LA-UR -91-558

LA-UR--91-558

DE91 008590

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405 ENG 36

TITLE AN EXPERT SYSTEM APPLICATIONS FOR NETWORK INTRUSION DETECTION

AUTHOR(S) KATHLEEN A. JACKSON
DAVID H. DUBOIS
CATHY A. STALLINGS

SUBMITTED TO 14TH NATIONAL COMPUTER SECURITY CONFERENCE

DISCLAIMER

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

An Expert System Application for Network Intrusion Detection*

(Computer Security Activities - Intrusion Detection, Expert System, Application, Prototype Development)

Kathleen A. Jackson (505) 667-5927, kaj@lanl.gov

David H. DuBois (505) 667-1732, dhd@lanl.gov

Cathy A. Stallings (505) 667-2804, cxxs@lanl.gov

Computer Network Engineering Group (C-5), MS B255
Computing and Communications Division
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

POC: Kathleen A. Jackson

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

An Expert System Application for Network Intrusion Detection

Abstract - This paper describes the design of a prototype intrusion detection system for the Los Alamos National Laboratory's Integrated Computing Network (ICN). The Network Anomaly Detection and Intrusion Reporter (NADIR) differs in one respect from most intrusion detection systems. It tries to address the intrusion detection problem on a network, as opposed to a single operating system. NADIR design intent was to copy and improve the audit record review activities normally done by security auditors. We wished to replace the manual review of audit logs with a near realtime[1] expert system. NADIR compares network activity, as summarized in user profiles, against expert rules that define network security policy, improper or suspicious network activities, and normal network and user activity. When it detects deviant (anomalous) behavior, NADIR alerts operators in near realtime, and provides tools to aid in the investigation of the anomalous event.

1 Introduction

The authentication and access control system in any network is the first defense against intruders from outside. Authentication is the identification of a user with reasonable assurance that the user is who he or she claims to be. Access control is a mechanism of restricting access by authenticated users to those parts of the network consistent with their clearance and need-to-know. It is obvious, given the industry-wide frequency of break-ins by outsiders that authentication and access control mechanisms can be compromised or bypassed. They alone cannot supply assurance against penetration by outsiders. Also, outside "hackers" are not he only source of security problems. Far more often they are a result of abuse by the privileged insider. Even the most secure system is vulnerable to abuse by insiders who misuse or try to misuse their privilege. This is obvious from well publicized reports in the last few years of incidences of unauthorized access and removal of classified information by insiders from otherwise secure computer systems.

In a large, complex, and rapidly changing computer network such as the ICN it is not realistic to expect to identify all security loopholes and vulnerabilities. Even if identified, it is not a given that they can be closed, since it may be impossible or impractical to do so. A primary reason for this is the need to strike a balance between security and the provision of convenient services to network users. Given the acknowledged doubt in the completeness of current security measures, we must supply some means to provide a reasonable assurance that the network is secure.

An auxiliary line of defense against both intrusions by outsiders and insider misuse is the maintenance and review of an audit record of important network activity. Attempts at audit data review result in security auditors wading through huge quantities of printed output in an ineffective attempt to spot invalid activity. The sheer volume of data makes it nearly impossible to detect suspicious activity that does not conform to a few obvious intrusion or misuse scenarios. Even these may be missed. To make this approach effective, the auditors need the capability for automated security analysis of the audit record. This capability combines the knowledge of security experts with a computer's capability to process and correlate large quantities of data. When done in near realtime, security personnel can be notified of suspicious activity quickly, and direct action taken to trace and stop an identified penetration attempt or other misuse.

2 Target System

The Integrated Computing Network (ICN) is Los Alamos National Laboratory's main computer network. It includes host computers, file storage devices, network services, local and remote terminals, and data communication interfaces. The core of the ICN includes the main host super-computers and their support devices. Through the ICN, any user inside the Laboratory may access any host computer (with authorization to do so and use of an approved access path) from office workstations or terminals. Outside users typically access the ICN through telephone modems, leased lines, or one of multiple world-wide networks. The core ICN has more than 8,000 validated users.

