Denial of Service

David Wetherall
djw@cs.washington.edu

Denial of Service in the News

Denial-of-service attack cripples Microsoft for second day

By John Stodden
Network World Fusion, 01/25/01

Adding insult to injury, attackers launched a denial-of-service attack against Microsoft Thursday that crippled access to the company’s Web sites for a second day.
What is Denial of Service?

- Attacker need not break into a system, but consumes enough of it’s resources that legitimate users are denied service … effectively render a Website down

- Big issue in practice and lack of effective solutions today

- Two broad classes:
  - Nasty packets trigger implementation bugs, e.g., Ping of Death
  - Packet floods target bandwidth, CPU, memory, e.g., SYN flood

Nasty Packet Attacks

- Example: Ping of Death

- Solution?
  - Patch OS bugs
Packet Floods

• Example: SYN Floods

• Solution?
  – Engineer/design protocol to tolerate better (SYN cookies)
  – But really need network infrastructure support to block traffic

Complication: Spoofed Addresses

• Why reveal your real address? Instead, “spoof” it.
  – Can implicate others and appear to be many hosts

• Solution?
  – Ingress filtering (ISPs check validity of source addresses) helps, but has poor incentive patterns and is not a complete solution
Complication: Reflectors & Amplifiers

- Some packets arriving "out of the blue" trigger a reply
  - Use this with spoofing to launder attack traffic (e.g., DNS)
  - Use with broadcast addresses to amplify attack (e.g., Smurf)

Distributed DOS (DDOS)

- Use automated tools to set up a network of zombies
  - Trin00, TFN, mstream, Stacheldraht, …