Global Information Assurance Certification Paper

Daniel K. Chandler

Planning Concerns, Considerations, and Tips for IDS in Federal IT Systems

As of: March 30, 2001

Introduction: Increasing network connectivity coupled with the growing reliance of the Federal Government on information technology (IT) systems has created a requirement for government agencies to be able to monitor, detect, and respond to various types of activities occurring in their IT systems. One security control that is being utilized to meet this requirement is intrusion detection.

Intrusion detection is needed in today's IT environment because it is impossible to keep pace with current and potential threats and vulnerabilities in IT systems. The IT environment is constantly evolving and changing, fueled by new technology and the Internet. To make matters worse, threats and vulnerabilities in this environment are also constantly evolving. Every new technology, product, or system brings with it a new generation of bugs and unintended conflicts or flaws. Additionally, the potential impacts from exploiting these vulnerabilities are constantly evolving. In a worst-case scenario, an intrusion may cause production downtime, sabotage of critical information, theft of confidential information, cash, or other assets, or even negative public relations.

This paper provides planning concerns, considerations, and tips for the installation, implementation, and deployment of intrusion detection systems (IDS) in Federal IT systems. The Federal IT environment is very unique and different from the commercial IT environment. The Federal IT environment utilizes a security compliance model where the IT system must comply with a set of prescribed security requirements. The commercial IT environment utilizes a security model based upon due diligence, industry best practices, and business case analysis. The Federal IT environment is divided into two separate entitities: IT systems processing "sensitive information" and IT systems processing "National Security Information." Only commercial or private sector industries such as the stock market, which has to comply with Federal regulations issued by the Securities Exchange Commission (SEC), face the same division. To provide some understanding of the Federal IT environment, the first portion of this paper relies on security policy published by OMB and NIST for sensitive IT systems. The second portion of the paper contains planning considerations and tips gained through personal experience over five years of assisting various Federal agencies with IDS projects and over 25 years as a military, federal, and private industry security specialist.

> The National Institute of Standards and Technology (NIST) defines intrusion detection is the process of monitoring the events occurring in an IT system and analyzing them for signs of intrusions. These intrusions are defined as attempts to compromise confidentiality, integrity, or availability, or to bypass the security mechanisms of an IT system. These intrusions are caused by attackers accessing systems from the Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them.[1]

These intrusions can be broken down into two main types. Misuse intrusions, well-defined attacks on known weak points of an IT system, can be detected by signature analysis or watching for certain actions being performed on certain objects. Anomaly intrusions, based on observations of deviations from normal IT system usage patterns, can be detected by pattern analysis or building up a profile of the IT system being monitored, and noting significant deviations from this profile. IDS offer significant detection and prevention capabilities against external attack and internal policy abuse.[2] Both signature analysis and pattern analysis are mainly based on passive packet capture utilizing some type of sniffer, breakdown of the packet according to some level of the OSI model, analysis of the packet to determine the load and the function, and reassembly of the packet. Intrusion detection can also function as a near real-time monitor for "honeypots" and passive traps. Honeypots are IT systems dedicated to deceiving hostile parties interested in a network. Passive traps use the "home field advantage" that network administrators enjoy for services available on their networks and for watching traffic headed for non-existent services. Packets being routed to these non-existent services may be an indication of port scanning, backdoors, or other hostile traffic.[3]

> IDS are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network and analyze them for signs of security problems.[4]

Based upon my experience, I have found that IDS are most easily broken up into up of three basic functional components: information sources, analysis, and response. The information sources are the sources of event information that the IDS draw upon such as firewalls, critical servers, routers, operating system, etc. The analysis component organizes and reviews the event information to see if an intrusion is taking place or has already taken place. The most common types of analysis approaches currently being used are misuse detection and anomaly detection. The response component implements a pre-defined set of actions once an intrusion has been detected based upon the type and severity of the intrusion. The IDS obtains event information from one or more information sources, performs a pre-configured analysis of the event data, and then generates specified responses, ranging from reports to active intervention when intrusions are detected.[5] The goal for deploying an IDS is to detect, identify, and monitor unauthorized use, misuse, and abuse of IT systems by both internal network users and external attackers.

