Standing Sentry Over Your Network

by Mark Merkow

last updated Thursday, April 13, 2000

Introduction

Corporate networks are built assuming certain levels of trust in how the information traversing them is accessed and used. When they're hooked into public networks, like the Internet, a safer -- and more intelligent -- route leads security administrators to trust no one on the outside.

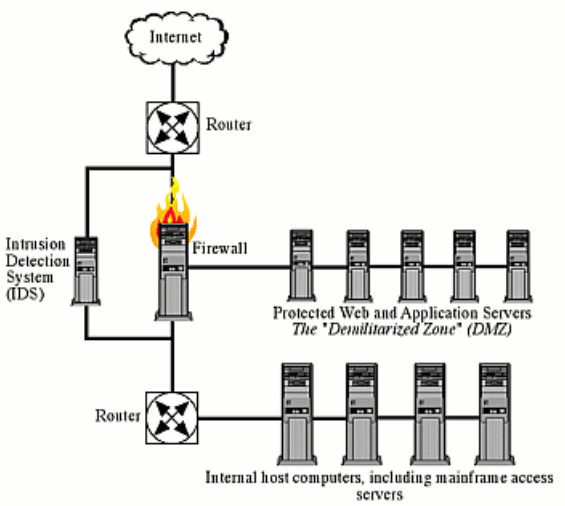
Working in conjunction with firewalls and routers, Intrusion Detection Systems (IDSs) installed as illustrated in Figure 1, can help you to automatically fend off attackers long before they can breach your perimeter of network security.

IDS technology is rapidly maturing, combining high-speed network traffic analysis with the cutting edge sciences of:

- Neural networks
- Statistics
- Artificial intelligence
- Pattern recognition, Cognitive psychology
- Information theory
- Decision theory

This article seeks to uncover how IDSs operate and how improvements in today's technology will help you to maintain the most precious asset of all -- a good night's sleep!

Figure 7-1: A Basic Network Security Model



Intrusion Detection Systems (IDSs)

An IDS attempts to detect intruders breaking into your system or legitimate users misusing system resources. The IDS operates constantly on your system, working in the background, and only notifies you when it detects something it considers suspicious or illegal.

Relevant Links

CSI Intrusion Detection System Resource
CSI

Network Flight Recorder
NFR

Axent
Axent Technologies

Cisco Secure
Cisco

The two major classifications of potential intruders are:

- Outside Intruders
- Inside Intruders

IDSs are needed to detect both types of intrusions -- break-in attempts from the outside, and knowledgeable insider attacks. Before you think about integrating an IDS into your networks, it's imperative that you begin with defining the security policies that dictate what's permitted and what's denied on your computer systems.

The two basic philosophies behind all policy development are:

- Prohibit everything that is not expressly permitted.
- Permit everything that is not expressly denied.

In general, people who are more concerned about security will exercise the first option. Policies will be in place that describe exactly what operations are allowed on a system. Any operation that is not detailed in the policy will be considered off-limits to the system.

Others who operate their systems under a spirit of cooperative computing will likely adopt the second philosophy. Unfortunately, this philosophy does not work well in today's hostile computing environments, like the Internet.

Computer intrusion detection systems were introduced in the mid-1980's to complement conventional approaches to computer security. Writers on IDS technology often cite Denning's 1987 seminal intrusion detection model, built on host-based subject profiles, systems objects, audit logs, anomaly records and activity rules. The underlying IDS model is a rules-based pattern matching system where audits are matched against subject profiles to detect computer misuse based on logins, program executions, and file access.

What Are Intrusions?

Before you can detect an intrusion, it's important to first understand what they are. Intrusions are defined relative to your security policy. Unless you've already decided what is and what is not allowed on your systems, it's pointless to try and catch intrusions.

An intrusion is defined as any set of actions that try to compromise the integrity, confidentiality, or availability of a resource. Intrusions are categorized into two main classes:

- Misuse intrusions are well-defined attacks on known weak points within a system. They can be detected by watching for certain actions being performed on certain objects.
- Anomaly intrusions are based on observations of deviations from normal system usage patterns. They are detected by building up a profile of the system under concern, and detecting significant deviations from this profile.

As misuse intrusions follow well-defined patterns, they're detectable by doing pattern matching on audit-trail and log information. Anomalous intrusions are detected by observing significant deviations from what's deemed normal behavior. An anomaly may be a symptom of a possible intrusion. Given a set of metrics that defines normal system usage, security violations may be detectable from abnormal

patterns of system usage.

Anomaly detection may also be performed using other mechanisms, such as neural networks, machine learning classification techniques, or trying to mimic biological immune systems. Anomalous intrusions are harder to detect. There are no fixed patterns that apply to all systems that could be monitored so a more fuzzy approach is needed. Ideally a system that can combine human-like pattern matching capabilities with the vigilance of a computer program could eliminate most security intrusion problems.

Many intrusion detection systems base their operations on analysis of operating system audit trail data. This data forms a footprint of system usage over time. Audit trails are convenient sources of data and are readily available on most systems. Using audit trail observations, the IDS can compute metrics about a computer network's overall state, and decide whether an intrusion is occurring.

