CSE 543 - Computer Security (Fall 2006)

Lecture 18 - Network Security
November 7, 2006
URL: http://www.cse.psu.edu/~tjaeger/cse543-f06/

Denial of Service

- Intentional prevention of access to valued resource
  - CPU, memory, disk (system resources)
  - DNS, print queues, NIS (services)
  - Web server, database, media server (applications)
- This is an attack on *availability* (*fidelity*)
- **Note**: launching DOS attacks is easy
- **Note**: preventing DOS attacks is hard
  - Mitigation the path most frequently traveled

D/DOS (generalized by Mirkovic)

- Send a stream of packets/requests/whatever …
  - many PINGS, HTML requests, …
- Send a few malformed packets
  - causing failures or expensive error handling
  - low-rate packet dropping (TCP congestion control)
  - "ping of death"
- Abuse legitimate access
  - Compromise service/host
  - Use its legitimate access rights to consume the rights for domain (e.g., local network)
  - E.g., First-year graduate student runs a recursive file operation on root of NFS partition