Networking Security Wrap-Up and How the Web Works

CMSC 23200, Spring 2026, Lecture 11

David Cash and Grant Ho, and
Special Guest Lecturer: Blase Ur!

University of Chicago, 04/28/2026
(Slides adapted from Vern Paxson)

Logistics

- Midterm: May 5 (next week) in-class!

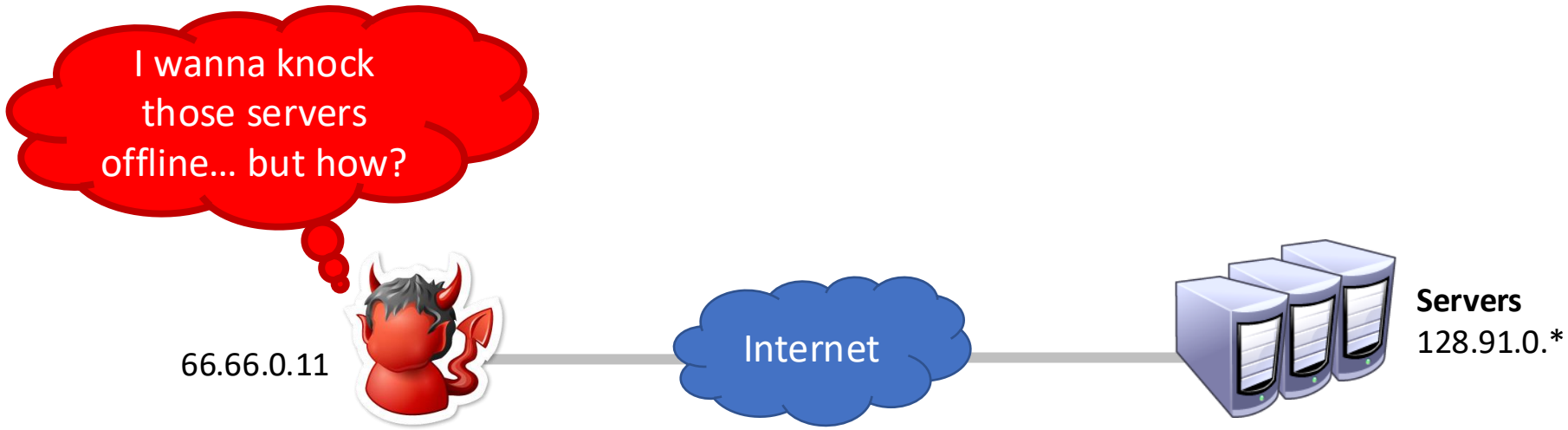
Outline

- Denial of Service (Network Availability Attacks)

- How the Web Works

Denial of Service (DoS) Attacks

- **Threat Model:** Active attacker who can freely send packets to target
- **Goal:** Prevent users from being able to access a target: specific computer, service, or piece of data (Disrupt Availability)



Denial of Service (DoS): Availability

Two main DoS Strategies:

1. Exploit program flaws (e.g., bug that crashes the target)
2. Exhaust the target's resources (CPU, memory, bandwidth, etc.)