The ICN consists of a unique arrangement of four "partitions," in which resources are dedicated to specific levels of processing. Each partition limits access to only those users cleared for the most sensitive information processed in the partition. A system of dedicated, special function, ICN nodes enforce partitioning throughout the network. These nodes perform specific services in the ICN, such as user authentication, access control, job scheduling, file

[1] For our purposes, we define a near realtime application as one that responds to data or user input in one to 30 seconds.

access and storage, and file movement between partitions. They are physically protected, have tightly restricted access, run only that software needed to perform a specific service, and do not execute user programs. Only these dedicated nodes may service multiple ICN partitions. Each of these nodes must produce and maintain an audit record of its activity.

3 Overview

Until recently, security auditors manually reviewed ICN audit records to identify potential security violations. Given the size of the audit records, manual review was limited to a small sampling or a cursory scanning. The auditors found many security violations, but there was no way to evaluate the general success or completeness of their effort. Also, the Laboratory's Internal Security (ISEC) office often requests audits that cover weeks of audit data from months or years in the past. As there was no automated way to do these audits, considerable effort was expended in completing them. It was for these reasons that development of an automatic audit record analysis, or intrusion detection, system was undertaken at Los Alamos.

The early research of Dorothy Denning and her colleagues, and the IDES research and development at SRI International, has heavily influenced intrusion detection development at Los Alamos. Denning proposed monitoring standard operations on a target system for deviations in usage. Her early research tried to define the activities and statistical measures best suited to do this [1, 3], and continued with the development of an IDES prototype [4]. Teresa Lunt and her colleagues continue this research with the development of the IDES system [5, 6, 9, 13]. They have expanded the idea by adding an expert system component that addresses known or suspected security flaws in the target system. This research has served to demonstrate two things. First, that statistical analysis of computer system activities provides a characterization of "normal" system and user behavior, and that activity deviating beyond normal bounds is detectable. Second, that known intrusion scenarios, exploitation of known system vulnerabilities, and violations of a system's security policy are detectable through use of an expert system rule base. The IDES approach puts a primary emphasis on the statistical detection of deviations from normal user and system behavior. This is combined with an expert system that is intended to catch those invalid activities missed by the first means [10].

Several intrusion detection systems have in recent years adapted the Denning model to their particular problem [7, 8, 11]. However, where the Denning model and most intrusion detection systems target specific operating systems, our effort addresses a *network* connecting many host systems, but not the hosts themselves [15]. Where Denning addressed the standard operations on a specific operating system (system logons, program executions, file and device accesses) we wished to address the standard operations on our network. The problems are similar in many respects, but with some important differences. While the ICN contains many standard functions such as those found on an operating system (authentication, access control, file access and storage, job control), these functions are distributed across the network. Also, the ICN implements a *distributed* multi-level secure system (the system of partitions and the controls over them), that must be monitored closely by any intrusion detection system. Nonetheless, if we view the ICN as one large distributed operating system, then the Denning model applies well to the problem of network intrusion detection.

Current network intrusion detection efforts have taken one of two approaches. One approach is to target network traffic at the service and protocol levels [12]. The second approach collects data from separate hosts on a network, for processing by a centralized intrusion detection system [14]. Although NADIR does not capture network traffic, it targets service level activity by targeting the nodes that handle and log standard ICN service operations. We decided to target the service nodes because of their critical nature, to keep the quantity of data to be processed at a manageable level, and because their audit record is sufficient to support an effective intrusion detection system.

