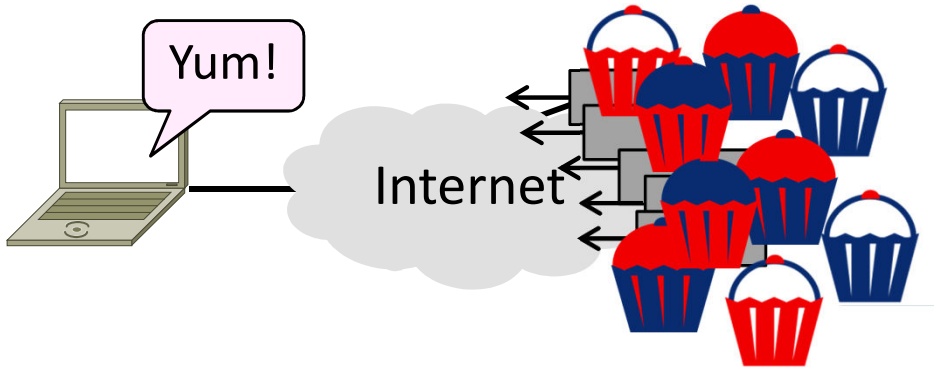
Computer Networks

Distributed Denial-of-Service

David Wetherall (djw@uw.edu)
Professor of Computer Science & Engineering
UNIVERSITY of WASHINGTON

