INTRUSION DETECTION SYSTEM (IDS)

PRODUCT SURVEY

Kathleen A. Jackson

Distributed Knowledge Systems Team
Computer Research and Applications Group
Computing, Information, and Communications Division
Los Alamos National Laboratory
Los Alamos, New Mexico
USA

LA-UR-99-3883

Abstract

This survey is intended to be a comprehensive compilation and categorization of currently available intrusion detection system (IDS) commercial products. It was undertaken at the instigation and with the support of the Global Security Analysis Laboratory at IBM's Zurich Research Laboratory in Rueschlikon, Switzerland. It is based almost entirely on published reports, published product evaluations, and vendor-supplied product information. Prior to publication, considerable effort was expended attempting to contact every referenced vendor, so that they might point out and suggest corrections. The comments by those who responded were reviewed carefully and incorporated where appropriate. This survey does not recommend or endorse any specific product or service; it is intended wholly as a resource for those interested in the current state and the ongoing evolution of IDS products and what that implies for IDS research and development.

Note:
All referenced brand or product names are trademarks or registered trademarks of their respective holders.

Version 2.1

06/25/99

Table of Contents

Table of Contents

1 Introduction

1.1 Purpose

This document attempts a comprehensive compilation and categorization of available intrusion detection system (IDS) products. Long studied and prototyped in academic and government circles, IDS have only in the last few years begun to emerge as a viable and useful commercial option. The first commercial IDS product was released in 1991, with a relative handful emerging in the subsequent half dozen years. Then, in the last couple of years, the field underwent explosive growth. Even after the apparent failure of several early releases, there still remain at least seventeen extant products that claim to provide effective intrusion detection in a networked environment. Given this recent growth, and the reported increased application of corporate resources to these products [3, 5, and 7], the time has come for a comprehensive review of the field. This survey is the result of that review. It is based almost entirely on published reports, published product evaluations, and vendor-supplied product information, with special contributions made by a small set of product users and IDS experts.

1.2 IDS Overview

Intrusion detection systems attempt to detect computer misuse. Misuse is the performance of an action that is not desired by the system owner; one that does not conform to the system’s acceptable use and/or security policy. Typically, misuse takes advantage of vulnerabilities attributed to system misconfiguration, poorly engineered software, user neglect and carelessness, and to basic design flaws in protocols and operating systems. While outsiders may frequently perpetrate misuse (i.e., intrusions), it is more often the result of malicious insider activity. This is because a legitimate (if untrustworthy) user can take advantage of physical access, some level of genuine privilege, and knowledge of local security measures (objects an outsider must endeavor to acquire illicitly).

IDSs automatically analyze on-line user activity for forbidden (i.e., invalid) and anomalous (i.e., atypical, inconsistent) behavior. They are based on the hypothesis that monitoring and analyzing network transmissions, system audit records, application audit records, system configuration, data files, and other information can detect misuse. This information encompasses vast quantities of data, effective analysis requires specialized and continually honed expertise, and at least near real-time detection[1] of misuse is frequently crucial. Without automatic computer-based IDSs, effective and timely misuse detection is, for all practical purposes, impossible. An IDS’s ability to apply the latest security and attack expertise to separate a relatively few potentially interesting events from a vast amount of benign activity enables much more effective network security administration and allows for the prospect of timely and effective response.

Intrusion detection is not a complete security solution in itself; no single security system or technique can be. Rather, an IDS should be one of several measures taken to protect an enterprise. The power of intrusion detection is that to circumvent security a perpetrator must penetrate other security barriers while *also* avoiding detection by an IDS. In addition, it provides a way to measure the performance of these other security measures and to assess the effectiveness of security policies.

1.3 Identifying Products

In order to select the targets of this survey from myriad possibilities while keeping the scope manageable, a selection process was required. The first step was to determine what comprises a product, the second, what comprises an *IDS* product.

1) What is a product? A product is merchandise that is distributed and, most important, supported by a recognized commercial venture. This definition eliminates research and prototype systems, unsupported freeware, and systems developed exclusively for specific sites.

[1] Fast enough processing for effective automated response to take place. This response, which may range from email notification to firewall reconfiguration, provides at least a possibility of thwarting an attack and mitigating damage.

2) Now, what comprises an IDS product? This was a little more difficult since there is some difference of opinion within the security community. First, IDSs must *detect*, and second, they must detect *misuse* of some sort. This does not mean detecting the environmental *potential* to misuse, as vulnerability scanners do, but detecting attempted (successful and unsuccessful) misuse itself. The term *intrusion* is ambiguous, since it implies misuse from only an external source, and it is generally accepted in the IDS community that the activity of a maliciously motivated insider are equally interesting and potentially even more harmful as those of a malevolent outsider. Therefore, the term intrusion may be taken to mean any intentional activity that is an infraction of a site's security policy, and which may lead to loss of confidentiality, denial of service, destruction of information, theft of information, or improper use.

   But what of malicious code detectors? It is clear that intrusion detection includes attempts to detect and respond to malicious code, as many (probably most) attacks are undertaken using pre-programmed scripts. So where to draw the line? An Internet-borne virus is malicious code that easily meets our criteria for intrusive activity. So may malicious Java applets and hostile ActiveX controls. Is detecting these kinds of codes the province of IDSs?

In the end the following three criteria were adopted:

1) Because they do not fit the above definition of an IDS, vulnerability scanners would not be examined, though indeed a vulnerability scanner may be a component of an IDS.

2) While they do fit the above definition of an IDS, products that are designed to only to detect and block malicious mobile code would not be examined. However, they may be a component of an IDS. In other words, a virus or active code detector would not be counted as an IDS product for the purposes of this survey, but an IDS product may, among other things, monitor for signs of hostile code in network traffic or on a system.

3) Finally, firewalls may monitor for, trace, and respond to potentially intrusive activity such as scanner probes. When these provide only a very rudimentary IDS and their primary purpose is not intrusion detection, they would also be excluded from this survey.

Every attempt was made to provide a fair and thorough characterization of the current IDS product scene, to identify and review all remaining IDS products. However, given the explosive recent growth and fluidity of the IDS marketplace, it cannot be guaranteed that every available product has been included, or indeed, that defunct products were excluded.

2 Product Assessment

Any IDS assessment must first characterize the IDS product; i.e., identify the kind of IDS being examined. Section 2.1 describes criterion for doing this. Once an IDS is characterized, the next step is to ascertain whether or not the product includes certain key attributes, as described in Section 2.2. Table 2-1 summarizes IDS product characterization and attributes. After this comes an inventory of the product's specific applicability (e.g., for what operating systems, applications, and/or network protocols is it designed). Section 2.3 and Table 2-2 provide this information. Finally, Section 2.4 summarizes the critical issues in ascertaining a product's actual attainment (i.e., how well it works relative to specific criteria). It was beyond the scope of this survey to thoroughly evaluate each product, though IBM's Global Security Analysis Laboratory (GSAL) is in the process of doing just that for the most likely of current products.

2.1 Characterization

There are four fundamental issues that must first be addressed when examining any IDS product [8]. The design choices made in response to these four issues determine the nature of the product, and will be of most interest to anyone considering using such a system. These issues are:

1. What information the IDS accesses and gathers;
2. What method or technique is used to process that information;
3. How frequently the information is processed; and,
4. How the IDS responds to the results of that processing.

2.1.1 Deployment

There are two basic deployment strategies for IDS products, *Host-based* and *Network-based*. An IDS product's placement on the network directly determines the kind of information that can be gathered and analyzed by the IDS. An IDS product may include both network- and host-based capabilities, which implies (and by our definition requires) that they share a common management interface and have at least some degree of interoperability (i.e., if both boxes are checked, the two are components of the same system).

Network-based IDS evaluate information captured from *network* communications. They analyze the stream of packets traveling across the network, and may also perform analysis of network traffic (e.g., who connected to whom and when did it happen). The packets are usually analyzed for both context and content for defined attacks. Network-based IDS comprise software that is installed on dedicated workstations that are placed at critical junctions of a network (e.g., just outside a firewall, in front of a Web server or in front of an e-mail server). These "sniff" (capture and read) the stream of IP packets traveling across the network.

Host-based IDS evaluate information found on some kind of host computer. This may include the contents of *operating system*, *file system*, and *application*, and perhaps, *other* logs. Host computers may include user workstations (including specialized applications such as web browsers), peripherals (such as printers), specialized servers such as web servers, or network components (such as firewalls, routers, and switches). Host-based IDS use software modules that are installed on each monitored host. These access and read logs and audit records of interest.

Key for Table 2-1:

- *network-based* means that the system is designed to capture and analyze network packets.
- *host-based* means that the system is designed to analyze information found on host computers.

2.1.2 Information Source

The information that an IDS product can access is determined by where it is deployed. How much of that information it can decipher and evaluate is determined by its capabilities. Network-based IDS always capture and analyze network packets, while host-based IDS products potentially have many information sources on the hosts where they are installed.

Key for Table 2-1:

- *network packets* means that the IDS includes a network-based sensor designed to capture and process network packets and decipher at least one network protocol (e.g., TCP/IP).
- *operating system* means that the IDS includes a host-based agent designed to process the audit record of at least one specific operating system (e.g., Solaris, Ultrix, Unicos).
- *application* means that the IDS includes a host-based agent designed to process the audit record of at least one specific application (e.g., a web server, a firewall, a network management system).
- *file system* means that the IDS includes a host-based agent designed to evaluate the file system and its directories on at least one specific operating system.
- *other* means that the IDS is designed to process information other than that specified in the previous choices.

2.1.3 Detection Method

Detection methodology falls into two basic types; *behavior-based* and *knowledge-based*. Behavior-based detection methods use information about repetitive and usual behavior on the systems they monitor. Also called *anomaly detection*, this approach notes events that diverge from expected (based on repetitive and usual) usage patterns. This approach has thus far proven difficult to engineer for commercial products, and is thus rarely used. Knowledge-based detection methods use information about known security policy, known vulnerabilities, and known attacks on the systems they monitor. This approach, also known as *misuse detection*, compares network activity or system audit data to a database of known attack signatures or other misuse indicators, and pattern matches produce alarms of various sorts. All commercial systems use some form of knowledge-based approach. Thus, the effectiveness of current commercial IDS is based largely on the validity (including how up-to-date) and expressiveness of their database of known attacks and misuse, and the efficiency of the matching engine that is used.

Key for Table 2-1:

- *knowledge-based* means that the IDS product uses some form of misuse detection.
- *behavior-based* means that the IDS product uses some form of anomaly detection.

2.1.4 Execution

The execution frequency (or periodicity) indicates how often an IDS analyzes data from its information sources. Most commercial IDS claim real-time processing capability (though the exact meaning of that term varies), and a few provide the capability for batch processing of historical data.

Key for Table 2-1:

- *dynamic* execution means that the IDS is designed to perform concurrent and continuous automated processing and analysis (implying real-time operation).
- *static* execution means that the IDS is designed to perform periodic processing and analysis (implying batch or other sporadic operation).

2.1.5 Response

There are two basic ways in which an IDS may respond to an identified attack, misuse, or anomalous activity. The first (and clearly universal) is a *passive* response, one where the IDS simply informs responsible personnel of an event. Less often, the IDS also has the capacity to engage in an *active* response to critical events, where (as specified by the user) it takes corrective or proactive action.

Key for Table 2-1:

- *active* means that the IDS has the capacity to engage in a corrective or proactive response to a critical event, such as correcting a system vulnerability, logging off a user, selectively increasing monitoring, re-configuring a firewall, or disconnecting a port.
- *passive* means that the IDS is designed to inform responsible personnel of an event by way of console messages, email, paging, and report updates.

2.2 Attributes

Next the IDS can be assessed on the basis of other critical attributes that include the product's environmental suitability, flexibility, susceptibility to tampering, interoperability with other products, monitoring range, ability to help manage events, ease of acquisition, and the level and quality of vendor support.

Table 2-1: IDS Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distrib-uted	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring											
IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	counter-measures	none

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	>30K	20-30K	10-20K	<10K	free

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none

2.2.1 Suitability

Each IDS product targets certain types of users and environments. This means not just the operating system upon which they run or monitor, but also the type, size, and speed of network involved, the protocols used on the network, the operating systems on the hosts, and the specific needs of the user. Any potential IDS user must evaluate the suitability the various IDS products to the user's environment and needs, or run the risk of ending up with an inappropriate product that may provide either more or less than required. This Section addresses IDS product suitability to the user's network environment. The product's *applicability* to specific systems, protocols, and applications is addressed in Section 2.3.

Both host and network-based IDS products usually have a distributed design; i.e., they comprise a *manager* and a number of *agents*. In rare cases, manager and agent functionality is not distributed; but in any case the functionality remains the same. Agents collect and process (to at least some degree) target system information, transfer the results to the manager, and sometimes actively respond to detected events. The manager consolidates and sometimes completes analysis of information from the agents, displays and transmits alarms, and generates reports. Host-based IDS use software agents that are installed at each information source (e.g., workstation or web server) to collect, initially process, and transfer alarms and other information to the manager. Network-based IDS agents are commonly called *sensors*. Sensor software is installed on dedicated workstations that are placed at critical junctions of a network (e.g., just outside a firewall, in front of a Web server or in front of an e-mail server). These agents "sniff" (capture and read) the stream of IP packets traveling across the network, process the packets, and send alarms and other information to the manager.

Many users require an IDS that can be easily managed in at least an extended LAN and frequently a WAN or enterprise environment. If the IDS is only needed for a simple LAN, the user should not obtain (and pay for) a system whose capability exceeds his or her needs. The features that can determine suitability include:

IDS architecture. The IDS should provide a distributed capability, since this component of scalability is vital for effective deployment of IDS in the vast majority of corporate networks. A distributed capability means that the IDS functionality is provided by both a central manager or managers and local collection/processing agents placed as needed throughout the monitored network. A product that consists of only a combined manager/agent (i.e., a local version) is next to useless in a large distributed environment. However, some products are available in both a local and distributed versions.

Key for Table 2-1:

- *local* means a local functionality is provided (i.e., that a version of the product is sold where both manager and agent functions are combined in one software package that must run together on one workstation or server).
- *distributed* means that a version of the product is sold where the IDS provides some effective means of distributed deployment.

IDS management scheme. Distributed management means the capability to dynamically load and configure agents or sensors, troubleshoot, collect and merge results, and generally manage the system as a whole from a remote network location, usually a management console. The most flexible provide the capability for the user to securely log onto the management console (see Section 2.2.3) and perform these tasks from any other console in the network. An IDS that does not support remote management is unusable for an enterprise environment, and unwieldy even for a simple LAN.

Key for Table 2-1:

- *any console* means that the product provides distributed management, and that such management may be performed from any console in the network (i.e., authorized personnel may securely log on to a management console from any console in the network).
- *central console* means the product provides distributed management, but that such management may be performed only from a specific management console (i.e., by authorized personnel who are physically located at a central management console).

- *none* means that even though the product has a distributed architecture, it does not provide a distributed management capability (i.e., that the user must manage each distributed IDS component individually).
- *n/a* means that since the product architecture is local, no distributed management capability is provided (i.e., that the user must manage each IDS component individually).

Agent to management console ratio. In order to be effective in a WAN or enterprise environment, an IDS must be capable of effectively administering a large number of agents or sensors. Enterprise environments may require agents on thousands of hosts, and sensors in many strategic network locations.

Key for Table 2-1:

- *high* means that a virtually unlimited number of agents can be managed from a central management console. This implies a sophisticated management hierarchy, that the entire system can handle bursts of event activity, and that there is a mechanism to effectively display and otherwise communicate what's being detected by the managed agents.
- *medium* means that a large number (low hundreds) of agents can be managed from a central management console, but that no management hierarchy exists. This implies that the single management console can effectively deal with bursts of event activity and that it has sufficient means to effectively display and otherwise communicate what's being detected by the managed agents.
- *low* means that only a few (tens) of agents may be effectively managed from a central management console.
- *n/a* means that since the system architecture is local, this concept is meaningless (i.e., there are no separate agents or sensors).

Communications robustness. The IDS must ensure that its operations are safe from the malfunctions that can happen on any network; i.e., it must provide a means of detecting and recovering from communications and system failures. Robust communication includes techniques that ensure that information being passed between the IDS manager and agents or sensors, and between the agents and network servers, is not lost, unduly delayed, or corrupted due to network and system failures.

Key for Table 2-1:

- *f/t ptp protocol* means that the IDS employs a fault tolerant, point-to-point protocol for communication between the manager and agents or sensors and other network servers.
- *other* means that the IDS employs effective but less rigorous techniques to ensure reasonable communication robustness.
- *none* means that the IDS does not use any means to ensure communication robustness.
- *n/a* means that since the system architecture is local, this concept is meaningless (i.e., there are no separate agents or sensors).

2.2.2 Flexibility

To mitigate the occurrence of both false positives (benign activity identified as events) and false negatives (missed events), an IDS product must be adaptable to the network or system being monitored. This means fine-tuning an IDS so that it monitors for and responds to attacks and prioritizes events in a manner that is consistent with local security policy and to at least some extent the network being monitored. This may also mean, for some users, adapting the IDS to specific network protocols or system audit records. In addition, a user will usually wish to modify as-delivered report templates to local requirements, and may wish to select security features that comply with local security policy. Meeting these needs implies the provision of a means to easily customize these features.

Key for Table 2-1:

Possible customizable features include:

- *attack and misuse definition* means that in addition to supplying and updating a comprehensive set of attack and misuse signatures, the IDS provides for modification of that set and also the addition of new attack or misuse signatures. For this feature to be useful, a means must also be provided to efficiently perform this function. This implies at least the provision of a signature or misuse definition language, a mechanism for checking for signature consistency and efficacy, and a way to merge user modifications into signature updates from the vendor. *Broad* means the user may safely and accurately modify not only vendor-supplied signatures but also to add as wide a variety of new signatures as desired. *Limited* means that the user may only undertake restricted modifications to vendor-supplied signatures. *None* means that the IDS does not allow the user to customize attack and misuse signatures.

- *attack and misuse response* means that in addition to supplying a set of default attack responses, the IDS provides for modification of that set and the addition of new responses. A minimal set of vendor-supplied attack responses should include email, voice-mail, pager activation, and console messages. There should be a means of escalating notifications to appropriate staff based on company-defined notification policies, such as who should be notified and in what manner, depending on the time of day, the severity of the problem or a combination of both. Some vendors also supply the capability for active responses, such as firewall and router re-configuration. The details of how and when (or if) any of these responses are used should be invoked should be up to the user, and for this a mechanism must be provided for the user to activate, modify, and test attack responses. *Broad* means the user may safely and accurately modify not only vendor-supplied passive responses but also add both passive and active responses as desired. *Limited* means that the user may only undertake restricted modifications to vendor-supplied passive responses. *None* means that the IDS does not allow the user to customize attack and misuse responses.
- *connection event* means that the IDS provides the capability for the user to respond in some way to specific connection events (e.g., based on protocol, source port, destination port, source IP address, or destination IP address). The details of how and when (or if) any connection event responses are used should be up to the user, and for this a mechanism must be provided for the user to activate, modify, and test connection event responses. *Broad* means that the user may safely and accurately define a wide range of connection events of interest. *Limited* means that the user may only undertake restricted modifications to vendor-supplied connection events. *None* means that the IDS does not allow the user to customize connection events.
- *protocol definition* means that in addition to supplying the capability to process a default set of network protocols, the IDS provides for the user definition of new protocols (for network-based IDS). This enables the IDS to interpret and process user-specified data sources. *Broad* means that either the user may safely and accurately define and test new protocols for the IDS. *Limited* means that the user may only make restricted changes to an existing protocol or must rely on (and pay) the vendor to make more comprehensive changes. *None* means that the IDS does not allow the user to customize protocol definitions.
- *audit record* definition means that in addition to supplying the capability to process a default set of audit records, the IDS provides for the user definition of new audit records (for host-based IDS). This enables the IDS to interpret and process user-specified data sources. *Broad* means that either the user may safely and accurately define new audit records for the IDS. *Limited* means that the user may only make restricted changes to an existing audit record protocol or must rely on (and pay) the vendor to make more comprehensive changes. *None* means that the IDS does not allow the user to customize audit record definitions.
- *reports* means that in addition to supplying a default set of Text, CSV or HTML reports, the IDS provides for the user modification of those reports and definition of a range of new reports. How and when reports are generated should also be up to the user, and for this a mechanism must be provided for the user to easily customize a wide variety of reports, ranging from executive summaries to detailed event reports. *Broad* means that the user may easily define the format, content, and periodicity of a large set of new reports. *Limited* means that the user may only make restricted changes to an existing set of vendor-supplied report templates. *None* means that the IDS does not allow the user to customize reports.
- *cryptography options* means that in addition to supporting data encryption (see Protection, Section 2.2.3), the IDS provides a user-configurable set of cryptography options (including disabling all cryptography). *Broad* means that a reasonable set of user-configurable cryptography options is provided, such as data encryption algorithm options (including the option to disable) and digital signatures. *Limited* means few user-configurable cryptography options are provided. *None* means that the IDS does not allow the user to customize cryptography options.
- *security options* refers to the means by which a system can ensure that its activities are resistant to malicious tampering. For more detail about what kind of options might be provided, see Section 2.2.3.

In addition, in order to conform to local security policies, the user may want to control access to IDS applications, restrict privilege, and restrict logons to specific locations (e.g., system console only, certain other consoles). *Broad* means that the user may have complete control over security options on both the management console and sensor workstations. *Limited* means that the user may only make restricted changes to a limited set of security options. *None* means that the IDS does not allow the user to customize security options.

- *other* means that the IDS provides at least one other significant feature not herein defined (this entry is provided as a means for a vendor to call attention to the feature). *Broad* means that the user may have complete control over this feature. *Limited* means that the user may only make restricted changes to this feature. *None* means that the IDS does not allow the user to customize this feature.

2.2.3 Protection

Given its criticality to the security of any enterprise, an effective IDS must also ensure that its activities are resistant to malicious tampering. The features that determine the IDS ability to resist tampering include:

Self-monitoring. This means that an IDS by some means effectively monitors its own activities for signs of interference and/or failure, and is capable of responding (if only with a console message) when such signs are found.

Key for Table 2-1:

- *yes* means that the IDS is designed to perform some type of self-monitoring.
- *no* means that the IDS is cannot perform effective self-monitoring.

Stealth techniques. This means that the IDS employs techniques that enable it to be effectively “invisible” on the monitored network (such as having no IP address), so as to be less vulnerable to being itself attacked.