4 Working Prototype

Once we decided to apply intrusion detection to the ICN service nodes, we adopted a set of basic technical goals. These goals support development of a flexible system that we could easily expand to multiple target systems. We decided to limit the audit record to that currently supplied by the target systems and keep target system changes to a minimum, to avoid degradation of target system performance. Also, because the ICN is a large, long-established network that has changed constantly over the last fifteen or so years, we had to take the following peculiarities into account:

- The Los Alamos developed network protocols are non-standard, so are not compatible with off the-shelf software.

- The ICN service nodes comprise several different hardware configurations, that run a variety of operating systems.
- The software on most service nodes has been subject to many changes and upgrades, and is programmed in several different languages.
- While each service node must maintain an audit record of its activity, the format and content of the audited data differ greatly from system to system.

We designed NADIR for easy expansion to these various multiple target systems, mainly by three design choices. First, to use dedicated workstations for intrusion detection processing. Second, to use flexible off-the-shelf interface and database software, that supports data translation between different operating systems and enables the merging of data into a single extended database. Third, to limit required target system changes to the capability to collect the proper audit record of user activity, transform the data into a specified canonical format, and transmit it to NADIR. Also, we designed NADIR software in a modular fashion, so that new target system expansions can be handled with a minimum of effort.

NADIR is to be implemented on a set of dedicated workstations, each of which will receive and correlate data from the target systems. As we add more target systems to NADIR, we plan a network of workstations, each contributing to a distributed database. This approach also minimizes the impact on target system performance, enable the collection of data from multiple diverse systems, and provides for maximum security. Ethernets will connect the workstations to the target systems and to each other, and we will implement a standard network protocol.

The NADIR prototype consists of one workstation, a SUN SPARCstation[2] with two 327 MByte disks. It uses the Sybase[3] relational database management system and a Los Alamos designed expert system. Sybase provides tools used to structure, maintain, and display all data on the system. The expert system is programmed almost entirely in Transact-SQL, an enhanced version of the SQL database language supplied by Sybase. Transact-SQL provides such capabilities as stored procedures, triggers, system administrator tools, and control flow language features, used extensively in NADIR. Also, we use C for a part of the user interface. NADIR communicates with each target system over a dedicated secure ethernet link.

NADIR monitors Network Security Controller (NSC)[4] and Security Assurance Machine (SAM)[5] activity on the ICN. The NSC is a DEC-8250[6] machine, which runs the VMS operating system. The SAM is a DEC-730 machine, which runs the UNIX[7] operating system. The changes called for on each system were minimal. Communication with NADIR by a target system calls for only the installation of Sybase supplied interface software, and the use of a standard DECnet or TCP/IP protocol. DB-Library packages for Fortran and C provide the interface to Sybase. The Multinet[8] software package provides an implementation of TCP/IP under VMS. We changed the target system code as little as possible. The target system must only format the audit record for NADIR and transmit it immediately after its occurrence. NADIR required data processing has not resulted in any measurable degradation in system performance on either system.

5 System Design

We are applying NADIR to the ICN service nodes in a sequence of planned phases. Each phase includes analyzing a node individually, processing its data separately, then integrating it into the NADIR system. As we add new nodes to NADIR, we correlate their user activity record with earlier included nodes to produce more complete profiles of ICN activity. Eventually, this will allow the tracking of users from the time they enter the ICN, until they leave the network. With the addition of each node, we define new expert rules that use the expanded information available. The rules describe more elaborate scenarios of invalid or suspicious user activity, and will, over time, improve the discrimination and judgement of the system. We have integrated the NSC and the SAM into NADIR. Work is in progress to integrate the Common File System (CFS)[9] and the Facility for Operator Control and User Statistics (FOCUS)[10].

The NADIR system has six functional components; Data Collection, Data Processing, Anomaly Detec-

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

[3] Sybase, Transact-SQL, and DB-Library are trademarks of Sybase Corporation

[4] The NSC is a dedicated, single function computer through which all ICN user authentications must pass.

