Karlsruhe Institute of Technology

Resilient Networking
Module 5: Denial of Service

Thorsten Strufe – *This module prepared in cooperation with Günter Schäfer, Mathias Fischer, and the members of the Chair.*

Winter Term 2020 – KIT/TUD

Competence Center for Applied Security Technology

Denial of Service

- Classification
- DoS examples
  - Exploiting IP fragmentation and assembly
  - Abusing ICMP: Smurf attack
  - TCP SYN-Flood attack
  - DDoS
  - Botnets
  - DRDoS
- Countermeasures against DoS
  - Crypto Puzzles
  - Stateless Protocols
  - Avoid IP address spoofing / identifying malicious nodes
  - Filtering attack traffic
  - Industry solutions to DDoS mitigation

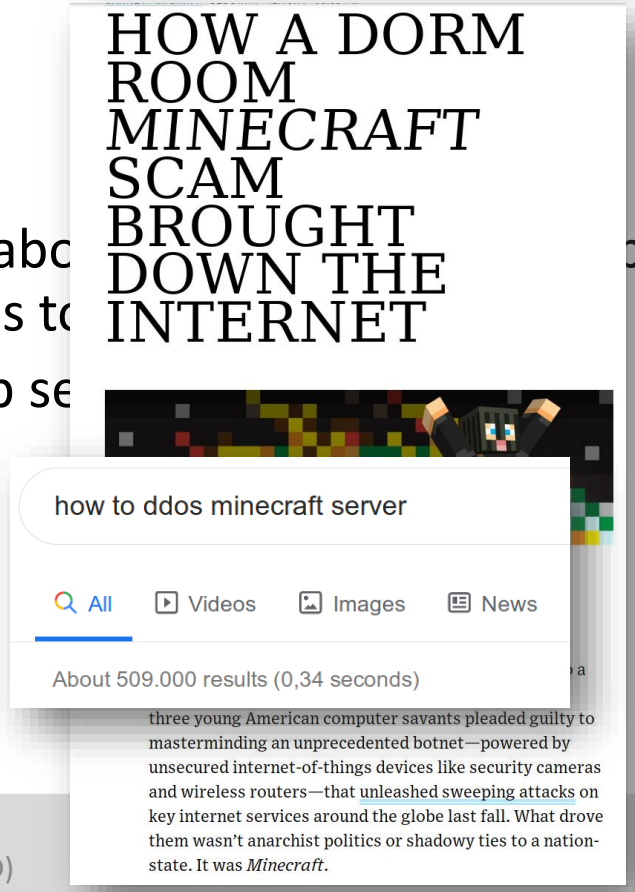
The Threat...

(source: Julie Sigwart - "Geeks")

