Outline

- Definition
- Point-to-point network denial of service
  - Smurf
- Distributed denial of service attacks
  - Trin00, TFN, Stacheldraht, TFN2K
- TCP SYN Flooding and Detection

Denial of Service Attack Definition

- An explicit attempt by attackers to prevent legitimate users of a service from using that service
- Threat model – taxonomy from *CERT*
  - Consumption of network connectivity and/or bandwidth
  - Consumption of other resources, e.g. queue, CPU
  - Destruction or alternation of configuration information
    - Malformed packets confusing an application, cause it to freeze
  - Physical destruction or alternation of network components

Status

- DoS attacks increasing in frequency, severity and sophistication
  - *32%* respondents detected DoS attacks (1999 CSI/FBI survey)
  - Yahoo, Amazon, eBay and MicroSoft DDoS attacked
  - About *4,000* attacks per week in 2000
  - Internet's root DNS servers attacked on
    - Oct. 22, 2002, 9 out of 13 disabled for about an hour
    - Feb. 6, 2007, one of the servers crashed, two reportedly "suffered badly", while others saw "heavy traffic"
    - An apparent attempt to disable the Internet itself