

Threats beyond TLS

CSE 461

Ratul Mahajan

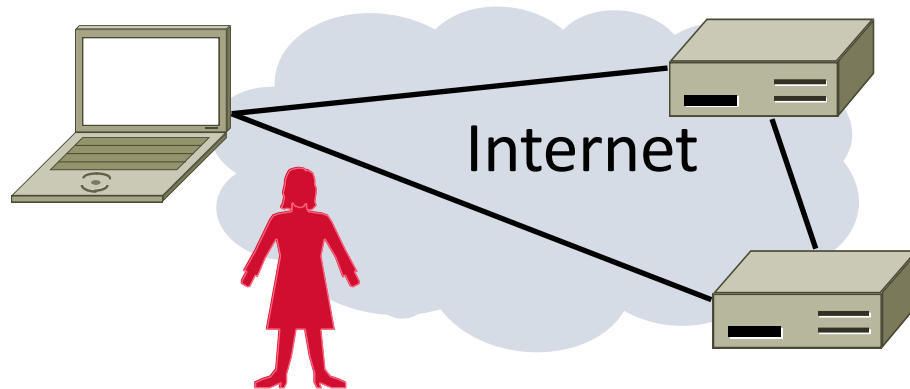
Threats beyond TLS

(confidentiality, integrity, authenticity)

- Metadata leaks
- Resource starvation

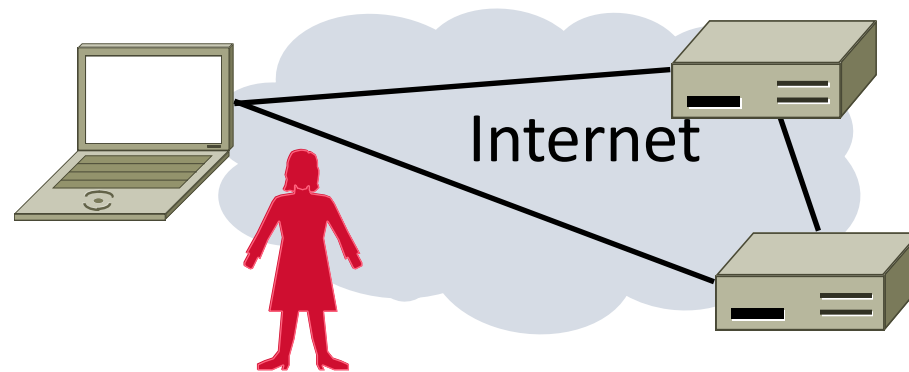
Topic

- Virtual Private Networks (VPNs)
 - Run as closed networks on Internet
 - Use IPSEC to secure messages



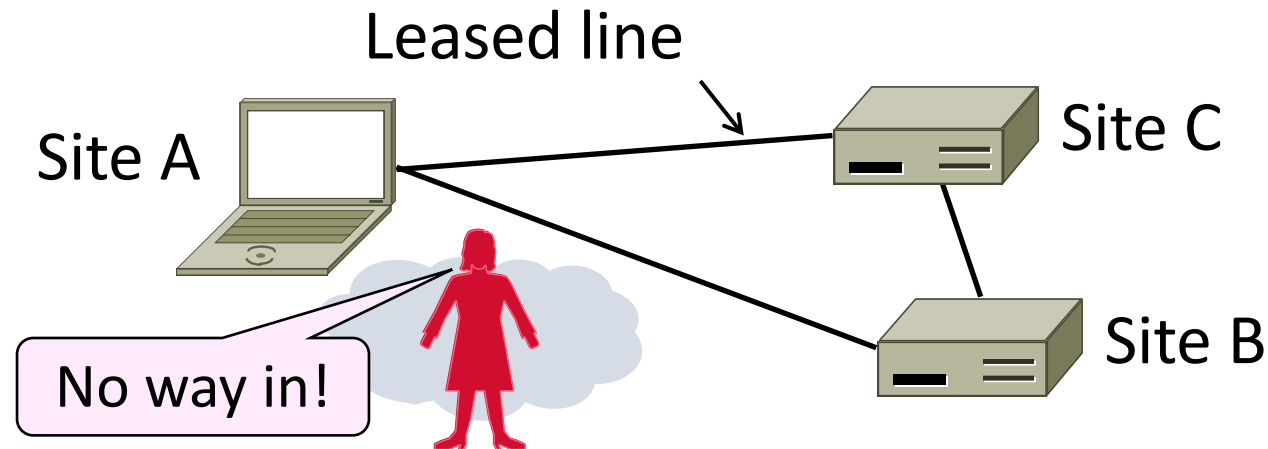
Motivation

- 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!
 - There's nasty stuff out there ...



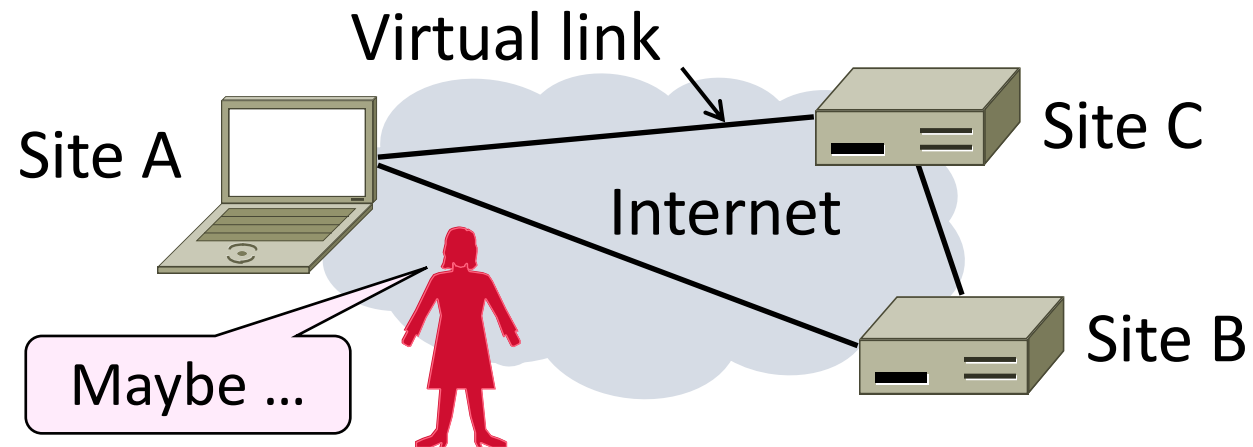
Motivation (2)