Introduction

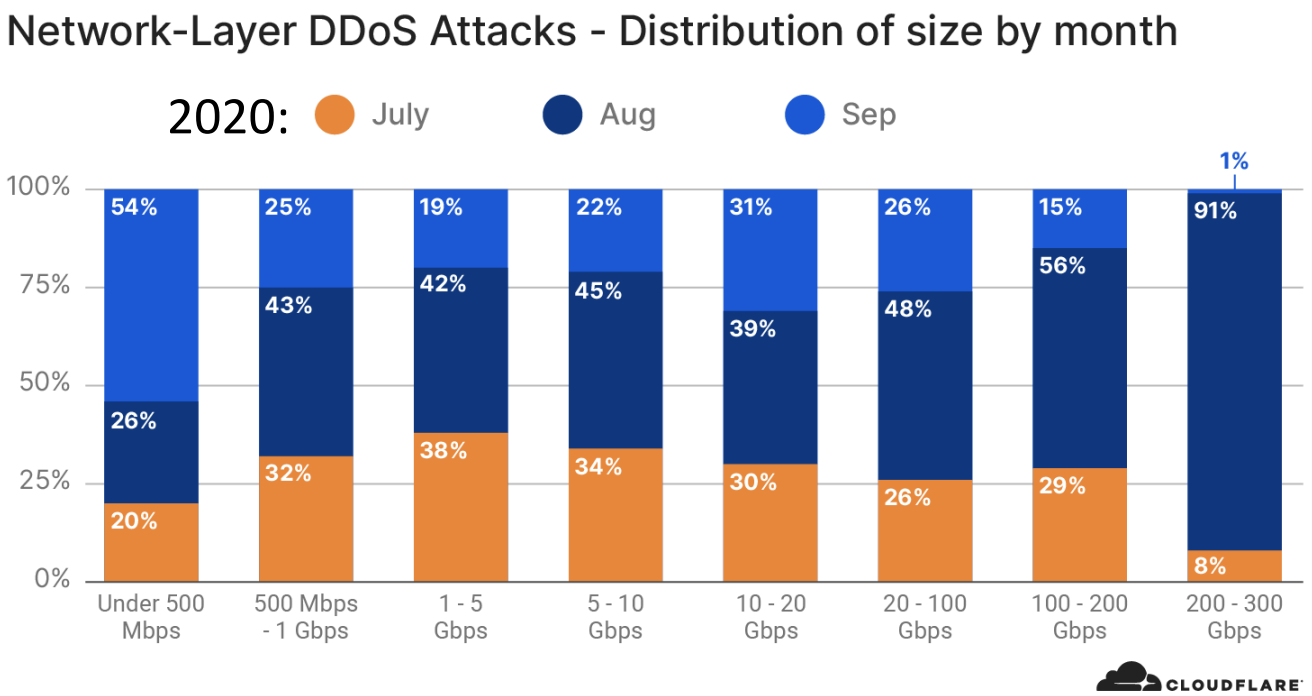
- What is Denial of Service?
  - Denial of Service (DoS) attacks aim at ***denying*** or ***degrading*** legitimate users' ***access to a service*** or network resource, or at bringing down the servers offering such services

- Motivations for launching DoS attacks:
  - Hacking (just for fun, by "script kiddies", ...)
  - Gaining information leap ($\rightarrow$ 1997 attack on bureau of labo ossibly launched as unemployment information has implications to
  - Discrediting an organization operating a system (i.e. web se
  - Revenge (personal, against a company, ...)
  - Political reasons ("information warfare")
  - Financial advantage (mirai and minecraft, 2016)
  - ...



How serious is the DoS problem? (1)

- Qualitative answer:
  - Very, as our modern information society depends increasingly on availability of information and communications services
  - Even worse, as attacking tools are available for download



