COM 5335 Network Security Lec 14 - Intrusion Detection & Prevention Systems

Scott CH Huang

Detecting an Intrusion?

- What is an intrusion?
  - It can be very hard to distinguish between genuine messages, failures and malicious activity
  - Consider an analogy
    - Someone points a flashlight at your house from the street
    - Is that an intrusion?
- A definition
  - An intrusion is a sequence of related actions by an attacker that results in the occurrence of unauthorized security threats to a target networking or computing domain

What is Intrusion Detection?

- It means many things to many people
  - Mathematical foundations of statistical processing of data
  - Firewall rules and filter policies
  - Methods of tracking and tracing attackers
  - Products and appliances that create alerts of suspicious network activity
- It is a fairly young field and is constantly developing
  - Hard to pin down what it exactly means

What is Intrusion Detection? (cont.)

- Process of identifying and responding to malicious activity targeting computing and networking resources
- Process
  - Involves people, technology and tools
  - Cannot work without involvement of human beings
- Identification
  - Temporal property - prior to, during or after the attack
- Response
  - After identification, what must be done?
    - Allow attack to proceed so Oscar can be traced,
    - Stop the attack to minimize damages, etc.

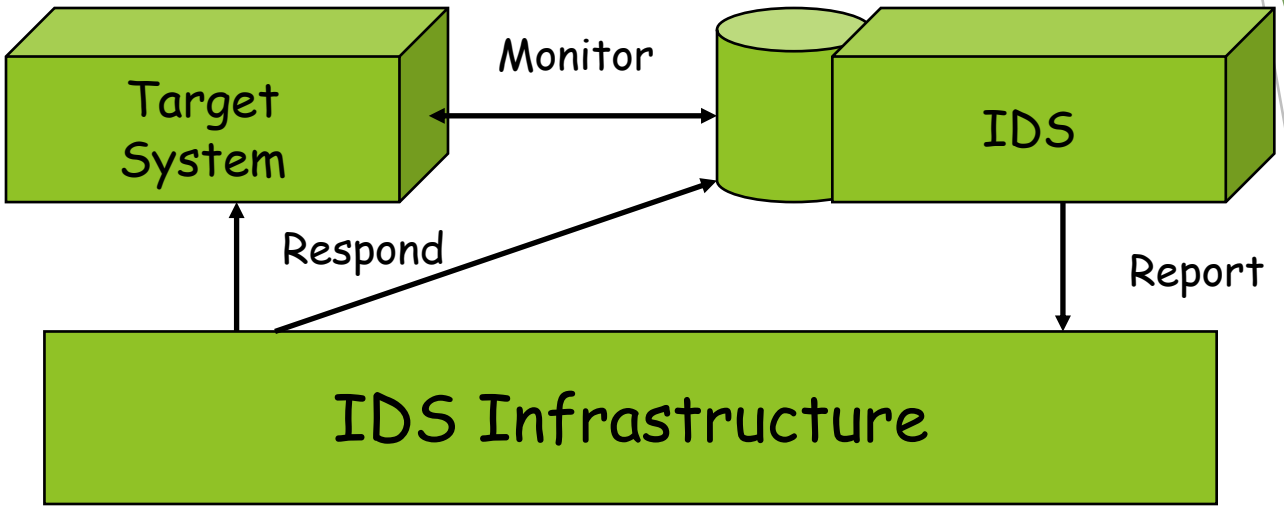
Why Intrusion Detection?

- You may never discover that your system/network has been attacked until it is too late
  - Can lead to loss of intellectual property, liability, etc.
- Helps you design better security for your system and patch vulnerabilities and loopholes rapidly
- Intrusion detection can
  - Detect reconnaissance, active attacks, etc.
  - Create alarms for security personnel to take action

IDS vs. Packet Filtering

- Packet filtering:
  - Operates on TCP/IP headers only
  - No correlation check among sessions
- IDS (Intrusion Detection System)
  - Deep packet inspection: look at packet contents (e.g., check character strings in packet against database of known viruses, attacks' strings)
  - Examine correlation among multiple packets
    - Port scanning
    - Network mapping
    - DoS attack

