Global Information Assurance Certification Paper

Choosing an Intrusion Detection System that Best Suits your Organization

Dennis Mathew

September 16, 2002

Abstract

There is a wide variety of Intrusion Detection Systems currently available, from network based IDS' to host based IDS', commercial and freeware. Its difficult to determine exactly what best fits your organization. To establish what you should be using, as with anything else, is a process. If this is your first attempt at securing your organization it may take more time and effort than for one that has made security a priority over the years. The technology, however, is only as effective as the people and processes that support it. Security is not simply a technology, but a mindset that must pervade the organization.

Choosing an intrusion detections system (IDS) can be a complex and time consuming project. This is especially true if the organization does not have a corporate security program. It is important to note that an IDS is in no way an all inclusive security solution, but if implemented correctly it can assist in detecting unauthorized activity and alert personnel to take action in the event of a security breach. In the following pages I will delve into exactly what an IDS is. This includes the various types of IDS' on the market and approaches taken to detect intruders. I will also identify key steps an organization should undertake prior to implementing an IDS solution. Performing a risk assessment of your organization and understanding existing controls and control deficiencies is a key step in securing the organization. Implementing a tool such as this is most effective when there is a grounded understanding of the organization as a whole and the critical processes within the company. Additionally, the organization should invest time and money into developing their personnel to ensure they are appropriately equipped to utilize the tool in a manner that will make full use of the systems functionality. Finally I will take a look at various commercial IDS' on the market today and the ever-evolving functionality of this technology. Although freeware tools are a very real and practical alternative I will limit the scope of this paper to the commercial market.

II. What is an IDS?

Primary Purpose

A security breach occurs when an individual gains unauthorized access to your systems. This unauthorized access can be further divided into two primary categories, intrusions and misuse. Intrusions occur when the security breach originates from outside the organization whereas misuse is an attack that originates from the inside, i.e. employees, intruders, etc. This unauthorized access can be for something as critical as stealing proprietary data or as trivial as utilizing your systems to play resource intensive role-playing games. Intrusion Detection Systems (IDS) is a security monitoring system that will gather and analyze data from various areas within a system or network to identify/detect possible intrusions and/or misuse. Intrusion Detection Systems perform a wide array of functions, which include:

- Monitoring and analyzing both user and system activities,
- Analyzing system configurations and vulnerabilities,
- Assessing system and file integrity,
- Ability to recognize patterns of typical attacks,
- Analysis of abnormal activity patterns, and
- Tracking user policy violations.

The system can be a key asset in pinpointing where attacks are coming from and when they are

being made. It will also indicate the primary targets of the attack and the types of attacks being utilized. The IDS can be your eyes and ears into your system and/or network.

Network Intrusion Detection System

NIDS monitor the network wire and attempt to detect an attacker targeting company systems. An attacker may attempt to break into your system or may cause a denial of service attack. NIDS utilize raw network packets as its data source. A basic example of a monitoring technique is a system monitoring TCP connection requests (SYN) to a wide range of ports on a target machine to determine if someone is attempting a port scan. A NIDS can run on a host machine, monitoring all traffic to that machine or on an independent machine, promiscuously monitoring network traffic. The system can be configured to analyze traffic passing through a network segment to pinpoint patterns and trends that may be indicative of an attack. These systems provide near real-time event monitoring to a centralized console.

NIDS, in general, are less expensive than their host-based counterparts, but are very different in nature. The NID sensors generally will not monitor or identify activity at the host level.

Host-based Intrusion Detection System

Host-based IDS (HIDS) typically monitor event, and security logs at the operating system level. When any of these critical files change, the IDS compares the new log entry with attack signatures to see if there is a match. If there is a match, the system will respond with various types of administrator alerts to initiate incident response procedures. Some also monitor activity and issue alerts if specific ports are being accessesed. This technology continues to develop, but managing HIDS' have become simpler than the past. Agents can be installed on multiple hosts and monitored from a central console. HIDS can be critical in determining whether or not an attack was successful. The HID data can also be used should legal matters arise and the altering of data needs to verified.