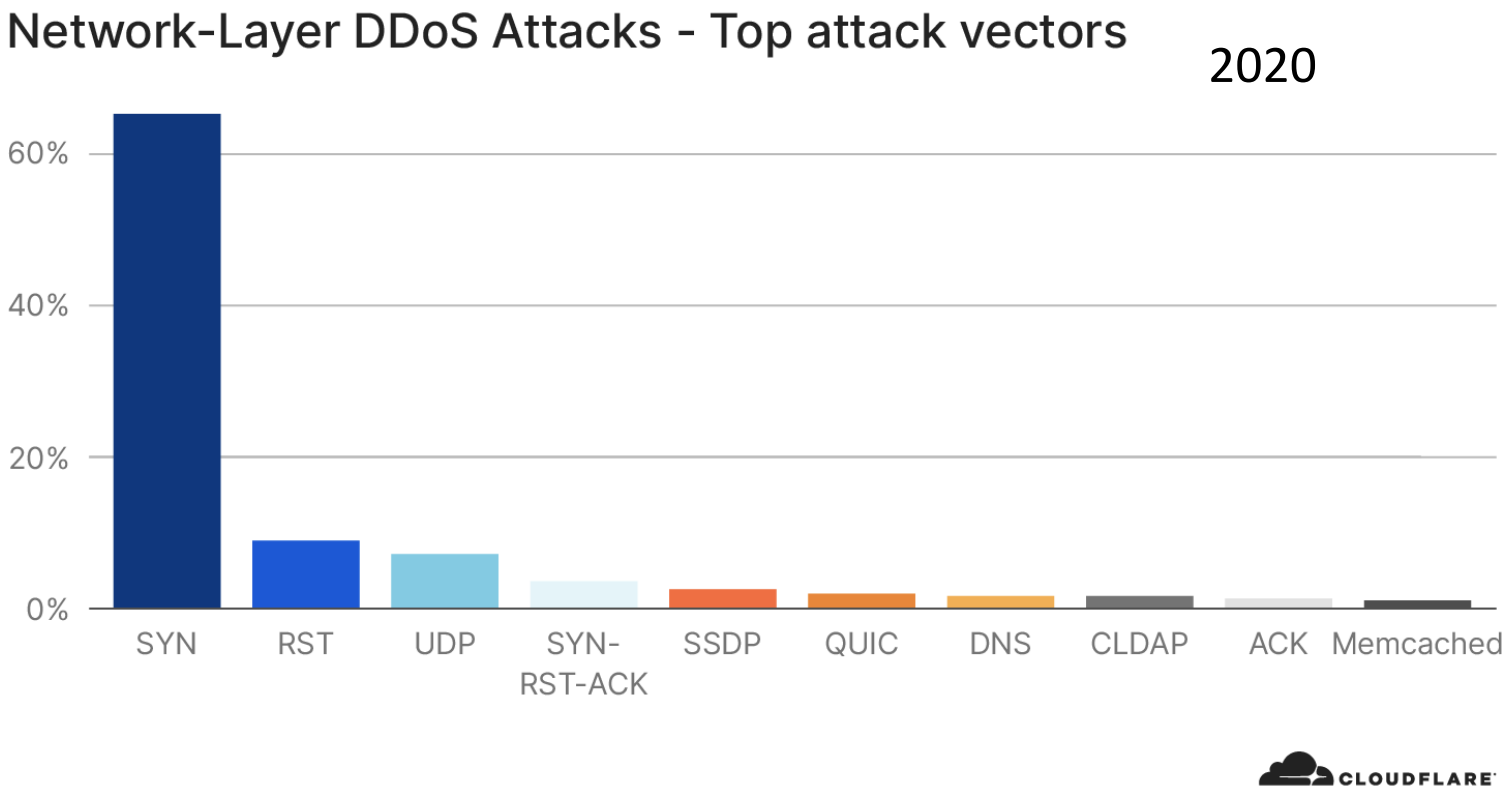
- Largest seen DoS attack so far: 2.3 Tbps (on Amazon AWS in 2020)

https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q3-2020/

How serious is the DoS problem? (2)

- Various attack vectors used

DDoS blackmailing is a lucrative business model!



https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q3-2020/

Denial of Service Attack Classes

Classification depending on different aspects:

- *Attack effect*
  - Resource destruction
  - Resource depletion

- *Origin of malicious traffic*
  - Single source with single / multiple (forged) source addresses
  - Multiple sources (Distributed DoS)

- *Attack target*
  - Victim
  - Infrastructure

Attack Effect in Denial of Service

- *Affected resource*
  - Network connectivity (uplink, transit link)
  - Computation
  - Memory

- *Resource **destruction***:
  - Hacking into systems
  - Making use of implementation weaknesses like buffer overflows
  - Deviation from proper protocol execution
  - Your common TU Dresden Excavator

- *Resource **depletion*** by causing:
  - Storage of (useless) state information
  - High traffic load (requires high overall bandwidth from attacker)
  - Expensive computations (“expensive cryptography”!)
  - Resource reservations that are never used (e.g. bandwidth)