Key for Table 2-1:

- *yes* means that the IDS is designed to operate in stealth mode.
- *no* means that the IDS is not designed to operate in stealth mode.

Management console security. These means that the IDS can in some way ensure that its management console is secure, and provide logon and administrative access controls that manage rights to specific applications. This may be accomplished via user authentication to the console (e.g., single use password, smart card), access control within the console, and privilege management.

Key for Table 2-1:

- *user authentication* means that the IDS management console requires user authentication at the local terminal, and for secure user authentication (i.e., no clear-text passwords) from remote terminals throughout the network, if remote logons are accepted at all (see Remote Management in 2.2.1). This capability limits the management console to authorized users.
- *user access control* means that the IDS management console provides the capability to control access to the various applications on the console (e.g., a user may be able to view event reports but not perform configuration updates).
- *user privilege management* means that the IDS management console provides the capability to control the system privilege of authorized users of the console.
- *None* means that no special provision is made for management console security.

Communications security. This means the IDS can ensure that routine communication between management console and agents is secure; that configuration and diagnostic information can be securely transported between manager and agents, and that alarms and incident data arrive complete and uncorrupted at the manager. The vendor should also ensure that signature and version updates are provided to users in a secure manner.

Key for Table 2-1:

- *manager-agent verification* means that the IDS can provide some means (e.g., digital signatures) to ensure trust in manager-agent communications (i.e., that agent communications received by the manager are from a valid agent; that manager communication received by an agent are actually from the manager).

- *manager-agent data encryption* means that the IDS provides a way to rigorously encrypt (i.e., at least very difficult, if not impossible, to break) communications between management console and agents. Encryption schemes may themselves provide for manager-agent verification.
- *secure software updates* means the IDS vendor provides a secure means to send updated attack definitions and new software versions to the user (for the method used, see Attack Definition Updates, Section 2.2.8). At the least, there should be some means of verifying software integrity (e.g., checksums).
- *none* means that the IDS vendor does not provide any means of communication security.

2.2.4 Interoperability

It is extremely advantageous if IDS products are able to interoperate at some level with other network management and security tools, including:

Comprehensive network management system (NMS). This feature enables a network administrator to incorporate the IDS into the overall network management architecture. Some IDS may be purchased and used as but one component in a comprehensive network management package. Most IDS developers regard this as the ideal way to package and use an IDS product, and many are actively striving to achieve this goal.

Key for Table 2-1:

- *component* means that the IDS is an integrated component within a comprehensive network management system.
- *compatible interface* means that the IDS can effectively communicate with and be managed by a comprehensive network management system.
- *none* means the IDS cannot be used (as delivered) with any comprehensive network management system.

Alternative management system. A simpler, perhaps less expensive, way of interfacing with the IDS product's agents or sensors is the use of another application's management console.

Key for Table 2-1:

- *compatible interface* means that there is an alternate management system with a compatible data interface to the IDS product's agents or sensors, and that this system may be configured to effectively manage received alarms and generate reports.
- *none* means that there are no other appropriate products that can interface to the IDS product's agents or sensors.

Vulnerability scanner. Scanners are effectively the flip side of intrusion detection; they look for (and sometimes help correct) vulnerabilities that might be exploited, while intrusion detection looks for efforts to exploit said vulnerabilities. In an ideal configuration, these systems should work interactively. For example, if an IDS detects an attack then a scanner can help find the responsible vulnerability. Or, if a scanner has detected a misconfiguration and an IDS an attack that is attempting to exploit that misconfiguration, then the overall event can be assigned a high priority. Or, the presence of vulnerabilities might be used to design an attack definition for the IDS database.

Key for Table 2-1:

- *interoperable* means that not only does the scanner share a management interface to the IDS, but the IDS also works interactively with the scanner (generally true only when both are part of the same product).
- *compatible interface* means that there exists a commercial vulnerability scanner that can effectively communicate with the IDS product's management console (which may, in fact, be a mutually compatible Network Management Console (see Comprehensive Network Management System, this Section)).
- *none* means that there is no vulnerability scanner that can interface to the IDS management console.

Separate host- (network-) based IDS. A comprehensive IDS solution for any environment must include both host- and network-based agents and sensors. A single product can theoretically include this capability (see Deployment in Section 2.1). However, it is also possible for a vendor to have two separate but compatible products, or to partner with another vendor to provide separate IDS tools that interface to a common management console or network management system.

Key for Table 2-1:

- *compatible interface* means that agents (or sensors) of the IDS product are provided (by either the same or a separate vendor) and can interface to this vendor's IDS management console (which may, in fact, be mutually compatible a Network Management Console (see Comprehensive Network Management System, this Section)).
- *none* means that there are no other IDS product that can interface to this product's IDS management console.

2.2.5 Comprehensiveness

Many IDS products provide capability that extends beyond the straightforward detection of intrusions. Additional features may include expanding the concept of intrusion detection to include more general misuse detection, the ability to perform security management functions on a monitored system, and even the ability to repair damage caused by a hacker.

Additional misuse monitoring. In addition to monitoring for familiar evidence of attacks, invalid (as defined by local security policy) user behavior, and (occasionally) suspicious changes in user behavior, an IDS may be designed to also monitor for a variety of other evidence of invalid activity (e.g., malicious mobile code).

Key for Table 2-1:

- *IRC* means that the IDS is designed to capture and monitor Internet Relay Chat.
- *active content* means that the IDS is designed to detect and block suspicious ActiveX controls.
- *java applets* means that the IDS is designed to detect and block suspicious Java applets.
- *encrypted sessions* means that the IDS is designed to detect and report at least the fact that encrypted sessions are taking place.
- *e-mail content* means that the IDS is designed to capture and monitor e-mail, and can detect objectionable (to the user) words and phrases.
- *specific keywords* means that the IDS is designed to monitor network traffic for objectionable (to the user) words and phrases.
- *specific urls* means that the IDS is designed to monitor for, and perhaps block, traffic that originates at specific web sites.
- *viruses* means that the IDS is designed to monitor for Internet-borne viruses.
- *data consistency* means that the IDS is designed to perform checks for Web, FTP, DNS Server content as well as Routing Table consistency.
- *system behavior* means that the IDS is designed to monitor for non-normal process and operating system behavior.
- *other* means that the IDS is designed to monitor for an additional but unspecified kind of misuse.
- *none* means that the IDS is not designed to monitor for additional kinds of misuse.

2.2.6 Event Management

It is essential that an IDS provide the means for the user to effectively manage security events. This may include the following attributes:

Event prioritization. Some scheme of event prioritization will enable the user to respond immediately to the most critical events, while not wasting time sorting through and evaluating all reported events, many of which are likely to be minor.

Key for Table 2-1:

- *yes* means that the IDS performs effective event prioritization.
- *no* means that the IDS does not perform effective event prioritization.

Report merging and data visualization. Some scheme for processing and merging of event reports from throughout the enterprise will allow the user to manage IDS reporting at a single management console. The console must provide the means to effectively visualize events and trends that may be occurring throughout a large and diverse network. Flexible and readable visual reports are needed to turn complex output into useful information that allows a user to understand what has occurred, how to respond to it, and how it can be prevented in the future. Visualization of processed, merged, and prioritized event reports from throughout the enterprise is essential if the IDS user is to make sense of, and respond appropriately to, events that affect an enterprise.

Key for Table 2-1:

- *broad* means that the IDS provides flexible and effective report merging and data visualization, including a GUI, and that the user has a broad capability to customize it as needed (see Reports, Section 2.2.2).
- *limited* means that the IDS provides effective report merging and at least a pre-packaged set of data visualization templates, including a GUI, and that the user has little or no capability to customize it as needed.
- *none* means that effective data visualization is not provided.

Event trace and replay. When an event is detected, an IDS should have the capability to perform a full event trace, i.e., save enough information to be able to reconstruct the event in full. The ability to, after the fact, “run” the event information (network packets, audit records) through the IDS and reproduce exactly the same result as initially. This capacity may include the ability to selectively increase monitoring when the event is first detected.

Key for Table 2-1:

- *yes* means that the IDS provides the capability for full event trace and replay.
- *no* means that the IDS does not provide the capability for full event trace and replay.

24/7 Vendor hotline. A twenty-four hour, seven days a week, hotline that provides attack management expertise.

Key for Table 2-1:

- *yes* means that the IDS vendor provides a fully staffed and responsive hotline.
- *no* means that the IDS vendor does not provide a fully staffed and responsive hotline.

Vendor-provided Attack Database. A vendor-provided attack response database is one that includes attack information and analysis, details vulnerability fixes, and suggests possible countermeasures. This database includes information about what each detected attack means, why it’s bad and how the user should respond in the short and long term. Such information helps enable the user to separate what's critical from what's not.

Key for Table 2-1:

- *information* means that the database includes basic and brief descriptive information that enables the IDS user to understand what type of attack has been detected.
- *analysis* means that the database includes enough information to put the attack in context and allows the user to understand its seriousness and what sorts of vulnerabilities led to it.
- *fixes* means that the database provides recommendations for vulnerability fixes that may help avoid further such attacks.
- *countermeasures* means that the database provides recommendations of further means (besides fixing vulnerabilities) by which the user may respond to the event.
- *none* means that no attack database is provided.

2.2.7 Active Response

Given the speed and frequency at which attacks can occur, it has long been envisioned that an ideal IDS would automatically respond to such attacks at machine speed and without requiring operator intervention (i.e., an active response capability). This expectation has not yet been fully achieved, largely because of the difficulty in eliminating false positives, but also because many available responses can comprise a denial of service for legitimate users. However, IDS products can provide a variety of active response mechanisms that may be used at the discretion of the user.

Session hijacking. The ability for the IDS to seize the connection of any user on the network, either automatically or under operator control. Generally, the user remains completely locked out while an administrator performs actions such as damage control or evidence collection.

Key for Table 2-1:

- *yes* means that the IDS provides a session hijacking capability.
- *no* means that the IDS does not provide a session hijacking capability.

Session termination. The ability for the IDS to, either automatically or under operator control, terminate the connection and/or account of any user on the network. Generally, the user remains completely locked out while the operator performs actions such as damage control or evidence collection.

Key for Table 2-1:

- *yes* means that the IDS provides a session hijacking capability.
- *no* means that the IDS does not provide a session hijacking capability.

Firewall reconfiguration. This is the ability to automatically re-configure firewalls. This feature enables the IDS to take active response to critical security events.

Key for Table 2-1:

- *yes* means that there is a capability for the IDS, when so customized (see Flexibility, Attack and Misuse Response, Section 2.2.2), to reconfigure specific firewalls (see Supported Applications, Firewalls, Section 2.3).
- *no* means that the IDS does not provide the ability for the IDS to reconfigure any firewall.

Router/Switch reconfiguration. This is the ability to automatically re-configure routers or switches. This feature enables the IDS to take active response to critical security events.

Key for Table 2-1:

- *yes* means that there is a capability for the IDS, when so customized (see Flexibility, Attack and Misuse Response, Section 2.2.2), to reconfigure specific routers or switches (see Supported Applications, Routers/Switches, Section 2.3).
- *no* means that the IDS may not reconfigure any router or switch.

Deception Techniques. The ability to automatically apply deception as a means to counter attacks. Typical methods include producing misleading output in response to a suspected attack, so as to delay the possible attacker while more evidence in gathered, or to divert the attacker away from critical systems.

Key for Table 2-1:

- *yes* means that there is a capability for the IDS, when so customized (see Flexibility, Attack and Misuse Response, Section 2.2.2), to apply deception responses to attacks.
- *no* means that there is no capability for the IDS to respond to attacks with deception.

Vulnerability correction. The ability to automatically correct misconfigurations that leave a system vulnerable to attack.

Key for Table 2-1:

- *yes* means that there is a capability for the IDS, when so customized (see Flexibility, Attack and Misuse Response, Section 2.2.2), to reconfigure vulnerable systems.

- *no* means that there is no capability for the IDS to reconfigure vulnerable systems.

2.2.8 Acquisition

Whether a user acquires a particular IDS product or not will depend on three features. They include how the product is implemented (which can affect its cost and usability), whether it can be exported as built, and its overall cost.

Implementation. Whether the IDS is implemented solely as software, or whether a specific and specially configured platform must also be used. Most commercial IDS are software solutions that can be installed on a variety of standard off-the-shelf (OTS) workstations (given sufficient memory and disk storage), but a few require specially configured versions of standard workstations. A very few are sold as integrated hardware/software systems. Hardware limitations can affect the flexibility and cost of an IDS product. On the other hand, some users may want the ease of a turnkey system.

Key for Table 2-1:

- *s/w* means that the IDS is sold as a software module that may be installed on a standard off-the-shelf commercial platform, provided CPU, memory, and disk storage requirements are met.
- *h/w* means that the IDS is sold as a software module but requires a specially configured version of a standard workstation; i.e., that the software is such that the system requires not only a dedicated machine, but also a specially configured one.
- *both* means that the IDS is sold only as an integrated hardware/software system.
- *turnkey* means that the IDS vendor offers the option of a complete, ready to run system.

Exportability. Whether a US-built IDS may be exported. To any user outside the US, a critical issue is whether the IDS may be exported at all as originally designed (i.e., some types of cryptography may not be exported). In some cases, the vendor may provide modified versions for export, but in this case the user must be aware of the ramifications.

Key for Table 2-1:

- *yes* means that the IDS may be exported, as built.
- *special* means that the IDS vendor provides a special version of the IDS for export.
- *no* means that the IDS may not be exported.

Deployment Cost. What it will cost the user for one management console, one sensor, the software for each, plus one year's support. This measure is intended only to provide a "ballpark" estimate for comparison reasons. It does not include the cost of personnel to install, manage, and use the system for that time period. Costs diverge widely from one IDS product to another.

2.2.9 Support

There are a number of features that can make an IDS product eminently more useful to a user; and in fact can determine whether the product is even considered for purchase, or if acquired, is effectively used. These include:

Product information. Critical to any product's success is readily available and comprehensive information about it. The first and most critical source is the product's Web site, which at the very least must provide top-level information along with directions to readily available additional documentation (e.g., urls, email or phone contacts). This is a measure of how difficult (or impossible) it was to obtain pertinent information, and the overall quality of the information (i.e., accurate, complete and up-to-date, comprehensible, and with a minimum of misleading hype).

Key for Table 2-1:

- *great* means that a web site exists, is easy to navigate, factual, complete (contains the information required to determine all product characteristics and features), and is generally of exceptionable quality. This also means that when requested, supplemental good-quality documentation was promptly provided.

- *ok* means that a web site exists, is of passable quality and content, but is incomplete and requires that the vendor be contacted for further explanation and clarification. This also means that, when contacted, the vendor responded, and supplied good information to supplement the web site.
- *poor* means that a web site exists but it is of such quality and content as to be only marginally useful (e.g., consists of superficial, incomplete, out-of-date, or erroneous information). This also means that either the vendor was impossible to contact, or when contacted, failed to provide supplemental good-quality documentation.
- *none* means that no web site exists.

Vendor response. A critical and sometimes neglected feature of any product is a workable means by which to query the vendor, coupled with a responsive vendor.

Key for Table 2-1:

- *great* means that vendor contact information was found on the product's web site, that at least an acknowledgement to queries was received within two work days, with a complete and accurate response following within another week.
- *ok* means that vendor contact information was found on the product's web site, that at least an acknowledgement to queries was received after no more than two queries, and that complete and accurate response was eventually received.
- *poor* means that vendor contact information was found on the product's web site, but that repeated queries were needed and/or the quality of the provided information was poor.
- *none* means that either no vendor contact information was found on the product's web site (or the product had no web site) or that no response to queries was received.

Attack definition update. A critical feature of knowledge-based IDS is a comprehensive a set of attack/invalid activity rules or signatures. The quality of the signature database, including its update frequency (i.e., are signatures provided immediately upon identification of a new attack, or must the user wait for a new version of the IDS).

Key for Table 2-1:

- *web* means attack definition updates are provided immediately after new attacks are incorporated on a secure web site.
- *e-mail* means attack definition updates are provided immediately after new attacks are incorporated via encrypted e-mail.
- *version* means attack definition updates are provided only with periodic software version updates.
- *none* means no attack definition updates are provided.

2.3 Applicability

Potential users of IDS products have endlessly varied enterprises. The features that determine the IDS product's ability to interpret the local environment's information include what operating systems, network topologies, protocols, and applications are supported. Table 2-2 specifies to which of these the IDS product is applicable.

2.3.1 Targets

Operating systems that the as-delivered system is designed to monitor. An effective host-based IDS must be designed to monitor a variety of (and at least the most common) operating systems.

Key for Table 2-2:

- A specific operating system is checked when the IDS is designed to monitor it.
- *other* means that the IDS is designed to monitor an operating system that is not specified.
- *none* means that the IDS is host-based but is not designed to monitor any operating system.
- *n/a* means the IDS is network-based, and therefore is not designed to monitor host-based activity.

Network topologies that the as-delivered system is designed to monitor. An effective network-based IDS must be designed to monitor a variety of (and at least the most common) network topologies.

Key for Table 2-2:

- A specific topology is checked when the IDS is designed to monitor it.
- *other* means that the IDS is designed to monitor a topology that is not specified.
- *n/a* means that the IDS is host-based, and therefore is not designed to monitor network activity.

Table 2-2: Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems											
SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a

Supported Protocols (Section 2.3.2)

Network Application Protocols												
DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a

Network Protocols														
UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers												
Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none	n/a

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a

Firewalls										
ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a

Reconfigured Applications

Web Servers											
Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none

Firewalls									
ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none

Switched network capability. With the spread of the use of switched networks, network-based IDS should make provision for cost-effective monitoring in such an environment. The solution must be an integral part of the product, must not be prohibitively expensive (such as a sensor for every broadcast domain or segment), and must not degrade the performance of either the IDS or some network component such as a switch or router.

Key for Table 2-2:

- *yes* means that the IDS includes some effective provision for switched networks.
- *no* means that the IDS does not include an effective provision for switched networks.
- *n/a* means that the IDS is host-based and thus the issue of switched networks is not applicable (i.e., the effectiveness of a host-based system is not directly affected by network architecture).

2.3.2 Protocols

Protocols monitored. To be useful, a network-based IDS must be able to interpret the network data stream extant in the user's environment. If a network-based IDS cannot interpret a given protocol, that information will be missed entirely.

Key for Table 2-2:

- A specific protocol is checked when the IDS, as delivered, is programmed to decode and monitor it.
- *other* means the monitored protocol is not among those specified.
- *n/a* means that the IDS is host-based and therefore is not designed to decipher network protocols.

2.3.3 Applications

Applications may be monitored by host-based IDS products and reconfigured (at least in theory) by any IDS product. For example, a host-based IDS may monitor a web server for misuse, then shut down and/or rebuild the server if misuse is detected. In another example, a network-based IDS may reconfigure a firewall as a response to detected intruder activity.

2.3.3.1 Monitored

Some host-based IDS products are designed to monitor a specific application, rather than a specific operating system, so must be able to interpret the appropriate audit records. Network-based IDS products do not monitor applications.

Key for Table 2-2:

- A specific application is checked when the IDS, as delivered, is programmed to monitor it.
- *other* means there is a monitored application is not among those specified.
- *none* means that the IDS is host-based, but is not designed to monitor this type of host-based application.
- *n/a* means that the IDS is network-based, and thus is not designed to monitor any host-based application.

2.3.3.2 Reconfigured

Some IDS products are designed to reconfigure specific applications such as routers and firewalls.

Key for Table 2-2:

- A specific application is checked when the IDS, as delivered, is programmed to reconfigure it.
- *other* means a reconfigured application is not among those specified.
- *none* means that the IDS cannot reconfigure any application.

2.4 Attainment

The final step in an IDS assessment is to determine how well each product actually performs critical functions in a real world environment, how well it measures up to its advertised capabilities, and how it compares to similar products. The general areas that must be addressed to measure product attainment are summarized in this Section. This document does not attempt to ascertain the attainment of any surveyed product. That step requires a full-scale product evaluation, something GSAL has not yet completed. However, where possible, links are provided to evaluations that have been undertaken by others.

2.4.1 Performance

Performance is a measure of the volume of information the IDS can effectively, accurately, and completely process in real-time. The IDS must be able to correctly handle, in real-time, the quantity of information generated on the systems it is purported to support, whether it be network traffic, system logs, or application output.

2.4.2 Robustness

Robustness is a measure of the IDS's ability to recover from system failure. Included must be a determination of whether a surge of network activity or the temporary failure of a communication path or critical node can cause the permanent loss of information or the failure of the IDS itself.

2.4.3 Accuracy

Accuracy encompasses the number of false negatives (missed events) and false positives (benign activity that is identified as malignant events). System accuracy is directly linked to such things as the comprehensiveness of the initial signature data base, the ability to fine-tune to the system being monitored, and. to timely and high-quality event signature updates.

2.4.4 Interference Potential

An effective IDS must be designed to perform its monitoring function without placing an unacceptable load on any portion (host, server, communications) of the monitored system. An unacceptable load is when the IDS interferes with or disrupts normal system operations. This interference may be indirect, as in cases when invoking sufficient audit records for the IDS to work disrupts other host activities or even causes a system to crash. This measure must be assessed for every operating system, application, or network topology, as the IDS product's system impact may vary from one system to another. Included must be a determination of whether a surge of invalid activity can lead to denial of service by causing the IDS to overload the network with event reports or overwhelm servers with connection requests.

2.4.5 Tamper Resistance

Tamper resistance is a measure of how well the IDS product protects itself from malicious interference and user carelessness. A tamper resistant IDS will effectively monitor itself for signs of abuse, employ stealth techniques on the network, protect its on-line information and especially communications with encryption, and employ a privilege management scheme on its management console. Included must be a determination the effect of system changes to allow exportation on the system's ability to protect itself.

2.4.6 Utility

Utility, or ease of use, encompasses the technical expertise needed to manage and use the IDS. A measure of the technical expertise to manage the IDS includes the level of technical capability needed to install and maintain the IDS, including making configuration changes and modifying attack definitions. A measure of the technical expertise to use the IDS includes the level of technical capability needed to generate and understand reports and respond to events. Required expertise will be influenced by vendor-provided documentation, the user interface, the types and clarity of alarms and reports, the level of vendor support, the worth of the vendor-supplied Attack Database, and of course how well the system is designed. A very high level of technical expertise for even system management, and especially system use, can directly and adversely affect overall system cost.