[5] The SAM controls and audits the down partitioning of unclassified files between partitions in the Common File System (CFS)

[6] DECnet, VMS, DEC 8250, and DEC 730 are trademarks of Digital Equipment Corporation

[7] UNIX is a trademark AT&T Bell Laboratories

[8] Multinet is a trademark of TGV, Inc

[9] The CFS is a large, centralized file management and storage system that provides long term file storage in all ICN partitions for ICN users

[10] FOCUS provides operations control, batch job scheduling, and accounting control for the ICN

tion, Report Generation, Event Assessment, and the User Interface. Figure 1 illustrates their relationship to each other.

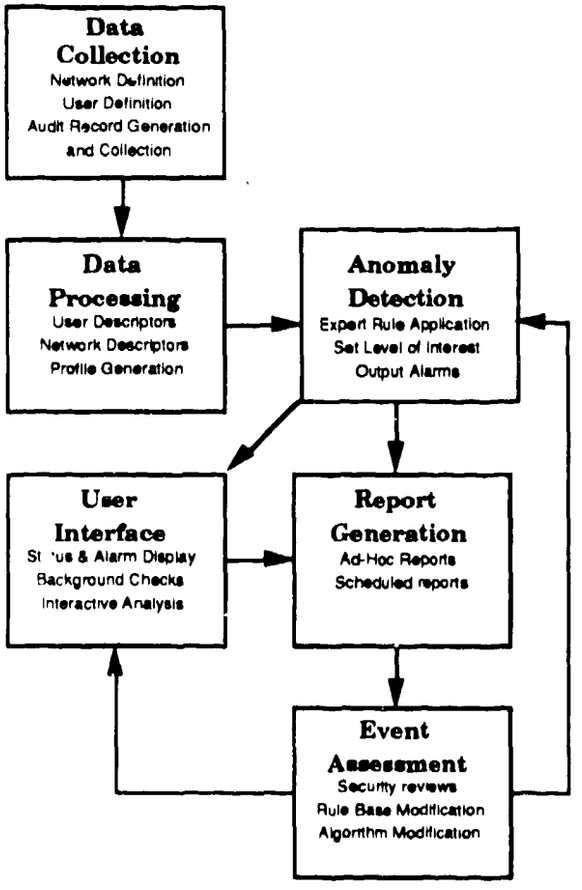

Figure 1: NADIR System Model

5.1 Data Collection

NADIR monitors target system activity as it happens. Each audit record describes a single event. Audit records from different target systems vary in format and contain mostly unique data, a result of the functionally different tasks done by those systems. Whatever the system, the audit record will contain a unique ID for the ICN user, the date and time of the user's activity, fields that describe the activity, and any errors that might have occurred.

5.2 Data Processing

NADIR summarizes all user and system activities, as represented by audit records from the target systems, into statistical profiles. These profiles are a description of current behavior in a set of defined parameters. NADIR maintains profiles for both separate ICN users and for a composite or total of all ICN users. They contain measures (count statistics) that summarize user activity. These measures keep a record of the occurrences of a particular event during a specified time. NADIR updates the profiles when it receives an audit record. It parses the data from each audit record and increments the proper measures in the profiles. NADIR maintains past profiles for comparison purposes and as a permanent record.

5.3 Anomaly Detection

Events are actions that may be measured in some way. NADIR finds them in either the contents of a single input audit record or from an examination of the user profiles. Single audit records define an event when any of the data fields in the record match a specified pattern. Events detected in the profiles represent activity that is spread across multiple audit records. They define an event when the profile measures match a specified pattern. NADIR compares proper and expected activity to observed events within either the audit record or the profiles. It does this through the application of expert rules, and identifies deviations[12]. NADIR assigns each deviant event (or anomaly) a Level-of-Interest[13]. It bases the Level-of-Interest on the number and type of rule that the user's behavior has fired. NADIR applies the Level-of-Interest to each unique user, host system, or entry point into the network. Every fired rule increases the Level-of-Interest, though the firing of one critical rule may be enough to bring immediate attention to the event. The current security status for each user and system is provided in the combination of Level-of-Interest and record of fired events.

