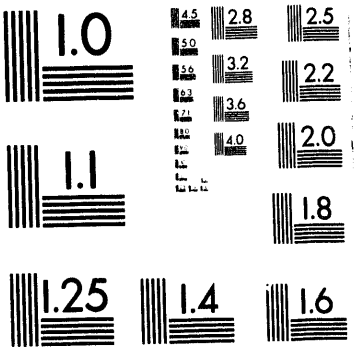
1.0
4.5
2.8
2.5
5.0
3.2
2.2
5.6
3.6
2.0
4.0
1.1
1.8
1.25
1.4
1.6

1 of 1

Conf-9405111--1

LA-UR- 94- 592

Title: MANAGEMENT ISSUES IN AUTOMATED AUDIT ANALYSIS

Author(s): K.A. Jackson, J. G. Hochberg, S. K. Wilhelmy, J. F. McClary, and G. G. Christoph

Submitted to: DOE Computer Security Group Training Conf., Denver, CO, May 2-5, 1994

MASTER

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Los Alamos
NATIONAL LABORATORY

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the University of California for the U.S. Department of Energy under contract W-7405-ENG-36. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy.

Form No. 836 R5
ST 2629 10/91

Management Issues in Automated Audit Analysis*

Kathleen A. Jackson, Judith G. Hochberg, Sharon K. Wilhelmy,
J. F. McClary, and Gary G. Christoph

Computing, Information and Communications Division
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

Abstract

This paper discusses management issues associated with the design and implementation of an automated audit analysis system that we use to detect security events. It gives the viewpoint of a team directly responsible for developing and managing such a system. We use Los Alamos National Laboratory's Network Anomaly Detection and Intrusion Reporter (NADIR) as a case in point. We examine issues encountered at Los Alamos, detail our solutions to them, and where appropriate suggest general solutions. After providing an introduction to NADIR, we explore four general management issues: cost-benefit questions, privacy considerations, legal issues, and system integrity. Our experiences are of general interest both to security professionals and to anyone who may wish to implement a similar system. While NADIR investigates security events, the methods used and the management issues are potentially applicable to a broad range of complex systems. These include those used to audit credit card transactions, medical care payments, and procurement systems.

1. Introduction

Providing security for the main computer network at Los Alamos National Laboratory is an enormous task. Computer work at Los Alamos ranges from Unclassified to Secret. Our main computer network, the Integrated Computing Network (ICN), serves nearly 9,000 users who enter the ICN some 2.5 million times a year. It includes six Cray-class supercomputers, several massively parallel machines, many smaller mainframe computers, and more than six thousand workstations. In addition, it includes requisite file storage devices, network services, local and remote terminals, and data communication interfaces. If authorized to do so and using an approved entry path, any user inside the Laboratory may access any host computer from office workstations or terminals. Outside users can enter the ICN through telephone modems, leased lines, or one of many world-wide networks.

As in most computing facilities, our first line of defense against security violations is formality of operations. This includes institutional practices such as

*Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy (DOE) under contract W-7405-ENG-36. This work was performed under the auspices of the United States Department of Energy.

training, physical security measures, and software controls that restrict access to the computing network, the individual systems that comprise it, and its files. Several factors limit the efficacy of these measures. The first is human nature. Users often see security procedures as unwelcome diversions from, or impediments to, the main thrust of their work. They therefore may fail to apply, or actively circumvent, even minimal security measures. Second, system managers must effect a compromise between conflicting concerns. Whereas security requires constraints, users often require access to distributed resources. Third, systems frequently contain undetected vulnerabilities. Finally, there is the threat of the insider who misuses his or her legitimate privileges.

Given these weaknesses, another (generally under-utilized) line of defense against inappropriate behavior is the maintenance and analysis of an audit record of network activity. Such an audit record contains network information; for example, who signed on, at what time, for how long, and on what node. We have maintained such an audit record at Los Alamos since the inception of the ICN. In theory, one can detect break-in attempts and other security violations by searching for abnormalities in the audit record. However, the traditional approach of manual audit analysis is problematic. Human data processing limitations restrict manual review to a sampling or cursory scanning of the large quantity of audit data typically generated. This approach can target only a few obvious misuse scenarios; it may miss even these because of human error.

As a result, misuse is all too often discovered more by luck than by design. For example, Clifford Stoll's adventure stalking the Hanover hackers began with but a $0.75 accounting discrepancy [1]. At Los Alamos, while periodic manual reviews by security auditors in the past did reveal instances of misuse, there was no way to evaluate the general success or completeness of this effort. Large-scale manual audits on demand also proved cumbersome and time-consuming.

We hypothesized that an automated audit record review would be more effective. Such an analysis can combine expert knowledge of security problems with a computer's capability to accurately process and correlate large quantities of data. In addition, the speed of machine processing can allow an automated system to inform auditors of suspicious activity in time for them to trace and stop it.