3 Utilizing Products

Commercial IDS are developing into beneficial network security tools (Section 3.1). However, several issues must be taken into account by anyone considering employing such a system in the near future (Section 3.2). First, IDS products clearly have inherent limitations that are a reflection of this emergent technology (Section 3.2.1). Second, implementation of IDS technologies has presented its own challenges, some of which have thus far resisted complete solution (Section 3.2.2). Third, IDS is an immature market where prices vary widely and major re-tooling probably will occur over the next couple of years (Section 3.3). Finally, given the combination of promise and limitation inherent in commercial IDS, realistic expectations by any potential user will not only facilitate decision-making, but also offer a much greater probability of product satisfaction (Section 3.4).

3.1 Benefits

When used conscientiously and knowledgeably, IDS products can provide worthwhile indications of malicious activity and spotlight security vulnerabilities, thus providing an additional layer of protection. Without them, network administrators have little chance of knowing about, much less assessing and responding to, malicious and invalid activity. Properly configured, they are especially useful for monitoring the network perimeter for attacks originating from outside and for monitoring host systems for unacceptable insider activity. In addition, they can help validate (or refute) the merit of local security policy and practices.

What current IDS products can do is automatically review massive amounts of network and system data in real-time, identify suspicious activity, provide real-time automated notification to security personnel; guide further investigation, and sometimes automatically respond to specified attacks. Properly used, an IDS product can detect common attacks, attempts to exploit known weaknesses, network probes, or critical resource overloads in a reasonably timely manner [4, 6]. Some products provide the capability (with customizing) to detect activity that is counter to local security policy. Many products keep comprehensive logs and generate good reports and some include the ability to analyze today's activity in view of yesterday's activity to identify larger trends (trend analysis). By identifying successful invalid activity, IDSs can indirectly spotlight network and system vulnerabilities, enabling fixes and fine-tuning. In sum, an IDS can enable network personnel to know what’s really happening on a network; thus enabling them to make informed security decisions.

3.2 Limitations

Proper selection and effective utilization of IDS products requires that the user be as aware of their limitations as their strengths. Current IDS product shortfalls are mostly a reflection of the uniqueness and recent development of IDS technology. IDS vendors know about and are addressing these shortfalls and there is every indication that the extremely competitive and growing market will result in the rapid technological innovation needed [11] to correct or mitigate them.

3.2.1 Inherent

Current IDS products are limited by what IDSs are designed to be, and by the technologies they currently employ:

1) Knowledge-based IDS can only detect that which they are programmed to detect, and thus require prior knowledge of invalid behavior. All knowledge-based commercial products use “signatures” for detecting attacks. These signatures are descriptions of known methods and procedures for exploiting known security holes. They are compared to current activity, and when a match is found an alarm is sounded. When a comprehensive and up-to-date set of attack signatures is used, this approach is fairly reliable but limited for the following reasons:

    a. The number of known security vulnerabilities is large and the techniques to exploit those vulnerabilities myriad. As a result, effective signature databases are difficult to design and maintain, and their execution may become huge and unwieldy.

    b. Many applications and systems have unknown and undocumented holes, so new vulnerabilities are constantly being discovered.

c. Attackers frequently find and exploit holes first, or find new exploits for known holes. The IDS will miss these until the vendor realizes the deficiency, updates the signature database, and provides it to the user.

d. Invalid behavior by the knowledgeable and privileged insider is harder to both predict and detect, since the insider already has access to the system (thus doesn't need to break in), can legitimately perform many activities, and sometimes considerable knowledge of applied security measures.

2) Behavior-based IDS attempt to "understand" the flow of traffic within the network or user behavior on a system, and to "learn" from it, so as to model what is "normal." They then attempt to detect invalid behavior by identifying anomalies from that normal (i.e., anomaly detection). While not requiring prior knowledge of invalid behavior, they thus far present technical difficulties that have limited their deployment in commercial products:

a. Normal (or usual) behavior may also include forbidden behavior, so excluding this activity from a normal data set in a production environment is extremely difficult.

b. Users very frequently do not present consistent behavior; i.e., while undertaking perfectly valid activity they often deviate from a "normal" profile and thus cause many false positives. Such things as deadline pressure, vacations, or just general user contrariness can cause deviations from normal. In the most extreme case, a completely new behavior profile may be immediately exhibited as a result of a job change or a new assignment.

c. If the system employs a profiling system that adjusts to new user activity over time, knowledgeable, patient, and malicious users can gradually (so as not to cause a suspicious level of alerts) "train" the system to accept invalid behavior.

d. Behavior-based IDS usually require extensive tuning to the local environment and security policy, and frequently require intervention to make adjustment for changes in user behavior, which calls for large operational overhead.

e. As a result of the above points, they are prone to generating unacceptable numbers of false alarms (false-positives).

3.2.2 Implementation

In addition to those inherent to the technology, IDS products are susceptible to a variety of implementation difficulties and limitations.

3.2.2.1 Network-Based IDS

1) Direct attack susceptibility. A recently released a study by Secure Networks, Inc. of leading network-based IDS products [2] found that network-based IDS are susceptible to:

a. Packet spoofing, which tricks the IDS into thinking packets have come from an incorrect location.

b. Packet fragmentation attacks that retransmit sequence numbers so that the IDS "sees" only what a hacker wants it to see.

2) Indecipherable packets. Because of network heterogeneity and the relative profusion of protocols, network-based IDSs often cannot decipher the packets they capture. In addition, in the absence of something like a corporate key, no IDS can decipher encrypted information.

3) Failure when loaded. A recent evaluation of leading network-based commercial products found that products that detect all tested attacks successfully on an empty or moderately utilized network have been found to start missing at least some attacks when the monitored network is heavily loaded [9].

4) Failure at wire speed. While network-based IDS can process packets on low-speed networks (10 Mbps), few claim to be able to keep up and miss no information at 100Mbps or higher.

5) Complete coverage. Most sensors are designed to be installed on shared-access segments, and can monitor only that traffic running through those segments. To provide coverage, the IDS user must se-

lect key shared-access segments for IDS sensors. Most frequently they place sensors in the demilitarized zone and, in some cases, in front of port and server farms. To monitor distributed ports, internal attack points, distributed Ethernet connections, and desktops, many sensors must be installed (at a considerable price). Even then, elastic (perhaps unauthorized) connections such as desktop dial-ins and modems will not be monitored.

6) Switched networks. To make matters worse, switching has replaced shared/routed networks as the architecture of choice. Switching effectively hides traffic from shared-access network-based IDS products. Switched networks fragment communication and divide a network into myriad micro segments that make deploying shared-access IDS prohibitively expensive (i.e., to provide coverage, very many sensors must be deployed). Vendors are aware of the problem and are beginning to address the issue, if only as part of their marketing[2]. Some recommend attaching hubs to switches wherever switched traffic must be monitored. Others suggest "mirroring" selected information (such as that moving to specific critical devices) to a sensor for processing. None of these are easy or ideal solutions.

7) Insiders. Network-based IDS focus is on detecting attacks from outside, rather than attempting to detect insider abuse and violations of local security policy.

3.2.2.2 Host-Based IDS

1) Indecipherable information. Because of network heterogeneity and the profusion of operating systems, no single host-based IDS can translate all operating systems, network applications, and file systems. In addition, in the absence of something like a corporate key, no IDS can decipher encrypted information.

2) Indirect information. Rather than monitor activity directly (as do network-based IDS), host-based IDS usually rely heavily or completely on an “audit record” of activity that is created by a system or application. This audit record varies widely in quality and quantity between different systems and applications, thus dramatically affecting IDS effectiveness.

3) Complete coverage. Host-based IDS are installed on the system being monitored. On very large networks this can comprise many (even tens of) thousands of workstations. Providing IDS on this scale is first, very expensive, and second, difficult to manage.

4) Outsiders. A host-based IDS can potentially detect an outside intruder only after the intruder has reached the monitored host system, not before, as can network-based IDS. To reach a host system, the intruder must have already bypassed network security measures.

5) Host interference. Host-based IDS have been known to place such a load on the host CPU as to interfere with normal host operations. On some systems, just invoking an audit record sufficient for the IDS can result in unacceptable loading.

3.2.2.3 All IDS

1) Direct attack susceptibility. The study by Secure Networks, Inc. also found that IDS products are susceptible to:

    a. The attacker deliberately invoking IDS countermeasures that cause it to cut connectivity to legitimate sites;

    b. Denial-of-service attacks that cause the IDS to flood routers, web servers, and firewalls with too many requests for connection, which can cause them to shut down.

2) Activity that leaves no record. No conventional IDS can detect passive activities such as sniffers (readily available tools that hackers use to watch traffic and capture passwords), though IBM’s GSAL is currently developing an innovative “decoy” approach to this issue [10].

[2] Given the information they process (i.e., audit records, files, directories, etc.), host-based IDS are not affected by network design choices. Therefore, a claim that a host-based IDS “solves” the problem of switched networks really fails to address the issue in question.

3) Integration. Better integration is needed among tools and products for centralized management of intrusion detection and other security services.

4) Correlation of events over an enterprise. Much work still needs to be done to correlate security events detected at various locations throughout an enterprise, and to generate from them a meaningful representation of enterprise-wide threats and vulnerabilities.

3.3 Evolving Market

Commercial IDS is a relatively immature, highly competitive, and rapidly evolving market. In response to lessons learned in their first years of deployment and rapidly increasing market demand [3. 7}, these systems are likely to undergo considerable technical change in the near future. These changes will include:

1) Integrating IDS into the fundamental network infrastructure (such as into routers and switches).

2) Adding agents or sensors that process information from a wider variety of sources (beyond the current reliance on host logs and network packets).

3) Consolidating IDS with other security tools (such as vulnerability scanners) and with network management tools.

4) Correlating the security events detected at various levels into a meaningful representation of enterprise-wide threats and vulnerabilities.

5) Enabling relatively easy customization to the local environment so as to avoid large numbers of false positives.

6) Solving wire speed processing problems.

3.4 Realistic Expectations

Potential IDS users often know little about product capabilities and must attempt to sort through a barrage of product claims. Given the issues covered in the previous Sections, what can realistically be expected from any current IDS product? We have concluded that:

1) It is unrealistic to expect an IDS to detect new hitherto unknown attacks. The problem of detecting something undefined is a difficult one, and effective means to do so are still under investigation. The only IDS products that can even attempt this are those very few that use a behavior-based approach, and even these have limited capability.

2) It is unrealistic to expect any IDS to detect all (or perhaps even most) malicious insider activity. Insiders have the benefit of some level of legitimate privilege and access (including physical access), and may be very knowledgeable of applied security measures.

3) It is realistic to expect at least some, and perhaps many, false alarms. IDS products unfortunately cannot measure intent, and well-meaning users can generate very suspicious-looking activity. Therefore, to work effectively, the IDS may need considerable on-going and expert fine-tuning.

4) It is unrealistic to expect IDS to be operable in "hands-off" mode; i.e., to need no expert attention once installed. Any existing IDS product or one available in the near future, will require constant monitoring, fine-tuning, alarm investigation, and maintenance by highly knowledgeable and capable technicians.

5) It is unrealistic to expect an IDS to be able to automatically protect a network from all threats (i.e., detect all attacks in real-time, and take automatic and effective deterrent action). First, because of the certainty of false alarms, and second, because automatic responses can be used by hackers to deny service, proactive responses must be approached with extreme caution. They are in themselves dangerous, since the reaction may cut off innocent individuals or shut down entire networks or services, thus cutting off many innocent (and furious) users. Mistakes of this sort are politically incorrect in most corporate and government entities. If done to another's network or users, they are usually illegal and inevitably bad press.

6) It is unrealistic to expect current IDS products to scale to an enterprise environment. Even though some are being marketed as "enterprise" solutions, they are not integrated sufficiently with other security tools and with sophisticated Network Management Systems to provide an enterprise solution. With their focus on the host and network level, they cannot yet provide an accurate assessment of enterprise level threats and vulnerabilities.

3.5 Conclusions

IDS technology is developing rapidly and its near-term future is very promising. It will soon be seen as an indispensable and integral component of any comprehensive enterprise security program. Properly and skillfully used, both network- and host-based IDS products can provide considerable value, but scale best to small- to moderate-sized networks.

However, the issues addressed throughout this Section lead to some inescapable conclusions:

1) While many attacks will be detected, some will be missed. For every real attack, there will be more (probably many more) false positives.

2) Even after installation, IDS products will need the continuous attention of a staff of knowledgeable and skilled technicians to:

   a. Tune and customize the IDS to the local environment in order to keep false positives to an acceptable level

   b. Investigate and respond to many alarms. Some of these will be false positives or nuisance attacks, but nonetheless must be investigated and resolved.

3) Network-based IDS currently work best in non-switched, fairly low-speed networks.

4) While many vendors advertise their IDS's active response capabilities, the installation of automatic active alarm responses in an environment where there are any false positives (i.e., anywhere) should be done with extreme care.

It is clear though, that under the pressures of a highly competitive market, IDS products will re-tool rapidly and overcome many current obstacles.

4 Products

The advent of IDS products is a relatively recent, and after a period of steady development the field is now undergoing explosive growth. IDS products have been in existence only since the early nineties, when CMDS (1991), Intruder Alert (1992), and Stalker (1993) were released. A few more products emerged within the following several years, including Kane Security Monitor (KSM), RealSecure, and NetRanger in 1996, and Anzen Flight Jacket (AFG) and WebStalker in 1997. Since then, at least ten new products have been announced. This period also saw the apparent departure[3] of several contenders, including InTouch INSA, CyberCop Network, CyberCop Server (née WebStalker), and Stalker. As of June 1999, we identified a total of seventeen seemingly extant IDS products. They are summarized in Table 4-1.

Table 4-1: Current IDS Products

Product	Deployment Strategy		Information Source							Method		Real-time Processing		Initial Release
	net-based	host-based	network packets	OS	Web server	router	firewall	file system	other	knowledge	behavior	yes	no	Year
1. Anzen Flight Jacket (AFJ)	X		X							X	X	X		1997
2. Centrax	X	X	X	X						X	X	X		1998
3. Computer Misuse Detection System (CMDS)		X		X			X			X	X	X		1991
4. Cross-Site for Security	X		X							X		X		1998
5. CyberCop Monitor		X		X						X		X		1999
6. Intruder Alert		X		X		X	X		X	X		X		1992
7. Kane Security Monitor (KSM)		X		X						X		X		1996
8. NetProwler	X		X							X		X		1997
9. Net-Ranger	X		X							X		X		1996
10. Reactive Intrusion Detection (RID)		X					X			X		X		1998
11. RealSecure	X	X	X							X		X		1996
12. SecureCom Switches	X		X							X		X		1997-8
13. SecureNet PRO	X		X							X		X		1997
14. SessionWall-3	X		X							X		X		1997
15. SMARTWatch		X			X			X		X		X		1998
16. Stakeout	X		X							X		X		1998
17. Tripwire		X						X		X			X	1998

Under the pressure of intense competition in this rapidly growing market, the last year has seen a flurry of acquisitions and product transformations, as major players in the field attempt to assemble comprehensive suites of security software:

- Trusted Information Systems (TIS) acquired Haystack Labs (which developed Stalker, WebStalker, and NetStalker), and shortly thereafter was itself acquired by Network Associates (NAI). Calling it CyberCop Server, for a few months NAI marketed WebStalker with their existing network-based product CyberCop Network (a version of NetRanger that had been acquired from Network General). Within months both CyberCop Network and CyberCop Server had vanished from NAI's product line, to be replaced by a new host-based product called CyberCop Monitor. CyberCop Monitor is marketed as one component of the NAI Intrusion Protection Suite, which includes a vulnerability scanner (Cyber Cop Scanner) and a decoy (i.e., honey pot) server (CyberCop Sting).

[3] While vendors are sometime somewhat precipitous in announcing new products, they rarely announce their demise. One sometimes has to deduce product status from such indirect evidence as long neglected web pages, the absence of press releases, and lack of response to queries.

- AXENT Technologies announced a network-based IDS called NetProwler to pair with its long-standing host-based IDS (Intruder Alert), then within months acquired the network-based IDS ID-Trak from Internet Tools and renamed it NetProwler. It appears the new NetProwler simply replaced the old. Both Intruder Alert and NetProwler are (or in NetProwler's case, will soon be) components of OmniGuard, AXENT's suite of integrated software tools.

- Cybersafe Corporation acquired Centrax Corporation and changed the name of Centrax's network and host-based IDS from eNTrax to Centrax. Centrax joins Cybersafe's suites of authentication (TrustBroker) and encryption (Defensor) security tools.

- Cisco Systems, Inc. acquired WheelGroup, Inc. and its network-based IDS NetRanger, retaining the product's original name. NetRanger joins Cisco's suite of vulnerability assessment (NetSonar), authentication, encryption, and policy management security tools. Cisco has the stated intention of integrating NetRanger into its line of routers, switches, and firewalls.

- Security Dynamics Technologies, Inc. acquired Intrusion Detection, Inc. and its host-based IDS Kane Security Monitor (KSM), retaining the product's original name. KSM is part of Security Dynamics' suite of authentication (SecureID), encryption (Keon), and vulnerability assessment (Kane Security Analyst) security tools.

- MEMCO Software, Inc. acquired Abirnet, Ltd., which developed SessionWall-3, in May 1998. MEMCO was in turn acquired by Platinum Technologies International, Inc. in August 1998. The product's original name has thus far been retained. SessionWall-3 joins Platinum's suite of hacker blocking (Secured) and auditing (Audit Central) security tools.

While none of these newly merged companies have yet to completely integrate their various security products, a clear trend emerges. It seems apparent that in the future most IDS products will be offered as part of a security solution, together with other security products, and in some cases integrated into all-inclusive security packages. They may also be included within comprehensive network management systems, or in some cases incorporated into the network infrastructure itself (i.e., into routers and switches).

Most IDS products offer either host or network-based processing, with network-based systems holding a small numerical edge. This edge becomes more pronounced when one observes that only five host-based products monitor operating system audit records; the rest monitor special applications and/or file systems and are quite limited in scope (albeit still useful). At least when using this criterion (number of product offerings), there appears a clear bias towards network-based IDS products. Given the looming twin challenges of high-speed and switched networks, it remains to be seen if this tendency will persist in the future.

Integration of the two deployment strategies (host and network-based) within one product has been slow in coming, even though they are complementary approaches and their effective combination has the potential to enhance monitoring capability. As of now, only two products offer both host and network-based processing in one package. Centrax, developed as a host-based system, has recently added a network-based component. RealSecure, conversely, was developed as a network-based system, and recently added a host-based component. In addition, one vendor (AXENT) offers both host and network-based IDS in its suite of tools (Intruder Alert and NetProwler, respectively). They can be managed from a common console, but are clearly separate products that can be sold and (at least for now) execute independently of each other.

It is interesting to note that knowledge-based methodology is universal while behavior-based methodology is rare. In the IDS research community, anomaly detection was initially expected to provide the foundation of intrusion detection [1]. However, difficulties were encountered when attempting to utilize anomaly detection, especially in products intended for many, varied, and constantly changing environments. Knowledge-based approaches are, in contrast, much more straightforward to implement and manage, and as a result have become the implementation of choice. In those cases where behavior-based methodology is included, it appears to be secondary to the knowledge-based component and in some cases is clearly optional.

Almost all IDS products support real-time processing; something that is mostly the result of processing realities. The quantity of data that usually must be managed (especially that produced by network traffic) makes after-the-fact processing untenable, except for such activities as specific event replay. In addition, almost universally held is the opinion that attempted intrusion and misuse must be detected immediately, even though reaction times to reported events are generally on a more human scale (automated responses being rarely invoked).

All available information for each product is assembled and categorized in the following Sections. No attempt is made to indicate *how well* the product performs each indicated capability; only to specify what it was designed to do. The amount, quality, and creditability of available information (e.g., on the Web, in the literature, through technical contacts, from vendors) varied widely, something that correlated most strongly (but not always) to product maturity. Vendor response to queries also varied widely; from none to substantial. As a result, the following individual product sections are somewhat uneven in quality and quantity of content. Prior to publication, considerable effort was expended attempting to contact each vendor, so that they might comment and provide input. This effort is an on-going process, as we continue to endeavor to maximize the content and accuracy of this survey. In this vein, we welcome criticism and commentary from our readers.

4.1 Anzen Flight Jacket

Table 4.1-1: Anzen Flight Jacket - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X		X					X	X	X			X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distrib-uted	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
X	X	X	X				X			X			

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse defini-tion			attack and misuse re-sponse			connection event			protocol defini-tion			audit record definition			reports			encryption options			security op-tions			other		
X			X			X			X					X		X				X	X					X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentica-tion	user access control	user privilege mgt	none	manager-agent verifi-cation	manager-agent data encryption	secure software updates	none
X		X		X	X	X		X	X	X	

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Man-agement System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
		X	X				X		X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java app-lets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data con-sistency	system behavior	other	none
				X		X		X	X	X	

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	informa-tion	analysis	fixes	counter-measures	none
X			X			X		X	X	X			

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X		X		X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X			X		X				X	X	

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X			X				X	X	X	

Table 4.1-2: Anzen Flight Jacket - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
												X

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	none	yes	no	n/a
X	X			X							X	

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
X	X	X		X	X	X	X	X	X	X		

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
X	X	X	X		X			X			X	X	X	

Supported Applications (Section 2.3.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
						X							X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company Anzen Computing, Inc.

Manager 450MHz Pentium II, with 96-128 MB RAM, 18 GB hard disk. Hardware for faster networks is available (500MHz, 384 MB).

A proven reliable network adapter card (ex. Intel Ether Express Pro and DECtulip) is a must, as some cards fail under bursty network traffic.

Anzen Flight Jacket for NFR is supported on BSD/OS > 3.x, OpenBSD >2.4, and Solaris >2.6.

Sensors Same as Manager or standalone NFR.

Targets

Topologies
10Mb/s Ethernet, 100Mb/s Ethernet, FDDI
Network Protocols
IP, TCP/IP, and UDP based protocols. Additional support for IPX/NETBUI is under consideration.
Application Protocols
DNS, HTTP, FTP, NFS, SNMP, TELNET, SMTP, and RSH. X-WIN and SSL/SSH are in development.

Interoperability

Apache Web Server, DataFellows communications software, Netscape Navigator.

Protection

Apache Web Server with SSLeay, Raven SSL module.
DataFellows Secure SSH communications software (optional).

Reports

Maintains data and can produce written reports on a segment by segment basis.

NFR provides a Java-based GUI that reports lists of events or a statistical analysis of events in HTML, plain text, or comma-delimited formats (for exporting). Also included are tools for generating bar graphs, pie charts, and scatter plots.

The NFR GUI also allows the user to browse the data and search for specific events.

