CSE 543 - Computer Security (Fall 2006)

Lecture 20 - Intrusion Detection
November 14, 2006
URL: http://www.cse.psu.edu/~tjaeger/cse543-f06/

Intrusion Detection (def. by Forrest)

- An IDS system find anomalies
  - "The IDS approach to security is based on the assumption that a system will not be secure, but that violations of security policy (intrusions) can be detected by monitoring and analyzing system behavior." [Forrest 98]
  - However you do it, it requires
    - Training the IDS (*training*)
    - Looking for anomalies (*detection*)

- This is an explosive area in computer security, that has led to lots of new tools, applications, industry

Intrusion Detection Systems

- IDS systems claim to detect adversary when they are in the act of attack
  - Monitor operation
  - Trigger mitigation technique on detection
  - Monitor: Network, Host, or Application events
- A tool that discovers intrusions "after the fact" are called *forensic analysis* tools
  - E.g., from system logfiles
- IDS systems really refer to two kinds of detection technologies
  - Anomaly Detection
  - Misuse Detection