CPSC 317 COMPUTER NETWORKING

Module 8: Security – Day 6 – Availability

Some slides based on Kurose/Ross original slides, found at https://gaia.cs.umass.edu/kurose_ross/ppt.htm

LEARNING GOALS

- Describe the security principle of availability
- Describe a denial-of-service attack
- Describe a distributed-denial-of-service attack
- Explain the principle of amplification in the context of denial-of-service
- Define malware, virus, worm, botnet

READING

- Reading: 8.9

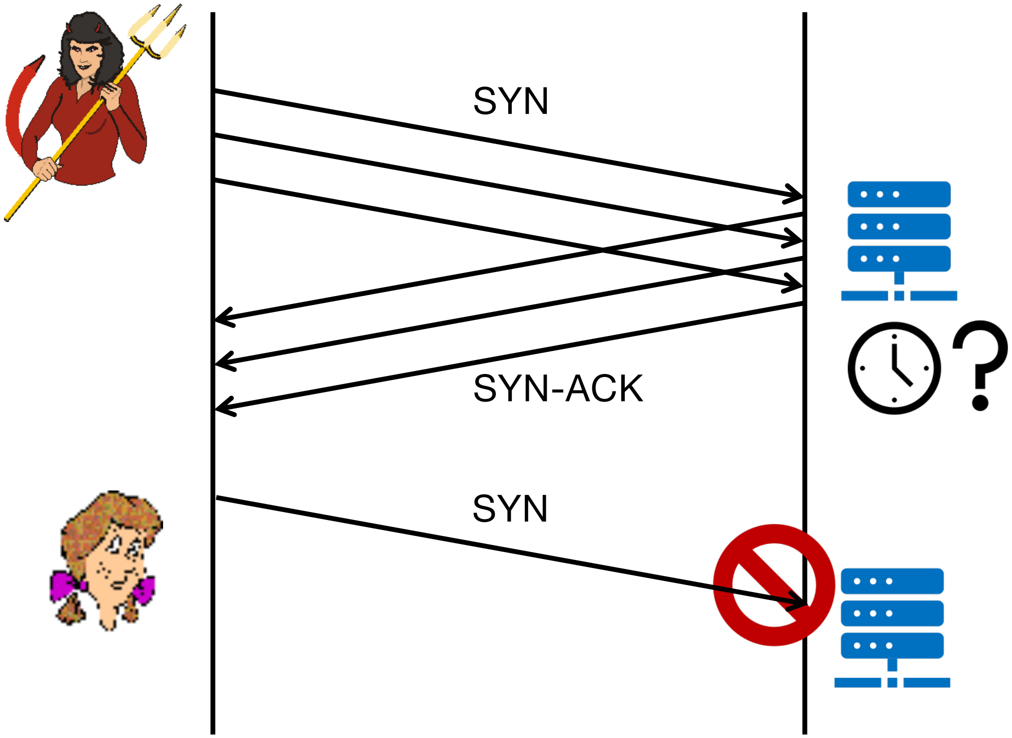
PRINCIPLES OF SECURITY

- ***confidentiality***: only the sender and the intended receiver should "understand" message contents
  - sender encrypts message
  - receiver decrypts message
- ***authentication***: the sender and receiver want to confirm each other's identity
- ***message integrity***: the sender and receiver want to ensure that the message is not altered (in transit, or afterwards) without detection
- ***access and availability***: services must be accessible and available to users