We put our hypothesis to the test by developing the Network Anomaly Detection and Intrusion Reporter, or NADIR, to provide automated computer misuse and intrusion detection on the ICN. NADIR has been in operation for four years. It targets all users who attempt to access the ICN, successfully or unsuccessfully. Perpetrators may be either insiders (authorized users) who misuse their privileges, or outsiders who attempt to clandestinely enter the ICN. Of these, we consider the insider threat the more serious since insiders perpetrate approximately 80% of computer misuses [2]. The insider's inherent user privileges, and knowledge of the computing system and its defenses, make him (or her) inherently more dangerous than all but the most skilled outsider [3].

Somewhat analogous to a threshing machine, NADIR separates the grain of suspicious activity from a much greater quantity of uninteresting straw. This process reduces potentially interesting users from more than 4000 a week (the number who logon to the network in an average week) to approximately 90. These users of interest are ranked according to an *anomaly score* assigned by NADIR as a result of the user's activity. Users with low anomaly scores get only a cursory review. We investigate users with higher scores in greater detail, often asking NADIR for further statistics of interest. The most anomalous users are interviewed by a security officer. Besides identifying anomalous users, NADIR provides textual and graphical representations of overall system activity.

Managing the design, implementation, and maintenance of an automated audit analysis system such as NADIR presents an interesting variety of challenges. These systems are relatively new and are often viewed as research. They involve a unique mixture of acceptance, legal, technical, and investigative difficulties not found in most other projects. Our emphasis in this paper will be on these unique management considerations, including the need to:

- Demonstrate the usefulness of automated analysis systems through cost-benefit analysis.
- Balance the institution's need for security with the user community's privacy expectations by codifying and disseminating an audit analysis policy and monitoring user reactions to investigations.
- Take into account the current legal status of auditing at different levels of detail.
- Ensure the integrity of the system and of the data it generates. An accurate *chain of evidence* is important for the effective use of automated auditing systems.

We will discuss these issues in turn following a brief description of the NADIR system and how we use it in our security operations.

2. NADIR in a Nutshell

2.1 Overview

The ICN consists of four partitions. Each partition processes at defined security levels. Each port into the ICN connects to one partition. Any workstation or terminal connected to a port can access computers in its partition. In addition, the workstation or terminal may access one additional partition at a less classified security level (if its partition is not itself the lowest level). A system of dedicated ICN *service nodes* link the partitions. These nodes perform network services such as user authentication and authorization, job scheduling, file access and storage, file movement between partitions, and hardcopy output. The service

nodes enforce the network partitioning. For example, they block unclassified users from accessing classified files or logging onto machines in classified partitions.

NADIR currently draws on data from three of these service nodes (see Figure 2-1). These nodes have important security responsibilities. They are the Network Security Controller (NSC), which performs centralized user authentication and authorization, the Common File System (CFS), which provides mass file storage (currently 37 TBytes), and the Security Assurance Machine (SAM), which provides for file migration between ICN security partitions. Each day these three nodes accumulate approximately 40,000 individual audit records, each record reflecting one application event. Each service node transmits its audit records to a SUN workstation for analysis.

Once a day, weekly, or on demand, NADIR summarizes the audit record into statistical profiles of individual users (e.g., how many files did the user access?), and for the network as a whole (e.g., how many logon failures resulted from password errors?). It compares the profiles to a set of expert rules that define suspicious behavior as well as violations of specific security policies. When a user 'triggers' a rule -- i.e., exhibits the behavior the rule describes -- NADIR increments his or her anomaly score. An anomaly score for the network as a whole is generated in a similar manner. Thus we seek indicators of out-of-bound behavior both for each user and for the whole network.

