CHALMERS

A survey of commercial tools for intrusion detection

Håkan Kvarnström

Chalmers University of Technology
Department of Computer Engineering
Göteborg 1999

A survey of commercial tools for intrusion detection

Technical Report 99-8

Håkan Kvarnström
Department of Computer Engineering
Chalmers University of Technology
Göteborg, Sweden
email: hakan.k.kvarnstrom@telia.se

Abstract

This report gives a review of commercial tools available for detecting intrusions in computer systems and networks. Seventeen systems are evaluated and a short introductory overview is provided for each. A classification especially designed for intrusion detection systems (IDS) is utilized to compare and evaluate different features and aspects of the products. This work identifies a number of important design and implementation issues which provide a framework for evaluating or deploying commercial intrusion detection systems.

1. Introduction

Intrusions in computer systems are an inherently increasing problem. Distributed system architectures that connects connect a large number of computers raise questions on how to better protect the integrity and availability of the systems. Intrusion detection (ID) is an emerging technology for detecting unauthorized users and suspicious behavior in computer systems. During the last decade, a large number of different intrusion detection systems (IDS) has been presented. Many of these are purely research prototypes and have no commercial counterparts. However, quite a number of commercial systems are available today and many more are expected over the next few years. This document provides an overview of the existing commercial products available. While it may not be complete, it should give the reader reasonable insight into and feeling for the products on the market. It should also empower the reader with a basic understanding of the functionality of each of the products presented. This understanding will hopefully provide guidance in the process of selecting appropriate tools for detecting intrusions. Other surveys in the area have previously been presented [2], but most of them are less complete and make no comparison of the systems according to a formal classification.

For a detailed discussion about research prototype systems, the reader should consult the work of Axelsson [1].

1.1 A generic ID architecture

Despite the differences among commercial products (each having different functionality and features), the core architecture seems to be quite similar in many respects. One framework for describing intrusion detection systems is the *Common Intrusion Detection Framework* (CIDF) [6]. CIDF is maintained by the CIDF working group which was originally formed as a collaboration between DARPA (Defense Advanced Research Projects Agency) funded intrusion detection and response (IDR) projects. The design goals of CIDF are to develop a set of specifications that allows different IDR components to interoperate and share information and allow different IDR subsystems to be re-used in contexts different from those for which they were designed.

CIDF defines four basic components:

- Event generators (E-boxes)
- Event analyzers (A-boxes)
- Event databases (D-boxes)
- Event response units (R-boxes)

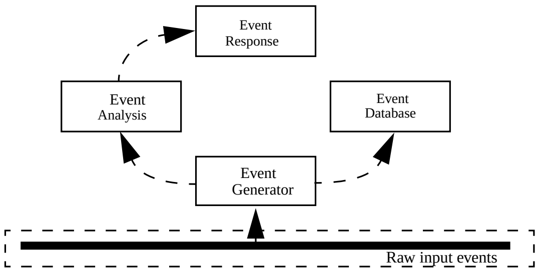

FIGURE 1. Components of the CIDF (Common Intrusion Detection Framework).

The *event generators* obtain information from sources of events throughout the computing environment. Events can originate from network elements, applications, host audit records or any other interesting subject. The events are collected and transformed into a standard format (gido) designed for interoperability.

Event analyzers receive information (gidos) from other components and try to analyze the data, looking for intrusions. Various mechanisms can be used, such as statistical analysis and pattern recognition searching for sequences of events.

Storage of events and information (gidos) are handled by *event databases.* Both low level (raw events) and high level events (i.e. interpreted by event analyzers) may require persistent (long term) storage.

The *response units* receive information about security related events and initiate the proper response mechanisms to abort or divert an attack. Possible responses may include killing processes, resetting connections and altering file permissions.

Despite the variety of intrusion detection architectures (IDA), most existing intrusion detection systems can be mapped onto CIDF in some way.

1.2 How to read and use this report

This report reviews commercially available systems for detecting intrusions, and more importantly, raises important design and implementation issues that provide a framework for evaluating these systems. Chapter 2 and Appendix A of this report present the systems included in this review. While many of the systems are only briefly covered, others are discussed in detail. The reason for the differences is the limited availability of publicly available information and documentation. Chapter 3 introduces the methodology used to evaluate the products. The methodology includes a five-tiered categorization that can be used independently for evaluating other (or new) products. Chapter 4 contains the comparative results organized according to the previously defined methodology. In Chapter 5, conclusions are drawn and some interesting observations are highlighted.

2. Systems analyzed

A total of 17 systems were analyzed in this survey (see Table 1). Due to the rather lengthy descriptions of the systems, they have been placed in Appendix A.

Product	Vendor	Ref.
RealSecure	Internet Security Systems (ISS)	[8]
Intruder Alert	Axent Technologies, Inc.	[9]
Net Ranger	Cisco Systems, Inc.	[10]
Stake Out I.D	Harris Communications, Inc	[11]
Kane Security Monitor	Security Dynamics (formerly Intrusion Detection, Inc.)	[12]
Session Wall-3	AbirNet	[13]
Entrax	Centrax Corporation	[14]
CMDS	Science Application International Corporation (SAIC)	[15]
SecureNet PRO	MimeStar, Inc.	[16]
CyberCop	Network Associates, Inc.	[17]
INTOUCH INSA	Touch Technologies, Inc	[18]
T-Sight	EnGarde Systems, Inc.	[19]
NIDES	SRI International	[20]
ID-Trak	Internet Tools, Inc.	[21]
SecureCom Suite	ODS Networks	[22]
PolyCenter	Compaq (formerly Digital Equipment Corp.)	[23]
Network Flight Recorder	Network Flight Recorder, Inc.	[24]

TABLE 1. List of products that are included in this review

3. Methodology

3.1 Source of information

In order to compare the different products on the market, we examined publicly available product documentation, published conference material (proceedings) and other material available for public review. As this report is an analysis of design specifications rather than a test of implementations, we have not performed any tests under laboratory or real-life conditions.

3.2 Comparison criteria

When comparing different products it is crucial to identify parameters that lend themselves to comparison. The following criteria are based upon such a classification defined by Axelsson [1]:

Granularity of data processing. The response time of an IDS depends partly on the granularity of data processing. Collected raw data can be processed continuously or in batches, at some regular interval.

Source of audit data (raw events). The source of audit data can be either network- or host-based. Network-based data are typically read directly off some multicast network (Ethernet). Host-based data (security logs) are collected from hosts distributed throughout the network and can include operating system kernel logs, application program logs and network equipment logs or other host-based security logs. One advantage of using network-based audit data is that it enables the intrusion detection system to see *all* traffic on the network. Hence, it is not limited to audit data destined to itself or any other specific host. However, the increase in the use of network encryption technologies, such as IPSEC [4], renders network-based audit data worthless. Even though the encrypted audit data can be collected, one cannot extract the semantics of the data because of the encryption.

Detection method. The detection method refers to the mechanism or method used to analyze the audit data searching for unauthorized events or behavior. Two different approaches for detecting intrusions are commonly used: *rule based* and *anomaly based.* These methods are further explained in section 4.1.6.

Response to detected intrusions. Responses to an intrusion can be either *passive* or *active*. Passive systems respond by notifying the proper authority. They do not take any measures to prevent or limit the damages caused by an attack. Active systems may not only notify the proper authority but also initiate the necessary countermeasures. These countermeasures often seek to limit the damage inflicted by the attack. In some cases, a counterattack may be necessary to prevent the attacker from causing further damage.

System organization. The organization of an intrusion detection system can be either centralized or distributed. In practice, it may be difficult to categorize a system as strictly centralized or fully distributed, as some subsystems may be centralized while other subsystems are distributed. In many cases, data collection is distributed while the data analysis is centralized.

Security. The ability of the intrusion detection system to withstand attacks against itself is called *security.* The classification would naively be on a high-low scale. As little research has been conducted in this field, most systems do not address these issues. Consequently, most IDS have a relatively low or negligible degree of security.

Degree of interoperability. The degree of interoperability measures the intrusion detection system's ability to cooperate with other similar systems. Interoperability can be of interest at various levels in the architecture serving many different purposes such as:

- Exchange of audit data records
- Exchange of security policies
- Exchange of misuse patterns or statistical information about user activities
- Exchange of alarm reports and event notifications

Manageability. This is the systems ability to be managed or send alarms to dedicated management systems such as HP Openview or BMC Patrol.

Adaptivity. Proprietary application and communication protocols may also be a target for misuse and intrusion attempts. Therefore, it is important that the intrusion detection systems can be adapted to site specific needs with relative ease.

System and network infrastructure requirements. System and network infrastructure restraints may limit the versatility of a product. Implementation cost and market requirements are possible causes of such restraints. Over the last years, TCP/IP has gained widespread use and is probably the dominant network topology of today. As a result, one can expect to see this reflected in the products available.

3.2.1 Classification of comparison criteria

Several of the above defined criteria share properties that benefit from being treated as a whole. Therefore, for readability, the original criteria are divided into five main categories addressing different aspects of the systems:

Aspect	**Criteria**
Functional aspects	Granularity of data processing Source of audit data Response to detected intrusion Degree of interoperability Detection method Adaptivity Detection capabilities
Security aspects	Security
Architectural aspects	System organization System and network infrastructure requirements
Operational aspects	Performance
Management aspects	Manageability

TABLE 2. Classification of comparison criteria

4. Results

As already mentioned, a total of 17 different intrusion detection systems were analyzed in this survey. The results are categorized using the criteria defined in chapter 2. For each category listed, it is the aim to give a comparative view of the conformance of the systems analyzed.

4.1 Functional aspects

4.1.1 Granularity of data processing

Almost all of the vendors allow intrusions to be detected in real-time. A relevant question in this context is how to interpret “real-time”. The time that elapses between the time an attack is initiated and until the system is penetrated varies depending on the nature of the attack. Assuming that automated tools are used for the attack, the time to a complete collapse of system security may be in the order of milliseconds. Therefore, in some cases, the attack may be completed before it is detected and reported to the proper authority. Another issue is the real-time characteristics of host-based intrusion detection systems. In this case, audit logs are collected in batches before they are processed or analyzed, with an even longer delay as a result. These delays may or may not be a problem, depending on the security of the intrusion detection system and its ability to track further activities (audit capabilities) and to terminate established sessions and processes.

