DDoS attacks on electronic payment systems

Sean Rijs and Joris Claassen
Supervisor: Stefan Dusée
Scope

- High volume DDoS attacks
- Electronic payment systems
  - Low bandwidth requirements:
    - €5 from account X to account Y
Research Question

What is the implementation difficulty and how effective is a subset of DDoS protection measures to keep electronic payment systems available?

- Whitelisting
- Robust DNS resolution
- Scrubbing
DDoS testing environment

Virtualisation host

Target VM

Switch

1 Gbps

Desktops

attackers with one legit desktop
DDoS testing environment

Generate attack packets from our C&C desktop:

```
parallel-ssh -h nodes \
sudo hping3 --flood -S 172.16.1.10 \
--destport 5001 --data 8000
```
Whitelisting
Whitelisting

Implementation difficulty:

iptables - A FORWARD -i eth0 - s 145.100.0.0/15 - j ACCEPT
iptables - A FORWARD -i eth0 - j DROP
ip6tables - A FORWARD -i eth0 - s 2001:610::/32 - j ACCEPT
ip6tables - A FORWARD -i eth0 - j DROP
Whitelisting

Hypothetical:
- Ingress link will be saturated
- Packet loss will occur on the opposite port
- Whitelisting should not be effective
Whitelisting

Test:
- `hping3 -c 1000 --fast targetvm`
- sends 1000 TCP packets, 10 packets per second
Whitelisting

Results:

- DDoS attack on VM with 1Gbps link
Whitelisting

Cause:

• Packets never reach the whitelist
Whitelisting

```
$snmpwalk -Os -c public -v 1 switchaddress ifOutDiscards
ifOutDiscards.1 = Counter32: 3248
...
ifOutDiscards.20 = Counter32: 3251
ifOutDiscards.21 = Counter32: 272661695
```

RFC1158:
"The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space."
Robust DNS Resolution

• DNS
  • Not designed with DDoS in mind
• Confidentiality, Integrity, Availability
  • DNS is not confidential
  • Integrity can be guaranteed using DNSSEC
    • But falls out of scope
  • Availability
Robust DNS Resolution

Hypothesis:

• TCP should be more reliable
  • Due to retransmitting of packets
• Distributing DNS
  • Anycast
Robust DNS Resolution

Test; UDP vs TCP:
Robust DNS Resolution

Cause:

• TCP ACK retransmit failed
  • More congestion
    • More TCP retransmits
  • TCP slows down packet flow
    • But this does not even matter
    • DDoS keeps the ingress link full
Robust DNS Resolution

- Anycast does work
  - Global network required
- DNS Root servers
  - Attacked many times
Scrubbing

Internet

Tunnel

Normal Traffic

Traffic while under DDoS

Border router(s)

Electronic Payment System

Users

Scrubbing Centre

Border router(s)
Scrubbing

• Traffic redirection
  • BGP anycast
  • On-demand / always-on

• Scrubbing Centre
  • Blackholing
  • Sinkholing
Scrubbing

Hypothesis:
• The local endpoint is vulnerable
• We can hide the local tunnel endpoint
Scrubbing

Test; hiding the local endpoint; no filter:

user@client:~$ traceroute 172.16.1.2
traceroute to 172.16.1.2 (172.16.1.2), 30 hops max, 60 byte packets
  1  172.16.1.1 (172.16.1.1)  0.267 ms  0.255 ms  0.246 ms  
  2  172.16.1.2 (172.16.1.2)  0.401 ms  0.356 ms  0.338 ms 

user@client:~$ traceroute -U 172.16.1.2
traceroute to 172.16.1.2 (172.16.1.2), 30 hops max, 60 byte packets
  1  172.16.1.1 (172.16.1.1)  0.293 ms  0.268 ms  0.250 ms  
  2  172.16.1.2 (172.16.1.2)  0.358 ms  0.342 ms  0.326 ms 

user@client:~$ sudo traceroute -T 172.16.1.2
traceroute to 172.16.1.2 (172.16.1.2), 30 hops max, 60 byte packets
  1  172.16.1.1 (172.16.1.1)  0.235 ms  0.207 ms  0.183 ms  
  2  172.16.1.2 (172.16.1.2)  0.347 ms  0.326 ms  0.320 ms 

21
Scrubbing

Test; hiding the local endpoint; applying filter:

Drop all incoming packets
iptables -A INPUT -i eth0 -j DROP
ip6tables -A INPUT -i eth0 -j DROP

Accept packet forwarding from tunnel endpoint
iptables -A FORWARD -i eth0 -s 172.16.1.3/32 -j ACCEPT
iptables -A FORWARD -i eth0 -j DROP
ip6tables -A FORWARD -i eth0 -s 2001:DB0::1/128 -j ACCEPT
ip6tables -A FORWARD -i eth0 -j DROP

Prevent packets to be sent out
iptables -A OUTPUT -i eth0 -j DROP
ip6tables -A OUTPUT -i eth0 -j DROP
Scrubbing

Test; hiding the local endpoint; after applying filter:

user@client:~$ traceroute 172.16.1.2
traceroute to 172.16.1.2 (172.16.1.2), 30 hops max, 60 byte packets
  1  *   *   *
  2  172.16.1.2 (172.16.1.2)  0.309 ms  0.324 ms  0.317 ms

user@client:~$ traceroute -U 172.16.1.2
traceroute to 172.16.1.2 (172.16.1.2), 30 hops max, 60 byte packets
  1  *   *   *
  2  172.16.1.2 (172.16.1.2)  0.519 ms  0.530 ms  0.525 ms

user@client:~$ sudo traceroute -T 172.16.1.2
traceroute to 172.16.1.2 (172.16.1.2), 30 hops max, 60 byte packets
  1  *   *   *
  2  172.16.1.2 (172.16.1.2)  0.386 ms  0.352 ms  0.394 ms
Scrubbing

But...

• No golden ticket

• Depends on secrecy of IP address
  • Of the local tunnel endpoint
  • Social engineering
    • Internal documents
Conclusion

• Whitelisting
  • Does not protect against high volume DDoS attacks

• Robust DNS Resolution
  • TCP performs worse than UDP
  • Anycast works
    • And helps keeping DNS-based applications available

• Scrubbing
  • Does protect against high volume DDoS attacks
  • But...
    • Only when combined with whitelisting
    • And secrecy of the local tunnel endpoint IP
Future research

• Layer 7 DoS attacks in electronic payment systems
• Combining layer 3/7 attacks also known as "smoke and mirrors"
• What is the best way to create a deterministic DDoS setup
Future research

DDoS attack on VM with 100Mbps link
Questions