

# Intrusion Detection

Cyber Security

Spring 2010

# Reading material

- Chapter 25 from Computer Security, Matt Bishop
- Snort
  - <http://snort.org>
- Distributed IDS – DShield
  - <http://dshield.org>
- Dark address space
  - <http://www.arbornetworks.com/dmdocuments/c>

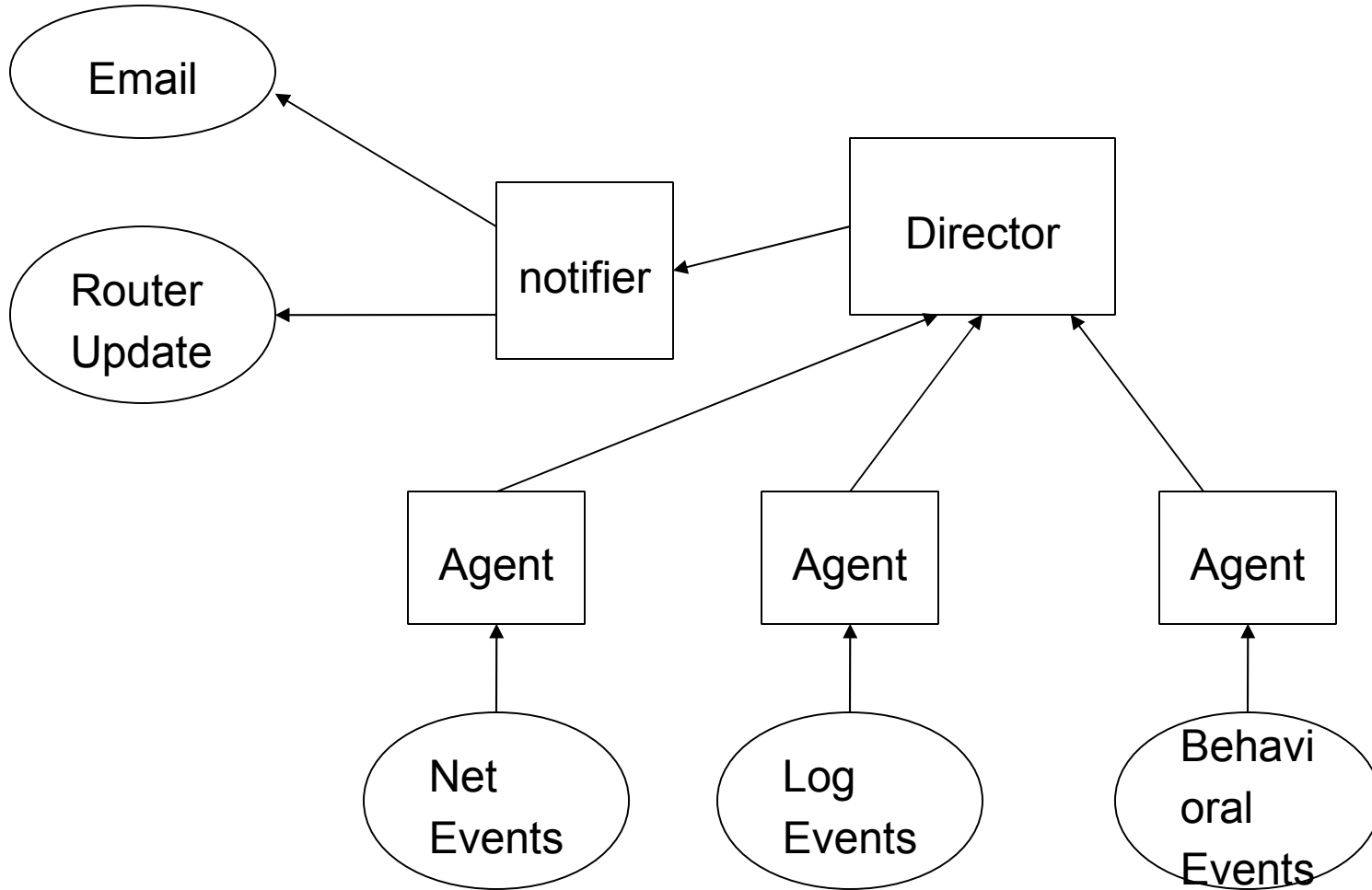
# Goal of Intrusion Detection

- Holy Grail: Detect and correct “bad” system behaviour
- Detection can be viewed in two parts
  - Anomaly detection: Use statistical techniques to determine unusual behaviour
  - Mis-use detection: Use signatures to determine occurrence of known attacks
- Detection can be performed on host data (HIDS), network data (NIDS), or a hybrid of both