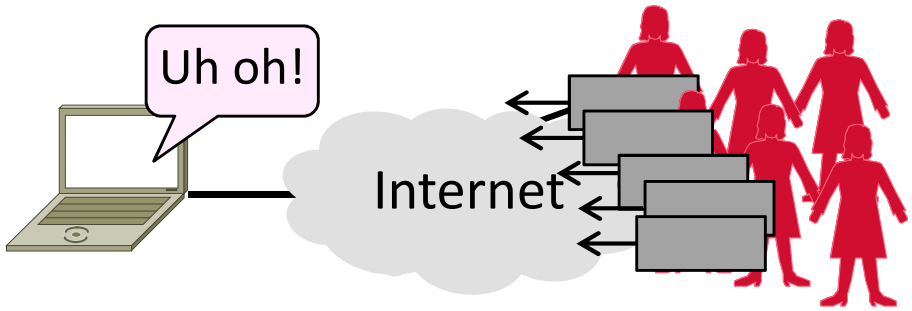
Topic

- Distributed Denial-of-Service (DDOS)
  - An attack on network availability



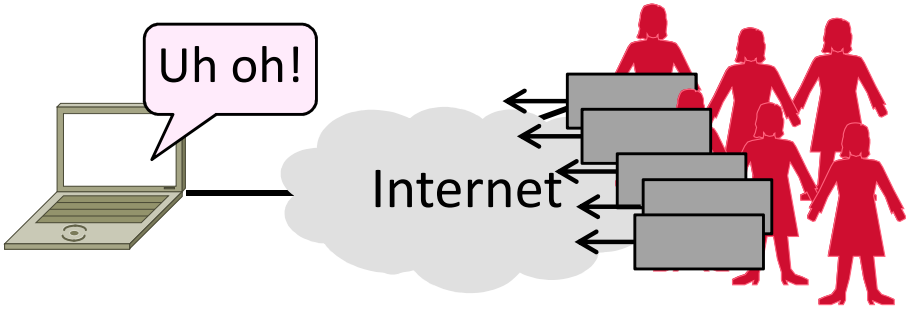
Topic

- Distributed Denial-of-Service (DDOS)
  - An attack on network availability



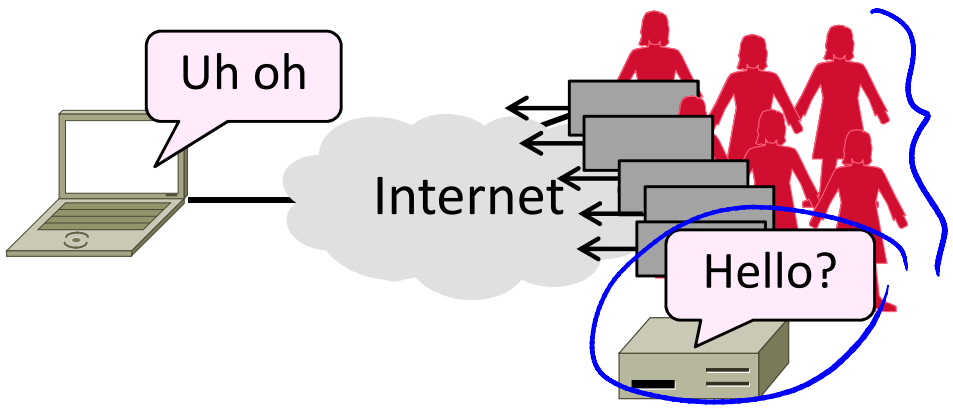
Motivation

- The best part of IP connectivity
  - You can send to any other host
- The worst part of IP connectivity
  - Any host can send packets to you!



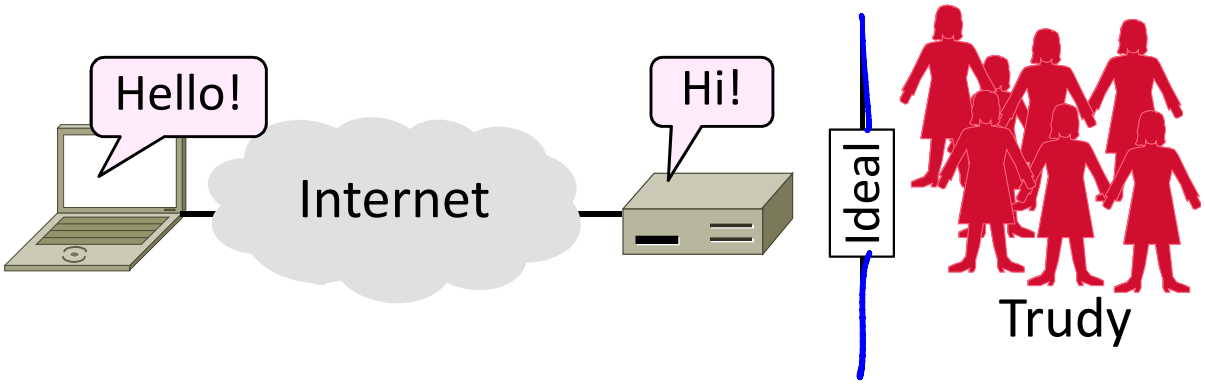
Motivation (2)

- Flooding a host with many packets can interfere with its IP connectivity
  - Host may become unresponsive
  - This is a form of denial-of-service



Goal and Threat Model

- Goal is for host to keep network connectivity for desired services
  - Threat is Trudy may overwhelm host with undesired traffic



Internet Reality

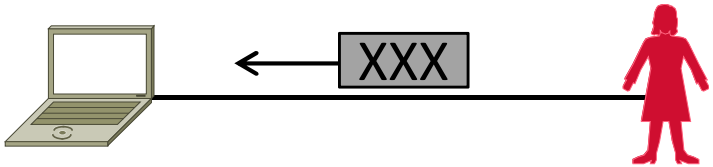
- Distributed Denial-of-Service is a huge problem today!
  - Akamai Q3-12 reports DDOS against US banks peaking at 65 Gbps …
- There are no great solutions
  - CDNs, network traffic filtering, and best practices all help

Denial-of-Service

- Denial-of-service means a system is made unavailable to intended users
  - Typically because its resources are consumed by attackers instead
- In the network context:
  - "System" means server
  - "Resources" mean bandwidth (network) or CPU/memory (host)