T-Sight form Engarde, Inc. has adopted a somewhat different scheme for detecting intrusions. T-Sight is focused on collecting and presenting data to the SSO, who then in turn tries to identify intrusions. Systems using manual intrusion detection schemes can certainly not be classified as “real-time” as they depend on the presence of a human user.

4.1.2 Source of audit data (Raw events)

A majority (9) of the analyzed systems are network oriented in terms of source of audit data. Only five systems are purely host-based and three systems support both host- and network-based audit data.

As previously mentioned in the section on comparison criteria the increasing use of switched network technologies and encryption jeopardizes the future of network-based systems. Still, most systems of today rely upon network audit data. Some vendors claim that switched networks can easily be analyzed using dedicated management ports on the switches. This may be true if the network is moderately loaded but it is unrealistic on medium or heavily loaded networks. An innovative solution is provided by ODS Networks Inc. They incorporate ID (provided by ISS Inc.) into their product line of switches, thus eliminating the restrictions posed by switching technology. Although solutions exist to address the problem of switching, network encryption is a greater challenge. Confidentiality requirements prevent IDS from interpreting the semantics of the data streams. From a confidentiality requirement standpoint, an IDS is just like any other unauthorized adversary. A scenario in which the IDS is allowed to decrypt and analyze the network data stream would violate the confidentiality requirements and must therefore be discarded as a viable solution.

Over the last decade, the trend has been moving from host-based to network-based systems. It remains to be seen whether this trend is will change.

4.1.3 Response to detected intrusions

Passive responses. Passive response means that an intrusion is brought to the attention of the SSO. Mechanisms for passive response may be sending e-mails, paging or displaying alert messages. All systems except T-Sight provide some support for passive response mechanisms.

Active response. All but three systems (Stake Out, Kane Security Monitor and T-Sight) support active response without human interaction. For network-based systems, active response include actions like terminating transport level sessions, which most active response systems claim they support. Some systems, such as SecureNet Pro, even allow the SSO to hijack a TCP session. This provides a means for closing or terminating sessions such as Telnet or Rlogin in a controlled manner.

Host-based ID systems have the advantage that they can also control hostile processes on the host on which they reside. Most host-based systems analyzed claim to support termination of processes. Kane Security Monitor does not have this feature. Entrax offers only the possibility to log out a user, disable a users account or shut down the entire computer, which can be seen as a drastic way of terminating processes. Emergency shutdown of the entire host can be useful when the system contains information whose confidentiality is more important than its availability. Systems contaminated by computer viruses may also benefit from being shut down to prevent further contamination.

One should keep in mind that ID systems that have the capability to shut down processes or terminate network sessions often run with superuser privileges. This may impose a threat to the availability, integrity and confidentiality of the host on which the IDS is executing. A security breach in the IDS itself may be exploited to attack the target system.

Interfaces to network management applications. SNMP is a UDP based network management protocol. The protocol can be used to send “traps” containing alarms, warnings or other important events. RealSecure, Intruder Alert, StakeOut, CyberCop, Securecom, ID-Trak, Kane Security Monitor, Entrax, NetRanger and SessionWall-3 all have built in support for sending SNMP traps. In addition, StakeOut supports the sending of DES-encrypted SNMP traps.

Interfaces to network elements. Several of the systems also have the capability to interface with firewalls and other network elements. This provides a means to terminate established sessions/connections and block further connection attempts. RealSecure, Intruder Alert and SessionWall-3 support the OPSEC protocol which can be used to manage a Firewall-1 (among others). Cisco´s NetRanger can dynamically manage (Cisco) routers access control lists to stop unauthorized activities. CyberCop´s active response module (ARM) can interface with Cisco´s Pix firewall.

For a complete list of response mechanisms for each product, see Table 3 on page 12.

Service availability aspects. In an environment where the availability requirements of services and resources are high, active response mechanisms should be used with caution. This is especially important when using intrusion detections mechanisms with a high probability of false positives (e.g. authorized activities falsely categorized as an intrusion).

Legal aspects. An active response by “returning fire” can be an effective approach to preventing future intrusion attempts. However, this controversial response mechanism must be used with extreme care. The chance is that an intruder deliberately tries to illude the IDS to believe that someone else is mounting the attack. This may lure the IDS to return fire at innocent users or servers. In many cases it may not even be legal to take such actions.

4.1.4 Degree of interoperability

Interoperability for IDS can be achieved in a number of different areas. Four important areas are:

- Exchange of audit data records
- Exchange of security policies
- Exchange of misuse patterns or statistical information about user activities
- Exchange of alarm reports, event notifications and response mechanisms

Exchange of audit data records. Having a well defined data format for the audit records would let several IDS analyze the same data. This would be of importance if a decision is made to change the IDS or to have a second IDS analyze the same set of data. Network-based IDS listen to the network-level data stream, and thus collection of data is not always necessary. However, for host-based systems, interoperability would be beneficial. To some extent, interoperability exists in the products of today. For example, many IDS can make use of operating system audit logs, which may have a well defined format. These data formats are defined by operating system vendors and are not tailored for the purpose of detecting intrusions, however. Exchangable audit data records specifically tailored for intrusion detection will probably improve the probability of detecting intrusions, as all necessary input parameters would be available to the detection mechanism.

Exchange of security policies. Having a series of protection mechanisms to protect a network increases the depth of protection. For example, a firewall may protect the perimeter of the network while an IDS is strategically placed inside the network perimeter. In this case, the IDS will be able to detect security violations within the network as well as detect external violations not detected by the firewall. Although this scenario would be beneficial, it can cause a management problem as the security policy must be distributed to both the firewall and the IDS. As of today, the security policy is usually defined in a proprietary format for each and every component and cannot easily be exported or shared by other components. A firewall cannot use the policy of an IDS or vice versa. This means that it may be necessary to maintain several sets of policies, although their semantics are the same. As far as we could find, none of the IDS vendors address this problem.

Exchange of misuse patterns or statistical information about user activities. This is perhaps one of the most controversial interoperability aspects. Vendors providing a large set of misuse patterns of known intrusions have a competitive edge, hopefully resulting in increased sales. Although a standardized way of representing, storing and distributing misuse patterns using some form of vulnerability database[5] would benefit the users of the IDS, the vendors will probably not provide this feature in the near future. No IDS analyzed here has this feature.

Exchange of alarm reports, event notifications and response mechanisms. As described in Section 4.1.3 on page 9, most systems have some way of sending alarms or notifications to external devices. Paging capabilities and the possibility of sending messages using SMTP (email) are the most common mechanisms. Table 3 shows the different response mechanisms supported for each product.

Exchange of alarm reports, event notifications and response mechanisms[a]								
Product	**SMTP**	**Paging**	**SNMP**	**OPSEC (Incl. FW-1)**	**Raptor (FW from Axent)**	**Pix (FW from Cisco)**	**Cisco routers**	**Lucent FW Security Mgmnt Server**
RealSecure	◆		◆	◆				◆
Intruder Alert	◆	◆	◆	◆	◆		◆	
Net Ranger	◆	◆	◆				◆	
Stake Out I.D.[b]	◆	◆	◆					
Kane Security Monitor	◆	◆	◆					
Session Wall-3	◆	◆	◆	◆			◆	
Entrax	◆	◆	◆					
CMDS[c]								
SecureNet PRO	◆							
CyberCop	◆	◆	◆			◆		
INTOUCH INSA[d]								
T-Sight[e]								
NIDES[d]								
ID-Trak	◆	◆	◆					
SecureCom Suite[f]	◆		◆	◆				◆
PolyCenter	◆							
Network Flight Recorder	◆	◆						

TABLE 3. Exchange of alarm reports, event notifications and response mechanisms

a. Note that third party applications may be required for some of the response mechanisms

b. Sending of Email and paging are available only in the Stake Out I.D. Enterprise version

c. Response mechanisms can be made available using customization services

d. No information about response mechanisms was available

e. T-Sight is a manual IDS. Thus no automatic response mechanisms are available.

f. SecureCom partly uses RealSecure for intrusion detection

4.1.5 Adaptivity (customization)

All systems except Kane Security Monitor and Stake Out I.D can be customized (to some extent) by the SSO. Customization may involve:

- Adding new intrusion patterns
- Adopting rules for site specific protocols and applications.

Some of the vendors even provide intrusion-database updates on a regular basis. RealSecure, Intruder Alert, Entrax, SecureNet Pro, CyberCop, and SecureCom can be updated without major software changes using installable modules.

Stake Out I.D., Kane Security Monitor, CMDS, NIDES, PolyCenter and INTOUCH INSA have the possibility to use an anomaly based detection scheme which automatically adapts to the "normal" behavior of input data. This is further explained in section 4.1.6.

Graphical user interfaces vs. scripting languages. Many products provide a graphical user interface for defining new attack signatures. Some systems provide powerful scripting- or programming-languages which allow finer control over the attack signature definitions. Both NIDES and NFS use programming languages when analyzing audit data. Generally, scripts or programs are easier to distribute and share with other systems having a similar configuration. The drawback is that such systems tend to have a steeper learning curve compared with systems with graphical user interfaces. It simply takes some effort to learn the language before new signatures can be defined.

4.1.6 Detection method

Rule based detection. The system detects the violation of a policy. A policy is described by a set of rules. This policy can be specified either in a default permit or in a default deny fashion. Using a default permit stance, the SSO specifies some kind of signature that describes illicit behavior. Finding these signatures can be as simple as performing pattern recognition or can be more advanced, e.g using some form of state machine. In a default deny stance, the SSO specifies the normal operation of the system, and deviations from the set norm are viewed as an attempted intrusion by the detection function.

When evaluating intrusion detection systems, one should not underestimate the value of the mechanism used for providing rule based detection. Some systems, for example RealSecure and Cisco's NetRanger, use a simple mechanism similar to regular expressions to find strings or patterns that violate some policy or rule. Although regular expressions or other pattern matching mechanisms can be powerful, they do not allow themselves to represent state information. Using some form of state-machine or programming language, arbitrary complex programming constructs may be used by the detection mechanism. This would allow detection of intrusions defined by complex sequences of events or non-trivial correlation between events.

