

## **CSE/EE 461 – Lecture 25**

### **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 Fontana  
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.



## Packet Floods

---

- Example: SYN Floods
  
- Solution?
  - Engineer/design protocol to tolerate better (SYN cookies)
  - But really need network infrastructure support to block traffic

djw // CSE/EE 461, Winter 2003

L25.5

## 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

djw // CSE/EE 461, Winter 2003

L25.6

## 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)

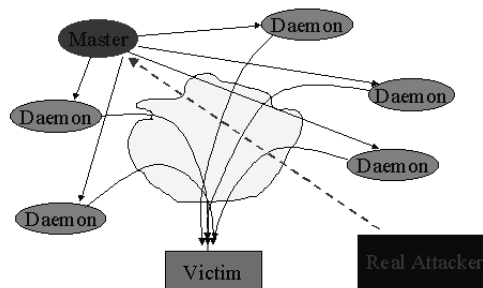
djw // CSE/EE 461, Winter 2003

L25.7

## Distributed DOS (DDOS)

---

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



djw // CSE/EE 461, Winter 2003

L25.8