Alarms

Basic Unix alerts to an attack, including console and syslog messages, e-mail, fax, and paging. SNMP Trap. Log and trace files.

Response to events

As shipped, does not provide reactive capabilities. However, a user can write a package (N-code and backend) to reactively respond to a specific condition. Additionally, reactive code can be added to the alert system to be executed when a specific alert condition occurs.

Performance

Anzen Flight Jacket for NFR is a distributed system able to handle a manager to sensor ratio of 1:20. Only a few seconds are required to install, reconfigure, or upgrade a sensor from a manager. AFJ sensors are able to comprehensively sniff loaded and high speed networks: full 100 Mbps Fast Ethernet (100baseT) or FDDI sniffing as indicated in Data Communications lab tests.

Customization

Extensive and flexible capability for the user to implement custom attack filters and the ability to decode additional protocols as deemed necessary by their individual site requirements.

Special Features

N-code custom traffic-analysis engine and end-user programmability.
Protocol verification.

History

Current version of AFJ for NFR v2.0 released in December 1998.
AFJ for NFR v2.1 proposed release date in Spring 1999.
NFR initial released in December 1997.

Information

Sites:
http://www.anzen.com/products/nfr
http://www.nfr.com/.
http://www.Datafellows.com/
http://www.covalent.com
Support:
Phone: (734) 669-0800
FAX: (734) 669-0404
e-mail: info@anzen.com

Cost

Anzen Flight Jacket costs about $15,000 with Hardware. It includes one year of NFR upgrades, one year of unlimited support via e-mail contact, one year of OS updates, and one year IDS subscription service.

A deployment cost of 10-20K includes:

1. a turnkey system
2. Anzen Flight Jacket for NFR
3. NFR commercial license and one year of upgrades
4. IDS subscription service and one year of support

A deployment cost of <10K includes:

the same as above only without hardware

Evaluations/ Comparisons

Digital sentries, InfoWorld May 4, 1998
http://www.infoworld.com/cgi-bin/displayTC.pl?/980504comp.htm
Intrusion Detection Systems: Suspicious Finds, Data Communications, August 1998 http://www.data.com/lab_tests/intrusion4.html.

Comments

A high performance Intel-based turnkey option is available.

Anzen Flight Jacket (AFJ) is a user-programmable, network-based intrusion detection and traffic analysis system. AFJ is an integrated software package containing Network Flight Recorder (NFR) technology, client software from DataFellows, and the BSD or Solaris operating system. AFJ applications are layered on the base NFR engine.

NFR was originally intended to be a generalized tool used for monitoring networks. It is a passive listening device that observes all network traffic in real-time and makes decisions based on traffic content. Its key strengths are: 1) its extensibility to perform a wide variety of network monitoring tasks and 2) its ability to view packets from the network layer through the application layer, including reassembled TCP streams and fragmented traffic. NFR itself offers only a framework for intrusion detection. To get NFR to monitor for malicious activity, N-code programming is required. The N-code language is a pre-emptive, event-driven scripting language that lets the creation of “filters” that are applied to the traffic analysis engine. Filters are written in N-code, which are read into the engine, compiled, and converted to byte code. NFR relies on resellers, like Anzen, to implement, upgrade, and customize the NFR solution to users' individual needs and provide technical support.

AFJ is implemented in a distributed architecture that comprises a centralized command console and one or more sensors that are placed at selected locations throughout the network. The command console provides a central environment for configuration management, administration, and the collection and analysis of security relevant status from each sensor. The sensors capture and analyze network packets and forward status information to the command console. AFJ may also be deployed in a stand-alone version that integrates management console and sensor functions into one system. AFJ can be used in switched environments where a monitor port is available for promiscuous monitoring of on a switch. Some switches have a 'traffic steering' capability which may be also used to send traffic to a sensor.

AFJ largely uses knowledge-based methodology. A set of pre-programmed NFR N-code misuse signatures is included in AFJ. An AFJ IDS managed subscription service can provide new N-code filters to protect against additional attacks. This list is constantly increasing as N-code is created for additional attacks. NFR updates signatures “as conditions warrant” and makes them available via their Web page. In addition, the Anzen Flight Jacket provides a broad and flexible capability for the user to implement custom attack signatures. AFJ also performs "protocol verification,” a form of anomaly detection where the system makes assertions about whether a given traffic stream follows the standard protocol, or deviates from it. This is implemented using state machines to follow each application protocol, as defined in appropriate RFCs. This methodology has been termed "transaction-based" or "equality matching" anomaly detection in the academic literature.

4.2 Centrax (née eNTrax) Security Suite

Table 4.2-1: Centrax - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X	X	X	X				X	X	X	X	X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X		X				X			X			

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
	X			X			X				X			X		X			X			X				X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt.	none	manager-agent verification	manager-agent data encryption	secure software updates	none
X			X	X					X		

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
		X		X	X				X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
				X	X	X			X		

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	counter-measures	none
X			X		X			X			X		

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X	X			X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X				X						X	

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X			X						X	

Table 4.2-2: Centrax - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI
	X				X	X					
DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
	X										X	

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
X	X	X	X	X	X	X	X	X				

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
	X		X											

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
						X							X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company Cybersafe Corporation

Manager IBM PC or compatible with 166 MHz processor, Windows NT Workstation or Server 4.0, 64 MB RAM, CD-ROM, 800x600 VGA monitor, 15 MB available disk space to install the program.

Sensors IBM PC or compatible with 166 MHz processor, Windows NT Workstation or Server 4.0, 64 MB RAM, CD-ROM, 800x600 VGA monitor, 15 MB available disk space to install the program.

Targets

Operating Systems

Windows Workstation or Server NT 3.5.1 or 4.0 and Solaris 2.5.1 and 2.6. Windows NT target computer requires an IBM PC or compatible with 80486 processor (minimum), Windows NT Workstation or Server 3.51 or 4.0, 32 MB of disk space to temporarily store audit data. Unix target requirements vary by platform.

Topologies

10Mb/s Ethernet

Network Protocols

TCP/IP

Application Protocols

DNS, HTTP, FTP, SMB, NFS, SNMP, TELNET, SMTP, and RSH

Interoperability

None specified.

Protection

All transmissions of audit policies, collection policies, and counter-measure responses between the command console and agents are encrypted.

Communication between agents and sensors uses a proprietary fault tolerant point to point protocol that persists even when the connection fails.

Centrax monitors attempts to access to it's executables and data files, generates an alert when connection to a target is lost, and alerts on unauthorized attempts to access to the audit data stream.

The current version of Centrax uses 40-bit Symmetric encryption, so it is exportable.

Reports

Customizable assessment reports. Reports may be output to console, printer, or file. They may be saved as various file formats: comma separated value, data interchange format, HTML, Lotus 1-2-3, RTF, text, Word, Excel.

Report types include:

- Activity Report by User
- Enterprise Activity Summary
- Enterprise Failed Logon Activity
- Enterprise Browsing Activity
- Enterprise Virus Activity
- Logon Session Report
- Statistical Report

Alarms

Console display of prioritized (3 levels), color-coded, alerts

E-mail, pager, or , or SNMP message to a management system.

Response to events

Increase security monitoring.

Log a user off.

Disable an account,

Shutdown a workstation.

Stopping a process.

Performance

One console can manage at least 100 sensors.

Customization

Audit policies.

Event logging.

Collection strategy (including event log delivery schedule).

Auditing strategy.

Specific intrusion response commands.

Reports by user, target, report type, date range, events, or activity signatures.

Special Features

In addition to intrusion detection, it provides periodic configuration assessment and configuration compliance checks.
Creates a comprehensive "paper-trail" that may be used for such things as prosecuting intruders and fraud detection.
Provides compound signatures that include events from both network sensors and host-based agents.

History

eNTrax was first released on 1 June 1998.
In March 1999, Centrax Corporation was sold to Cybersafe Corporation, and the IDS product eNTrax was renamed Centrax.
Current version is Centrax 2.2

Information

Sites:
http://www.cybersafe.com
Service:
Toll-Free Support: 1-888-246-8674
support@cybersafe.com
Information:
info@cybersafe.com
1-888-391-9922 or (425) 391-6000

Cost

The Centrax Security Suite is listed for NT with prices starting at $12,995 for one Command Console with agents for monitoring a network with 10 NT servers and 100 NT workstations. Actual cost is usually below $10K.

Evaluations/ Comparisons

eNTrax lags server guards, PC Week Labs, June 17, 1998 http://www.zdnet.com/pcweek/reviews/0615/15entrax.html

Comments

The Web page has been expanded and improved enormously in the last 6 months, and there have been many press releases.

Centrax is a combined host-based and network-based intrusion detection system that uses built-in attack signatures and statistical profiles to detect different types of misuse. The network-based and host-based components are an integrated package; they are not sold as two separate programs. In addition, a security configuration assessment (vulnerability scanner) component is included in the package. Centrax can alert an administrator when an attack is detected and can also respond in various ways, such as disabling an account or shutting down a workstation. In addition, it allows administrators to define both new attack signatures and attack responses. Centrax is designed to preserve an evidentiary trail, maintaining a log of unmodified raw event logs and supporting detailed data forensics.

Centrax is implemented in a distributed architecture that comprises a centralized command console and one or more agents that are installed on each target workstation or server and/or sensors that are placed at selected locations throughout the network. The command console provides a central integrated environment for configuration management, administration, and the collection and analysis of security relevant status from each agent or sensor. The agents collect and analyze the target system audit record, forward status information to the command console, and respond to threats detected by the command console.

The host-based component of Centrax detects misuse through event log analysis, periodic configuration assessment, and configuration compliance checks. It uses both behavior-based (statistical trending profiles and profile deviations) and knowledge-based methodology (misuse patterns and attack signatures) for alerts. The network-based component captures and analyzes network traffic and uses knowledge-based methodology (signature analysis) for alerts. The system can apply compound signatures that include events from both network sensors and host-based agents.

An audit policy editor allows administrators to create custom policies from a common interface. It allows the definition of event logging configuration settings for users, files, directories, and registry keys. A target manager allows Centrax to download collection strategies (including event log delivery schedule), auditing strategies, and issue specific intrusion response commands.

4.3 Computer Misuse Detection System

Table 4.3-1: CMDS - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
	X		X	X			X	X	X	X		X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distrib-uted	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X		X				X				X		

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
	X			X				X			X		X			X				X		X				X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentica-tion	user access control	user privilege mgt	none	manager-agent verifi-cation	manager-agent data encryption	secure software updates	none
X			X	X				X	X		

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
		X		X			X		X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data con-sistency	system behavior	other	none
											X

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	informa-tion	analysis	fixes	counter-measures	none
X		X			X		X						X

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X	X			X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X					X					X	

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X			X				X			

Table 4.3-2: CMDS - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI
X	X					X		X			
DG-UX	**AT&T (NCR)**	**Novell NetWare**	**Linux**	**Cray Unicos**	**Convex**	**Mach**	**SCO**	**Sequent Dynix**	**Sequent Ptx**	**other**	**none**	**n/a**
X												

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
									X			X

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
												X

Network Protocols

UDP	TCP	ICMP	IP	AppleTalk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
														X

Supported Applications (Section 2.3.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun WebServer	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none	n/a
											X	

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP OpenView	IBM Netview	other	none	n/a
					X							X	

Firewalls

ANS Interlock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
X		X		X						

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun WebServer	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP OpenView	IBM Netview	other	none
					X						X

Firewalls

ANS Interlock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company Science Applications International Corporation (SAIC)
(Partnered with ODS Networks, Inc.)

Manager Sun Solaris 2.5 or Higher
Hewlett-Packard/UX 10.x
Data General/UX 3.5 B2 with Security Option 4.12

Sensors N/A for a purely host-based system.

Targets

Operating Systems
SunOS 4.1.X C2
Solaris 2.X BSM
Trusted Solaris 1.X (CMW) (future)
Data General/UX 4.10DSO
Hewlett-Packard/UX 10.0
Microsoft Windows NT 4.0
Firewalls
ANS Interlock
Raptor Eagle
Cybershield

Interoperability

CMDS will be marketed as part of the ODS Networks, Inc. security package (announced Nov '98).

Protection

Data is encrypted for transfer from agent to manager.

A user ID and password is required to start the console. The console requires authentication to access the database server. Databases are user ID and password controlled.

For US domestic Triple DES is used. For export 56 bit DES.

All packets are authenticated between the agent manager and console.

CMDS can detect DOS attacks, and can temporarily disconnect attacked ports to stop such attacks. It also uses secure socket connections, built-in configuration validation, and secure validated command and control connections. It also monitors the agent heartbeat.

CMDS does not respond to pings, display a banner, or return 'destination unreachable or ICMP redirect messages.

Reports

Both fixed set and customizable.

Graphical trending reports from profiles, warnings, and alerts.

Alarms

Warnings and alarms to manager console. In real-time mode, alerts display as they are generated (in batch or on-demand mode, alerts will display when processed).

Response to events

Four "push-button" responses are available to the CMDS operator when a real-time alert occurs; ignore, increase observation, deny access to the perpetrator (a process kill), and emergency shutdown of the target system.

Performance

Can monitor up to 250-300 servers and 600 user workstations using a standard, off-the-shelf Intel platform, and can manage a rate of 300 Mb of audit data per hour from all targets.

An Intel-based console can handle at least 10 managers at full bandwidth. Using a product like Oracle or Sybase with distributed database capabilities, a large number of SQL servers can be combined in a single system.

Configuration takes about 20 seconds per target system.

CMDS was designed to handle up to 50 GB of audit data per day.

The agent processor overhead is typically between 2 to 7%.

Customization

Environment-specific requirements such as specific audit formats, special alert processing and summary report information. However, customization of CMDS operation to satisfy unique user needs generally requires employing SAIC's professional services.

With CLIPS programming capability, the user may modify the rule set.

Response options.

Special Features

On-demand user, file, or IP address monitoring.

CMDS provides a behavior-based capability, building a statistical user profile over a (default) ninety-day period.

History

CMDS was originally released in 1991, and has had several releases since then. CMDS is currently at version 4.0.

Information

Sites:
http://www.saic.com/it/cmds/menu.htm
http://www.ods.com/
Support:
Tel: (972) 234-6400
Fax: (972) 234-1467
cmds@ods.com
Installation and maintenance price quotes:
Tel: 972-234-6400

Cost

CMDS is licensed for each platform and on a per-agent basis. Server agent prices start at $995.00 for UNIX servers and $795.00 for Windows NT Servers. Workstation agent prices start at $100.00 for UNIX workstations and $75.00 for Windows NT Workstations. The CMDS console is priced at $6,995.00.

Evaluations/ Comparisons

None have been found.

Comments

The major portion of analysis is performed on the manager; the agents just handle collection, compression, encryption and formatting. This means CMDS can centrally integrate event data, can perform attack correlation activities, and can undertake detailed event trace and replay.

The Computer Misuse detection System (CMDS) is a host-based intrusion detection system that can monitor the audit record from a variety of operating systems and firewalls. In addition, it is designed to be customizable by SAIC to any audit source and policy. CMDS provides both knowledge-based and behavior-based methodology. Its signatures can detect a range of generally suspicious activity, and it supports administrator definition of both new detection requirements and expanded reporting capability. It relies heavily on administrator decision-making and intervention for both attack evaluation and response.

CMDS is a distributed application that is deployed in three components; a GUI console, a manager, and an agent. Agents are installed at each audit source and collect, compress, encrypt, and transfer entire audit logs to the manager. The manager consolidates and analyzes this information for misuse. In this, CMDS is different from other IDS products, in that the major part of its processing is performed at the manager level rather than at the agent level. The console provides a GUI with ad hoc data analysis, reporting, and charting tools, and can integrate and correlate event data from a number of managers.

CMDS supports three modes of operation: real-time, batch, and on-demand replay. In real-time mode an agent runs on the target system and gathers the data locally, parses it into the common CMDS format, buffers, and encrypts the data for transport to the manager. The manager receives the data, processes it, and in real-time generates alerts that may be sent to the console, via email to another location, or to a pager. In batch mode the agent and manager run on the same machine. Data is transferred on a regular basis (e.g., every hour) from the target system to the manager for processing. The CMDS administrator uses on-demand mode to replay data on request. This mode offers the option to perform misuse detection on audit data from archives.

CMDS implements three detection mechanisms: statistical deviations, signature recognition, and trending-analysis reports. Using statistical profiling methods, CMDS automatically builds daily and historical profiles for each user, based on their patterns of use. Once a threshold of normal user activity is established, CMDS monitors for statistical anomalies. CMDS also maintains a database of threat and attack signatures. It generates warnings and real-time alerts when a user's behavior matches a pre-defined threat signature, whether by engaging in activity which is "out-of-profile" or when an attack signature is detected. The various detection mechanisms can be run both in parallel and sequentially. The parallel option is provided so that each mechanism can create an alert independent of the other two. In addition, any one mechanism can feed into any other mechanism for sequential operation.

4.4 Cross-Site for Security

Table 4.4-1: Cross-Site for Security - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X		X					X		X			X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X	X					X				X		

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
X				X				X			X			X		X				X			X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X		X	X				X	X		

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
X				X	X				X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
			X		X	X					

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	counter-measures	none
X			X			X		X		X			

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X		X		X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X						X			X		

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X				X			X	X		

Table 4.4-2: Cross-Site for Security - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
												X

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
X	X										X	

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
X	X	X	X	X	X	X	X				X	

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
	X		X								X	X		

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
						X							X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company Tivoli Systems, Inc.

Manager

Solaris 2.5.1 or 2.6
Windows NT 4.0 or later
with Oracle 7.3.4 or later or MS SQL Server 6.5 or later
or
Web servers Netscape Enterprise Server 3.5.1

Sensors

Windows NT 4.0 with SP3 or 4
Windows 95 or 98

Targets

Topologies
10BaseT Ethernet, 100 BaseT Ethernet
Network Protocols
TCP/IP, NetBIOS, CIFS/Samba
Application Protocols
SMB, NFS, DNS, HTTP, FTP, TELNET, SNMP, SMTP, RPC

Interoperability

With the Tivoli Enterprise console, Tivoli NetView, HP OpenView.

Protection

The sensor uses 128 bit SSL encrypted HTTP when communicating with the management console.

The absence of a sensor will be noticed and the administrator notified.

Reports

Data is collected in a relational database management system, allowing the user flexible report generation.

There a built-in report generation capability and there are a selection of pre-defined templates.

Alarms

These may include a message on the management console, an e-mail to appropriate personnel, a page, or execution of a file.

Response to events

Range from notification of responsible personnel to execution of custom procedures to take specific corrective actions.

Performance

Each console can manage up to 100 sensors.

Neither console nor sensors require a dedicated box. While monitoring all traffic for a network segment, a sensor is lightweight enough so that it can function on an otherwise occupied production server without impacting performance (on a heavily loaded NT box serving Lotus Notes they report less than 3% degradation in performance.)

Customization

The user has a broad capability to set policy for network scanning and intrusion detection, and has extensive capability to define signatures.

Special Features

Cross-Site enables the sharing of selected security information with trusted partners.

History

Tivoli Cross-Site will be available domestically in December1998. International availability is planned for late 1999.

Information

Sites:
http://www.crosssite.com/
http://www.crosssite.com/products/sec/
Support:
http://www.crosssite.com/support/

Cost

Management Console is $5,000, each sensor is $5,000

Evaluations/ Comparisons

None found.

Comments

It is possible to access a Cross-Site management server securely from any machine that runs a Java VM. By this means an administrator can reach the management server from consoles throughout the network.

Does not require a dedicated system, but one with a interface card that can be placed in promiscuous mode.

Cross-Site for Security is a network-based intrusion detection system that also includes a vulnerability scanner component. It is part of the Tivoli Cross-Site management suite, an integrated set of management applications. Cross-Site for Security provides the following key capabilities:

1. An intrusion detection component that monitors network traffic and detects pre-defined attack signatures in real-time.
2. A vulnerability scanner that surveys a set of computer systems on a network, locating and recognizing the active servers, and performing tests for known security vulnerabilities on those servers.
3. Integration with Tivoli's Enterprise applications, enabling users to augment their enterprise management capabilities with those provided by Tivoli Cross-Site for Security and the Cross-Site suite.
4. A real-time, self-updating capability that minimizing the time and cost associated with upgrades.

The intrusion detection component of Cross-Site for Security is a distributed system that consists of a management console and a number of sensors. The management console collects data from the sensors, initiates responses to security breaches, and provides reporting capabilities. The sensors watch for evidence of external scans and intrusions. The management console enables users to set security policy for network scanning and intrusion detection, perform network scans, produce activity reports, and share selected information with trusted partners. The sensor monitors for scans and intrusion attempts in real time and when an attack or scan is recognized, the sensor sends an event to the management console, which logs the information and initiates a response in one or multiple forms. This response can consist of a message on the management console, e-mail to appropriate personnel, paging, or execution of a file. The console can be attached and run from anywhere in the network.

Network scanning and intrusion monitoring can run interactively or at scheduled intervals, which facilitates selective evaluation of specific situations as well as continuous surveillance. Scanning and intrusion detection data are collected in a relational database, allowing a flexible report capability. This enables the user to collect extensive information for issue resolution, security audits, and the automatic creation of records that may be used for legal action.

A set of attack signatures is provided with the system. Both the management console and the sensor can be automatically updated to detect newly identified vulnerabilities or to recognize the latest intrusion signatures using embedded deployment technology.

Users can customize responses to intrusive activities or non-conforming network configurations. Responses range from a simple notification to internal or partner personnel, to the execution of procedures to take specific corrective actions. Cross-Site for Security provides an event mechanism that can be forwarded on to other network management tools. The Tivoli Enterprise Console can be used to correlate events from across the network, and will allow configuration for active response according to the needs of their environment.

For switched networks Cross-Site for Security suggests configuring network routers to forward network traffic to a sensor.

4.5 CyberCop Monitor

Table 4.5-1: CyberCop Monitor - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
	X		X				X		X		X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distrib-uted	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X		X					X				X	

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse defini-tion			attack and misuse re-sponse			connection event			protocol defini-tion			audit record definition			reports			encryption options			security op-tions			other		
	X			X				X			X			X		X				X			X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authen-tication	user access control	user privilege mgt	none	manager-agent verifi-cation	manager-agent data encryption	secure software updates	none
	X		X				X				X

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Man-agement System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
		X	X			X			X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java app-lets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data con-sistency	system behavior	other	none
											X

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	informa-tion	analysis	fixes	counter-measures	none
						X		X					X

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X		X		X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X				X							

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
		X			X						X

Table 4.5-2: CyberCop Monitor - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems												
SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI	
						X						
DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
										X		

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	none	yes	no	n/a
									X			X

Supported Protocols (Section 2.3.2)

Network Application Protocols												
DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
												X

Network Protocols														
UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
														X

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers												
Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
											X	

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
					X							X	

Firewalls										
ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
									X	

Reconfigured Applications

Web Servers											
Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						X

Firewalls									
ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company	Network Associates (NA)
Manager	Uses Network Associates Security Management Interface (SMI) framework.
Sensors	N/A for a purely host-based system.