Intruder Alert's NetProwler module allows extensive customization using a graphical user interface. Boolean-, comparative- and other operators can be used to build a signature of events or sequences of events. Intruder Alert's host-based agent looks for strings in event logs or subsystems. RealSecure's system agent is similar, that is it looks for strings in text-based logs. RealSecure's (network) engines have only limited string matching capabilities. Instead, RealSecures's network agent focuses on analyzing source- and destination IP-addresses and combinations of UDP/TCP port numbers. CMDS uses CLIPS for rule based detection. CLIPS is a full-forward-chaining expert system developed by NASA. ID-Trak uses a method called SDSI (Stateful Dynamic Signature Inspection) to analyze network packets. It uses an virtual processor that allows attack signatures to be executed as a set of instructions. Perhaps the most flexible solution is the one provided by NFR, which uses a programming language to analyze network data that provide virtually unlimited detection capabilities. However, due to its flexibility, such efforts would require great skill and time.

Anomaly based detection. The system reacts to anomalous behavior, as defined by some history of the monitored target. In this definition, we also include the systems ability to automatically learn from the past. Anomaly based detection often uses some form of statistical or artificial intelligence (AI) engine. For example, PolyCenter, Stake Out I.D. and KSM use AI for that purpose. CMDS and NIDES find anomalies by calculating statistical deviations. Network Flight Recorder's flexible programming language should make it possible to implement customized detection methods such as anomaly based detection.

Table 4 lists the detection method used for each product. Note that T-sight is a manual

Detection method		
Product	**Rule based**	**Anomaly based**
RealSecure	◆	
Intruder Alert	◆	
Net Ranger	◆	
Stake Out I.D.	◆	◆
Kane Security Monitor	◆	◆
Session Wall-3	◆	
Entrax	◆	
CMDS	◆	◆
SecureNet PRO	◆	
CyberCop	◆	
INTOUCH INSA	◆	◆
T-Sight[a]	-	-
NIDES	◆	◆
ID-Trak	◆	
SecureCom Suite	◆	
PolyCenter	◆	◆
Network Flight Recorder	◆	

TABLE 4. Detection methods

a. T-Sight is a manual IDS.

intrusion detection system and thus cannot be categorized according to detection method.

4.1.7 Detection capabilities

The detection capabilities between products vary quite extensively. In general, a network-based IDS has greater capabilities owing to its ability to capture and analyze packet at the underlying network. Host-based ID systems are limited to audit-logs provided by the operating system or application logs. Due to the large number of different intrusions recognized, this paper present only an overview of the types of attacks each product can detect. Some of the products, such as RealSecure and Intruder Alert, include up to 200 different known intrusion signatures out of the box. Table 5 shows

Product	**Physical- and datalink layer**	**Network- and transport layer**	**Operating Systems**	**Applications, databases, management and support systems, office automation**
RealSecure				
Intruder Alert				
Net Ranger				
Stake Out I.D.				
Kane Security Monitor				
Session Wall-3				
Entrax				
CMDS				
SecureNet PRO				
CyberCop				
INTOUCH INSA				
T-Sight[a]				
NIDES				
ID-Trak				
SecureCom Suite				
PolyCenter				
Network Flight Recorder[b]				

TABLE 5. Detection capabilities mapped onto a protocol stack.

a. The dotted line indicates that the system detection capability is only limited by the perception of the T-sight user

b. The dotted line indicates that NFR's programming language can be used to extend its detection capabilities.

the detection capabilities mapped onto a simple protocol stack.

Table 6 presents a summary of all function aspects. Interoperability, adaptivity and capabilities are judged on a low-high scale. These values should be considered estimates and are not calculated using scientific methods. Rather, they are based on “feeling” gained by reading publicly available product documentation.

Functional aspects						
Product	**Granularity of data processing**	**Source of audit data**	**Response to detected intrusion**	**Degree of interoperability**	**Adaptivity**	**Detection capabilities**
RealSecure	Realtime	NW/H	Active	Medium	High	High
Intruder Alert	Realtime	NW/H	Active	Medium	High	High
Net Ranger	Realtime	NW	Active	Medium	Medium	High
Stake Out I.D.	Realtime	NW	Passive	Low	Medium	High
Kane Security Monitor	Realtime	H	Passive	Low	Medium	Medium
Session Wall-3	Realtime	NW	Active	Medium	Medium	High
Entrax	Realtime	H	Active	Low	High	Medium
CMDS	Realtime	H	Active	Low	High	Medium
SecureNet PRO	Realtime	NW	Active	Low	High	High
CyberCop	Realtime	NW/H	Active	Medium	High	High
INTOUCH INSA	Realtime	NW	Active	Low	Medium	Medium
T-Sight	Manual	NW	Passive	None	-	-
NIDES	Realtime	H	Active	Low	Medium	High
ID-Trak	Realtime	NW	Active	Low	Medium	Medium
SecureCom Suite	Realtime	NW	Active	Medium	High	High
PolyCenter	Realtime	H	Active	Low	Medium	Low
Network Flight Recorder	Realtime	NW	Active	Low	Medium	High

TABLE 6. Summary of functional aspects

4.2 Security aspects

4.2.1 Security

The security of an IDS is a complex variable that depends on a number of different parameters. One of the most important requirements is the ability of the IDS to maintain an expected level of service despite the presence of attacks. Mechanisms for protecting the availability and integrity of the IDS are necessary to meet that requirement.

Few of the vendors discuss these issues, probably because they fail to meet the necessary requirements. However, there are some products that do have mechanisms to protect the system from attack.

The following six subsections highlight some important security requirements relevant for IDS:

Confidentiality of audit data. Most current IDS use a series of components to provide collection, analysis and storage of audit data. In a distributed environment, the analysis of audit data requires input from hosts distributed throughout the network. Depending on the security policy of the domains, collecting audit data from these distributed hosts may violate the confidentiality requirements of the policy. An intrusion in a strategic IDS component may lead to disclosure of classified information originating from distributed hosts. All distributed systems analyzed follow the CIDF architecture presented in Figure 1 on page 5. Thus, one should carefully select audit logs that can be made visible to the IDS. In some cases, simple anonymization of audit logs may be a viable solution to the problem.

Integrity of audit data. Raw input data are the basis for all analysis in a search for intrusions. Hence, an intruder violating the integrity of the audit data may seriously affect the detection capability. Even the most advanced IDS will fail to meet its operational requirements if the integrity of audit data has been violated.

Audit data are usually protected using encryption between the managers and the agents. Thus, encryption of sessions are commonly used to address this problem.

Confidentiality of the detection policy. The detection and response policy of an IDS reflects the corporate security policy. A malicious adversary gaining access to the detection policy may use that information to circumvent existing security measures. This is possible since he (or she) may find attacks that are not part of the detection policy in practice. Therefore, the confidentiality of the detection policy is of the greatest importance.

Integrity of detection policy. The detection policy states which activities are considered intrusions and which are not. Hence, manipulation of the detection policy may cause the IDS to fail in detecting an intrusion. Therefore, the detection policy should be protected against unauthorized alteration, deletion and insertion.

Protection of response mechanisms. Integrity and availability are important aspects of response communication. When a response has been decided upon, it must be protected from interference. If an intruder is able to delete or alter this communication he can potentially stop the IDS from carrying out responses as a result of detected policy violations.

The IDS must also be protected from unauthorized response initialization. If an attacker finds a way to trick the system into responding to non existing intrusions, this can potentially, depending on the configuration of the responses, cause considerable damage to the availability of the target system.

Availability. An intrusion detection system designed to operate in real-time must process its input, raw input events, at the same speed as it is generated. As computers and networks become faster, we can process more raw input events per time unit. However, at the same time, computers or networks produce raw input events at a much higher rate. The performance of an IDS is, thus likely to remain an issue for some time to come. If the IDS is not able to keep up with its input flow, the SSO should be notified. An attacker can use this performance limitation to escape the detection of an intrusion by flooding the IDS with input data. This would be a denial-of-service attack aimed at the functionality of the IDS.

The requirements above can be fulfilled using different security services and mechanisms. Encryption, application- and operating system access-control are the most commonly used ways to ensure the integrity, confidentiality and availability of the systems.

Encrypted communication channels. The communication channels between the management console and the distributed data collectors (or agents) are among the channels it is most important to protect. An adversary that has control over data flowing between entities may delete or alter audit records, thus affecting the availability of the IDS. RealSecure, Intruder Alert, Entrax, CyberCop, KSM, CMDS, Session Wall 3, StakeOut and SecureNet PRO claim to support encrypted channels between manager and agents. NetRanger uses “fault-tolerant protocols” which address only the secure delivery of packets between sensors and the director. It does not provide encryption. NetRanger (and other systems not supporting encryption) relies upon router-to-router IPSEC encryption for that purpose. An option would be to create a separate management network for this purpose. Although this may benefit security, it may be costly in heavily distributed environments.

Heartbeat functions. The absence of security events normally means that no intrusions or intrusion attempts are taking place. In a hostile environment in which the distributed agents may be under attack, the absence of audit records may also mean that the agents are being prevented for some reason from delivering those events. For example, denial-of-service attacks toward the agents may degrade or completely block the delivery of events. For this purpose, a heartbeat function may be useful. It ensures that the communication between the manager and agents is working properly by sending heartbeat messages at regular intervals. Once the heartbeats of an agent stops, the manager can assume that the agent is no longer capable of delivering security events, which may indicate that the agent is under attack.

RealSecure, Intruder Alert, CyberCop and NetRanger are the only products with documented heartbeat functionality.

Stealth behavior. Every network component having a valid IP-address (or even an Ethernet MAC-address) are more or less susceptible to attacks. A stealth system listens only to the network traffic (passively) without using an IP-address (or MAC-address) Stealth behavior applies only to network-based systems. In distributed environments, where audit logs must be transferred from agents to a manager, stealth behavior is not possible unless an exclusive management network exists for that purpose.

NetRanger and RealSecure have the capability to operate in stealth mode and thus having no IP-address. In that case, communication between the manager and agents is accomplished using a second network adapter card.