# Intrusion Detection

- Use audit trail
- React rather than directly prevent
  - Find “bad actions”
  - Work with access control mechanisms to stop them from happening
- May be hindered by confidentiality mechanisms
  - Like access control may not be able to see enough of traffic stream to detect

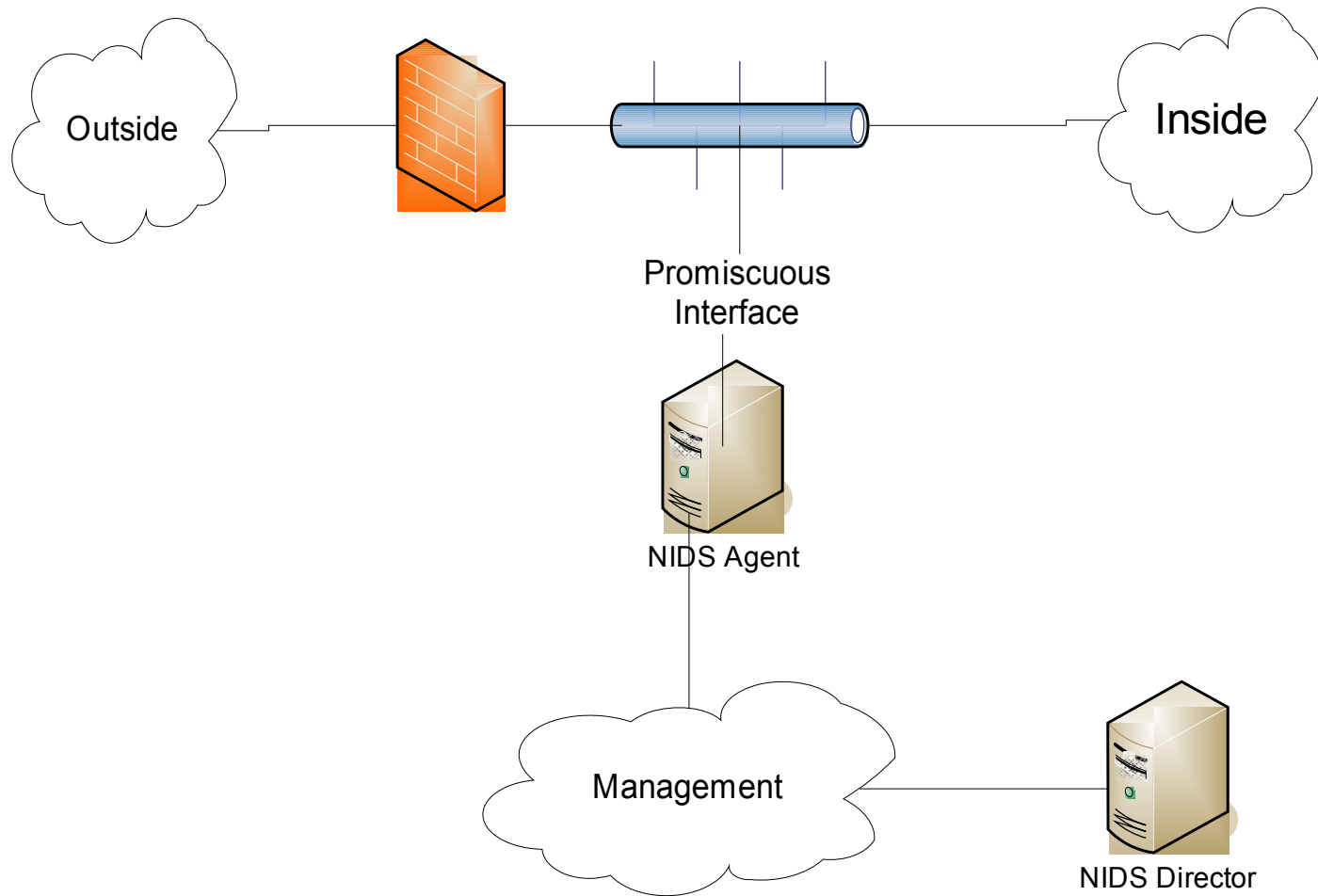
# IDS Architecture



# IDS Architecture

- Agents run at the lowest level gathering data.
- Agents send data to a Director that performs more significant processing of the data.
  - Potentially there is a hierarchy of agents and directors
- Directors invoke Notifiers to perform some action in response to a detected attack
  - Popup a window on a screen
  - Send an email or a page
  - Send a new syslog message elsewhere.
  - Access control mechanism to block future action from the attacker
    - Update firewall config
    - BGP blackhole

# Classical NIDS deployment



# NIDS Remediation Options

- Log the event
- Drop the connection
- Reset the connection
- Change the configuration of a nearby router or firewall to block future connections



# Mis-use/Signature Detection

- Fixed signatures are used in most deployed IDS products
  - E.g., Cisco, ISS, Snort, Bro
- Like virus scanners, part of the value of the product is the team of people producing new signatures for newly observed malevolent behaviour
  - Dedicated attacker can adjust his behaviour to avoid matching the signature.
  - Cannot find what we don't know about
- The volume of signatures can also result in many false positive.
  - Must tune the IDS to match the characteristics of your network
  - Can result in IDS tuned too low to miss real events
  - Can hide real attacks in the mass of false positives

# Example Signature

- Signature for port sweep
  - A set of TCP packets attempting to connect to a sequence of ports on the same device in a fixed amount of time
- In some environments, the admin might run nmap periodically to get an inventory of what is on the network
  - You would not want to activate this signature in that case