Commercial IDS' on the market

There are an array of Intrusion detection systems on the market as this space continues to grow. Free ware tools have been known to be very effective and if configured and managed properly are powerful tools. Since it would be difficult to discuss both free and commercial tools in the limited size of this project I will focus my attention on the commercial tools. Some of the leaders in this space are listed below:

Network Based IDS	**Host Based IDS**
Internet Security Systems Real Secure	Internet Security Systems Real Secure
Network Security Wizards Dragon IDS	Symantec Intruder Alert
Symantec Net Prowler	Cyber Safe Centrax
Cisco Systems Net Ranger	Tripwire
Network Flight Recorder Intrusion Detection Appliance	
Network Ice Black Ice Defender	
CyberSafe Centrax	

Approaches to Intrusion Detection

There are multiple approaches taken to perform intrusion detection. The primary methods are rule-based intrusion detection (RBID) and statistical-based intrusion detection (SBID).

Statistical-Based Intrusion Detection (SBID)

SBID systems will attempt to identify security violations by systematically analyzing audit trail data. The system will compare log activity with typical or predicted attack profiles. This

eliminates the need to manually sift through log files to try and identify unusual network traffic or system activity. The system automates this process and will perform this analysis in a structured manner. For this analysis to be effective there must be a preexisting classification of system or user activity that is considered to be normal. This characterization is usually called a profile. This profile is based on a series of events found in system audit data and can be used to configure expected behavior. User profiles can be customized to each user and are maintained dynamically. This allows the user's profile to change as the user's behavior changes. Administrators should be able to review these profiles to ensure that they make sense for their organization. This method of using profiles is not used by RBID's. Statistically significant deviations above the predefined profile are considered intrusion attempts.

Rule-Based Intrusion Detection (RBID)

RBID systems are considered expert systems that will analyze extensive log files to differentiate between intrusive and normal day-to-day behavior. The system is centered on the assumption that it is possible to identify intrusion attempts based on a specific sequence of user activity that typically resembles activities that lead to system compromises. RBID expert system properties will initiate pre-defined rule sets when log data and system files indicate what appears to be unauthorized activity. These rule sets will attempt to compare patterns in audit data to patterns customarily seen during a penetration attempt. Systems can be configured to alert specified individuals if a penetration is in process or has occurred. The systems can provide details surrounding the alert as well as user specific information of the suspected intruder.

There are two primary types of RBID systems, state based and model based. The state based approach will code the rule base with terminology or wording found in the audit trails. Intrusions are defined by sequences in system state, the system will systematically analyze the states the system takes on. These system states are defined by audit trail information. The system is initially considered to be in a limited access state and, if compromised, is then considered to be in a final compromised state. The model based approach uses known intrusion attempts and models them as sequences of user behavior. These events are then modeled and matched to an event in an audit trail or log file. The IDS will determine how user behavior translates into the audit trail.

III. Organizational Steps Prior to Making a Decision

Performing a Risk Assessment of Your Organization

Prior to implementing an effective security-monitoring program, which can include the utilization of an IDS, a systematic risk assessment of your organization should be completed. This will assist management personnel in gaining a comprehensive understanding of the organization, the IT environment and the potential risks involved.

Risk is inherent within any organization and industry. The first step is understanding the risk unique to your environment. Risk varies from industry to industry, i.e. the risks associated with a banking institution vary from that of an automobile parts manufacturer. Information is widely available on the internet, in the news, etc. as to who and what have been targets of hackers in recent days and weeks. It is difficult, however, to ascertain an accurate picture of who has or has not been hacked because most companies that have been compromised are not always ready to divulge that information.

In any event, just because your industry is obscure or your company is low profile does not mean you are out of the woods. Most hackers are not targeting specific companies or industries, but are simply scanning the internet for vulnerable systems. An FBI study revealed that there are approximately 4000 denial of service attacks each week. The overwhelming majority of these attacks are neither publicized in the media nor prosecuted in courts. Of the survey respondents 90% said they have detected computer security breaches in the last 12 months. This puts most everyone at some level of risk.

Before completing this assessment there needs to be a sound understanding of what exactly falls

into the category of a risk. Risk is defined as the potential for harm or loss. This is best addressed in the context of these four questions:

- What could happen? (What is the threat?)
- How bad could it be? (What is the impact or consequence?)
- How often might it happen? (What is the frequency?)
- How certain are the answers to the first three questions? (What is the degree of confidence?)

