February 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

INTRUSION DETECTION AND PREVENTION SYSTEMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Intrusion detection and prevention systems (IDPSs) are composed of software that helps organizations to monitor and analyze events occurring in their information systems and networks, and to identify and stop potentially harmful incidents. With the growing dependence of organizations on information systems to carry out essential activities and with the increasingly frequent and intense attacks on systems, IDPSs have become an essential component of the security infrastructure of nearly every organization. The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently updated its recommendations to organizations about the use of intrusion detection and prevention systems.

NIST Special Publication (SP) 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*

NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology*, was published in February 2007. The publication explains how intrusion detection and prevention systems can help organizations strengthen the security of their information systems, and recommends ways that organizations can design, implement, configure, secure, monitor, and maintain intrusion detection and prevention systems. Written by Karen Scarfone and Peter Mell, the publication replaces NIST Special Publication 800-31, *Intrusion Detection Systems*.

NIST SP 800-94 explains the basic concepts of intrusion detection and prevention. It provides an overview of IDPS technologies, including typical components, general detection methodologies, and implementation and operation assistance. Four classes of IDPS products - network-based, wireless, network behavior analysis, and host-based systems - are presented to help users compare them and to determine the appropriate type or types of IDPS needed for their environments. Also included are descriptions of other technologies that can detect intrusions, such as security information and event management software and network forensic analysis tools. The publication focuses on helping organizations that are implementing enterprise-wide IDPS solutions, but most of the information is also applicable to standalone and small-scale IDPS deployments.

One section of the publication provides specific information to help organizations in the selection of IDPS products after they have determined the particular type of IDPS technology needed. The guide discusses the identification of general requirements that the IDPS products should meet. Sets of criteria are provided to enable organizations to evaluate four aspects of IDPS technologies: security capabilities, performance, management, and life cycle cost. The guide provides a discussion of how to perform hands-on and paper evaluations of products, and when each evaluation technique is most appropriate.

The appendices to NIST SP 800-94 provide extensive information about intrusion detection and prevention systems. Included are a glossary, an acronym list, and lists of in-print resources and online tools and resources. The intrusion detection and prevention guide is available on NIST's web pages at:

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since March 2006:

- *Minimum Security Requirements for Federal Information and Information Systems: Federal Information Processing Standard (FIPS) 200 Approved by the Secretary of Commerce, March 2006*
- *Protecting Sensitive Information Transmitted in Public Networks, April 2006*
- *An Update on Cryptographic Standards, Guidelines, and Testing Requirements, May 2006*
- *Domain Name System (DNS) Services: NIST Recommendations for Secure Deployment, June 2006*
- *Protecting Sensitive Information Processed and Stored in Information Technology (IT) Systems, August 2006*
- *Forensic Techniques: Helping Organizations Improve Their Responses to Information Security Incidents, September 2006*
- *Log Management: Using Computer and Network Records to Improve Information Security, October 2006*
- *Guide to Securing Computers Using Windows XP Home Edition, November 2006*
- *Maintaining Effective Information Technology (IT) Security Through Test, Training, and Exercise Programs, December 2006*
- *Security Controls for Information Systems: Revised Guidelines Issued by NIST, January 2007*

http://csrc.nist.gov/publications/nistpubs/index.html.

Functions of Intrusion Detection and Prevention Systems

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not; for example, a user could enter an incorrect address of a system and accidentally attempt to connect to a different system without authorization.

An intrusion detection system (IDS) is software that automates the intrusion detection process. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) have many of the same capabilities, so for brevity this publication refers to them collectively as intrusion detection and prevention systems (IDPS).

Intrusion detection and prevention systems identify possible incidents, log information about them, attempt to stop them, and produce reports for security administrators. The systems also assist organizations in identifying problems with security policies, documenting threats, and deterring individuals from violating security policies.

Four Types of IDPSs

NIST SP 800-94 discusses four types of IDPSs, which are based on the type of events that they monitor and the ways in which they are deployed:

- **Network-Based** systems monitor network traffic for particular network segments or devices and analyze the network and application protocol activity to identify suspicious activity. This type of system can identify many different types of events of interest, and is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks.

- **Wireless** systems monitor wireless network traffic and analyze it to identify suspicious activity involving the wireless networking protocols themselves. This type of system cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. It is most commonly deployed within range of an organization's wireless network to monitor it, but it can also be deployed to locations where unauthorized wireless networking could be occurring.

- **Network Behavior Analysis (NBA)** systems examine network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (e.g., a client system providing network services to other systems). NBA systems are most often deployed to monitor flows on an organization's internal networks, and are sometimes deployed where they can monitor flows between an organization's networks and external networks.

- **Host-Based** systems monitor the characteristics of a single host and the events occurring within that host for suspicious activity. The types of characteristics that a host-based IDPS might monitor are network traffic for that host, system logs, running processes, application activity, file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

Components, Architecture, Security Capabilities, and Management Issues

NIST SP 800-94 explains in detail the components and architecture, security capabilities, and management issues related to each of the types of IDPSs.

The typical components of an IDPS are sensors or agents, management servers, database servers, and consoles. Sensors and agents monitor and analyze activity; sensors are used to monitor networks and agents are used to monitor hosts. Management servers handle information from sensors or agents and manage them. Database servers are repositories for event information recorded by the sensors or agents and by management servers. Consoles are programs that provide interfaces for IDPS users and administrators. These components can be connected to each other through an organization's standard networks or through a separate network that is designed for security software management. A management network helps to protect the IDPS from attack and to ensure it has adequate bandwidth under adverse conditions. A virtual management network can be created using a virtual local area network (VLAN) to provide protection for IDPS communications.