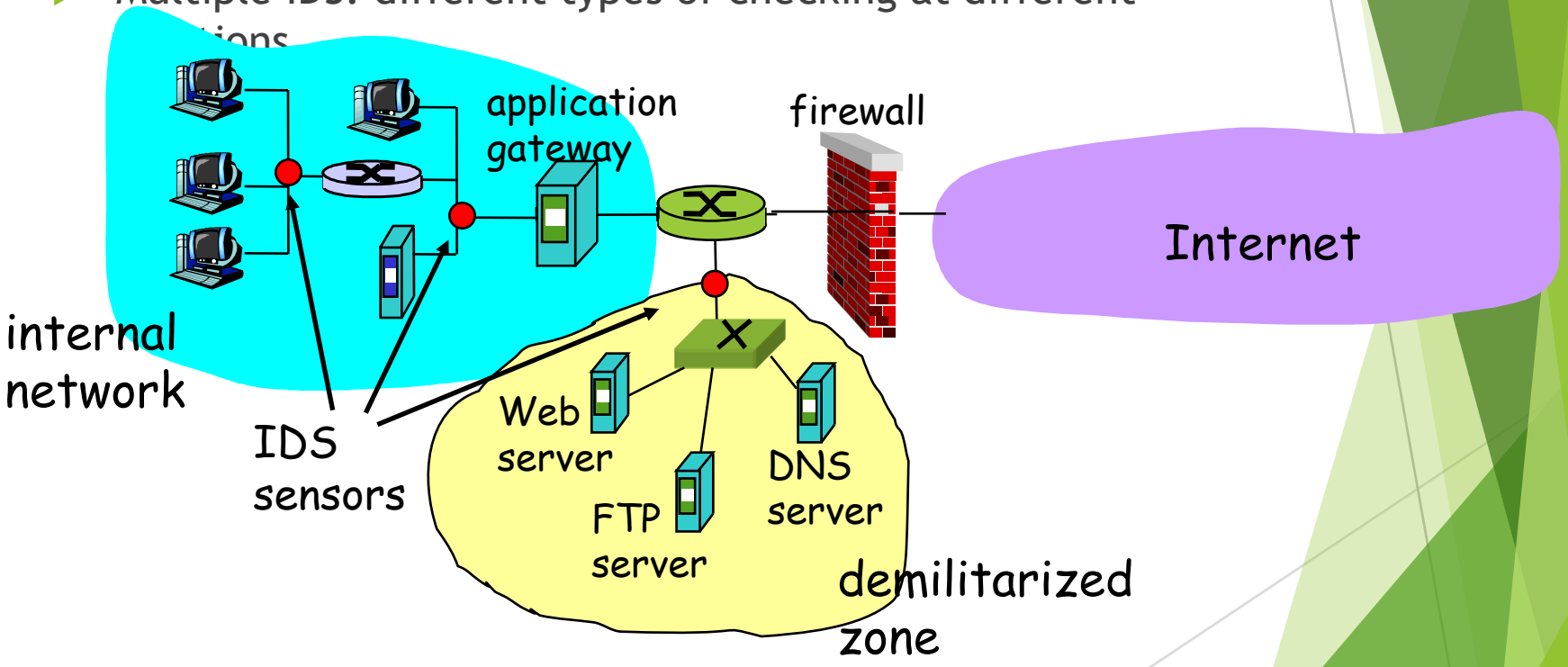
Basic Components of IDS



- Monitoring
  - IDSs examine and process data/information
  - Has technical and operational implications - timeliness, confidence in information, processing power required and so on
- Reporting
  - Monitored information has to be reported to an appropriate infrastructure
- Responding
  - Actions that are taken by the IDS to reduce security risks

Intrusion Detection and Prevention Systems

- Multiple IDS: different types of checking at different



IDSs – Classification

- Signature-based IDS
  - Maintains an extensive DB of attack signatures
  - Signature: Set of rules pertaining to an intrusion activity
    - e.g., a list of characteristics of a single packet, a series of packets
    - What can be a signature for port scanning attack?
- Statistical anomaly-based IDS
  - Understand patterns of normal usage and abnormal usage and flag potential problems

IDSs – Classification (cont.)