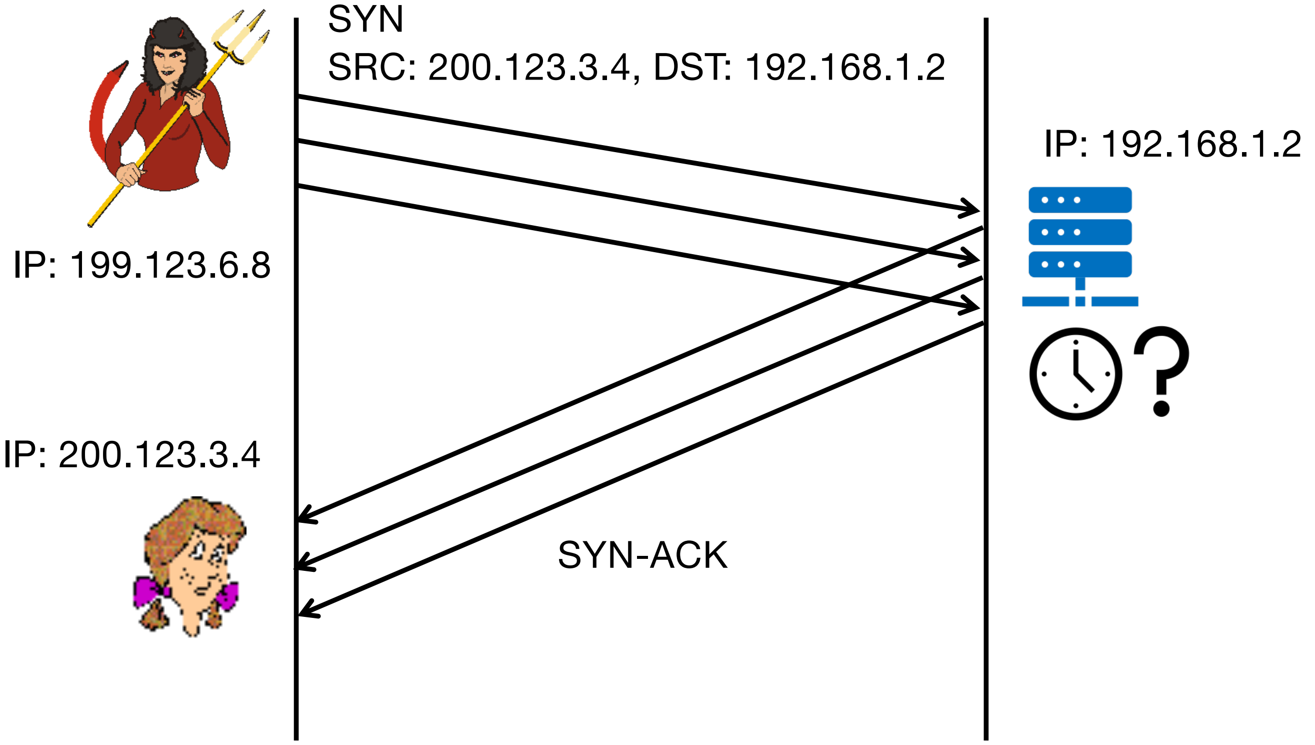
HOW CAN TRUDY MAKE A SERVICE UNAVAILABLE?

- Crash a service or the host it runs on
  - Depends on some vulnerability in the service or the host
- Overwhelm the service with data so it doesn’t have time or other resources to do its “normal” work
- Denial of service attack can target any resource
  - Bandwidth
  - Connections
  - Memory

