DoS Attacks

Ramin Sadre

DoS Attacks

- Goal: Overload or crash a server to make the service unavailable to legitimate users

- Two types of attacks:
  1. Semantic (“smart”) attacks
  2. Brute-force attacks

Semantic attacks

- Goal: Make the server busy/non-functional by sending specific requests
- Examples:
  - Send SQL queries to a SQL database that need a lot of CPU/disk/memory
  - Send requests that trigger programming errors in the server and crash it
  - Slowloris: Send “half” HTTP request to a web server. The server will keep the connection open and wait for the remainder of the request → running out of TCP connections

- Semantic attacks are “cheap” for the attacker but require specific knowledge of the target

Brute-force attacks

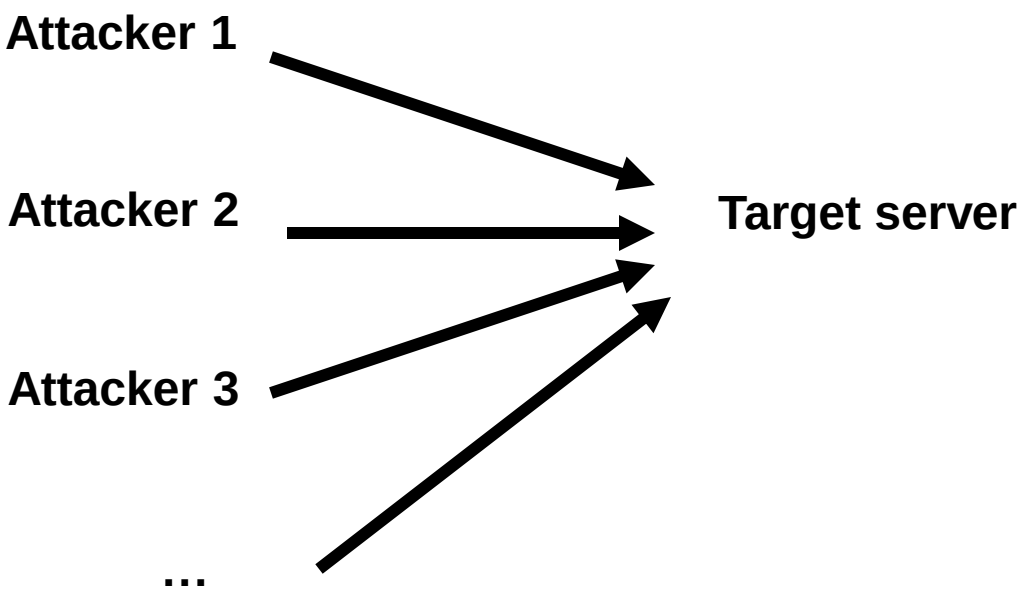
- Goal: Overwhelm the server by sending many requests
- Examples: Send many requests to …
  - fill the network link of the server
  - exhaust number of TCP connections in server (SYN flooding)
  - exhaust number of application sessions in server

- Brute-force attacks do not need special knowledge, but the attacker needs enough resources (network bandwidth, CPU,…)
- Furthermore, it is easy to defend against such an attacker: block their IP address

- How to “improve” such attacks?

