and Peter Neumann, *Proceedings of the National Information Systems Security Conference*, Baltimore, MD, 1997
- [ST99] Investigating Computer Related Crime, Peter Stephenson, CRC Press, 1999 – ISBN
- [ST00] “Intrusion Management: A Top Level Model for Securing Information Assets in an Enterprise Environment”, Peter Stephenson, *Proceedings of EICAR 2000*, Brussels, Belgium, March 2000
- [SK99-1] “Tamperproof Audit Logs as a Forensics Tool for Intrusion Detection Systems”, B. Schneier and J. Kelsey *Computer Networks and ISDN Systems*, 1999
- [SK99-2] “Minimizing Bandwidth for Remote Access to Cryptographically Protected Audit Logs”, John Kelsey and Bruce Schneier, 2nd *International Workshop on Recent Advances in Intrusion Detection – RAID 99*
- [CD99] “Air Force Intrusion Detection System Evaluation Environment”, Terrence G. Champion and Robert S. Durst, 2nd *International Workshop on Recent Advances in Intrusion Detection – RAID 99*
- [MM99] “Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems”, Peter Mell and Mark McLarnon, 2nd *International Workshop on Recent Advances in Intrusion Detection – RAID 99*
- [CO99] “Guidelines for Forensic Investigations” and additional documents and data sheets, Michael Corby, Internal documents, Netigy Corporation, 1999
- [IC95] Computer Crime: A Crimefighter’s Handbook, D. Icove, K. Seger & W. VonStorch, O’Reilly & Associates, Inc., 1995 - ISBN

[SG99] “A study in the Feasibility of Performing Host-based Anomaly Detection on Windows NT”, Aaron Schwartzbard and Anup K. Ghosh, 2nd *International Workshop on Recent Advances in Intrusion Detection – RAID 99*

[SA99] “On a Difficulty of Intrusion Detection”, Stefan Axelsson, 2nd *International Workshop on Recent Advances in Intrusion Detection – RAID 99*

[CH85] Communicating Sequential Processes, C.A.R. Hoare

[WR97] The Theory and Practice of Concurrency, William Roscoe, pub Prentice Hall International Series in Computer Science