DPRO-95367
Ant Allan

Technology Overview
4 January 2002

Intrusion Detection Systems (IDSs): Perspective

Summary

An IDS is a “burglar alarm” on a company’s networks and servers. Malicious activity that evades other security will sound the alarm, but the organization needs the capability and will to respond.

Table of Contents

List Of Tables

Gartner

The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Technology Basics

The Need for Intrusion Detection

According to a recent study by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI), a staggering 70 percent of organizations surveyed reported a security incident. This figure is up from 42 percent reported in 1996. Taking into account organizations’ reluctance to admit to incidents or their inability to detect them, the true figure is likely to be higher.

E-business has driven organizations to open their networks to wider audiences over the Internet—home and mobile workers, business partners, suppliers, and customers—in order to stay competitive. But such open networks expose the organizations to *intrusions*—attempts to compromise, the confidentiality, integrity, or availability, or to bypass the security mechanisms of a computer system or network.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusion.

But why is intrusion detection necessary? Is it not enough for an organization to use a firewall to control access to its network and maybe a virtual private network (VPN) to secure communications? Deploying firewalls and VPNs is a good thing. A robust firewall policy can minimize the exposure of many networks. Nevertheless, such countermeasures alone are not enough.

Attackers Are Getting Smarter

Attackers are evolving their attacks and network subversion methods. These techniques include e-mail-based Trojan horses, stealth scanning techniques, and tunneling attacks in which an attacker masks traffic that should be screened by the firewall by encapsulating it within packets corresponding to another network protocol, such as Internet Control Message Protocol (ICMP) or domain name system (DNS).

Vulnerabilities Are Proliferating

Attackers also take advantage of vulnerabilities attributed to system misconfiguration, poorly engineered software, user neglect and carelessness, and basic design flaws in protocols and operating systems. There is an ever-growing list of application vulnerabilities, and attackers are very good at exploiting these via protocols, such as HTTP, that are let through by almost any firewall.

“Hacker” Tools Make Attacks Easier

Although many network scanning and attack techniques have been known for several decades, it is only recently that the tools to conduct sophisticated analysis of a target network have become widely available. As the sophistication of “hacker” tools has increased, the technical knowledge required to attack a network has fallen, so organizations are exposed to a rapidly growing number of potential attackers.

Insider Attacks Are Still Predominant

While outsiders may frequently and increasingly perpetrate misuse, it is still more often the result of malicious insider activity. This is because a legitimate (but 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). Perimeter defenses cannot protect against this kind of attack.

Intrusion Detection Systems (IDSs): Perspective

Intrusion Detection Systems

An *intrusion detection system* (*IDS*) is a software product or hardware device that automates the intrusion detection process. Without such automation, effective intrusion detection is practically impossible. An IDS's capability 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 facilitates timely response.

Functional Components

An IDS is made up of three functional components:

- information sources,
- analysis, and
- response.

The system obtains event information from one or more information sources, performs a preconfigured analysis of the event data, and then generates specified responses, ranging from reports to active intervention when it detects intrusions. There is also a management system that allows a security or network administrator to monitor and configure the system and to analyze the data. These components may or may not be running on the same box, and all of them may not be present.

System Monitoring Approaches

Broadly, the two system monitoring approaches are:

- *network-based IDS* (*NIDS*) and
- *host-based IDS* (*HIDS*).

NIDS

A NIDS monitors all network traffic passing on the segment where the agent is installed, reacting to any anomaly or signature-based suspicious activity.

NIDSs come in the guise of turnkey appliances that just plug in to the network or software that installed on commercial off-the-shelf (COTS) computers. A NIDS usually has two logical components:

- a sensor and
- a management station or console.

The sensor sits on a network segment, analyzing every network packet for attack signatures. The console receives alarms from the sensor(s) and displays them to an administrator. The sensors are usually dedicated systems that exist only to monitor the network. They have a network interface in promiscuous mode, which means they receive all network traffic, not just that destined for their IP address, and they capture passing network traffic for analysis.

HIDS

In its narrowest sense, a HIDS is an IDS that monitors platform and application event logs from multiple sources for suspicious activity.

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). HIDSs use software modules installed on each monitored host.

HIDSs can detect computer misuse from trusted insiders as well as from those who have infiltrated a corporate network. They look for unusual activity confined to the local host such as logins, improper file access, unapproved privilege escalation, or alterations on system privileges:

- *Application-based IDSs* are a special subset of HIDSs that analyze events within a software application based on the application's transaction log files. Application-based IDSs can also detect suspicious behavior where authorized users exceed their authorization.
- Switched and/or high-speed networks create problems for NIDSs: many are unreliable at high speeds, dropping a high percentage of network packets; and switched networks often prevent a NIDS from seeing passing packets promiscuously. *Network-node IDSs* (*NNIDSs*) delegate the network IDS function down to individual hosts alleviating these problems.
- *Hybrid IDSs* combine NNIDS and HIDS in a single package. Most commercial off-the-shelf (COTS) "HIDS" are actually hybrid IDSs, and many include application-based intrusion detection as well.
- *File-integrity assessment* (*FIA*) tools are a special kind of HIDS. Tripwire is perhaps the best-known example. When a system is compromised an attacker will often alter certain key files to provide continued access and prevent detection. FIA works by applying a cryptographic *hash function* to critical files and then checking the files periodically to ensure that the hash result, or checksum, is unchanged. (A hash function is an algorithm that computes a unique fixed-length value, the hash result, for each file.) Detecting a change will trigger an alert. Furthermore, following an attack the same files can be assessed to determine the extent of the compromise.

