Intrusion Detection

Intrusion Detection

- **Some attacks will get through in spite of every protection measure. Intrusion detection is targeted to detect such attacks.**
  - *Detection is a solution of last resort*

- **Assumption: *Behavior* under attack differs from “normal” behavior**
- **Approach: Detect these changes in behavior**

Intrusion Detection Behaviors

- **Behaviors of**
  - Users
  - Systems
    - processes, kernel modules, hosts, networks, …

Intrusion Detection Observation Points

- **Network-based (Network intrusion detection systems)**
  - Benefits
    - Unintrusive: plug a dedicated NIDS device on the network
    - Centralized monitoring
  - Problems
    - Encryption
    - Level of abstraction too low
    - Difference between data observed by NIDS and victim app.
- **Host-based**
  - Strengths/weaknesses complementary to NIDS
  - May be based on
    - system-call interception
    - audit logs and other log files
    - file system integrity (TripWire)
    - keystrokes, commands, etc.

Intrusion Detection Techniques

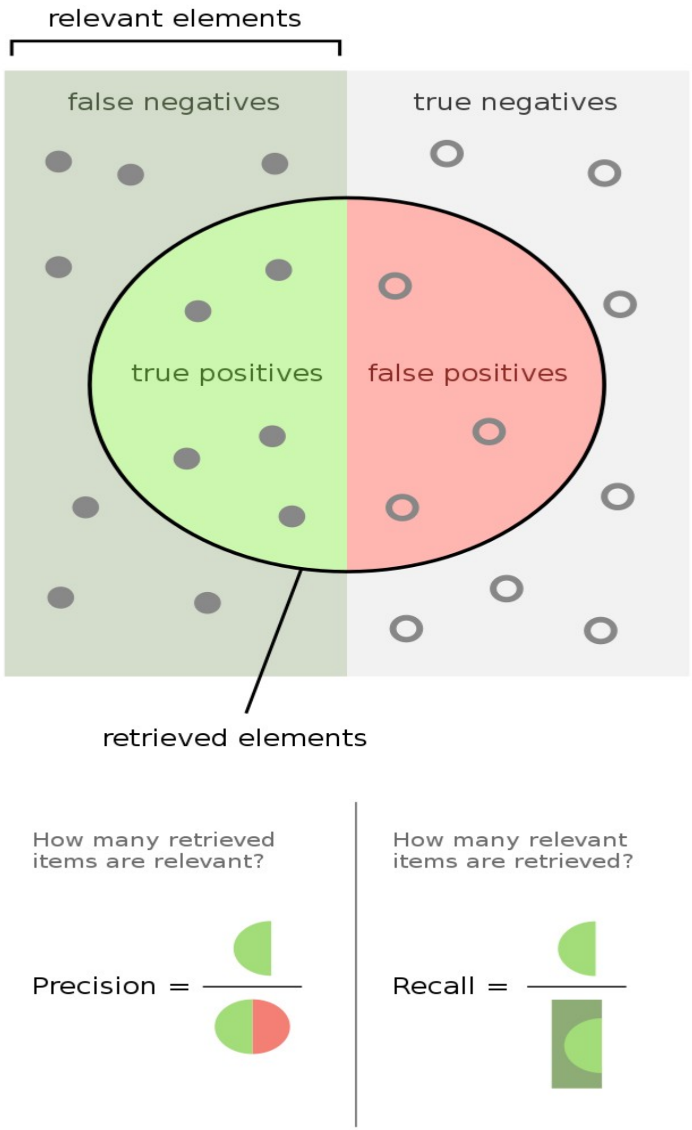
- **Anomaly detection**
  - Use machine learning techniques to develop a profile of normal behavior
  - Detect deviations from this behavior
  - Can detect unknown attacks, but have high FA rate
- **Misuse detection**
  - Codify patterns of misuse
  - Attack behaviors usually captured using signatures
  - Can provide lower false alarm rate, but ineffective for unknown attacks
- **Behavior (or policy) based detection**
  - Specify allowable behavior, detect deviations from specifications
  - Can detect new attacks with low FA, but policy selection is hard

Intrusion Detection Metrics

- **Detection rate**
  - What fraction of attacks are detected
- **False alarm rate**
  - May be measured in multiple ways
    - how many false alarms per day
    - what fraction of normal behavior is flagged as attack
    - what fraction of behavior reported as attack is *not* an attack (false alarm ratio)
  - Considerable disagreement on which measure to use
    - but the third criteria is probably the best
    - But IDS vendors don't like it
      - – Will you buy a system will FA rate of 98%?
      - – But you may not mind 10 false alarms a day!

Intrusion Detection Metrics

- **Recall**
  - TP/(TP+FN)
  - Same as *detection rate*
- **Precision**
  - TP/(TP+FP)
  - 1-FAR from previous slide
  - Conditional probability of a real attack when an alarm occurs.



Classes of Attacks

- **Probing: Reconnaissance before attack**
  - Port sweeps
  - OS/application finger printing
- **Denial of Service (DoS)**
- **Privilege escalation**
  - Remote to user
    - attacker without any access to the victim machine gains access as a normal user, e.g., userid *nobody*
  - User to root
    - attacker with access as normal user gains administrative privileges through an attack
  - These two privilege escalation attacks may be chained

Intrusion Detection Algorithms

- **Pattern-matching**
  - Most commonly used in misuse and behavior based techniques
- **Machine-learning**
- **Policy-driven**

Mimicry Attacks

- **For most sophisticated attacks, hiding the attack is often a bigger goal than succeeding in the attack**
  - Attackers will go to great lengths to evade detection
- **Mimicry attacks: Attacks crafted with knowledge of IDS**
  - Mimic normal behavior of applications as seen by the IDS
    - e.g., execute only system calls (or sequences of system calls) that the application normally executes
- **Attacks are carried out by attacker's malware, so attackers have the degree of control needed to carry out such attacks**