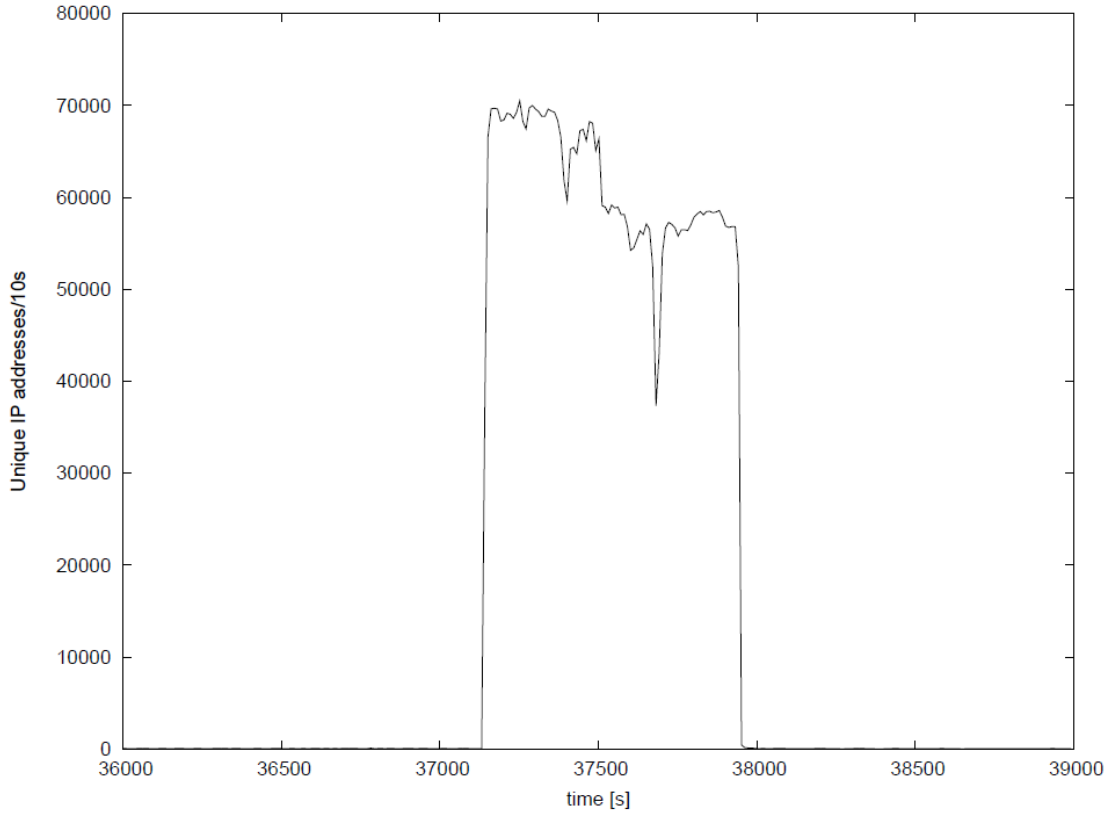
Distributed DoS (DDoS)

- Coordinated attack from multiple hosts
- More attack resources + makes blocking harder