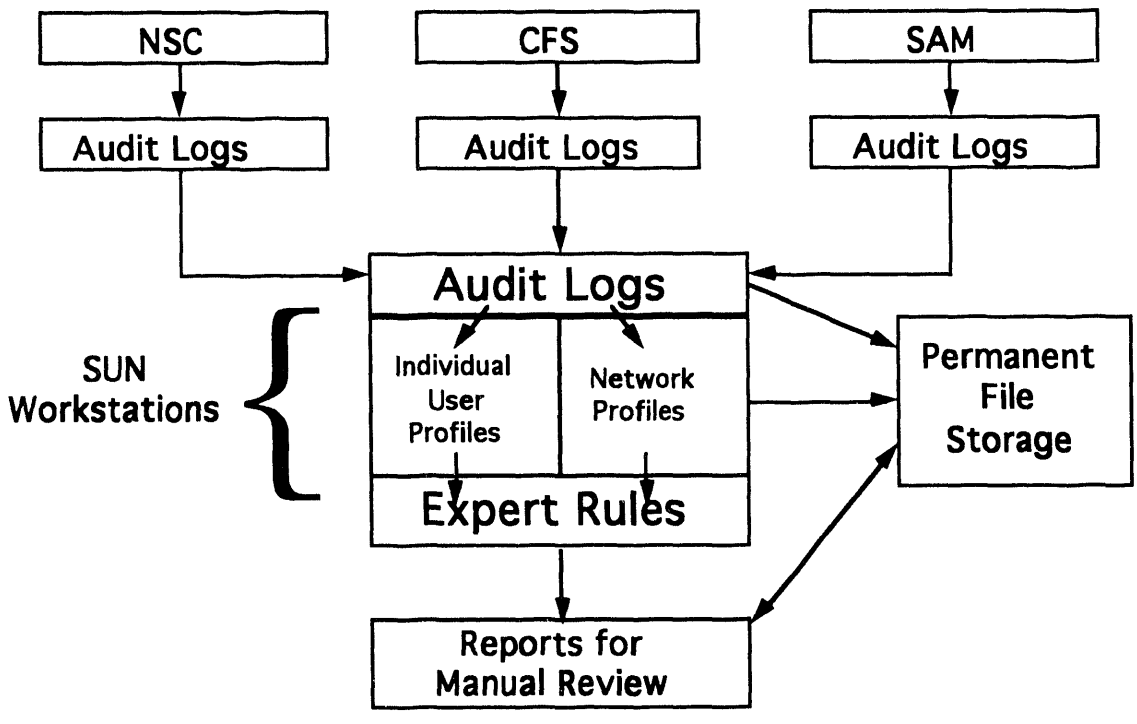

Figure 2-1: NADIR System Overview

A key element of a successful audit analysis mechanism is an effective reporting facility. The mechanism must generate timely, easily readable, and comprehensive reports of suspicious users and events. Each day, NADIR generates a summary report. Every week, it generates both a summary report and a more detailed report that includes data from the audit record. It stores these reports electronically for review by authorized personnel. Besides daily and weekly reporting, NADIR can produce, as necessary, reports on demand. On-the-spot reports have proved invaluable in analyzing ongoing emergencies detected by system operators. Finally, we use raw or profiled data, kept in long-term storage, to perform ad-hoc background analyses of current and past activity for selected users. Authorized personnel can examine this data using a relational data base manager's built-in facilities, or pipe data to a statistical software package for more detailed analysis.

As our focus in this paper is management issues, we refer the reader to the referenced papers [4, 5] for further design and implementation details.

2.2 Investigations

Follow-up investigations of flagged users and events are another necessary function of every successful audit analysis mechanism. Los Alamos security personnel have long investigated computer security events. However, NADIR detects many more events than were found in the past, all of which must be evaluated, and many must be investigated at some level. To help with this additional workload, NADIR provides an on-line interactive investigative capability. This gives computer security officers access to vast quantities of information with minimal effort.

2.2.1 System Events

NADIR daily and weekly reports provide a variety of information about current and past system activities. Over a period of weeks or months, these reports help security officers develop a feeling for what normal system behavior looks like, thus enabling them to spot abnormalities. To get an overall impression of current activity, the officer first views each system at a top level. Spreadsheets make it easy to compare current activities with equivalent prior periods. Raw numbers, percentages, means, standard deviations, and variances are provided. Bar charts pinpoint specific problems by providing hourly breakouts of various system activities. This granularity is adequate to highlight unusual events, and provides a visual comparison of one period (hour, shift, or workday) to another. An anomaly is defined as any value two standard deviations from the mean, either in the spreadsheets or the bar charts. Anomalies may stem from a single value (spike), cluster of values (burst), or repetitive pattern of spikes (periodicity). In a typical week, half a dozen such system anomalies (or events) are found. For example, we readily detect incipient hardware failures, major project deadlines,

end-of-accounting period activity, certain kinds of runaway jobs, and coding errors in system libraries.

For each system-wide anomaly, the security officer first collects background information by querying the NADIR system. The officer finds out which users were using the system at the time of the anomaly and what they were doing. The officer then contacts these individuals to ensure they were really on the system (to rule out masquerades), and to determine the cause of the anomaly. The officer formalizes all findings in a report that is maintained indefinitely in electronic form. Security management reviews these reports at regular meetings. These regular reviews are an important component of the program.

2.2.2 User Events

NADIR provides information on anomalous users as well as system anomalies. In a typical week about 1% of all ICN users are flagged as anomalous; i.e., are assigned positive anomaly scores based on their triggering some expert rule or rules (recall section 2.1). This amounts to no more than 90 anomalous users per week. Of these, about 75% have low anomaly scores, nearly all the rest are moderately suspicious, but perhaps two or three are very suspicious. For moderately or highly suspicious users, a security officer reviews the user's recent activities, past anomalous activity, and previous investigation reports. The officer then interviews the user to determine if the user caused the anomaly (to rule out masquerades), and to determine the cause of the anomaly. Interviews take place in person, by telephone, or by email. All user investigations result in reports that are also maintained indefinitely in electronic form. As with the system anomaly reports, security management reviews these reports in regular meetings.

While true security infractions are dealt with sternly, most anomalies are not the result of deliberate user action to subvert security. They stem from well-intentioned individuals who are simply struggling with their own misunderstanding or inexperience. Most have simply not mastered the security and computing learning curves. Many are new users or are learning new techniques. Some are careless. Many have made mistakes, such as programming errors. In these cases, investigations provide an opportunity to obtain valuable feedback on the use of our network and to educate our users on proper network usage and security policy. This has the added benefit of establishing goodwill with our users, who come to view security personnel as helpers, not adversaries.