IDS are tools that can assist in protecting Federal agencies from intrusion by expanding the options available to manage the risk from threats and vulnerabilities. Intrusion detection capabilities can help a Federal agency secure its information. The IDS can be used to detect an intruder, identify and stop the intruder, support investigations to find out how the intruder got in, and stop future intruders from exploiting the intrusion. The correction or patch can then be applied across the enterprise to all similar platforms.

IT Security Policy Base: The basic security requirements for Federal IT systems are contained in the Computer Security Act of 1987 (P.L. 100-235) and the Computer Fraud and Abuse Act of 1986 (P.L. 99-474). The Office of Management and Budget (OMB) implements the requirements contained in these laws for Federal IT systems processing unclassified information through OMB

Circular A-130, Management of Federal Information Resources, February 1996, which establishes general policy for the management of Federal IT systems. Appendix III of OMB Circular A-130 implements the basic requirements of these laws by specifically detailing the minimum set of IT security controls for Federal IT systems as well as security programs for all agencies and departments of the Executive Branch of the Federal Government. Currently, Appendix III does not require the deployment of an IDS as a required security control measure, but it does require that Federal agencies assure that each system appropriately uses effective security products and techniques, consistent with the standards and guidance from the NIST.[6]

> Further, NIST recommends that IDS be deployed as an industry best practice, noting: "As network attacks have increased in number and severity over the past few years, intrusion detection systems have become a necessary addition to the security infrastructure of most organizations."[7]

Even with published guidance and advice from OMB and NIST, it has been my experience that some Federal IT managers are hesitant to acquire and deploy IDS because of the potential impacts on network performance by the IDS, the expense of acquiring and implementing the IDS, and the resources required to support the effective operations of the IDS. However, there are compelling reasons to acquire and use IDS in Federal IT systems:

- To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system.
- To detect attacks and other security violations that are not prevented by other security measures.
- To detect and deal with the preambles to attacks.
- To document the existing threat to an organization.
- To act as quality control for security design and administration, especially of large and complex enterprises.
- To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.[8]

Federal agencies normally deploy IDS to detect malicious and inappropriate network activity directed towards and occurring within the protected perimeter of an IT system.

> NIST Special Publication 800-14 states, "If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection. Intrusions can be detected in real time or through the use of other kinds of warning flags/notices, by examining audit records as they are created or after the fact, by examining audit records in a batch process."[9]

Based upon my experience, near real-time IDS is targeted at unauthorized outsiders attempting to gain access to a Federal IT system, but IDS can also be used to detect changes in the Federal IT system's performance by integrating it with the enterprise management system. Also, IDS can be utilized for after-the-fact identification to indicate that unauthorized access was attempted or successful. Then IDS can be used to focusing follow-on activities on damage assessment or reviewing the security controls that were attacked.

IDS are necessary tools to assist in managing threats and vulnerabilities in a changing environment. The most common approaches to intrusion detection are anomaly detection and pattern-matching detection. Anomaly detection utilizes anomaly detectors to identify behavior on a network or host that is a departure from the norm. Pattern-matching detection utilizes misuse detectors to analyze system activity that match a pre-defined attack signature[10]. IDS that operate on a host to detect malicious activity on that host are called host-based IDS, and IDS that operate on network data flows are called network-based IDS. The following are characteristics of sound IDS:

- The IDS must run continually without human supervision.
- The IDS must be fault tolerant.
- The IDS must resist subversion.
- The IDS must impose minimal overhead on the IT system.
- The IDS must observe deviations from normal behavior.
- The IDS must be easily tailored to the system in question.
- The IDS must cope with changing system behavior over time as new applications are being added.
- The IDS must be difficult to fool.