- Often desirable to separate network from the Internet, e.g., a company
 - Private network with leased lines
 - Physically separated from Internet



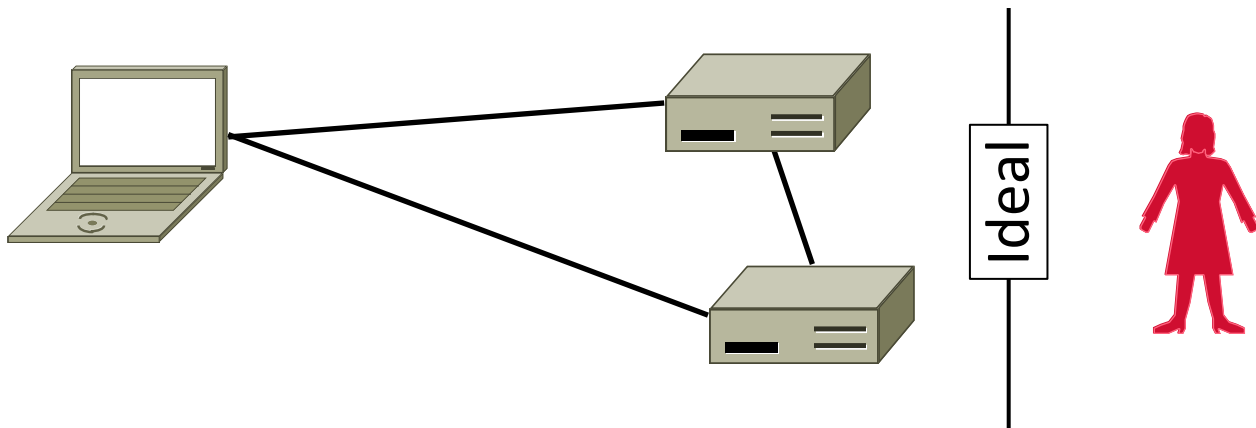
Motivation (3)

- Idea: Use the public Internet instead of leased lines
 - cheaper!
 - Logically separated from Internet ...
 - This is a Site-to-site Virtual Private Network (VPN)



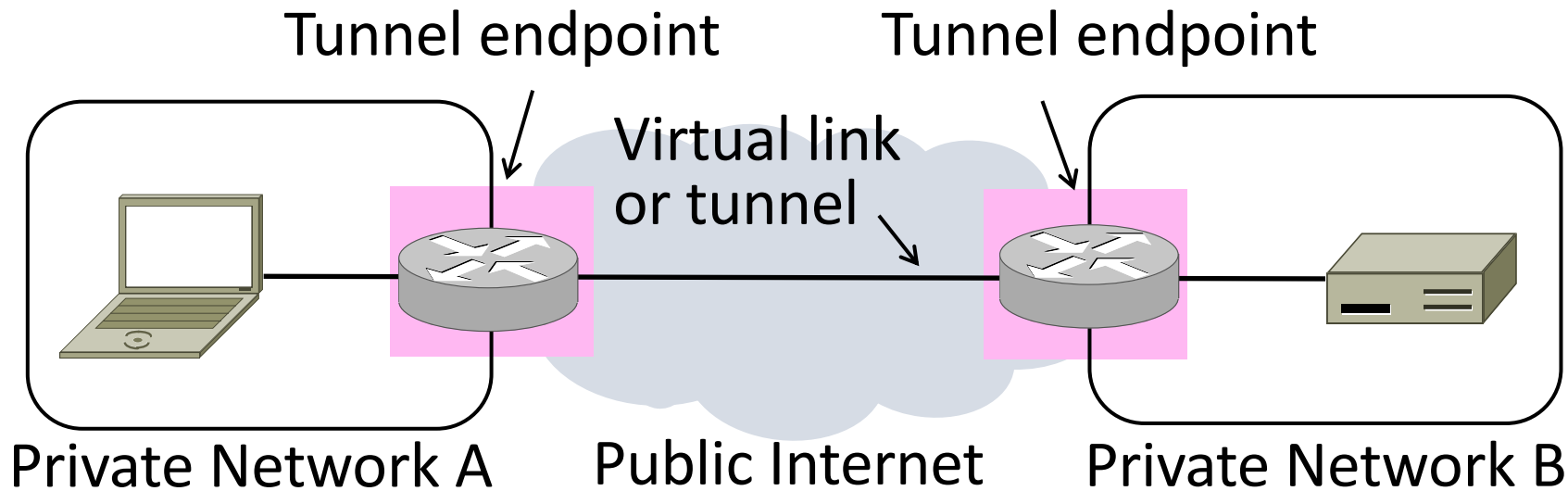
Goal and Threat Model

- Goal is to keep a logical network (VPN) separate from the Internet while using it for connectivity
 - Threat is Trudy may access VPN and intercept or tamper with messages