- Host-based IDS
  - System Centric
    - Use *Audit Trail Processing*, watch logins, catch Trojan code deployments
  - Deployed on target hosts
  - Source-based or Destination-based IDS
    - @Source: Ultimate goal of today's systems (not enough data!, e.g., DDoS)
    - @Destination: Too late! (Access to all the traffic)
- Network-based IDS
  - Parse packets that flow into/out of the network
    - Where: Internet access routers
    - Sometimes they are simply glorified sniffers
    - Goal: detect and respond ASAP and as near as possible to the source of the attack
  - Compare signatures of known attacks with sniffed packets and issue alerts

Audit Trail Processing

- Idea: Who did what?
  - Use system logs from various hosts and devices
  - Performed off-line (no real-time analysis)
  - Logs are parsed and information is processed
- Storage, processing and protection of audit data is important
  - Special audit probes may be installed on target systems
  - Potential issues are how the performance of the target may degrade because of the audit probes

On-the-Fly Processing

- Performs both real-time and non real-time analysis
  - Usually associated with network-based IDSs
  - Monitors and parses all packets
  - Looks for “dirty words” like /etc/passwd or \winnt\system32\config
  - Can use tcpdump and other sniffers in promiscuous mode to capture packets
- Issues
  - Buffering capacity may impact on whether all packets are captured and examined

Using Normal Behavior Profiles

- Idea
  - First capture expectations about user and system activity
  - Estimate initial profiles of normal activity
  - Keep refining the profiles with time (fine tuning)
  - Use all sources for profiling
    - Not just electronically available information
- Example:
  - A user that never logs in after 6.00 p.m. logs in at 1.00 a.m.
  - Other sources tell you that he is traveling to Malaysia

Using Abnormal Behavior Signatures

- Most common approach to intrusion detection
- Idea
  - Attack signatures are known like virus databases
    - Example: Smurf attack (what is the attack signature?)
  - Parse packets to see if they match any attack signature to detect intrusions
- Remarks
  - It is based on the knowledge of attack types (attack signatures) that IDS has. IDS can miss potential new attacks or variations of attacks!
  - Sometimes, suspicious strings are also matched

Some Simple Examples of Signatures

- LAND (Local Area Network Denial) Attack
  - This is a DoS attack where the source and destination IP addresses are identical
  - Someone may launch it from inside your network
- WinNuke
  - Sets the URG flag in TCP and sends a packet to port 139 on Windows systems causing them to crash
- Xmas Tree
  - TCP flags set to 1 (URG, PSH, FIN)
  - Also a DoS attack

Monitoring: tcpdump

- *tcpdump* allows you to monitor packets on the link in a network
  - It provides information based on the packets it sniffs
  - You need root access to sniff packets on a linux/unix/mac os X machine
  - There is a Windows equivalent called *windump*
- Idea
  - The NIC operates in a promiscuous mode capturing all packets, not just the ones intended for it

tcpdump: Details

- It produces one line of output for each frame that it picks up
- It has the following fields
  - Timestamp - the seconds field is reliable only up to 10s of ms
  - If IP, it shows the source and destination addresses as well as port numbers of TCP or UDP segments
  - Also interprets other types of frames like arp, ICMP, etc.
  - Attempts to interpret the payload to the extent possible
  - You can use filters to collect output selectively
- Example output
  - 17:26:11.679220 arp who-has 136.142.117.80 tell 136.142.117.1
  - 17:30:08.024113 IP 136.142.117.1 > all-systems.mcast.net: igmp query v2

tcpdump: Some Examples

- Example of TCP 3-Way Handshake

TCP SYN from 136.142.117.221 to netgroup-serv.polito.it Web Server

136.142.117.221.51144 > netgroup-serv.polito.it.http: S 3578668852:3578668852(0) win 65535 <mss 1460>

TCP SYNACK from netgroup-serv.polito.it back to 136.142.117.221

netgroup-serv.polito.it.http > 136.142.117.221.51144: S 4156350971:4156350971(0) ack 3578668853 win 64240 <mss 1460>

TCP ACK from 136.142.117.221 to netgroup-serv.polito.it

136.142.117.221.51144 > netgroup-serv.polito.it.http: . ack 1 win 65535 <nop,nop,timestamp 489021280 0>

- The example shows sequence numbers - starting and ending
- Sequence numbers change from absolute to relative values with the final ack packet of the handshake
- The port number used by the client 136.142.117.221 is 51144
- The server port number is 80 (http)

tcpdump: Some Examples (cont.)