Karlsruhe Institute of Technology

KASTEL

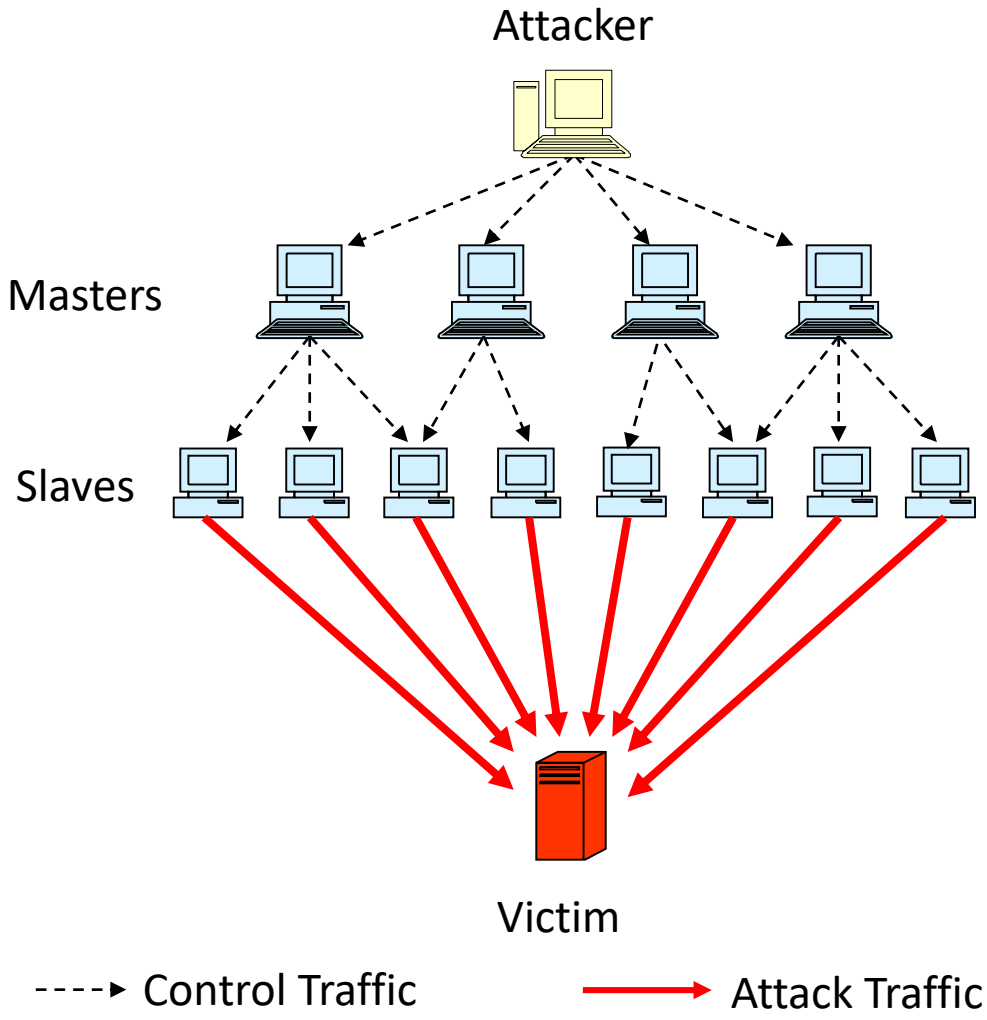
So how is it done?

Attacking Techniques

- ***Reflector*** attacks: Generate traffic indirection
- Request service in the name of the victim (e.g. spoofed IP – *which protocols*?)
- Hides attack source, allows for external amplification