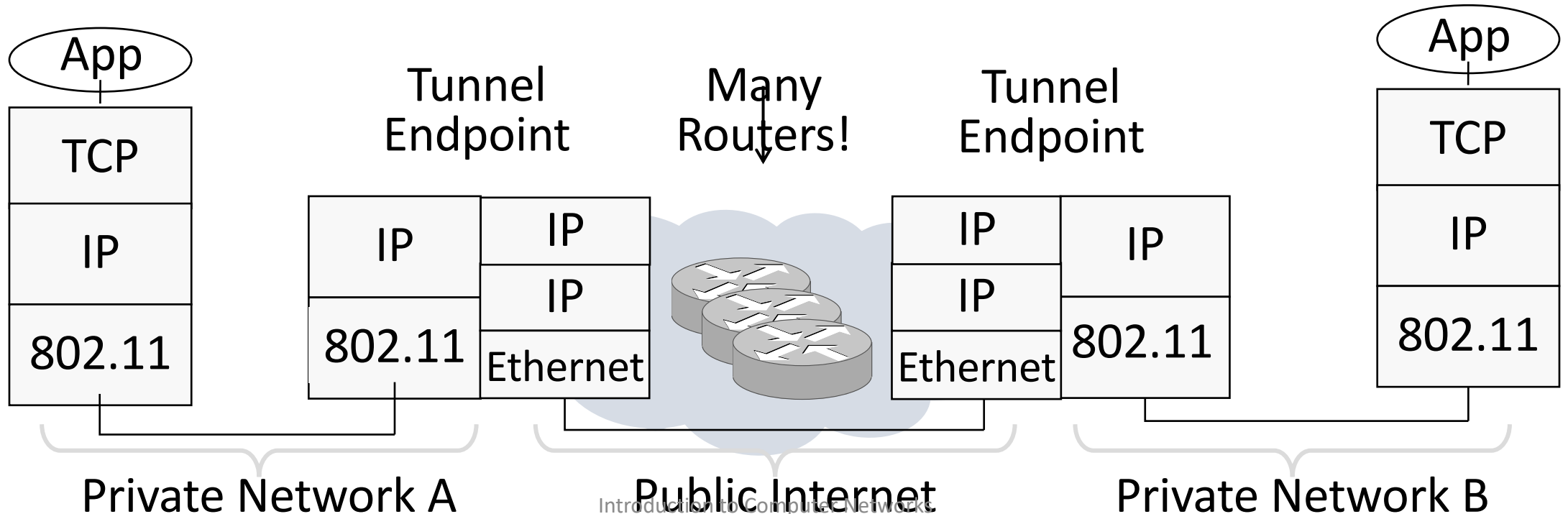
Tunneling

- How can we build a virtual link? With tunneling!
 - Hosts in private network send to each other normally
 - To cross virtual link (tunnel), endpoints encapsulate packet



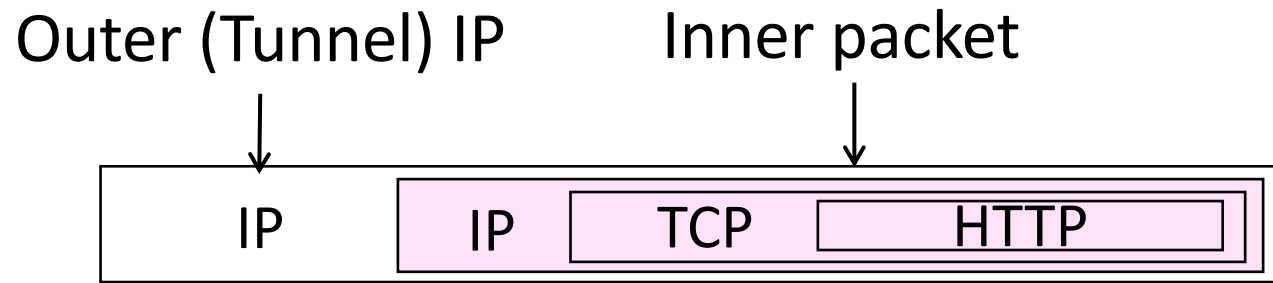
Tunneling (2)

- Tunnel endpoints encapsulate IP packets (“IP in IP”)
 - Add/modify outer IP header for delivery to endpoint



Tunneling (3)

- Simplest encapsulation wraps packet with another IP header
 - Outer (tunnel) IP header has tunnel endpoints as source/destination
 - Inner packet has private network IP addresses as source/destination

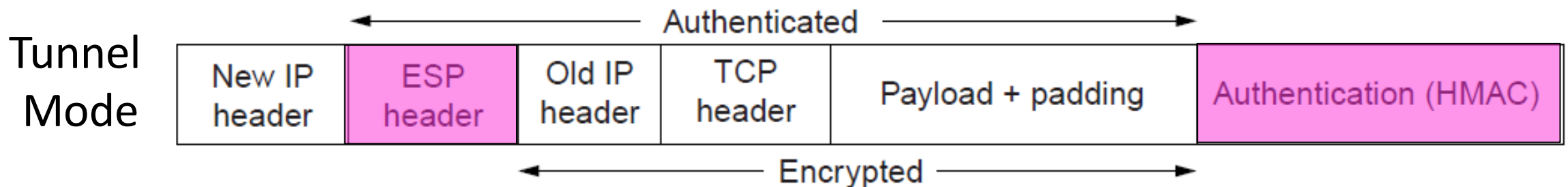


Tunneling (4)

