

## Intrusion Detection Systems

Intrusion Detection Systems (IDSs) are an important, evolving technology for protecting computer networks. All sectors of society, from government to business to universities, increasingly depend on networks to be reliable and secure. For many e-commerce organizations, their very existence in the marketplace demands expert computer security practices. For instance, in the 1980s and early 1990s, denial-of-service (DoS) attacks—a kind of attack that floods the network until it can no longer handle legitimate traffic—were infrequent and not considered serious. Today, successful DoS attacks can cause great financial loss to organizations such as online stock-brokers and retailers and can cause a wide array of unwanted disruptions to government computer networks. (For more on denial of service attacks, see the Spring 2000 issue of *news@sei* available at <http://www.sei.cmu.edu/products/news.sei/news-spring00.pdf>.)

The goal of intrusion detection systems is to accurately detect anomalous network behavior or misuse of resources, sort out true attacks from false alarms, and notify network administrators of the activity. Many organizations now use intrusion detection systems to help them determine if their systems have been compromised, but it can be difficult to find unbiased information to help organizations understand and evaluate the available tools and how to best use them.

Although intrusion detection and response technology is still immature, it remains a key element in a layered, enterprise-wide security plan that often includes detailed security policies, a computer security incident response team (CSIRT), firewalls, virus protection, encryption, authentication, access control, virtual private networks (VPNs), and more. IDSs are essential because, at best, they provide increased near real-time detection that can help limit compromise and damage to networks, reduce costs through automated detection, and stem DoS attacks.

The CERT® Coordination Center (CERT/CC) at the SEI publishes security improvement modules (each of which addresses an important but narrowly defined problem in network security) and technical reports, and offers courses that contain intrusion detection information. The technical report *State of the Practice of Intrusion Detection Technologies* offers detailed guidance about all phases of selecting, deploying, and maintaining IDSs. The following sections outline some important concepts from CERT/CC publications.

### Selecting an IDS

When selecting an IDS, organizations need to consider the level of privacy needed, how much the organization can afford to spend, and whether there are internal constraints on the types of software the organization can use. Other important topics include specifics about IDS capabilities, such as detection and response characteristics, use of signature

and/or anomaly-based approaches, accuracy of diagnosis, ease of use, and effectiveness of the user interface.

Since the new product cycle for commercial IDSs is rapid, information and systems quickly become obsolete. Staff of the CERT/CC have conducted experiments with commercial and public domain tools, and found that commercial IDS tools were easier to install than public domain tools, but neither had an understandable, easy-to-use, configuration interface. The majority of IDSs provide good capabilities for enhanced network monitoring rather than for intrusion detection, given that some post-IDS-alert data analysis was normally required. In many cases, determining which features are most important to an organization will be the deciding factor.

Although an IDS is an important element in an organization's overall security plan, it is only effective if it has support from management at the level of the corporate chief information officer and the information security manager. They must ensure that the IDS is properly deployed and maintained.

## Deploying an IDS

Once an IDS is selected, a number of decisions will determine whether it is deployed effectively. These include decisions about how to protect the organization's most critical assets, how to configure the IDS to reflect the organization's security policies, and what procedures to follow in case of an attack to preserve evidence for possible prosecutions. Organizations must also decide how to handle alerts from the IDS and how these alerts will be correlated with other information such as system or application logs.

Additional information and guidance in selecting an IDS are available from SEI publications, including:

**State of the Practice of Intrusion Detection Technologies**

<http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html>

**Preparing to Detect Intrusions**

<http://www.cert.org/security-improvement/modules/m09.html>

**Responding to Intrusions**

<http://www.cert.org/security-improvement/modules/m06.html>

An IDS does not prevent attacks. In fact, if attackers realize that the network they are attacking has an IDS, they may attack the IDS first to disable it or force it to provide false information that distracts security personnel from the actual attack. Many intrusion detection tools have security weaknesses that could include failing to encrypt log files, omitting access control, and failing to perform integrity checks on IDS files.

## Maintaining an IDS

An IDS must be constantly monitored after it is deployed. Procedures must be developed for responding to alerts; these procedures will determine how staff members analyze and act on alerts, and how staff monitors the outcomes of both manual and automatic responses. In addition, as upgrades become available, they should be installed to keep the IDS as current and secure as possible.

Technology alone cannot maintain network security; trained technical staff are needed to operate and maintain the technology. Unfortunately, the demand for qualified intrusion analysts and system/network administrators who are knowledgeable about and experienced in computer security is increasing more rapidly than the supply.

When an IDS is properly maintained, it can provide warnings about when a system is being attacked, even if the system is not vulnerable to the specific attack. The information from these warnings can be used to further increase the system's resistance to attacks. An IDS can also confirm whether other security mechanisms, such as firewalls, are secure. If the necessary time and effort is spent on an IDS through its life cycle, its capabilities will make it a useful and effective component of an overall security plan.

---

Copyright © 2001 Carnegie Mellon University

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

® CMM, Capability Maturity Model, Capability Maturity Modeling, Carnegie Mellon, CERT, and CERT Coordination Center are registered in the U.S. Patent Trademark Office.

SM ATAM; Architecture Tradeoff Analysis Method; CMMI; CMM Integration; CURE; IDEAL; Interim Profile; OCTAVE; Operationally Critical Threat, Asset, and Vulnerability Evaluation; Personal Software Process; PSP; SCAMPI; SCAMPI Lead Assessor; SCE; Team Software Process; and TSP are service marks of Carnegie Mellon University.

TM Simplex is a trademark of Carnegie Mellon University.