Introduction to Intrusion Detection

Thomas R. Peltier, CISSP

Driving eBusiness Performance ***SM***

Network Vulnerability Assessment

- **Intrusion detection -** Systems and networks are subject to attacks both internally and externally. The increasingly frequent attacks on Internet-visible systems could be attempts to steal your company jewels, personal employee and customer information or use of your computer resources. Intrusion detection systems collect information from a variety of vantage points within the operating systems and networks.

Network Vulnerability Assessment

- This session will examine intrusion-detection and vulnerability-assessment technologies that will allow your organization to protect the enterprise from losses associated with network security problems. We will review how intrusion detection and vulnerability assessment products fit into the overall security architecture; case histories; and product features.

Objectives

- At the conclusion of this session, attendees should be better able to:
  - Define key concepts in intrusion detection
  - Explain what intrusion is
  - Identify standard security architectures
  - Answer frequently asked questions on security measures

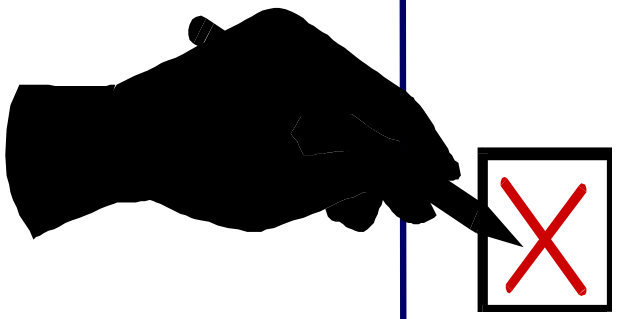
Objectives (continued)

- At the conclusion of this session, attendees should also be better able to:
  - Explain IDS features and functions
  - Examine where to find additional information
  - Identify who are the current IDS players

Format

- This workshop has been developed for you.
- Please feel free to:
  - ask questions
  - offer advise
  - provide observations
  - participate

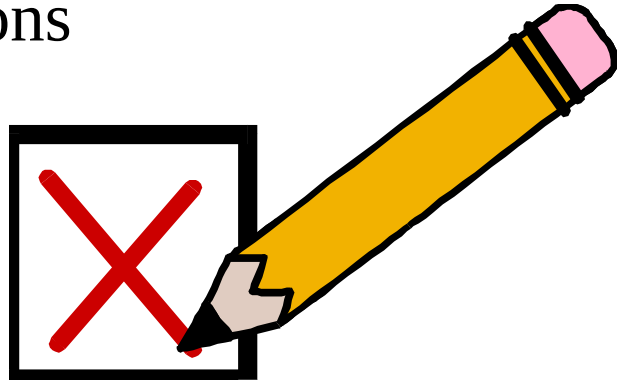
Agenda



- Intrusion Detection Introduction
- Definition of Key Concepts
- Intrusion Detection Functions
- Why IDS is Believed to be Necessary
- What IDS can do
- What IDS Cannot do

Agenda (continued)

- Frequently Asked Questions
- Vulnerability Assessment Products
- IDS Features and Functions
  - Application-based
  - Host-based
  - Target-based
  - Network-based
  - Batch or Interval Orientated
  - Real Time



Agenda (continued)

- IDS Features and Functions
  - Location of Analysis
- Types of Analysis
  - Signature
  - Statistical
  - Integrity
- Products and Vendors

Intrusion Detection

Introduction

- Intrusion detection systems help computer systems prepare for and deal with attacks.
- They collect information from a variety of vantage points within computer systems and networks, and analyze this information for symptoms of security problems.
- Vulnerability Assessment systems check systems and networks for system problems and configuration errors that represent security vulnerabilities.
- Both intrusion detection and vulnerability assessment technologies allow organizations to protect themselves from losses associated with network security problems.

Intrusion Detection (continued)

- Protecting critical information systems and networks is a complex operation, with many tradeoffs and considerations.
- The effectiveness of any security solution strategy depends on selecting the right products with the right combination of features for the system environment one wishes to protect.
- In this session, we will provide the information needed to make informed decisions regarding intrusion detection systems.

Definitions

- ***Network Security*** is the property of computer systems and networks that specifies that the systems in question and their elements can be trusted to act as expected in safeguarding their owners' and users' information.
- The goals of security include:
  - confidentiality (ensuring only authorized users can read or copy a given file or object),
  - *control* (only authorized users can decide when to allow access to information),
  - *integrity* (only authorized users can alter or delete a given file or object),
  - *authenticity* (correctness of attribution or description),
  - *availability* (no unauthorized user can deny authorized users timely access to files or other system resources), and
  - *utility* (fitness for a specified purpose).

Definitions

- ***Intrusion Detection*** systems collect information from a variety of system and network sources, then analyze the information for signs of intrusion (attacks coming from outside the organization) and misuse (attacks originating inside the organization.)
- ***Vulnerability Assessment (scanners)*** performs rigorous examinations of systems in order to locate problems that represent *security vulnerabilities.*
- ***Security vulnerabilities*** are features or errors in system software or configuration that increase the likelihood of damage from attackers, accidents or errors.

Definitions

- ***Security Policy*** is the statement of an organization's posture towards security. It states what an organization considers to be valuable, and specifies how the things of value are to be protected.
  - In practical use, security *policies* are coarse grained (*i.e.*, generalized statements that apply to the organization as a whole) and drive finer-grained *procedures*, *guidelines*, *and practices*, which specify how the policy is to be implemented at group, office, network, and system, and user levels.

Definitions

- ***Security infrastructure*** is the complement of measures, ranging from policy, procedures, and practices to technologies and products that represent an organization's security initiative.
- The goals of security counter-measures are to:
  - *prevent* problems from occurring;
  - *detect* when problems occur;
  - *contain* damage; and
  - *recover* from the effects of error and attack.
- From this perspective, vulnerability assessment and intrusion detection are necessary parts of the security infrastructure but do not, by themselves, represent a complete security infrastructure.

What is Intrusion Detection?

- Intrusion detection systems help computer systems prepare for and deal with attacks.
- They accomplish this goal by collecting information from a variety of system and network sources, then analyzing the information for symptoms of security problems.
- In some cases, intrusion detection systems allow the user to specify real-time responses to the violations.

What is Intrusion Detection?

Intrusion detection systems perform a variety of functions:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis for abnormal activity patterns
- Operating system audit trail management, with recognition of user activity reflecting policy violations

What is Intrusion Detection?

- Some systems provide additional features, including:
  - Automatic installation of vendor-provided software patches
  - Installation and operation of decoy servers to record information about intruders.
- These features combined allow system managers to more easily handle the monitoring, audit, and assessment of systems and networks.
- Ongoing assessment and audit activity is a necessary part of sound security management practice.