An investigation may result in a warning to the user, or in the user losing, at least temporarily, his or her privileges. More often, it results in a positive learning experience for the user. The auditors file a short report at the completion of each investigation, giving details of its resolution. These reports, and periodic reviews of NADIR by the security auditors, provide valuable feedback in continuing efforts to improve the system.

3. Cost-Benefit Analysis

Managers are always concerned with value. They want to know, "What will this effort cost and what will it buy for me?" While we can approximately quantify the cost in man-hours of developing and operating NADIR, its benefits are harder to measure because its major benefit is the avoidance of potentially catastrophic events. We believe that the value of preventing such an event is virtually beyond cost, especially in a classified environment such as ours. The cost of repairing a damaged network, rebuilding months of work on system software, or having one's military equipment fail in battle, dramatically outweighs that of systems such as NADIR. NADIR can therefore be thought of as inexpensive insurance, not because it enables us to replace lost information, but because it helps prevent loss first. However, we understand the need to justify this expenditure to a possibly skeptical management.

3.1 Cost

Achieving and maintaining automated data collection and analysis at Los Alamos has been a relatively inexpensive undertaking. This section details our personnel, hardware, and software expenses, both for initial development and for ongoing system maintenance.

Personnel. Personnel costs to interpret our security policy, define misuse, and develop the system to date are approximately six man-years. Approximately three man-years were required to design and implement the initial system, incorporating Network Security Controller data. The remaining two man-years were used to add data from the Common File System and the Security Assurance Machine to the system. Two full-time equivalents (FTE's)[1] are now working to add additional data sources.

Two FTE's are assigned to train security officers, review incidents, interview suspicious users, and occasionally repair or upgrade the operating system. Of these, at least one and a half FTE's have replaced our previous staff commitment for manual review rather than adding to our payroll. Finally, user cooperation in interviews involves a small time cost to the user community.

Hardware. To date we have bought six SUN SPARCstations[2] with associated disk and memory expansions, tape and CD-ROM drives, and printers. Three workstations are currently production systems. Three are being used for development of the next NADIR expansion. This hardware cost approximately $130,000, plus hardware support costs.

---

[1]Equivalent to one full-time employee, but actually may comprise two or more part-time employees.

[2]SUN SPARCstation and SUN workstation are trademarks of SUN Microsystems, Inc.

Software. Since the most expensive and limited resource is our people, we have minimized staff time by using off-the-shelf software and existing ICN audit records. These choices have reduced the need to develop new software and to modify existing auditing systems. Our primary software purchase was the Sybase relational database manager.[3] We have bought primary and secondary licenses for Sybase SQL servers, Data Workbenches, APT Workbenches, and DB Libraries. This software cost approximately $70,000, plus software support costs. Annual recurring license and maintenance costs amount to less than $1,000.

The use of Sybase has reduced our development time enormously. It provides a development interface that allows for rapid prototyping and implementation. It is flexible, handling different types of data from a large variety of sources, including different hardware and operating systems. It offers a 'point-and-click' interface, allowing administrative functions to be performed within the fast and intuitive graphical interface of the SUN workstation.

3.2 Benefit

We believe that NADIR's benefits substantially outweigh its cost. Its primary benefit has been meeting its goal of discovering suspicious users and events. We estimate that NADIR is at least ten times as effective as our previous manual efforts. This effectiveness is corroborated by two other findings. First, as far as we can determine NADIR does not miss suspicious users and events (false negatives). In four years' operation we have found no after-the-fact evidence of omissions, and have successfully detected all staged (but 'blind' to us) events by security personnel. Second, the system does not flag as suspicious an unacceptable number of ordinary users and events (false positives). Though most suspicious users turn out to be innocent of intentional wrongdoing, our security personnel have agreed with NADIR that they are worth investigating. Suspicious events that are not actual security incidents often indicate system malfunctions; an additional, unanticipated benefit.

NADIR's effectiveness is enhanced by the fact that it is not the only barrier to ICN intrusions and misuse. No single system should be. Rather, NADIR is one of several measures taken to protect our system, along with authentication and authorization systems and file protection mechanisms. To circumvent ICN security, a perpetrator would need to penetrate these other barriers *while* avoiding detection by NADIR.

NADIR has provided the following additional benefits:

- Suspicious users and events are detected much more quickly. NADIR reports are evaluated daily, so events are detected within a day, rather than

[3]Sybase, Data Workbench, APT Workbench, and DB Library are trademarks of the Sybase Corporation.

long after the fact, if at all. We plan to upgrade the system to detect events within minutes or possibly seconds of their occurrence.