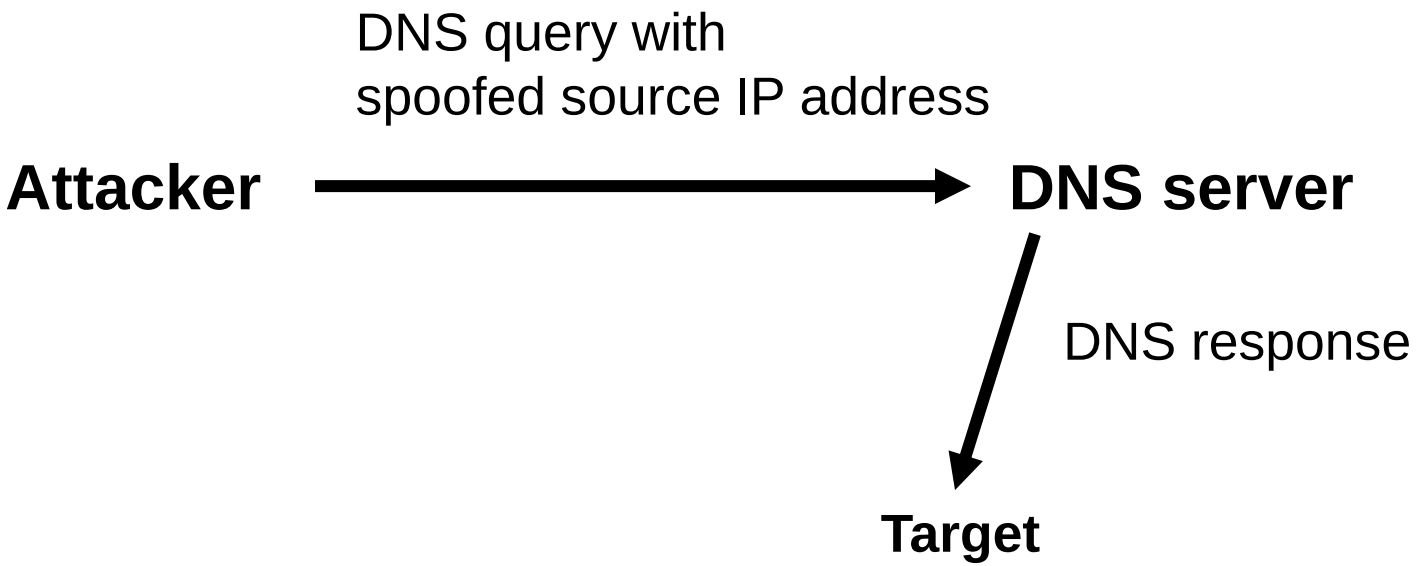


DDoS against IRC Server

- 375 Million SYN packets in 800 seconds



Reflected DoS Attack (DRDoS)



- Usually as DDoS attack: multiple attackers, multiple DNS servers
- DRDoS attacks are useful to hide your IP address from the target, but there is also another advantage…

Amplification

- Amplification = The response is larger than the request
- “Solves” the bandwidth problem for the attacker
- Example DNS:
  - Original DNS version: 60 bytes query → 512 bytes answer (8.5x) maximum
  - EDNS (RFC 2671) allows larger answers
  - Combining different response types:
    answers larger than 4000 bytes possible (>60x)

- In 2006, Vaughn&Garon studied DDoS attacks with up to 140,000 DNS servers, resulting in 10Gbps
- In 2016, attack of 65Gbps observed

Amplification (2)

- DNS servers are very popular for such attacks because
  - They are open to anybody
  - They use UDP (perfect for spoofing)
  - They are made to handle high loads
- Open + Large number of servers + High amplification factor = perfect for DRDoS