Table 1: Strengths and Weaknesses of Network-Based Intrusion Detection Systems

Strengths	Weaknesses
A few well-placed sensors can monitor a large network.	A NIDS may be overwhelmed by very high traffic volumes, may not be able to process all packets, and so may miss an attack. Few current (December 2001) products can operate effectively at gigabit line speeds.
Sensors are passive devices that listen to network traffic in real time without interfering with normal operation. A NIDS can be fitted to a network with little impact.	Switched networks pose problems. A sensor cannot see beyond a single segment, which can limit the range to a single host, and force the organization to deploy many sensors. Switches that provide monitoring or scanning port can at least partially mitigate this issue.
Sensors can be made very secure against attack and can even be made invisible to attackers.	A NIDS cannot analyze encrypted network traffic, e.g., if the organization uses VPNs. This will become more important as organizations migrate to IPv6.
A NIDS can detect an attack before it reaches the targeted system.	A NIDS cannot determine with certainty whether an attack was successful.
A NIDS is typically platform-independent and relatively easy to deploy. (More so for a NIDS appliance.)	Sensors may transmit large volumes of data to the management console, eating available bandwidth and causing latency problems.

Table 2: Strengths and Weaknesses of Host-Based Intrusion Detection Systems

Strengths	Weaknesses
A HIDS monitors events local to a host and thus can detect attacks that a NIDS cannot. It will see in detail exactly what the attacker does: command execution, file access, system calls, etc.	An OS-specific or sensor must be installed, configured, and maintained on each host to be protected.
A HIDS can distribute the load associated with monitoring across available hosts on a large network.	A sensor uses the resources of the host it is monitoring and, hence, inflicts a performance cost.
A HIDS is unaffected by encrypted network traffic as data has been decrypted (or has not yet been encrypted) when it is seen by the sensor.	As a HIDS depends on event and audit logs, it is important that logging is correctly configured to generate all required records, possibly impacting business application software.
A HIDS can monitor interaction between users and servers/applications allowing it to trace misuse to a known individual.	Technicians other than network/security people will likely maintain the host, and a sensor is at risk of being disabled if it appears to get in the way of business application software. A HIDS might be attacked and disabled as part of an attack on the host. A HIDS can be disabled by certain denial-of-service attacks.

Analysis Strategy

Analysis strategies fall into two basic types: *knowledge-based misuse detection* and *behavior-based anomaly detection*. Vendors, however, are often leery of having their proprietary analysis strategies categorized so simply.

Knowledge-Based Misuse Detection

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.

The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. More sophisticated IDSs use *state-based* analysis techniques; for example:

- reassembling fragmented packets to detect attacks where the attacker has deliberately split up to avoid detection;
- reassembling streams to detect session-based attacks, which occur over the course of a dialog between two systems and would likely not be contained in a single packet.

HIDSs generally use rule-based engines for analyzing activity. An example of such a rule might be, “superuser privilege can only be attained through the *su* command.” Therefore successive login attempts to the root account might be considered an attack. All commercial systems use some form of knowledge-based approach. Thus, the effectiveness of current commercial IDSs is based largely on the validity, currency, and expressiveness of their database of known attacks and misuse, and the efficiency of the matching engine that is used.

Behavior-Based Anomaly Detection

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.

One technique is *threshold detection*, in which certain attributes of user and system behavior are expressed in terms of counts, with some level established as permissible. Such behavior attributes can include the number of files accessed by a user in a given period; the number of failed attempts to log in to the system; and the amount of CPU used by a process.

Another technique is to perform *statistical analysis* on the information, build statistical models of the environment, and look for patterns of anomalous activity (e.g., accesses that occur at strange times, or an unusual number of failed logins). Some vendors are now incorporating this technology in commercial products, but it is difficult to engineer for commercial products, as well as uncommon.

There is now a considerable amount of active research in *adaptive systems*. These start with generalized rules for the environment, then learn, or adapt to, local conditions that would otherwise be unusual. After the initial learning period, the system understands how people interact with the environment, and then warns operators about unusual activities.

Table 3: Strengths and Weaknesses of Misuse Detection

Strengths	Weaknesses
Misuse detectors are very effective at detecting attacks without generating an overwhelming number of false alarms.	Misuse detectors can only detect those attacks they know about—therefore they must be constantly updated with signatures of new attacks.
Misuse detectors can quickly and reliably diagnose the use of a specific attack tool or technique. This can help security managers prioritize corrective measures.	Many misuse detectors are designed to use tightly defined signatures that prevent them from detecting variants of common attacks. State-based misuse detectors can overcome this limitation, but are not commonly used in commercial IDSs.
Misuse detectors can allow system managers, regardless of their level of security expertise, to track security problems on their systems, initiating incident-handling procedures.	