Often very easy to perform… but difficult to mitigate ☹

DoS from program flaws = fairly straightforward

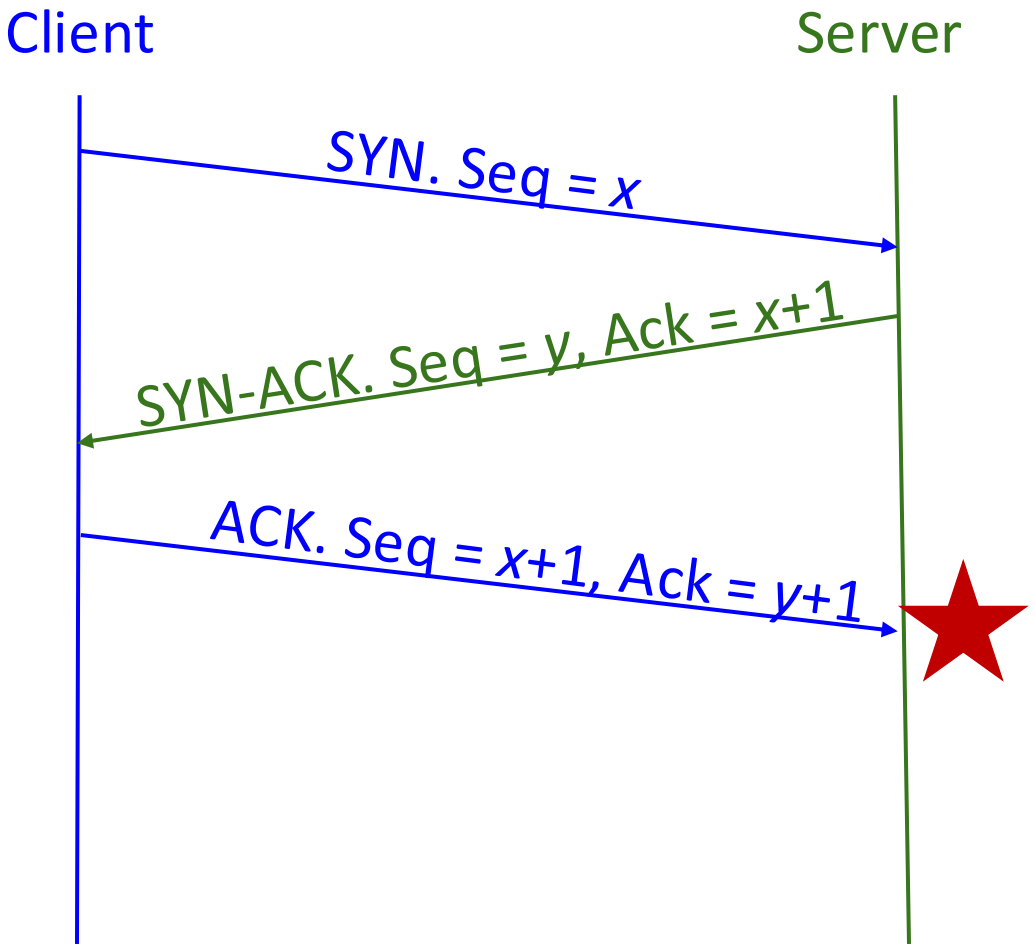
- Most attacks we'll discuss focus on resource exhaustion

DoS Attack Parameters

- Asymmetric Attack:
  - Attacker either generates a much larger cost at the target, or has much more resources (e.g., bandwidth) than the target

- What kind of packets does the attacker send to the victim?
  - Minimize effort and risk of detection for attacker
  - While also maximizing damage to the target

TCP SYN Flooding



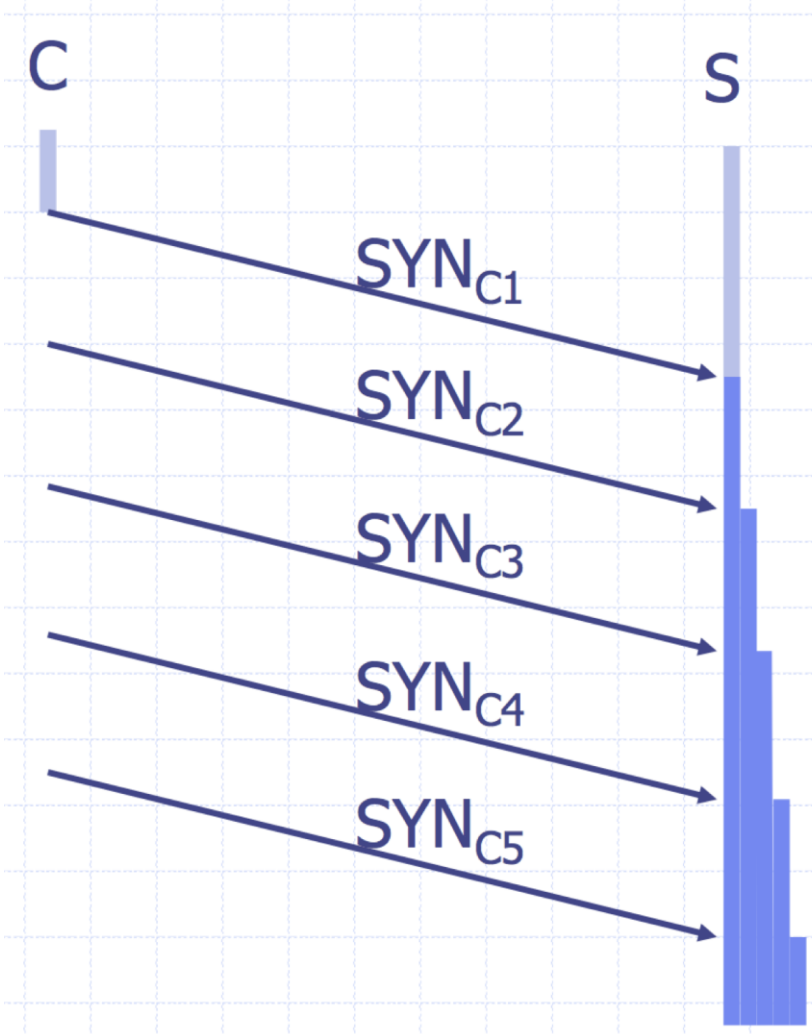
Server stores state during TCP handshake:

- Allocates memory to validate that client's ACK number is correct

Attack: Flood the target with SYN packets

- Exhausts available memory for target: no more connections
- Asymmetry: Easy to Spoof many SYN packets & attacker doesn't need state

TCP SYN Flooding



Single machine:

- SYN Packets with **random source IP addresses**
- Fills up backlog queue on server
- No further connections possible

SYN Flooding Defenses

- **Core Problem:** Server commits resources without confirming client's identity or requiring them to commit resources

- **Defense Approach #1:** Overprovision
  - Have lots of servers with lots of memory
  - Drawbacks: expensive + target server might not be able to acquire sufficient resources vs. motivated attacker

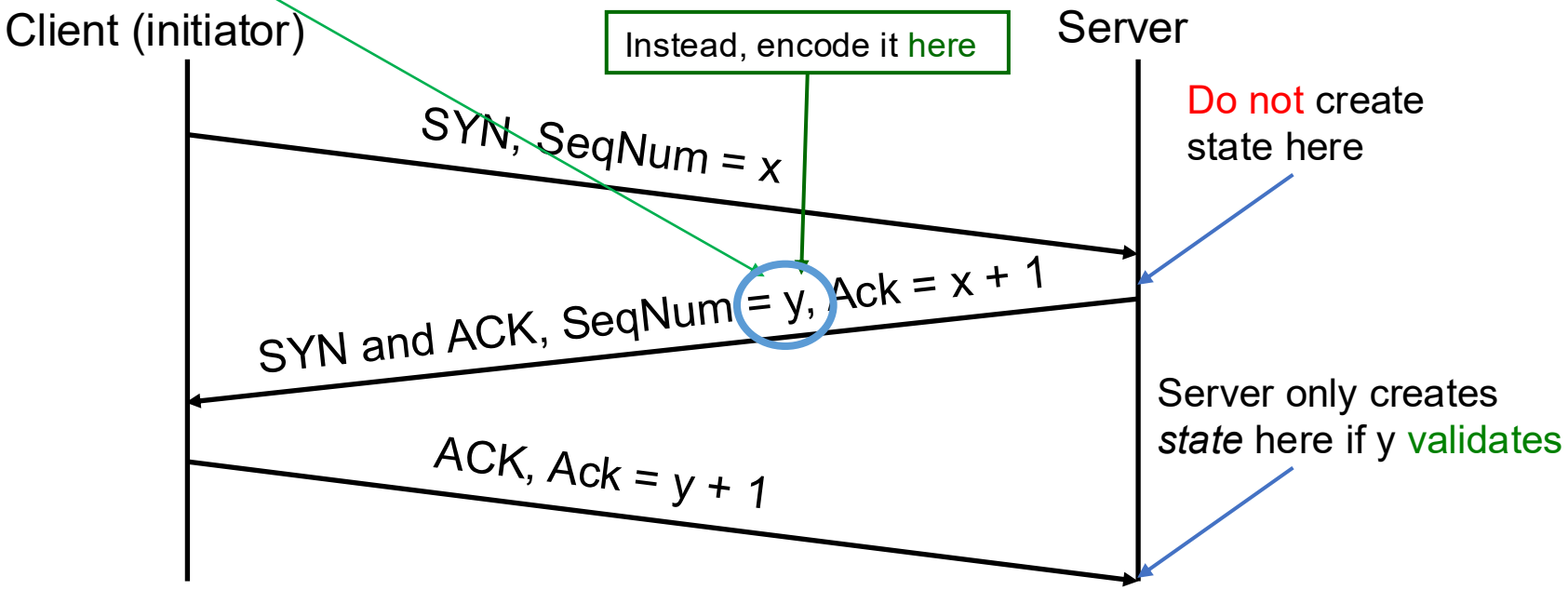
SYN Flooding Defenses

- **Approach #2:** Detect & Filter
  - Server can try to identify packets that are SYN Flooding & ignore them
  - Drawbacks: hard to identify them
    - Only have src IP address in packets
    - But the attacker can spoof these src IP addresses!