Intrusion Detection

- **Products Can Be Successfully Deployed in Operational Environments**
- The objective of intrusion detection and vulnerability assessment is to make complex, tedious, and sometimes virtually impossible system security management functions possible for those who are not security experts.
- Products are therefore designed with user-friendly interfaces that assist system administrators in their installation, configuration, and use.

Intrusion Detection (continued)

- **Products Can Be Successfully Deployed in Operational Environments**
- Most products include information about the problems they discover, including how to correct these problems, and serve as valuable guidance for those whom need to improve their security skills.
- Many vendors provide ***consulting and integration*** services to assist customers in successfully using their products to achieve their security goals.

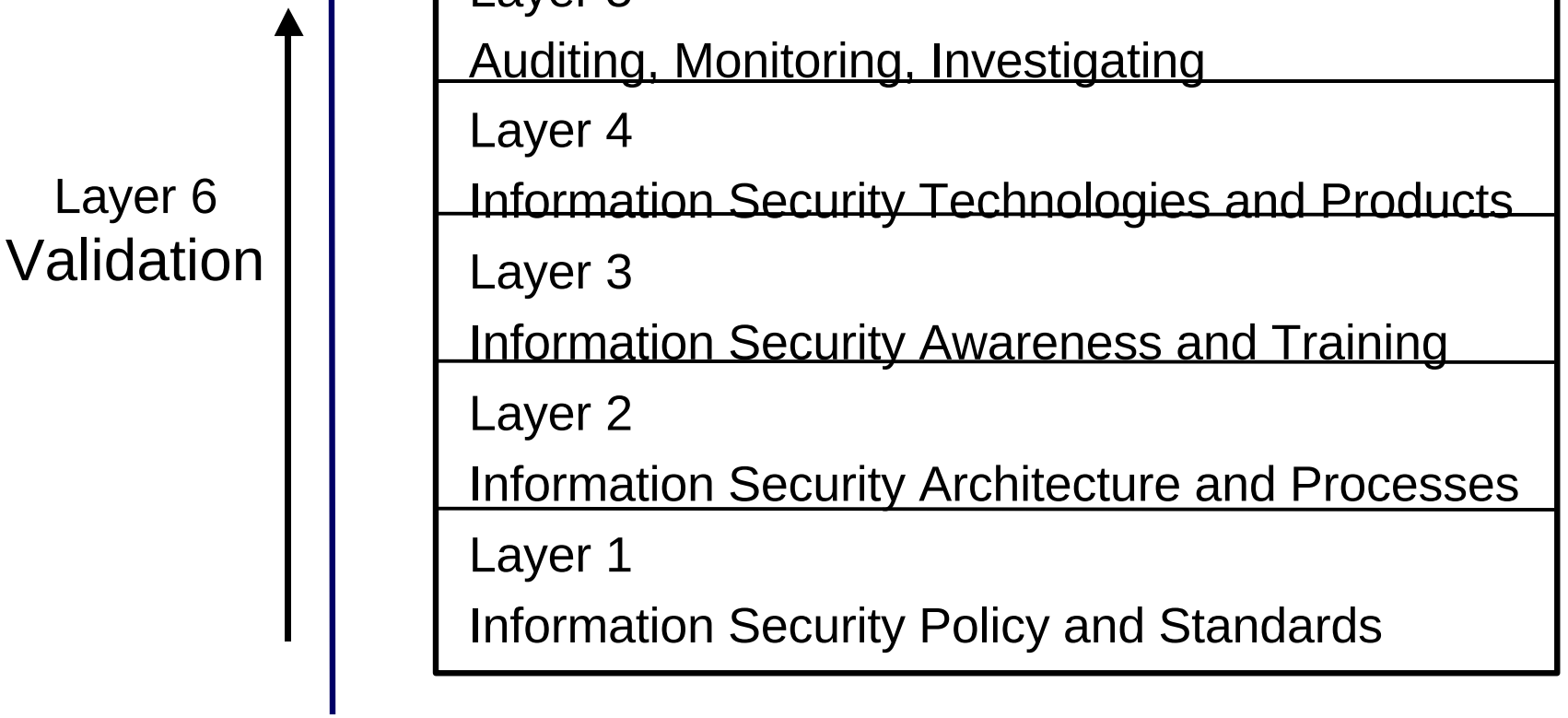
Network Security Management

- Network Security Management is a process in which one establishes and maintains policies, procedures, and practices required for protecting networked information system assets.
- Intrusion Detection and Vulnerability Assessment products provide capabilities needed as part of sound Network Security Management practice.