Table 4: Strengths and Weaknesses of Anomaly Detection

Strengths	Weaknesses
IDSs based on anomaly detection detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.	Anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviors of users and networks.
Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.	Anomaly detection approaches often require extensive “training sets” of system event records in order to characterize normal behavior patterns.

Timing of Information Sources and Analysis

An IDS might work in either *batch mode* or *real-time mode*.

All COTS products that vendors *market* as IDSs work in real time or “near” real time. NIDS are generally true real time. HIDS can be real time, but this demands a mechanism to capture an event at the same time that the audit record is being written, which is technically more challenging. It is easier for a HIDS to read the logs just after the records have been written, which imposes a small delay. This delay is not significant where an organization is trusting in a manual response, but can reduce the effectiveness of an automatic active response (e.g., forcibly terminating a user's session) by the IDS.

A system performing analysis of network packets or audit records at intervals longer than about 15 minutes cannot respond quickly enough to meet most organizations' expectations for an IDS. Nevertheless, batch mode analysis of IDS data can be valuable in at least two ways:

- Trend analysis, to establish extended probing activity that may signal a future attack.
- Forensic analysis, to build up a picture of how an attack succeeded and the vulnerabilities it exploited.

Other IDS Functionality

Response Options—Passive or Active

An IDS may respond to an identified attack, misuse, or anomalous activity in two ways. The first (and clearly universal) is a *passive* response, one where the IDS simply informs responsible personnel of an event by way of console messages, e-mail, cellular phones or pagers, and report updates. Some commercial IDSs generate Simple Network Management Protocol (SNMP) alarms and alerts, reporting them to a network management system.

Less often, the IDS also has the capacity to engage in an *active* response to critical events where (as specified by an administrator) it takes corrective or proactive action. Actions can include:

- correcting a system vulnerability,
- logging off a user,
- terminating a connection,
- selectively increasing monitoring,
- reconfiguring a firewall (to block an address that was the source of the detected intrusion or to throttle the amount of traffic allowed through a port), and
- disconnecting a port.

Reporting Mechanisms

When it detects a threat, an IDS generally sends an alert to a centralized management console where alert information can be recorded and brought to the attention of an administrator. Some IDSs can generate reports of system events and intrusions detected over a particular reporting period (say, a week or a month). Some provide intrusion data in formats suitable for inclusion in database systems or for use in report-generating packages (such as Crystal Decisions' Crystal Reports).

IDS Configuration

Typically, an IDS provides capabilities for selecting which attacks are monitored. Depending on the specific implementation of an IDS, an administrator might be able to select:

- which attacks will be monitored,
- what the response will be for each detected intrusion,
- specific source and destination addresses to be monitored or excluded, and

- characterizations of the class—the importance or severity—of each alarm.

This capability is critical to optimize the monitoring capability for an IDS. In this way, it is possible to focus the sensor on specific events of interest, and the response that the IDS will have on the detection of events.

Technology Analysis

Business Use

Intrusion detection allows organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Given the level and nature of modern network security threats, the question for security professionals should not be whether to use intrusion detection, but which intrusion detection features and capabilities to use. IDSs have gained acceptance as a necessary addition to every organization’s security infrastructure.

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, IDSs are especially useful for monitoring the network perimeter for attacks originating from outside and for monitoring host systems for unacceptable insider activity.

IDS products 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. By identifying successful invalid activity, IDSs can indirectly spotlight network and system vulnerabilities, enabling fixes and fine-tuning.

Benefits and Risks

Benefits

Deters Problem Behaviors

By increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system, an IDS can serve as a significant deterrent to insiders who would violate an organization’s information security policy.

Detects Misuse That Other Countermeasures Cannot Prevent

Although vendors and administrators are encouraged to address vulnerabilities that an attacker can exploit, this is not possible in many situations:

- In many legacy systems, the operating systems cannot be patched or updated.
- Even in systems in which patches can be applied, administrators sometimes have neither sufficient time nor resource to track and install all the necessary patches. This is a common problem, especially in environments that include a large number of hosts or a wide range of different hardware or software environments.
- Users can have compelling operational requirements for network services and protocols that are known to be vulnerable to attack.

- Access control mechanisms can allow legitimate users to perform actions that are ill advised or that overstep their authorization.

An IDS can detect when an attacker has penetrated a system by exploiting an uncorrected or uncorrectable flaw. Furthermore, it can serve an important function in system protection, by bringing the fact that the system has been attacked to the attention of the administrators who can contain and recover any damage that results and, perhaps, address the vulnerability against future attacks.