- Tunneling alone is not secure ...
 - No confidentiality, integrity/ authenticity
 - Trudy can read, inject her own messages
 - We require cryptographic protections!
- IPSEC (IP Security) is often used to secure VPN tunnels

IPSEC (IP Security)

- Longstanding effort to secure the IP layer
 - Adds confidentiality, integrity/authenticity
- IPSEC operation:
 - Keys are set up for communicating host pairs
 - Communication becomes more connection-oriented
 - Header and trailer added to protect IP packets



Client-server VPNs

Use cases

- Secure access to remote resources



Want these resources to be accessible by only authorized users

Hosts/applications not necessarily aware of user identity

Client-server VPNs

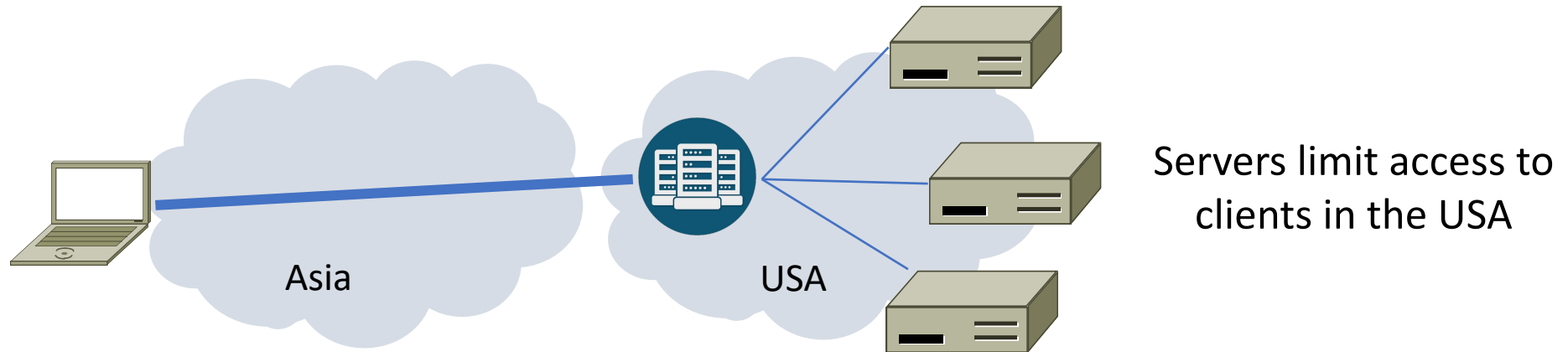
Use cases

- Secure access to remote resources
- “Teleportation” to another region



Servers limit access to clients in the USA

Client-server VPN operation



1. Client and VPN server establish an encrypted connection
2. VPN software creates a logical network interface on the client
3. Applications send traffic to this interface
4. The VPN software tunnels the traffic to the VPN server
5. The VPN server unwraps the traffic, NATs the packet, and sends it to the destination
 - a) The destination only see the VPN server IP
6. The destination sends reverse traffic to the VPN server
7.

Takeaways

VPNs help build private networks atop the Internet

- Virtual links encapsulate packets
- Alters IP connectivity for hosts

VPNs need crypto to secure messages

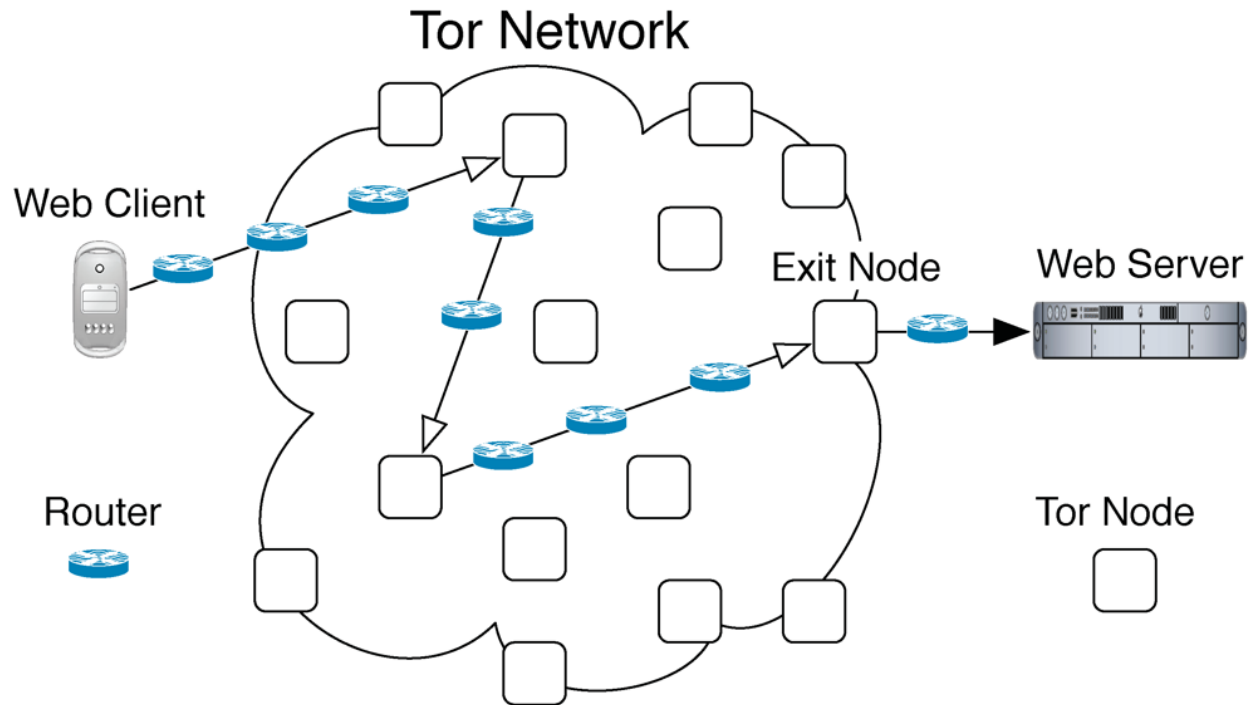
- Encrypted tunnels are used for confidentiality, integrity/authenticity across the two endpoints