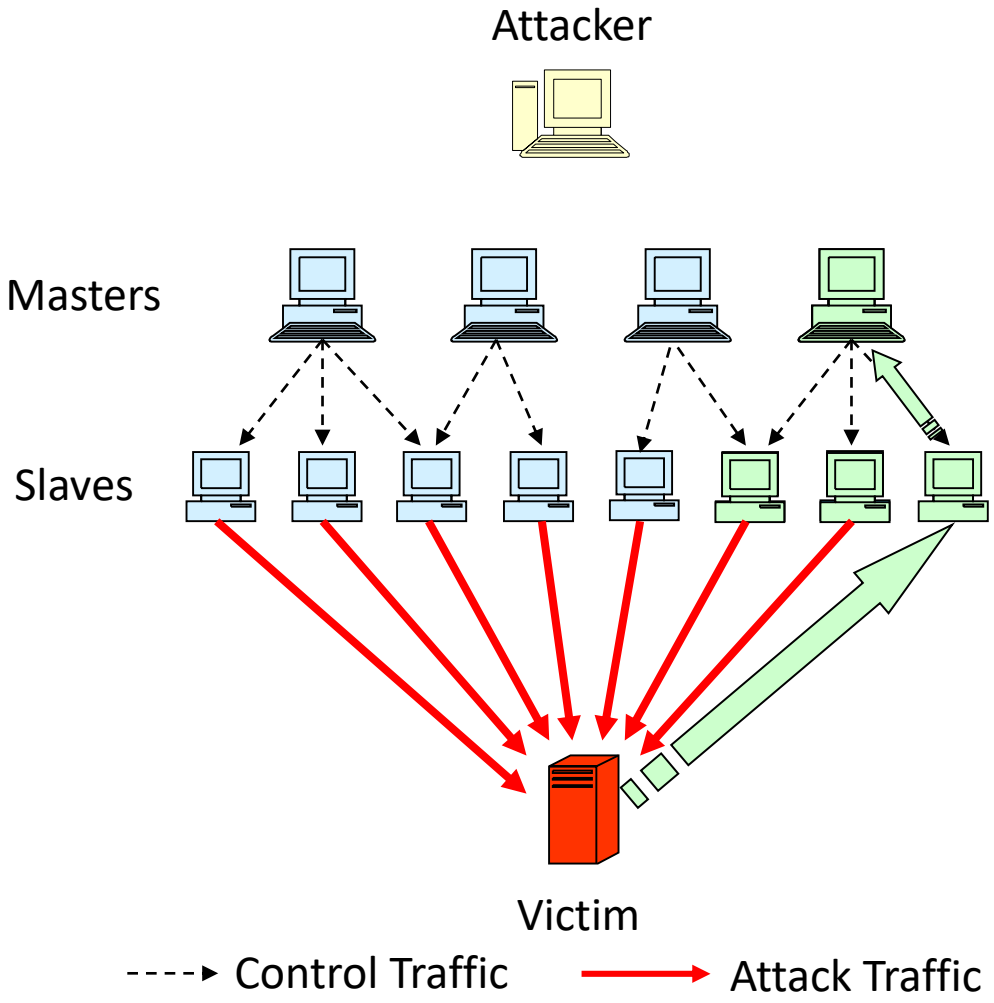
- ***Amplification*** attacks: Leverage asymmetry in protocols
- Send lightweight requests (low cost) that generate heavyweight responses or heavy load on the service (crypto)
- Increases damage

DoS Tools: Botnets 101



- The attacker classifies the compromised systems in:
  - Master systems
  - Slave systems
- Master systems:
  - Receive command data from attacker
  - Control the slaves
- Slave systems:
  - Launch the proper attack against the victim
  - During the attack there is no traffic from the attacker

Botnet Strategies: Partitioning



- Each master system only knows some slave systems
- Therefore, the network can handle partial failure, caused by detection of some slaves or masters

Karlsruhe Institute of Technology

KASTEL

Resource Destruction

Resource Destruction – Examples (1)

- *Resource Destruction:*
- Physically/Logically destroy a resource that is vital for targeted service

- *Hacking:*
  - Exploiting weaknesses that are caused by careless operation of a system
  - Examples: default accounts and passwords not disabled, badly chosen passwords, social engineering (incl. malware attachments), etc.

- *Making use of implementation weaknesses*
  - Buffer Overflows, Format-String-Attacks, ...

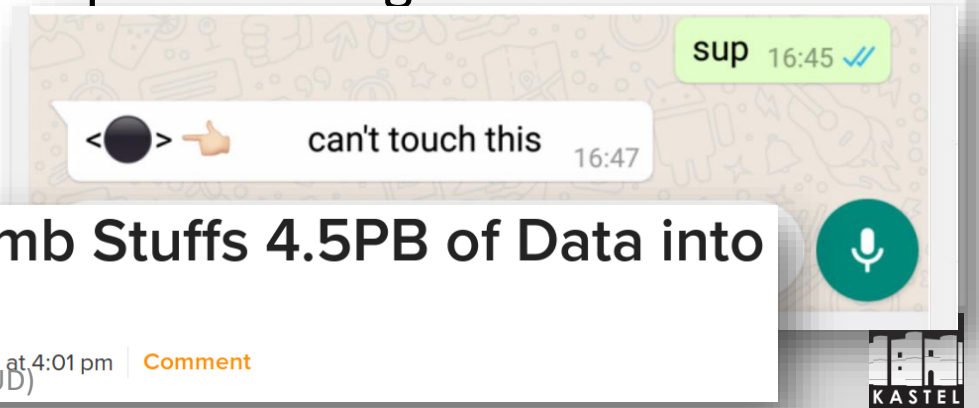
- *Deviation from proper protocol execution:*
  - Example: exploit IP's fragmentation & reassembly