Targets

Operating Systems

Windows NT 4.0 platforms, using any supported Intel-based hardware, including multiprocessor systems.

Minimum requirements:

- Windows NT Server Standard Edition 4.0 with Service Pack 4.0*
- Internet Explorer 4.0
- 266 MHz Pentium processor
- 64 MB of RAM
- 50 MB of free disk space

Microsoft Data Access Components (MDAC) 2.1 recommended but not required.

Monitors multiple event sources (Windows NT Event log, LSA module, and network data) for attack "signatures.

Interoperability

Part of the CyberCop Intrusion Protection Suite, which includes CyberCop Scanner, CyberCop Sting, and CyberCop CASL.

Integrated with NAI's Security Management Interface (SMI).

Protection

Information not supplied.

Reports

Graphical and text based reports are available through the SMI.

Alarms

Records entries in a remote Event log, sends e-mail, and supports Windows popup messages.

Response to events

Can terminate unauthorized actions immediately.

Can shut down specific ports on Gauntlet Firewalls.

Integrates with the Windows NT Local Security Authority (LSA), which allows CCM block a user before they enter the system, rather than after they have already gained access and the necessary time has elapsed for notification of access to reach the Event log.

Performance

Information not supplied.

Customization

Configuration editor allows for custom settings and thresholds.

Special Features

History

Announced that CyberCop Monitor 2.0 will be available 2nd quarter 1999, but as of June 1999 was still in Beta testing.

Information

Sites:

http://www.nai.com/products/security/cybercop_scanner/monitor.asp

Support:

http://www.nai.com/about/contact/default.asp

Customer service: 408-988-3832

Product information: 1-800-332-9966

Corporate Office: 408-988-3832

support@nai.com

Cost

Licensing and pricing options are based on per server installation node count.

Evaluations/ Comparisons

None found.

Comments

The product is still in Beta testing and information is sparse.

CyberCop Monitor is a new intrusion detection system from Network Associates (NAI). Within the last few months both CyberCop Network (a version of NetRanger developed by Network General with technology licensed from WheelGroup) and CyberCop Server (née WebStalker) vanished without explanation from the NAI product line, to be replaced by CyberCop Monitor and the NAI Intrusion Protection Suite. NAI states that it is undertaking a new direction in its security products.

CCM is a host-based intrusion detection system. It uses knowledge-based methodology with attack and misuse signatures that detect different types of invalid activity on the host system. It does not appear to allow administrators define new attack signatures or attack responses, but only to select from a pre-defined set. Based on detected events and the user's needs, CyberCop Monitor can terminate unauthorized actions immediately and notify the network manager by email or console message. It is designed to detect specific system misuse and notify the administrator in real-time. A report file is maintained for each event, that details the identity of the violator, as well as when, where, and how the violation occurred.

CCM supports a distributed architecture that implements a centralized command console and one or more agents that are installed at each target workstation or server. The centralized command console supports distribution of security policies and the collection and analysis of security relevant status from each workstation or server in the enterprise. CCM uses Network Associates Security Management Interface (SMI) framework, which provides a single console window from which to manage all NAI security applications. SMI allows installation and management of CCM either locally or remotely on many machines from a single console. Centralized database capabilities allow gathering of CCM data from remote machines and viewing of data with graphical and text based reports.

4.6 Intruder Alert

Table 4.6-1: Intruder Alert - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
	X		X	X	X		X		X	X	X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X	X					X				X		

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
X			X					X			X		X		X					X			X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X		X	X	X	X		X	X	X	

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	interoperable	compatible interface	none	compatible interface	none	compatible interface	none
X	X		X			X			X	X	

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
											X

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	countermeasures	none
X		X				X	X		X				

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X	X		X		X			X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X	X								X		

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X					X		X	X		

Table 4.6-2: Intruder Alert - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI
X	X	X	X	X	X	X	X	X			

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
	X	X								X		

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
									X			X

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
												X

Network Protocols

UDP	TCP	ICMP	IP	AppleTalk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
														X

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun WebServer	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none	n/a
											X	

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP OpenView	IBM Netview	other	none	n/a
					X							X	

Firewalls

ANS Interlock	Raptor Eagle	Cybershield	Cisco	Gauntlet	Firewall 1	Borderguard	Checkpoint	other	none	n/a
									X	

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun WebServer	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP OpenView	IBM Netview	other	none
X											X

Firewalls

ANS Interlock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
	X		X	X			X		

Company	AXENT Technologies
Manager	**Interface Console (**View and Admin) Windows NT4, 95 (AXENT does not plan to implement a Unix GUI) **Managers** Windows NT NetWare (3x, 4x) UNIX (all in the Target list)
Sensors	N/A for a purely host-based system.

Targets

Operating Systems
IBM AIX 3.2.5, 4.1+, 4.2
HP-UX 9.05+, 10.01+, 10.20
Sun OS 4.1.3_U1+
Sun Solaris 2.4+, 2.6
Digital OSF/1 3.0+
Digital UNIX 4.0+
Silicon Graphics 5.3, 6.2+
AT&T (NCR) 2.3+, 3.0+
NetWare 3.11+, 4.1+, 5
Windows NT 3.5.1+
Windows 95 win95
(binary C2 audit logs on HP-UX & Solaris)

System Audit Records
UNIX - Syslog, WTMP/UTMP, Process Accounting, or user-defined
Windows NT - Security log, applications log, systems log, or user-defined
NetWare - Operating system direct monitoring, or user-defined.
Can also support C2 audit logs.

Firewalls
Raptor and Gauntlet
Cisco Routers.
"Various" webservers.

Interoperability

AXENT's Enterprise Security Manager, a system vulnerability scanner.
AXENT's NetRecon, a network vulnerability scanner.
Tivoli, BMC/Patrol & HP/OpenView integration.

Protection

Agent registration and data encryption (Diffie Helman Key Exchange) of network activity. With each communication, a new key is negotiated.

Administrators can set up individual user accounts, where each account has its own respective password and privileges.

Attack signature updates are made available via the SWAT Team Web site.

A throttle is used on agent to manager communications so that IDA does not use excessive network bandwidth even during bursts of activity.

Each host running a manager is required to also run an agent, which can then be used to monitor the system.

Since every manager can control many agents and every agent can report to more than one manager, it is possible to design and build robust architecture, with redundant communication and multiple management domains.

If a manager loses communication with one of its agents, it tries to report errors to other managers through its own agent. Similarly, if an agent looses communication with one of its managers, it tries to report lost communications problems to the other managers.

Reports

Reports can be plotted in charts, graphs, text views, etc., and automatically update in real-time, or in offset, user-defined time specifications.

Display chronological listing of all related events.

Review historical data, and look for trends in security vulnerabilities.

A network-wide summary report for user defined domains of systems.

Alarms

Paging, e-mail, message to console.
Alerts according to event frequency.

Response to events

Can take actions such as communicate with firewalls/routers to block packets from a presumed attacker's IP net address, disable a user account, execute a user-defined command procedure, terminate local or remote user session, and kill processes.

Performance

Both the Manager and the Agent have very little overhead on fast systems. Agent usually utilizes 1% - 2% during the normal operations, and up to 6% during activity peaks. Resource utilization by the Manager depends on the number of Agents reporting to it, but is in the 1% - 5% range.

One Manager can support up to 50 agents. AXENT asserts it is possible to build a system that consists of 1000 Agents managed by 20 Managers.

Customization

A customizable rules-based policy library which allows the user to easily define complex, context-based and content-based intrusion signatures.

The user can customize monitoring focus on critical devices throughout the network (routers, firewalls, Web servers, etc.)

Customization involves using solution packs for major operating systems, firewall vendors, Web-server vendors, database applications, and router manufacturers.

Special Features

Attack signatures are updated to a web site every one to two weeks.

Drag and drop capability in a GUI for all system configuration, customization, and other management tasks.

History

Initially released in 1992.

Current version 3.0/SR2 (Service Release 2).

Information

Sites:
http://www.axent.com/product/ita/ita.htm
http://www.axent.com/product/smsbu/ITA/default.htm
http://www.axent.com/iti/netprowler/idtk_ds_word_1.html

Support:
www.axent.com/swat/swat.htm
(801) 227-3700 (phone)
(801) 227-3788 (fax)
support@axent.com

Cost

The manager costs $1995, the console is free, and agents cost $995 per server or $95 per workstation. Signature updates are included in software maintenance fees.

Evaluations/ Comparisons

Hot Products Awards, Intruder Alert, Data Communications, January 1998 http://www.data.com/hot_products/webstalker.html

OmniGuard/ITA thwarts insider attacks, PC Week Labs, March 1998 http://www.zdnet.com/pcweek/reviews/0309/09guard.html

Cracker Tracking: Tighter Security with Intrusion Detection, Byte Magazine, May 1998 http://www.byte.com/art/9805/sec20/art1.htm

One if by Net, Two if by OS, PC Week Labs, February 1999 http://www.zdnet.com/pcweek/stories/news/0,4153,389071,00.html

Comments

AXENT acquired firewall vendor Raptor in February 1998 and plans to enhance Intruder Alert to reconfigure Raptor firewalls.

AXENT has partners and security products that may ship with Intruder Alert pre-installed.

The only response from the vendor was that our query would be passed on as appropriate. No further response has been received.

Intruder Alert (ITA) is a component of OmniGuard, AXENT's suite of integrated software tools. ITA is a host-based tool that analyzes audit data from a wide variety of operating systems, and can with modification perform device monitoring (using SNMP traps) from other applications such as management frame-works, firewalls and routers[4]. It will shortly share a management console with a network-based IDS called NetProwler (see Section 4.8).

ITA is deployed in three components; a GUI console (comprising ITA Admin and ITA View), a manager, and an agent. The reason for having two GUI components is to separate administrator and operator roles[5].

1) ITA Admin connects to each manager, and allows the definition and activation of security policies on the agents that belong to the manager. Policies can be simple (one or two rules) to complex (many rules with timers, flags, and inter-rule dependencies). Managers maintain security policies for a number of agents that are grouped into domains. Managers collect events from agents and store them in a database. ITA View then queries the database and displays events of interest.

2) ITA View allows querying of the event database generated by the manager. The event database can be queried for events with a combination of different query criteria: alert level, policy, time offset, date and time, and agent. The query results window in ITA View acts as the "alert window" and automatically updates each minute.

3) Agents run on the systems being monitored and do most of the processing. They collect information, execute both knowledge-based rules based on defined security policies, and take appropriate actions. Actions include sending alarms to the manager for display, sending email notification, activating pagers, killing processes, or terminating user sessions. Agents are registered to managers to provide a secure communications path. Each time communications occurs between manager and agent, a password exchange and verification takes place. Each session is encrypted using a one-time key.

Log files created by ITA have a format that is operating system independent, though of course the information provided by each operating system will vary widely. ITA can be used to manage large number of different audit logs. It can filter logs at the agent level, consolidate them to a central location and purge or archive them based on a pre-set schedule. Log entries are formatted in a human readable format. They can be sent to a monitoring console, to be prioritized and displayed.

ITA employs a rules engine, and processes the inputs it receives based on rules applied to the specific system it is monitoring. Some rules may be designed to look at a specific sequence of events. If a particular sequence is detected, ITA can be programmed to take various actions. Other rules detect behavioral anomalies within the system. These rules filter out defined normal activities, leaving the exceptions to be acted upon or investigated as needed. ITA comes with a package of predefined security policies (attack signatures). With the addition of appropriate rules by the user ITA can detect almost any kind of predefined intrusion. With the addition of required software, it can also statistical profiles of user activity and identify out-of-profile activity.

ITA 3.0 enables users to connect the GUI to more than one manager at a time. Users can drag and drop rules, clauses, etc., from one manager to another. The agents collect and process events from the system log files, system accounting (Unix), system auditing (NT), applications and database logs according to the security policies maintained by the Managers.

The AXENT SWAT web site provides a place from which additional signatures that can be downloaded and installed. AXENT has a team of security professionals who provide intrusion signature updates within one day to two weeks if a new vulnerability (exploit) is discovered, depending on severity of vulnerability.

[4] An ITA user reports that at least his version of ITA did not include any software, SNMP MIB, or policies that send SNMP notification. If this is the case, a user would have to set up his own MIB (or use MIB-II trap definitions), and use third party SNMP agents (e.g., the CMU SNMP toolkit) in order to make Intruder Alert send SNMP traps to HP Open View or other SNMP managers.

[5] Although reportedly the same password is used for both components.

4.7 Kane Security Monitor

Table 4.7-1: KSM - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
	X		X				X		X			X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X		X				X					X	

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
		X		X				X			X			X		X				X			X		X	

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X		X				X	X			

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	interoperable	compatible interface	none	compatible interface	none	compatible interface	none
	X		X			X			X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
											X

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	counter-measures	none
X			X			X		X					X

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X	X			X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X				X						X	

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X				X					X	

Table 4.7-2: KSM - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI
						X					

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
									X			X

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
												X

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
														X

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none	n/a
											X	

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
					X							X	

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
									X	

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company Security Dynamics Technologies, Inc.

Manager Will work on any NT supported hardware platform including Intel-based or DEC Alpha based systems.

Sensors N/A for a purely host-based IDS.

Targets

Operating System
Microsoft Windows NT
System Audit Records
The NT product audits the SAM database, NT registry, NT system log, NT security log, NT application Log, NT event logs, user profiles, rights, audit and account policies, and Explorer drive properties.

Interoperability

Configuration checker Kane Security Analyzer (KSA).
HP's OpenView.
IBM's TMG.
Computer Associates Unicenter by delivering alarms to these management systems consoles as SMTP alerts.
Cheyenne's InocuLAN anti-virus product.
Crystal Reports Custom Reporting Module.

Protection

No authentication or encryption is provided, just an agent verification scheme. Agents are "registered" to a KSM Auditor Service as they are installed and configured. Each time communications occurs between manager and agent, a security verification process takes place.

Reports

Interactive user interface as an extensive set of pre-configured reports.

Alarms

Via e-mail, fax, voice mail, or audible alarm at manager console.
Color-coded event icons.

Response to events

Documents the event and its details (such as the point of origin and indicated user).

Performance

Advertised to process each event log “in seconds”.
A single KSM console can manage hundreds of server agents and thousands of workstation agents. No limit to the number of agents that can be monitored, given enough memory for console workstation.
Each server can manage a 430-agent production environment.

Customization

Specific workstations or servers can be given higher alarm status for individual or specific events.
Management console display.
Reports may be selected from an extensive set.

Special Features

Distributed architecture and management.
On-demand user, file, or workstation monitoring.

History

NetWare version initially released in1991 by Intrusion Detection Inc. (IDI)
NT Version initially released in 1996
IDI was purchased in May 1998 by Security Dynamics
Current NT version 4.4 released in June 1998
Current NetWare ver. 4.4 released in June 1998
NT, NetWare v4.6 scheduled for release in June/July, 1999

Information

Sites:
http://www.securitydynamics.com/products/
http://www.securitydynamics.com/products/intrusion.html
Support:
sales@intrusion.com

Cost

US List Price for KSM is $1495 for the first protected server (auditor and console included). Additional workstation agents start at $295 each. Discounts are available for volume purchase. Signature updates are included in software maintenance fees.

Evaluations/ Comparisons	Cracker Tracking: Tighter Security with Intrusion Detection, Byte Magazine, May 1998 http://www.byte.com/art/9805/sec20/art1.htm One if by Net, Two if by OS, PC Week Labs, February 1999 http://www.zdnet.com/pcweek/stories/news/0,4153,389071,00.html

Comments

The Kane Security Monitor (KSM) is a host-based intrusion detection system that runs on Windows NT workstations and servers. It provides network security monitoring and detailed event log analysis for Windows NT networks, and checks for security policy conformity; i.e., for password length, excessive rights, etc. It supports a distributed architecture that implements a centralized monitoring console, an auditor, and one or more agents that are installed at each target workstation or server. The agents collect and analyze the target system audit record and forward statistics to the auditor. The centralized command console (consisting of a collection auditor and alerting engine) collects and analyzes of security relevant status from the agents. The security administrator uses the console GUI to receive alerts and look at historical reports and real-time activity.

The KSM is a knowledge-based system with a database of expert security information. It provides prebuilt security attack patterns for a wide variety of attacks and operating situations, and provides a limited capability for the user to customize attack responses by changing the alarm status for specific events. Once an event has been identified, alerts are sent via e-mail or audible alarm at the manager console. If a particular abuse pattern is detected, KSM notifies the security staff, and documents the event and its details (such as the point of origin and indicated user).

Installation of agents throughout a network can be done from a single manager. The KSM comes with a built-in database of sample alerts and alarms for training purposes.

The KSM management console displays events as different color-coded icons. The different colors represent different levels of severity of each event. The KSM manager can customize this display. Each security pattern checked can be configured on a scale of 1 to 100 as to its severity. KSM can also alert the security staff via email, or forward an alert to an existing network management software system. Detailed reports and graphs of security events can be displayed in both animated charts and text reports.

4.8 NetProwler (née ID-Trak)

Table 4.8-1: NetProwler - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X		X					X		X		X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X	X					X				X		

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
X			X			X					X			X	X					X			X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X	X		X	X	X		X	X	X	

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	interoperable	compatible interface	none	compatible interface	none	compatible interface	none
X	X		X		X			X			X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
											X

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	countermeasures	none
X		X			X		X						X

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X	X		X		X			X	X	

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X				X					X		

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
		X					X				

Table 4.8-2: NetProwler - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
												X

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
											X	

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
	X		X											

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
						X	X						

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X	X					

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
	X		X	X					

Company AXENT Technologies, Inc.

Manager **Interface Console (**View and Admin)
Windows NT4, 95 (AXENT does not plan to implement a Unix GUI)
Managers
Windows NT
NetWare (3x, 4x)
UNIX (all in the Target list)

Sensors

A Windows NT or Windows 95 PC with a Pentium processor, 32-megabyte RAM, 1.0-Gigabyte hard disk, 800x600 display, CD-ROM drive and a NIC. For enterprise-wide deployment, a central data repository with Windows NT 4.0 and MS-SQL server 6.5 are required.

Targets

Topologies

Information not supplied.

Network Protocols

TCP/IP

Application Protocols

Information not supplied.

Interoperability

Microsoft's BackOffice Server.

Given the recent acquisition, it is likely to soon be interoperable with the AXENT suite of tools, and share a console with Intruder Alert.

Protection

Enforced access control to the IDS server based on time-of-day.

Further information not supplied.

Reports

Text, CSV or HTML reports.

Attack analysis provided.

Alarms

Send an SNMP alert, email, fax or page.

Session logging, session termination.

Response to events

Terminate unauthorized use.

Take a full trace of the application session.

Customizable reaction upon detection of an attack, such as stopping the attacker, taking a full trace of the application session, sending SNMP alert, email, fax or page.

Performance

Information not supplied.

Customization

Users can design their own resource-specific signatures against more intricate, company-specific security violations. New attack signatures can be immediately deployed and dynamically accepted by the SDSI virtual processor.

Users can also define attack responses.

Users can specify time of day resource access.

Special Features

Provides automatic configuration scans.

Fixes configuration errors.

Data consistency checks for Web, FTP & DNS Server content as well as Routing Table consistency checks.

A configuration scanner that is designed to detect and automatically fix vulnerabilities.

ID-Trak Enterprise will provide application-specific security add-ons that automatically build attack signatures based on company context and vulnerabilities (for the BackOffice Server).

History

ID-Trak was released 1 May 1998 by Internet Tools, Inc. The first indication of ID-Trak Enterprise was a product announcement in November 1998.

First version of NetProwler was announced by AXENT November 1998.

AXENT purchased ID-Trak in January 1999, and announced that it will be integrated into OmniGuard and be named NetProwler. We assume this will replace the earlier NetProwler, but will wait to upgrade the description when more information is available.

AXENT expects the result of this integration, a stand-alone network-based intrusion detection solution, will debut in Q1 1999 in North America and Q2 1999 worldwide.

Information	**Sites:** http://www.internettools.com/ http://www.axent.com/iti/netprowler/idtk_ds_word_1.html **Support:** (801) 227-3700 (phone) (801) 227-3788 (fax) support@axent.com
Cost	The manager console costs $1995 Each network engine costs $7995
Evaluations/ Comparisons	ID-Trak was a finalist for the Best of Show awards for the NetWorld+Interop 98 tradeshow, in the Network Security and Performance category. Secure Computing Magazine picked ID-Trak best of the year for network-based intrusion detection solutions.
Comments	Information about ID-Trak was is limited to a few news articles and product announcements, and a sparse web site. Since its acquisition by AXENT, little more new information has been found. Queries to the vendor have not been answered.

Because of the recent acquisition of ID-Trak and its on-going integration into the AXENT tool suite, up-to-date implementation details are sparse. We integrated the information that was provided for the original ID-Trak product with information about the common console that it will share with Intruder Alert. This Section will be updated when more current information is provided.

NetProwler is a network-based intrusion detection system runs on Windows NT or Windows 95. It examines packets at near wire speed to identify, log and terminate unauthorized use. Its built-in attack signatures can detect a set of known TCP/IP Intranet and Internet attacks, and new attack signatures will be made available for users to download as soon as new Internet attacks are discovered. In addition, it lets administrators easily define both new attack signatures (in real-time) and attack responses. NetProwler alerts an administrator when an attack is detected and also can respond in various ways. For example, if a specific IP address is flagged too many times in a specific interval, NetProwler can perform a full trace and shut down the session.

NetProwler is based on Stateful Dynamic Signature Inspection (SDSI) technology. SDSI is stateful because it keeps track of current states of all application sessions on the network, and is dynamic because new signatures can be defined and added in real-time. This technology uses an intrusion-detection-specific virtual processor that executes attack signatures in the form of a set of instructions. This allows the SDSI processor to be independent of the attack signatures. Attack signatures are defined through an extensive set of primitives to accommodate complex intrusion signatures.