Characteristics of Good Intrusion Detection Systems

An intrusion detection system should address the following issues, regardless of your choices of equipment or network integration:

- It must run continually without human supervision. The system should be reliable enough to allow it to run in the background of the system being observed.
- It must be fault tolerant to survive a system crash without requiring the rebuilding of the IDS's knowledge base each time the system is restarted.
- Similarly, it must resist subversion. The system should monitor itself to assure that it has not been subverted.
- It must impose minimal overhead on the attached network.
- It must observe deviations from normal behavior.
- It must be easily tailored to the network in question. Every system has different usage patterns, and the defense mechanisms should adapt easily to these patterns.
- It must cope with changing system behavior over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt.
- It must be difficult to fool.
- Issues related to false positives, false negatives, and subversion attacks

While it's operating, an IDS might incorrectly identify an attack in one of these possible ways:

- A false positive occurs when the system classifies an action as anomalous (a possible intrusion) when it is legitimate.
- A false negative occurs when an actual intrusive action has occurred but the system allows it to pass through as non-intrusive behavior.
- A subversion error can occur when an intruder modifies the operation of the intrusion detector to force false negatives to occur.

False positive errors will lead users of the intrusion detection system to ignore its output, as it will classify legitimate actions as intrusions. The occurrences of this type of error should be minimized (it may not be possible to completely eliminate them) so as to provide useful information to the operators. If too many false positives are generated, the operators will come to ignore the output of the system over time, which may lead to an actual intrusion being detected but ignored by the users.

A false negative error occurs when an action proceeds even though it is an intrusion. False negative errors are more serious than false positive errors because they give a misleading sense of security. By allowing all actions to proceed, a suspicious action will not be brought to the attention of the operator. The intrusion detection system is now a liability since the security of the system diminished from the state it was in before the intrusion detector was installed.

Subversion errors are more complex and tie in with false negative errors. An intruder could use knowledge about the internals of an intrusion detection system to alter its operation, possibly allowing anomalous behavior to proceed. The intruder could then violate the system's operational security constraints. This may be discovered by a human operator examining the logs from the intrusion detector, but it would appear that the intrusion detection system still is working correctly.

Fool Me Will You?

Another form of subversion error is fooling the system over time. As the detection system is observing behavior on the system over time, it may be possible to carry out operations each of which when taken individually pose no threat, but taken as an aggregate form a threat to system integrity. How would this happen? As mentioned previously, the detection system is continually updating its notion of normal system usage. As time goes by a change in system usage patterns is expected, and the detection system must cope with this. But if an intruder could perform actions over time which were just slightly outside of normal system usage, then it is possible that these actions could be accepted as legitimate. The detection system would have come to accept each of the individual actions as slightly suspicious, but not a threat to the system. What it would not realize is that the combination of these actions forms a serious threat to the system.

IDS For The Future

The next generation of IDSs will require the fusion of data from a myriad of heterogeneous sensors distributed across the network to effectively combat an ever-growing army of intelligent and devious malevolents.

A majority of security professionals agree that today's real-time IDS are not technically advanced enough to detect sophisticated attacks by trained professionals, and further research is needed.

The IDSs that examine operating system audit trails or network traffic, like those described above, have still not matured to a level where sophisticated attacks are reliably detected, verified, and assessed. The comprehensive and reliable systems needed tomorrow will appear with high degrees of complexity. The designs for these next generation advanced systems are only beginning to emerge.

Multisensor data fusion will provide an important framework for building the next generation IDSs and network situational awareness. Defensive IT operations and IDSs are primarily needed to ward off denial of service (DoS) attacks, unauthorized disclosure of information, and the modification or destruction of data. Automated detection and immediate reporting of these events is required to defend against attacks on your networks and computers.

Significant challenges remain for IDS developers to combine data and information from numerous heterogeneous distributed networks into a process that's useful for evaluating the security of a system. Thanks to ongoing research and development,

security professionals will be poised to increase their reliance on IDSs without sacrificing trust or confidence.

Building Security Assurance With A Layered Approach

With packet-filtering routers, firewalls, proxies, and modern intrusion detection systems in place, you can rest better at night knowing that you're protected from both internal and external threats, while still keeping the channels of communications open for both your customers and employees on the outside.

Thanks go out to CERT, CERIUS, the research staff at Carnegie-Mellon University, and Tim Bass of Silkroad for his insightful paper published by the Association of Computing Machines (ACM), entitled, "Intrusion Detection Systems & Multisensor Data Fusion: Creating Cyberspace Situational Awareness" for the information contained in this article.

Mark Merkow, CCP, is an E-commerce Security Specialist for a Fortune 50 financial-services company in Phoenix, Arizona, where he's gained over ten years of experience in project management, systems- and database-administration, Internet systems analysis, design, development, and security.

Mark's first book, Breaking Through Technical Jargon, was published in 1990. He's since authored or co-authored several other books: "Building SET Applications for Secure Transactions," with Jim Breithaupt and Ken Wheeler, "Thin Clients Clearly Explained," with Joseph Sinclair, "Virtual Private Networks for Dummies," and a book to be released in June 2000 from the American Management Association, entitled, "The Complete Guide to Internet Security."