LA-UR -91-334

LA-UR--91-334

DE91 007481

TITLE A PHASED APPROACH TO NETWORK INTRUSION DETECTION

AUTHOR(S) K. A. Jackson, D. H. DuBois, and C. A. Stallings, C-5

SUBMITTED TO DOE Computer Security Group Conf.,
Concord, CA
May 7-9, 1991

DISCLAIMER

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

A Phased Approach to Network Intrusion Detection

Kathleen A. Jackson, David H. DuBois, Cathy A. Stallings

Computer Network Engineering Group
Computing and Communications Division
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

Abstract - This paper describes the design and development of a prototype intrusion detection system for the Los Alamos National Laboratory's Integrated Computing Network (ICN)*. The development of this system is based on three basic assumptions: 1) that statistical analysis of computer system and user activities may be used to characterize normal system and user behavior, and that given the resulting statistical profiles, behavior which deviates beyond certain bounds can be detected, 2) that expert system techniques can be applied to security auditing and intrusion detection, and 3) that successful intrusion detection may take place while monitoring a limited set of network activities. The Network Anomaly Detection and Intrusion Reporter (NADIR) design intent was to duplicate and improve the audit record review activities which had previously been undertaken by security personnel, to replace the manual review of audit logs with a near realtime[1] expert system.

1 Introduction

The authentication and access control system in any network is the initial 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 portions of the network consistent with their clearance and need-to-know. Given the industry-wide frequency of break-ins by outsiders, it is unfortunately obvious that authentication and access control mechanisms can be compromised or bypassed and that they alone cannot be completely relied upon to ensure that no penetration by outsiders occurs. In addition, security problems are caused not only by the proverbial outside "hacker", but far more often by the privileged insider who abuses that privilege. That even the most secure systems are vulnerable to abuse by insiders who misuse or attempt to misuse their privileges is obvious from the number of 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 that all security loopholes and vulnerabilities will be identified. 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 that a balance must be struck between security and the requirement that reasonably convenient services be provided to network users. Given the acknowledged uncertainty in the completeness of current security measures, some means must be provided to monitor known loopholes, watch for activity which may lead to the identification of previously unknown security problems, and help provide a reasonable assurance that a 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 significant network activity. In the absence of an automated system, security personnel must attempt to review huge quantities of printed output in an often futile 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, and even these may be missed. What is needed is the capability for automated security analysis of the audit record; a capability which combines the knowledge of security experts with a computer's capability to process and correlate large quantities of data. When this analysis is done in near realtime, security personnel may be notified of suspicious activity in a timely manner, and direct action taken to trace and stop an identified penetration attempt or other misuse.

*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 on behalf of the United States Department of Energy.

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

2 Target System

The Integrated Computing Network (ICN) is Los Alamos National Laboratory's main computer network. It consists of host computers (which execute user programs), file storage devices, network services, local and remote terminals, data communication interfaces, and distributed processors (DPs). DPs are remote processors which range from workstations (personal and mini computers) to full-scale computers. The "core" of the ICN is considered to be the main host computers and their support devices, while the DPs are considered to be the "extended" network. Through the ICN, any user inside the Laboratory may access any host computer (if the user has authorization to do so and the access path is approved) 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 four "partitions"; the Open, Administrative, National Security, and Secure partitions. ICN Partitions are dedicated to specific levels of processing, and are limited to users cleared for the most sensitive information processed in a given partition. The Open partition is available to anyone who has a legitimate need to compute at Los Alamos and is limited to unclassified, non-sensitive computing. The Administrative partition is primarily dedicated to processing sensitive unclassified data or data subject to a privacy act. The National Security partition is dedicated to processing of DOD classified and unclassified data. The Secure partition is dedicated to processing DOE classified and unclassified data.

Partitioning is enforced throughout the network by a system of dedicated, special function, ICN nodes. These nodes perform specific services in the ICN, such as user authentication, access control, job scheduling, file access and storage, and file movement between partitions. They are physically protected, have tightly restricted access, are limited to only that software needed to perform a specific service, and do not execute user programs. Only these dedicated nodes are allowed to service multiple ICN partitions. Each of these nodes is required to produce and maintain an audit record of its activity.

Because of the critical nature of the services performed by the special function ICN nodes, and to keep the quantity of data to be processed at a manageable level, it was decided to apply anomaly and intrusion detection processing to these systems. Though the audit log of the combined services performed by these systems provides an extensive record of user activity on the ICN, it does not provide a complete record of user activity on the host computers. However, given the scope of the problem, it was decided that the network service data was the place to start.