- **Approach #3:** Change the ACK validation so the server doesn't have to store state!
  - Practical Defense: SYN cookies

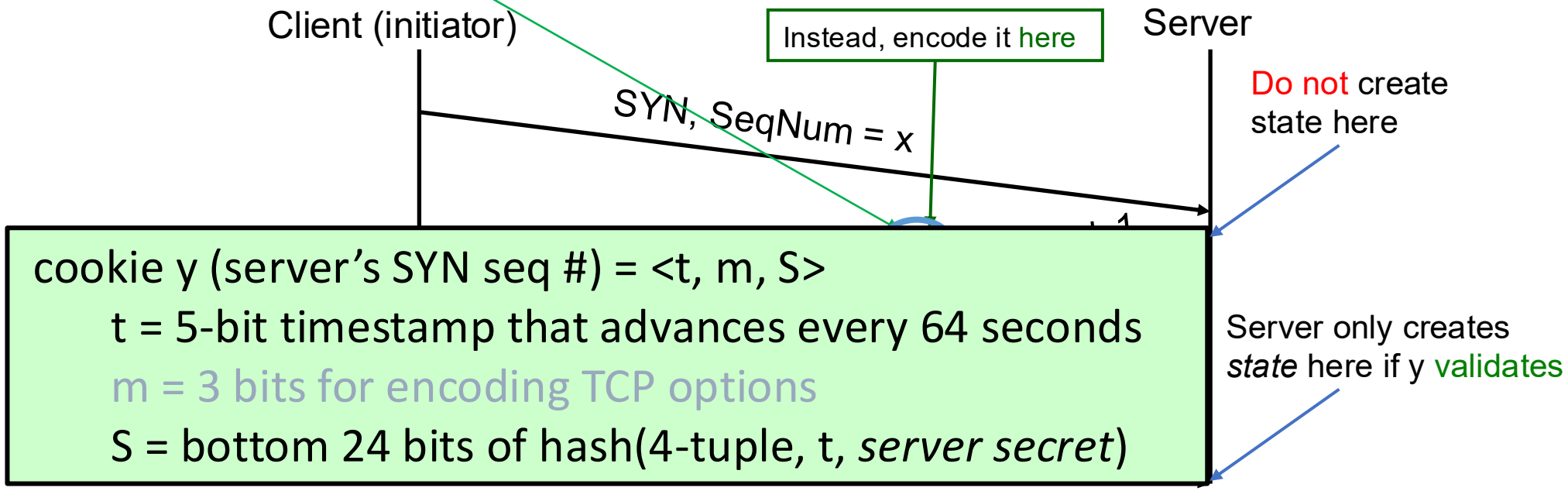
Practical Defense: *SYN Cookies*

- Server: when SYN arrives, encode critical state entirely within SYN-ACK's sequence # y !
  - y = *encoding* of necessary state, using server secret
- When ACK of SYN-ACK arrives, server only creates state ***if*** value of **y** from it agrees w/ secret



Practical Defense: *SYN Cookies*

- Server: when SYN arrives, encode critical state entirely within SYN-ACK's sequence # y !
  - y = *encoding* of necessary state, using server secret
- When ACK of SYN-ACK arrives, server only creates state ***if*** value of **y** from it agrees w/ secret