- Follow-up investigations are much more timely, systematic, and complete.
- Use of the system has enhanced security awareness throughout our user community, as users see Laboratory security policy being enforced on a regular basis. We are convinced that the community's awareness of NADIR helps to deter would-be misusers.
- NADIR statistics have helped us and system managers to better understand how the ICN really works, as opposed to how it was believed to work. In many cases NADIR has helped identify system flaws and failures.
- We can respond more effectively, and with less expense, to external audits and requests for special reports.

A more general benefit is that NADIR provides the electronic equivalent to a manager's 'walking his or her space'; e.g., touring a plant facility. Most managers agree that such efforts are worthwhile, providing an opportunity to get an overall impression of current conditions, to spot and evaluate specific problems, and to talk with staff. Similarly, NADIR gives our computer security officers a summary of system operation, points out suspicious users and events, and creates an opportunity for officers to meet and talk with those users who most need guidance.

4. Privacy and Policy

4.1 General Issues

Privacy is extremely important. Our society generally accepts and constitutionally guarantees a right to privacy. However, exactly what we mean by privacy, especially for policy purposes, is unclear. Privacy involves such related concerns as autonomy, individuality, personal space, solitude, and anonymity. Monitoring people without good reason is at least socially and ethically unacceptable, and is in some cases illegal. Few people object to the presence of video cameras in banks or other businesses, or the presence of scanning devices in airports. They see such monitoring as contributing to a well-understood common good. On the other hand, there has been considerable concern about the propriety of auditing computer systems. Perhaps computer auditing systems are threatening because of the level of activity they can oversee. They can not only audit overt activity, but also can be used to measure detailed performance and evaluate personal communications. In addition, auditing user activity in the workplace is a highly emotional issue, suggesting to opponents the specter of sweat shops and slave labor.

The privacy debate centers on the right of a business to control (and defend) its corporate data and computer investment versus the right of the individual to privacy, even while using corporate resources. Many organizations, including ours, believe they have the right to audit all activity on their computer and communications systems. This is based on the belief that individual privacy rights must be weighed against the safety, security, and privacy needs of the community as a whole. It's obvious that most, if not all, individuals who comprise a community benefit when the needs of the whole group are met. Effective security, including auditing, does this because it helps *provide* privacy for most individuals, especially in vulnerable distributed electronic information systems. Audit analysis allows a few individuals to monitor selected information and thus helps protect all information from unauthorized access and misuse, benefiting both individual and corporation.

Because of user privacy rights and attendant legal consequences, every institution should have a written policy dealing with employee use of corporate communications and computational resources. The absence of a policy is an invitation to misunderstandings, and publication of the policy is essential. Quite simply, it is not fair for management to expect employees to comply with rules that are undocumented or unknown to the employee population. Unfair treatment of employees in the workplace is likely to elicit negative employee attitudes, and is inherently counterproductive to security that depends upon user cooperation and vigilance. Misunderstandings between management and employees can result in morale problems and may lead to contentious and expensive lawsuits. In contrast, explaining policy to employees will increase the chance that they will 'buy in' and assist in discovering and reporting security problems.

Management should carefully review auditing technologies and construct a sound, comprehensive policy governing the conduct of auditing activities on their systems. The policy should be brief, and should:

- Spell out what user behaviors are unacceptable.
- Clearly explain the rationale for conducting the auditing.
- State what the employees can expect in terms of privacy and confidentiality.
- Identify any activities that management will *not* deliberately audit, and give some assurance that if these items are made evident by the auditing, that management will not use them as a basis for action against the employee.
- Detail the measures that management can and will take in response to the detection of policy violations.

The policy should be announced to all affected employees, preferably with a signed acknowledgment or receipt as evidence that each employee is aware of the policy.

The policy should address all forms of electronic communications, including telephone, voice mail, and electronic mail, and treat them equitably and consistently. Without a clear policy, employees will project expectations learned from telephone usage and printed mail to voice mail and electronic mail. Differences between these media may cause confusion, or discourage employees from using newer and more efficient means of communication.

4.2 Los Alamos Policy

Privacy issues are less controversial at Los Alamos than at many other sites. Because we are a classified facility, most of our users are subject to background investigations and have accepted some loss of privacy as a condition of employment. In addition, we have a clear governmental mandate to enforce computer security. The Computer Security Act of 1987 requires each Federal agency to protect its computer resources "from the loss, misuse or unauthorized access to or modification of ... information" [6]. The DOE has responded by requiring the Laboratory to safeguard its computer resources "against theft, fraud, waste, and misuse" [7, 8]. DOE Orders state that besides appropriate administrative, technical, physical, and personnel protective measures, controls to prevent misuse and abuse should include reviews of the contents of computer system files at unannounced intervals and by means of random sampling [7]. They further state that multi-user classified systems must maintain an audit record of selected user activity that is audited by appropriate security personnel for anomalous activity "on a scheduled basis but at least weekly." As computer system Protection Index (PI)[4] levels increase, the Order requires more comprehensive auditing of system activity. For PI of 3 or greater networks (such as the ICN), the Order requires continuous, on-line analysis of audit trails, and real-time notification of any anomalies [9].