- Other services possible, of course
  - NTP
  - CharGen
  - memcached
  - …

DoS Mitigation

Best practices

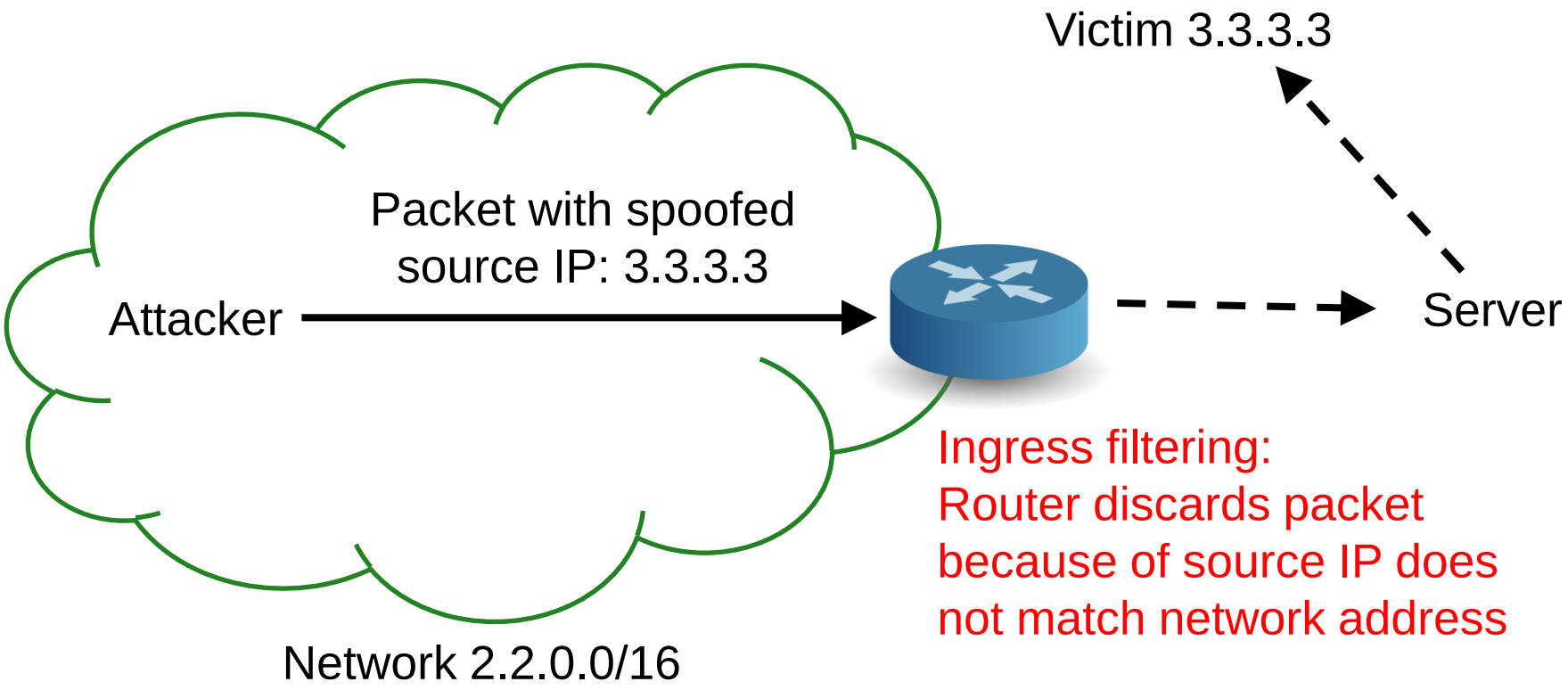
- Do not let open services that can be misused for DRDoS attacks
  - Switch off unused services
  - Filter accesses to such services

  … more or less impossible for DNS

- Implement ingress filtering against reflective attacks

Network Ingress Filtering

- IETF Best Current Practice document #38 (BCP38)
- Unfortunately, many networks still do not implement BCP38