Access control. Configuration parameters, alarms and other sensitive information can be held confidential and integrity protected using access-control. At the system level, this is ensured by the underlying operating system security mechanisms. Some systems, such as NetRanger and INTOUCH INSA, use dedicated hardware provided by the IDS vendor. Non standard hardware and software usually make life harder for hackers and other evil minds seeking to breach the security of a system. At the ID application level, many systems provide controlled access for SSO and other users. See also section 4.5.2.

Weaknesses of network-based systems. Recent research has disclosed some serious security flaws in network-based intrusion detection systems. A report by Ptacek and Newsham [3] shows that differences in the implementation of TCP/IP stacks between the IDS and the target hosts may have serious consequences. By exploiting these differences, packets can be created that are interpreted differently by the IDS and the target hosts. This enables an attacker to perform insertion or evasion of data into the protocol stack of the IDS, which in turn could reduce the IDS capability of detecting ongoing attacks.

In the report, Real Secure, NetRanger, Session Wall, and Network Flight Recorder are shown to be vulnerable to such attacks. However, there is nothing to indicate that other network-based ID systems would be resistant to insertion and evasion of data.

4.3 Architectural aspects

4.3.1 System organization

Virtually every system can operate in a distributed environment. Only INTOUCH INSA and T-Sight are limited to a single host or network segment. Intruder Alert (IA) is partly distributed. While the host-based IA can operate distributed under centralized control, its network-based system (NetProwler) cannot. For further discussions of distributed management models, see section 4.5.4.

4.3.2 System and network infrastructure requirements

Operating systems. Despite the market trend to migrate applications to Windows NT, a surprisingly number of ID systems operate in various UNIX environments. Table 7 contains a summary of the operating system requirements for the manager and agent side for each IDS. It is worth mentioning that Axent supports an impressive number of operating systems for Intruder Alert.

Network technology. As expected, TCP/IP is the dominating protocol suite supported. Table 8 gives a summary of network technologies supported by each product.

Architectural Aspects - Operating systems		
Product	**Operating system Manager side**	**Operating system Agent side**
RealSecure	Solaris, NT	NT, (Solaris)[a]
Intruder Alert	Solaris, AT&T/NCR SVR4, IBM-AIX, OSF/1, Digital/UNIX, HP-UX, IRIX, SunOS, Novell, NT	Solaris, AT&T/NCR SVR4, IBM-AIX, OSF/1, Digital/UNIX, HP-UX, IRIX, SunOS, SVR Motorola 88000, Novell, NT
Net Ranger[b]	HP/UX, Solaris 2.6	Solaris x86 v2.6[c]
Stake Out I.D.	Solaris	Solaris
Kane Security Monitor	NT	NT
Session Wall-3	NT, W95/98	NT, W95/98

TABLE 7. Operating system requirements

Architectural Aspects - Operating systems		
Product	**Operating system Manager side**	**Operating system Agent side**
Entrax	NT	NT, UNIX[d]
CMDS	Solaris	Solaris, NT
SecureNet PRO	Solaris, FreeBSD(x86), Linux(x86), BSDi(x86)	Solaris, FreeBSD(x86), Linux(x86), BSDi(x86)
CyberCop	Solaris, NT	Solaris, NT
INTOUCH INSA	Digital Unix (Alpha)[e]	Not applicable[f]
T-Sight	WIndows NT	-”-
NIDES	SunOS	SunOS
ID-Trak	NT	NT
SecureCom Suite	Solaris, NT	Solaris, NT
PolyCenter	SunOS, OpenVMS	SunOS, OpenVMS
Network Flight Recorder	Java based user interface[g]	BSD/OS (x86), FreeBSD (x86), HP-UX,OpenBSD(x86),Solaris, NetBSD (x86), RedHat Linux (x86), Slackware Linux (x86), Debian Linux (x86)

TABLE 7. Operating system requirements

a. Host-based agent is available only for NT. A Solaris version is expected in an upcoming release
b. Also requires HP OpenView run time license and preferably a database manager
c. Uses dedicated hardware and a customized Solaris version
d. No specific UNIX versions specified
e. Uses dedicated hardware (Alpha server)
f. Centralized system
g. Will run on any operating system supporting one of the following web browsers: Microsoft Internet Explorer 3.02 or higher, Netscape Communicator 4.0 or higher, Netscape Navigator 3.01 or higher

Architectural Aspects - Protocols[a]		
Product	**Datalink layer protocol[b]**	**Network layer protocol**
RealSecure	Ethernet, FDDI, Token Ring	TCP/IP
Intruder Alert	Ethernet	TCP/IP, IPX/SPX
Net Ranger	Ethernet, FDDI, Token Ring	TCP/IP
Stake Out I.D.	Ethernet	TCP/IP
Kane Security Monitor	-	TCP/IP, Named Pipes
Session Wall-3	Ethernet, FDDI, Token Ring	TCP/IP
Entrax	-	-
CMDS	-	-
SecureNet PRO	Ethernet	TCP/IP
CyberCop	Ethernet	TCP/IP
INTOUCH INSA	Ethernet	TCP/IP

TABLE 8. Requirements of datalink- and network layer protocols

Architectural Aspects - Protocols[a]		
Product	Datalink layer protocol[b]	Network layer protocol
T-Sight	Ethernet	TCP/IP
NIDES	Ethernet	TCP/IP
ID-Trak	Ethernet	TCP/IP
SecureCom Suite	Ethernet, FDDI, Token Ring	TCP/IP
PolyCenter	-	-
Network Flight Recorder	Ethernet	TCP/IP

TABLE 8. Requirements of datalink- and network layer protocols

a. In the case in which datalink layer protocol or network layer protocol is not specified, Ethernet and TCP/IP is assumed.

b. The Datalink layer access point is often provided by the underlying operating system. This column only lists the protocols that were explicitly mentioned in the documentation.It is possible (or likely) that some products may support other protocols accessible through the operating systems' datalink provider interface.

4.4 Operational aspects

4.4.1 Performance aspects

Communication overhead. Few of the analyzed systems specify the communication overhead induced by deploying intrusion detection. For network-based intrusion detection, the overhead is caused by the distribution of audit data and the communication between the various subsystems of the IDS. For RealSecure, ISS reported a network load overhead of 5-10%

Computational overhead. Computational overhead applies mainly to host-based IDS. While network-based ID systems usually run on a dedicated system, host-based IDS execute and collect audit data on the target they monitor. The performance penalty depends greatly on such parameters as granularity of data processing, size and growth rate of system logs, size and complexity of the ID rulebase etc. Owing to these uncertainties, it is impossible to give an estimate of the overhead. However, it is important to understand that all host-based ID systems will cause a computational overhead on the target system. Centrax report that their product, Entrax, typically degrades host performance by less than 2%. Axent reports a typical host load of less than 5% for their Intruder Alert.

4.5 Management aspects

Management of a system for intrusion detection is crucial for efficient deployment in corporate network infrastructures.

4.5.1 Configuration management

Configuration management provides functions to exercise control over, identify, collect data from and provide data to entities that are part of the IDS. For the purpose of intrusion detection, configuration management includes management of the detection capability and the corresponding response mechanisms used.

All systems support some form of configuration management.

4.5.2 Security management

Access security. An SSO should be allowed only be allowed to manage those domains belonging to his jurisdiction. It should also be possible to define different management views for different SSOs.

Audit trails and security alarms. An SSO with limited access rights may be granted access to view audit trails and security event information. Security alarms may indicate an attempted attack against a target system or against the IDS itself. It should be possible to define access rights to audit trails and security alarms.

Real Secure, Intruder Alert, Net Ranger, Session Wall 3 and CyberCop have documented support for controlling access to configuration parameters and alarms.

Security of management. Management operations must be protected to prevent an intruder from accessing information or controlling IDS resources. Security of management for IDS includes:

Authenticity. All management operations must be proceeded by a proper identification and authentication of the managing entity. A managing entity may be a human user or a system entity.

Integrity. All management operations must be protected against integrity attacks. It should not be possible to insert, delete or alter a management operation.

Confidentiality. All management operations must be protected against confidentiality attacks. It should not be possible to deduce the semantic meaning of any management operations (e.g. by wiretapping or placing sniffer attacks). Confidentiality of management operations is of special importance for security management operations and detection policy management.

Availability. Management of the intrusion detection system must be possible even when the IDS malfunctions. An attack against the network infrastructure, the IDS itself or the monitored target must not affect the availability of the management service.

Most products covered in this review use the same communication channel for both manager and data transfer. Thus, a protected link between the manager and its agents also provides protection for management operations. Unfortunately, this has an effect on the availability of the management service. In section 4.2.1, security of these communication links are discussed.

Protection of the availability of the management service can be enforced in many different ways. The use of heart beat functionality is one commonly used method (see section 4.2.1).

4.5.3 Management interfaces

Interoperability between components from different vendors usually requires some form of standardized (or common) communication interface. For management, a standardized interface would allow a site to design and create an ID capability using standard components from different vendors. For example, using SNMP for management, would allow a site to integrate the IDS into their existing HP OpenView environment. Currently, Net Ranger is the only product that is fully integrated into a management application (HP Openview). This enables the SSO to manage the entire IDS within the existing management environment. In addition, alarms are presented in the same environment (see section 4.1.3). Intruder Alert and RealSecure can be extended to cooperate with HP Openview. In addition, Intruder Alert has support for Patrol from BMC.

4.5.4 Management model

Centralized control and management are essential for successful deployment of intrusion detection, especially in distributed environments in which a larger number of ID components may be utilized. It should be possible to define a hierarchy of manager-agent relationships so that a single management operation is applied to the whole range of distributed components. For example, a change in access-rights for a SSO should need to be applied only once, even in heavily distributed ID systems having a large number of components. The following relationships have been identified:

Many-to-Many. Several management consoles can manage many distributed agents.

One-to-Many. One management console can manage many distributed agents

One-to-one. One management console can manage a single agent.

Real Secure, Intruder Alert, Net Ranger and SecureNet PRO are examples of a many-to-many relationship. Net Ranger also supports construction of hierachial management relationships, where a tree of managers and agents can be managed from a single, higher level manager. ID-Trak, Poly Center, KSM, CMDS and CyberCop support one-to-many relationships. NFR and NIDES' flexible architectures make it hard to categorize them according to the management models above. The remaining systems not mentioned above lack information regarding the management model.