Reflection & Amplification Attacks

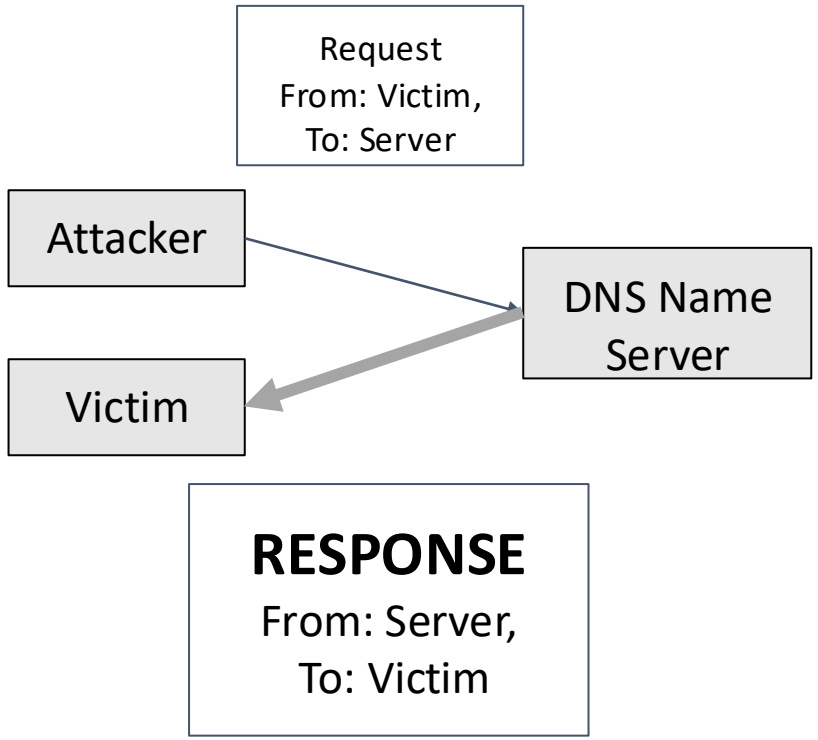
SYN Flooding: exhaust *memory* of server

Network DoS: exhaust *network bandwidth* of server / client

- Amplification Attacks: Exploit asymmetry in protocols, where a network request packet generates much greater response traffic
- Reflection Attacks: Use third-party machines (not controlled by attacker) to flood the target
- Amplification + Reflection often used together

UDP Amplification & Reflection

- Some protocols / commands generate large responses for a single (small) request
  - DNS: Query type "*ANY*" returns all records server has about a domain
  - NTP: MONLIST returns list of last 600 clients who asked for the time recently
- Attack: Spoof requests from target machine's src IP address to other services
  - Typically use UDP-based protocols: Why?