The IDS must be able to identify and eliminate errors that occur in the system such as false positives, false negatives, or subversion errors. A false positive occurs when the IDS classifies an action as a possible intrusion when it is a legitimate action. A false negative occurs when an actual intrusive action has occurred but the IDS allow it to pass as non-intrusive behavior. A subversion error is defined as when an intruder modifies the operation of the IDS to force false negatives to occur.[11]

Host-based IDS: Host-based IDS operate on information collected from within an individual IT system and are becoming more widely used in Federal IT systems. Host-based IDS involves loading a piece or pieces of software on the system to be monitored. The loaded software uses

log files and/or the system's auditing agents as sources of data. Host-based IDS analyzes operating system and application system logs and events to compare system events against a database of known security violations and custom security policies. Also, the host-based IDS agent watches different aspects of the server security such as operating system logs files, access log files, as well as user-defined application policies. Host-based IDS involves not only looking at the communications traffic in and out of a single computer, but also checking the integrity of system files and watching for suspicious processes.

To get complete coverage at the site with host-based IDS, the software must be loaded on every computer. If a breach of policy occurs, the host-based IDS can react by logging the action, alerting the administrator, and in some cases stopping the action prior to execution. Host-based IDS falls into two basic categories: host wrappers/personal firewalls and manager/agent. Host wrappers or personal firewalls can be configured to look at all network packets, connection attempts, or login attempts to the monitored machine. This can also include dial-in attempts or other non-network related communication ports.

> A manager/agent host-based IDS application involves placing agents on each network host and on all, or a group of network devices throughout the enterprise. These agents are connected to managers, which in turn are connected to a central management console. Agents can remotely install/upgrade new versions and attack signature rules. This type of configuration allows security administrators to define or distribute the rules from one central location.[12]

In addition, host-based agents may be able to monitor accesses and changes to critical system files and changes in user privilege. Either approach is much more effective in detecting trusted-insider attacks than is network-based IDS, and both are relatively effective for detecting attacks from the outside. To ensure that the host-based IDS agents are performing as expected, each specific agent must be configured and tuned based upon the results of on-going traffic analysis for the location where it is installed. Also, policies and procedures must exist for how the host-based system is going to receive updated signatures. A recommended location for initial deployment of host-based IDS is on critical servers. "Once the operation of host-based IDS is routine, the Federal agency may consider installing host-based IDS on the majority of their hosts."[13] While working with Federal agencies, I have noted other reasons to consider host-based IDS, including:

- Verifying success or failure of an attack B host-based system uses logs containing events that provide early warning and verification whether an attack is successful or not.

- Monitoring specific system activities B host-based system monitors user and file access activity including file accesses, changes to file permissions, attempts to install new executables or access privileged service.

- Detecting attacks that network based systems miss B host-based system can detect

attacks from the keyboard of a critical server that do not cross the network.

- Well-suited for encrypted and switched environments B Since host-based system resides on various hosts throughout and enterprise, the system can overcome some of deployment challenge in switched and encrypted environments.

- Near-real-time detection and response B host-based system does not offer true real time response however it can come extremely close if implemented correctly.

- No additional hardware needed B host-based system resides on existing network including file servers, web servers, and other shared resources. As a result, it makes host based systems very cost effective.

Network-based IDS: Network-based IDS detect attacks by capturing and analyzing network packets and are the most common type of IDS currently being utilized within Federal IT systems. A network-based ID system monitors the traffic on its network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network traffic on other segments, and traffic on other means of communication cannot be monitored. Network-based IDS utilizes traffic analysis to compare session data against a known database of popular operating system and application attack signatures. Network-based IDS performs its attack detection based upon a comparison of parameters of the user's session and the user's commands to a rules-base of techniques used by attackers to penetrate an IT system.