5. Conclusions

The role of IDS in corporate security infrastructures. In recent years, there has been a dramatic increase in the use of security services such as firewalls. A common belief is that, once a firewall is installed, all security problems are solved. Of course, this is not the case, in contrast to what certain market forces lead us to believe. The same enthusiasm can be found among advocates of intrusion detection systems. However, it is important to understand that intrusion detection systems are not a substitute for other security services such as firewalls, authentication servers etc. They should be regarded as a complement to other security services that further extend the level of protection of the target systems, resources or information.

Host-based versus network-based IDS. IDS began as a technology for analyzing host-based audit data. In recent years, network-based systems have appeared and extended the capabilities of intrusion detection systems. This survey shows that the majority of the commercial ID systems are network-based systems. In fact, nine of 17 are network-based whereas only five are purely host-based. However, the increasing use of encryption in network infrastructures such as IPSEC seriously limits the IDS ability to access network-based audit data. This limitation may mandate a second shift towards analysis of higher layer protocols for the purpose of intrusion detection. Further, the need for efficient deployment of intrusion detection for security services such as firewalls, authentication services, directory services etc. requires the IDS to access information generally not visible to network probes. Examples of such information are processes, threads, internal datastructures and security logs of the target host. It is the author's belief that host-based intrusion detection systems will become increasingly popular because of these circumstances. Possibly, hybrid systems (host-based with limited network visibility) will emerge.

Security of IDS. The security of current commercial ID systems is questionable. Although encryption is used to protect communication links between different components, it is unclear how the information contained in the IDS is protected as a whole. For example, how is the company security policy protected from disclosure if a malicious adversary manages to penetrate one of the components of the IDS? The development of a formal security model for IDS could provide a basis for improvements in the security of future products.

Lack of modularity and interoperability. The modularity of current commercial systems leaves much to be desired. Most often, there are no clear boundaries between raw input event collection, detection and response functions. This seriously limits the versatility of the IDS as it does not allow an ID capability to be built using components from different vendors. One of the best examples of this is databases containing known intrusions. Each vendor provides his own proprietary database which cannot be used by other products. In fact, the proprietary databases create a competitive edge toward other vendors. Therefore, it is not likely that an initiative leading to interoperability between intrusion databases would come from a major vendor. The research community and small vendors trying to break the market dominance are more likely to take on such a task. A paper by Lindqvist et al [5] proposes an intrusion data library enterprise to address these problems.

Background of vendors. In the information age of today, the boundaries between software applications and network technologies are fading away. Traditional software vendors are providing applications and services tightly coupled with network infrastructures. A good example of this is IP telephony. At the same time, traditional network element providers are seeking to broaden their portfolio by delivering software packages to assist their traditional range of products. As a result, both parties fall into the pitfalls of each other's traditional domains. It appears that the commercial intrusion detection systems of today are an example of this. An intrusion detection system is an advanced piece of software requiring great software engineering and programming skills to design and create. On the other hand, an IDS is also a high-performance network component with extremely high availability and dependability requirements. As most office PC users are painfully aware, availability and dependability are not part of the vocabulary of software vendors. It is the author's belief that most

ID systems originate from traditional software vendors rather that from network infrastructure vendors. Most of today’s IDS are not yet mature enough for large scale, enterprise wide deployment.

6. References

[1] S. Axelsson, “Research in Intrusion-Detection Systems: A Survey”, Chalmers University of Technology TRxxx, 1999.

[2] M. Crosbie and K. Price, “Intrusion Detection”, COAST Laboaratory, Purdue University; http://www.cs.purdue.edu/coast/intrusion-detection/ids.html (Last visited september 17, 1999)

[3] T. H. Ptacek, T. N. Newsham, “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection”, Secure Networks, Inc.

[4] S. Kent, R. Atkinson, RFC2401 - “Security Architecture for the Internet Protocol”, Available at http://www.ietf.org (Last visited september 17, 1999)

[5] U. Lindqvist, D. Moran, P.A. Porras, and M. Tyson. "Designing IDLE: The intrusion data library enterprise." Abstract presented at RAID’98 (First International Workshop on the Recent Advances in Intrusion Detection), Louvain-la-Neuve, Belgium, September 14–16, 1998.

[6] S. Staniford-Chen, B. Tung, and D. Schnackenberg, “The Common Intrusion Detection Framework (CIDF)”. Position paper accepted to the Informatio Survivability Workshop, Orlando FL, October 1998.

[7] H. Debar, M. Dacier, A. Wespi, “Towards a Taxanomy of Intrusion-Detecton Systems”, IBM Research Division, Zurich Research laboratory, 1998.

[8] Internet Security Systems (ISS), RealSecure, http://www.iss.net/prod/rs.php3 (Last visited august 22, 1999)

[9] Axent Technologies Inc, Intruder Alert, http://www.axent.com/product/smsbu/ITA/default.htm (Last visited august 22, 1999)

[10] Cisco Systems Inc, Netranger, http://www.cisco.com/warp/public/cc/cisco/mkt/security/nranger/index.shtml (Last visited august 22, 1999)

[11] Harris Communications Inc, Stake Out I.D, http://www.commprod.harris.com/network-security (Last visited june 17, 1999)

[12] Security Dynamics, Kane Security Monitor, http://www.securitydynamics.com/products/datasheets/ksmds.html (Last visited august 22, 1999)

[13] AbirNet, Session Wall-3, http://www.abirnet.com/swoverview.html (Last visited august 22, 1999)

[14] Centrax Corporation, Entrax, http://www.centraxcorp.com/products.html (Last visited august 22, 1999)

[15] Science Application International Corporation (SAIC), CMDS, http://cp-its-web04.saic.com/satt.nsf/5e06b1c4626c490d8825674a007eb460/dd58da9a34f5479b882566ba0058e37e/$FILE/Proctor.pdf (Last visited august 22, 1999)

[16] MimeStar Inc, SecureNet PRO, http://www.mimestar.com/html/data_sheet.htm

(Last visited august 22, 1999)

[17] Network Associates Inc, CyberCop, http://www.nai.com/asp_set/products/tns/ccmonitor_intro.asp (Last visited august 22, 1999)

[18] Touch Technologies Inc, INTOUCH INSA, http://www.ttisms.com/tti/nsa_www.html (Last visited june 17, 1999)

[19] EnGarde Systems Inc, T-Sight, http://www.engarde.com/software/t-sight/overview.html (Last visited august 22, 1999)

[20] SRI International, NIDES, http://www.sdl.sri.com/intrusion (Last visited june 17, 1999)

[21] Internet Tools Inc (Aquired by Axent Tecnologies), NetProwler (formerly ID-Trak), http://www.axent.com/iti/netprowler/idtk_ds_word_1.html (Last visited august 22, 1999)

[22] ODS Networks, SecureCom suite, http://www.ods.com/products/product.htm?product=6000SecureSwitch&label=Security+Products (Last visited august 22, 1999)

[23] Compaq (formerly Digital Equipment Inc), PolyCenter, http://www.digital.com/info/security/id.htm (Last visited august 22, 1999)

[24] Network Flight Recorder Inc, Network Flight Recorder (NFR), http://www.nfr.net/products/ida-facts.html (Last visited august 22, 1999)

A Introductory overview of the intrusion detection systems

A.1 RealSecure

Product	**RealSecure**
Vendor	Internet Security Systems (ISS)
Platforms	Solaris (Sparc and x86), Windows NT
Data source	Host and network-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.1.1 Introduction

RealSecure is a network and host-based intrusion detection and response system that operates in real-time. It uses predefined attack and misuse signatures to detect activities that violate the stated security policy.

A.1.2 Architecture

RealSecure consists of three main components:

- RealSecure Engines
- RealSecure Agents
- RealSecure Manager

A.1.2.1 RealSecure Engines

The RealSecure Engines runs on dedicated hosts and captures and analyses network packets. The packets found on the network are compared against its attack signature database which (hopefully) uniquely identifies an undergoing attack.

The internal architecture of the RealSecure engine has five components:

- Network interface
- Packet Capture Module
- Filter Module
- Attack recognition Module
- Response Module

Network Interface. The network interface provides the physical and media access to the network being monitored. A number of different network topologies are supported such as Ethernet, Fast Ethernet, FDDI and Token-ring.

Packet Capture Module. The packet capture module is responsible for the collection and queuing of packets to be processed by RealSecures other modules. On Windows NT this is implemented as a network service. The Solaris implementation uses the Data Link Provider Interface (DLPI) to perform this task. DLPI is a streams-module for accessing the datalink network layer and is more or less standard on most SYSV unix systems.

Filter Module. The responsibility of the filter module is to limit the number of packets passed on to the *attack recognition module (ARM)*. ISS states that approximately 20% of the packets found on the network are of interest to the ARM.

Attack Recognition Module. The attack recognition module handles packet passed on by the filter module. It reassembles sessions and searches for indications of suspicious activity. RealSecure ships with a set of attack signatures, although it is possible to define new or fine-tune existing attack signatures.

Response Module. Depending on the nature of the attack, RealSecure may respond differently. A severe attack may require that the system respond by terminating sessions or services, reconfiguring firewalls etc. A less severe attack may only mandate that the event is logged and brought to the attention of the site security officer (SSO).

RealSecure offers a number of response options for a given event:

- Logging a summary of the event to a persistent storage. Thin may include information such as event name, source and destination IP, source and destination ports etc.
- Logging of the entire binary content of a session.
- Kill/Terminate the associated session. This is performed by sending spoofed TCP-reset messages to each communicating party.
- Reconfigure a CheckPoint Firewall-1 to reject future traffic from a specified source address for a period of time. ISS plans to expand this functionality into an application programming interface (API) that can be used to dynamically update firewalls and routers from other vendors.
- Generate SNMP traps containing information about the event occurred. This is useful in an environment where SNMP-based management tools are being used to manage the operation of the network.
- Send alarms to a Lucent Managed Firewall Security Management Server (SMS).
- Send E-mail notifications about events.
- View (binary) contents of a session in real-time.
- Execute specified programs/applications to perform user-specified/site specific tasks.