Detects and Deals With the Preambles to Attacks

Preparatory activity is commonly experienced as network probes and other “doorknob rattling.” When adversaries attack a system, they typically do so in predictable stages. The first stage of an attack is usually probing or examining a system or network, searching for an optimal point of entry. In systems with no IDS, the attacker is free to thoroughly examine the system with little risk of discovery or response and will eventually find a vulnerability and exploit it to gain entry to various systems. The same network with an IDS presents a much more formidable challenge to that attacker. Although the attacker may probe the network for weaknesses, the IDS will observe the probes, will identify them as suspicious, may actively block the attacker’s access to the target system, and will alert security personnel who can then take appropriate actions to block subsequent access by the attacker.

Documents the Existing Threat to an Organization

An IDS substantiates claims that networks and systems are likely to be attacked or are even currently under attack—many people mistakenly deny that anyone (outsider or insider) would be interested in breaking into their networks. Furthermore, if an organization understands the frequency and characteristics of attacks, it can better determine what security measures are appropriate to protect against those attacks.

Acts as Quality Control for Security Design and Administration

When an IDS runs over a period, patterns of system usage and detected problems can become apparent. These can highlight flaws in the design and management of security for the system, in a fashion that supports security management correcting those deficiencies before they cause an incident.

Provides Useful Information About Intrusions That Do Take Place

Even when IDSs are not able to block attacks, they can still collect relevant, detailed, and trustworthy information about the attack that supports incident-handling and recovery efforts. Furthermore, this information can, under certain circumstances, enable and support criminal or civil legal remedies. Ultimately, such information can identify problem areas in the organization’s security configuration or policy.

Risks

An IDS Is Not a Panacea

Despite the positive impact it can have on an organization, no IDS is indestructible and certainly should not be the only security measure that an organization employs. Only by combining an IDS with other countermeasures—such as firewalls, VPNs, and antivirus products—does an organization protect from a realistic range of security attacks. This combination is sometimes called *security in depth* or *defense in depth*.

Active Response Can Create Not Prevent Problems

Because hackers can use automatic responses to deny service, organizations must approach proactive responses 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 users, who may, as a result, become furious. Within an organization, mistakes of this sort create hostility towards security and might result in loss of earnings. Externally, they might leave the organization legally liable and will inevitably create bad press.

The IDS That Cried "Wolf!"

If there are 10 real attacks per million sessions—which is almost certainly an overestimate—then even if the system has a "false positive" rate as low as 0.1 percent, the ratio of false alarms to real alarms will be 100:1. (The problem is much worse where anomaly detection is employed to alert administrators about unusual activity that might signal a new form of attack, as this technique generates far more false positives.) This is a well-known issue for guards' response to burglar alarms and for medics running screening programs for diseases where the test error exceeds the organism's prevalence in the population. In general, where real alarms are so rare in comparison with false alarms, an alarm system is likely to so fatigue the guards that even the genuine alarms get missed.

Human Intervention Is Still Required

While the IDS can identify that an intrusion has occurred or is in process, and it may be able to provide the intruder's IP address, the security administrator or network manager must then investigate the attack, determine how it occurred, and correct the problem. In short, an organization must have both the capability and, moreover, the will to respond promptly to any alert at any time.

An organization should have incident-handling procedures describing how it will handle security incidents, such as viruses, insider abuse of systems, and attacks. These should, at a minimum, assign roles and responsibilities for all parties within the organization, outline the actions that are to be taken when an incident occurs, and establish schedules and content for training everyone about their responsibilities in the incident-handling process. Furthermore, the organization should make provisions to conduct "fire drills" in which all organizational parties step through their specific responsibilities and assignments.

Standards

Intrusion Detection Exchange Protocol (IDXP)

The Internet Engineering Task Force (IETF) Intrusion Detection Working Group (IDWG) (Internet: www.ietf.org/html.charters/idwg-charter.html) is working to define data formats and exchange procedures for sharing information of interest to intrusion-detection and response systems and to management systems that may need to interact with them. The design involves sending XML-based alerts over an HTTP-like communications format. The WG has paid a lot of attention to the needs of IDS analysis, and to making the protocol work through firewalls in a straightforward way.

Its recent Internet Drafts include *The Intrusion Detection Exchange Protocol* (*IDXP*) (11 September 2001) and *Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language* (*XML*) *Document Type Definition* (November 2001), and appears to be close to publishing Requests for Comments (RFCs).

The IDWG has built on some of the work of Common Intrusion Detection Framework (CIDF) (Internet: www.gidos.org/), begun in 1997, but which has been dormant since early 2000.

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) WD 15947: 1999 Information Technology—Security Techniques—IT Intrusion Detection Framework

Intrusion Detection Systems (IDSs): Perspective

The ISO/IEC Joint Technical Committee 1 Subcommittee 27 Working Group 1 (JTC 1/SC 27/WG 1) is working to define a framework for detection of intrusions into IT systems. It seeks to establish common definitions for intrusion-detection terms and concepts. It describes the methodologies and concepts and the relationships among them, addresses possible orderings of intrusion detection tasks and related activities, and attempts to relate these tasks and processes to an organization's procedures to demonstrate the practical integration of intrusion detection within a corporate security policy.