Most IDPSs can provide a wide variety of security capabilities. Some products offer information-gathering capabilities, such as collecting information on hosts or networks from observed activity. IDPSs can perform extensive logging of data related to detected events. This data can be used to confirm the validity of alerts, investigate incidents, and correlate events between the IDPS and other logging sources. Logs of collected information should be stored both locally and centrally to support the integrity and availability of the data. IDPSs offer extensive, broad capabilities to detect events, but may require at least some tuning and customization to improve their detection accuracy, usability, and effectiveness. Most IDPSs offer multiple prevention capabilities; the specific capabilities vary by IDPS technology type. IDPSs usually allow administrators to specify the prevention capability configuration for each type of alert. This includes enabling or disabling prevention, as well as specifying which type of prevention capability should be used.

Architectural considerations include component placement, solution reliability, interoperability with other systems, management network architecture, and necessary changes to other security controls.

Who We Are
The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

NIST Recommendations for Implementing IDPSs

NIST recommends that organizations carry out the following activities when implementing IDPSs:

- Ensure that all IDPS components are secured appropriately.

Securing IDPS components is very important because IDPSs are often targeted by attackers who want to prevent the IDPSs from detecting attacks or want to gain access to sensitive information in the IDPSs, such as host configurations and known vulnerabilities. IDPSs are composed of several types of components, including sensors or agents, management servers, database servers, user and administrator consoles, and management networks. All components' operating systems and applications should be kept fully up to date, and all software-based IDPS components should be hardened against threats. Specific protective actions of particular importance include creating separate accounts for each IDPS user and administrator, restricting network access to IDPS components, and ensuring that IDPS management communications are protected appropriately, such as encrypting them or transmitting them over a physically or logically separate network. Administrators should maintain the security of the IDPS components on an ongoing basis, including verifying that the components are functioning as desired, monitoring the components for security issues, performing regular vulnerability assessments, responding appropriately to vulnerabilities in the IDPS components, and testing and deploying IDPS updates. Administrators should also back up configuration settings periodically and before applying updates to ensure that existing settings are not inadvertently lost.

- Consider using multiple types of IDPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity.

The four primary types of IDPS technologies—network-based, wireless, NBA, and host-based—each offer fundamentally different information-gathering, logging, detection, and prevention capabilities. Each technology type offers benefits over the others, such as detecting some events that the others cannot and detecting some events with significantly greater accuracy than the other technologies. In many environments, a robust IDPS solution cannot be achieved without using multiple types of IDPS technologies. For most environments, a combination of network-based and host-based IDPS technologies is needed for an effective IDPS solution. Wireless IDPS technologies may also be needed if the organization determines that its wireless networks need additional monitoring or if the organization wants to ensure that rogue wireless networks are not in use in the organization's facilities. NBA technologies can also be deployed if organizations desire additional detection capabilities for denial of service attacks, worms, and other threats that NBAs are particularly well-suited to detecting. Organizations should consider the different capabilities of each technology type along with other cost-benefit information when selecting IDPS technologies.

- Consider whether or not the IDPSs should be integrated when planning the use of multiple types of IDPS technologies or multiple products of the same IDPS technology type.

Direct IDPS integration most often occurs when an organization uses multiple IDPS products from a single vendor, and has a single console that can be used to manage and monitor the multiple products. Some products can also mutually share data, which can speed the analysis process and help users to better prioritize threats. A more limited form of direct IDPS integration is having one IDPS product provide data for another IDPS product but preventing data sharing in the opposite direction. Indirect IDPS integration is usually performed with security information and event management (SIEM) software, which is designed to import information from various security-related logs and correlate events among them. SIEM software complements IDPS technologies in several ways, including correlating events logged by different technologies, displaying data from many event sources, and providing supporting information from other sources to help users verify the accuracy of IDPS alerts.

- Define the requirements that the products should meet before evaluating IDPS products.

Evaluators need to understand the characteristics of the organization's system and network environments, so that a compatible IDPS can be selected that can monitor the events of interest on the systems and/or networks. Evaluators should articulate the goals and objectives they wish to attain by using an IDPS, such as stopping common attacks, identifying misconfigured wireless network devices, and detecting misuse of the organization's system and network resources. Evaluators should also review their existing security policies, which serve as a specification for many of the features that the IDPS products need to provide. In addition, evaluators should understand whether or not the organization is subject to oversight or review by another organization. If so, they should determine if that oversight authority requires IDPSs or other specific system security resources. Resource constraints should also be taken into consideration by evaluators. Evaluators also need to define specialized sets of requirements for the following:

- **Security capabilities**, including information gathering, logging, detection, and prevention.

- **Performance**, including maximum capacity and performance features.

- **Management**, including design and implementation (e.g., reliability, interoperability, scalability, product security), operation and maintenance (including software updates), and training, documentation, and technical support.

- **Life cycle costs**, both initial and maintenance costs.

- Consider using a combination of several sources of data on the products' characteristics and capabilities when evaluating IDPS products.

Common product data sources include test lab or real-world product testing, vendor-provided information, third-party product reviews, and previous IDPS experience from individuals within the organization and trusted individuals at other organizations. When using data from other parties, organizations should consider the fidelity of the data because it is often presented without an explanation of how it was generated. There are several major challenges in performing in-depth hands-on IDPS testing, such as the considerable resources needed and the lack of a standard test methodology and test suites, which often make it infeasible. However, limited IDPS testing is helpful for evaluating security requirements, performance, and operation and maintenance capabilities.

More Information

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. For information about NIST standards and guidelines that are referenced in the intrusion and detection guide, as well as other security-related publications, see NIST's web page: http://csrc.nist.gov/publications/index.html

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.