3 History

Until recently, most security auditing of ICN activity was performed by manually scrutinizing system logs and thus identifying potential security violations. Given the magnitude of the audit records, manual review of these records was limited to a small sampling or a very cursory scanning. A number of security violations were identified over a period of time, but there was no way to evaluate the success or completeness of this approach. In addition, when suspected security violations were identified by other means, the Laboratory's Internal Security (ISEC) personnel frequently requested audits that covered periods of time months in length, which were months or years in the past. Since there was no automated way to perform these audits, considerable effort was expended in completing them. It was for these reasons that development of an automatic audit record analysis system was undertaken at Los Alamos. Development was heavily influenced by the initial research of Dorothy Denning and her colleagues [1, 3, 4], and the current IDES research and development being carried out by Teresa Lunt and her colleagues at SRI International [5, 6, 9, 10, 13]. They have demonstrated that 1) the statistical analysis of computer system activities may be used to characterize "normal" system and user behavior and, given such statistical profiles, that user and system activity that deviates beyond certain bounds is detectable, and 2) 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. Their approach puts a primary emphasis on the detection of deviations from normal user and system behavior by statistical means, combined with an expert system which encodes intrusion scenarios that are intended to catch those invalid activities missed by the first means [10]. Another approach has been demonstrated by the development of the Multics Intrusion Detection and Alerting System (MIDAS), which has been implemented on the National Security Center's Dockmaster system [7, 8]. Although heavily influenced by the work at SRI, the major emphasis on MIDAS was to encode a set of *a priori* rules that define invalid activity and intrusion scenarios. This approach has also been successfully applied to security audit log analysis by means of an expert system (AudES) developed at IBM [12].

In late 1988, an intrusion detection feasibility study was undertaken at Los Alamos. Its purpose was to look into the possibility of developing an intrusion detection system for the Los Alamos network. It was determined that an expert system approach to the problem of ICN audit record analysis using a set of pre-determined rules would work, that invalid user activity could be detected, and in fact such a system would be relatively easy to implement [11]. In the spring of 1989, with the receipt of funding from the Operational Security Division at Los Alamos, the Network Anomaly Detection and Intrusion Reporter (NADIR) project was initiated.

The major goals for the development of the NADIR system were to:

- Develop a better understanding of the patterns and range of user activity on the ICN, for future planning and development.
- Develop a means by which to detect and evaluate unanticipated security vulnerabilities.
- Provide a more efficient method of past and current audit record review, as required by ICN security personnel.
- Develop a near realtime method by which to detect a range of security relevant events, including attempted break-ins to the ICN by outsiders and invalid activity or abuses by insiders.

In addition to the stated project goals, providing useful tools to network and security personnel during each phase of development was given a high priority.

4 Working Prototype

NADIR was designed to be implemented on a dedicated workstation. This was done so that its processing would not impact target system performance, for reasons of security, and because it was to receive and correlate data from multiple systems. At this time there is one NADIR workstation. However, as additional target systems are added to NADIR, we envision a network of workstations, each processing the audit record from one or more target systems and each contributing to a distributed database.

The current NADIR prototype is 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 which are 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, which is provided by Sybase. Transact-SQL provides such capabilities as stored procedures, triggers, system administrator tools, and control flow language features, which are used extensively in NADIR. In addition, C was required for a portion 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 required to each system were minimal. Communication with NADIR by a target system requires only the installation of Sybase provided interface software, and the use of a standard DECnet or TCP/IP protocol. An implementation of TCP/IP under VMS was provided by the Multinet[8] software package. Interfaces to Sybase were provided by DB-Library packages for Fortran and C. The target system code was changed only to format the audit record for NADIR, and to provide for the transmission of a record of each user activity immediately after its occurrence. The NADIR required data processing on either system has not resulted in any measurable degradation in system performance.

The combined load of NSC and SAM audit data is relatively light. The NSC performs a user authentication every 2.6 seconds during peak times, and much less than that most of the time. SAM activity is even lower than this, with less than 100 logons a week involving 30-40 separate users. Normally, each of these users enters only a small number of commands. NADIR uses 100 MBytes of disk space for the database generated from the NSC and SAM audit records. NADIR is able to process an audit record and report any suspicious behavior found within .25 seconds of the time the record is received

[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.