This Technical Report (TR) has languished as a Working Draft (WD) since December 1998. All target dates for further drafts and the final TR have passed.

Common Criteria Protection Profiles

A Protection Profile (PP) is an implementation-independent set of security requirements for a category of products or systems that meet specific consumer needs, as defined by the Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408:1999). The Information Assurance Technical Framework Forum (IATFF), an organization sponsored by the U.S. National Security Agency (NSA), has published a number of PPs for IDSs and vulnerability assessment (VA) scanners. (Internet: www.iatf.net/protection_profiles/intrusion.cfm)

Common Vulnerabilities and Exposures (CVE)

CVE is a list of standardized names for vulnerabilities and other information security exposures. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures in order to make it easier to share data across separate vulnerability databases and security tools. While CVE may make it easier to search for information in other databases, CVE is *not* a vulnerability database.

The content of CVE is a result of a collaborative effort of the CVE Editorial Board, which includes representatives from numerous security-related organizations such as vendors, academic institutions, government agencies, and prominent security experts. The MITRE Corporation maintains CVE and moderates Editorial Board discussions.

The current version of CVE is free to use and available for download from the CVE Web site (Internet: www.cve.mitre.org/about/).

Selection Guidelines

Suitability

Organizations should consider requirements and constraints imposed by their network topology and hardware and software infrastructure:

- *Applicability to an organization's target network and systems*—Can the IDS interpret the information of the local environment?
  - Operating systems—specific Unix OSes, MS Windows, Novell NetWare, etc.
  - Network topologies—Ethernet, T1/E1, etc.
  - Switched networks.
  - Protocols—ICMP, IP v4, IP v6, TCP, User Datagram Protocol (UDP), etc.
  - Applications—FTP, HTTP, Secure Shell (SSH), Telnet, etc.
- *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.

- *IDS management scheme*—An IDS that does not support remote management is unusable for an enterprise environment, and unwieldy even for a simple LAN. The most flexible IDS provides the capability for the user to securely log onto the management console and perform these tasks from any other console in the network.
- *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.
- *Communications robustness*—Robust communication includes techniques which 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.
- *Implementation*—Most commercial IDSs are solely software solutions that can be installed on a variety of commercial off-the-shelf (COTS) 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 organizations may want the ease of a turnkey system.
- *Performance*—An 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.
- *Accuracy*—The rates of false negatives (missed events) and false positives (benign activity that is identified as malignant events). Accuracy is directly linked to such things as the comprehensiveness of the initial signature database and the ability to fine-tune to the system being monitored as well as to timely and high-quality event signature updates.

Flexibility

An IDS product must be adaptable to the network or system it monitors. It should provide the organization with the means to customize monitoring, attack responses, event prioritization, and so on. Possible customizable features include:

- *Attack and misuse definition*—i.e., the addition of new attack or misuse signatures.
- *Attack and misuse response*—e.g., a means of escalating notifications to appropriate staff based on company-defined notification policies; a means for the organization to define, activate, modify, and test active responses.
- *Connection event response*—the capability for the IDS 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).
- *Protocol and audit record definition*—a means for the organization to define new protocols (for NIDS, NNIDS) and new audit records (for HIDS) so the IDS can interpret and process user-specified data sources.
- *Reports*—provision for user modification of supplied reports and report schedules and definition of a range of new reports.
- *Cryptography options*—provision for a user-configurable set of cryptography options, e.g., which algorithm to use, disabling all cryptography.

- *Security options*—the capability to control access to IDS applications, restrict privilege, and restrict logons to specific locations (e.g., system console only, certain other consoles).

Protection

Given its criticality to the security of any enterprise, an effective IDS must be resistant to malicious tampering. The features that determine this include:

- *Self-monitoring*—an IDS monitors its own activities for signs of interference or failure, and is capable of responding (if only with a console message).
- *Stealth techniques*—an IDS is effectively “invisible” on the monitored network (e.g., having no IP address), making it less vulnerable to attack.
- *Management console security*—provision of user authentication to the console (e.g., password, smart card), access control within the console, and privilege management.
- *Communications security*—communication between management console and agents should be secure so that:
  - configuration and diagnostic information can be securely transported between manager and agents, and
  - alarms and incident data arrive complete and uncorrupted at the manager.

Interoperability

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

- *Network management system* (*NMS*)—so a network administrator can incorporate the IDS into the overall network management architecture.
- *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.
- *Vulnerability assessment* (*VA*) *products*—in an ideal configuration, IDS and VA products should work interactively; for example:
  - if a scanner has detected a misconfiguration and an IDS detected an attack that is attempting to exploit that misconfiguration, then the event can be assigned a high priority;
  - the presence of vulnerabilities might be used to define attack signatures for the IDS database.
- *Complementary IDS*—a comprehensive IDS solution for any environment must include both host-based and network-based sensors. Often these are combined in a single product, but where a vendor offers separate NIDS and HIDS products, these should interface to a common management console or network management system. (Similarly, if a vendor offers only a NIDS or a HIDS, it should interoperate with other vendors’ complementary products.)