A.1.2.2 RealSecure Agents

The agents are the host-based counterpart of engines. They analyses host logs in a similar manner as the RealSecure Engine analyses network packets. Once an attack is detected the agent has the capability to terminate processes or disable user accounts. The RealSecure agents can also reconfigure engines and firewalls to prevent/block future intrusions/attacks. Currently, the agent software is only available for Windows NT platforms. However, ISS claims that agents for Solaris will soon be available.

A.1.2.3 RealSecure Manager

The RealSecure manager is a management console that gives the SSO a single view of the entire system of engines and agents. The console provide three basic services:

- Central real-time alarm display
- Central data management
- Central engine configuration

Central real-time alarm display. The central real-time alarm display lets the SSO view all threats and activities in the network and hosts.

Central data management. Databases from engines and agents are collected and stored into a single data store. Data can be exported to enterprise database systems and the built-in report system can generate reports from this database. RealSecure has a set of pre-defined reports, although user-defined reports can be generated.

Central engine configuration. The configuration of every engine in the network can be adjusted from the RealSecure manager.

A.2 Intruder Alert

Product	**Intruder Alert**
Vendor	Axent Technologies, Inc.
Platforms	Solaris (Sparc), SunOS, Windows 95/NT, NetWare, AIX, Digital Unix, HP-UX, IRIX, SVR4 (Motorola 88000), AT&T GIS (NCR), OpenVMS
Data source	Host and network-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.2.1 Introduction

Intruder Alert is a real-time, rule-based intrusion detection system. It monitors audit trails from hosts throughout a distributed environment. Detection of intrusion attempts and intrusions are based on *rules* and/or *exceptions*. The rule based detection engine look for specific pre-defined sequences of data. These sequences are called “footprints” and uniquely identifies anomalous behavior/patterns in the audit trails.

The exception based model detects behavioral anomalies within the system. Normal behavior is filtered out, leaving the anomalies for further investigation. Intruder Alert also provides a number of automated response options such as e-mail, pager notifications and session termination.

A.2.2 Architecture

Intruder Alert consists of three main parts:

- •Interface console
- •Manager
- •Agents

Interface console and manager. The interface console and manager let the SSO configure the rules according to the site security policy. Although Intruder Alert managers and agents are supported on numerous platforms (including UNIX), the interface console and manager only runs on Windows NT/95.

Agents. The agents are processes and daemons running on the hosts under surveillance. The agents collects audit data and apply a rule set as configured by the SSO. All agents must be registered to a manager before they can be configured. During the register phase, a secure communication channel is set up to protect data exchanged by the communicating parties.

A.2.2.1 Intruder Alert Domains

Intruder Alert domains are groups of agents/hosts that report to the same manager application. Domains can be organized in a number of ways. For example, a site may have domains organized by application, operating systems or geographical boundaries of the system/hosts.

A.2.2.2 Intruder Alert Policies

Every Intruder Alert domain define a set of rules that reflects the security policy of the site. These set of rules are called *policies* and are categorized into four parts:

- •Drop & Detect Policies
- •Detect and respond Policies
- •Custom-configurable Policies
- •Carte Blanche

Drop & Detect Policies. Intruder Alert ships with a set of predefined “footprints” that can be immediately activated upon installation of the system. Since new attacks are constantly published and exploited, Axent Technologies provides a “swat-team” that publishes “footprint” updates. These policies can be downloaded (for a charge) from their web-site and “dropped” into the system.

Detect and respond Policies. Detect and respond policies are pre-configured policies that requires some customisation. For example the address to a web site to monitor or what countermeasure a certain event should generate.

Custom-configurable Policies. Policies can be tailored to meet specific needs of a site. Depending on the nature of the policy and the skill of the user, these custom made configurations can be made by the user or in cooperation with Axent's security consultants.

Carte Blanche. The last and most advanced approach is to define the policy starting with a blank piece of paper. This means that none of the pre-configured policies are used. This would require great expertise and experience and cannot be recommended for most sites.

A.2.2.3 NetProwler

In addition to the host-based audit data analyses, Intruder Alert can analyze packets from the network. This is actually performed by separate product. It collects data by putting the network interface card into "promiscuous mode" which allow the agent to capture packets destined to other addresses than the agent itself. Axent Technologies call this "Net*Prowler* technology". NetProwler is based on another product, ID-Trak. Recently, Axent Inc. aquired Internet Tools Inc., owner of ID-Trak. ID-Trak's stateful signature inspection technologi (SDSI) will strengthen the network-based detection capabilities of Intruder Alert. A strength of NetProwler is its capability to access data at the datalink layer. It is therefore possible to define attack recognition signatures for other protocols than IP. Currently, the host-based and network-based modules operate independent of each other. Both configuration and displaying of alarms uses separate consoles. However, using SNMP, alarms from NetProwler can be sent to the IA manager. In future releases of IA, a higher degree of integration of the two will be provided. Currently, NetProwler is only available for the Windows NT platform.

A.2.2.4 Intruder Alert module for PATROL

Organisations having large networks and a large number of hosts often use some kind of network/host management application to reduce the administrative costs of management. Concerning security, two types of management apply. *Security of management* means that the management operation itself must be secure and that only authorized parties may perform management operations. *Management of security* means that the system security parameters can be managed just as any other system parameter in the network or on a host.

PATROL, from BMC Software is a management suite that can be used to manage a large number of hosts in a distributed environment. Intruder Alert can operate with PATROL in several ways:

Management of security for Intruder Alert. PATROL can be used to remotely manage the Intruder Alert configuration. One of the main advantages of this solution is that system managers are offered a single management environment that can be used to perform management operations on both hosts and the Intruder Alert software itself.

Security of management for Intruder Alert. SNMP is widely used management protocol. Intruder Alert can monitor SNMP traps from applications such as firewalls, routers and management applications. Rules can be defined to detect suspicious management operations.

Homogenous management console. Alarms and events generated by Intruder Alert can be sent to the PATROL management environment. This let the system managers treat security alarms just as any other alarm using a single management view.

A.3 NetRanger

Product	**NetRanger**
Vendor	Cisco Systems, Inc
Platforms	Dedicated hardware and Solaris x86 v.2.6
Data source	network-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.3.1 Introduction

The NetRanger is a real-time intrusion detection system biased towards detecting attacks on the network infrastructure. It is purely network-based intrusion detection system and it analyses both headers and payload of the packets found on the network. A misuse model of intrusion is used to find policy violations. NetRanger also has real-time response capabilities which may terminate current sessions and block further intrusion attempts.

A.3.2 Architecture

NetRanger has three fundamental components:

- Sensors
- Director
- Post office

The system architecture of NetRanger is one of its greatest strength. Sensors and directors can form hierarchies, which allow monitoring of large numbers of network segments.

A.3.2.1 Sensors

The sensors of the system are the devices that listens to the network traffic and collect information. Normally, one sensor monitors a single network segment. An expert system is used to reduce the network traffic into relevant security events. String matching signatures can be defined to look for suspicious behavior. For example, a user could define a signature matching a specific word such as “confidential” or “proprietary”. NetRanger can also scan Cisco routers syslogs for security policy violations .

In the current product release sensors are available for Ethernet, Fast Ethernet, Token Ring and FDDI.

In the event of a security policy violation, the sensors can respond by killing active TCP-sessions or dynamically update the access control lists (ACL) of a router or firewall.

Unauthorized events (attacks) are categorized as follows:

Named attacks. Named attacks are the ones that usually are given a name. For example SYN-attack, SMURF-attack and LAND-attack are such attacks. They are usually distributed through various web-sites and news-groups on the Internet and the exploits can normally be used by quite unexperienced attackers.

General Category attacks. The General Attack Category include attacks that in some way violate the IP-protocol suite. For example fragmented packets with overlapping offsets or packets containing out-of-band data. Note that many of the Named Attacks can also be put under this category. For example the Teardrop attack is based on out-of-band data. This category has the strength to detect new types of attacks or variations of existing attacks.

Extraordinary attacks. The Extraordinary attack category look for attacks with a much more complex structure. For example illegal sequences of packets such as IP-hijacking and E-mail spam.

A.3.2.2 Director

The Director provides central management of sensors distributed throughout the network. From the Director, the SSO may monitor and manage the sensors and analyze the (lack of) security of the system. The Director are also used to export data to reporting systems and to download/create new attack-signatures.

A.3.2.3 Post office

The communication between directors and sensors are handled by the *Post Office.* The Post Office uses a UDP-based application protocol with features for authentication and fault tolerance. The addressing scheme of directors and sensors are based on a three-part address including organization, host and application. Features for fault-tolerance include heart-beat messages and alternate routes for messages. Up to 255 alternate routes can be specified and the Post office automatically switch route if the current route fails. For redundancy, sensors can distribute their messages to more than one Director.

A.4 Stake Out I.D.

Product	**Stake Out I.D.**
Vendor	Harris Communications, Inc.

Platforms	Solaris (Sparc)
Data source	network-based
Model of intrusion	Rule and anomaly based detection model
Behaviour	Detection

A.4.1 Introduction

Stake Out is a network oriented intrusion detection and surveillance system specializing in logging and tracking intrusive subjects as they penetrate the network. It monitors the activity on the network by observing the packets on the local network segment. Stake Out examines the packets looking for “learned” patterns to detect suspicious or potentially malicious behavior. The packets are compared against a catalog of known patterns. If a match is found, extensive logging and surveillance can be activated providing an “evidence log” of the intrusion.

In addition to the pattern matching capabilities, network specific characteristics is learned over time providing an anomaly based detection scheme. Characteristics such as time of day, number of packets, type of packets, source and destination of packets are analyses using artificial intelligence technology (AI). Every packet or sequence of packets that deviates form “normal” behavior activates the alert notification, evidence collection and incident analysis systems.

Stake Out I.D. is available in two versions: Stake Out I.D Workstation and Stake Out I.D. Enterprise. Stake Out I.D Workstation monitors traffic on a network segment, suitable for small networks. Stake Out I.D. Enterprise is for larger companies with large wide-area networks.

A.4.2 Architecture

The architecture of Stake Out has five major components:

- Network Observation
- Intrusion Detection
- Evidence logging
- Alert Notification
- Incident Analyzer/Reporter

Network Observation. The network observation module collects data from the network and feeds it into the Intrusion detection module. Observation modules can only collect data from TCP/IP based networks.