An attack signature can be any pattern or sequence of patterns, which constitutes a known security violation. The level of sophistication of attack identification ranges from single violations, events over time which comprise a violation, and sequential actions which comprise a violation. Upon detection, the network-based IDS can react by logging the session, alerting the system administrator, terminating the session, and/or hardening a firewall. Network-based IDS can be divided into two sub-categories: one utilizes a built-in attack signature database, and the second relies on signature information being dynamically loaded into the IDS.[14]

Current network-based IDS products (first generation) use a predominantly passive approach to collect data via protocol analysis by watching traffic on the network. Most IDS have been built on signature-based and anomaly detection, providing the capability to look for set "patterns" in packets, but they can also be tuned to look for things the average employee should never see. The additions of specific string search signature (i.e., look for "confidential"), logging, and TCP reset features have greatly enhanced IDS capability as a detection and protection tool. Due to the inability of network-based IDS to see all traffic on switched Ethernet, some Federal agencies are now turning to host-based IDS (second generation). These products can use far more efficient intrusion detection techniques such as heuristic rules and analysis. Depending on the sophistication of the sensor, it may also learn and establish user profiles as part of its behavioral database by charting what is normal behavior on the network over a period of time.

Based upon my experience, I recommend several locations for network-based IDS, including: outside the firewall; behind the firewall; in a demilitarized zone (DMZ); in front of key application servers; in a server farm; behind network connections; within remote work groups to protect sensitive information; all direct connections to customers and suppliers; high-value sub-nets such as test, research etc.; networks with a large number of transient consultants/temporary employees; and sub-nets that are often accessed targeted by outsiders. Network-based IDS can only see traffic based on the segment on which they are installed and can only protect hosts that have static IP addresses.

I have noted that both network-based and host-based IDS sensors have pros and cons; as a result, I recommend that Federal agencies use a combination. Deploying both network-based and host-based IDS solutions provides the best possible security by monitoring both network-based traffic and host specific exploits directly on targeted workstations. This IDS combination provides significant attack protection and policy enforcement. Figuring out where to use each type and how to integrate the data is a real and growing concern. The person responsible for monitoring the IDS needs to be an alert, competent System Administrator, who is familiar with the host machine, network connections, users and their habits, and all software installed on the system. This does not mean that he or she must be an expert on the software itself, but rather needs a feel for how the IT system is supposed to be running and what programs are legitimate. Many break-ins have been contained by attentive System Administrators who have noticed something "different" about their systems or who have noticed a user logged on at a time not typical for that user.

Planning Considerations and Tips: The following are planning concerns, considerations, and tips for installation, implementation, and deployment of IDS in Federal IT systems that I have gained from assisting several Federal agencies with the deployment of IDS in their operational IT environment. Senior managers from various Federal IDS projects have expressed concerns that IDS technology is still at its infancy, and intrusions get missed due to its immaturity. In order to resolve this problem, new IDS technology will have to develop the capability for real time data capture and analysis. In order to reach its full potential as a forensic tool, IDS technology must include better logging and improved evidence tracking. New attack techniques are coming out each month, and IDS technology must adapt to these rapid changes. The list of all known attacks constantly changes, rendering codifying the statistical "signature" of a new attack a daunting task for research and development labs. Additionally, the dissemination of the updated attack signatures to the field in an efficient matter is still a major problem.

The power of IDS is that it demonstrates a positive degree of readiness, which may be critical for long term success. Federal IT system security risks and weaknesses include non-existent or weak IT architectures and/or security architectures; poor IDS operations procedures; poor IT system definitions including system boundaries, topologies, diagrams, and hardware/software inventories; no centralized IDS logging capability; inadequate IDS event notification procedures; and lack of a formal incident response capability. As an IT planner, I know that all of these security risks and weaknesses can and will influence the planning process for the installation, implementation, and deployment of IDS in Federal IT systems.

One of the most common occurrences is that Federal agencies do not have a formal IT architectures and/or security architectures even though they are required by the Information Technology Reform Act. NIST recommends that Federal agencies use a concept called defense-in-depth in the development of their security architecture. Defense-in-depth strategy calls for the use of multiple, overlapping protection approaches to ensure that the failure or circumvention of any individual protection approach will not leave the system unprotected. The use of IDS is considered to be a key component of a sound security architecture.[15] Employing the tenets of defense-in-depth, a Federal agency can deploy successive compensatory measures such as IDS to further prevent system compromise or mitigate damage should the perimeter defenses be breached. A defense-in-depth philosophy ensures that the security of IT systems will not be wholly dependent on any single element of the design, construction, maintenance, or operation of its architecture. The division of internal roles and responsibilities between the various parts of organizations can complicate the successful use of IDS. As an example, there must be reliable, repeatable methods in place for coordination and notification of IT system or security engineering changes. Coordination methods and mechanisms are needed for all phases of IT system engineering, to include design, implementation, management, and notification of changes.