Completing a risk assessment can often times be a complex and subjective process. A primary objective of the security risk assessment should be to build the foundation of this process on objectivity and not subjectivity. There are a number of approaches that are utilized to perform a risk analysis; I will discuss two that are the benchmarks and an additional methodology that has been gaining popularity.

Quantitative Analysis

This approach factors together two primary elements: the probability of an event occurring and the likely loss should it occur. These two elements are multiplied together to produce the 'annual loss expectancy', the basis for this analysis. This equation allows us to theoretically rank events in order of risk and come to "sound" conclusions. There are some fundamental problems with this approach; one being unreliable and inaccurate data. Probabilities are difficult to quantify into an exact science and are seldom precise. Additionally, multiple interrelated events and potential existing controls that may be in place complicate the equation and are difficult to factor in. Given the uncertainties involved, the numbers can at least be a general guideline to be used and the exercise of developing this analysis will allow personnel consider critical assets and possible events.

Qualitative Analysis

This is the most widely utilized risk analysis methodology. In this approach the organization will use estimated potential loss and not incorporate probability. This methodology will use a number of elements, including the following:

- Threats;
- Vulnerabilities; and
- Controls.

Threats are defined as things that can or may go wrong with the system or attack the system. Threats are constantly present for every component of your network architecture; fires, hackers, viruses, theft, are examples of threats. Threats are essentially the vehicle by which a vulnerability may be exploited. Vulnerabilities make a system more prone to attack or more likely to be compromised if attacked i.e. a laptop that is not secured is more likely to be stolen than one that is chained to the desk.

Controls are countermeasures to vulnerabilities and can reduce risk levels substantially if implemented appropriately. Controls can be subdivided into three primary categories: pervasive, specific, and monitoring controls. Pervasive controls are controls that facilitate reducing risk (such as unauthorized access) over the span of a process, i.e. strong passwords that will assist in protecting an AP system. Specific controls are controls that will facilitate reducing risk within the process, i.e. field checks that will only allow data of a specified format to be entered into the AP system. Finally there are monitoring controls; these controls are usually reports and reviews that are done to ensure specific and pervasive controls are working appropriately. Controls can either be preventative or detective. Preventative controls, such as NIDS will provide alerts prior to an

incident occurring, detective controls such as file integrity checking will alert you of an incident once it has occurred. A combination of these controls will greatly reduce risk within the organization.

Octave Analysis

Another methodology used to perform an organizational security risk analysis is the Octave method developed by Carnegie Mellon University. This method utilizes a three-phased approach. The first phase consists of building asset based threat profiles. The organization must identify the most critical assets to the organization and what is currently being done to protect those assets. To do this effectively discussions must be held with senior management, operational management and staff level personnel. Once this data has been compiled it can be analyzed to select critical assets, set security parameters around those assets and begin identifying potential vulnerabilities. The next phase will analyze key information infrastructure to identify technology vulnerabilities that can lead to unauthorized activity on critical assets. This will include analyzing key systems and components for technology related weaknesses. At this point vulnerability tools are utilized (software tools, scripts, etc.) to systematically identify potential security holes that may adversely affect the organization's IT environment. During the last phase of this approach the organization can now identify key risks to the organization's critical assets and decide what mitigation activities should be utilized to effectively protect these areas.

Whichever method your organization decides to utilize the key is ensuring a structured approach is used throughout the risk assessment process. This will allow management and IT personnel to gain a clear understanding of the company's environment, critical infrastructure, and critical data. This will also focus security efforts around key areas and divert attention away from non-essential data and infrastructure. This will allow the implementation of an IDS solution to be immensely more effective than simply purchasing and implementing a tool in and ad hoc manner.

Organizational Requirements

As with all other IT related initiatives there must be buy in and support from top-level management for a company's security initiative to be successful. At the time of deployment management must understand, in at least at a high level, the threat of hackers and their ever increasing advanced methodologies utilized to compromise company systems. This will spur support for funding to acquire necessary tools and to implement appropriate methodologies, but in addition to funding there must be an investment in time and effort to develop associated policies and procedures around the ongoing usage and maintenance of the IDS. Once the tool is deployed, if it is not properly monitored and maintained, it will lull the company into a false sense of security. If security has not been a priority in the past a change in corporate culture will be required in addition to the implementation of the IDS to facilitate securing the organization.