Preventing Spoofing: Ingress & Egress Filtering

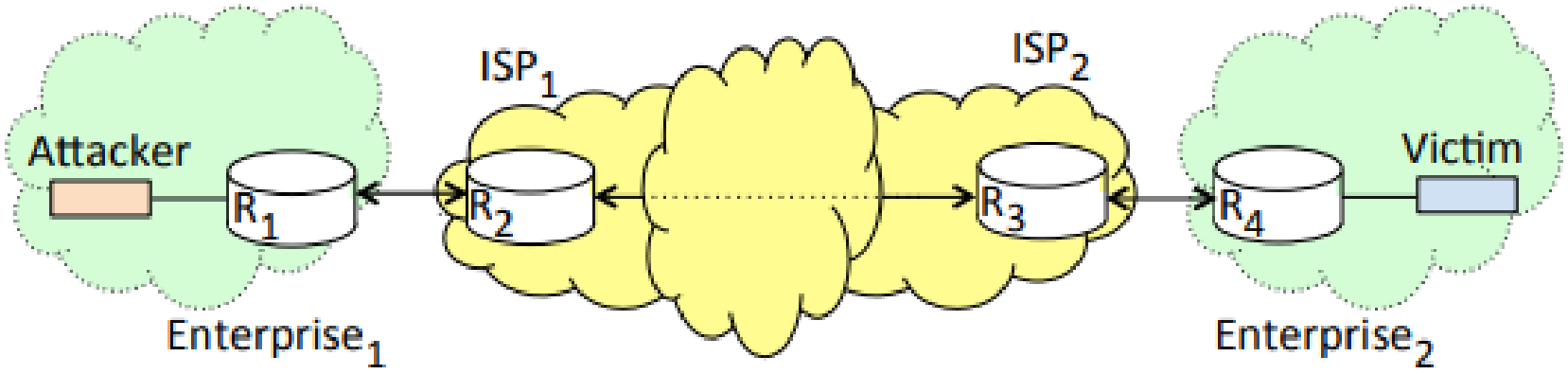
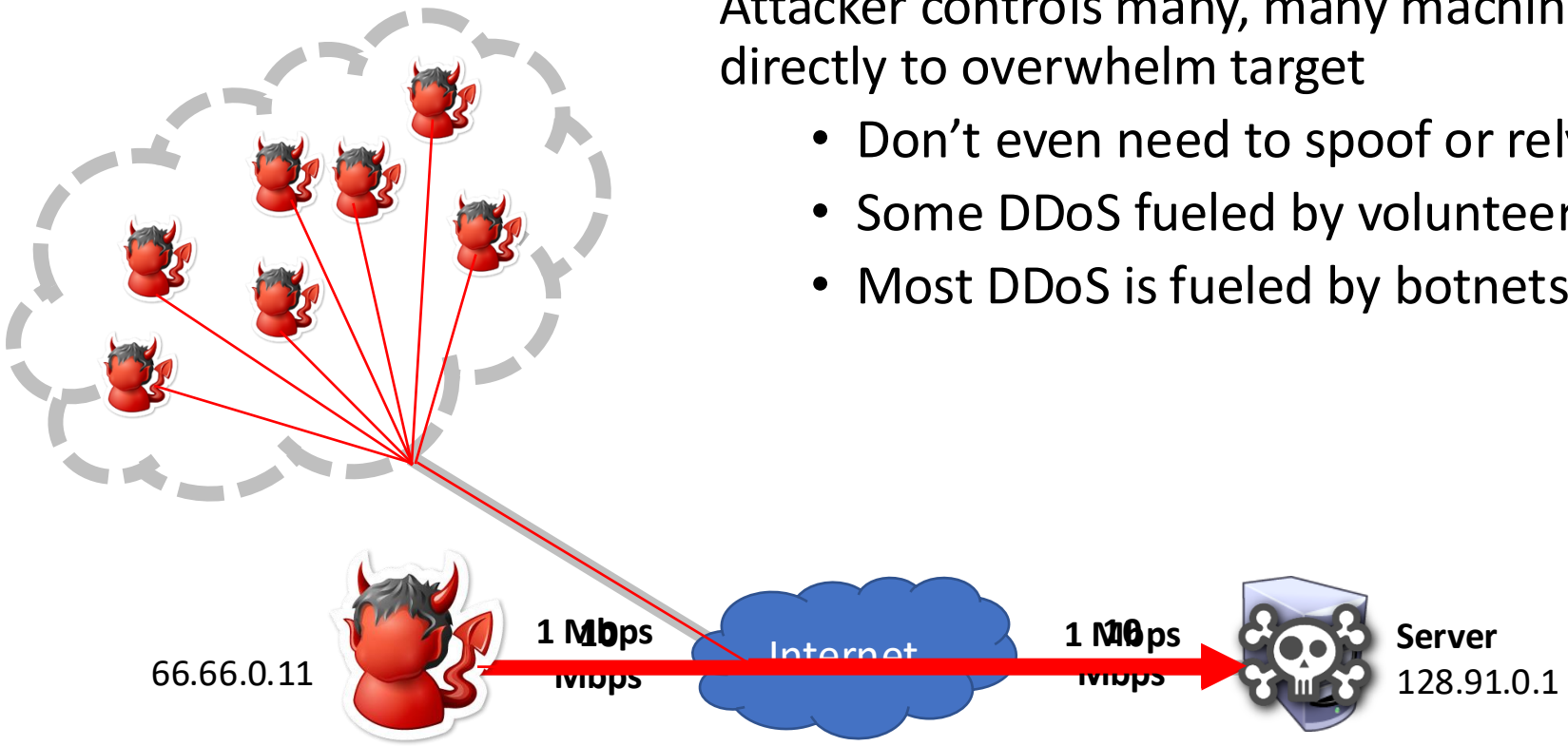


Figure 11.6: Ingress and egress filtering. An attacker may use a spoofed source IP address in traffic sent to a victim. ISP_1 does ingress filtering at R_2 for traffic entering from $Enterprise_1$. $Enterprise_1$ does egress filtering at R_1 for traffic leaving to ISP_1. For firewall rules to implement ingress and egress filtering, see Table 10.1 in Section 10.1.

- Networks know which IP addresses belong to them and
- ISPs/ASNs know which IP addresses they've given to sub-networks

Distributed Denial of Service (DDoS) Attacks



Attacker controls many, many machines and uses them directly to overwhelm target

- Don’t even need to spoof or rely on UDP protocols
- Some DDoS fueled by volunteers (e.g. Anonymous)
- Most DDoS is fueled by botnets (e.g., Mirari)

Content Delivery Networks (CDNs)

- CDNs help companies scale-up their websites
  - Cache customer content on many replica servers
  - Users access the website via the replicas
- Examples: Akamai, Cloudflare, Rackspace, Amazon Cloudfront, etc.
- Side-benefit: DDoS protection
  - CDNs have many servers, and a huge amount of bandwidth
  - Difficult to knock all the replicas offline
  - Difficult to saturate all available bandwidth
  - No direct access to the master server
- Cloudflare: 15 Tbps of bandwidth over 149 data centers

Content Delivery Networks (CDNs)