One IDS project I worked on taught me how critical it is for Federal agencies to have adequately integrated IDS procedures into day-to-day IT operations to develop integration plans. Areas for integration include use of alerts, escalation procedures, and enterprise management capability. The alerts generated by the IDS must be employed in operational management of IT security. Paging and notification mechanisms must be activated in the IDS to send alerts immediately to appropriate staff. Escalation procedures must be defined, promulgated, and rehearsed. All involved organizations and staff members need to understand their roles in using IDS and responding to potential incidents. They also must have an understanding of the roles played by other participants in order to minimize redundancy and improve efficiency. IDS should be integrated technically and operationally with the enterprise management capability. Even though IDS is not enterprise management software, it can enhance the capability of the enterprise management engineers to understand the composition of IT system traffic.

IDS implementation requires rigorous processes for design, deployment, configuration management, and documentation, as well as continuous refinement to reflect changes in the rest of the enterprise. I have noted that most Federal agencies lack accurate IT system definitions for system boundaries, topologies, diagrams, and hardware/software inventories. Engineering decisions, in particular those related to the implementation of an IDS, require well-written documentation, definition, and configuration control. Most importantly, it must be regarded by the staff as an important source of reference material. If IDS design is to be repeatable for other systems and other sensors, future designs must be able to refer to the current placement. The implementation of IDS is a significant systems engineering project that never concludes; rather, it evolves with the enterprise. I tell my clients that IDS is not a COTS solution that can be implemented once and forgotten.

Logging of all incidents in a central repository is very important for near-term and long-term intrusion detection; however, I routinely see Federal agencies that do not have a centralized IDS

logging capability. In order to fully exploit the IDS capabilities, accurate and useful records must be kept in a secure manner. This repository allows the IDS staff to analyze the historical evolution of attacks in order to detect trends and protect against them. It will also provide the raw material for management oversight, law enforcement activities, training programs, and future dry runs. During early phases, I recommend that the Federal agency conduct initial log analysis and evaluation utilizing an automated centralized tool for the collection, correlation, and initial reporting on data from their firewalls, IDS, and mission essential systems. Centralizing collection, correlation, and reporting on data from firewalls, IDS, and mission essential systems into a single automated feedback loop will provide for a single source of analysis, a more accurate recognition of enterprise-wide attack patterns, and thorough documentation of intruder activities in the event of a security compromise. Additionally, data collected from vulnerability scans should be brought back into the feedback loop for correlation against firewall and IDS configurations. This allows for the immediate focus on potential security "hot spots" while saving less critical events for later review and analysis.

Another situation that I have experienced is that some Federal agencies lack a comprehensive log analysis and reporting solution that processes a variety of system and server logs to include logs from the firewalls, IDS, web servers, FTP servers, and other high-interest server and system logs. During the second phase, the Federal agency will conduct long-term trend analysis to detect inappropriate, incorrect, or anomalous activity on their IT networks. Implementing an off-line network IDS system to periodically conduct long-term trend audit and analysis of TCP/IP network log data can assist in detecting network vulnerabilities, understanding the behavior of network resource consumers, and establishing a baseline analysis so that System Administrators can use exception reports to identify suspected intrusions. Such implementation will also transform TCP/IP network transactions into data suitable for techniques and tools associated with warehousing, mining, and exception reporting. Data warehouse tools will allow System Administrators to build a read-only, analytical data warehouse, which will be used as the foundation for managing large quantities of incoming TCP/IP traffic data. Once TCP/IP traffic data is loaded into the data warehouse, a data-mining tool will be utilized to visualize the data and model results. Once the appropriate data structure has been created, IDS models can be formulated. These models can be applied on a near-real-time basis against incoming TCP/IP data to detect unauthorized activity. Both short and long-term trend analysis programs must be integrated with the Incident Response Capability.