5.4 Report Generation

NADIR generates anomaly reports from deviant events. The frequency of reports is dependent on the Level-of-Interest associated with each event. All events are documented in routine weekly reports. Those events determined to be very interesting, but not critical, are output in daily reports. Very suspicious events of a critical nature, such as a probable attack under way, are output immediately. NADIR generates detailed follow-up reports as part of any investigation.

[12] The identification of a deviation by an expert rule is generally referred to as having "fired" or "triggered" the rule.

[13] The Level of Interest is the calculated seriousness of an event.

5.5 Event Assessment

Upon receipt of a NADIR report, whether critical or routine, security auditors review all anomalous activity. To process anomaly reports quickly, specific auditors investigate certain categories or types of ICN users. They review each anomalous user in detail, and decide whether to investigate further. This may include interviewing the user. If the user's activity warrants it, the user is blacklisted[14] during the investigation. The auditors file a short report at the completion of each investigation, giving details of its resolution. They supply this information to us, so we may have immediate feedback on system performance. The auditors hold periodic reviews to evaluate NADIR effectiveness and to make recommendations for improvements. We use their feedback to change the expert rules on NADIR and improve the discrimination and judgement of the system.

5.6 User Interface

The user interface uses Sybase front end tools, graphics packages, and Los Alamos designed routines to provide a preliminary interface for the knowledgeable user. It provides warnings, alarms, and status displays. For users who have the proper access and privilege, the user interface allows a choice of built-in queries or allows ad-hoc queries against the raw audit data, the separate user and composite profiles, and status information. Data may be displayed in a variety of ways, including graphically, and reports generated. Security personnel at Los Alamos often have the need to do background reviews of user activity on the ICN. NADIR provides tools for interactive background analysis of current and past activity. It maintains indefinitely the audit data needed for this activity.

6 Expert Rules

An expert rule base has separate reasoning rules encoded in a condition-action form (if-then-else statements in the old days), that provide the criteria for end determination. The rules watch for unusual separate events and attempt to evaluate the meaning of a group or series of events. NADIR expert rules, whether they are rules that enforce security policy or result from a statistical determination of normal behavior, define an expected standard of behavior for all users.

[14] A blacklisted user is denied access to the ICN by the NSC. Removal of the blacklist requires the prior approval of security personnel.

The NADIR rule base includes four logical filters; each designed to separate out certain types or levels of anomalous activities. Following a knowledge engineering approach successfully implemented at Textronic [2], the rule base definition started with the abstraction of the well-understood part of the problem. This included ICN security policy and well-defined invalid and suspicious behavior, which resulted in rules for the Characteristic Filter. Report requirements supplied rules for the Report Filter. From there evolved further refinements, implemented in the Misuse and Attack Filters. These rules involve heuristic associations that sometimes make intuitive leaps not always explicitly justified. NADIR activates the rule base filters in stages, as illustrated in Figure 2.