5 System Design

A phased approach was taken in applying NADIR to the ICN service nodes. Nodes were (and are being) individually analyzed, their data initially processed separately, and then combined in the NADIR system. As NADIR adds new nodes, their user activity record is correlated with previously included nodes to produce more complete profiles of each ICN user and of overall ICN activity. This will eventually allow the tracking of individual users as they enter the ICN, move from host to host, access and move files, and run jobs, until they leave the ICN. With the addition of each node, new expert rules are being defined which use the expanded information available, describe more elaborate scenarios of invalid or suspicious user activity, and will over time improve the discrimination and judgement of the system. The NSC and the SAM have been integrated 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 consists of six functional components; Data Collection, Data Processing, Anomaly Detection, Report Generation, Event Assessment, and the User Interface. Their relationship to each other is illustrated in Figure 1.

5.1 Data Collection

NADIR monitors target system activity as it occurs and is recorded in audit records which are generated by the target systems. Each audit record describes a single event. Audit records from different target systems vary in format and contain in many respects unique data, a result of the functionally different tasks performed 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 which describe the activity, and any errors which may have occurred.

NADIR data collection was designed to be relatively easily expanded to multiple targets, which consist of a number of different hardware and software systems. This effort was supported by two design choices; 1) the use of flexible off-the-shelf interface and database software, which was selected to expedite data translation between different operating systems and to enable the merging of data into a single extended database, and 2) the limitation of required target system changes to the capability to collect the appropriate audit record of user activity, transform the data into a specified canonical format, and transmit it to NADIR. In addition, NADIR software is designed in a modular fashion, so that new target system expansions can be handled with a minimum of effort.

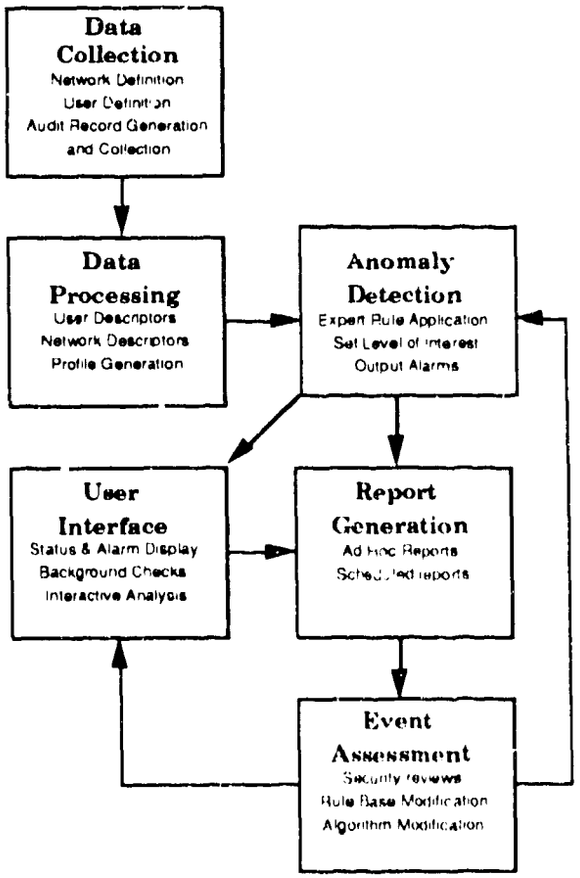

Figure 1: NADIR System Model

5.2 Data Processing

All user and system activities, as represented by audit records from the target systems, are summarized into statistical profiles. These profiles are a description of current behavior, with respect to a set of defined parameters. Profiles are maintained for both individual ICN users and for a composite of all ICN users. The profiles are updated as each record of activity occurring on any target system is received by NADIR. As users alter their behavior, their profiles will change. Rather than the detail contained in each audit record resulting from a user's activity, the profiles contain count statistics which summarize the activity. When a new audit

[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.

record is received, the data is parsed and the appropriate counts in the profiles are incremented. At this point in development, new profiles are generated for each week. Past weekly profiles are maintained for comparison purposes and as a permanent record.

5.3 Anomaly Detection

Observed events within the profiles are compared to expected and proper behavior by means of the application of expert rules and deviations identified (the identification of a deviation by an expert rule is generally refered to as having "fired" or "triggered" the rule). Each deviant event (or anomaly) is assigned a level of interest. The level of interest is based on the number, type, and combination of expert rules which have been fired by the user's behavior. It may be applied to an individual user, to a system, or to an 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 combination of the level of interest for each monitored user or system, and the record of events fired by each, provides an ongoing summary of the security status for each user and system being monitored. The expert rule model and its application on NADIR is covered in more detail in section 6 of this paper.