- The following shows examples of sequence and ack numbers
  - 136.142.117.221.51144 > netgroup-serv.polito.it.http: P 1:568(567) ack 1 win 65535
  - netgroup-serv.polito.it.http > 136.142.117.221.51144: . 1:1449(1448) ack 568 win 63673
  - netgroup-serv.polito.it.http > 136.142.117.221.51144: . 1449:2897(1448) ack 568 win 63673
  - 136.142.117.221.51144 > netgroup-serv.polito.it.http: . ack 2897 win 65535
- ACK Scan - some fields removed
  - oscar.in > 136.142.117.221.23: . ack 456321003 win 2048
  - oscar.in > 136.142.117.201.23: . ack 456321003 win 2048
  - oscar.in > 136.142.117.221.53: . ack 456321003 win 2048

tcpdump: Remarks

- Analysis of *tcpdump* output
  - Knowing some of the attacks discussed in class, you should be able to figure out if a certain set of packets could be a potential attack
- Questions to ask
  - What are the source and destination IP addresses?
  - What protocol is it (ICMP, TCP, UDP, arp, etc.)?
  - Is it reasonably normal behaviour?
    - e.g., TCP shows a proper 3-way handshake, icmp echo reply shows prior icmp echo request
  - If abnormal, does it resemble any attack scenario?

Care with Signatures

- Example of Nimda worm
  - Sends HTTP requests that look like this
    - `GET /scripts/..%c0af../winnt/system32/cmd.exe?/c+dir`
  - The string %c0af = / in unicode
  - The request traverses the root directory to exploit a bug in Microsoft's IIS
- What should a signature look for?
  - If it looks just for the specific request above, it may miss a variation of the request
  - Some IDSs actually decode the request and see what it is asking for

False Positives

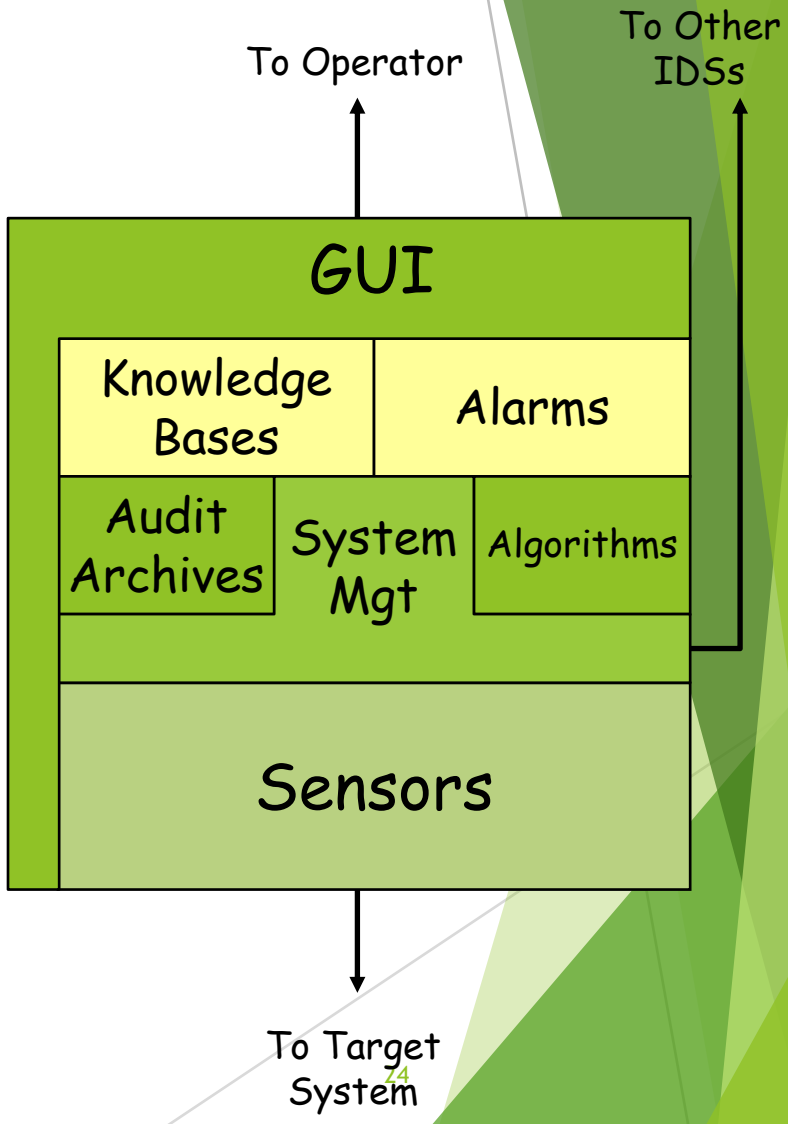
- Report that there is an intrusion when there is none
- Certain with all IDSs
- Depends on the signature and how close it is to some normal activity
- Occurs with generalized signatures
  - Example: Any request containing cmd.exe anywhere
    - May reject a URL that contains cmd.exe-analysis.html
    - May reject access to nascmd.exe
- Too many false positives may make an operator shut off a particular signature