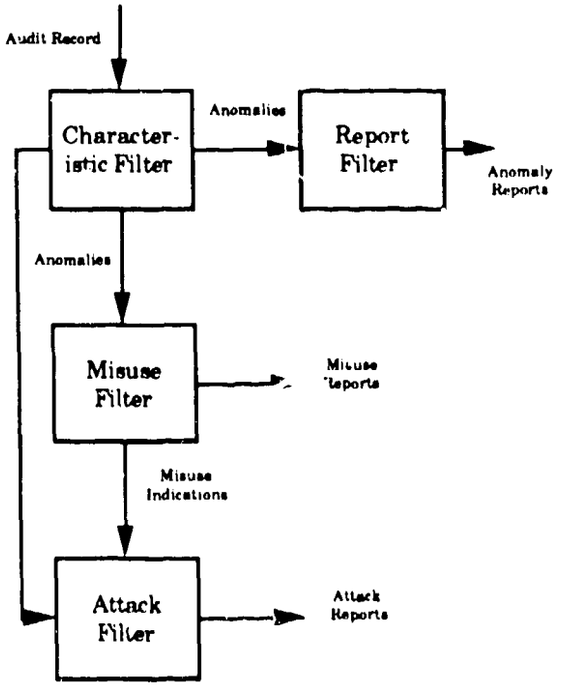

Figure 2: NADIR Rule Base Structure

• *Characteristic Filter* - applies rules that are straightforward descriptions of simple activities; each serving to distinguish a separate feature of anomalous behavior. NADIR applies these rules individually; it does not correlate one with another. It assigns a Level-of-Interest to each anomaly defined by these rules. This Level-of-Interest, as applied to each user or system, is incremental; with each rule fired it increases by a specified amount.

• *Report Filter* - applies rules to the anomalies output by the Characteristic Filter, to produce appropriate reports of anomalous behavior.

• *Misuse Filter* - applies rules to the anomalies identified by the Characteristic Filter. These rules try to identify patterns of anomalous activity that have a good chance of being systematic misuse. They specify what action to take when fired, such as the output of warning messages.

• *Attack Filter* - applies rules that try to correlate the recorded Characteristic anomalies and Misuse Indications with various Attack Scenarios. Attack Scenarios identify patterns of anomalous activity that have a good chance of being attacks on the system. They specify what action to take when fired, such as the output of alarm messages.

6.1 Characteristic Rules

NADIR applies Characteristic rules to either the input audit record or to profile data. As it finds each anomaly, it either generates or updates the Anomaly Record, whichever is appropriate. The Anomaly Record includes a Level-of-Interest for the involved user or system, and an indication of the fired rule. Characteristic rules fall into three basic categories:

1. Security Policy

These rules are the implementation of ICN security policy. They result from interviews with security personnel and documentation reviews. They detect and immediately report potential or certain security violations. An example of a security violation rule:

IF NADIR has detected an "Improper Location" error,
  AND the terminal used is in the Open Partition,
  AND the password used is classified,
THEN update the Anomaly Record, and assign the user a high Level-of-Interest,
EXPLANATION: Use of a classified password from an unprotected terminal is reason enough to consider the password compromised. The password will be immediately invalidated.

2. Individual Anomaly

NADIR applies these rules to separate user profiles, to detect when a user's behavior departs from that which is normal and valid ICN user behavior. They result from statistical analysis of the past behavior of ICN users, and interviews with security personnel. An example of an individual anomaly rule:

IF the Failure Ratio[15] of a user is >n1,
  AND the user has logged on >n2 and ≤n3 times,
THEN update the Anomaly Record, and assign the user a proper Level-of-Interest,
EXPLANATION: If a user has logged onto the ICN at least n2 times then the user is not new to the ICN. Since the average ICN user has a Failure Ratio that is much less than n1, then a Failure Ratio of n1 is significant. NADIR applies a sliding scale of concern, balanced between the total number of logons and the Failure Ratio, to this rule.

3. Composite Anomaly

NADIR applies these rules to composite user profiles, to detect when that activity departs from that which is normal and valid for the system. They result from statistical analysis of the past behavior of the composite of ICN users. An example of a composite anomaly rule:

IF "Unknown User" errors are >n3/hour, **OR** >n4/day, **OR** >n5/week,
THEN update the Anomaly Record, and assign the system a proper Level-of-Interest,
EXPLANATION: The normal number of attempted authentications that contain a user number that is not valid for the ICN is statistically very consistent. Extreme variations from this expected activity could be a sign of a break-in attempt. NADIR applies a sliding scale of concern to this rule, that depends on the variation from normal.

6.2 Report Rules

These rules do periodic checks of anomalous user activity levels, and define what reports to generate after specific intervals. Designated report intervals may be daily, weekly, or any other period. They analyze the Anomaly Record for the indicated interval, and generate reports that summarize and detail anomalous activity.