Los Alamos security managers are candid about the effect of these Orders on user privacy at Los Alamos:

> *"While using a Government owned resource, a user should have no expectation of privacy. The Department of Energy, the University of California, and Los Alamos National Laboratory have the authority and responsibility to detect and prevent misuse of Government property."[10]*

These sentiments, however, are not our formal policy on audit analysis of computer and communications information. That policy is, in full, as follows:

---

[4] A measure of perceived risk determined from the combination of the security clearance level of users and the classification level of the data on a classified automated information system.

Los Alamos National Laboratory computing systems and their associated communications networks may be used for official business only. The Laboratory is charged with preserving the integrity and confidentiality of both classified and unclassified computerized information. In addition, it must prevent fraud, waste and abuse. The Department of Energy, the University of California, and the Laboratory have the responsibility and the authority to detect and prevent misuse of Government property. Auditing is one of the necessary tools for these tasks. Thus, while using Government owned or administered computer and communication resources, a user should have no expectation of privacy, as there is legitimate need to audit any activity at any level of detail.

Audit information is considered privileged and highly sensitive and is treated as such. Users have assurance that this information will not be normally shared with their managers or coworkers; only those security personnel who have need-to-know will systematically review it. Auditing may be done routinely or randomly, manually or automatically, to provide information about legitimate and illicit computer usage. Any computerized data or communication may be monitored, including, but not limited to, audit records, computer files, and electronic mail.

When misuse of Laboratory resources is detected, Laboratory management will be notified. Response will be appropriate to the seriousness of the offense and may comprise immediate, formal disciplinary action, up to and including termination. Evidence of fraud, waste or abuse collected during audit analysis may be shared with law enforcement agencies.

While still under review for formal acceptance to the Laboratory Administrative Manual, this is our working policy.

ICN users are informed of Laboratory policy in two ways. First, to become an authorized user and obtain a system password, each individual must sign a form that contains the following statement:

"NOTE: All Laboratory computing systems, and their associated communications systems, are to be used only for official business. By completing this form and signing for the ICN Password(s), users signify their agreement not to misuse the ICN. The Computing and Communications Division and the Operational Security Safeguards Division have the responsibility and authority to periodically audit users' files."

Second, the following warning banner is displayed at the beginning of all ICN sessions on audited systems:

NOTICE

This computer system is for authorized use only. All use is subject to audit, and all use may be monitored. This computer system is operated under the auspices of the U.S. Department of Energy. Any misuse or unauthorized access is prohibited

and is subject to criminal and civil penalties. Evidence of unauthorized activity may be provided to law enforcement officials.

4.3 User Reactions

At Los Alamos, user reaction to contact by a security officer following up on a NADIR report usually varies from neutral to positive. Table 4-1 summarizes our security officers' subjective breakdown of these reactions. We attribute the relative lack of negative reactions (5%) to three elements of our security environment. First, our users are accustomed to work in a classified environment. Second, they have all been informed about our established and explicit policy and are aware of security auditing activities. Third, investigating security officers are trained to treat all interviewees with consideration and courtesy.

Table 4-1: User Reaction to Security Investigations

Percent	Reaction	Description
60	Passive	These users respond politely but do not prolong the security interview. They do not fear or question the security officer's attention. Rather, they deal with it expeditiously to minimize its demand on their time and energy.
20	Curious	These users are intrigued or flattered by the unexpected contact. They enjoy explaining their behavior and want to know more about the NADIR system.
15	Appreciative	These users are grateful for the security auditor's efforts to help them understand the system and minimize their errors. They believe that security plays an important role in protecting their work.
3	Fearful	These users regard contact by a security auditor as a possible first step toward job loss and/or criminal prosecution.
2	Antagonistic	These users view the contact as an infringement on their personal rights. They are offended by the 'big brother' implications, or view it as a waste of organizational resources (theirs and the security officer's).

5. Legal Issues

5.1 Auditing Level

In evaluating the legality of automatic auditing systems, a key concept is that of different levels of monitoring. A good way to understand this concept is by analogy to telephone monitoring. The lowest (most detailed) level of telephone monitoring is a wiretap that allows monitoring of the content of telephone conversations. In the United States, telephone conversation monitoring is severely

limited by Federal statutes [11]. Wiretapping is prohibited unless allowed by court order or under other specific conditions described in the statutes. No such restrictions apply to higher-level monitoring of telephone records, called *traffic analysis*. Yet such an analysis can be very informative: one can learn much from who calls whom, for how long, and in what sequence, even without knowing what is said.

In the domain of computer security, wiretapping is analogous to low-level *session monitoring*. This can involve auditing user-to-computer session transmissions (keystroke monitoring), or the contents of user-to-user communications (e-mail monitoring). Traffic analysis is analogous to monitoring a computer audit record containing higher-level information such as who logged onto what system, when they logged on and off, and which files they accessed. NADIR is such a system.