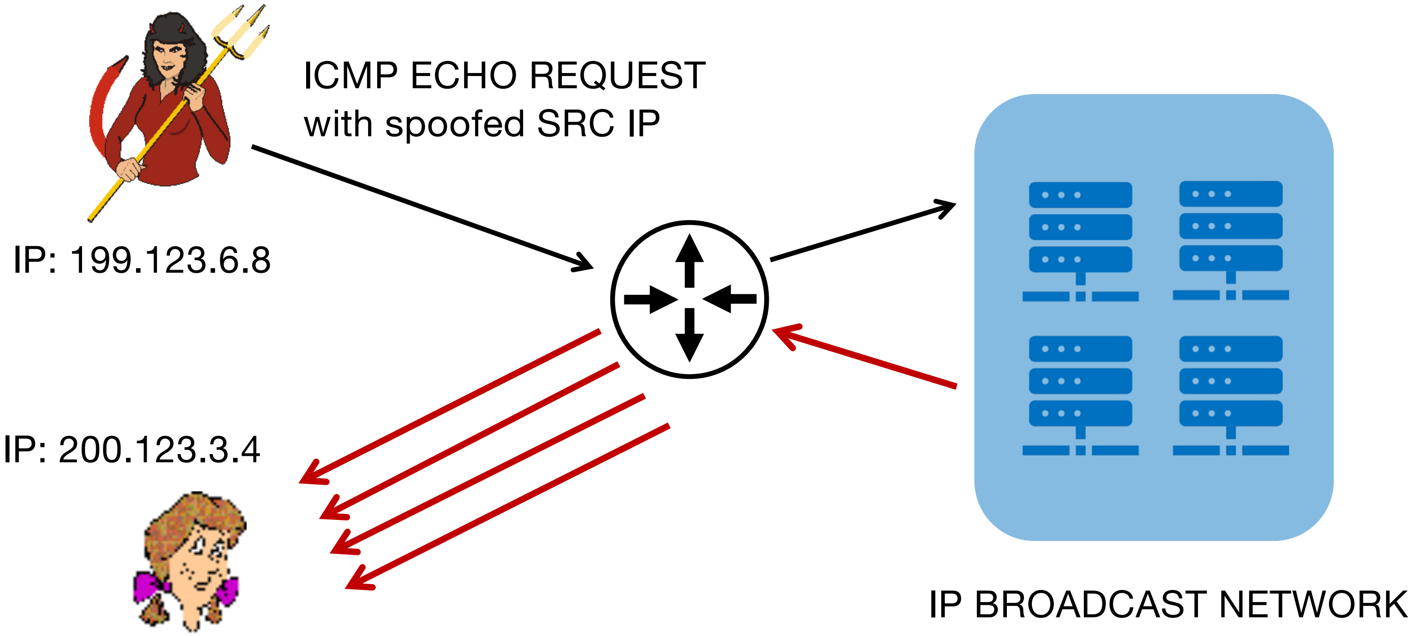
SYN FLOOD ATTACK – PART 1



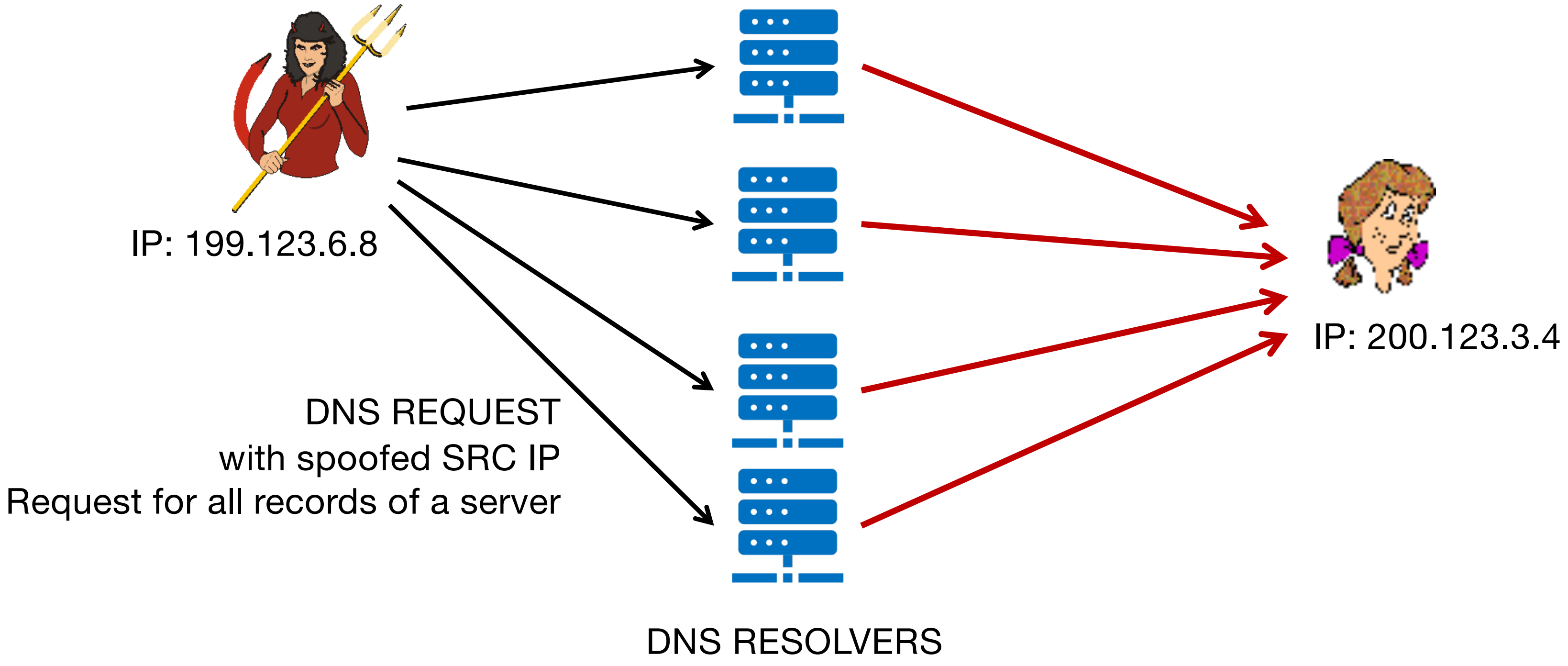
SYN FLOOD ATTACK – PART 2



SMURF ATTACK



DNS AMPLIFICATION ATTACK



DOS MITIGATIONS

- Disable broadcast addresses
- Firewalls
  - Reject UDP traffic from outside
  - Rate limit ICMP pings
- Source IP verification
  - ISPs reject traffic with spoofed IP addresses
- Reduce open DNS resolvers
  - Respond only to queries from trusted sources

AMPLIFICATION EFFECT

- Most effective denial-of-service attacks exploit amplification
  - An attacker triggers their botnet to all send data to a particular service or host
    - 1 attacker -> 10000 bots

MALWARE

- Anything designed to compromise or harm a host
- Malware goals include:
  - Accessing private data
  - Destroying data
  - Holding data hostage
  - Controlling the host for other purposes

VIRUS

- Malware that depends on a user action to infect the host
- Compromised:
  - Executable files
  - Documents
  - Email messages
- Phishing emails containing links

WORM

- Malware that infects a host without user action
- Takes advantage of software with vulnerabilities
- Especially vulnerable is software that accepts data across the network:
    - Web servers
    - SSH servers
    - Database servers

BOTNET

- A collection of compromised hosts used for evil purposes
- Sending spam email
- Organized attacks on other services

FAMOUS DDOS ATTACKS