Resource Destruction – Examples (2)

- Original Teardrop attack: exploit IP's fragmentation & reassembly
  - Send IP fragments to broadcast address 192.168.133.0
  - BSD-based OS used to respond to broadcast messages, messages can be fragmented
  - Response requires ***reassembly,*** first
  - If an attacker sends a ***lot of fragments without*** ever sending a ***first / last fragment***, the buffer of the reassembling system gets ***overloaded***
  - (Routers use BSD-based TCP/IP stacks -> attack on network infrastructure)

  - Sending a series of fragmented IP datagram pairs with overlapping offset to target
  - Windows 95: crashed when trying to reassemble one pair of datagrams

More recently: ⚐0 ;-)



Defending Against Resource Destruction DoS

Karlsruhe Institute of Technology

Defenses against disabling services:

- Hacking:
  - Good system administration
  - Firewalls, logging & intrusion detection systems
- Implementation weakness:
  - Code reviews, stress testing, etc. (in theory: verification and microkernels)
- ***Protocol deviation:***
  - Fault tolerant protocol design
  - Attack-aware protocol deployment (fail2ban, rate limiting, etc)
  - “DoS-aware protocol design”:
    - Be aware of possible DoS attacks when e.g. reassembling packets
    - Do not perform expensive operations, reserve memory, etc., before authentication

Karlsruhe Institute of Technology

KASTEL

Resource Depletion

Background: Internet Control Message Protocol

- Internet Control Message Protocol (ICMP) has been specified for communication of error conditions in the Internet
- ICMP PDUs are transported as IP packet payload and identified by value “1” in the protocol field of the IP header

- Two main reasons make ICMP particular interesting for attackers:
  - It may be addressed to broadcast addresses
  - Routers respond to it

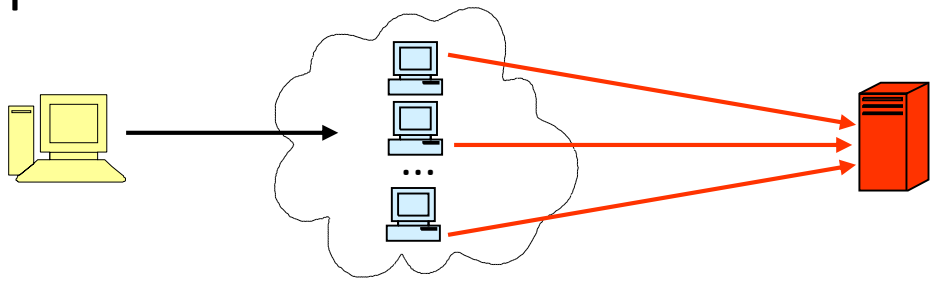
ICMP Functions

- ***Announce network errors:*** e.g. a host or entire portion of the network being unreachable, or a TCP or UDP packet directed at a port number with no receiver attached (destination unreachable)
- ***Announce network congestion:*** routers generate ICMP source quench messages, when they need to buffer too many packets
- ***Assist troubleshooting:*** ICMP supports an Echo function, which just sends an ICMP echo packet on a round trip between two hosts
- ***Announce timeouts:*** if an IP packet's TTL field drops to zero, the router discarding the packet may generate an ICMP packet (time exceeded)
- ***Announce routing detours:*** if a router detects that it is not on the route between source and destination, it may generate an ICMP redirect packet

The mother of DoS: Smurf – ICMP Bandwidth Depletion

- Two reasons make ICMP particular interesting for attackers:
  - It may be addressed to broadcast addresses
  - Routers respond to it

- The ***Smurf attack*** - ICMP echo request to broadcast:
  - Routers (sometimes) allow ICMP echo requests to broadcast addresses…
  - An attacker sends an ICMP echo request to a *broadcast address* with the *source address* forged to refer to the victim
  - All devices in the addressed network respond to the packet
  - The victim is flooded with replies to the echo request
  - With this technique, the network being abused as an (unaware) attack amplifier is also called a *reflector network*:



More recent examples…

Jonker, Mattijs, et al. "Millions of targets under attack: a macroscopic characterization of the DoS ecosystem." *Proceedings of the 2017 Internet Measurement Conference*. ACM, 2017.

