

Realistic Expectations for Intrusion Detection Systems

Richard Wiens 2001-03-19

Realistic Expectations for Intrusion Detection Systems

by *Richard Wiens*

last updated March 19, 2001

Intrusion detection forms an increasingly important segment of the security technology market. While intrusion detection systems were, until recently, both expensive and difficult to maintain, they have become more affordable. With the arrival of less expensive off-the-shelf solutions, IDSs are becoming a more common feature of security regimens.

The emergence of IDSs causes some security commentators to see them as a panacea, solving all of the complex and diverse threats to network security. However, as does any weapon in the security arsenal, an IDS has limited capabilities. To expect too much of an IDS places the user's network at risk. This article will discuss reasonable expectations of Intrusion Detection Systems (IDSs). Its purpose is to help users and potential users realize the increasing importance of intrusion detection in all organizations, while also pointing out the realistic outcomes to be expected from current IDS products. The discussion will also discuss future trends in IDS development.

Realistic Expectations of Intrusion Detection Systems

Intrusion detection is considered by many to be the logical complement to network firewalls, thus extending the security management capabilities of system administrators to include security audit, monitoring, attack recognition and response. The following real-world examples point up the concrete tasks that IDSs can be expected to perform efficiently, ensuring increased real security protection.

IDSs monitor the Internet to detect possible attacks

Monitoring the Internet for potential attack is both time-consuming and tedious. By performing the ongoing task of monitoring the Internet to detect possible attacks, intrusion detection systems allow security personnel to accomplish other essential security functions. However, IDS vendors include extensive attack signature databases against which they match information from the user's system. Vendors have expert staffs that monitor the Internet and other sources for new attack tools and techniques. They then use this information to develop new signatures

that are provided to customers, thereby enabling network administrators to keep up-to-date without expending valuable time and monetary resources.

IDSs help organizations to develop and implement an effective security policy.

Many intrusion detection systems offer security policy tools that help to define and implement the security policy of the organization. All organizations should have a security policy in place. This policy should clearly dictate from the CEO level the security priorities of the organization and define a procedure for what happens when an intrusion is suspected. An effective security policy should consider the following: operating systems, services (web servers, e-mail servers, and databases), network IDSs, firewalls, and the network management platform (such as OpenView). IDSs should be included as part of the overall security policy of an organization: they help to enforce the security policy by detecting prohibited traffic and/or activities, and they play an active role in the identification of incidents for which the security policy outlines specific responses.

IDSs allow non-technical project members to perform comprehensive security management.

Intrusion detection systems allow security features to be performed by personnel with low or moderate security management experience. Widely available off-the-shelf IDSs feature accessible graphic user interfaces, such as windows-based point and click screens, that offer users easy set-up and configuration in a logical, readily understood fashion. As a result, organizations that do not have the resources to hire highly-experienced, technically-trained security personnel can still benefit from the advantages that IDSs have to offer.

File integrity checkers acknowledge and report changes to data files

IDS can alert users to damage that has been inflicted on their network. Putting Trojan Horses in critical system files is a standard attack technique. Similarly, the alteration of critical information files to mask illegal activity, damage reputations, or commit fraud is common. File integrity assessment tools utilize strong cryptographic checksums to detect unauthorized changes in the files and, in the case of a tampering problem, quickly ascertain the extent of damage. This enables administrators to be aware of intrusions that may have taken place and to prevent any further damage from being inflicted on their network or, in the case of distributed denial of service attacks, from their network.

IDSs trace user activity from the point of entry to the point of exit or impact

IDSs enhance the protection provided by perimeter protections, such as firewalls. Expert attackers can often penetrate firewalls. Therefore, the ability to correlate observed activity with a particular user will improve security within the boundaries of a network. The advantage of tracing user activity using IDSs is to develop a baseline containing information about user logins, file activity and CPU usage so that the IDS can respond whenever there is a change in this baseline.

IDSs make sense of complex system information sources

Operating system audit trails and other system logs are a treasure trove of information about what's going on internally within a user's systems. Unfortunately, they are also often incomprehensible, even to expert system administrators and security officers. IDSs allow administrators and managers to tune, organize, and comprehend what these information sources tell them, often revealing problems before loss occurs.

IDSs lend a greater degree of integrity to the rest of the security infrastructure

Because they monitor the operation of firewalls, encrypting routers, key management servers and files that are critical to other security mechanisms, intrusion detection systems provide additional layers of protection to a secured system. The strategy of a system attacker will often include attacking or otherwise nullifying security devices protecting the intended target. When conventional security devices fail due to configuration, attack, or user error, IDSs can recognize the problem and notify the right security people. IDSs can recognize the first hallmarks of attack and issue alerts, allowing network administrators to respond to them, thereby mitigating damage. IDSs can also help network managers to be aware of suspicious activity. For instance, all SNMP devices should send "Authentication Failure" traps and management consoles should alert administrators when these go off.