Intrusion Detection. Using a combination of pattern databases and artificial intelligence, the intrusion detection module searches the system for potentially malicious behavior.

A pattern database containing predefined patterns are used to find malicious patterns on the network. The current release of Stake Out I.D. does not allow the SSO to write customer customized patterns. If a packet or a sequence of packets matches a known pattern, extensive logging and surveillance can be activated.

Artificial intelligence is used to analyze network specific characteristics found on the network. A database containing “normal” behavior is built over time and is used to find network operations that is deemed outside of normal tolerances.

In the event of a possible intrusion, Stake Out I.D.creates a datastructure containing date/time stamps, source and destination IP and an event identifier. This datastructure is passed to the Alert Notification module for further processing.

Evidence Logging. Intruders often try to cover their tracks by removing system logs. Stake Out I.D. records the activities after an intrusion is detected. These recordings serve as evidence logs provides reliable data for determining appropriate response activities, such as restoring lost data, removing unauthorized applications, or terminating network routes. Note that Stake Out I.D. does not have automated responses like termination of sessions or automatic network element reconfigurations. An alarm is sent and evidence logging is activated, but the response must be performed manually by the SSO.

If the attacker initiates a secondary attack within the system, the Incident Analyzers will collect all network traffic between the attacking system and the new target. This gives the SSO a chance to “follow” an attacker as he/she jump from node to node in the network.

Alert Notification. Immediately after a detected intrusion attempt, characteristics of the attack scenario gets encapsulated and time stamped. Alert messages can be sent to the regular system console or to other network management applications such as HP Openview and Sun Netmanager. SNMP trap PDUs are used for that purpose. DES encryption can be used to protect the content of the SNMP PDUs.

Incident Analyzer/Reporter. All security related events are written to log files. The Event Log Analyzer will continuously attempt to recognize events and assign event-identifiers to them. Once identified, the event is brought to the attention of the SSO using the standard console or snmp-based network management system.

A.5 Kane Security Monitor

Product	**Kane Security Monitor**
Vendor	Intrusion Detection, Inc (Subsidiary of Security Dynamics)
Platforms	Windows NT
Data source	host-based
Model of intrusion	Rule and anomaly based detection model
Behavior	Detection

A.5.1 Introduction

Kane Security Monitor (KSM) is a host-based intrusion detection system for the Windows NT environment. It collects system security logs from the hosts of the network looking for certain activities and patterns. An artificial intelligence engine (ShadoWare) is used for the analysis of the logs. Misuse “patterns” are also used to find suspicious and unauthorized activity. Examples of patterns that are provided include:

- Failed Login Attempts
- Failed File Access Attempts
- Browsing & Curious Users
- Denial of service
- Excessive Privilege Granting
- Ghost IDs
- Masquerading users
- Password cracking
- Administrative ID Abuse
- Supervisor Abuse

Upon recognizing a pattern of misuse, the system can actively respond in customer-defined manner. For example sending alert messages to network management application using SNMP, E-mails or pagers.

A.5.2 Architecture

KSM consists of four main parts:

Monitoring Console. The monitoring console application runs on the SSO´s workstation used to manage and monitoring the entire system.

Collection Auditor and Alerting Engine. These two reside on the management station and are responsible for the collection of logs, analysis of logs and alarm reporting of security events.

Intelligent Agents. Intelligent Agents reside on the workstations and servers being monitored. Agents are registered to the Auditor as they are installed and configured. The communication between agents and the auditor is protected by some security mechanism, but the nature of these mechanisms is not known to the author of this document.

Agents can collect information from Windows NT – Security log, applications log and systems log.

A.6 SessionWall-3

Product	**SessionWall-3**
Vendor	AbirNet
Platforms	Windows 95/98/NT4/NT5
Data source	network-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.6.1 Introduction

SessionWall-3 (SW3) is basically a fancy network sniffer that scans the contents of the packets found, displays, logs, reports and alerts. “Unobtrusive” blocking is used to block inappropriate or unauthorized traffic based on a set of rules. SW3 runs on Microsoft Windows platforms and can process network traffic from one or more network interfaces. The interface types supported are Ethernet, Token Ring and FDDI. SW3 cannot collect network traffic from other sources in a distributed (agent) environment.

A.6.2 Architecture

The architecture of SW3 is quite simple. It is an integrated package running on a single host. The package provide:

- Network Usage Reporting
- Network Security
- WEB and Internal Usage Policy Monitoring and Controls
- Company Preservation

Network Usage Reporting. Ranging from high level statistics down to specific user usage.

Network Security. Includes content scanning, intrusion detection (service denial attacks, suspicious activity, malicious applets, viruses), blocking, alerting and logging.

WEB and Internal Usage Policy Monitoring and Controls. Used to monitor and enforce WEB access and inter-company policies by user id, IP address, domain, group, content, and control list.

Company Preservation. Monitoring e-mail content, logging, viewing and documentation.

The rule set used to detect suspicious behavior can be customized by the SSO New rules can be created or existing ones can be fine tuned. Automated active responses can be defined for events. Response mechanisms include session termination, E-mails, pagers etc. SW3 can also generate SNMP traps to send alerts and alarms to network management systems. It also has the capability to interface with a FireWall-1 using the OPSEC interface. This gives SW3 the power to block unauthorized hosts/users from accessing the target systems.

A.7 Entrax

Product	**Entrax**
Vendor	Centrax Corporation
Platforms	Windows NT, Agents for selected Unix platforms.
Data source	host-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.7.1 Introduction

Entrax is a host-based intrusion detection tool for distributed environments. Distributed agents collect audit data at the host and sends it back to a centralized manager station. A set of “activity signatures” are used detect find suspicious patterns in the audit logs. A data forensics reporting capability for damage assessment, trending, and attack anticipation focuses on identifying insider misuse and threats.

An active automated response capability provides response to alerts such as disabling user accounts, logging out a user, or shutting down a host.

A.7.2 Architecture

Entrax is comprised of two main components:

- Command Console
- Target Agent

A.7.3 Command Console

The Command Console serves as a centralized integrated environment for configuration, administration and analysis of the entire system. It is further divided into number of sub-component.

Assessment Manager. An *Assessment Manager* examines targeted hosts for configuration problems, reports the problem. It also recommends how to improve the system and its configurations in plain English.

Alert Manager. The *Alert Manager* display notifications on the Command Console about detected threats. Information such as events, user, time and host can be included in the alert message.

Detection Policy Editor. Lets the SSO to create policy by defining a set of activity signatures. A list of predefined signatures are available for different suspicious behavior such as various hacking attempts, failed logins, decoys, viruses, Trojan horses etc. Automatic response and notifications can be defined. Examples of response mechanisms include E-mail, pagers, on-screen alerts and SNMP traps.

Audit Policy Editor. Creates a policy for system-, file-, folder-, registry key-, and log size settings for distribution to the target agents.

Collection Policy Editor. Creates a policy to collect audit data from collections of targets. Audit data is collected in a centralized database.

Report Manager. Generates customized reports from the centralized database. This gives the SSO a feeling for trends of activities by target and/or by user.

A.7.3.1 Target Agent

The target agents are available for Windows NT and some Unix platforms. The target agents collect raw audit data information from their hosts and sends it back to the command console.

The Entrax product has recently been renamed to Centrax.

A.8 CMDS (Computer Misuse Detection System)

Product	**CMDS**
Vendor	SAIC
Platforms	Unix (Various platforms), Windows NT
Data source	host-based
Model of intrusion	Rule and anomaly based detection model
Behavior	Detection and response

A.8.1 Introduction

CMDS from SAIC is a data forensics and audit-trail analysis tool. I provide real-time detection of unauthorized behavior in a distributed environment. The main focus of CMDS is to detect internal misuse. Basically it can monitor any device that has the capability to generate some kind of audit logs. For example firewalls, Unix systems, databases etc.

A number of different mechanisms are used to detect misuse. Statistical profiling is used to find anomalies in the behavior of the systems. An expert-system database with known attack signatures is utilized to detect intrusions and intrusion attempts.

A.9 SecureNet PRO

Product	**SecureNet PRO**
Vendor	MimeStar, Inc.
Platforms	Solaris (Sparc), FreeBSD (x86), Linux (x86) BSDi (x86)
Data source	network-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.9.1 Introduction

SecureNet PRO (SNP) is a network-based, misuse intrusion detection system with automated response mechanisms. SNP passively listens on the network traffic found on the physical Ethernet segment it is installed on. Currently, SNP only support Ethernet segments, but other network transport mechanisms are planned for future releases.

SNP consists of two parts. *Secure Net PRO servers* and *administrative consoles*. Each SNP server relay information to one or more administrative consoles. One server is required for each physical Ethernet segment. A console may manage one or more remote SNP servers distributed throughout the network.

SNP provides extensive logging, detection and automated response such as termination of sessions and suspicious activities. One interesting feature of SNP is that it provides mechanisms to hijack a session. This allows the SSO to instantly seize the session/connection (such as telnet) of any user on the network. Most of the TCP/IP based protocols can be analyzed such as TCP, UDP, ICMP, IPIP, IGMP.

MimeStar make a distinction between *context-based* and *content-based* attacks. Context based attack detection include IP-fragmenting, SYN-flooding and other attacks that exploits vulnerabilities of the TCP/IP protocols. Content-based attacks include attacks against applications, services and programs such as ftpd, sendmail, httpd, and rlogind. Custom-made attack signatures may be added by the SSO.

A.10 CyberCop

Product	**CyberCop**
Vendor	Network Associates, Inc.
Platforms	Windows NT, Solaris 2.5, 2.6 (Sparc)
Data source	Host and network-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.10.1 Introduction

Network Associates provides a line of intrusion detection products under the CyberCop brand name. CyberCop Network, and CyberCop Server are part of Network Associates' network security suite, Net Tools Secure.

CyberCop Network (CCN) provides real-time intrusion detection using information found on the local network. CyberCop Server (CCS) focus on protecting servers and other hosts in a networked environment.

Sensors are placed strategically throughout the network to look for suspicious behavior. Sensor work in concert with a management server that log suspicious events and send alarm to management consoles. Automated response mechanisms are available to terminate sessions or notify administrators using e-mails, SNMP traps, and pagers etc. CCN also has a heart-beat function that protects to sensors from being disabled.