5.4 Report Generation

Anomaly reports are generated for all deviant events. The frequency of reports is dependent on the seriousness or level of interest associated with each event. All events are documented in weekly reports. Those events which are determined to be very interesting, but not critical, are output in daily reports. Very suspicious events of a critical nature, such as a highly probable attack underway, are output immediately.

NADIR generates routine reports on a weekly basis. Summary hardcopies are routed to project developers and security personnel. A complete report, which includes data from the audit record to support the findings of the summary, is stored in the Secure partition of the ICN's Common File System, where it may be accessed and reviewed electronically by authorized personnel. The weekly hardcopy report is 18-20 (two sided) pages in length, and contains:

- Summary statistics of all activity on the ICN for the week (one page).
- Graphical representation of all user activity for the week, including anomalous activity, plotted over time with a granularity of one hour (eighteen plots).
- A list of all anomalous users for the week (usually 65-85 users), listed in order of their level of interest. Of the total, 7-10 will be very suspicious, 20 or so moderately suspicious, and the rest various levels of interesting. For each user, the list contains the level of interest, a user ID, and the user's name, group, and type.
- A detailed description of each user's anomalous activity, including which rule(s) were fired.
- A list of all users who moved files from a higher to a lower level ICN partition (an activity which is closely monitored), sorted on the basis of the classification of their computing activity.
- Two pages of descriptive boilerplate.

If a critical event is detected, security personnel are contacted as quickly as possible. An appropriate short report is generated, the contents of which depend on the nature of the event. Detailed follow-up reports may be requested as part of an investigation.

5.5 Event Assessment

Upon receipt of a NADIR report, whether it be critical or routine, security personnel perform a review of all anomalous activity, even the relatively uninteresting. In order to process the weekly reports in a timely manner, specific security personnel are assigned responsibility for various categories or types of ICN users. Each anomalous user's activity is reviewed in detail, and a decision made whether further investigation is required. This may include interviewing the user. If the user's activity warrants it, the user is blacklisted during the investigation. A short report is filed at the completion of each investigation, giving details of its resolution. This information is provided to the NADIR developers, so they may have immediate feedback on system performance. Periodic reviews are held with security personnel to evaluate the system's effectiveness and to make recommendations for improvements. Where indicated, the expert rules on NADIR are modified to 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 warning and alarm displays, and current status displays. For users who have been provided the appropriate access and privilege, the user interface allows a choice of built in queries or allows ad-hoc queries against the raw audit data, the individual user and composite pro-

files, and current status information. It allows the review of all the audit data associated with a particular user, a particular machine, or any other parameter over any selected period of time. Data may be displayed in a variety of ways, including graphically, and reports generated.

Security personnel at Los Alamos frequently have the need to perform background reviews of user activity on the ICN, based on information received from a variety of sources, and for many different reasons. These reviews usually involve one individual ICN user, but have at times involved such things as all users from a particular source. To support this need, NADIR provides the capability for interactive background analysis of current and past activity, for a particular user or users, or any other parameter in the database, over any specified period of time. The audit data required for background analysis is maintained indefinitely at Los Alamos. A complete audit record, starting in October 1989, and continuing to date, is readily available. Older audit data is archived and would require some processing to be usable by NADIR.

6 Expert Rules

NADIR rules try to detect attempted break-ins by outsiders, masqueraders, and misuse by insiders. To detect attempted break-ins by outsiders, NADIR uses rules involving such deviations from normal behavior as abnormally large numbers of logon failures by known users, abnormal blacklisting[1] of known users, abnormal numbers of logon failures by unknown users (the user ID is not defined on the ICN), abnormal numbers of failures from a single source (especially if the source is a dial-up line), high rates and/or precise timing of attempted logons (automation), and the use of unusual activity times. To detect masqueraders, NADIR uses rules involving unusual or abnormal user logon parameters (time, location, partition, computing level, etc.), especially when logon failures are combined with these parameters, and such things as simultaneous (or nearly) logons from physically separate locations. To detect misuse by insiders, NADIR uses rules involving attempted access to classified or sensitive partitions, suspicious movement of files between partitions, automated logons, abnormal logon rates, logons to an abnormal number of machines, logons from an abnormal number of sources, and misuse of restricted (special usage) user numbers.