- Estonia attack (Apr 2007)
  - Targeted online govt. services, financial institutions, media outlets
  - Considered the first act of cyber warfare
- Mirai Dyn attack (Oct 2016)
  - Attacked Dyn, a major DNS provider
  - Mirai botnet consisted of 100,000s of compromised IoT devices (cameras, smart TVs, and even baby monitors)
  - Disrupted Airbnb, Netflix, PayPal, Visa, Amazon, NYT, Reddit, Github …

FAMOUS DDOS ATTACKS

- Github attack (Feb 2018)
  - Attacked memcached, a database caching service
  - Peak attack rate: 127 million packets/s, 1.3 Tbps
- AWS attack (Feb 2020)
  - Attacked LDAP web servers (user access control)
  - Peak attack rate: 2.3 Tbps!

FAMOUS DDOS ATTACKS

- HTTP/2 Rapid Reset attack (Aug 2023 – Oct 2023)
  - Cloudfare - 201 million requests per second
  - Google – 398 million requests per second
  - AWS - 155 million requests per second
    - Total web request rate is 1-3 billion requests per second
  - Botnet of 20,000 machines
  - Depends on a weakness of HTTP/2 – Rapid Reset
  - A client can create and cancel requests without limits
    - The server sees and at least starts work on all of them

DDOS MITIGATIONS

- Prevention
  - Change default passwords on IoT devices
  - Update OS
  - Do not click on suspicious links
- Mitigation of an attack can take time
  - Monitor traffic and detect attack
  - Activate firewalls, rate limits
  - Find root of botnet

FILL UP SEI SURVEY

IN-CLASS ACTIVITY

- ICA86