False Negatives

- Signature fails to generate an alert which should have been generated
- Occurs when a signature is very specific and fails to match a variation
- Example:
  - Nimda
    - Check for /winnt/system32/cmd.exe
    - Fails to issue alert for /winnt/system32/../system32/cmd.exe
    - May also allow /winnt/system32/cmd.%65xe
  - Fragmented packets are another example

System Architeture of IDSs

- Abstract View
- Vendors have specific architectures that may be different
- Some components may also be referred to differently
- Note that many IDSs may interact with each other to provide a higher level of reliability



IDS Components Expanded

- Sensor
  - Component that provides necessary information about the target system
  - Also called probe, monitor, feed, tap, event boxes, etc.
- System Management
  - A layer that enables communication between the sensors and other components
  - It is becoming common to use SNMP or other management protocols for this purpose
- Algorithms
  - They form part of the processing engine
  - This is the most non-trivial part of an IDS and involves decision making, data mining, pattern matching and so on

Deployment of Sensors

- Multiple sensors must be placed in the target system
  - Redundancy against failures
  - Ability to tune them to pick up certain kinds of traffic
    - Also helps in case of high traffic volumes
  - Many network segments may exist
- Typically, sensors are paired with firewalls and packet filters
  - If possible, sensors must be deployed on both sides of a firewall (why?)
- Care must be taken in switched networks to ensure that sensors **can see all the traffic**
- Deploying a separate network for sensor communications may be advisable for security, performance, etc.

IDS Components Expanded (cont.)

- Knowledge bases
  - They usually contain profiles of users and systems, attack signatures, information for correlation, etc.
  - Come in all flavors and types
  - Common standards for encoding the knowledge base is ongoing work
- Audit archives
  - Store audit logs and other archived information
  - Needs considerable thought as to how long such information must be kept, how often it must be refreshed, etc.

IDS Components Expanded (cont.)