NetProwler Enterprise provides application-specific security add-ons that automatically build attack signatures based on company context (as determined by profiling the application). This capability has thus far only been announced for Microsoft's BackOffice Server. NetProwler BackOffice Option utilizes two distinct components to automatically create company-specific attack signatures that augment BackOffice protection. A scanning agent is deployed on a BackOffice server in order to assess the system configuration of such components as Microsoft Internet Information Server, Exchange Server, Proxy Server and SQL Server applications. This configuration data is obtained by the centralized NetProwler data repository, which in turn builds custom attack signatures on the fly. It then deploys in real-time these custom attack signatures to the appropriate NetProwler data collectors guarding the BackOffice servers. The result is specific BackOffice protection using company-specific context.

4.9 NetRanger

Table 4.9-1: NetRanger - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X		X					X		X		X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X	X					X			X			

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
	X			X				X			X			X			X			X			X		X	

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X		X	X	X			X	X		

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	interoperable	compatible interface	none	compatible interface	none	compatible interface	none
	X			X			X		X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
					X						

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	countermeasures	none
X		X			?		X		X	X	X	X	

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X	X		X		X			X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X	X		X			X	X				

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X					X				X	

Table 4.9-2: NetRanger - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI	
DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
												X

Network Topologies / **Switched Nets**

10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
X	X		X	X			X				X	

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
X	X	X		X	X	X	X				X	

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
X	X	X	X											

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
												X

Routers / **Management Systems**

Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
						X							X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none

Routers / **Management Systems**

Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
X				X							

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company Cisco Systems, Inc.

Manager Manager (director) software runs on a Sun or HP workstation (Solaris 2.6, HPUX 10.2, and AIX 4.3.). It requires HP OpenView Network Node Manager and (optionally) a RDBMS like Oracle for storing event history and reporting.

Sensors

Sensors are generally pre-installed on turnkey hardware that can be placed directly on the network, but a software version is now available.

Sensors are available in two performance levels:

Single 400-MHz Pentium Processor (Ethernet or Token Ring Monitoring Configurations)

Dual 400-MHz Pentium Processors (Fast Ethernet or FDDI Monitoring Configurations)

Targets

Topologies

10/100BaseT Ethernet

100BaseT Ethernet

FDDI

Token Ring

T3 (45Mbps) WAN links

100Mbps FDDI

100Mbps Ethernet

Network Protocols

TCP/IP only, but will not interrupt the flow of other protocols such as IPX.

Application Protocols

SMB, NFS, DNS, HTTP, FTP, TELNET, SNMP, SMTP, RPC.

Interoperability

Routers

Cisco 2500

Cisco 4500

Cisco 4700

Cisco 7500

Firewalls

StorageTek BorderGuard 1000

StorageTek BorderGuard 2000

Nortel Passport

Network Managers

HP OpenView Network Node Manager™ running on HP/UX 10.10 or Solaris 2.51

IBM NetView™ 4.1 running on AIX 4.1

Protection

Optional SKIP-based encryption between sensors and director.

Fault tolerant point-to-point protocol.

Attack signature updates are provided on CD with each new release. License keys unlock software for specific users only.

Reports

Other than providing scripts for loading the event logs into a relational database and providing a number of sample database queries, NetRanger does not include a tool for generating written reports. Event data is moved to a database where standard queries can be performed and historical and trend reports can be generated. NetRanger needs integration with third-party tools to print nice reports.

Alarms

Color-coded icons in real-time to a GUI interface on the Director in real time denoting a violation or attack. These icons change colors depending on the severity of the attack.

Alarms include attacker and destination IP addresses, destination port, and attack descriptions.

NetRanger has pull down menus for additional information requests, and the user may click on icons for additional information.

NetRanger groups alarms so that repeated alarms of the same type do not generate new icons, but only increase the alert count next to the icons representing the alarm.

NetRanger also supports pager and e-mail notification.

Response to events

The NetRanger Sensor can kill an attack session with TCP Resets, or reconfigure an Access Control List (ACL) in a router (Cisco or BorderGuard) to block attacker traffic.

Captures and logs the address of the electronic point of origin of the attack.

Performance

Each director can monitor and control up to 50 remote sensors. Directors can be arranged in a tiered fashion to control a virtually unlimited number of sensors.

Each sensor is capable of sending alarm information to up to 32 directors.

Bandwidth is highly variable depending on hardware used for sensor, type of traffic and size of packets in the data stream, tightness of security policy, and so forth.

Sensors can monitor network segments from 56 Kbps to speeds over T3, including 4/16 Mbps Token Ring, 10/100 Mbps Ethernet, and FDDI, which permits NetRanger security to be used where lower-performing security devices are not acceptable

Customization

Attack signatures and attack responses, but these require high product-specific expertise to set up, configure and maintain.

The event priority levels, up to 255 different levels.

Special Features

Path-doubling: if one link goes down, information can flow along an alternate path.

Context monitoring (i.e., clues gained from multiple packets) as well as single-packet content monitoring.

When NetRanger detects an attack, it saves the raw packet data to a log file. This data can then be viewed with an add-on tool like the public domain PacketMan.

NetRanger can provide full functionality on StorageTek BorderGuards encrypted networks. In cases of other encryption, NetRanger will function but is limited to context processing.

History

Initially released in August 1996 by WheelGroup, which was bought by Cisco Systems in 1998.

Current version and release date: ver. 2.2.0, released July 1998.

Information

Sites:
http://www.cisco.com/
http://www.cisco.com/warp/public/778/security/netranger/
Support:
800 553 2447 or +1 408 526 7209

Cost

NetRanger's sensor software costs $9000 each, and at least a Pentium PC for the sensor. Total cost = $13,000 per Sensor. NetRanger's director (manager) software costs $10,000, and a Sun SparcStation running OpenView or NetView. Total cost = $25,000 per Director. One user has said that NetRanger requires specially-configured hardware from Dell Computer. Signature updates are included in software maintenance fees.

Evaluations/ Comparisons

Cracker Tracking: Tighter Security with Intrusion Detection, Byte Magazine, May 1998 http://www.byte.com/art/9805/sec20/art1.htm

Digital sentries, InfoWorld May 4, 1998 http://www.infoworld.com/cgi-bin/displayTC.pl?/980504comp.htm

Intrusion Detection Systems: Suspicious Finds, Data Communications, August 1998. http://www.data.com/lab_tests/intrusion.html

Comment	Versions of NetRanger are used in network management and security systems via partnerships with NetSolve, Inc. (ProWatch Secure) and Storage Technology Corporation (NetSentry MONITOR). SecureIT Inc. markets CISCO NetRanger. WheelGroup contributed to a separate IDS product by Network General (CyberCop Network), Hewlett-Packard announced that it will license CISCO NetRanger. HP will incorporate the network intrusion detection software into its OpenView network management software, calling it HP OpenView Node Sentry. According to Cisco, the future enhancements to NetRanger include improving the GUI, integrating with Cisco's firewalls (and other commercial firewalls further down the road) for active shunning, and moving NetRanger into router and switch hardware.

NetRanger is a network-based intrusion detection system that applies a knowledge-based methodology. Its attack signatures are designed to detect a set of known attacks and misuse. It allows administrators to define both new attack signatures and attack responses. NetRanger not only alerts an administrator when an attack is detected, but also can respond in various ways. NetRanger is a distributed application that consists of three elements: a manager (or director), one or more sensors that are located at the network connections to be monitored, and a communications system that manages communication between sensors and directors. It uses HP OpenView for its management console.

The director is a workstation that provides command and control functions. It has a GUI for reporting sensor alarms and managing configurations. It logs all incidents and lets users create historical and trend reports. Each director can monitor and control more than 100 remote sensors. The director can load new signatures, receive and process alarms from each sensor, and display the results in graphical format. Directors can be arranged in a tiered fashion and are designed to control a virtually unlimited number of sensors. The director console displays color-coded (depending on the severity of the event) icons of each sensor it manages. The user can specify which levels of alarms that they wish to monitor based on their operational mission.

Sensors, either working independently or in conjunction with a router, switch, or firewall, analyze network traffic. Looking at the content and context of the data stream, the sensor searches for signatures indicative of hacking attacks or other security violations. Once it detects an attack, a sensor can act to block it (depending on the requirements of the user) and send a real-time alarm to the director. The sensor captures and logs the address of the electronic point of origin of the attack. If a customer requires a hierarchical reporting architecture, the sensor can be configured to deliver different alarm levels to different directors.

The communications system provides message delivery over UDP. It is based on a proprietary, fault tolerant, point-to-point protocol that connects one or more sensors to the director. It can route messages via other sensors and directors to their final destination to overcome either a lack of network connectivity between sender and receiver or unexpected network failures. It can also be used to construct hierarchies of directors and propagate event information to more than one director. In its base configuration, NetRanger does not encrypt communications between its distributed components. However, it will work with off-the-shelf Virtual Private Network (VPN) solutions like Sun's Simple Key management for IP (SKIP).

NetRanger can be used in three basic configurations: 1) a standalone system that watches for suspicious activity, alerts the user whenever suspicious activity occurs, and can terminate individual TCP sessions. 2) an intrusion detection engine with shunning capabilities. This option is provided in conjunction with routers, and works identically to 1), with the additional capability of managing and reconfiguring Cisco routers to permanently block attackers out of a network. 3) an intrusion detection engine with shunning and packet filter monitoring. This option works with routers and firewalls, and provides all the functionality of 1) and 2), with the additional capability of packet filter firewalling, and monitoring of those filters.

Attack signatures are updated with each new release of the product, which has been approximately every 4 months. They are working on a dynamic update capability so administrators can pull new updates from a secure Web site or via ftp.

4.10 Reactive Intrusion Detection

Table 4.10-1: Reactive Intrusion Detection - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
	X			X			X		X		X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distrib-uted	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse defini-tion			attack and misuse re-sponse			connection event			protocol defini-tion			audit record definition			reports			encryption options			security op-tions			other		
	X			X			X				X			X			X			X			X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authen-tication	user access control	user privilege mgt	none	manager-agent verifi-cation	manager-agent data encryption	secure software updates	none
	X		X								

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Man-agement System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
							X		X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java app-lets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data con-sistency	system behavior	other	none

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	informa-tion	analysis	fixes	counter-measures	none
					X								

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X		X	X			X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X											X

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
		X					X				

Table 4.10-2: Reactive Intrusion Detection - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems											
SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
											X	

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
									X			X

Supported Protocols (Section 2.3.2)

Network Application Protocols												
DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
												X

Network Protocols														
UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
														X

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers												
Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
											X	

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
					X							X	

Firewalls										
ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
				X						

Reconfigured Applications

Web Servers											
Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						X

Firewalls									
ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
				X					

Company	LURHQ Corporation
Manager	Information not supplied.
Sensors	Information not supplied.
Targets	Information not supplied.
Interoperability	Gauntlet Firewall.
Protection	Information not supplied.

Reports Information not supplied.

Alarms Information not supplied.

Response to events Information not supplied.

Performance Information not supplied.

Customization Can be customized to meet the local security policies through multiple reaction profiles, signature thresholds, and trusted hosts configuration.

Special Features Designed to run in conjunction with a specific firewall application.

History First released November 6, 1998.

Information
Sites:
http://www.lurhq.com/rid
Support:
Info@lurhq.com
T: 843-347-1075
F: 843-347-1076

Cost Free.

Evaluations/ Comparisons None found.

Comments Little information is available about this product, and no response to queries has thus far been received from the vendor. This section will be updated when more information is available.

LURHQ Corporation released a new of a host-based intrusion detection product for use with Network Associates' Gauntlet Firewalls. The Gauntlet Firewall is a preventative measure designed to provide secure access and Internet work communications between trusted and untrusted networks. The addition of RID is designed to enable the firewall to intelligently react to potential attacks in real-time, so that it can disable an intruder's access to and through the firewall, alert the administrator of suspicious activity, and maintain a database all suspicious activity for analysis. RID is being offered free of charge to companies using the Gauntlet Firewall and can be downloaded from the company’s web site. The software is part of LURHQ Corporation's Managed Security Service.

RID is a designed to integrate seamlessly into an existing Gauntlet Firewall and increase its security. It is managed through Gauntlet's administration program and can be customized to meet the specific enforcement policies of different networks through multiple reaction profiles, signature thresholds, and trusted hosts configuration. RID's attack signature database includes well known port scanners such as SATAN, CyberCop, and strobe, Trojans such as root kit and BackOrifice, Denial of Service, DNS, sendmail, IP spoofing, source routing, and attacks specifically aimed at Microsoft Servers. As new attacks and vulnerabilities are discovered, LURHQ Corporation plans to release an updated signature database so that RID is always aware of the latest attacks and vulnerabilities, ensuring that its users have complete and continuous protection.

4.11 RealSecure

Table 4.11-1: RealSecure - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X	X	X					X		X	X	X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X		X				X				X		

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])																										
attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
	X			X		X					X			X		X		X					X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X	X		X				X	X	X	

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
	X			X		X			X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring											
IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
	X	X									

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	counter-measures	none
X		X			X		X			X	X		

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X	X		X			X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X						X			X		

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X			X						X	

Table 4.11-2: RealSecure - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems												
SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI	
DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
												X

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
X	X			X			X				X	

Supported Protocols (Section 2.3.2)

Network Application Protocols												
DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
X	X	X	X	X	X	X	X				X	

Network Protocols														
UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
X	X	X	X								X	X		

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers												
Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
						X							X

Firewalls										
ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers											
Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						

Firewalls									
ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
							X		

Company Internet Security Systems (ISS)

Manager Windows NT® 4.0, with Service Pack 3
Solaris (SPARC) 2.4/2.5
Linux, kernel versions 1.3.x

Sensors A workstation with a network adapter card that can run in promiscuous mode: Windows NT® 4.0, with Service Pack 3, Solaris (SPARC) 2.4/2.5, Linux, kernel versions 1.3.x

For a saturated T-1 line: a Pentium II 200 MHz. or better, with 128 MB RAM and 1 GB disk storage.

ODS Network's SecureAuditor, SecureDetector, or SecureSwitch.

Targets

Operating Systems

Windows NT servers or workstations

Topologies

Ethernet networks (10 Mbps)

Fast Ethernet networks (100Base-T only, 100 Mbps)

Token Ring networks (4 Mbps to 16 Mbps).

FDDI

Network Protocols

TCP/IP, NetBIOS, and Microsoft CIFS/SAMBA traffic for Windows networking environments.

Application Protocols

SMB, NFS, DNS, HTTP, FTP, TELNET, SNMP, SMTP, RPC.

Interoperability

Check Point Firewall-1.

ISS is partnered with ODS Networks, Inc. to use RealSecure in ODS's SecureDetector and SecureSwitch integrated hardware/software products as sensors.

ISS is partnered with SecureIT, Inc. to use RealSecure to automatically reconfigure FireWall-1 in response to a network attack.

GTE Internetworking is blending RealSecure with a number of monitoring programs that all feed into a central security console. One of these custom-designed programs checks buffers to watch for denial of service attempts. Another monitors the physical boxes. RealSecure will watch the wire.

RealSecure will interface to ISS' management product SAFEsuite Decisions, which automates the collection, integration, analysis and reporting of enterprise-wide security information from multiple sources and locations including not only integrated data from ISS' intrusion and vulnerability detection systems, but also third-party security safeguards such as firewalls. SAFEsuite 1.0 is scheduled to begin shipping in the fourth quarter of 1998.

SAFEsuite will be interoperable (then integrated) with Nortel Networks product lines. Interoperable the first quarter of 1999, integrated by second half of 1999. RealSecure will be integrated with Passport and NetSentry. This is aimed at providing optimal IDS in a switched network environment.

Protection

All communications between the engine and the console use TCP only (no UDP) and are encrypted, using encryption technology from Certicom and RSA. On Windows NT hosts, encryption functions use the Microsoft Cryptographic API. Communication between console and engine can be authenticated and encrypted with 128-bit RSA. Are authenticated with a public-private key exchange algorithm. Are verified, with checksums appended and checked for each message.

Attack signature updates may be downloaded securely from the ISS Web site or may be sent via encrypted e-mail.

Reports

Session-recording tool.

Tool for generating written reports that summarize the daily event log.

DBMS reporting features that allow the administrator to sort and format event data by priority, source address, destination address, or network service over some period of time.

Alarms

Sent to the console, e-mailed to any Internet mail gateway, generate an SNMP trap or send a user-defined executable such as a pager-dialing application.

Response to events

Terminate the attack automatically.

Reconfigure a Check Point™ Firewall-1® to reject traffic from the attacking source address.

Send an alarm to the management console indicating that the event occurred.

Send an SNMP trap to an off-the-shelf management platform.

Log the event, including date, time, source, destination, description, and data associated with the event.

View the raw content of the session in real-time (or record for later playback).

E-mail a notification to the administrator.

Execute a user-specified program. This option can be used to initiate any response that can be expressed in an executable binary (or batch file/shell script) form. Examples include initiating a pager call, playing a sound, or reconfiguring a network device that RealSecure does not currently support.

Log event to an ODBC-compliant database for later replay.

Performance

Each management console can manage up to 50 engines at one time.

Can get close to supporting 100Mpbs bandwidth.

Customization

Define connection events based on protocol (TCP, UDP, ICMP), source port, destination port, source IP address, and/or destination IP address.

Define response to event to one or more of a pre-defined set.

Special Features

Has session-playback mechanism.

Will recommend fixes for security holes.

History

Initially released in December 1996

Version 3 was released in January 1999

Information

Sites:

http://www.iss.net/

http://www.iss.net/prod/rs.html

Support:

Information not supplied.

Cost

Sensor: 200-MHz Pentium Pro 64MB RAM = $1,300

Console: 200-MHz Pentium II 128 MB RAM monitor supporting 800X600 and 256 colors = $1,800

Each NT software agent = $750

Each software detection engine = $8,995

Console software is free

Unlimited support and attack updates cost 20% of the purchase price each year = $1990. Signature updates are included in software maintenance fees.

Evaluations/ Comparisons

Individual Review RealSecure Version 1 for NT - InfoWorld July 21, 1997 http://www.infoworld.com/cgi-bin/displayArchive.pl?/97/29/nr02-29.52a.htm

Lightning fast RealSecure 2.0 hobbled by signature bugs, InfoWorld Feb 16, 1998 http://www.infoworld.com/cgi-bin/displayTC.pl?/reviews/980216realsecure.htm

RealSecure fends off network attacks, PC Week Labs, February 25, 1998 http://www.zdnet.com/pcweek/reviews/0223/23sec.html

Digital sentries, InfoWorld, May 4, 1998 http://www.infoworld.com/cgi-bin/displayTC.pl?/980504comp.htm

Cracker Tracking: Tighter Security with Intrusion Detection, Byte Magazine, May 1998 http://www.byte.com/art/9805/sec20/art1.htm
Intrusion Detection Systems: :Suspicious Finds, Data Communications, August 1998 http://www.data.com/lab_tests/intrusion.html
RealSecure 3.0 halts host intrusion but can't cover the enterprise, PC Week Labs, February 15, 1999 http://www.zdnet.com/pcweek/stories/news/0,4153,389071,00.html

Comments

Both manager and agents are designed to run on separate and dedicated hosts. The vendor recommends that they *not* be run on the same host except for demonstration purposes.
Check Point Software has contracted to sell RealSecure under its name.

RealSecure is a combined host-based and network-based intrusion detection system that uses built-in attack signatures and statistical profiles to detect different types of misuse. The network-based and host-based components are an integrated package (they are not sold as two separate programs) and are controlled from a single management console. The network-based component captures and analyzes network packets, and interprets invalid activity from network traffic patterns and content. The host-based component monitors system-level activity. Once an attack or misuse is recognized, an administrator is alerted via email and an alarm is displayed on the management console. The attack or misuse can be terminated automatically, logged to a database, or recorded for later playback and maintenance of legal evidence. RealSecure can run reports on the attacks found and recommend a fix for each affected system. RealSecure is implemented in a distributed architecture, comprising a console and multiple sensors. The sensors monitor different networks or network segments and report to one or more central management consoles.

The sensor engine is installed on a dedicated UNIX or Windows NT host with one or more network adapter cards (for monitoring multiple networks). Each active session is maintained and tracked, so that attack patterns that span many packets can be detected. As the sensors detect unauthorized activity they take appropriate action and then send a message to the management console. Sensors can also upload their local log files and databases to the management console periodically, so that the user has a centralized report of network activity. A single sensor can report to one or multiple (up to 50) management consoles at the same time.[6]

The management console displays alarms, consolidates sensor data, provides report generation capabilities, and acts as a centralized engine management point. It can manage up to 50 sensors at one time. The user can choose to establish a steady flow of real-time information from the sensors to the management console(s) or to emphasize post-facto forensics over real time response. The management console displays real-time alarm data in a standard Windows NT activity tree mode, where the data in the tree can be sorted by destination address, source address, or event name. Events contain an icon that indicates the severity as well as a distinct event name. Multiple occurrences of the same event are combined into a single notification. Event data can also be stored in an ODBC-compliant database for generation of reports. Reports are available in text and graphic formats and the user can launch customized reports from the interface, if desired. Reporting features allow the administrator to sort and format event data by priority, source address, destination address, or network service over some period of time.

RealSecure uses a secure channel for passing messages between engine and console. This channel guarantees; 1) delivery with no retry logic required by the caller; 2) securely encrypted data; 3) data integrity checks; and, 4) that no invalid data stream proxying occurs.

RealSecure is shipped with a set of intrusion detection signatures. Updates are posted on the ISS web site with each new software version (http://www.iss.net) and users are notified of the new software via e-mail. There are four ways to customize RealSecure: 1) tailor connection events, 2) select from a number of event responses, 3) tune some attack signatures to the local environment, and 4) instruct the filtering logic to ignore certain kinds of traffic.

[6] RealSecure recommends careful use of this feature, since it could (in the event of a burst of activity) consume huge amounts of network bandwidth and become a denial of service event in itself.

4.12 SecureCom Switches

Table 4.12-1: SecureCom Switches - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X		X					X		X			X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distrib-uted	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
X					X				X				X

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
	X			X				X			X			X		X				X			X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authen-tication	user access control	user privilege mgt	none	manager-agent verifi-cation	manager-agent data encryption	secure software updates	none
	X		X								X

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
		X	X				X		X	X	

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data con-sistency	system behavior	other	none
											X

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	informa-tion	analysis	fixes	counter-measures	none
	X					X							X

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X		X		X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X	X			X							

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X				X						X

Table 4.12-2: SecureCom Switches - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
												X

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	none	yes	no	n/a
X				X	X					X		

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
X	X	X	X	X	X	X	X				X	

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
X	X	X	X	X	X									

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
						X							X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company	ODS Networks, Inc. (SecureCom)
Manager	A customer-supplied (in addition to the switch) Windows NT system running 4.0+), and 96 MB of RAM, 100BaseTX network adapter card.
Sensors	ODS Network's SecureAuditor, SecureDetector, or SecureSwitch.

