Denial of Service Attacks

Mendel Rosenblum

Denial of Service Attacks (DOS Attacks)

- An attack that causes a service to fail by using up resources
  - Could be an accident (e.g. upload too big of a file) or on purpose
- Example from our Photo App:
  - User uploads photos, comments, user registration until our storage fills.
  - Establish so many connections our web server falls over
- Resource could be at networking layer
  - Use all the bandwidth of the network coming into our website
  - Use all the network sockets

Distributed **D**enial **o**f **S**ervice (DDoS) Attacks

- DOS attack that uses many attacking machines
  - Example: Get control of a million machines and point them at someone's web server
- Botnets - Collection of compromised machines under control
- Has become an extortion business

Web App DOS mitigation

- None perfect - really hard problem
  - Do want to take steps to avoid accidental DOS and make purpose-driven DOS harder
  - Abuse analysis step required
- Resource quotas
  - Track resource consumption per user and provide way of cutting off users
  - Good for catching accidents, less so for malicious attacks
- Make resources cost money
  - Raises the cost or hassle for an attacker
  - Not always possible under business model
- Network layer: Need to push back on attack stream
  - Do things like cut off traffic coming from some part of the internet