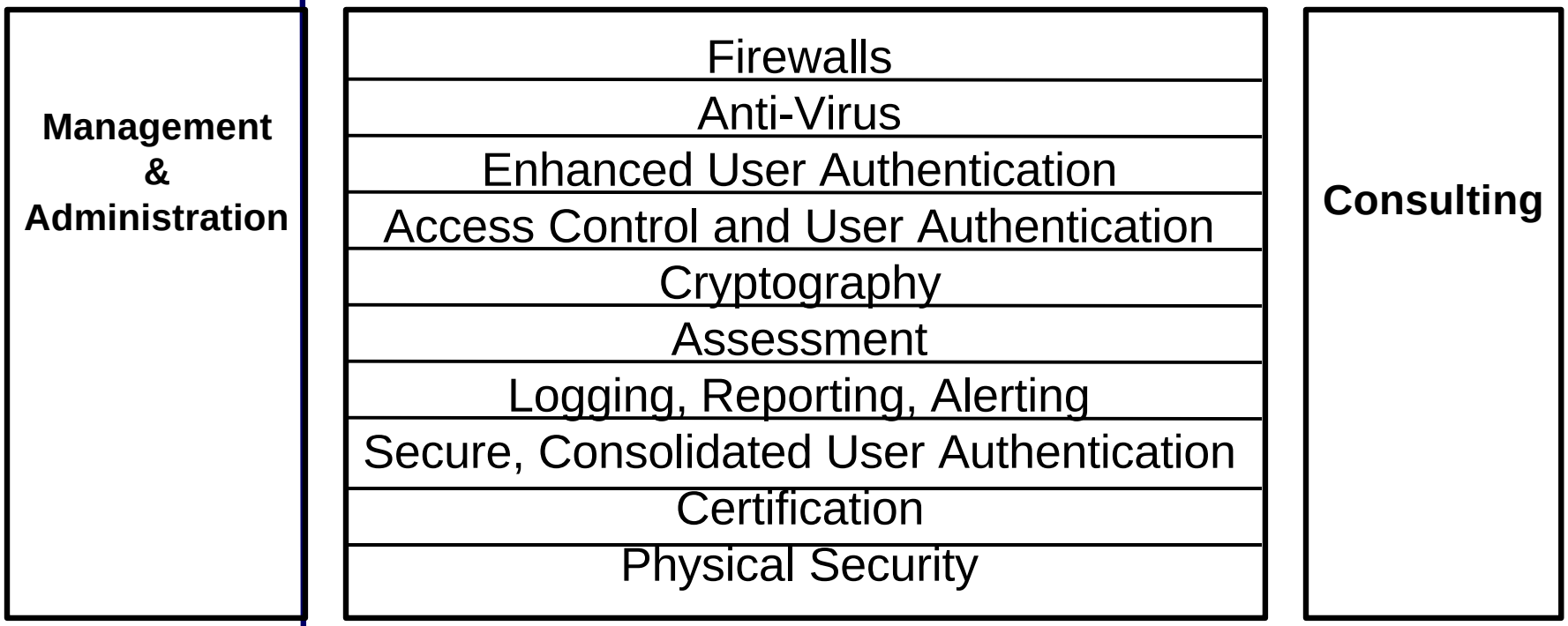
Intrusion Detection

- **The Security Hierarchy**
- The following diagram outlines an Information Security Hierarchy. It outlines the security measures that comprise the foundation for any security technology.
- Note that in order to achieve enterprise-wide security results, Layers 1-3 must exist in order for the technologies and products in Layer 4 to be effective.

Intrusion Detection



Intrusion Detection



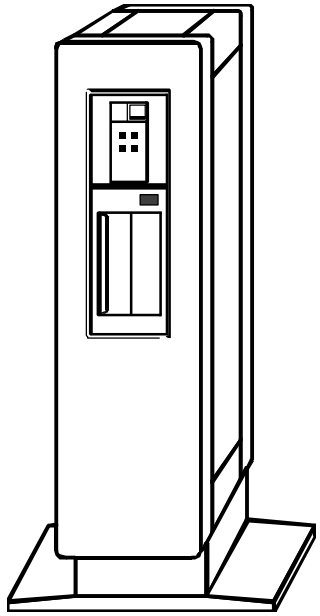
Why Firewalls aren't enough

- A common question is how intrusion detection complements firewalls. One way of characterizing the difference is provided by classifying security violation by *source*—whether they come from outside the organization's network or from within.

- Firewalls act as a barrier between corporate (internal) networks and the outside world (Internet), and filter incoming traffic according to a security policy.

Intrusion Detection

- **Why Firewalls aren't enough**
- This is a valuable function and would be sufficient protection were it not for these facts:
  - Not all access to the Internet occurs through the firewall.
  - Not all threat originates outside the firewall
  - Firewalls are subject to attack themselves



Intrusion Detection

- **Who Guards the Guard?**
- Another area of discussion when considering the value of intrusion detection systems is the need to monitor the rest of the security infrastructure.
- Firewalls, identification and authentication (I & A) products, access control products, virtual private networks, encryption products, and virus scanners all perform functions essential to system security.

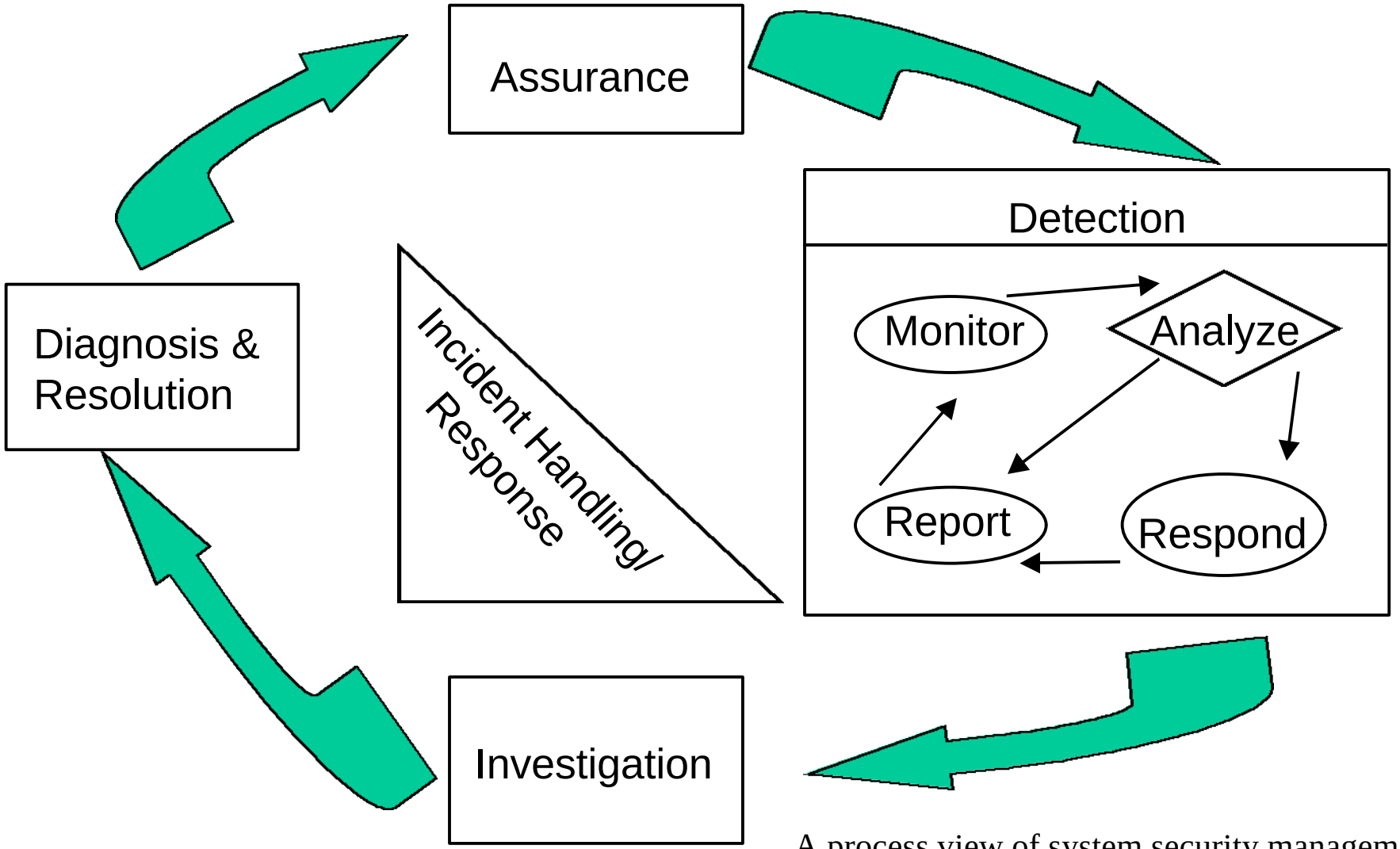
Who Guards the Guard? (continued)

- Given their vital roles, however, they are also prime targets of attack by adversaries.
- On a less sinister note, they are also managed by mere mortals, and therefore subject to human error.
- Whether due to configuration problems, outright failure, or attack, the failure of any of these components of the security infrastructure jeopardizes the security of the systems they protect.