A person or persons will need to be properly trained in configuring and maintaining the IDS to ensure optimal and successful usage. Training should include understanding potential threats and common attacks; these threats may originate externally or internally. An emphasis should be placed on monitoring both areas of threat to obtain maximum coverage. In addition to initial configuration, attack signature updates will need to be performed on a regular basis to detect new vulnerabilities. The individual will need to be diligent in identifying new vulnerabilities and attacks that may be a threat to their organization. They will also be required to tune the IDS properly to appropriately classify the severity of alert events and eliminate false positives.

Understanding Your Technical Environment

Throughout the Risk Assessment process a thorough understanding of your organizations technical environment should be attained to ensure all critical assets are being secured. This is especially necessary prior to implementing an IDS solution. This is the only way to strategically place IDS sensors in such a way that paths into the organization and critical assets are being monitored. If all access points are not identified, one weak link could jeopardize the entire

effort. A rogue modem, wireless access point, old web or email server, etc. could be the weak link in the perimeter defense. This process will also identify critical hosts that would require monitoring at a host level. This will allow the company to focus its time and resources on the appropriate systems.

Audit tools are now available that can survey an organizations environment and identify technical infrastructure. Commercial tools as well as freeware tools will crawl the network to identify servers, workstations, routers, etc, basically anything with an IP address. This is a vital asset in large organizations or in companies with technically savvy users who have installed systems and equipment on their own. Identifying rogue modems is also a key step in securing the organization. Companies should analyze their switches to determine if any lines have been configured as analog lines and if so why. The use of analog lines should be well controlled because this could be a hole into the organization that circumvents all other security efforts if not properly monitored and controlled. Companies may also want to consider utilizing war-dialing techniques, on an annual or bi-annual basis, against the organizations block of assigned numbers to identify any analog carriers.

Cost-Benefit Analysis

Before deciding on exactly which IDS the company should acquire the organization should perform a cost/benefit analysis. Cost is a very real and important factor in the decision making process of all management personnel. Someone is always worried about answering to someone else as to exactly why funds were allocated in the way they were. This analysis can be performed effectively once the organizations risk analysis has been performed. This risk analysis will give the organization a very real sense of the costs associated with down time, data corruption, data theft, and loss of reputation. A financial institution has a heavy cost associated with being compromised by a hacker, whereas a small manufacturing firm may not deal with the same types of costs and issues.

There are many CBA methodologies that can be used; I will discuss one that puts some structure behind the process. The analysis may be performed by one person, but should include the input of many from the organization. Individuals familiar with IT systems development and operation, budget, finance, statistics, procurement, and IT architecture should be included. The process should determine and define objectives for the IDS initiative. This will clearly communicate to management the thought process behind implementing a solution such as this and how it relates to the company. Identify and quantify any future considerations that may be required. For an IDS system this will be limited to upgrades, maintenance, etc. From here cost data should be compiled. Several sources of data are historical organization experience, current system costs, market research, publications, analyst judgment, and special studies. Multiple alternatives should then be sought out. The search can be narrowed at a future time, but it is essential that management feels that they are being presented with the full picture. At this point there should be an estimate of all costs associated with this project. There should be an understanding of equipment costs as well as time and resources costs, direct and indirect costs, etc. This will hopefully take all cost factors into consideration. At this point the benefits associated with an IDS should also be examined. Benefits such as increased security, the ability to respond to unauthorized activity, the ability to prevent reputation defamation are all critical factors to consider. This cost benefit analysis will help make the process of deciding whether or not to implement an IDS and which IDS to choose a more straightforward decision.

IV. Choices, Choices, Choices….

Choosing the Right IDS

Before choosing an IDS it is important to realize that this is not the answer to all of your security issues. It is simply a piece of the overall security solution. For a security initiative to be truly effective there needs to be a movement to alter organizational culture. The policies, and associated tools are only as effective as the people utilizing them. With this being said there are a number of IDS' to choose from that may suit your needs. Once the risk assessment has been

performed and a clear understanding of the organizations risks, critical data, network infrastructure, etc. has been attained the IDS selection process can begin. A combination of host-based and network based IDS systems will provide the optimal coverage, but again that decision is based on the risk assessment and cost benefit analysis performed for your organization.