6.3 Misuse Indication Rules

NADIR fires these rules when it receives a sequence or combination of Characteristic anomalies that have a low chance of happening. They suggest possible serious misuse of the network. They do not try to define anything as specific as an attack, but their firing shows something is seriously amiss. The fol

[15] Failure Ratio = $\frac{\text{Invalid Logons}}{\text{Successful Logons + Invalid Logons}}$

lowing simplified Misuse Indication rule examines overall ICN user activity:

IF the Level-of-Interest for >n6 ICN users is >0,
  OR the Level-of-Interest for >n7 ICN users is >x,
  OR the Level-of-Interest for >n8 ICN users is >x + x/2,
  OR the Level-of-Interest for >n9 ICN users is >2x,
THEN output an immediate report, that includes an urgent warning message to the user interface.
EXPLANATION: The number of ICN users who reach a particular Level-of-Interest is statistically very consistent. Extreme variations from the normal level of anomalous activity could be a sign of some type of organized misuse of the network. NADIR applies a sliding scale of concern to this rule, that depends on the users involved and their Level-of-Interest.

The following simplified Misuse Indication rule examines the Anomaly Record of a separate user:

IF Characteristic rule 003 is set,
(a separate user has many logons this week)
  AND Characteristic rule 056 is set,
  (the user has an unusual distribution of logon tries during the swing and weekend shifts),
  AND Characteristic rule 053 is set,
  (the user has only unsuccessful ICN logon tries during the night shift),
  AND Characteristic rule 043 is set,
  (the user has an unusual distribution of unsuccessful logon tries on the weekend),
  AND Characteristic rules 040, 041, 044, 45, 046, and 047 are not set,
  (the user does not show a like pattern of failures during the day shift or on weekdays),
THEN output an immediate report, that includes a message to the user interface.
EXPLANATION: The fired Characteristic rules show a greater than normal usage of the ICN, combined with abnormal usage during off hours. Also, the user has had an abnormal number of failures during off hours without showing a like pattern of failure during normal working hours. This could be a try at masquerading, and is quite suspicious.

6.4 Attack Scenario Rules

These rules may define one Characteristic anomaly or Misuse Indication, or a combination of these, that have a low chance of happening. They suggest a known or postulated attack. It is the sequence and combination of these rules that make for an increasing certainty that an attack may be proceeding. Attacks are events that could lead to the compromise or bypass of authentication and access control mechanisms, destruction or compromise of data, or denial of service. Attack Scenario rules are in the definition stage for NADIR.

7 Results

The NADIR working prototype has been in operation since June of 1990. During this time NADIR identified and aided in the investigation of invalid activity by unknown users, and in the investigation of many cases of misuse or suspicious behavior by insiders. It has helped identify unanticipated network vulnerabilities, that have been remedied where possible or are being closely monitored. NADIR development has resulted in the identification of unanticipated misuse conditions, that have led to the definition of new expert rules. Finally, NADIR has supported background analyses during investigations of several current and past ICN users.

NADIR has also supplied unanticipated network management benefits. It has enabled us to detect hardware and software problems with some nodes of our network. It has also supplied detailed, statistical reports of network activity that were useful in such areas as accounting and network planning.

8 Future Directions

Future targets will be other network service nodes that control file access, storage, and movement, and operations control. We will develop a network of SUN workstations, each processing the audit record of multiple nodes, distributing the functional applications and database, and optimizing performance. Anomaly and event notice now consists of terminal messages and periodic reports. For serious security events, the ultimate goal is to give notice on a near realtime basis. Some kinds of invalid user activity, if allowed to continue, could lead to break-ins or denial of service to legitimate users. As a result, another goal is the notification of the proper ICN node of extremely suspicious activity, and the development of effective responses by that node. This would consist of taking direct action to stop an identified penetration attempt. The node's actions must be proportional to the extent that the monitored activity has deviated from valid behavior, what damage could result from allowing an invalid activity to continue, and denial of service considerations. We have not determined the criteria for such a response. Lastly, we would like to identify and use a rigorous method by which to validate and verify the performance,

consistency, and completeness of the NADIR expert rule base.

