CS530
Intrusion Detection

Bill Cheng

http://merlot.usc.edu/cs530-s10

Intrusion Detection

- Security enforcement mechanisms are not foolproof, so we need a way of knowing when they are not working
  - or even better, before they stop working
- We need ways to detect insider misuse
  - detect suspecious activities
    - e.g., is this employee selling information?

Taxonomy for Intrusion Detection

- What is detected
  - *misuse detection* - look for "bad" bahaviors
    - e.g., virus checker, spam filters - need to download new "definition files"
  - *anomaly detection* - look at behavior and detect out of profile activities
    - need to compare against a *baseline*
- Where detected
  - network based
  - host based - system logs
  - application based
- When attack is detected
  - real time
  - after the fact / post mortem