Network/Host Based blends:

1. ISS was one of the first companies to release a commercial intrusion detection system and their network intrusion detection system, RealSecure, is still considered to be the standard by many security professionals. Real Secure consists of the following components, the workgroup manager, the console, the network sensor and the OS sensor. The network sensor is considered the network intrusion detection piece of the tool and the OS sensor is considered to be the host-based intrusion detection piece of the tool. A single console can monitor multiple sensors and a sensor can report back to multiple consoles. In the 2nd scenario only one console is granted master status and has the capability to adjust sensor settings. There are multiple policies that are pre-defined that come with the system, but the system administrator must take some time to consider the level of coverage required for the organization. Policies that provide 'maximum coverage' may employ an excessive amount of resources. Defining custom policies is a very straightforward process; you can simply rename and customize existing policies to provide you with a starting point. For various events that are flagged there are a number of responses that can be defined, i.e. log, send email, kill session, view session, etc. You have the option of viewing alerts on a real-time basis or after they have been logged. Once activity has been logged reports can be generated in text and in graphical format.

2. Cybersafe Centrax provides many solutions in one package. Centrax has host-based capabilities, network-based capabilities, and basic vulnerability assessment capabilities. The tool is particularly strong in the host based area as well as its audit policy management across the entire enterprise. The centralized management console is an added bonus to the product that allows you to define security policy, control target agents, as well as monitor and respond to real-time results and perform high-level vulnerability assessments. The console consists of three parts, the GUI, the collection engine and the detection engine. The GUI is used to manage the Command Console and communicate with clients, the collection engine receives all files from the target agents and forwards them to the detection engine and the detection engine analyzes audit data, populates the database and archives the original audit data. Centrax sets itself apart by having a wide range of Target Agents available including host-based and network-based agents.

Network Based Options

1. Dragon Senor is a packet-based network intrusion detection system that resides on UNIX. The system is command-line or GUI managed and can reside on Linux; a low cost platform that is also supported by Dragon. The attack signatures available within Dragon are comprehensive and have the capabilities of identifying unique data patterns in network traffic that facilitate the identification of network attacks, misuse, vulnerabilities, etc. These signatures can be easily modified and additional signatures can be created and implemented. Dragon does not exclusively use pre-defined signatures, but can also detect protocol violations; this includes port scans, ports sweeps, suspicious fragmentation, etc. Dragon will terminate suspected sessions and emit false responses to confuse potential attackers.

2. Cisco Secure IDS (formerly known as NetRanger) is known for being an easy to implement system. It is a dedicated network appliance that is supplied with all the hardware and software necessary to be operational quickly and easily. There are three variations to choose from depending on the complexity of your network environment and

your security needs. Management on the appliance can be performed over one of the network interfaces; the other network interface is used solely for network sniffing on the live network to be monitored. Sensors can be deployed strategically around the network depending on where critical data and resources are located. These sensors can be managed centrally with the Windows based Cisco Secure Policy Manager (CSPM). CSPM is extremely straightforward which makes it very easy to configure security policies. It is possible to customize each sensor and indicate which security policy to be used, how addresses are blocked, whether event log files should be generated, etc. Reporting capabilities are limited and are still reliant on partners such as netForensics for more in depth reporting.

3. NetProwler is the network IDS in Symantec's suite of tools. The tool utilizes a similar architecture to Intruder Alert in that it also has an Agent, a Manager and a Console. The console is divided into two primary areas, configure and monitor. The configure module allows users to configure Managers, add and manage Agents, and define security policies and actions to be taken when there are alerts. The user interface is a drawback, it is confusing and fairly complicated. The tool, however, is powerful and flexible, which may be what makes the interface so confusing. The engine does not monitor everything coming across the wire, the agents are assigned one or more IP addresses to be monitored. Attack signatures are assigned to various IPs depending on the host operating system. Configuration appears to be a bit complex, but is facilitated by the automated configuration tool called the Profiler. It scans the network for live systems and identifies the hosts' operating system and the services that are running on them. Network attacks can be monitored on a real-time basis and provides in depth real-time statistics. Additionally, a wide range of reports can be produced via the Crystal reports engine. However, reporting is not a strength of this product , no ad hoc reporting capabilities are available and is limited on the number of records that may be reported upon.