9 Summary

NADIR shows the feasibility of the automation of security auditing on a distributed environment such as the ICN, and the benefits of applying an expert system to the problem. It shows the benefits of a phased approach to applying intrusion detection in a distributed environment. The working prototype is a start to a longer-range goal of expanding the system to more ICN nodes, and correlating their information to produce complete profiles of user activity on the ICN.

10 Acknowledgments

We wish to acknowledge the contributions of Jimmy McClary, who introduced us to the basic ideas, organized our funding, contributed enormously to our expert rule base, and supported us throughout the project. Valuable contributions to our rule base were made by members of the Operational Security Division. We are indebted to Harry Martz for his knowledge of statistics, and to Steve Ruud and Dorothy Merrigan for their contributions to the implementation of the NADIR system.

11 References

[1] D. Denning and P. Neumann. *Requirements and Model for IDES - A Real-Time Intrusion Detection Expert System, Final Report* (Computer Science Laboratory, SRI International, August 1985).

[2] M. Freiling, J. Alexander, S. Messick, S. Rehfuss, S. Shulman. *Starting a Knowledge Engineering Project: A Step-by-Step Approach* (The AI Magazine, Fall 1985).

[3] D. Denning. *An Intrusion Detection Model* (IEEE Proceedings, 118-131, April 1986)

[4] D. Denning, D. Edwards, R. Jagannathan, T. Lunt, P. Neumann. *A Prototype IDES: A Real-Time Intrusion Detection Expert System* (Computer Science Laboratory, SRI International, August 1987).

[5] T. Lunt and R. Jagannathan. *A Prototype Real-Time Intrusion-Detection Expert System* (Proceedings of the IEEE Symposium on Security and Privacy, April 1988).

[6] T. Lunt, R. Jagannathan, R. Lee, S. Listgarten, D. Edwards, P. Neumann, H. Javitz, A. Valdes. *IDES: The Enhanced Prototype A Real-Time Intrusion Detection Expert System* (SRI International, October 1988).

[7] M. Sebring, E. Shellhouse, M. Hanna, R. Whitehurst. *Expert Systems in Intrusion Detection: A Case Study* (Proceedings of the 11th National Computer Security Conference, October 1988).

[8] L. Halme and B. Kahn. *Building a Security Monitor with Adaptive User Work Profiles* (Proceedings of the 11th National Computer Security Conference, October 1988).

[9] T. Lunt. *Real-Time Intrusion Detection* (Proceedings of COMPCON, Spring1989).

[10] T. Lunt, R. Jagannathan, R. Lee, A. Whitehurst. *Knowledge-Based Intrusion Detection* (Proceedings of the 1989 AI Systems in Government Conference, March 1989).

[11] G. Tsudik and R. Summers. *AudES - An Expert System for Security Auditing* (Proceedings of AAAI Conference on Innovative Applications in AI, May 1990).

[12] L. Heberlein, G. Dias, K. Levitt, B. Mukherjee, J. Wood, and D. Wolber. *A Network Security Monitor* (Proceedings of the IEEE Symposium on Research in Security and Privacy, May 1990).

[13] T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. Neuman, C. Jalali. *IDES: A Progress Report* (Proceedings of the 6th Annual Computer Security Applications Conference, December 1990).

[14] J. Winkler. *A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks* (Proceeding of the13th National Computer Security Conference, October 1990).

[15] K. Jackson, D. DuBois, and C. Stallings. *A Phased Approach to Network Intrusion Detection* (Proceedings of the DOE Computer Security Group Conference, May 1991, LA-UR-91-334).