Intrusion Detection

Who Guards the Guard? (continued)

- By monitoring the event logs generated by these systems, as well as monitoring the system activities for signs of attack, intrusion detection systems provide an added measure of integrity to the rest of the security infrastructure.
- Vulnerability assessment products also allow system management to test new configurations of the security infrastructure for flaws and omissions that might lead to problems.



A process view of system security management

Intrusion Detection

- **DEBUNKING MARKETING HYPE**
- Every new market suffers from exaggeration and misconception. Some of the claims made in marketing materials are reasonable and others are misleading.

- Let’s look at how to interpret intrusion detection marketing literature.

Intrusion Detection

Realistic benefits

- Intrusion detection systems, because they monitor the operation of firewalls, encrypting routers, key management servers and files critical to other security mechanisms, 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. Intrusion detection systems can recognize these first hallmarks of attack, and potentially respond to them, mitigating damage.
- In addition, when these devices fail, due to configuration, attack, or user error, intrusion detection systems can recognize the problem and notify the right people.

Intrusion Detection

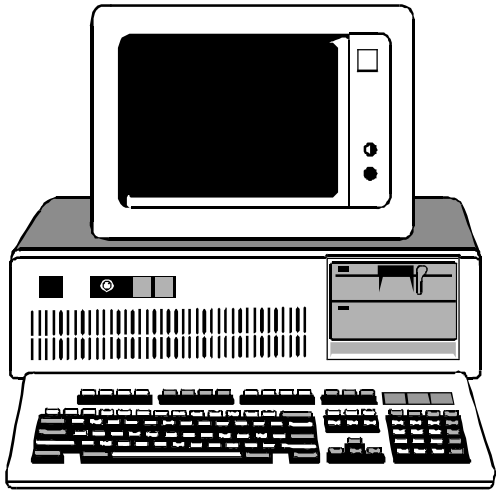
Intrusion detection systems can:

- make sense of often obtuse system
- trace user activity from point of entry to point of exit or impact
- recognize and report alterations to data files
- spot errors of your system configuration that have security implications, sometimes correcting them if the user wishes
- recognize when your system appears to be subject to a particular attack.
- relieve your system management staff of the task of monitoring the Internet searching for the latest hacker attacks

Intrusion Detection

Intrusion detection systems can also:

- make the security management of your systems by non-expert staff possible.
- provide guidelines that assist you in the vital step of establishing a security policy for your computing assets.



Intrusion Detection

Unrealistic expectations

- ***They are not silver bullets***
  - Security is a complex area with myriad possibilities and difficulties.
  - In networks, it is also a “weakest link” phenomenon—i.e., it only takes one vulnerability on one machine to allow an adversary to gain entry and potentially wreak havoc on the entire network. The time it takes for this to occur is also minuscule.
  - There are no magic solutions to network security problems, and intrusion detection products are no exception to this rule. However, as part of a comprehensive security management they can play a vital role in protecting your systems.

Intrusion Detection

Intrusion detection systems cannot:

- compensate for weak identification and authentication mechanisms
- conduct investigations of attack without human intervention
- provide insight to the contents of your organization security policy
- compensate for weakness in network protocols

Intrusion Detection

Intrusion detection systems cannot:

- compensate for problems in the quality or integrity of information the system provides
- analyze all of the traffic on a busy network
- always deal with problems involving packet-level attacks
- deal with modern network hardware features

Case 1: Integrity Analysis

In 1996, one of the early online web-based stock trading sites was placed in full operation, and was infiltrated by an outside attacker. The trading system consisted of approximately twenty web servers connected to a central database server. When the system manager realized that an attacker was on the loose inside the firewall, and was actively logging into the server, there was an understandable amount of alarm.

Case 1: Integrity Analysis (continued)

- In situations like this, damage containment should be the first priority. However, in this case, shutting down or disconnecting all the web servers from the Internet was not an acceptable option.
- First, doing so would constitute a “trading halt” event, and would cause the corporation to be fined in 15-minute increments by the SEC.
- Second, the damage to reputation caused by a shutdown would be extremely high, as would the damage associated with the possibility of word leaking out that an intruder had successfully broken into the system.

Intrusion Detection

- **Case 1: Integrity Analysis (continued)**
  - Because the system manager had already deployed a product using integrity analysis, it was possible to ascertain quickly which machines were compromised and to determine the scope of the infiltration. The customer computed that they saved about 260 hours of system administration time, in a case where each minute was valued at an extreme premium. Time is critical when an attacker is on the loose in your network.

Intrusion Detection

- **Case 1: Integrity Analysis (continued)**
  - This story ends happily. Only a fraction of the machines were compromised, and were promptly shut down. The database server was found to be intact, which allowed the web site to continue functioning on the remaining web servers. The system administration team conducted damage eradication and recovery at a more leisurely pace.

Intrusion Detection

Case 2: Vulnerability Assessment

A consulting company that does network design, security assessment and integration services is frequently called in when a company establishes or restructures a network. Their President says, “Many companies do not realize that when Windows NT is installed ‘out of the box,’ it’s designed to be wide open to allow for flexible network implementations. And it’s pretty difficult to get a global picture of your environment, because you have to go through a lengthy process of ‘machine by machine’, or ‘share by share’, or ‘domain by domain.’ They simply do not have the training, background and expertise to know what specific rights and permissions to turn off.”

Intrusion Detection

- **Case 2: Vulnerability Assessment (continued)**

  "We use a vulnerability assessment product combined with a network management product to help uncover information about user rights, permissions, account access, account restrictions, and users that have easily-guessed passwords. One eye-opening experience we found at a customer site was where someone with user privileges granted themselves administrator rights."

Intrusion Detection

- **Case 2: Vulnerability Assessment (continued)**

  "When we ran a user access report we found a user who had used a hack to make himself an administrator. To make matters worse, the account was active, and it belonged to a former employee that had been gone for two months. It would have taken us forever to find this situation because it is extremely time consuming to manually check each and every user account for security violations. But it is much easier with a vulnerability assessment product where information across an entire enterprise can be consolidated into one single report."