# Example Snort Rule

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 \  
  (content: "|00 01 86 a5|"; msg: "external mounth access");)
```

- Rule header up to ‘(
  - Identifies packets of interest
- Rule options after ‘(
  - What to do to matching packets

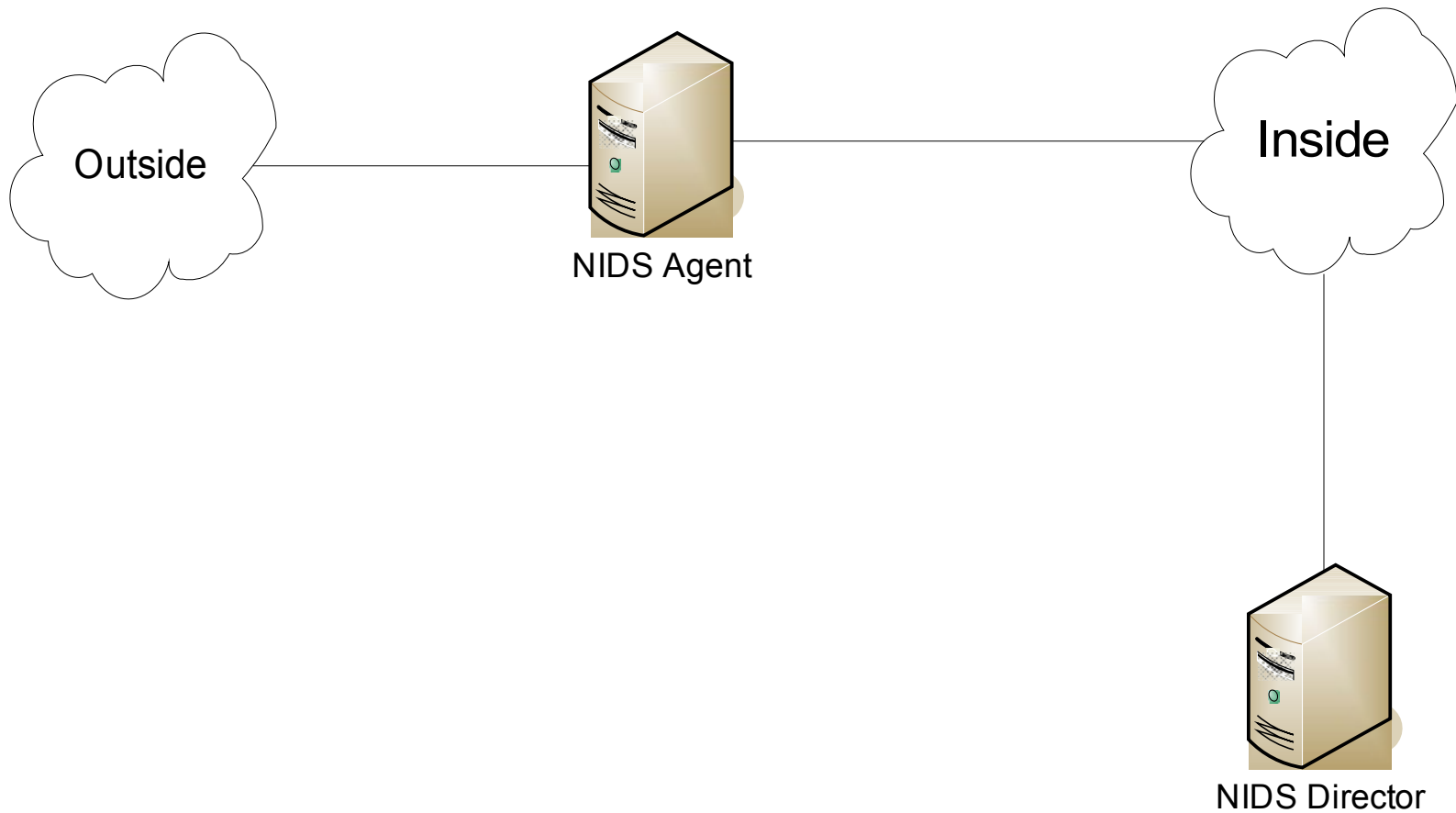
# Anomaly/statistical detection

- Seems like using statistics will result in a more adaptable and self-tuning system
  - Statistics, neural networks, data mining, etc.
- How do you characterize normal?
  - Create training data from observing “good” runs
    - E.g., Forrest’s program system call analysis
  - Use visualization to rely on your eyes
- How do you adjust to real changes in behavior?
  - Gradual changes can be easily addressed. Gradually adjust expected changes over time
  - Rapid changes can occur. E.g., different behavior after work hours or changing to a work on the next project

# Intrusion Protection Systems (IPS)

- Another name for inline NIDS
- Requires very fast signature handling
  - Slow signature handling will not only miss attacks but it will also cause the delay of valid traffic
  - Specialized hardware required for high volume gateways