[1] Blacklisting is applied to an individual user with the occurance of five sequential authentication failures. A blacklisted person is denied access to the ICN by the NSC. Removal of the blacklist must be approved by security personnel.

The NADIR rule base comprises of four logical filters, each designed to separate out certain types or levels of anomalous activities. Basically following a knowledge engineering approach which has been successfully implemented at Textronic [2], the rule base definition started with the abstraction of the reasonably well-understood part of the problem; ICN security policy and well-defined invalid and suspicious behavior. This resulted in rules for the Characteristic Filter. Report requirements provided rules for the Report Filter. From there evolved progressively less well-understood refinements, which are being implemented in the Misuse and Attack Filters. These rules involve heuristic associations which sometimes make intuitive leaps that are not always explicitly justified, and as a result may have to be periodically reconsidered. The rule base filters are activated in stages, as illustrated in Figure 2.

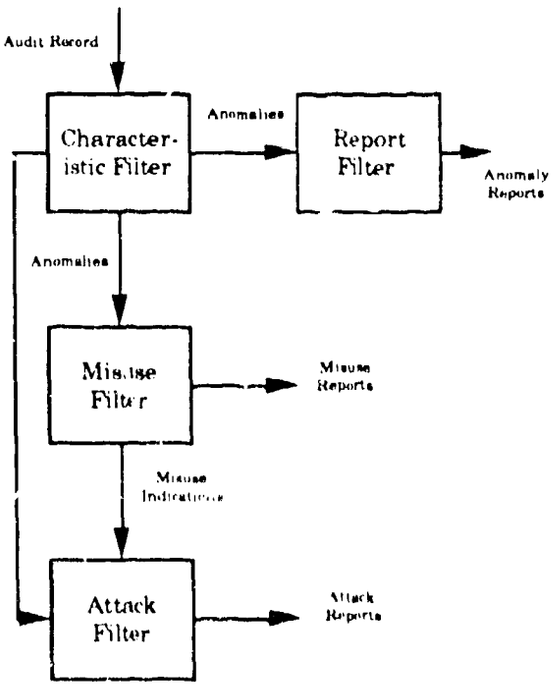

Figure 2. NADIR Rule Base Structure

• *Characteristic Filter* - applies rules which are straightforward descriptions of simple activities, each one serving to reveal and distinguish an individual feature of anomalous behavior. Each Characteristic rule is applied individually; no attempt is made to correlate one with another. A level of interest is associated with 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. Characteristic rules are applied prior to other rule types. Anomalies defined by these rules set the stage for the application of all other rules.

- *Report Filter* - applies rules to the anomalies output by the Characteristic Filter, to produce appropriate reports of anomalous behavior. These rules specify what report is to be generated and when it is to be generated. What and when are determined by the level of interest associated with an anomaly, and by specified time periods.

- *Misuse Filter* - applies rules to the anomalies identified by the Characteristic Filter. These rules attempt to identify patterns of anomalous activity which have a high probability of being systematic misuse. They specify an action to be taken when fired, such as the output warning messages. The Misuse Filter also supplies input to the Attack Filter.

- *Attack Filter* - applies rules which attempt to correlate the recorded Characteristic anomalies and Misuse Indications with various Attack Scenarios. Attack Scenarios identify patterns of anomalous activity which have a high probability of being attacks on the system. They specify an action to be taken when fired, such as the output of alarm messages.

6.1 Characteristic Rules

Characteristic rules are applied either to the input audit record as it is received by NADIR, or to profile data immediately after it is updated from the audit record. As each anomaly is found, an Anomaly Record is either generated or updated, whichever is appropriate. The Anomaly Record includes a level of interest for the involved user or system, and an indication of which rule has been fired. Any increase in the level of interest depends on the severity of the anomaly detected by the rule. Characteristic rules fall into three basic categories:

Security Policy - These rules are the implementation of ICN security policy, and were obtained by interviewing security personnel and reviewing documentation. They are intended to detect individual events which are potential or certain security violations, or which because of the activity type, are inherently interesting and must be included in periodic reports. An example of a security violation rule:

IF [illegible]
AND [illegible]
AND [illegible]
THEN update the Anomaly Record, and assign the user a high level of interest.
EXPLANATION: Use of a classified password from an unprotected terminal [illegible] considered reason enough to consider the password compromised. The password will be immediately invalidated.