Host Denial-of-Service

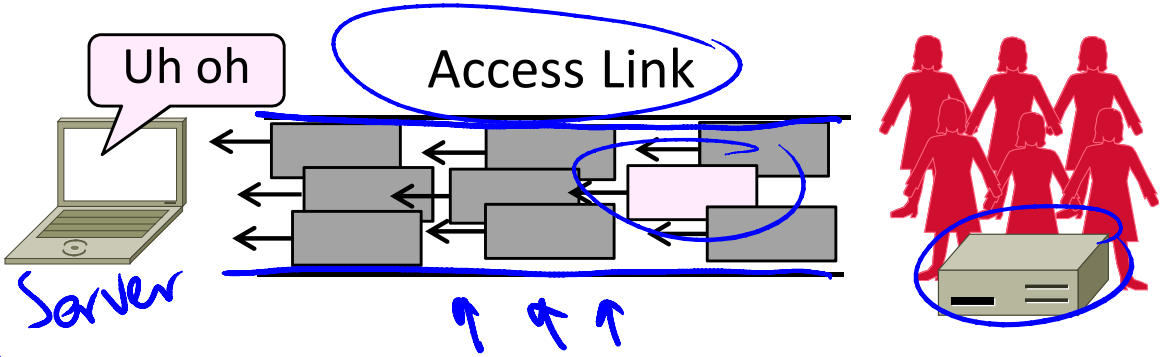
- Strange packets can sap host resources!
  - "Ping of Death" malformed packet
  - "SYN flood" sends many TCP connect requests and never follows up
  - Few bad packets can overwhelm host



- Patches exist for these vulnerabilities
  - Read about "SYN cookies" for interest

Network Denial-of-Service

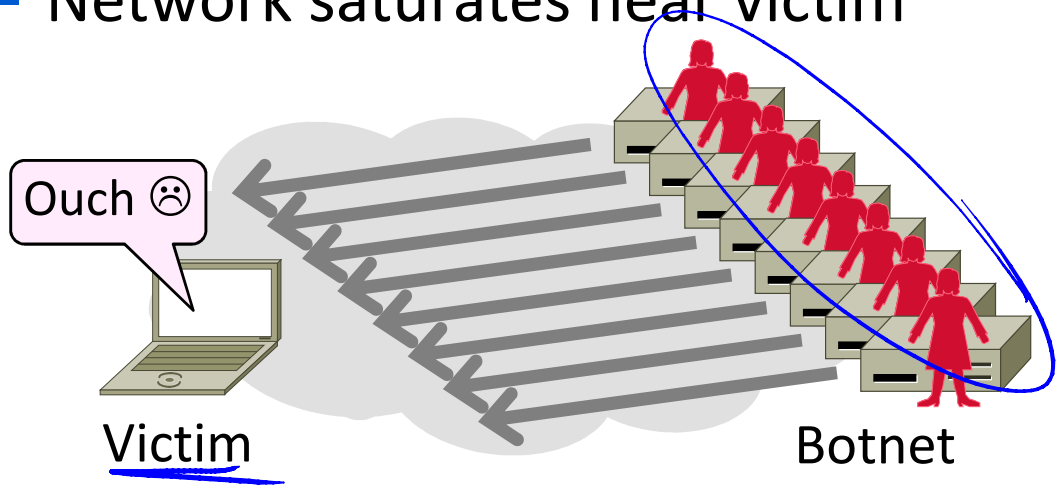
- Network DOS needs many packets
  - To saturate network links
  - Causes high congestion/loss



- Helpful to have many attackers … or Distributed Denial-of-Service

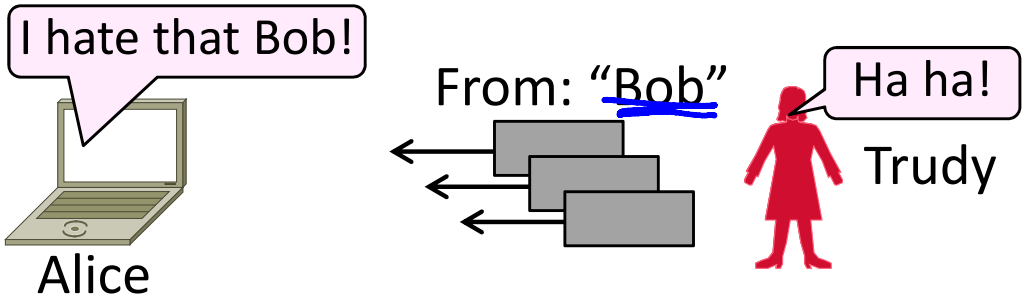
Distributed Denial-of-Service (DDOS)

