Critical Components of Intrusion Detection Systems

Jill Oliver
Vice President
CitiCorp Information Security Office
Citibank
jill.oliver@citicorp.com

Panelists:

Lee Sutterfield
Executive Vice President
WheelGroup Corporation
lsutt@wheelgroup.com

Mark Crosbie
Audit & Intrusion Detection Engineer
Hewlett-Packard
mcrosbie@xsvr3.cup.hp.com

Dan Esbensen
Director of Advanced Research
Touch Technologies, Inc.
dan@ttinet.com

Christopher Klaus
Chief Technology Officer
Internet Security Systems, Inc.
cklaus@iss.net

Intrusion detection systems are coming of age. Today's products include capabilities to look at intrusion detection at a system-of-systems level, report suspected intrusions to a home office, and react locally to suspected intrusions by automatically denying access to the suspected attacking node. The panel members represent vendors and experienced users. They will discuss what's important and why for current and future capabilities.

Business

1. How can management determine quickly where their enterprise is being attacked and what protection a given Intrusion Detection System is offering their company?

2. A firewall is a tool, an IDS is a tool, an authorization server is a tool. You don't need only one of those, you need all of them. How does intrusion detection (ID)

fit in with other security measures (such as filtering, proxies, etc.) available? What are the redundancies, and what do IDS systems offer that is unique; is a firewall still needed?

3. How is "intrusion detection" different than what a firewall does? Can a good intrusion detection system replace having a firewall?

Technical

1. What are the major drawbacks to intrusion detection systems? Where should network-based systems be placed relative to firewalls? If inside, then all attacks appear to come from firewall, and internal traffic is not monitored. If outside, it may be difficult to determine whether the firewall repelled the attack or not. How does one address the drawbacks of each location?

2. How can an IDS protect itself against attack, and ensure that it does not become the vehicle for other attacks (denial of service being my favorite)?

3. Can "local wisdom" be built in? An enterprise-wide IDS has to run across many systems, spread through diverse groups, with different mission statements and goals. One overall strategy for the on-line operation of this IDS will simply not work. How can we build a system that both supports reporting and data gathering on the local level, and report generation for the enterprise-wide view?

4. Can we *trust* the data we are giving to the IDS? Do you trust syslog more than kernel audit data? Do you trust them more than application data? Is a firewall to be trusted when it's half-way around the world? Do we have to build a hierarchy of value for information, based on its source?

Management

1. If we equate Intrusion Detection and Response to a burglar alarm, how can we electronically make an Intrusion Detection System (IDS) invisible to attackers and how can we offer a quick and effective response? How flexible can this response be?

2. Can I assess vulnerabilities that may exist in my network and fix them before an attack is launched? If so, can an IDS offer these capabilities?

3. How can an electronic IDS be updated before a given attack is launched? Where would the new attack profiles come from? How would an IDS be updated to defend against these attacks?

4. How will my existing staff manage an IDS? What special training might they need? How will the management of the IDS interface to existing network management strategies?

5. How are ID systems of the future going to reduce the amount of data (and the false alarm rate) presented and help analysts focus on the real intrusions? (Expert system analysis?) A large enterprise may be faced with receiving data from numerous sites, different types of ID systems (host vs. network based), and different implementations (i.e. different vendor). How are we going to effectively integrate this data? Can we integrate data from other systems, such as firewalls, proxies, and routers? What kind of activity can we detect if we were able to make use of all this data?

Real time

1. Compare and contrast real time alarming with off line analysis. What staffing is required for each? Who operates the IDS? (What role or position do they have, what training do they have, other duties, authority, etc.)

2. What kinds of actions can an intrusion detection system take when an incident occurs?

3. How should an IDS scale? How can we simplify reporting to management? What performance restraints must be considered to deploy large scale Intrusion Detection? How does the equation change if we add real time response? What impact would scalable management have on performance?