Host Based Options

1. Intruder Alert is a host based IDS that is designed to complement NetProwler, both of which are in the Symantec suite of IDS solutions. Both can be configured to work together and can be monitored by a central console. Agents are installed on the host to be protected; the hosts will report back to one or more Managers. Managers are controlled by a central administrator component and events are viewed via the event viewer. GUI interfaces are available for both the Viewer and the Administrator. The Administrator is utilized to define and implement security policies throughout the ITA system. The policy library contains a number of predefined security policies; policies can also be customized by the organization. Many rules and clauses can be combined to create a policy, these rules can also be combined together. These policies can be pushed out to Agents in various domains with a few clicks. ITA comes with extensive reporting capabilities and can be customized depending on user requirements.

2. Tripwire is a variant of host-based IDS'; this product focuses on file integrity checking. Tripwire creates a database of critical system files; it is essentially a snapshot of a system in a known secure state. You can specify the directories and files that should be monitored and properties associated with each. Properties such as last write time, file size, access permissions, etc. can be stored in the database. You can now compare the state of these systems at any given time with what has been stored in the database. If there are changes in these properties and they are authorized then the database can be updated, if they are not authorized incident response actions can be initiated. Tripwire now includes a Manager that can control agents that are installed on multiple hosts. Policies and schedule files can be deployed to all machines from the Tripwire manager.

V. Conclusion

The products mentioned above are just a few of the numerous options currently available on the

market. In addition to these there are a number of freeware tools that are also effective if implemented and maintained appropriately. This will at least provide a flavor for the different options available. The process of choosing an IDS solution can be extensive, but if it is done properly it will facilitate the process of securing your organization. The steps outlined here may appear to be simple exercises, but are actually critical steps to attaining a successful IDS implementation. At the end of the day only the organization itself should determine what is best for them, but it is better to make a well-informed decision based on facts rather than simply guessing or listening to the suggestions of others. A comprehensive understanding of the risks facing the organization, the organizational adjustments that will need to be made and the various IDS options available should be attained for the organization to formulate a decision. This will allow the company to determine the optimal value for the money being spent and move forward in securing the organization. The IDS will not be the answer to all of the organizations security issues, but can be an integral part in appropriately securing the organization. The IDS along with strong organizational policies and procedures, securely configured routers and firewalls, periodic vulnerability assessments, etc. can greatly reduce the level or risk the organization faces.

VI. Appendix A - References

1. Office of The Deputy Chief Information Officer October. "Cost-Benefit Analysis Guide For NIH IT Projects." May 1999. http://wwwoirm.nih.gov/itmra/cbaguide.html#2 (August 2002).

2. Walder, Bob. "Intrusion Detection Systems" Group Test. Edition 3. July 2002. http://www.nss.co.uk/ids/edition3/index.htm (August 2002).

3. "Introduction to Security Risk Analysis." http://www.security-risk-analysis.com/introduction.htm (August 2002).

4. Meinel, Carolyn. "The ABCs of IDSs." http://messageq.ebizq.net/security/meinel_2.html (September 2002).

5. Alberts, Christopher. Dorofee, Audrey. "Volume 1: Introduction." Octave Method Implementation. Version 2.0. June 2001. http://www.cert.org/octave/omig/Volume_01_Introduction_v2.1.pdf (August 2002).

6. Gerken, Mark. "Intrusion Detection." 10 Jan 97. http://www.sei.cmu.edu/str/descriptions/intrusion.html (September 2002).

7. McHugh, John. Christie, Alan. Allen, Julia. "Defending Yourself: The Role of Intrusion Detection Systems." October 2000. http://www.computer.org/software/so2000/pdf/s5042.pdf (September 2002).

8. Graham, Robert. "FAQ: Network Intrusion Detection Systems." Version 0.8.3. March 21, 2000. http://www.robertgraham.com/pubs/network-intrusion-detection.html#1.1 (September 2002).

9. Walder, Bob. Parkhouse, Jayne. "UNEARTHING THE INVADERS." July 2001. http://www.scmagazine.com/scmagazine/2001_07/testc/prod1.html (August 2002)