- Alarms
  - In today's IDSs, alarms typically only alert a human being
  - Alarms are evolving to actually interact with sensors through the system management layer to trap intruders, divert traffic, selectively disable access, etc. (response)
- Graphical User Interface
  - What is actually displayed to the operator can be crucial in certain actions being taken in a timely manner
  - Most GUI's are based on known attacks and what information appears to be critical
  - It is important to discover the true use of information by operators in real situations

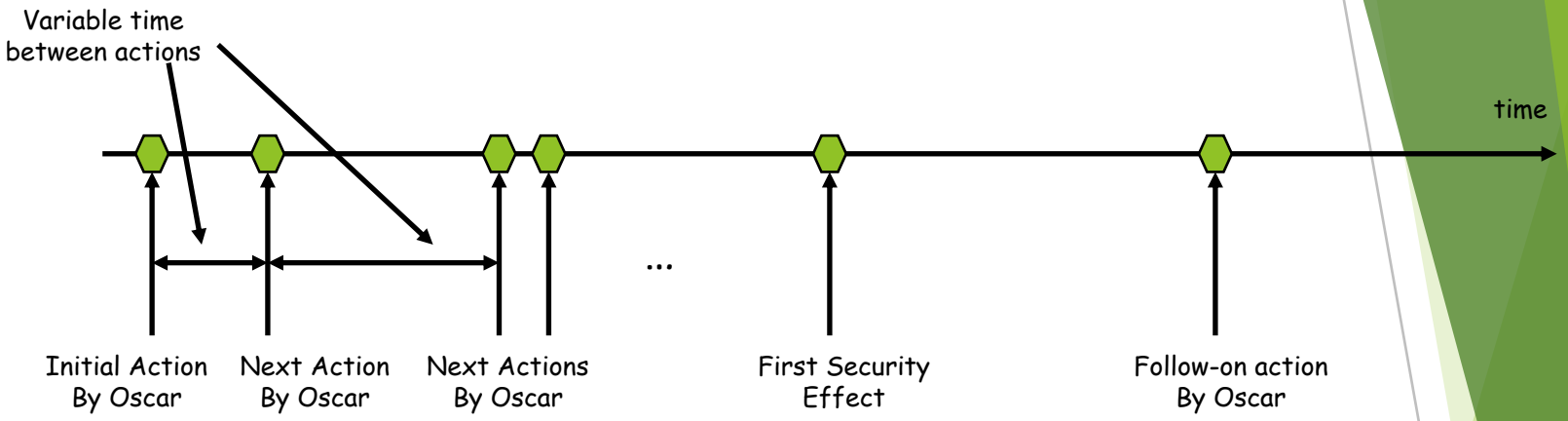
Cautions about IDSs

- A single IDS may be too weak to detect security attacks
  - One should use a network-based IDS with a host-based IDS and correlate information
  - Redundant IDSs should be employed to prevent attacks occurring if one IDS fails
- IDSs are susceptible to attacks
  - Tunneling of data, packet fragmentation and so on can fool IDSs
  - IDSs can also be foiled using so-called “insertion and evasion attacks”
    - Host rejects or sees information that the IDS sees or rejects
  - IDSs can be susceptible to DoS attacks
    - Many IDSs do not have an IP address, but can sniff packets

Expanding on Intrusion

- Sequence
  - There are many activities ordered in time that result in an intrusion
  - To detect an intrusion, it is important to pick up the sequential pattern as early as possible
- Related actions
  - Includes seemingly unrelated actions taken by the intruder to evade detection
  - One way of evading detection is to allow “time” to pass between actions so that they appear to be unrelated (correlation)
- Occurrence
  - Intrusions occur only if it occurs
  - Planning for an intrusion is not really an intrusion
  - Intrusion attempts must also be detected even if they are unsuccessful

Temporal Model of Intrusion



- Model intrusion as a sequence of actions
- Some of the actions may be responses by the target network/system
- The sequence becomes an “attack signature”
- Requires separation of intrusion-related and intrusion-unrelated events/actions in time

Information Correlation

- Correlating information is extremely important to detect intrusions
  - It involves interpretation, combination and analysis of information from all available sources for detecting and responding to intrusions
- Three classes of correlation
  - Single and multiple session correlation of packets
  - Real-time and after-the-fact correlation of information
  - In-band and all-band correlation of information

Single vs. Multiple Session Correlation

- Single session
  - Typically involves one TCP session
  - Begins with a 3-way handshake and then ends with two FINs
  - What packets were sent during the session? Are they related? Are states properly transitioned?
  - Look at the series of client and server responses and actions
  - More difficult with session-less protocols like UDP
- Multiple sessions
  - Sources and destinations may be different or may be the same
    - It may be the same source, but it may report that it is a different source (spoofing)
  - Clocks may be different and hence hard to synchronize the actions, responses and events
  - Much harder than correlating packets in a single session