Tor: “The Onion Router”

Basic idea:

1. Many volunteers act as routers in the overlay
2. Generate circuit of routers will send packet
3. Encrypt the packet in layers for each router
4. Send the packet
5. Each router receives, decrypts their layer, and forwards based on new info
6. Routers maintain state about circuit to route stuff back to sender
 - But again, only know the next hop

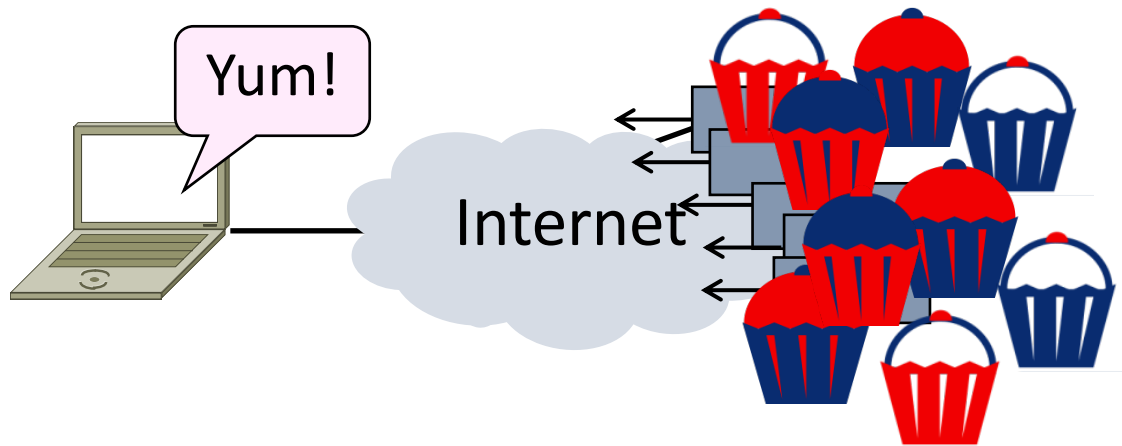


Performance?

