# Styles of Intrusion Detection

- Misuse intrusion detection
  - Try to detect things known to be bad
- Anomaly intrusion detection
  - Try to detect deviations from normal behavior
- Specification intrusion detection
  - Try to detect deviations from defined "good states"

# Misuse Detection

- Determine what actions are undesirable
- Watch for those to occur
- Signal an alert when they happen
- Often referred to as *signature detection*

# Level of Misuse Detection

- Could look for specific attacks
  - E.g., SYN floods or IP spoofing
- But that only detects already-known attacks
- Better to also look for known suspicious behavior
  - Like trying to become root
  - Or changing file permissions

# How Is Misuse Detected?

- By examining logs
  - Only works after the fact
- By monitoring system activities
  - Often hard to trap what you need to see
- By scanning the state of the system
  - Can't trap actions that don't leave traces
- By sniffing the network
  - For network intrusion detection systems

# Pluses and Minuses of Misuse Detection

+ Few false positives
+ Simple technology
+ Hard to fool
  - At least about things it knows about
– Only detects known problems
– Gradually becomes less useful if not updated
– Sometimes signatures are hard to generate

# Misuse Detection and Commercial Systems

- Essentially all commercial intrusion detection systems primarily detect misuse
  - Generally using signatures of attacks
- Many of these systems are very similar
  - Differing only in details
- Differentiated primarily by quality of their signature library
  - How large, how quickly updated

# Anomaly Detection

- Misuse detection can only detect known problems
- And many potential misuses can also be perfectly legitimate
- Anomaly detection instead builds a model of valid behavior
  - And watches for deviations

# Methods of Anomaly Detection

- Statistical models
  - User behavior
  - Program behavior
  - Overall system/network behavior
- Expert systems
- Pattern matching of various sorts
- Misuse detection and anomaly detection sometimes blur together

# Pluses and Minuses of Anomaly Detection

+ Can detect previously unknown attacks
+ Not deceived by trivial changes in attack
– Hard to identify and diagnose nature of attacks
– Unless careful, may be prone to many false positives
– Depending on method, can be expensive and complex

# Anomaly Detection and Academic Systems

- Most academic research on IDS in this area
  - More interesting problems
  - Greater promise for the future
  - Increasingly, misuse detection seems inadequate
- But few really effective systems currently use it
  - Not entirely clear that will ever change
  - What if it doesn't?

# Specification Detection

- Define some set of states of the system as good
- Detect when the system is in a different state
- Signal a problem if it is

# How Does This Differ From Misuse and Anomaly Detection?

- Misuse detection says that certain things are bad
- Anomaly detection says deviations from statistically normal behavior are bad
- Specification detection defines exactly what is good and calls the rest bad

# Some Challenges

- How much state do you have to look at?
  - Typically dealt with by limiting observation to state relevant to security
  - Easy to underestimate that . . .
- How do you specify a good state?
- How often do you look?
  - Might miss attacks that transiently change the state

# Protocol Anomaly Detection

- Really a form of specification intrusion detection
- Based on precise definitions of network protocols
- Can easily detect deviations
- Incorporated into some commercial systems
  - E.g., Snort and Checkpoint

# Pluses and Minuses of Specification Detection

+ Allows formalization of what you're looking for
+ Limits where you need to look
+ Can detect unknown attacks
- Only effective when one can specify correct state
- Based on locating right states to examine
- Maybe attackers can do what they want without changing from a "good" state