It has yet to be determined whether the legal system will respect this analogy: that is, whether routine (non-court-ordered) session monitoring will be treated the same as an unauthorized telephone wiretap. United States Federal wiretap statutes predate the computer revolution, and the issue has never been tested in court. Many system administrators (though not Los Alamos') are taking advantage of this current legal ambiguity to perform session monitoring. However, the United States Department of Justice cautions system administrators, as a precaution, to advise their users of all monitoring no matter what the level [12]. In particular, they suggest that a warning banner similar to ours (section 4.2) be displayed on the terminal screen each time a user logs onto a monitored system.

5.2 Chain of Evidence

A second key legal concept concerns the reliability of the evidence produced by automated audit analysis. While, to our knowledge, no such evidence has yet been used in a criminal or civil case, one can extend general rules of evidence to this specific type of evidence.

A successful audit analysis system informs security officers that a potential misuse has occurred and thus focuses their attention on the event. However, its usefulness is limited if it cannot detail the exact scope of the perpetrator's conduct so that security officers can assess the seriousness of the event. They must be able to determine whether the event requires the expenditure of further investigative resources. The system must also support the determination of damage assessments. Finally, the system must provide a sufficient 'chain of evidence' if the perpetrator is to be prosecuted.

Following an event investigation, prosecutors may submit evidence in court. This evidence must show a jury how the event was first discovered, and prove that the defendant is the perpetrator. Evidence reliability is tested twice in the legal process. First, the court must find the evidence reliable to admit it at all. For evidence to be admissible in court it must be authentic, that is, it must be what it is purported to be. Second, the jury must accept the evidence as true [13].

This means that it must be explainable and persuasive to a layman -- in our case, one who is probably computer illiterate. Throughout this process, the defense will be working actively to show the court and the jury that the evidence is not reliable. The burden of proof is on the prosecution.

In applying these general rules of evidence to the specific case of evidence produced by an automated audit analysis system, two questions must be addressed. First, how can one prove that the method the system uses to find misuse is reliable? Since all audit analysis systems do not rely on the same methodology, this must be done individually for each system. Second, how can one prove that the specific evidence, as provided by the system and maintained by the system security officer, is reliable? We reiterate that neither of these two questions has been thrashed out in court; however, we can make reasonable inferences based on common sense and on background knowledge of how other types of evidence are proven reliable.

Common sense suggests two ways of demonstrating system reliability. First, one can describe how the system works and demonstrate, through expert testimony, that its 'reasoning' is sound. If the system is well designed one should be able to make such an argument convincingly to a judge and jury. This will likely be easier for a rule-based system like NADIR than one that uses more sophisticated algorithms such as neural networks. A second means of demonstrating reliability focuses on verifiability. The prosecution must prove that, given identical data as input, the system would reach the same conclusion, as opposed to behaving unpredictably.

To demonstrate evidence reliability, it is critical that security officers and system managers document how they have gathered and protected evidence. Establishing who did what at what time is essential to a successful prosecution. If there is reason to believe that prosecution is contemplated, or for justification of employee termination, the law enforcement officials and computer security experts offer the following advice:

- Do not try to conduct your own investigation. This may prevent evidence from being used or otherwise botch the investigation.

- Note the time and context of every contact with investigators or law enforcement agents.

- Keep a handwritten log of security events and during the process of gathering and preparing evidence. This log should record the facts of an event; it should not draw any conclusions. It should contain the date and time of each event. The log should be dated *and signed* on each page.

- Keep copies of all files accessed or changed by the perpetrator.

- Keep all evidence relating to an event in a secure place such as a locked safe or cabinet. It is essential to prove evidence has not been tampered with, from the time it was collected until presentation at trial. This includes the event log and all pertinent computer listings or other media.

- Be prepared to help investigators and prosecutors, since they will probably not know either the technology or the specific system.

6. Conclusion: Technology and Policy

An idealistic model of system development supposes that management specifies the important issues and sets relevant policies before authorizing the development of any significant system. In the real world, of course, this process often works the other way around. As a technology is developed and implemented, its developers become aware of the relevant issues and bring them to the attention of management so that policy can be formulated. These issues may have been previously acknowledged but not acted on. In the case of a truly new technology, the development process may create new issues that must be understood and dealt with for the first time.

The case of automated audit analysis is clearly one of technological development driving policy, rather than the other way around. Researchers in educational, governmental, and industrial settings have been developing a variety of such systems for several years [14, 15, 16, 17]. As systems approach a critical level of feasibility, the security community has been forced into awareness of the several issues discussed in this paper, with the privacy and legal issues getting the most attention.

This pattern holds for Los Alamos National Laboratory's experience with automated audit analysis. We began developing NADIR in response to DOE security requirements; our simple goal was to detect misuse. During the development process, the issues we dealt with were purely technical. Most of the management issues discussed in this paper became evident only after the NADIR system was already implemented. As we began using the system we quickly realized that automated audit analysis raised privacy problems that cursory manual review did not. We developed an informal working policy for maintaining user privacy, and began reading papers and attending conferences on this subject.

