Basics of Intrusion Detection

- Watch what's going on in the system
- Try to detect behavior that characterizes intruders
- While avoiding improper detection of legitimate access
- At a reasonable cost

Intrusion Detection and Logging

- A natural match
- The intrusion detection system examines the log
  - Which is being kept, anyway
- Secondary benefits of using the intrusion detection system to reduce the log

On-Line Vs. Off-Line Intrusion Detection

- Intrusion detection mechanisms can be complicated and heavy-weight
- Perhaps better to run them off-line
  - E.g., at nighttime
- Disadvantage is that you don't catch intrusions as they happen

Failures In Intrusion Detection

- False positives
  - Legitimate activity identified as an intrusion
- False negatives
  - An intrusion not noticed
- Subversion errors
  - Attacks on the intrusion detection system

Desired Characteristics in Intrusion Detection

- Continuously running
- Fault tolerant
- Subversion resistant
- Minimal overhead
- Must observe deviations
- Easily tailorable
- Evolving
- Difficult to fool

Host Intrusion Detection

- Run the intrusion detection system on a single computer
- Look for problems only on that computer
- Often by examining the logs of the computer

Advantages of the Host Approach

- Lots of information to work with
- Only need to deal with problems on one machine
- Can get information in readily understandable form

Network Intrusion Detection

- Do the same for a local (or wide) area network
- Either by using distributed systems techniques
- Or (more commonly) by sniffing network traffic

Advantages of Network Approach

- Need not use up any resources on users' machines
- Easier to properly configure for large installations
- Can observe things affecting multiple machines

Network Intrusion Detection and Data Volume

- Lots of information passes on the network
- If you grab it all, you will produce vast amounts of data
- Which will require vast amounts of time to process

Network Intrusion Detection and Sensors

- Use programs called *sensors* to grab only relevant data
- Sensors quickly examine network traffic
  - Record the relevant stuff
  - Discard the rest
- If you design sensors right, greatly reduces the problem of data volume

Wireless IDS

- Observe behavior of wireless network
  - Generally 802.11
- Look for problems specific to that environment
  - E.g., attempts to crack WEP keys
- Usually doesn't understand higher network protocol layers
  - And attacks on them

Application-Specific IDS

- An IDS system tuned to one application or protocol
  - E.g., SQL
- Can be either host or network
- Typically used for machines with specialized functions
  - Web servers, database servers, etc.
- Possibly much lower overheads than general IDS systems