CyberCop Network is based on intrusion detection technology from Wheelgroup, Inc (Nowadays owned by Cisco). In fact Cisco's NetRanger and CyberCop Network uses the same set of intrusion detection signatures to detect attacks. The main difference between CyberCop Network and NetRanger is that NetRanger is more focused on protection the perimeter of the network using a firewall or a router to block intrusions whereas CyberCop Network focuses on protecting the network from internal attacks.

Subjects that CyberCop suite detects attacks on include:

- Unix and Windows/Windows NT hosts
- Network Services
- Web servers and browser
- Various applications
- Protocol stacks

A.10.2 Architecture

CyberCop has two main parts:

- CyberCop Sensors
- CyberCop Management Server

A.10.2.1 CyberCop Sensors

The sensors are distributed throughout the network configured to detect intrusion based on information found on the network segment to which they are connected. Network Associates recommends that sensors are placed at points of high risks such as:

- •Wide Area Links
- •Dial-in connections
- •Server clusters
- •Other critical segments

As a sensor detect an intrusion it forwards a record of the suspicious event to the CyberCop Management Server. Fault tolerance of the system is improved by using a heart-beat function to detect sensor failure.

A.10.2.2 CyberCop Management Server

The Management Server collects audit data from the sensors and provides logging and alarm notification. A WEB-based user interface is used which let the SSO administer the system from any location. Security of the system is improved by using encryption to protect the communication channels between sensors-managers and the user's browser interface.

A.11 INTOUCH INSA

Product	**INTOUCH INSA**
Vendor	Touch Technologies, Inc.
Platforms	Digital Alpha (Dedicated hardware)
Data source	network-based
Model of intrusion	Rule and anomaly based detection model
Behavior	Detection and response

A.11.1 Introduction

INTOUCH INSA (II) is a network-based intrusion detection system running on a dedicated Digital Alpha RISC system. It scans the network for intrusions by passively listening on the network activity. Patterns of known intrusions are provided with the system. However, the patterns to be scanned for can be customized using a built-in Network Security Manager.

In addition to basic attack signature recognition (patterns), II tries to recognize anomalies using source/destination analysis and network load analysis. II can configured to record sessions and allows the SSO to track and analyses historical incident details. In the event of a possible intrusion, both real-time and retrospective analysis are provided. Intrusion alerts can automatically trigger events/actions.

A.12 T-sight

Product	**T-sight**
Vendor	En Garde Systems, Inc
Platforms	Windows NT
Data source	network-based
Model of intrusion	(Manual) Anomaly based detection model
Behavior	Detection

A.12.1 Introduction

T-sight uses a somewhat different approach to intrusion detection. It is created around the philosophy of manual intrusion detection. Using a number of visualization techniques, suspicious activities are detected by looking for “footprints” of an intruder. En Garde Systems believes that the SSO has a basic idea of what constitutes suspicious behavior on the network. T-sights also provide a set of reporting and graphing tools that can be used for post-mortem compromise analysis.

T-sight monitors the network using *Handlers.* A set of handlers are provided with the system. Currently these handle the following protocols: Telnet, DNS, Rlogin, Rsh, FTP, HTTP, SMTP and Finger. A handler collect data from the network and report it back to T-sight. T-Sight collects and condenses data from the handles into a usable format. The main windows of T-sight allow the SSO to sort connections by protocol, IP source or destination address, start and end time, source or destination port.

Handlers for customer-specific applications and protocols can be designed to examine site-specific information and/or proprietary protocols.

Once a suspicious activity is detected, the SSO has the possibility to terminate or take over sessions using session hi-jacking techniques.

A.13 NIDES

Product	**NIDES**
Vendor	SRI International
Platforms	SunOS
Data source	host-based
Model of intrusion	Rule and anomaly based detection model
Behavior	Detection and response

A.13.1 Introduction

NIDES is a real-time host-based intrusion detection system developed by SRI International. SRI has a long history of research within the field of intrusion detection. NIDES operates by analyzing audit logs collected from the monitored systems looking for suspicious user behavior. NIDES is designed to run on a dedicated workstation and both misuse- and anomaly based detection are supported. Statistical analysis is used to create *statistical profiles* for each user of the target systems. All user activity that deviate from normal behavior raises an alarm. The statistical profiles are constantly updated through an ageing mechanism. This anomaly type of detection is primarily designed to detect intrusion where an intruder masquerades as a legitimate user. Misuse detection is realized using pattern matching techniques which can be customized to meet site specific needs. New rules are added to the systems by compiling them into the running system. If this is possible without restarting the system is not clear from the publicly available documentation.

A screening function is used to filter alarms before reporting them to the site security officer. This prevents flooding the SSO with redundant alarms. An archive facility is available that stores audit records, analysis results, and alerts. In addition, a monitoring facility is used to display alerts, status of the data archiver, and various daily summaries. Alarm can also be sent to a list of e-mail recipients.

A nice feature of NIDES is that it has a test environment where new parameter settings can be tested before they are applied to the running system. For example, statistical test data sets for different time-periods can be constructed using archived audit data.

A.14 ID-Trak

Product	**ID-Trak**
Vendor	Internet Tools, Inc.
Platforms	Windows NT
Data source	network-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.14.1 Introduction

ID-Trak is a network-based intrusion detection system based on Internet Tools' SDSI technology. The SDSI (Stateful Dynamic Signature Inspection) technology uses a SDSI virtual processor and a set of low-level instruction which can be used to model attack signatures. The SDSI architecture is dynamic in the sense that new attack signatures can be added in real-time to the virtual engine. It is also stateful in the sense that it uses a register cache to store application protocol sessions. A large number of predefined attack signatures (> 200) are provided and new signatures can be added or customized using the same set of rules in real-time.

Once an attack is detected, various action can be taken to stop suspicious sessions or notifying the SSO using e-mail, pagers, SNMP traps etc. Extensive logging (full trace of sessions) can also be enabled.

ID-Trak can be used in distributed network environments. The system can be placed at strategic points in the network and managed through a centralized console.

In 1998, Internet Tools Inc. was aquired by Axent Technologies. ID-Trak is now part of Axent's line of products under the name "NetProwler". For more information about Axent's tools for intrusion detection, see section A.2

A.15 SecureCom

Product	**SecureCom**
Vendor	ODS Networks
Platforms	Windows NT, Solaris 2.5, 2.6 (Sparc)
Data source	network-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.15.1 Introduction

Secure Detector is an intrusion detection component in ODS Networks' SecureCom software suite. The Secure Detector itself is composed of two separate software packages. The first package is RealSecure from Internet Security Systems. A separate section on RealSecure can be found elsewhere in this document. The Second package is SecureInvestigator (SI). SI enhance the functionality provided by RealSecure by providing a network-centric view of the network. SecureInvestigator monitor a network searching for:

- Physical or logical changes to the network infrastructure
  Foreign hardware, IP-spoofing etc.
- Unusual TCP/IP port activity
- Alien conversations
  Data is exiting from within the corporate network to outside the enterprise.
- Modem backdoors
- Suspicious internal conversations
  A conversation of an employee or user that is suspected of problems.
- Bottlenecks and overutilized network segments

A single Secure Detector module can simultaneously monitor up to ten 10Mbps ethernet segments. Efforts has been made to integrate intrusion detection technology with network infrastructure components. SecureSwitch, a high-speed network switch from ODS Technology, can be configured to include data collection modules for Secure Investigator and RealSecure. The switch is designed to handle ethernet, fast ethernet with uplinks for Gigabit ethernet, FDDI and ATM.

A.16 POLYCENTER

Product	**POLYCENTER**
Vendor	Compaq (former Digital Equipment Corp.)
Platforms	SunOS 4.1.1, 4.1.2, OpenVMS
Data source	host-based
Model of intrusion	Rule and anomaly based detection model
Behavior	Detection and response

A.16.1 Introduction

PolyCenter is host-based intrusion detection system running on hosts throughout the network. It detects intrusions and intrusion attempts by looking at audit logs from the hosts.

PolyCenter can be configured to detect several categories of intrusions such as:

- Attempts to execute unauthorized and privileged programs
- Suspicious network file transfers
- Suspicious activities involving a specific host, user or file.
- Activities outside of normal working hours

The analysis of the audit data uses artificial intelligence (AI) research results from Digital Equipment Corp. A knowledge base of existing methods and objectives of attackers are available and is used to detect suspicious activities that could indicate that the host is under attack. A “case” model, similar to a “criminal case”, assigns virtual agents to monitor certain suspects (suspicious behavior). The agent starts monitor the suspect and file evidence (logs) to the case. By analyzing each security event within the context of a case, PolyCenter tries to distinguish between real threats and innocent behavior.

When necessary, Polycenter can notify the SSO about critical events as they are detected. The system can also be configured to take countermeasures without human intervention.

A.17 Network Flight Recorder

Product	**Network Flight Recorder**
Vendor	
Platforms	Windows NT, Solaris 2.5, 2.6 (Sparc)
Data source	network-based
Model of intrusion	Rule based detection model
Behavior	Detection and response

A.17.1 Introduction

The Network Flight Recorder (NFS) from the company with the same name is not marketed primarily as an IDS, although it has some IDS capabilities. As the name suggests, NFS is primarily intended for postmortem analysis of network events, for example when the SSO wants to find out what actually happened on the network during an intrusion or some other kind of detected anomaly.

NFR provides recording and filtering of network traffic for logging or statistical analysis, and can be configured to trigger alerts on certain events. According to the developers, NFS is designed to be the “bottom-half” of an IDS rather than a complete system for intrusion detection. It uses a “packet sucker” based on libpcap to collect packets from the monitored network. Packets are passed to a decision engine, where they are evaluated through filters written in N-code, a language developed specifically for NFR. In such a filter, it is possible to record selected information from the filtered packets to disk and to trigger alerts. After filtering, the original captured packets are discarded. The information saved on disk can be accessed through a query backend which is separate from the recording mechanism. Users interact with the query mechanism by pointing their standard Web browser to a HTTP server set up by NFR. The browser downloads and executes Java applets which constitute the user interface to NFR. Query results can be visualized by the Java client as different types of lists or charts.