The importance and general interest of this and other issues was brought home to us when a NADIR team member giving a technical talk on the system at a European security conference was besieged with questions about cost-benefit analysis, user reactions, privacy, etc. When we embarked on this paper, partly in response to those questions, additional issues arose for the first time. We found, for example, that while the Laboratory's Computer and Communications Security Group has developed a written automated audit analysis policy, it has yet to complete the approval process required for incorporation into the Laboratory's Administrative Manual. We also have not yet instituted all the pro-

cedures we have recommended here for safeguarding the chain of evidence. In the meantime we have taken a conservative approach to these issues, verifying that what we have implemented does fall within the established practices and (sometimes unwritten) policy of the Laboratory.

We hope that our heightened sensitivity to these management issues will soon help to bring our actual policy and procedures in line with the ideal. Once an appropriate policy is in place, it should be relatively simple to keep technology and policy in step with each other as we continue to improve our system. We hope that our experience will assist other institutions as they, too, wrestle with these issues.

Acknowledgments

We are indebted to many participants of the *Future Directions in Computer Misuse and Anomaly Detection* workshops (1992-93) for their assistance in clarifying some of the topics covered in this paper. In particular, the privacy and legal issues explored in Sections 4 and 5 greatly benefited from discussions at these workshops. We are especially beholden to Scot Charney (Chief, Computer Crime Unit, General Litigation and Legal Advice Section, Department of Justice), Fred Smith (Attorney and former New Mexico Attorney General), Jim Koloueh (FBI), Gene Spafford (Purdue University), and John Smith (Investigator with the Santa Clara CA District Attorney's office). We thank the members of the Computer and Communications Group, Operational Security & Safeguards Division, especially Charlene Douglass, who contributed to the formulation of an audit analysis policy. We appreciate the time Alex Marusak took to review this paper, and we are grateful for his comments on legal and privacy issues.

References

[1] C. Stoll, *The Cuckoo's Egg,* (New York, Doubleday, 1989)

[2] J. Maglitta and J. P. Mello. *The Enemy Within* (Computerworld, December 7, 1992)

[3] J. Hochberg, K. Jackson, J. McClary, D. Simmonds, *Addressing the Insider Threat* (Proceedings of the 1993 United States Department of Energy Computer Security Group Conference, May 1993, LA-UR-93-1181)

[4] K. Jackson, D. DuBois, and C. Stallings. *An Expert System Application for Network Intrusion Detection* (Proceedings of the 14th National Computer Security Conference, October 1991, LA-UR-91-558)

[5] J. Hochberg, K. Jackson, C. Stallings, J. McClary, D. DuBois, J. Ford, *NADIR: An Automated System for Detecting Network Intrusion and Misuse* (Computers and Security, Elsevier Science Publishers Ltd., Volume 12, Number 3, May 1993, LA-UR-93-137).

[6] *Computer Security Act of 1987* (U.S. Public Law No. 100-235, 40 U.S.C. 759)

[7] *Unclassified Automated Information System Security Program* (Department of Energy Order 1360.2B, Office of Administration and Management, April 1992).

[8] *Classified Automated Information System Security Program* (Department of Energy Order 5639.6A, Draft, Office of Administration and Management, April 1993)

[9] *Security Requirements for the Classified Automated Information System Security Program* (Department of Energy Manual 5639.6A-1, Draft, Office of Administration and Management, April 1993)

[10] Charlene Douglass, Group Leader, Computer and Communications Security Group, Operational Security & Safeguards Division, Los Alamos National Laboratory (Personal communication, June 1993)

[11] *Federal Wiretap Statutes* (18 U.S.C. 2510 *et sequens*)

[12] Robert S. Mueller, Assistant Attorney General, Criminal Division, United States Department of Justice, (Memo to James H. Burrows, Director of the Computer Systems Laboratory, National Institute of Standards & Technology, United States Department of Commerce, October 1992)

[13] S. Charney, *The Role of Intrusion Detection Systems in the Investigation and Prosecution of Computer Crime Cases* (Proceedings of the workshop on Future Directions in Computer Misuse and Anomaly Detection, University of California, Davis, April 1992)

[14] S. Snapp, J. Brentano, G. Dias, T. Goan, L. Heberlein, C. Ho, K. Levitt, B. Mukherjee, S. Smaha, T. Grance, D. Teal, and D. Mansur. *DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and Early Prototype* (Proceedings of the 14th National Computer Security Conference, October 1991)

[15] T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, C. Jalali, H. Javitz, A. Valdez, P. Neumann, and T. Garvey, *A Real-Time Intrusion Detection Expert System (IDES), Final Technical Report* (Technical report, Computer Science Laboratory, SRI International, Menlo Park, CA, February 1992)

[16] L. Heberlein, B. Mukherjee, and K. Levitt. *Internetwork Security Monitor: An Intrusion Detection System for Large-Scale Networks* (Proceedings of the 15th National Computer Security Conference, October 1992)

[17] S. Smaha. *Tools for Misuse Detection* (Proceedings of the ISSA '93 National Conference, April 1993)

DATE
FILMED
5/2/94

END