Real-Time vs. After-the-Fact Correlation

- Factors
  - Processing power, availability of information, ability of human to react in real-time, etc.
- In real-time correlation, it is not possible to look-forward
  - In after-the-fact analysis, it may be possible to guess what might have happened and look for it
- If audit trails are used, it has to be after-the-fact since they are processed in batch mode
- Sometimes, the incident may still be occurring as intrusion information is being processed

In-Band vs. All-Band Correlation

- In-band = computing and networking activity related to target system
  - Includes all header information, protocol information, payloads, network time, etc.
- All-band = extraneous information about user or activity
  - Can be virtually anything (e.g., someone broke into the building)
- In-band components may have been spoofed
  - Logs may have been overwritten for example
- Confidence levels of information can be different for the types of information

Intrusion Responses from an IDS

- Passive response
  - Monitor traffic from Oscar more closely than before
- Examples of active responses
  - Send crafted RST packets to Oscar to terminate TCP connections
  - Set new rules in a firewall or change access controls
- Care must be taken in the case of active responses
  - It may be a false positive and you may be denying service to a legitimate connection
    - Example solution: deny service to a connection if you have received more than N alarms

Trends in IDS

- Distributed IDS
  - Idea
    - Operators from all over the world submit their logs from their sensors, firewalls, etc., to a distributed IDS service
    - The distributed IDS site performs correlations to identify attacks
    - Examples:
      - Attack Registry and Intelligence Service (ARIS) at http://aris.securityfocus.com
      - Dshield at http://www.dshield.org
- Outsourced IDS
  - Allow an external IDS management company to perform IDS for you
  - Security implications and lack of knowledge of internal environment may hamper results
  - Correlation from many sites may be useful

Trends in IDS (cont.)

- IETF's Intrusion Detection Working Group
  - Looking at interoperability of distributed IDSs
  - What data formats and exchange procedures need to be in place
  - Facilitate sharing information between intrusion detection and response systems
- The working group is considering
  - Requirements for communication based on scenarios
  - Common intrusion language specification for data formats
    - Intrusion Detection Message Exchange Format - IDMEF
  - Framework to identify protocols for exchanging data between IDSs
    - Intrusion Detection Exchange Protocol - IDXP

IDS Tools

- There are many vendors for IDSs
  - Examples:
    - Enterasys Dragon - Robust, UNIX based system, highly customizable
    - Cisco Secure - sells appliances for IDS
    - Others - ISS Blackice, ISS RealSecure, Symantec NetProwler
- Open source IDSs
  - Snort: http://www.snort.org
  - Analysis console for intrusion databases (ACID) at http://www.cert.org/kb/acid
  - SNARE and SHADOW

What to Look for in an IDS

- Depth of Coverage
  - What kinds of attacks can the IDS detect?
  - What customization features are available?
  - What OSs can it support?
- Accuracy of coverage
  - Harder to determine - how many false positives and false negatives exist?
- Robustness
- Scalability
  - Can it handle heavy traffic volumes?
  - Can it display information if it becomes too voluminous?
- Management framework
  - How easy it is to manage the IDS and get information from it?
- Complexity, Updates

Intrusion Prevention Systems (IPSs)

- Hybrid Firewalls and IDSs are available these days
  - Example: Hogwash http://hogwash.sourceforge.net/oldindex.html
- IPSs
  - Combine the blocking capabilities of a firewall with deep packet inspection
  - See article at http://www.symantec.com/connect/articles/intrusion-prevention-systems-next-step-evolution-ids
  - Needs powerful processors to perform functions correctly

More about IPSs

- IPSs come in two kinds
  - Rate-based IPS products: block traffic based on load
  - Content-based IPS products: use signatures to block traffic (e.g., Nimda)
- Example products and vendors
  - Rate-based: TopLayer's Attack Mitigator IPS
  - Content-based: Checkpoint InterSpect