Intrusion Detection

Case 3: Host-based Intrusion Detection

In December 1998 a medium size California bank decided that they needed better control of their internal security. They needed both consistency in their security configurations as well as monitoring for suspicious behaviors from authorized users inside the system. They selected a host-based intrusion detection tool that also provided host-based assessment.

Case 3: Host-based Intrusion Detection (continued)

The agents were deployed to 10 servers and a handful of workstations. After installation, an audit policy was deployed that reduced the amount of data collected to a reasonable level. A detection policy was also established that matched the objective of monitoring for anomalous behavior. The security officer then used the assessment capabilities to bring all the servers up to a consistent level of security configuration that was acceptable to the security officer.

Intrusion Detection

Case 3: Host-based Intrusion Detection (continued)

Within 24 hours of initial monitoring, the security officer observed irregular use of 2 administrative accounts. They were being used to read mail and edit documents during regular working hours. The security policy specified that administrative accounts were only to be used for tasks requiring administrative privilege and were not to be used for daily activities such as reading mail. The employees who were using their admin accounts were reprimanded and the activity stopped.

Intrusion Detection

Case 3: Host-based Intrusion Detection (continued)

Within 48 hours of monitoring the security officer observed an unauthorized account using the backup software. The immediate security risk was that the backup software had privilege to read every file on the system bypassing all access control. The security officer called the account owner and quickly determined that the backup software had been installed under the wrong account, making this powerful software vulnerable to compromise. The software was re-installed under a better-protected account.

Case 3: Host-based Intrusion Detection (continued)

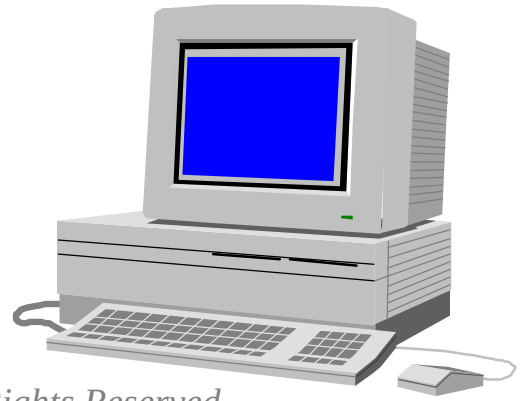
Within 72 hours of monitoring, the security officer observed regular account logins from a set of three accounts at 1:30 AM, 2:30 AM, and 3:30 AM. All the indications were that this was an automated program using these 3 accounts to login at the same time everyday. By using the data forensics capabilities of the intrusion detection tool, the security officer looked back over the last 3 days to determine other accesses and executions by these accounts during these times.

Case 3: Host-based Intrusion Detection (continued)

The next effort was to talk to the account owners to determine if they had knowledge of programs under their control during this time. Through a combination of analyzing the data and interviewing the end-users it was determined to be MAPI interactive logons for mail. This pattern is now recognized as authorized.

Frequently Asked Questions About Intrusion Detection

- *What is an Intrusion Detection System?*
  - An intrusion detection system monitors computer systems, looking for signs of intrusion (unauthorized users) or misuse (authorized users overstepping their bounds).



Frequently Asked Questions About Intrusion Detection

- *What does an Intrusion Detection System do?*
  - Intrusion Detection Systems monitor a variety of information sources from systems, analyzing this information in a variety of ways.
  - The first, most common, is that it compares this information to large databases of *attack signatures*, each reflecting an attempt to bypass or nullify security protections.
  - The second is that it looks for problems related to authorized users overstepping their permissions (e.g., a shipping clerk searching executive payroll records).
  - Finally, some intrusion detection systems perform statistical analysis on the information, looking for patterns of abnormal activity that might not fall into the prior two categories (e.g., accesses that occur at strange times, or an unusual number of failed logins.)

Frequently Asked Questions About Intrusion Detection

- *But we already have a firewall–why do we need an intrusion detection system, too?*
  - The firewall is the security equivalent of a security fence around your property and the guard post at the front gate. It can keep the most unsavory of characters out, but cannot necessarily tell what is going on inside the compound. Intrusion detection systems are the equivalent of multi-sensor video monitoring and burglar alarm systems. They centralize this information, analyze it for patterns of suspicious behavior in much the same way a guard at a monitoring post watches the feeds from security cameras, and in some cases, deals with problems they detect. Most loss due to computer security incidents is still due to insider abuse. Intrusion detection systems, not firewalls, are capable of detecting this category of security violation.
  - Perhaps more importantly, firewalls are subject to circumvention by a variety of well-known attacks.

Frequently Asked Questions About Intrusion Detection

- *What can an intrusion detection system catch that a firewall can't?*
  - Firewalls are subject to many attacks. The two considered most worrisome are tunneling attacks and application-based attacks.
  - Tunneling attacks arise due to a property of network protocols. Firewalls filter packets, and make pass/block decisions based on the network protocol. Rules typically check a database to determine whether a particular protocol is allowed, if so, the packet is allowed to pass. This represents a problem when an attacker masks traffic that should be screened by the firewall by encapsulating it within packets corresponding to another network protocol.

Frequently Asked Questions About Intrusion Detection

- *What can an intrusion detection system catch that a firewall can't?*
  - Application-based attacks refer to the practice of exploiting vulnerabilities in applications by sending packets that communicate directly with those applications.
  - Therefore, one could exploit a problem with Web software by sending an HTTP command that exercises a buffer overflow in the web application. If the firewall is configured to pass HTTP traffic, the packet containing the attack will pass.

Frequently Asked Questions About Intrusion Detection

- *We've invested in a lot of security devices for our network resource source. We have token-based Identification and Authentication, we require our employees to encrypt their e-mail, have firewalls, require users to use good passwords and change them often why do we need intrusion detection, too?*
  - Even when you have a great existing security infrastructure, you still need the added assurance that intrusion detection systems provide. No matter how well designed the security point products, they are still subject to failure, due to hardware or software anomalies or user problems. Users sometime nullify the protection afforded by the products by disabling or bypassing them. Intrusion detection systems, because they are capable of monitoring messages from the other pieces of the security infrastructure, are able to detect when failure occurs. In some cases, they can tell you what happens until someone can restore them to service.