Targets

Topologies:
SecureAuditor, SecureDetector: 10/100Mbps Ethernet
SecureSwitch: Ethernet. Fast Ethernet
Network Protocols:
IP, IPX, or Appletalk
Application Protocols:
N/A

Interoperability

ODS Network's SecureAuditor, SecureDetector, or SecureSwitch hardware.
ISS RealSecure in SecureDetector and SecureSwitch.
Microsoft Access

Protection

Not addressed

Reports

Multiple pre-defined security reports
Customizable reports using Microsoft Access software

Alarms

Reports to console.

Response to events

Information not provided.

Performance

Allows the monitoring of 10 different segments at one time.

Customization

Customizable reports using Microsoft Access software

Special Features

Conversation monitoring rather than packet monitoring

History

Information not provided.

Information

Information:
http://www.ods.com/
Support:
Information not provided.

Cost

Information not provided.

Evaluations/Awards

None found.

Comments

ODS claims to address wire-speed monitoring, and states that not only are they compatible with current high-speed networks, but will also be compatible with the gigabit networks to come. It is not clear, however, whether this really allows RealSecure to work effectively at such speeds, or just SecureInvestigator.

SecureAuditor is a multi-port switch/probe. This system can monitor multiple simultaneous high-speed links, by providing ten 10/100 probe-monitoring ports and one port to attach to the server running the SecureInvestigator application. Also included is a security management card that listens on the switch/probe's backplane to record data on the activity on monitored network segments. SecureAuditor requires an external Windows NT workstation for the SecureSwitch Investigator software. It includes 10 available links for 10/100Mbps traffic monitoring and analysis.

SecureDetector is an integrated hardware/software system incorporating ODS's enterprise-level network equipment with a built-in Windows NT engine, ODS SecureInvestigator software, and RealSecure software. It can be deployed on critical segments of a network and monitor virtually all network traffic passing through these segments. It includes 10 available 10/100Mbps Ethernet ports (for simultaneous traffic analysis), a built-in Windows NT system running the RealSecure probe engine, and SecureInvestigator and RealSecure console software. It requires an external Windows NT (4.0 or higher) workstation for the SecureInvestigator and RealSecure console software.

SecureSwitch is an integrated network hardware/software system that includes advanced LAN switching from ODS Networks, a built-in Windows NT system running RealSecure software, and ODS SecureInvestigator software. SecureSwitch monitors virtually all network traffic passing through the segment. Because SecureSwitch is implemented as part of the corporate network, it is able to detect internal and external violations that would escape even the most sophisticated network probe. SecureSwitch provides both packet-level and session-level (conversation level) analysis of network traffic. It includes ODS Networks Ethernet/Fast Ethernet switching, built-in Windows NT system (for RealSecure engine), and ODS management card. It requires an external Windows NT (4.0 or higher) workstation for the SecureInvestigator and RealSecure console software.

The ODS SecureSwitch tracks conversations (at OSI RMON2) and can determine such things as the point of entry and what resources are being accessed. This approach has the ability to capture information on network traffic directly from the switched backplane packet bus. This eliminates the limitation (imposed by most switches) of being able to capture traffic from only one port (a problem when port mirroring is used to capture traffic from a switch for a conventional IDS). All SecureCom products provide this kind of monitoring capability, and can be deployed as either a switch or as a conventional IDS sensor. In addition, SecureCom firmware allows the switching functionality to be disabled and allow traffic to be directed to a single output port. This allows the deployment of SecureAuditor and SecureDetector as multi-port probes. This configuration enables the use of SecureCom products to monitor multiple strategic points in a network (firewalls, WAN routers, security components, etc.).

SecureInvestigator is designed to work with ODS Network’s SecureAuditor, SecureDetector, or Secure-Switch hardware. These systems incorporate ODS's enterprise-level network equipment with a Windows NT engine that monitors network traffic for security violations and security risks. In the case of SecureAuditor, only SecureInvestigator is used. In the cases of SecureDetector and SecureSwitch, RealSecure (see Section 4.11) is added to the package so that in effect the bundle becomes a network-based sensor with a RealSecure engine and the added benefits of SecureInvestigator. This approach attempts to address the problem of switched networks (see Section 3.2.2.1, Issue 6), unlike other vendors that address the problem of switched networks by performing port mirroring (which can severely effect performance).

The SecureInvestigator software is a database application that tracks layer three (IP and IPX) network activity, monitors for open TCP ports, tracks changes to the physical and logical infrastructure, monitors for modem back-doors, provides spoof detection, and other types of security-relevant activity. The SecureInvestigator console hardware platform is based on a Pentium 200 running Windows NT or Windows 95. SecureInvestigator software includes a relational database that logs network threats and network breaches, allowing network or security administrators to compile reports and develop histories of unauthorized network activity.

SecureInvestigator taps into the management bus on SecureAuditor, SecureDetector, or SecureSwitch hardware, monitoring all conversations being probed or switched by this network equipment. Rather than focus on packet patterns that indicate hacker threats (a function performed by ODS RealSecure software), SecureInvestigator examines who is talking to whom, and what protocols they are using in these conversations. It compares these conversations to known threat patterns and also allows administrators to develop and apply their own threat patterns. By doing so, SecureInvestigator can perform traffic analysis and infrastructure analysis functions.

SecureInvestigator includes a number of pre-configured reports, including:

1) Alien conversation (i.e., invalid or unusual communications) reports. These reports allow an administrator to prune out most normal traffic, leaving unusual traffic for review and response.

2) Infrastructure Report. This report allows an administrator to look for unusual patterns (e.g., IP hosts with unusual or lacking DNS entries).

3) SNMP Community String Analysis. The report will also show any inconsistencies between current or past used community strings.

4) IP or IPX Conversation Analysis. This report provides a record of all devices a specific user has accessed on the network.

In addition, the SecureInvestigator database may be examined, and custom reports may be generated, using Microsoft Access software.

4.13 SecureNet PRO

Table 4.13-1: SecureNet PRO - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X		X					X		X		X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X		X			X				X			

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
X			X					X			X			X			X			X			X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X		X	X				X	X		

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	interoperable	compatible interface	none	compatible interface	none	compatible interface	none
		X		X			X		X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
					X	X				X	

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	countermeasures	none

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
X		X			X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X						X					

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X						X				

Table 4.13-2: SecureNet PRO - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI	
DG-UX	**AT&T (NCR)**	**Novell NetWare**	**Linux**	**Cray Unicos**	**Convex**	**Mach**	**SCO**	**Sequent Dynix**	**Sequent Ptx**	**other**	**none**	**n/a**
												X

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
X	X										X	

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
		X					X				X	

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
X	X	X	X										X	

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
						X							X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company MimeStar, Inc.

Manager A Pentium-class PC or Sparc 5, with an Ethernet card capable of promiscuous mode.
Solaris-Sparc
Linux-x86
FreeBSD-x86
BSDi-x86

Sensors

A Pentium-class PC or Sparc 5.
Solaris-Sparc
Linux-x86
FreeBSD-x86
BSDi-x86

Targets

Topologies
Standard Ethernet networks.
Support for FDDI and other network transport mechanisms will be added in future releases.
Network Protocols
All TCP/IP-based protocols. These include TCP, ICMP, UDP, IPIP, IGMP, and others.
Application Protocols
Default services include web, e-mail, news, login, file transfer, talk, and many others. May be configured to monitor any TCP/IP-based network services.

Interoperability

None found.

Protection

Fault-tolerant proprietary communications system.
56-bit DES, 168-bit triple DES, 128-bit Blowfish, and fully exportable proprietary encryption.
MD5 authentication of all communications.

Reports

No information found.

Alarms

Update console or via e-mail.

Response to events

Suspicious connections can be automatically killed.
Sessions may be terminated.
Event fully logged for later playback.
Any TCP/IP-based network service may be blocked.
Entire web-server addresses or specific urls on web-servers may be blocked.

Performance

Each console may manage a virtually unlimited number of remote SecureNet PRO agents.

Customization

The administrator may configure the system:

- To monitor and block any TCP/IP-based network service
- With new attack signatures and attack responses
- To monitor for key words and the response to them
- To block access to specified web sites or report attempts to access those web sites

Special Features

Keystroke monitoring,
Key word detection.
Session hijacking.

History

No known.

Information

Sites:
http://www.mimestar.com/html/products.htm
Support:
No information email address or telephone number found.

Cost

Information not provided.

Evaluations/ Comparisons

None found.

Comments

Web site was last updated in 1997.

SecureNet PRO is a real-time network intrusion detection system. It combines several technologies, including session monitoring for intrusion detection, firewall activities, keyword-based misuse detection, and session hijacking. It captures and analyzes network packets in real-time, and interprets hostile or invalid activity by recognizing the network traffic patterns and content that indicate attacks and other misuse. Once an attack or misuse is recognized, appropriate personnel may be alerted via e-mail. In addition, the attack or misuse can be terminated automatically, suspicious connections can be automatically killed, the activity logged to a database, or recorded for later playback.

SecureNet PRO is implemented in a distributed architecture. Multiple sensors can monitor different networks or subnets and report to one or more central management consoles. The sensors provide all network monitoring, intrusion detection/response, and logging capabilities. The console provides a graphical management environment for controlling multiple SecureNet PRO sensors. The SecureNet PRO sensor and administrative console may run on the same host. If they do, then no additional network traffic is produced. However if multiple SecureNet PRO sensors and administrative consoles are deployed across the network then the amount of traffic generated is very small, limited to client/server communications and network stream modifications such as termination and session hijacking. Each SecureNet PRO administrative console may manage a virtually unlimited number of remote SecureNet PRO agents. Each SecureNet PRO sensor may be configured to relay information to multiple administrative consoles to provide multiple monitoring or network management stations.

SecureNet PRO enables an administrator to perform TCP hijacking; i.e., the administrator may seize the connection of any user on his local area network. The user remains completely locked out while the administrator performs actions such as damage control or evidence collection.

SecureNet PRO supports the definition of custom attack signatures and response rules. It may be configured to monitor and if required, block, any TCP/IP-based network service. Default service monitoring includes web, e-mail, news, login, file transfer, talk, and others. It may be configured to block entire webserver addresses or specific urls on web-servers. Finally, it may be configured to block use of profane or politically incorrect language over a network.

4.14 SessionWall-3

Table 4.14-1: SessionWall-3 - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X		X					X		X		X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X		X				X					X	

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
X			X			X			X					X	X				X			X				X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X	X		X				X	X		

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	interoperable	compatible interface	none	compatible interface	none	compatible interface	none
		X		X		X			X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
	X	X		X	X	X	X				

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	countermeasures	none
	X	X				X		X	X	X		X	

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X	X		X		X			X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X				X				X	X	X	

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X				X			X			

Table 4.14-2: SessionWall-3 - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI	
DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
												X

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
X	X			X	X		X				X	

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
	X	X				X	X					

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
X	X	X	X											

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
X													X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
					X					

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
X											X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
					X				

Company	Platinum Technology International, Inc.
Manager	Windows 95/98 or Windows NT4.0/5.0 Intel Pentium, 166 MHz or faster 64MB RAM (64MB recommended) 200MB free space
Sensors	N/A, since its not a distributed system.

Targets

Topologies
Ethernet, Token Ring and FDDI
Network Protocols
TCP/IP, UDP, ICMP
Application Protocols
HTTP, FTP, TELNET, SNTP

Interoperability

Interfaces with FireWall-1 using the OPSEC interface.
Interfaces with Cisco Routers.

Protection

Provides logon and administrative access controls to control access rights to application and logs.
Capability to assign passwords for different levels of access to the logs

Reports

Network usage reporting, ranging from high level statistics to specific user activity, and real-time snapshots of network statistics, but only one intrusion detection report template. Automatic report scheduling. SNMP trap alert. Report export to different file formats (including Microsoft Word, Excel, CSV, HTML, and others).

Alarms

E-mail, fax, paging, and audible alerts and message to the manager console.
Logs data to an .mdb file.

Response to events

SNMP traps and SessionWall-3 log and NT event log entries.
Blocks inappropriate traffic based on rules or in response to a specific alert.

Performance

Intended to monitor a LAN segment per NIC installed (NICs supported).

Customization

Can define rules for monitoring, filtering, and blocking network traffic.

Special Features

Extensive internet misuse detection.
Extensive blocking capabilities.
Logs all e-mail, WEB browsing, news, Telnet, and FTP activity.
Identifies and blocks abusers by their by their Windows NT or Remote Access Service User ID (most products identify users only by their IP or Media Access Control addresses)

History

Abirnet developed SessionWall-3.
MEMCO acquired Abirnet in May 1998.
MEMCO was acquired by Platinum Technologies International Inc. in August 1998.

Information

Sites:
http://www.abirnet.com/
Support:
support@abirnet.com

Cost

Depends upon the concurrent traffic monitored and options chosen. Base price of $1,495 for 125 concurrent sessions, and $14,950 for unlimited sessions. Optional accessories for central console management and consolidated logging cost $3,000 and $6,500, respectively, for five console servers.

Evaluations/ Comparisons	SessionWall-3: Soup-to-nuts security, PC Week Labs, October 1, 1997 http://www.zdnet.com/pcweek/reviews/0929/29wall.html Digital sentries, InfoWorld, May 4, 1998 http://www.infoworld.com/cgi-bin/displayTC.pl?/980504comp.htm Intrusion Detection Systems: :Suspicious Finds, Data Communications, August 1998 http://www.byte.com/art/9805/sec20/art1.htm One if by Net, Two if by OS, PC Week Labs, February 1999 http://www.zdnet.com/pcweek/stories/news/0,4153,389071,00.html SessionWall-3 Ids Abusers, PC Week Labs, May 20, 1999, http://www.zdnet.com/pcweek/stories/news/0,4153,2262953,00.html
Comments	It can serve as a firewall of sorts, a usage-and-content monitor, and it also can block Web traffic based on url, site ratings, viruses, or active content. There is a limited range of attacks in the current version.

SessionWall-3 is a network-based network protection product that includes not only intrusion detection but also watches for other activities that fall more accurately under the term misuse detection. It combines scanning, blocking, detection, response, logging, alerting and reporting capabilities in a single integrated package. It works somewhat like a firewall, but rather than acting at the entry point to a network it applies prioritized rules to the activity it captures from a network segment. It can serve as a firewall of sorts, a usage-and-content monitor, and it also can block Web traffic based on url, site ratings, viruses, or active content.

It includes the following functions:

1) Network usage reporting ranging from high level statistics down to individual user activity.
2) Network security activities that include:
   - content scanning
   - monitoring for service denial attacks, suspicious activity, malicious applets, and viruses)
   - blocking
   - alerting and logging
3) Web monitoring and access enforcement by address, domain, group, and content.
4) E-mail content scanning, viewing and documentation.

SessionWall-3 is delivered with:

1) A set of attack signatures
2) A url control list of more than 200,000 categorized sites
3) A Java/ActiveX malicious applet detection engine
4) A virus scanner
5) A content scanning engine
6) An intrusion detection engine
7) A content viewer
8) Reporting capabilities

SessionWall-3 can be installed on any network attached Windows 95 or NT machine and can process the network traffic from an Ethernet, Token Ring and FDDI local network segment. It includes policy folders for Web access, for monitoring/blocking/alerts, for intrusion detection, and for suspicious activity detection. These policy folders contain the rules that SessionWall-3 uses to scan all the communications. These rules specify the patterns, protocols, addresses, domains, urls, content, etc. and the actions to be taken should these be encountered. New rules can easily be added or the existing rules can be changed using menu driven options. All network activity that is not associated with a rule is identified for statistical and real-time analysis, thus identifying the need for additional rules.

SessionWall-3 provides logon and administrative access controls to control access rights. Capability to assign passwords for different levels of access to the logs.

The SessionWall-3 reporter tool can query snapshots of network statistics, create graphic reports, and export them to different file formats (including Microsoft Word, Excel, CSV, HTML, and others). The report scheduler can create any of the reports at intervals as short as 15 minutes and e-mail them at the appointed time.

4.15 SMARTWatch

Table 4.15-1: SMARTWatch - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
	X		X		X		X		X		X	X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distrib-uted	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
	X		X				X				X		

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse defini-tion			attack and misuse re-sponse			connection event			protocol defini-tion			audit record definition			reports			encryption options			security op-tions			other		
	X			X				X			X			X			X		X				X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authen-tication	user access control	user privilege mgt	none	manager-agent verifi-cation	manager-agent data encryption	secure software updates	none
X			X	X	X	X			X		

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Man-agement System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
		X		X			X		X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java app-lets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data con-sistency	system behavior	other	none
						X				X	

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	informa-tion	analysis	fixes	counter-measures	none
X		X			X			X					X

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X		X		X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
		X				X			X		

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X				X						X

Table 4.15-2: SMARTWatch – Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI
						X	X				

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
									X			X

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
												X

Network Protocols

UDP	TCP	ICMP	IP	Apple-Talk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
														X

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none	n/a
											X	

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP Open-View	IBM Net-view	other	none	n/a
					X							X	

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
									X	

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun Web-Server	MS ISS	O'Reilly Website Pro	IBM Inter-net Con-nection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP Open-View	IBM Net-view	other	none
					X						X

Firewalls

ANS Inter-lock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company WetStone Technologies, Inc.

Manager NT, Windows 95 and 98 servers and workstations.

Sensors NA for a purely host-based IDS.

Targets **Operating Systems**
NT, Windows 95 and 98 servers and workstations.

Interoperability None known.

Protection

Self-monitoring for signs of tampering.
User authentication, account control, and privilege management on management console.
Manager to agent data encryption (Datakey SignaSURE Token (RSA cryptography)).

Reports

Information not provided..

Alarms

System console and email.

Response to events

Can replace illegally modified files with a backup version and launch a (user-defined) application to assist in data collection and other defensive efforts.

Performance

Information not provided.

Customization

The user can specify the frequency of checks, the resources to be monitored, criticality of those resources, and the desired reaction to identified misuse.

Special Features

None known.

History

Information not provided.

Information

Sites:
http://wetstonetech.com/index.htm
http://wetstonetech.com/smartwatch.htm
http://www.wetstonetech.com/smartwatch.htm
Support:
Phone: (607) 539-9981
FAX: (607) 539-9930
info@wetstonetech.com

Cost

Information not provided.

Evaluations/ Comparisons

None found.

Comments

This appears to be a new system. The information found about it is limited.

The SMARTWatch System Integrity Checker is a host-based an intrusion detection and reaction program that is designed to help identify and respond to malicious or accidental Windows NT system security breaches. It monitors files, directories, Web Pages, and the Windows Registry for changes and notifies users visually and via email of suspicious activity. The system is based on the premise that many of the known hacks for Windows operating systems involve changing some part of the system to obtain access or damage the system. These changes include, but are not limited to changing the Windows SAM settings, adding files to be run at startup, changing network configuration settings, adding utilities, removing traces of a hack from log files, and trojanizing common applications.

SMARTWatch uses digital signatures to sign system and application files, directory structure and content, URLs, Registry structure and content. Signed files include SMARTWatch’s own database files, which are signed every time the application is closed and validated every time the application is started. Users are alerted to any failure in database validation, which could indicate that the intrusion detection function has been tampered with.

SMARTWatch can use various means to deploy countermeasures in the event of a invalid activity. These include replacing illegally modified files with a backup version and launching a (user-defined) application to assist in data collection and other defensive efforts.

SMARTWatch uses the Datakey SignaSURE Token (RSA cryptography) to provide secure, tamper resistant digital signatures that provide assurance that registered files are original and have not been tampered with. File attributes are also monitored for changes in file access privilege. SMARTWatch can be configured to monitor files that expand, like log files, by validating only the portion of the file that was present when the file was signed, and, optionally, resigning the resource when an increase in size is detected. SMARTWatch file markers can be added to text files so that only portions of the file are signed and validated, thus allowing dynamic or non-critical file sections to change. When designating files to be monitored by SMARTWatch, users can opt to automatically replace changed files with a backup of the original file in the event that a change is detected. SMARTWatch can also monitor the contents of a directory and the contents of a registry tree for change. Administrators can be notified in the event of files being added to or deleted from a directory.

As changes to the Windows Registry can be catastrophic to Windows machines and to a Windows network, SMARTWatch monitors the Windows Registry for both changes in the Registry's structure and in the Registry's content. Registry settings include Access Control Lists, passwords, certificates, hardware settings, network settings, and much more. SMARTWatch can be configured to monitor for unauthorized changes in any portions of the Registry that they choose.

4.16 Stake Out

Table 4.16-1: Stake Out - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
X		X					X		X			X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distrib-uted	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
X	X												

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X		X								

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	inter-operable	compatible interface	none	compatible interface	none	compatible interface	none
		X	X				X		X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring

IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
											X

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	counter-measures	none
					X								

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X		X		X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X									X		

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
		X					X				

Table 4.16-2: Stake Out – Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
												X

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	n/a	yes	no	n/a
											X	

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a

Network Protocols

UDP	TCP	ICMP	IP	AppleTalk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun WebServer	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP OpenView	IBM Netview	other	none	n/a
						X							X

Firewalls

ANS Interlock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun WebServer	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP OpenView	IBM Netview	other	none
					X						X

Firewalls

ANS Interlock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company	Harris Communications
Manager	Information not supplied.
Sensors	Information not supplied.

Targets

Network Topologies
Information not supplied.
Network Protocols
TCP/IP
Application Protocols
Information not supplied.

Interoperability

Harris Network Management (HNM)
http://www.commprod.harris.com/network-mgmt/hnm-index.html
Sun Netmanager
HP Openview

Protection

Encrypted inter-process communications.

Reports

Information not supplied.

Alarms

Console messages and page and/or e-mail system administrators.

Response to events

Complete event logging.

Performance

Information not supplied.

Customization

Information not supplied.

Special Features

Information not supplied.

History

Information not supplied.

Information

Sites:
http://www.commprod.harris.com/network-security/
Support:
1-800-4-HARRIS, extension 4701

Cost

Local agent only costs $7,995.00. Distributed management must be provided by a comprehensive network management system.

Evaluations/ Comparisons

None found.

Comments

For distributed capability must be combined with the Harris Network Management (HNM) system (or another similar network management system).

Stake Out is a network-based intrusion detection system that is an optional software component of the Harris Network Management (HNM) system, but may also be run as a local stand-alone IDS. In addition, it may output alerts any other SNMP compliant network management system, such as Sun Netmanager or HP Openview.