Resource Attacks

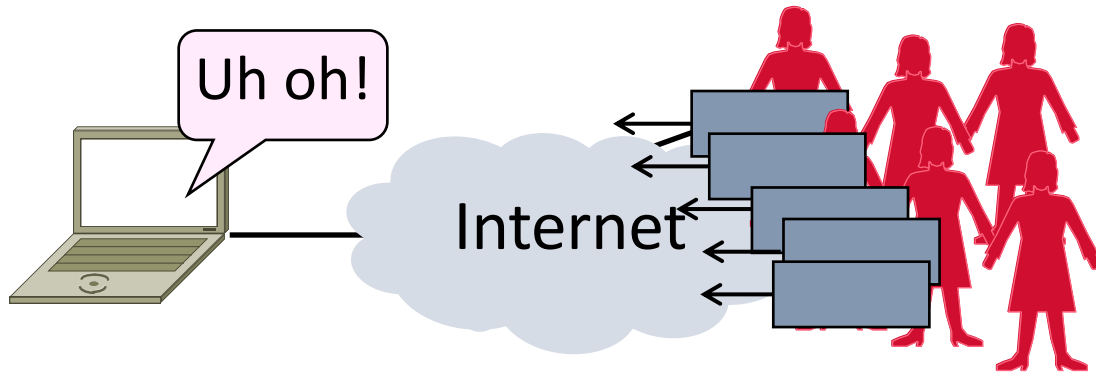
Topic

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



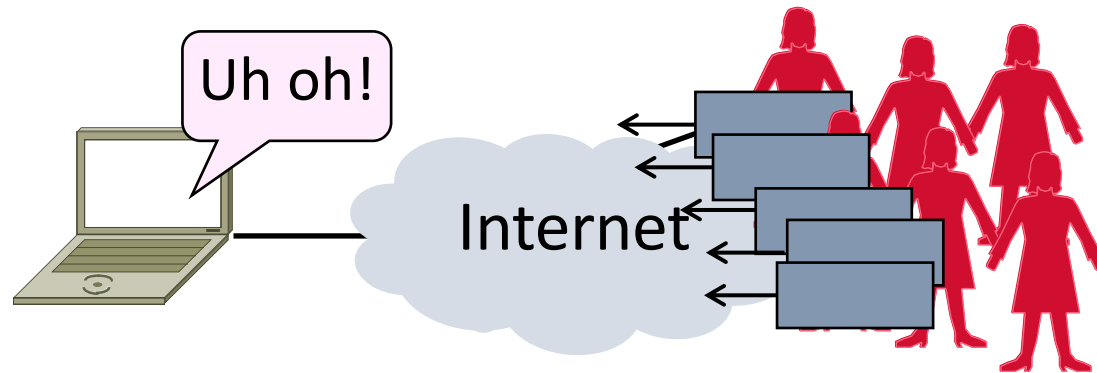
Topic

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



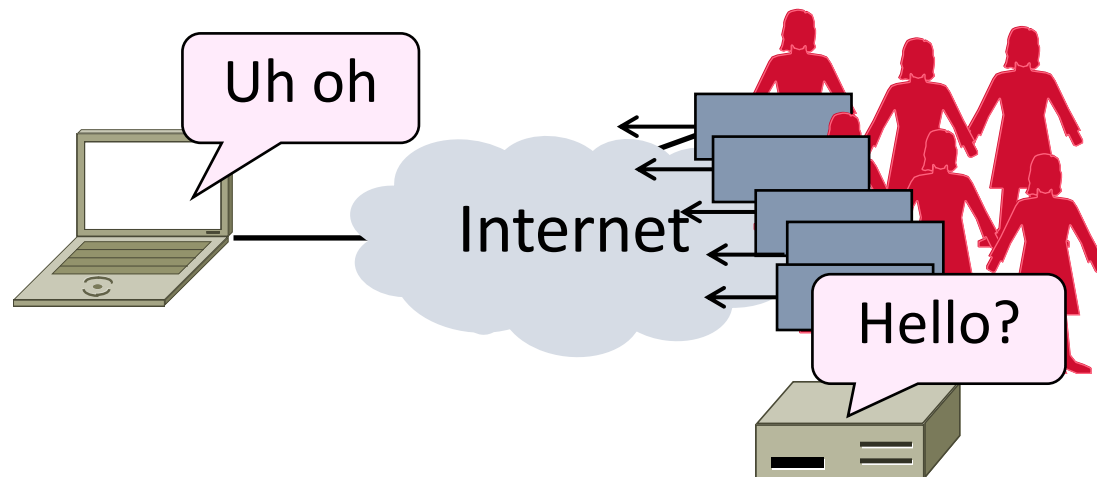
Motivation

- 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 (DoS)

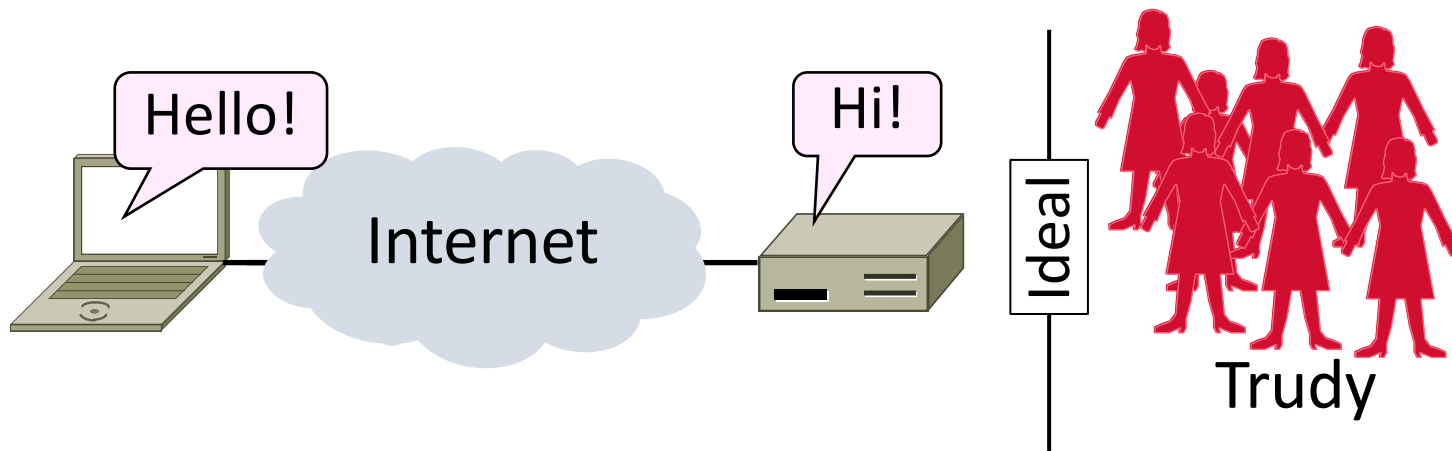


Denial-of-Service

- 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)

Goal and Threat Model

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



SHARE

SHARE
14021

TWEET

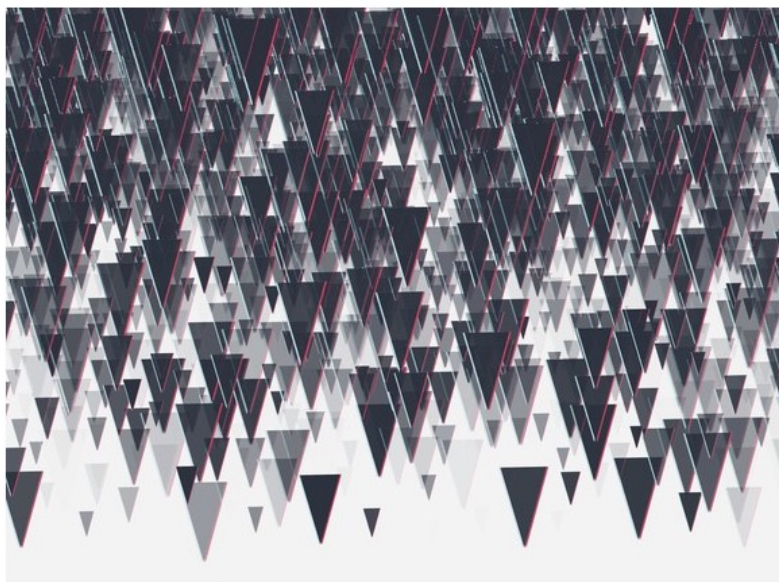


COMMENT



EMAIL

LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM

GITHUB SURVIVED THE BIGGEST
DDOS ATTACK EVER RECORDED

GETTY IMAGES

ON WEDNESDAY, AT about 12:15 pm EST, 1.35 terabits per second of traffic hit the developer platform GitHub all at once. It was the most powerful distributed denial of service attack recorded to date—and it used an increasingly popular DDoS method, no botnet required.