Event Management

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

- *Event prioritization*—to 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 minor.

- *Report merging and data visualization*—an IDS should be able to:
  - provide a single view of events (potential attacks) across the whole enterprise;
  - present the data in a way that allows a user to understand what has occurred, how to respond to it, and how it can be prevented in the future.
- *Event trace and replay*—an IDS should save enough information to be able to reconstruct any event in full.
- *24*×7 vendor hotline—the IDS vendor should be able to provide the organization with expert advice to properly respond to attacks.
- *Attack database*—the IDS vendor should provide a database that includes attack information and analysis, details vulnerability fixes, and suggests possible countermeasures.

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. Critical support factors include:

- *Product information*—Readily available and comprehensive (accurate, complete, and up to date) and comprehensible information about it.
- *Vendor response*—A workable means by which to query the vendor, coupled with a responsive vendor.
- *Attack definition update*—A comprehensive a set of attack signatures, etc., which is updated frequently (e.g., signatures provided immediately upon identification of a new attack) in a simple way (e.g., automatic, secure downloads from a vendor site).

Technology Leaders

The IDS research field is still comparatively young, with most research dating from the 1980s and 1990s, and wide-scale commercial use from the mid-1990s. However, the intrusion-detection market has grown into a significant commercial presence. Gartner Research reported a 73 percent growth in the $153 million IDS software market in 2000. The leader by market share is Internet Security Systems (ISS) with 47 percent. The second largest is Computer Associates with 29 percent. Symantec and Network Associates also have IDS offerings, although they currently have little share and are seeing low growth. (Cisco is not represented in these figures as it offers a *hardware*-based IDS.)

Table 5: Leading IDS Products

Vendor/Product(s)	Description
Cisco Systems, Inc. • Secure IDS (formerly NetRanger) • IDS Host Sensor (Internet: www.cisco.com)	Secure IDS is a NIDS appliance that can also be implemented as software on Cisco's PIX Firewall and Internet Operating System (IOS) routers and as a "blade" in Cisco's switches. Cisco has a strong position in the IDS market because of its presence in the network infrastructure of a majority of organizations. Cisco is winning customers for its IDS, in part through competitive pricing and increased performance. An announced partnership to rebrand and resell Entercept Security Technologies' HIDS gives Cisco a comprehensive IDS solution. The challenge for Cisco will be to create a robust, easy-to-use, central management console that can correlate and report on incidents from host-based and network-based agents.

Table 5: Leading IDS Products

Vendor/Product(s)	Description
Enterasys Networks, Inc. • Dragon IDS (Internet: www.enterasys.com)	Dragon IDS comprises Dragon Sensor (NIDS) and Dragon Squire (HIDS) with a common Dragon Server console. Dragon Squire monitors host platforms, applications, firewalls, and other vendors' NIDSs and HIDSs. After its acquisition of Network Security Wizards, Enterasys has integrated Dragon IDS into a comprehensive set of tools that works well with its line of hardware (enterprise switches). Channel relationships with ISPs and MSSPs, such as Verio and Riptech, indicate wide acceptance of Dragon for IDS.
Internet Systems Security, Inc. (ISS) • Real Secure IDS (Internet: www.iss.net)	RealSecure integrates RealSecure Network Sensors (NIDS) and RealSecure Server Sensors (HIDS) with a common RealSecure Manager console. RealSecure IDS was struggling to keep up with the throughput demands being placed on it by the advancing needs of e-businesses. ISS made a strategic acquisition of NetworkICE, whose NIDS appliance will get RealSecure to gigabit wire speed analysis by 1Q02.
Snort • Snort (Internet: www.snort.org)	Snort is a lightweight, fast NIDS, available under a GNU General Public License. Snort is the leading open-source NIDS and ranks highly in comparison with commercial NIDS products, and higher than any commercial product in signature coverage. The rapid evolution of the rulesets is an important advantage of an open-source system, where a large community can create new rules promptly. In some cases, a Snort rule is posted to BugTraq with the original vulnerability report. Additionally, Snort also allows plug-ins: ways to incorporate additional detection functionality into the system. Snort has been making growing inroads into the marketplace, but many organizations will have been reluctant to adopt it because of the lack of commercial support. Silicon Defense (Internet: www.silicondefense.com), however, announced in March 2001 that it would begin providing commercial support contracts for organizations using Snort and looking for professional support.
Symantec Corp. • Intruder Alert • NetProwler (Internet: www.symantec.com)	Intruder Alert is Symantec's HIDS and NetProwler its NIDS. Symantec added both products to its portfolio with its acquisition of AXENT Technologies in December 2000. AXENT originated Intruder Alert in 1996 and added NetProwler by acquisition. Symantec is in a good position with Intruder Alert and NetProwler in both areas of IDS, but has so far provided only limited interoperability.
Tripwire, Inc. • Tripwire for Servers • Tripwire for Web Pages • Tripwire for Routers and Switches (Internet: www.tripwire.com) • Tripwire Open Source for Linux (Internet: www.tripwire.org)	Tripwire for Servers is the leading FIA product for MS Windows and Unix operating systems (including FreeBSD and Linux). Tripwire Manager is a cross-platform management console for managing up to 2,500 Tripwire installations. Tripwire for Routers and Switches checks Cisco router and switch configuration. Tripwire for Web Pages extends Tripwire protection to Web pages running on Apache Web servers. While Tripwire is unlikely to be an organization's only IDS product, it should consider a FIA product as part of a comprehensive intrusion-detection implementation. An open source, stand-alone version of Tripwire for Linux servers is only available as a free download.