Vulnerability Assessment Products

- *What are Vulnerability Assessment Products?*
  - Vulnerability Assessment Products, also known as "Vulnerability Scanners," are software products that perform security audits on systems, searching for signs that the systems being scanned are vulnerable to certain systems attacks.
- *How do they work?*
  - Vulnerability Assessment Products take two approaches to locating and reporting security vulnerabilities. The first approach, a "passive" scan, inspects system settings such as file permissions, ownership of critical files, path settings, etc., for configurations that, in the past, have lead to security problems. The second approach, an "active" scan, actually reenacts a series of known hacker attacks, recording the results of the attacks. Some products also perform password cracking on password files to discover bad/weak passwords that might be easily guessed by hackers. Finally, the products record their findings in a result screen and in a report mechanism.

Vulnerability Assessment Products

- *What is the value added in Vulnerability Assessment Products?*
  - Vulnerability Assessment Products are a valuable part of any organization's system security management program.
  - They allow system managers to baseline the security of a new system.
  - They allow periodic security audits to determine the security health of a system at a given time.
  - Many of them provide the ability to perform "differential analysis" by archiving the results of scans, then comparing subsequent scans to the archives, reporting when new vulnerabilities or unexpected changes appear.

Technical Concepts and Definitions

- Intrusion Detection Systems are security management tools that:
  - Collect information from a variety of system sources,
  - Analyze that information for patterns reflecting misuse or unusual activity,
  - In some cases, automatically respond to detected activity, and
  - Report the outcome of the detection process.

IDS Features and Functions

- Application-based
  - Application-based intrusion detection sensors collect information at the application level. Examples include logs generated by database management software, web servers, or firewalls. With the proliferation of Web-based electric commerce, security will increasingly focus on interactions between users and application programs and data.
- Advantages of application-level monitoring
  - This approach allows targeting of finer-grained activities on the system (e.g. one can monitor for a user utilizing a particular application feature.)
- Disadvantages
  - Applications-layer vulnerabilities can undermine the integrity of application-based monitoring and detection approaches.

IDS Features and Functions

- **Host-based**
  - Host-based intrusion detection agents (also called *sensors)* collect information reflecting the activity that occurs on a particular system. This information is sometimes in the form of operating-system audit trails. It can also include system logs, other logs generated by operating system processes, and contents of system objects not reflected in the standard operating system audit and logging mechanisms.

IDS Features and Functions

- **Advantages of Host-based Systems**
  - can monitor information access in terms of "who accessed what"
  - can map problem activities to a specific userid
  - can track behavior changes associated with misuse
  - can operate in encrypted environments
  - can operate in switched network environments
  - can distribute the load associated with monitoring across available hosts on large networks, thereby cutting deployment costs

IDS Features and Functions

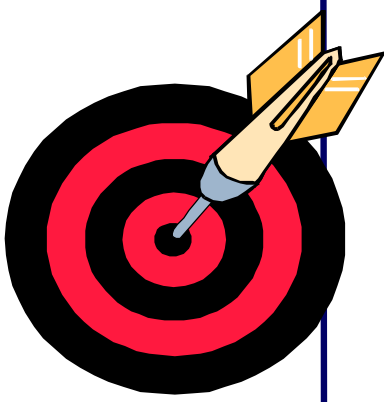
- **Disadvantages of Host-based Systems**
  - Network activity is invisible to host-based detectors
  - Running audit mechanisms can incur additional resource overhead
  - When audit trails are used as data sources, they can take up significant storage
  - Operating system vulnerabilities can undermine the integrity of host-based agents and analyzers
  - Host-based agents must be more platform-specific, which adds to deployment costs
  - Management and deployment costs are usually greater than in other approaches

IDS Features and Functions

- **Target-Based Approaches**
  - Integrity analysis enables one to implement a focused and effective monitoring strategy for systems in which data integrity and process integrity are of primary concern. This approach monitors specific files, system objects and system object attributes for change, looking at the *outcome* of attack processes rather than the *details* of the attack processes. Some systems use *checksums* (computations whose value depends on the original constitution of the system object) to detect breaches of integrity.

IDS Features and Functions

- **Advantages of Target-Based Approaches**
  - Because it does not depend on historical records of behavior, integrity analysis may detect intrusions that other methodologies do not;
  - This approach allows reliable detection of both placement and presence of attacks that modify the system (e.g., Trojan horses);
  - Because its footprints and intrusiveness are low, this approach can be useful for monitoring systems with modest processing or communications bandwidth;
  - This approach is effective for determining which files need to be replaced in order to recover a system, rather than reinstalling everything from the original source or backup, as is often done.



IDS Features and Functions

- **Disadvantages of Target-Based Approaches**
  - Depending on the number of files, system objects and object attributes for which checksums are computed, this approach may still levy an appreciable processing load on low-end systems;
  - The approach is not well suited to real-time detection processes, as it monitors for the outcome of attacks, not for the attacks themselves while they are in progress.

IDS Features and Functions

- **Network-based**
  - Network-based intrusion detection sensors collect information from the network itself. This information is usually gathered by packet sniffing, using network interfaces set in promiscuous mode; however, some agents are integrated in network hardware devices.
- Advantages:
  - The data come without any special requirements for auditing or logging mechanisms; in most cases collection of network data occurs with the configuration of a network interface card.
  - The insertion of a network-level agent does not affect existing data sources.
  - Network-level agents can monitor and detect network attacks. (e.g., SYN flood and packet storm attacks).

IDS Features and Functions

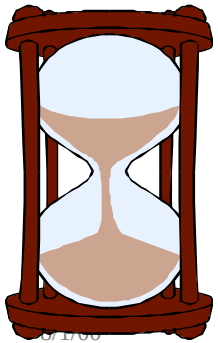
- **Disadvantages of Network-based**
  - Although some network-based systems can infer from network traffic what is happening on hosts, they cannot tell the outcome of commands executed on the host. This is an issue in detection, when distinguishing between user error and malfeasance.
  - Network-based agents cannot scan protocols or content if network traffic is encrypted.
  - Network-based monitoring and intrusion detection becomes more difficult on modern switched networks. Switched networks establish a network segment for each host; therefore, network-based monitors are reduced to monitoring a single host. Network switches that support a monitoring or scanning port can at least partially mitigate this issue.
  - Current network-based monitoring approaches cannot handle high-speed networks.

IDS Features and Functions

- **Integrated approaches**
  - Some intrusion detection products combine application, host, and network-based sensors.
- Advantages:
  - As agents at applications, host, and network levels are used, the system can target activity at any or all levels.
  - It is easier to see patterns of attacks over time and across the network space; this assists in damage assessment and system recovery; it also aids in investigating the incident and pursuing legal remedies (e.g. criminal prosecutions).
- Disadvantages:
  - There are no industry standards on interoperability of intrusion detection components; therefore it is difficult or impossible to integrate components from different vendors.
  - Integrated systems are more difficult to manage and deploy.