GitHub briefly struggled with intermittent outages as a
Introduction to Computer Networks

MOST POPULAR



CULTURE

Tweets Cost Kevin Hart the Oscars. His Apology Made It Worse

BRIAN RAFTERY



SECURITY

John McAfee Fled to Belize, But He Couldn't Escape Himself

JOSHUA DAVIS



SECURITY

14 Questions Robert Mueller Knows the Answer To

GARRETT M. GRAFF



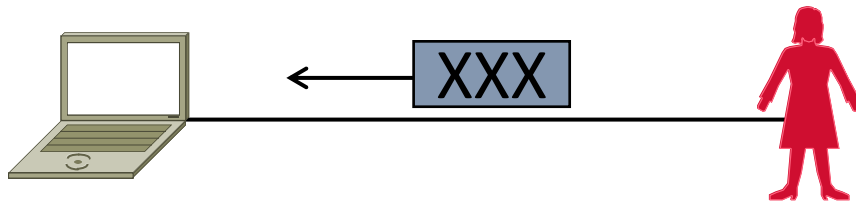
MORE STORIES

Internet Reality

- DDoS is a huge problem today!
 - GitHub attack of 1tbps
- There are no great solutions
 - CDNs, network traffic filtering, and best practices all help

Host Denial-of-Service

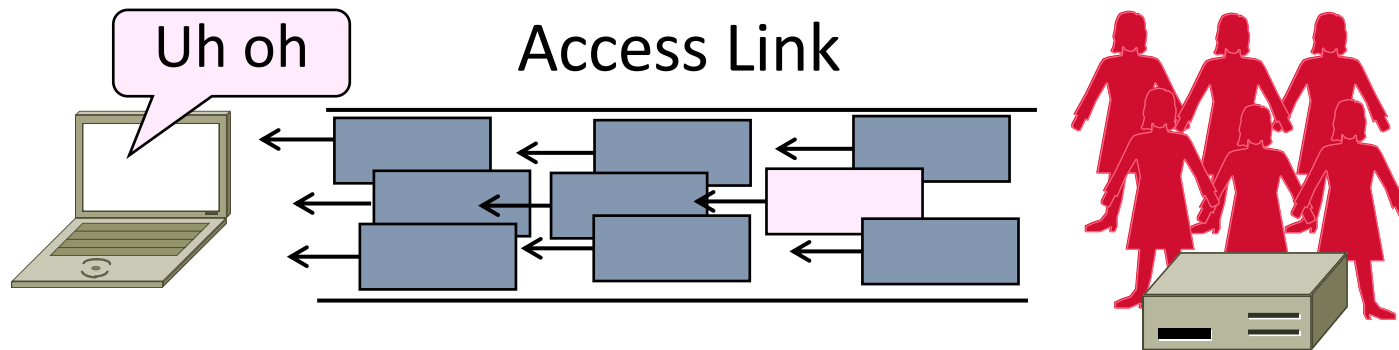
- Strange packets can sap host resources!
 - “Ping of Death” malformed packet
 - “SYN flood” sends many TCP connect requests and never follows up
 - Few bad packets can overwhelm host



- Patches exist for these vulnerabilities
 - Read about “SYN cookies” for interest

Network Denial-of-Service

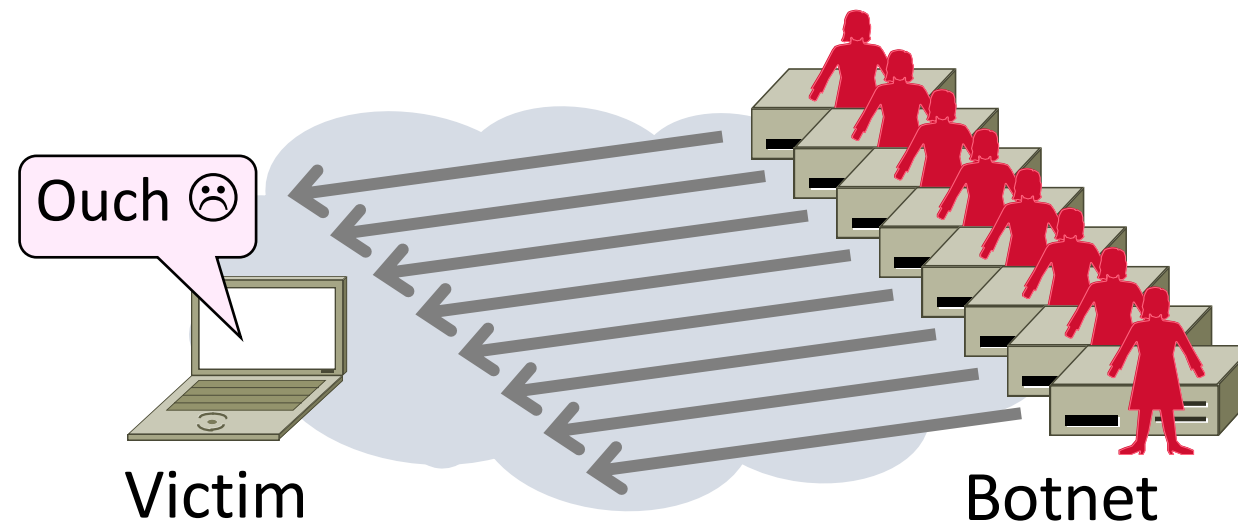
- Network DOS needs many packets
 - To saturate network links
 - Causes high congestion/loss