Other Vendors

- Computer Associates International, Inc.—eTrust Intrusion Detection (NIDS) and eTrust Audit (a consolidated audit management product). (Internet: www.ca.com)
- Entercept Security Technologies (formerly ClickNet)—Entercept (HIDS), also offered by Cisco as IDS Host Sensor, and Entercept Web Server Edition (WSE). (Internet: www.entercept.com)
- Intrusion Inc.—SecureNet Pro software and SecureNet appliances (NIDS). (Internet: www.intrusion.com)
- Lancope, Inc.—StealthWatch appliance (NIDS). (Internet: www.lancope.com)
- NFR Security, Inc.—NFR Network Intrusion Detection (NFR NID) and NFR Host Intrusion Detection (HID). NFR HID is based on Centrax technology that NFR recently (December 2001) acquired from CyberSafe Corp. (Internet: www.nfr.com)
- NIKSUN, Inc.—NetDetector (NIDS). (Internet: www.niksun.com)
- Raytheon Company—SilentRunner (NIDS). (Internet: www.raytheon.com)
- Recourse Technologies, Inc.—ManHunt (NIDS). (Internet: www.recourse.com)

HIDS for IBM z/OS and OS/390

None of these IDS vendors offers a HIDS product for IBM zSeries eServer hosts (mainframes). A number of specialist vendors do offer batch-mode System Management Function (SMF) audit log analysis tools:

- BETA Systems Software AG—BETA 89 Automated Security Auditor for OS/390. (Internet: www.betasystems.com)
- CONSUL Risk Management b.v.—Consul/zAudit for RACF, Consul/zAudit for ACF2. (Internet: www.consul.com)
- Eberhard Klemens Co. (EKC), Inc.—EKC Security Reporting Facility (ESR-F), for both CA eTrust CA-ACF2 and RACF. (Internet: www.ekcinc.com)
- Vanguard Integrity Professionals—Vanguard Advisor. (Internet: www.go2vanguard.com)

Of these, BETA and Vanguard now offer real-time alerting, with CONSUL developing this functionality.

Super-IDS Products

A number of vendors offer products that consolidate information from IDS products and other sources (firewalls, routers, OSes, etc.), present it to a unified monitoring console, and analyze and correlate events across the organization's infrastructure. Some vendors brand these products as *threat management* solutions.

Vendors offering such products include:

- Advisor Technologies, Inc.—Security Advisor. (Internet: www.advisortechnologies.com)
- e-Security, Inc.—e-Sentinel. (Internet. www.esecurityinc.com)
- GuardedNet—NeuSecure. (Internet: www.guarded.net)
- IBM/Tivoli Software—Tivoli Risk Manager and Tivoli Intrusion Manager. (Internet: www.tivoli.com)
- Intellitactics Inc.—Network Security Manager (NSM). (Internet: www.intellitactics.com)

- netForensics, Inc.—Security Information Management (SIM). (Internet: www.netforensics.com)

Future Trends

Commercial IDSs are still in their formative years. Some commercial IDSs have received negative publicity due to their large number of false alarms, awkward control and reporting interfaces, overwhelming numbers of attack reports, lack of scalability, and lack of integration with enterprise network management systems. However, the strong commercial demand for IDSs will increase the likelihood that vendors will successfully address these problems in the near future.

It is very likely that certain IDS capabilities will become core capabilities of network infrastructure (such as routers, bridges, and switches) and operating systems. In this case, the IDS vendors will be able to better focus their attention on resolving some of the pressing issues associated with the scalability and manageability of IDS products.

Other trends in computing will affect the form and function of IDS products including the move to appliance-based IDSs. It is also likely that certain IDS pattern-matching capabilities will move to hardware in order to increase bandwidth.

Technology Alternatives

Consolidated Audit Management (CAM) Products

A number of vendors offer products that gather, normalize, and analyze event and audit data from multiple platforms. While some of these include a real-time HIDS component, the main benefit of these products is not prompt response to attack. By securely aggregating all data, and evaluating them consistently against a “universal” policy, these products allow:

- Identification of suspicious activity—rather as a batch-mode HIDS.
- Reporting of legitimate but high impact activity—e.g., a system administrator changing the configuration of the trusted computing base (TCB).
- Data mining—e.g., to track the activity of a single person across multiple systems.
- Trend analysis—to discover patterns of events that are innocuous if unrepeated but suspicious over an extended period.
- Statistical analysis—to discover security “hot spots” in the organization’s infrastructure.
- Archiving of audit data—for future forensic use, as evidence in any litigation that might follow an attack.