Unrealistic Expectations for Intrusion Detection Systems

Despite all of the benefits that IDSs offer to security personnel, it would be a dangerous mistake to believe that they are some sort of magic bullet that will prevent all hostile attacks. While IDSs are improving to encompass such capability as additional sensor inputs, improved analysis techniques, and more extensive signature databases, shortcomings remain.

IDSs only protect against known signatures

To date, commercial IDSs have concentrated mostly on string matching and other forms of signature identification to detect classes of outsider attacks. These techniques all rely on previously-encountered attack signatures for their defence. While the easy part of the problem seems to have been addressed by the commercial community, research advances in the community at large appear to have slowed, resulting in an increased emphasis on detecting known types of outsider attacks.

Unfortunately, as any experienced security administrator knows, as soon as one method of attack is foiled, intrepid attackers invent new ones to circumvent existing defences. Detecting, identifying, and responding to hitherto unknown attacks and anomalies remain as very challenging problems, including highly coordinated attacks, subtle forms of misuse by insiders, and anomalous network behavior resulting from malfunctions and outages. Providing global rather than local analysis is still a very important research area that is relatively uncharted. Generalizations beyond known security attacks are also challenging.

IDSs do not strengthen inherent security weaknesses

Security is a complex area with myriad possibilities and difficulties. In networks, it is also a "weakest link" phenomenon - it only takes one vulnerability on one machine to allow an adversary to gain entry and wreak havoc on the entire network. The time it takes for this to occur is minuscule. There are no magic solutions to network security problems, and intrusion detection products are no exception to this rule. IDSs do not patch vulnerabilities in operating systems or applications, and they cannot protect against vulnerabilities created by user error. However, as part of a comprehensive security management they can play a vital role in protecting your systems.

Furthermore, while leading-edge research in intrusion detection asserts that sophisticated statistical analysis of user behaviour can assist in identification of a particular person by observing their system activity, this fact is far from demonstrated. Therefore, we must still rely on other means of identification and authentication of users. This is best accomplished by strong authentication mechanisms (including token-based or biometric schemes and one-time passwords). A security infrastructure that includes strong identification and authentication as well as intrusion detection is stronger than one containing only one or the other.

IDSs do not take the place of an effective Security Policy

Intrusion-detection expert systems increase in value when they are allowed to function as both hacker/ burglar alarms and policy-compliance engines. These functions will not only spot the high-school hacker executing the "teardrop" attack against your file server, but will also spot the programmer accessing the payroll system after hours. However, this policy compliance checking can exist only if there is a security policy to serve as a template for constructing detection signatures.

IDSs do not provide for incident handling

Even in very secure environments, incidents happen. In order to minimize the occurrence of incidents as well as the possibility of resulting damage, security personnel must perform incident handling. They must investigate the attacks, determine, where possible, the responsible party and then diagnose and correct the vulnerability that allowed the problem to occur, reporting the attack and particulars to authorities where required. In some cases, especially those involving a dedicated attacker, finding the attacker and then pursuing criminal charges against the attacker is the only way to make the attacks cease. However, an IDS is not capable of identifying the person at the other end of the connection without human intervention. The best that it can do is identify the IP address of the system that served as the attacker's point of entry, the rest is up to a human incident handler.

IDSs do not necessarily identify the origin of the attack

TCP/IP and many other network protocols do not perform strong authentication of host source/ destination addresses. This means that the source address that is reflected in the packets carrying an attack does not necessarily correspond to the real source of the attack. As a result, while the IDS may identify the network or system from which the attack is being launched, it may only be identifying a machine that is occupied and is being used to launch an attack remotely, without the knowledge of the system's administrator or owners. It is difficult to identify who is attacking one's system; it is very difficult to prove the identity of an attacker in a court of law-for example, in civil or criminal legal processes.

IDSs are only as accurate as the information they rely upon

In other words, "garbage in garbage out" still applies. System information sources are mined from a variety of points within the system. Despite the best efforts on the part of system vendors, many of these sources are software-based; as such, the data are subject to alteration by attackers. Many hacker tools (for example "cloak" and "zap") explicitly target system logs, selectively erasing records corresponding to the time of the attack and covering the intruders' tracks. This argues for the value of integrated, sometimes redundant, information sources; each additional source increases the possibility of obtaining information not corrupted by an attacker.