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

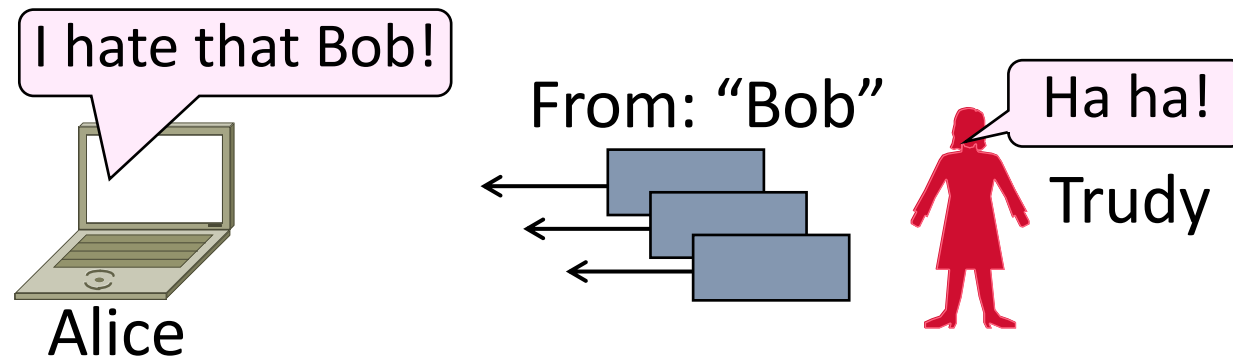
Distributed Denial-of-Service (DDOS)

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



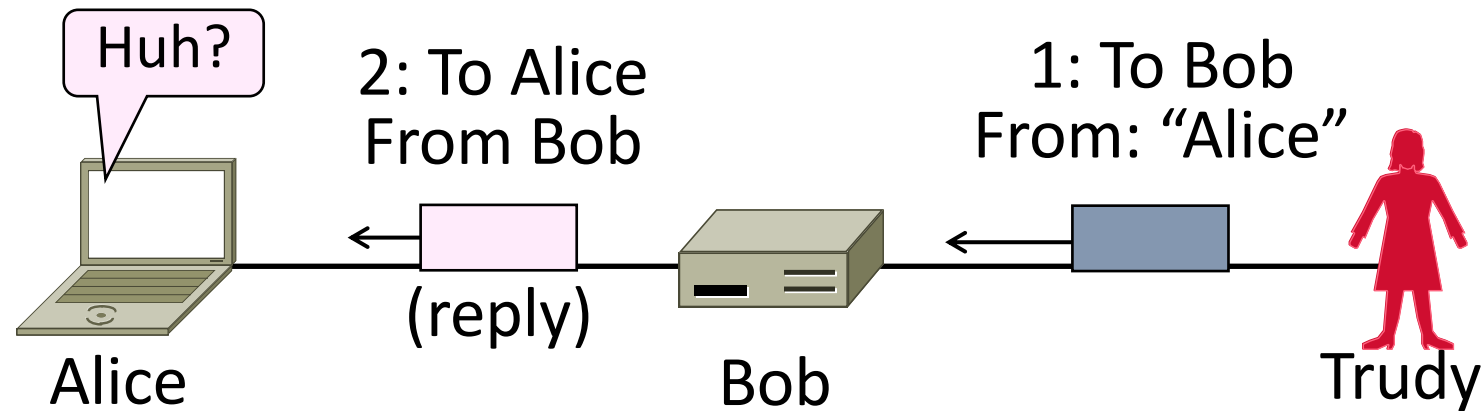
Complication: Spoofing

- 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



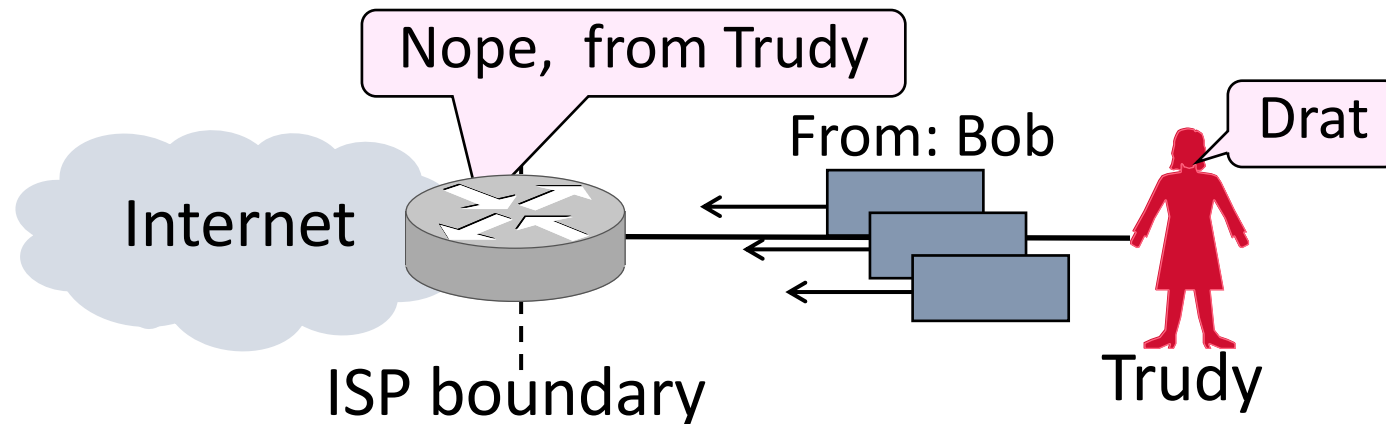
Spoofing (2)

- 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