Vendors offering CAM products include:

- Computer Associates International, Inc.—*e*Trust Audit. (Internet: www.ca.com)
- CONSUL Risk Management b.v.—Consul/eAudit. (Internet: www.consul.com)

These products are an alternative to dedicated real-time HIDS products, but offer limited or no real-time responses and poor interoperability with NIDS products and management consoles.

Managed Security Monitoring (MSM)

An IDS is only a tool. To get benefit from it, an organization needs people—people who can analyze alerts and detect real attacks, and people who know how to respond to attacks. Considerable expertise and continuous vigilance are required to detect all attacks and to respond effectively to them. Few enterprises can recruit, train, and retain enough people with the necessary expertise.

Most MSM offerings leverage the organization's investment in IDSs and other security technology; some use vendor-specific NIDS devices. They use a combination of sophisticated proprietary software and human expertise to detect attacks on the organization's networks and to respond to those attacks—typically by advising the organization's on-site technicians.

For about the cost of one security expert an MSM customer gets a team of security experts trained in attack recognition and diagnosis that monitors the organization's network 24×7. Nevertheless, the organization itself must be prepared to take prompt remedial action and properly follow up any security incident.

A number of vendors offer MSM services, most in combination with other managed security services:

- Activis (Internet: www.activis.com)
- Counterpane Internet Security, Inc. (Internet: www.counterpane.com)
- Internet Security Systems (ISS) (Internet: www.iss.net)
- Riptech, Inc. (Internet: www.riptech.com)
- SecureWorks, Inc. (Internet: www.secureworks.net)
- Ubizen, Inc. (Internet: www.ubizen.com)
- Veritect (Internet: www.veritect.com)
- Vigilinx, Inc. (Internet: www.vigilinx.com)

Other Complementary Products

A number of products are more widely recognized as complementing IDSs. These countermeasures each address a particular security threat to an organization's system—and each has weak and strong points. Only by combining them together with an IDS—*defense in depth*—does an organization protect from a realistic range of security attacks:

- *Firewalls* are widely used: a firewall is typically one of the first security mechanisms that an organization deploys to protect the perimeter of the network. In too many cases, it is the only such mechanism used. Although firewalls provide good protection against intrusions from external sources, like the Internet, organizations should realize that not all access to their enterprise infrastructure occurs through the firewall. For example, impatient employees might establish an unauthorized modem connection to the intranet. Similarly, organizations must understand that not all intrusions occur outside of the firewall. For example, some employees may accidentally or maliciously try to access files or systems.
- *Antivirus* products are a necessary defense against the damage that viruses and other malicious code can do. But the protection this offers is decreasing as virus writers and the viruses themselves get smarter and antivirus product vendors and organizations struggle to keep pace with antivirus updates.
- *Vulnerability assessment* (*VA*) products (also known as *vulnerability scanning* or sometimes, wrongly, as *risk assessment* products) scan for security flaws that may leave a computer system or network open to attack. VA products can be thought of as a kind of IDS—they are essentially batch mode

misuse detectors that operate on system state information and results of specified test routines. VA is a very powerful security technique, but is complementary to IDS, not a replacement for it. VA products can reliably generate a "snapshot" of the security state of a system at a particular time and enable a security manager to audit computer systems and networks for compliance with a particular system security policy. Furthermore, some IDSs can make use of VA results to tune the analysis; prioritizing attacks where the vulnerability it exploits is known to exist; deprioritizing attacks where the vulnerability it exploits has been handled.

- *Honey pots*. A honey pot is a computer system that is expressly set up to attract and "trap" attackers. To set up a honey pot, an organization can:
    - Install the operating system without patches installed and using typical defaults and options
    - Make sure that there is no data on the system that cannot safely be destroyed
    - Add the application that is designed to record the activities of the invader

Maintaining a honey pot requires a considerable amount of attention and may offer as its highest value nothing more than a learning experience—that is, the organization may not catch any attackers. A honey pot is probably the last defense-in-depth component that an organization should consider.

Insight

IDS technology has improved dramatically over time. Initially developed to automate tedious and difficult log parsing activity, IDS products have developed into sophisticated applications with the ability to monitor network traffic and host audit logs to expose malicious activity. But, like a firewall, an IDS is not itself a complete security solution. Network-based and host-based IDSs must be used along with complementary countermeasures—firewalls, antivirus software, vulnerability assessment products, etc.—as a component of defense in depth. IDSs will soon be seen as an indispensable and integral component of any comprehensive security program and will likely become as ubiquitous as firewalls. Even so, while many attacks will be detected, some will be missed, and for every real attack, there will be more (probably many more) false alarms. IDS products will need the continuous attention of a staff of knowledgeable and skilled technicians to tune and customize the IDS and to investigate and respond to all alarms. Organizations lacking security staff, or having three or more IDS sensors, may benefit from managed security monitoring services to help them identify and investigate attacks. But any organization must have the capability and will to respond—otherwise an IDS is completely ineffective.