Stake Out is available in two versions: Stake Out Workstation and Stake Out Enterprise. Stake Out Workstation is a stand-alone system which is designed to monitor traffic on a network segment and includes Motif-based interface for configuration and alert display. It is intended for small networks with few segments or for remote sites where response to an intrusion alert must be coordinated with staff local to the attacked system. Stake Out Enterprise is designed for companies with large wide-area networks and includes security plug-in for network management systems and includes a powerful graphical user interface. Both versions deliver: real-time detection of probes and intrusion to a networked system, allow centralized monitoring through compatible network management systems, visibility of network activity, and integration of security management with enterprise network management systems.

For every detected event, it logs the date and time, source/destination address and port numbers, type of attack detected, complete network packets involved in the attack, and a continuous log of the suspected attacker's network traffic following the initial suspicious activity.

4.17 Tripwire

Table 4.17-1: Tripwire - Characterization and Attributes

Characterization (Section 2.1)

Deployment		Information Source					Method		Execution		Response	
network based	host based	network packets	operating system	application	file system	other	knowledge based	behavior based	dynamic	static	active	passive
	X				X		X			X		X

Attributes (Section 2.2)

Suitability (Section 2.2.1)

Architecture		Remote Management				Agent to Console Ratio				Communication Robustness			
local	distributed	any console	central console	none	n/a	high	medium	low	n/a	f/t ptp protocol	other	none	n/a
X					X				X				X

Flexibility (Section 2.2.2)

Customizable Features (Key: [broad, limited, none])

attack and misuse definition			attack and misuse response			connection event			protocol definition			audit record definition			reports			encryption options			security options			other		
X					X			X			X			X		X				X			X			X

Protection (Section 2.2.3)

Self-Monitoring		Stealth Technology		Console Security				Communication Security			
yes	no	yes	no	user authentication	user access control	user privilege mgt	none	manager-agent verification	manager-agent data encryption	secure software updates	none
	X		X				X		X		

Interoperability (Section 2.2.4)

Comprehensive Network Management System			Alternate Management System		Vulnerability Scanner			Separate Host-based IDS		Separate Net-based IDS	
component	compatible interface	none	compatible interface	none	interoperable	compatible interface	none	compatible interface	none	compatible interface	none
		X		X			X		X		X

Comprehensiveness (Section 2.2.5)

Additional Misuse Monitoring											
IRC	active content	Java applets	encrypted sessions	e-mail content	specific key words	specific urls	viruses	data consistency	system behavior	other	none
								X			

Event Management (Section 2.2.6)

Event Prioritization		Report Merging and Data Visualization			Event Trace & Replay		24/7 Vendor Hotline		Vendor-provided Attack Database				
yes	no	broad	limited	none	yes	no	yes	no	information	analysis	fixes	countermeasures	none
	X			X		X	X						X

Active Response (Section 2.2.7)

Session Hijacking		Session Termination		Firewall Reconfiguration		Router or Switch Reconfiguration		Deception Techniques		Vulnerability Correction	
yes	no	yes	no	yes	no	yes	no	yes	no	yes	no
	X		X		X		X		X		X

Acquisition (Section 2.2.8)

Implementation				Exportability			Deployment Cost				
s/w	h/w	both	turnkey	yes	special	no	> 30K	20-30K	10-20K	< 10K	free
X				X						X	

Support (Section 2.2.9)

Product Information				Vendor Response				Attack Definition Updates			
great	ok	poor	none	great	ok	poor	none	web	e-mail	version	none
	X			X							X

Table 4.17-2: Tripwire - Specific Applicability

Target Systems (Section 2.3.1)

Operating Systems

SunOS	Solaris	DEC OSF	DEC Ultrix	SGI Irix	IBM AIX	MS NT	MS 98	HP-UX	Free BSD	Net BSD	BSDI
X	X	X	X	X	X	X		X	X	X	X

DG-UX	AT&T (NCR)	Novell NetWare	Linux	Cray Unicos	Convex	Mach	SCO	Sequent Dynix	Sequent Ptx	other	none	n/a
			X	X	X	X	X	X	X			

Network Topologies										Switched Nets		
10Mb/s Ethernet	100Mb/s Ethernet	1000Mb/s Ethernet	45Mb/s T3 links	100Mb/s FDDI	ATM	ISDN	Token Ring	other	none	yes	no	n/a
									X			X

Supported Protocols (Section 2.3.2)

Network Application Protocols

DNS	HTTP	FTP	SMB	NFS	SNMP	TELNET	SMTP	RSH	X-Win	SSL/SSH	other	n/a
												X

Network Protocols

UDP	TCP	ICMP	IP	AppleTalk	IPX/SPX	ISDN	ATM	Ethernet	Token Ring	DEC	CIFS	NetBIOS	other	n/a
														X

Supported Applications (Section 2.2.3)

Monitored Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun WebServer	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none	n/a
												X

Routers							Management Systems						
Cisco	Ascend	Bay Nets	3Com	other	none	n/a	Back Office	SAP	HP OpenView	IBM Netview	other	none	n/a
						X							X

Firewalls

ANS Interlock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none	n/a
										X

Reconfigured Applications

Web Servers

Netscape Enterprise /FastTrack	Tandem CyberWeb	Cisco Web Server	CERN	NCSA HTTPd	Sun WebServer	MS ISS	O'Reilly Website Pro	IBM Internet Connection	Apache	other	none
											X

Routers						Management Systems					
Cisco	Ascend	Bay Nets	3Com	other	none	Back Office	SAP	HP OpenView	IBM Netview	other	none
					X						X

Firewalls

ANS Interlock	Raptor Eagle	Cyber-shield	Cisco	Gauntlet	Firewall 1	Border-guard	Checkpoint	other	none
									X

Company	Tripwire Security Systems, Inc.
Manager	A management console is slated for release later in 1999.
Sensors	N/a, for a purely host-based IDS.

Targets

Operating Systems
NT 4.0 or later
Sun Solaris (SPARC), Solaris (Intel), SunOS
Linux
HP HP/UX
IBM AIX
DEC OSF/1, DEC Ultrix
Free BSD, Net BSD, BSDI BSD/386
SGI Irix
Sequent Dynix, Sequent Ptx
Convex
Cray Unicos
Mach
SCO

Interoperability

None.

Protection

Detects changes using digital signatures so as not to compromise data confidentiality.
Cryptographically signed configuration, policy, and database files.

Reports

Includes overall summary as well as more detailed output. Events are sorted by user defined severity, and marked with user defined labels.

Alarms

Email.

Response to events

Generates a report.

Performance

Hashes van be very CPU intensive, though the commercial product is significantly faster than the free version. Every integrity check can be designated as to how much is checked at that time, allowing scheduled checks of differing usage of system resources.

Customization

May be customized to any file system and security policy.

Special Features

None.

History

In August 1998 Visual Computing Corporation (VCC) changed its name to Tripwire Security Systems, Inc.
Gene Spafford and Gene Kim (Chief Technology Officer at Tripwire Security Systems, Inc) originally developed tripwire at Purdue University.

Information

Sites:
http://www.tripwiresecurity.com
http://www.tripwiresecurity.com/support/price_guide.html
Support:
support@tripwiresecurity.com

Cost

A free release of Tripwire 1.3 is available that will compile on most Unix based operating systems. This version has limited support and no feature enhancements from the original Purdue releases.
Sliding scale based on number of computers. For example, for 1 – 4 computers, the standard software license fee is $495, and expended support is $175 per station, per year.
Government pricing is $257.

Evaluations/ Comparisons

None found.

Comments

A C compiler, lex, yacc, and make (for source release distribution) are required to run Tripwire.
Tripwire as delivered is a local system product.

Tripwire is a functionally narrow host-based intrusion detection system that monitors files (e.g., data, system files, user executables) for unauthorized alterations. Tripwire is a local IDS, and does not comprise a manager with one or more remote agents. It is an all-inclusive software tool that that is run on each host individually. It monitors every file and directory information on that host system. It automatically compares the properties of designated files and directories against information stored in a previously generated database. All changes to these files are flagged and logged, including those that are added or deleted. It lets the user specify file system exceptions that can change without being reported. On the other hand, the user can specify that unauthorized modifications in a user's group or permission, changes in system files, or unexpected changes in program files be tracked and always be reported.

Tripwire automates the creation of input lists and output lists of files. It supports extensible arbitrary file systems. It includes a simple way to describe the portions of the file system to be checked. In cases where files are likely to be added, changed, or deleted, Tripwire makes it easy to update the checklist database. File attributes such as the file size, ownership, inode number, inode values and timestamps are compared between the input and output lists. For each file, the Tripwire program computes a digital signature. A digital signature is a fixed-sized output generated by a signature function whose input is an arbitrary file. If the contents of a file are changed in any way, then the signature should also change. Tripwire contains eight signature functions including the 16-bit additive checksum, and 16 and 32-bit CRC function. The 16-bit additive checksum adds the values of all the bytes in the file and outputs the lower 16 bits (remainder). However the 16 and 32-bit signature functions are easy to break. One can generate an identical signature using a different input file. A solution to this is to use message digest algorithms. These functions use "one-way" functions that are difficult to invert and that usually generate a large value, making exhaustive searches for duplicate signatures more computationally difficult than those with 32 bits.

The Tripwire program can be set up to run on a regular user-determined schedule to detect file changes. It is also possible to run the program manually to check a smaller set of files for changes.

5 Acknowledgements

The author gratefully acknowledges the expert assistance and input of Marc Dacier, Andreas Wespi, Hervé Dubar, Dominique Alessandri, Stephane Schitter, and Andreas Tscharner of the IBM Zurich Global Security Analysis Laboratory; Mike Puldy of IBM’s Emergency Response Service; and Alexey Yankovski of Akvilon Ltd.

6 References

1. *An Intrusion Detection Model*, Dorothy Denning, IEEE Transactions on Software Engineering, Vol. 13, No. 2, February 1987.

2. *Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection*, Thomas H. Ptacek, Timothy N. Newsham, Secure Networks, Inc., January 1998 http://www.secnet.com/papers/ids-html/

3. *Adaptive Network Security: Solutions for Managing Risk in an Interconnected World*, Aberdeen Group, Vol. 11, No. 5, January 1998.

4. *CSI Intrusion Detection System Resource*, Computer Security Institute, 1998 http://www.gocsi.com/intrusion.htm

5. *Hacker Stoppers? -- Companies Bought $65 Million Worth Of Network-Intrusion Tools Last Year, But Capabilities Still Lag What's Promised*, Information Week, April 1998 http://www.techweb.com/se/directlink.cgi?IWK19980420S0066

6. *Cracker Tracking: Tighter Security with Intrusion Detection*, Byte Magazine, May 1998 http://www.byte.com/art/9805/sec20/art1.htm

7. *Adaptive Network Security Management: Intrusion Detection and Security Assessment Come of Age*, The Yankee Group Data Communications Report, Vol. 13, No, 10, June 1998.

8. *Towards a Taxonomy of Intrusion Detection Systems*, Hervé Dubar, Marc Dacier, and Andreas Wespi, IBM Research Division, Zurich Research Laboratory, July 1998.

9. *Intrusion Detection Systems: Suspicious Finds*, Data Communications, August 1998 http://www.data.com/lab_tests/intrusion.html

10. *Design and Implementation of a Sniffer Detector*, Stephane Grundschober, Proceedings of RAID’98 workshop, September 1998 http://w3.zurich.ibm.com/~dac/Prog_RAID98/Program.html http://www.zurich.ibm.com/Technology/Security/extern/gsal/sniffer_detector.html

11. *Security for Midsize Enterprises: The Trouble with Tools*, J. O’Reilley, Gartner Group, September 1998.

7 Glossary

Active response The kind of IDS response to an attack or anomaly that involves taking corrective or deterrent action.

Agents IDS agents collect and process target system information, then transfer the results to the IDS manager. In some cases they do little more than collect and preprocess the information before sending it to the manager; in others they perform most of the IDS processing and response and send only final reports to the manager. In the case of host-based IDS, agents are software modules that are installed at each monitored system. In the case of network-based IDS, agents are software modules that are installed on dedicated hardware systems that are placed at critical junctures of the network to capture and process network packets.

ANSI American National Standards Institute.

Attack Invasive, invalid, and sometimes destructive activity, generally but not always undertaken by an unauthorized outsider. A successful attack is one leading to an intrusion.

Attack scenario A logical sequence of actions applied by a malicious user to reach a particular strategic goal. These actions are typically applied to different network nodes, using a variety of tools. To complicate matters, many different attack scenarios may be used to reach the same goal.

Attack definition Encoded attack scenario that is used by an IDS to detect a particular attack (also called an attack signature).

ATM Asynchronous Transfer Mode. ATM is a transfer mode in which all types of information is organized into fixed form cells for delivery on an asynchronous or non-periodic basis over a range of media. ATM is generally associated with high speed and advanced networking. It is often the preferred technology for corporate backbone networks

Audit source The kind of information an IDS analyzes (e.g., host audit logs, network packets).

Backbone A term used to describe the central communication link of an organization’s networks (hence the name).

Bandwidth The measurement in bits per second required to exchange information between computers over a LAN, WAN or serial connection. Since time is a premium, more bandwidth is needed to exchange the ever-increasing amount and frequency of data between clients and servers.

Behavior-based A detection method that uses information about the normal behavior of the system being monitored.

Behavior on detection The response, either active or passive, of an IDS when it detects an attack or anomaly.

CIFS Common Internet File System. Microsoft Windows networking environment.

Connection event An IP-based connection that matches any combination of protocol, source IP address, destination IP address, source port, and destination port.

Content-based detection Identifies attacks destined for specific software services and programs (e.g., ftp, sendmail, http, and rlogin)

Context-based detection Identifies protocol-based attacks such as source routing, IP fragmenting, and SYN flooding.

Corrective action The removal of system vulnerabilities that enable an attack (e.g., installing security patches).

Cryptography The science and practice of encoding messages to protect them from being read by those who are not authorized to do so.

CSV Common Services Verbs (interface) [Microsoft].

DBMS Data base management system.

DEC Digital Equipment Corporation.

Detection The action of identifying that a system state is erroneous.

Detection Method The means by which an erroneous state may be determined.

DNS Domain Naming System.

Dynamic operation Performs continuous analysis by acquiring information about the actions taken on the monitored environment immediately after they happen. Dynamic operation implies real-time information processing.

Enterprise Enterprise network or environment refers to combinations of LANs and WANs that serve a logically related group of systems, such as those belonging to a large, widely dispersed company.

Ethernet Ethernet is the most popular local area network (LAN) for transmitting information between computers at speeds of 10 Mbps over a range of media including twisted pair and fiber optics. Ethernet standards are developed under the direction of the IEEE 802.3 committee.

Event **1.** A significant security incident as indicated by an IDS (e.g., a probable (not necessarily certain) attack by an intruder, misuse (perhaps unintentional) by an insider, etc.). **2.** The transition of a computer or network to a significant altered state; one that is considered worth reporting.

False positive Benign activity that is identified as an event.

False negative Missed events.

Fast Ethernet Fast Ethernet is quickly becoming the next most popular LAN technology for connecting power workstations and servers at ten times the speed of Ethernet over a similar range of media. Ethernet standards are developed under the direction of the IEEE 802.3 committee of which ODS remains an active participant.

Fault **1.** An adjudged or hypothesized cause of an error. **2.** Error cause that is intended to be either avoided or tolerated. **3.** Consequence for a system that has interacted or is interacting with the system under consideration.

FDDI Fiber Distributed Data Interface. A popular backbone technology for transmitting information at high speed with a high level of fault tolerance. FDDI standards are developed under the direction of ANSI.

Firewall A network device designed to provide a protection layer between the secure internal networks and insecure external networks. Firewalls examine traffic for patterns and protocols and reject unauthorized or dangerous packets and sessions.

Frequency How often the IDS analyzes the audit sources (e.g., continuous, periodically, snapshot).

FTP File Transfer Protocol [Internet].

GUI Graphical User Interface.

Host For our purposes, a computer that executes application code (e.g., mainframes, user workstations, and network servers).

Host-based IDS that monitor system- or server-based information (e.g., application logs, OS audit logs, security logs, data files and directories, and configuration information). This method focuses on misuse on the local system (which is frequently the result of malicious insider activity).

HTML HyperText Markup Language.

HTTP HyperText Transfer Protocol.

Hub A networking device which provides LAN connectivity on one or more shared segments.

ICMP Internet Control Message Protocol [Novell].

IGMP Internet Group Multicast Protocol.

IDS Intrusion Detection System.

IETF Internet Engineering Task Force.

IIS Internet Information Server [Microsoft]

Insider An individual who has some level of legitimate access to and privilege within a system.

Internet A collection of packet switching networks inter-connected by gateways, with protocols that allow them to function logically as a single, large, virtual network. The Internet uses the TCP/IP protocol suite, and provides worldwide connectivity.

Intrusion Explicitly defined as computer misuse that is undertaken by an outsider. However, the term is frequently used in reference to any computer misuse.

IP Internet Protocol. The collection of protocols used to interconnect computers locally and externally over the Internet or a private Intranet. Their development is coordinated by the IETF.

IPX Internetwork Packet Exchange [Novell]

IRC Internet Relay Chat.

ISDN Integrated Services Digital Network.

Knowledge-based A detection method that uses information about known attacks on the system it monitors.

LAN LANs are high-speed networks used to connect together components at a single location. They are a collection of interfaces and protocols that enable the exchange of information between local computers. The IEEE 802 committee and its working groups govern most LAN standards. Popular LANs include Ethernet, token-ring, and 10base-T (twisted-pair). LANs typically run at 10 megabits/sec or faster.

Manager An IDS manager consolidates and in some cases completes analysis of information from the IDS agents. It usually manages agent configuration, displays alarms, and generates reports. It sometimes activates pagers, sends email, and performs other actions in response to events (sometimes agents perform these tasks).

Mbps, Mb/s Megabits per second.

Misuse 1) A deliberate action that leads to the compromise of computing resources or the information handled by them. 2) Use of a service offered by a system to perform an action that is undesired and therefore does not conform to the appropriate acceptable use and/or security policy. The user performing this action is abusing the privileges (if any) granted to her/him. 3) Introduces an intentional system fault.

NA Network Associates Inc.

NCSA National Center for Supercomputing Applications.

NetBIOS Network Basic Input/Output System [IBM].

Network-based IDS that monitor network activity (e.g., traffic, and packets). This type of IDS focuses on network or infrastructure attacks by intruders.

Network Management The mechanism by which the central functions of the network are managed and controlled. These include isolation of faults, configuration, performance measurement and security. Network management components include intelligent agents, standard protocols like SNMP/RMON and a suite of applications for access, reporting and analysis.

NFS Network File System [Sun].

Network Interface Card Provides connection to a network for the internal bus of a host workstation, PC, or server via cable links. Also called a network adapter card.

ODBC Open Data Base Connectivity [Microsoft]

OTS Off the shelf.

Outsider An individual who must clandestinely enter a system, and has no legitimate privilege there.

Packets A predetermined amount of data that varies between networking technologies. Generally used to describe how a large block of data is segmented when sent through a network. In addition to the data, each packet typically includes information such as source and destination addresses.

Passive response The kind of IDS response to an attack or anomaly that is merely alarm (e.g., email, paging, console message) or report generation.

Periodicity Processing frequency.

Proactive action Direct steps to thwart an attacker (e.g., logging off possible miscreants, closing down services).

Promiscuous mode An operational state of a network interface card in which all packets on the network segment (for Ethernet and Token Ring) are made available to the host computer.

PTP Point to point.

Real-time IDS An IDS that is fast enough for: 1) Complete processing of the monitored flow of data (e.g., network packets) without loss, and 2) Effective automated response to take place.

Router A network layer device which supports multiple LAN interfaces and segments LANs into smaller collision and broadcast domains. As a network layer device, routers maintain a hierarchical network and service the interconnection of computers on different networks in that hierarchy. Route maintenance is extremely CPU intensive and dependent on the supported LAN protocols like IP in the network.

RSH Remote Shell.

SAMBA Microsoft Windows networking environment.

SATAN Security Administrator's Tool for Auditing Networks.

SDI Security Dynamics Inc.

Security policy The set of rules and practices that regulate how an organization manages and protects that which an the organization considers valuable.

Sensor The more common name for network-based IDS agents.

SMB Server Message Block (protocol) [MII].

SMTP Simple Mail Transfer Protocol.

SNMP Simple Network Management Protocol. SNMP is the collection of protocols and variables that enable a client to communicate with a server over an IP network for the purpose of exchanging operation and maintenance information. Standard SNMP variables along with company specific extensions in devices including hubs and switches enable remote configuration and control by an SNMP client running on a network management station.

SPX Sequenced Packet Exchange [Novell].

SSH Secure Shell. One of the most widely used network security protocols. It provides user authentication and the encryption of the transferred data (for confidentiality and integrity) in conjunction with the TCP/IP protocol. It can be implemented easily over any IP based network without changing the network configuration.

SSL Secure Socket Layer.

Static operation Performs periodic analysis by acquiring information about the actions taken on the monitored environment at some point after they happen. Static operation implies batch (or periodic) information processing.

STT Secure Transaction Technology [Microsoft]

SUN Sun Microsystems, Inc.

Target system The system monitored by the IDS, whether a host or a network segment.

TCP/IP Transmission Control Protocol/Internet Protocol. A broad-based standard communications protocol that provides reliable, full-duplex service between applications on different networked computers.

TIS Trusted Information Systems, which was purchased by Network Associates in 1998.

Token Ring The second most popular (after Ethernet) local area network (LAN) for transmitting information between computers at speeds of 16 Mbps over a range of media including twisted pair and fiber optics. Token Ring standards are developed under the direction of the IEEE 802.5 committee.

Traffic analysis An analysis of network headers to determine who connected to whom and when did it happen.

Trend analysis Analysis of today's activity in view of yesterday's activity to identify larger trends.

Trending reports Summarize current and historical patterns of misuse activity.

UDP User Datagram Protocol.

URL Uniform Resource Locator.

User For our purposes, this is the owner and operator of the IDS product.

Vulnerability A weakness in a computer system or network that could lead to accidental, inadvertent, or deliberate actions that violate system security.

WAN WANs are slower-speed networks that are typically used to connect sometimes geographically remote LANs together. They are a collection of interfaces and protocols that enable the exchange of information between computers on a wide area basis. WAN examples include frame relay, ISDN, T1-T3 and ATM. Standards governing these technologies are developed by organizations like the ITU.

Windows Registry A hierarchical data structure that is used to store configuration information for the operating system and many installed applications. It is used to store user certificates, startup information, user and group account information, passwords, network setting, and much more.