Individual Anomaly - These rules are applied to individual user profiles, to detect when a user's behavior departs from that which has been determined to be normal and valid ICN user behavior. These rules were obtained by means of a statistical analysis of the past behavior of all individual ICN users, and by interviewing security personnel. An example of an individual anomaly rule:

IF the Failure Ratio[12] of a user is [illegible],
AND the user has logged on >n2 and ≤n3 times,
THEN update the Anomaly Record, and assign the user an appropriate level of interest.
EXPLANATION: If a user has logged on to the ICN enough (n2 times) not to be considered a new user, and since the average ICN user has a Failure Ratio that is much less than n1, then a Failure Ratio of n1 is considered significant. A sliding scale of concern, balanced between the total number of logons and the Failure Ratio, is applied to this rule.

Composite Anomaly - These rules are applied to composite user profiles, to detect when the composite of all user activity departs from the pattern which has been determined to be normal and valid for the system. These rules were obtained by means of a statistical analysis of the past behavior of the composite of ICN users. An example of a composite anomaly rule:

IF [illegible] **OR** [illegible] day, **OR** [illegible] week,
THEN update the Anomaly Record, and assign the system an appropriate level of interest.
EXPLANATION: [illegible]

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

```
depends on the amount of variation from
normal.
```

6.2 Report Rules

These rules are based on designated time intervals. They perform periodic checks of anomalous activity levels, and define what reports are to be generated at the end of these intervals. Designated report time intervals may be daily, weekly, or any other desired interval. They analyze the Anomaly Record for the indicated time period, and generate reports which summarize and/or detail the appropriate anomalous activity. An examples of an Anomaly Report rule:

```
IF it is the end of the week (midnight
Sunday),
THEN for each individual user in the
last week's Anomaly Record, do the fol-
lowing:
  IF there is any level of interest as-
  sociated with the user,
  THEN include the user in the weekly
  anomaly report.
EXPLANATION: All anomalous users are
included in the weekly anomaly report.
```

6.3 Misuse Indication Rules

These rules are fired by one Characteristic anomaly, or a sequence or combination of anomalies, which have a low probability of occurring, and which indicate possible serious misuse of the network. They do not attempt to define anything as specific as an attack, but their firing indicates something is seriously amiss. The following Misuse Indication rule examines the activity of all users:

```
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, which
includes an urgent warning message to
the user interface.
EXPLANATION: The number of ICN users
who, in a given period of time, reach a
particular level of interest is statis-
tically very consistent. Extreme varia-
tions from the normal level of anoma-
[illegible]
[illegible]
network. A [illegible]
represented by this rule, which depends on
[illegible]
[illegible]
```

The following Misuse Indication rule examines the Anomaly Record of an individual user:

```
IF Characteristic rule 003 is set,
(an individual user has an abnormally
large number of logons this week)
  AND Characteristic rule 036 is set,
  (the same user has an unusual
  distribution of logon attempts during
  the swing and weekend shifts).
  AND Characteristic rule 031 is set,
  (the same user has an unusual distri-
  bution of unsuccessful logon attempts
  during the swing shift AND has a
  large number on logon attempts during
  that shift).
  AND Characteristic rule 033 is set,
  (the same user has only unsuccessful
  ICN logon attempts during the night
  shift).
  AND Characteristic rule 043 is set,
  (the same user has an unusual distri-
  bution of unsuccessful logon attempts
  on the weekend).
  AND Characteristic rules 044, 045,
  046, and 047 are not set,
  (the same user does not show a simi-
  lar pattern of failures during the
  day shift).
  AND Characteristic rules 040 and 041
  are not set,
  (the same user does not show a simi-
  lar pattern of failures on weekdays).
THEN output an immediate report, which
includes a message to the user inter-
face.
EXPLANATION: The fired Characteristic
rules show a much greater than normal
usage of the ICN, combined with abnor-
mal usage during off hours. In addi-
tion, the user has had an abnormal num-
ber of failures during off hours, while
not showing a similar pattern of fail-
ure during normal working hours. This
could be an attempt at masquerading,
and is certainly suspicious.
```

6.4 Attack Scenario Rules

These rules may define one Characteristic anomaly or Misuse Indication, or a combination of these, which have a low probability of occurring, and which indicate a known or postulated attack. It is the sequence and/or combination of these rules that make for an increasing certainty that an attack may be under way. Attack Scenarios are obtained from security personnel and other experts in system penetration. Attacks are events which could result in the compromise of passwords, denial of service, or "swamping" of one of the ICN service systems.