The most common weakness that I have found is that some Federal agencies do not have adequate IDS event notification procedures. The reports of events detected by IDS are not transmitted to any designated or dedicated person or organization. This is analogous to a burglar alarm system that neither rings a bell nor calls police. This type of notification is sufficient for post-action forensics, but does not support near-real-time response. Most IDS include capabilities for sending notification of events to a pager or an e-mail address. IDS staff should activate these options and install a dial-out modem for the pager feature. IDS should be configured so that only serious attacks generate notifications. Low-level signatures such as port scans should not generate pager or e-mail notifications but can be dealt with during the next business day. Implementation of this type of recommendation effectively creates a virtual 24x7 staff.

Conclusion: Currently IDS are not required as a mandatory security control in Federal IT systems, but the trend appears to be building that IDS will become as common place and routine as firewalls have become during the last ten years in Federal IT systems. As this occurs, the concerns, considerations, and tips outlined above should be planned for and incorporated into the near, mid, and long term IDS deployment plan in order to gain the maximum benefit from the IDS. In order to incorporate IDS into day-to-day operations, the Federal agency must be prepared to recognize attacks and respond to them according to a plan. Some Federal agencies do not have a formal incident response capability to respond to intrusion events and must develop such a plan. The response plan should address the following steps: IDS notification appropriate to the detected threat level; management decisions on appropriate response; coordinated action to be taken by a responsible component; and management reporting within a set timeframe to request escalation or to document the after-action results. In order to foster the appropriate organizational behavior and habits, the Federal agency should begin by writing plans for a few attacks, publishing them throughout the organization, and practicing them using simulated attacks. These practice sessions may be paper based, with the participants seated at a conference room and playing roles, and should lead to complete exercises of the agency's response.

---

[1] National Institute of Standards and Technology. *NIST Special Publication on Intrusion Detection Systems*. Draft. 2001. Page 5. csrc.nist.gov/publications.
[2] Intrusion Detection Pages. Page 4. http://www.cerias.purdue.edu/coast/intrusion-detection/classification.html.
[3] Martin Roesch. Snort - Lightweight Intrusion Detection for Networks. Page 9. http://www.snort.org.
[4] National Institute of Standards and Technology. *NIST Special Publication on Intrusion Detection Systems*. Draft. 2001. Page 5. csrc.nist.gov/publications.
[5] National Institute of Standards and Technology. *NIST Special Publication on Intrusion Detection Systems*. Draft. 2001. Page 8. csrc.nist.gov/publications.
[6] Office of Management and Budget. *Management of Federal Information Resources*. OMB Circular A-130. February 8, 1996. Appendix III, Section 3.b.2.e. www.whitehouse.gov/omb.
[7] National Institute of Standards and Technology. *NIST Special Publication on Intrusion Detection Systems*. Draft. 2001. Page 5. csrc.nist.gov/publications.
[8] National Institute of Standards and Technology. *NIST Special Publication on Intrusion Detection Systems*. Draft. 2001. Page 6. csrc.nist.gov/publications.
[9] National Institute of Standards and Technology. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Special Publication 8000-14. 1996. Page 50. csrc.nist.gov/publications.
[10] National Institute of Standards and Technology. *NIST Special Publication on Intrusion Detection Systems*. Draft. 2001. Page 18-19. csrc.nist.gov/publications.
[11] Intrusion Detection Pages. Page 6. http://www.cerias.purdue.edu/coast/intrusion-detection/classification.html.
[12] Axent Technologies, Inc. *Everything You Need to Know About Intrusion Detection*. Rockville, Maryland, 1999. Page 11.
[13] National Institute of Standards and Technology. *NIST Special Publication on Intrusion Detection Systems*. Draft. 2001. Page 37. csrc.nist.gov/publications.
[14] Axent Technologies, Inc. *Everything You Need to Know About Intrusion Detection*. Rockville, Maryland, 1999. Page 13
[15] National Institute of Standards and Technology. *Engineering Principles for IT Security*. Draft. February 5, 2001. Page 4. csrc.nist.gov/publications.