- The inline intrusion detector can take direct steps to remediate
- If you move IDS into the network processing path, how is this different from really clever firewalling?

# Network IPS scenario



# Free vs Commercial IDS

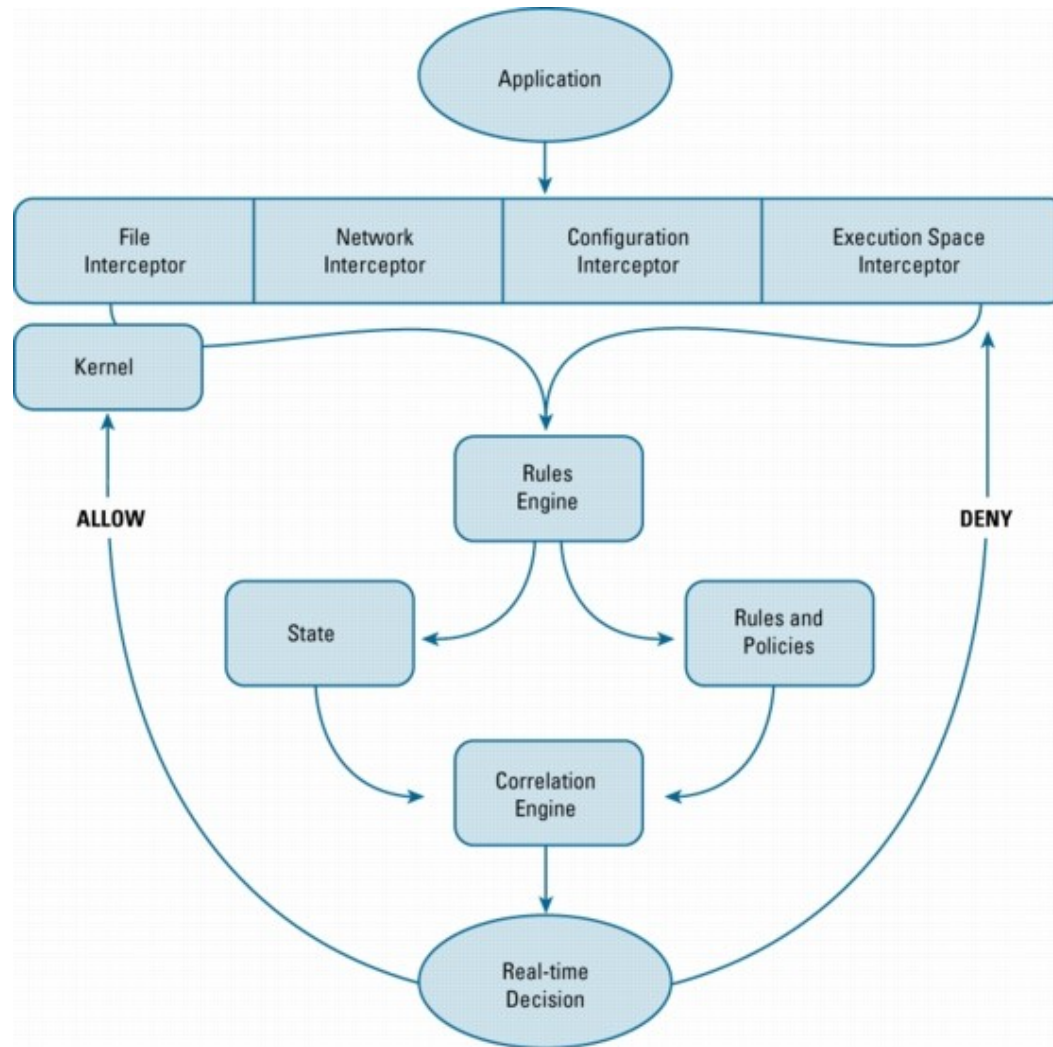
- What do you get by paying?
  - Better hardware
  - Better signature and alert management tools
  - Timely and reviewed signatures

# Host Based IDS

- Tripwire – Very basic detection of changes to installed binaries
- More recent HIDS. Look at patterns of actions of system calls, file activity, etc. to permit, deny, or query operations
  - Cisco Security Agent
  - Symantec
  - McAfee Enterccept



# Cisco Security Agent Architecture



# Honey Pots

- Attract attacks with “fake” system
- Target must interact to some degree
  - Ensure target does not become a nuisance
- Honeyd – Virtually presents an entire network - <http://www.honeyd.org/>
- Honey Net – Tools to create a real network of honey pots- <http://www.honeynet.org>

# Netflow as an IDS basis

- Netflow is a logging format that tracks connections (source, destination, protocol and ports)
  - Original developed to support traffic engineering
  - Emerged as a good source of IDS traffic analysis
- Arbor Networks
  - <http://arbornetworks.com/>
  - Analyzes router netflow data
  - Uses patented algorithms to detect anomalous activity
- Netflow visualization
  - NVisionIP and VisFlowConnect projects at NCSA
  - <http://www.projects.ncassr.org/sift/>

# Large Scale IDS

- Internet Storm Center and dshield.org
  - A very coarse level statistical analysis to find outliers in port activity
  - Uses a donated firewall logs from people all over the internet
  - Detect new worms or other widespread malware
  - <http://dshield.org>

# More large scale IDS

- Dark addresses are routable addresses that are not completely connected. May be routable from one part of the internet but not another
- Any traffic in the dark address space is invalid
  - It is a random target of a worm attack
  - It is a temporarily or locally routable address that is being used as the non-traceable source of an attack
- Hone in on activity on these dark address spaces
  - Internet motion detectors and network telescopes propose placing sensors at strategic points in the Internet
  - Use the information on these sensors as early warnings for emerging attacks.