Attack Scenario rules are in the definition stage for NADIR.

7 Results

NSC audit data has been continuously processed for invalid activity since November of 1989 (for part of this time in weekly batch mode), using a growing and improving expert system. SAM audit data has been processed since August of 1990, starting in batch mode. The NADIR working prototype has been in operation since June of 1990. Reports have been generated on a weekly basis for this entire time period, and statistics of ICN activity maintained. Rather than try to validate the system by use of artificially constructed test cases and intrusion scenarios, we used the audit data normally generated by the target systems, and a process of extensive evaluation of the results. The following has been accomplished:

- Invalid activity by unknown (presumably external) users was identified and investigated.
- Numerous cases of misuse or suspicious behavior by insiders were identified, including automated logons, misuse of restricted user numbers, apparent (unsuccessful) attempts to logon using another person's user number, attempted logons (unsuccessful) from terminals in partitions to which the user did not have access, and attempted use (unsuccessful) of computers in partitions to which the user did not have access.
- Unanticipated network problems which had not previously been identified were uncovered, which have been remedied where possible or are being closely monitored.
- Misuse conditions which had not previously been identified were uncovered. These resulted in the definition of new expert rules.
- Support was provided in the background analyses that were required during investigations of a number of current and past ICN users.

In addition to benefits in the area of anomaly detection, NADIR has provided unanticipated benefits. It has enabled us to:

- Detect problems with some nodes of our network as they occurred. For example, a surge of invalid network messages from a source machine could be the first indication of a hardware or software failure rather than a user induced problem. We were able to tell the difference between the two types of activity and encode it into our rule base.
- Provide detailed reports upon request of network activity that was useful to personnel in such areas as accounting and networking, which included statistics of network and computer usage.

We have found it difficult to come up with a number that accurately describes our "false positive rate". It's true that most of the flagged individuals and events are not intruders, spies, or even users deliberately misusing the system. It's also true that their behavior, for one reason or another looked suspicious, and for our security personnel that's reason enough for at least a preliminary investigation. We believe that as long as the list of flagged users and events is short enough for quick review, it is better to have "false positives" than to miss anything significant.

8 Future Directions

Anomaly and event notification currently consists of terminal messages and periodic reports. For serious security events, the ultimate goal is to have notification on a near realtime basis. This notification will be broadcast to the Los Alamos Network Operations Center (NOC), which is manned 12 hours a day, with personnel who are reachable 24 hour a day.

Future targets will be additional network service nodes which control file access, storage, and movement, and operations control such as job scheduling. We plan to develop a network of SUN workstations, each processing the audit record of one or more nodes, distributing the functional applications and database, and thus optimizing performance.

Since some kinds of invalid user activity, if allowed to continue, could result in break-ins or denial of service to legitimate users, another goal is the notification of appropriate ICN node(s) of extremely suspicious activity, and the development of responses by the node(s) to that activity. This would consist of taking direct action to stop an identified penetration attempt. The node's actions will have to be proportional to the extent that the monitored activity has deviated from what is considered valid, what damage could result from allowing an invalid activity to continue, and denial of service considerations. The criteria for such a response have yet to be determined.

Finally, 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. This has become an even greater concern as the system is expanded to additional ICN nodes, and the resulting rule base has become correspondingly more complex.

9 Summary

NADIR demonstrates 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 demonstrates the benefits of a phased approach to applying intrusion detection in a distributed environment. The working prototype is a start towards a longer-range goal of expanding the system to additional ICN nodes, and cross correlating their information to produce more complete profiles of user activity on the ICN.

10 Acknowledgments

We wish to acknowledge the contributions of Jimmy McClary (the ICN CSSO) who introduced us to the basic concepts, 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, including Dottye Alexander, Charlene Douglass, Lois Sylvia, Donna Stevens, and Mona Wecksung. We are indebted to Harry Martz for his expertise in 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] T. Lunt. *Automated Audit Trail Analysis and Intrusion Detection: A Survey* (Proceedings of the 11th National Computer Security Conference, October 1988).

[8] 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).

[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] K. Jackson. *Development and Analysis of User Authentication Profiles for an ICN Intrusion Detection System* (Los Alamos National Laboratory, June 1989).

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