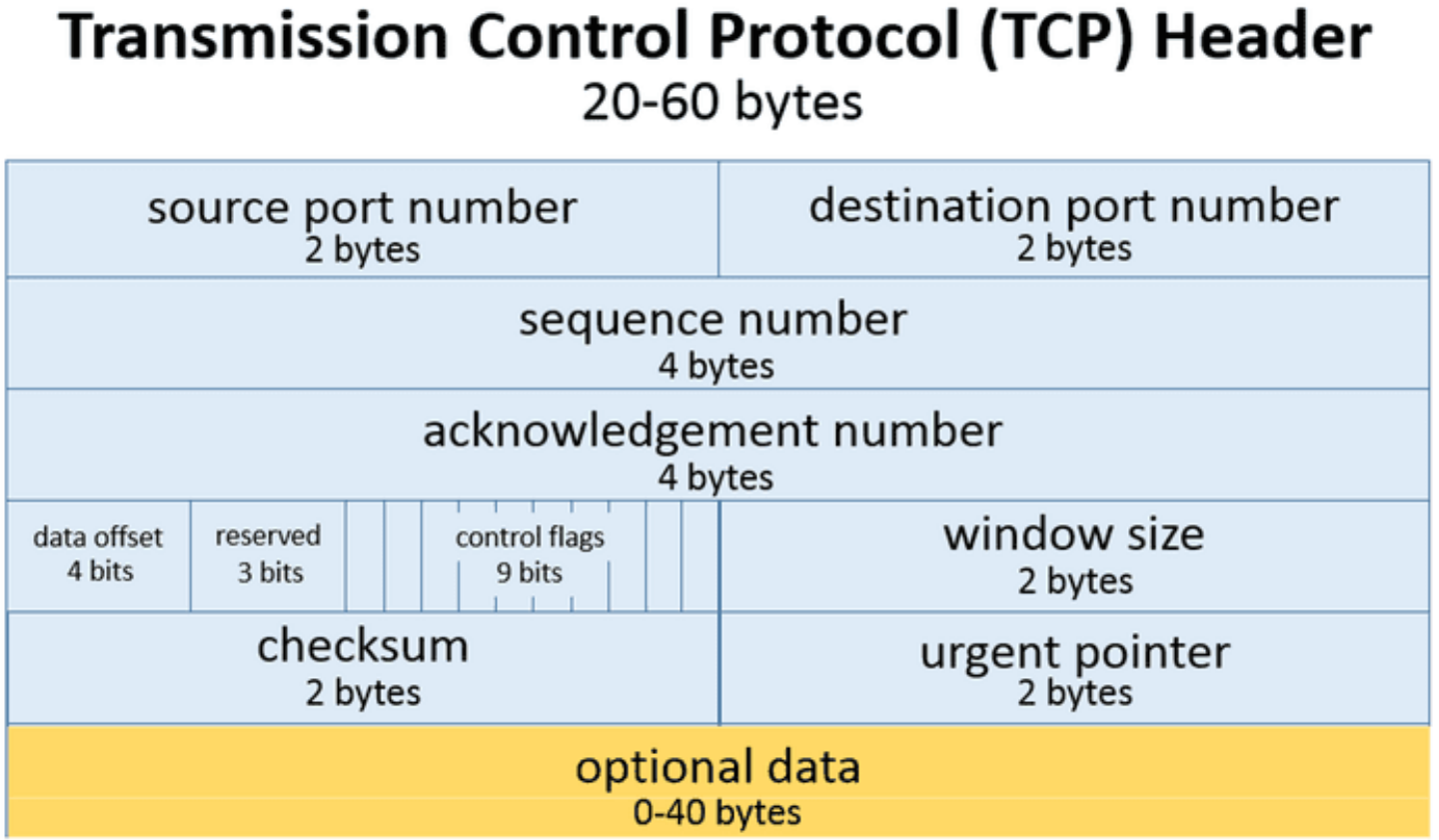
Protection against SYN Flooding

- Normal TCP handshake between hosts A and B
  1. A sends SYN packet to B
  2. B sends SYN+ACK packet to A
  3. A sends ACK packet to B

- In SYN flooding, host A sends many SYN packets to B
  - Each SYN packet consumes memory in B because the operating system allocates data structures for the (assumed) TCP connection

- How to avoid that?

TCPv4 Header



https://www.lifewire.com/tcp-headers-and-udp-headers-explained-817970

SYN Cookies

1. A sends SYN packet to B (e.g. the webserver)
2. B sends SYN+ACK packet to A
   - The packet contains a special value N ("SYN cookie") as initial 32-bit sequence number
     - 6 bits = lower 6 bits of a clock with 64s resolution
     - 2 bits = maximum segment size sent by the client
     - 24 bits = result of cryptographic hash function applied to the timestamp, IP addresses and port numbers of A and B
   - B does not allocate memory for the connection!
3. A sends ACK with ack number $N + 1$ to B
   - B checks N. If the cookie is okay and not too old, it is very likely that A sent SYN before
   - B now allocates memory for the connection

SYN Cookies (2)

- Advantages:
  - Only has to be implemented in the server
  - No modifications in the client required
  - By putting the cookie in the sequence number field of TCP, everything is TCP conform
- Disadvantages:
  - Server will forget all TCP options sent by the client in the TCP SYN packet (except MSS)
  - Only four different values for MSS

- More details:

https://blog.cloudflare.com/syn-packet-handling-in-the-wild/

DoS protection services

- Companies like Akamai, Cloudflare,… offer (paid) protection against DoS attacks for web sites

- How it works:
  1. The protection service has a very powerful infrastructure (datacenters, cloud) with DoS filters
  2. Traffic to the website is redirected to the infrastructure. Different ways possible:
     - Change DNS record of the web site
     - BGP diversion
  3. The infrastructure “cleans” the traffic and then forwards it to the original website