IDS Features and Functions

- **Timing of Information Collection and Analysis**
  - Once the *location(s)* of intrusion detection system agents are established, the *timing* of the information collection and analysis are of interest.
- **Batch or Interval Oriented**
  - In batch-oriented (also called *interval-oriented)* approaches, operating-system audit mechanisms or other host-based agents log event information to files and the intrusion detection system periodically analyzes these files for signs of intrusion or misuse.



IDS Features and Functions

- **Advantages of Batch or Interval Oriented (continued)**
  - They are well suited to environments in which threat levels are low and single-attack loss potentials high (e.g., financial institutions). In these environments, users are often more interested in establishing accountability for problems than immediately responding to suspected incidents. In this situation, batch-oriented analysis will likely be combined with other investigative process in order to identify the person responsible for the incident and support criminal prosecution for the incident.
  - Batch mode analysis schemes impose less processing load on systems than real-time analysis, especially when collection intervals are short and data volumes are therefore low.

IDS Features and Functions

- **Batch or Interval Oriented**
- Advantages:
  - Batch-oriented collection and analysis of information are particularly well suited to organizations in which system and personnel resources are limited. Organizations that have no full-time security personnel may find that real-time alarms generated by intrusion detection systems are seldom used. In such circumstances, it makes little sense to tolerate the processing load associated with real-time analysis and alarms.
  - Attacks on computer systems often involve repetitive attacks on the same targets. For example, an attacker may enter a system via a password-grabbing attack, then install a Trojan horse “back door” in order to return later and continue the attack. Batch-mode analysis can usually recognize such *attack signatures.*

IDS Features and Functions

- **Advantages of Batch or Interval Oriented (continued)**
  - Many current legal practices relating to computer evidence were established with batch-mode collection and manual analysis in mind. Therefore, it may be easier to submit system logs collected and processed in batch mode as evidence.
- **Disadvantages of batch-mode analysis**
  - Users will seldom see incidents before they are complete.
  - Therefore, there is virtually no possibility of actively countering incidents as they happen in an attempt to minimize damage.
  - The aggregation of information for batch-mode analysis consumes more disk storage on the analysis system. This can result in huge amounts of data for enterprise networks.

IDS Features and Functions

- **Real Time**
  - Real time systems provide information collection, analysis, and reporting (with possible responses) on a continuous basis.
  - The term “real-time” is used here as in process-control systems; that is, the detection process happens quickly enough to hinder the attack.
  - Real-time systems provide a variety of real-time alarms (many support off-site alarming mechanisms such as e-mail, pagers, and telephone messaging), as well as automatic responses to attacks.
  - Typical responses range from simple notification to increasing the sensitivity of the monitoring, terminating the network connection from the source of the attack or changing system settings to limit damage.

IDS Features and Functions

- **Advantages of Real Time**
  - Depending on the speed of the analysis, attacks may be detected quickly enough to allow system administrators to interrupt them;
  - Depending on the speed and sensitivity of the analysis, system administrators may be able to perform incident handling (leading to recovery of system operations) more quickly;
  - In cases that occur on systems where legal remedies are available, system administrators may be able to collect information that allows more effective identification and prosecution of intruders.

IDS Features and Functions

- **Disadvantages of Real Time**
  - They tend to consume more memory and processing resource on the analysis system than *post facto* systems;
  - There are serious legal issues associated with automated responses that attempt to harm the attacking systems, a feature associated with some real-time systems;
  - Configuration of real-time systems is critical; a badly formed signature can generate so many false alarms that a real attack goes unnoticed.

IDS Features and Functions

- **Location of Analysis**
  - As in sensors, analysis functions can reside at host-level, at network-level, or both. Performing analysis strictly at the host level has the advantage of minimizing network load.
  - However, it has the disadvantage of not allowing the detection of broad scale attacks targeting a network of machines (for instance, an attacker sequentially hopping through a network performing brute force password guessing against each host).

IDS Features and Functions

- **Location of Analysis**
  - Consolidating raw data and performing analysis strictly at the network level (in the case of systems with sensors at both host and network levels) offer the capability to detect attacks that involve more than one host on the network. The disadvantage to this approach is that the network load associated with transferring raw host-level information to the analysis engine can be crippling.
  - As in sensor placement, the optimal strategy for performing analysis of logs is one in which analysis is done at both host and network levels.
    - The analysis done at the host level can be simple or extensive depending on the nature of the sensor information generated in that host or the signature against which the information is matched.

IDS Features and Functions

- The network-level analysis can take the results from the host-level analysis and use it to detect signs of network-wide attack or suspicious behavior without incurring as heavy a network load.

– In larger networks, this sort of approach can be applied hierarchically:
  - Groups of hosts can report to a network analysis engine, which in turn reports its results to another analysis engine that collects results from a number of other network analysis engines and so on.
  - This hierarchical structure lets intrusion-detection products succeed even in larger organizations.

IDS Features and Functions – Types of Analysis

- **Signature analysis**
- Signatures are patterns corresponding to known attacks or misuses of systems. They may be simple (character string matching looking for a single term or command) or complex (security state transition written as a formal mathematical expression). In general a signature can be concerned with a process (the execution of a particular command) or an outcome (the acquisition of a root shell.)
- Signature analysis is pattern matching of system settings and user activities against a database of known attacks. Most commercial intrusion detection products perform signature analysis against a vendor-supplied database of known attacks. Additional signatures specified by the customer can also be added as part of the intrusion detection system configuration process. Most vendors also include periodic updates of signature databases as part of software maintenance agreements.

IDS Features and Functions – Types of Analysis (continued)

One advantage of signature analysis is that it allows sensors to collect a more tightly targeted set of system data, thereby reducing system overhead. Unless signature databases are unusually large (say hundreds of thousands or millions of complex signatures), signature analysis is usually more efficient than statistical analysis due to the absence of floating point computations.

IDS Features and Functions – Types of Analysis (continued)

- **Statistical analysis**
  - Statistical analysis finds deviations from normal patterns of behavior. This feature, common in research settings, is found in few commercial intrusion detection products. Statistical profiles are created for system objects (e.g., users, files, directories, devices, etc.) by measuring various attributes of normal use (e.g., number of accesses, number of times an operation fails, time of day, etc.). Mean frequencies and measures of variability are calculated for each type of normal usage. Possible intrusions are signaled when observed values fall outside the normal range. For example, statistical analysis might signal an unusual event if an accountant who had never previously logged into the network outside the hours of 8 AM to 6 PM were to access the system at 2 AM.