Network-based IDSs are vulnerable to overload

Network-based intrusion detection is capable of monitoring traffic of a network, but only to a point. First, given the vantage point of network-based intrusion detection sources that rely on network adapters set to promiscuous mode, not all packets are visible to the systems. Second, as traffic levels rise, the associated processing load required to keep up becomes prohibitive and the analysis engine either falls behind or fails. In fact, vendors themselves characterized the maximum bandwidth at which they had demonstrated their products to operate without loss with 100% analysis coverage at 65 MBPS.

Network-based IDSs may misinterpret the outcome of a malicious transaction

There are weaknesses in packet-capture-based network IDSs. The heart of the vulnerabilities involves the difference between the IDSs' interpretation of the outcome of a network transaction (based on its reconstruction of the network session) and the destination node for that network session's actual handling of the transaction. Therefore, a knowledgeable adversary can send a series of fragmented and otherwise doctored packets that elude detection, but launch attacks on the destination node. Worse yet, an adversary can use this sort of packet manipulation to accomplish a denial of service attack on the IDS itself by overflowing memory allocated for incoming packet queues.

Fragmented packets can be problematic

Dealing with fragmented packets can also be problematic. This problem has serious ramifications when one considers modern high-speed ATM networks that use packet fragmentation as a means of optimizing bandwidth. Other problems associated with advances in network technologies include the effect of switched networks on packet-capture-based network IDSs. As the effect of switched networks is to establish a network segment for each host, the

range of coverage for a network IDS is reduced to a single host. This problem can be mitigated in those switches offering monitoring ports or spanning capability; however, these features are not universal in current equipment.

Summary and Future Trends

Up to this point, commercial vendors have put their attention and effort into solving the easiest part of the intrusion detection problem, namely IDSs that function mainly by 'string matching' or other forms of signature identification schemes to detect outsider attacks. Research advances in the community at large seem to have slowed along with the increased emphasis on detecting known types of outsider attacks. Detecting, identifying, and responding to hitherto unknown attacks and anomalies remain as very challenging problems. Examples of such unknown attacks or anomalies may include highly coordinated attacks, subtle forms of misuse by insiders, and anomalous network behavior resulting from malfunctions and outages. Providing global rather than local analysis is still a very important research area that is relatively uncharted.

Internal Network Issues

Encryption is growing in popularity and products including encryption features are becoming ubiquitous. As more organizations utilize these products to secure their data as it travels over public networks, adversaries will adapt their attack strategies to accommodate this. The predictable outcome is that attacks will shift to those areas in which data is not generally encrypted: the internal network.

At the same time, corporate employment practices will continue to focus on outsourcing, strategic partnerships with other organizations, and telecommuting. All of these typically involve remote access to the internal network, thereby expanding the security perimeter of the organization to areas that not physically protected. IDSs are the only part of the IDS/Firewall protection infrastructure that are privy to the traffic on the internal network. Therefore, they will become even more important as security infrastructures evolve.

Future Capabilities and Trends for Intrusion Detection

The capabilities for intrusion detection are growing as new products enter the marketplace, and existing organizations expand their product offerings to allow additional sensor inputs, improved

analysis techniques, and more extensive signature databases. Thanks to government and military interest in Information Warfare, of which Intrusion Detection is a vital defensive component, funding of research efforts has skyrocketed, with no end in sight. This increased activity will result in enhanced understanding of the intrusion detection process and new features in future products. Plans are afoot to embed intrusion detection products as standard components of major governmental and financial networks.

As intrusion detection remains an active research area, look for future products to implement new techniques for managing data and detecting scenarios of interest. Look also for additional products that function at application level and that interoperate with network management platforms. Finally, look for product features that are integrated into a bevy of special purpose devices, ranging from bandwidth management products to "black box" plug-ins for targeted environments.

Richard H. Wiens holds the position of Senior Secure Systems Engineer with Getronics Government Solutions, LLC, based in the Netherlands. He has broad responsibility for defining, analyzing, and improving security requirements for system security needs, identifying security vulnerabilities, and conducting security certifications and accreditations. He has also been involved with the security-related issues inherent to Electronic Commerce since 1994.

Relevant Links

[Computer Operations, Audit, and Security Technology \(COAST\): Intrusion Detection Pages](#)
Purdue University

[Computer Operations, Audit, and Security Technology \(COAST\)of Purdue University: Intrusion Detection Resources](#)
Purdue University

[Next-Generation Intrusion Detection Expert System \(NIDES\)](#)
SRI International

[SANS Institute Online](#)
SANS Institute

[IDIOT - Intrusion Detection In Our Time](#)
Sandeep Kumar and Eugene H. Spafford, Purdue University

[Privacy Statement](#)

Copyright 2006, SecurityFocus