- Botnet provides many attackers in the form of compromised hosts
  - Hosts send traffic flood to victim
  - Network saturates near victim



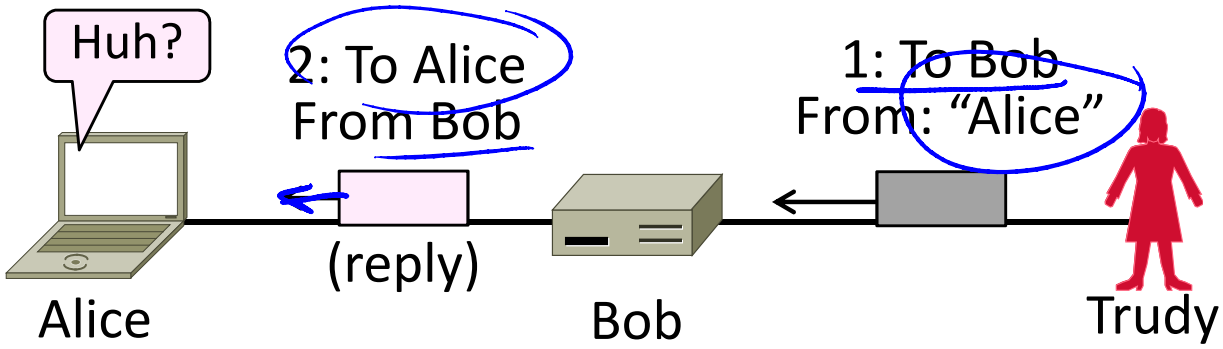
Complication: Spoofing

- Attackers can falsify their IP address
  - Put fake source address on packets
    - Historically network doesn't check
  - Hides location of the attackers
  - Called IP address spoofing



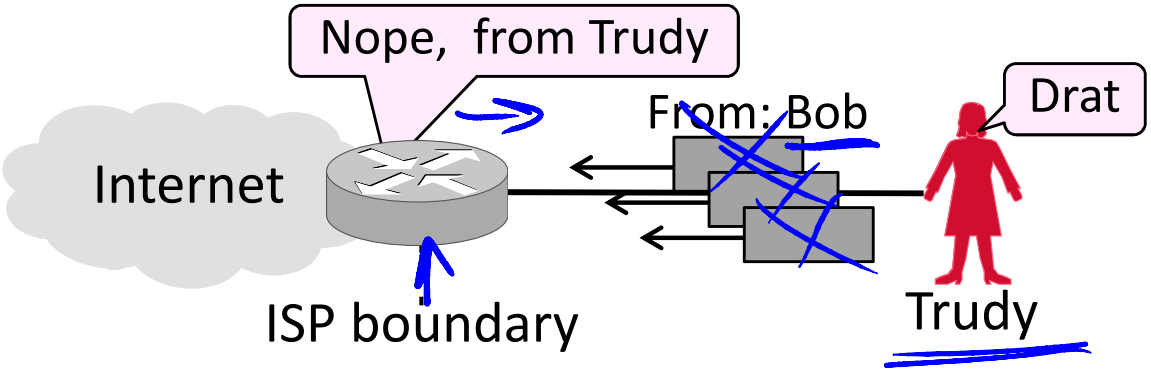
Spoofing (2)

- Actually, it's worse than that
  - Trudy can trick Bob into really sending packets to Alice
  - To do so, Trudy spoofs Alice to Bob



Best Practice: Ingress Filtering

- Idea: Validate the IP source address of packets at ISP boundary (Duh!)
  - Ingress filtering is a best practice, but deployment has been slow



Flooding Defenses

1. Increase network capacity around the server; harder to cause loss
   - Use a CDN for high peak capacity
2. Filter out attack traffic within the network (at routers)
   - The earlier the filtering, the better
   - Ultimately what is needed, but ad hoc measures by ISPs today

END