IDS Features and Functions – Types of Analysis (continued)

- **Statistical analysis**
- The advantages of statistical analysis are:
  - The system may detect heretofore unknown attacks;
  - Statistical methods may allow one to detect more complex attacks, such as those that occur over extended periods.
- Disadvantages of statistical analysis (at this time) are:
  - It is relatively easy for an adversary to trick the detector into accepting attack activity as normal by gradually varying behavior over time;
  - The possibility of false alarms is much greater in statistical detectors; Statistical detectors do not deal well with changes in user activities (e.g., when the manager assumes the duties of a subordinate in an emergency). This rigidity can be a problem in organizations where change is frequent. This can result in both false alarms and false negatives (missed attacks).

IDS Features and Functions – Types of Analysis (continued)

- **Integrity analysis**
  - Integrity analysis focuses on whether some aspect of a file or object has been altered. This often includes file and directory attributes, content and data streams. Integrity analysis often utilizes strong cryptographic mechanisms, called *message digest (*or *hash) algorithms,* which can recognize even subtle changes.
- Advantages:
  - Any successful attack where files were altered, network packet grabbers were left behind, or root-kits were deployed will be detected regard-less of whether or not the attack was detected by signature or statistical analysis.
- Disadvantages:
  - Because current implementations tend to work in batch mode, they are not conducive to real-time response.

Summary and Conclusion

- **Wide range of goals for product users**
  - Users of intrusion detection products span public and private institutions, running the gamut of industries. The goals realized by users of intrusion detection systems include:
    - Support of internal audit
    - Control of liability exposure
    - Incident handling and investigative support
    - Improved damage assessment and recovery
    - Improved security management process
    - Discovery of new problems/issues before damage occurs
    - Documentation of compliance with legal and statutory requirements
    - Recovery of systems suffering security violations

Summary and Conclusion

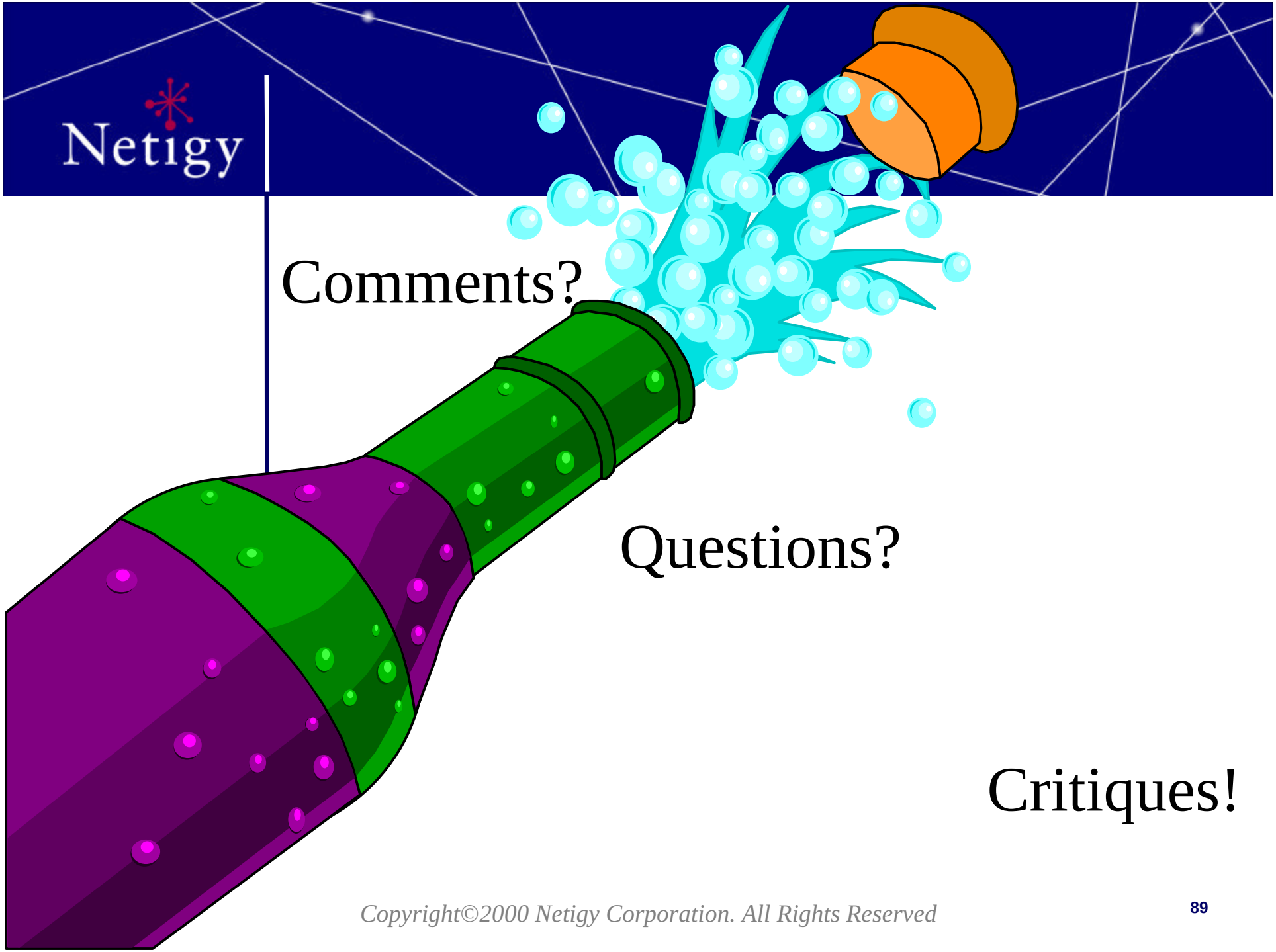
- **AXENT Technologies, Inc.** (www.axent.com)
- **BindView Development Corporation** (www.bindview.com)
- **Computer Associates Inc.** (www.cai.com)
- **Cybersafe Corporation** (www.cybersafe.com)
- **IBM** (www.ers.ibm.com)
- **Internet Security Systems, Inc.** (www.iss.net)
- **Network Associates, Inc.** (www.nai.com)
- **Qwest Communications International, Inc.** (www.qwest.com)
- **RSA Security, Inc.** (www.rsasecurity.com)
- **Tripwire Security Systems, Inc.** (www.tripwiresecurity.com)

Summary

- We have discussed:
  - Key concepts in intrusion detection
  - What is intrusion detection
  - Standard security topologies
  - Frequently asked questions on security measures

Summary

- We have discussed:
  - IDS features and functions
  - Where to find additional information
  - Who are the current IDS players



Introduction to Intrusion Detection

Thomas R. Peltier, CISSP

Driving eBusiness Performance ***SM***