Rossow, Christian. "Amplification Hell: Revisiting Network Protocols for DDoS Abuse." *NDSS*. 2014.

"Identifying the scan and attack infrastructures behind amplification DDoS attacks." *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016.

Schuchard, Max, et al. "Losing control of the internet: using the data plane to attack the control plane." *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010.

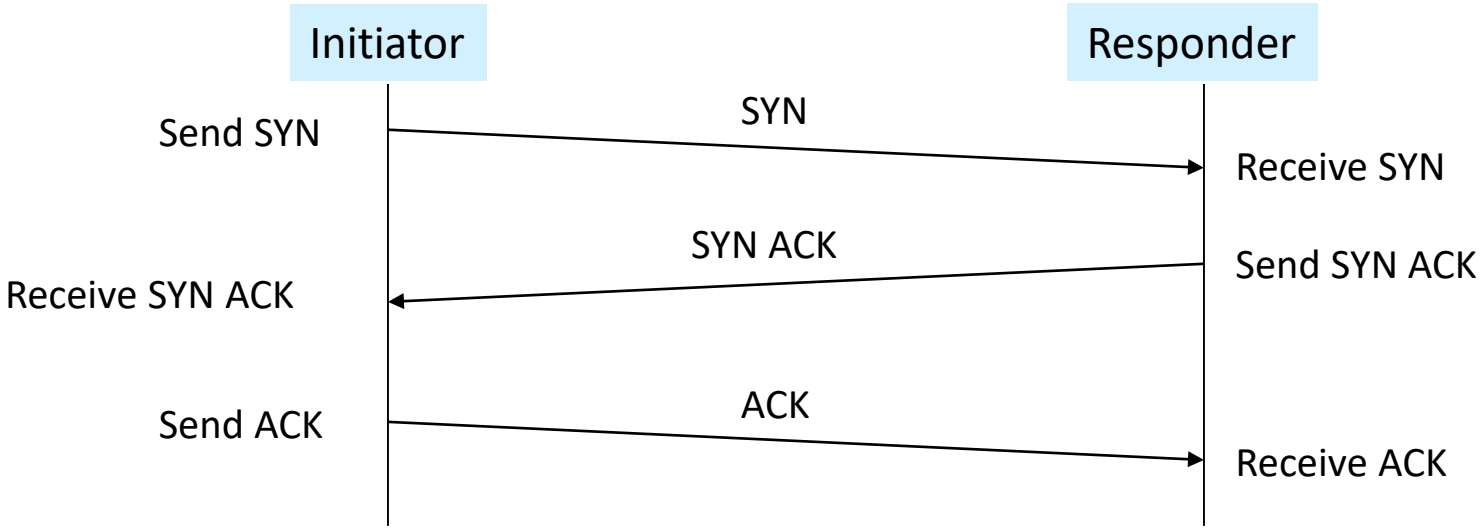
Smith, Jared M., and Max Schuchard. "Routing around congestion: Defeating DDoS attacks and adverse network conditions via reactive BGP routing." *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018.

Global Distributed Denial-Of-Service (DDoS) Protection Market 2019 – …nie Networks, ARBOR NETWORKS, Imperva …uard

The global "Distributed Denial-Of-Service (DDoS) Protection" market report …ted Denial-Of-Service (DDoS) … also assesses the Distributed Denial- … of topography, technology, and consumers. The report also covers the volume … of the market during the projected … ted Denial-Of-Service (DDoS) … sentation of the Distributed Denial- … he global and regional level. **The key** … OR NETWORKS, Imperva Incapsula

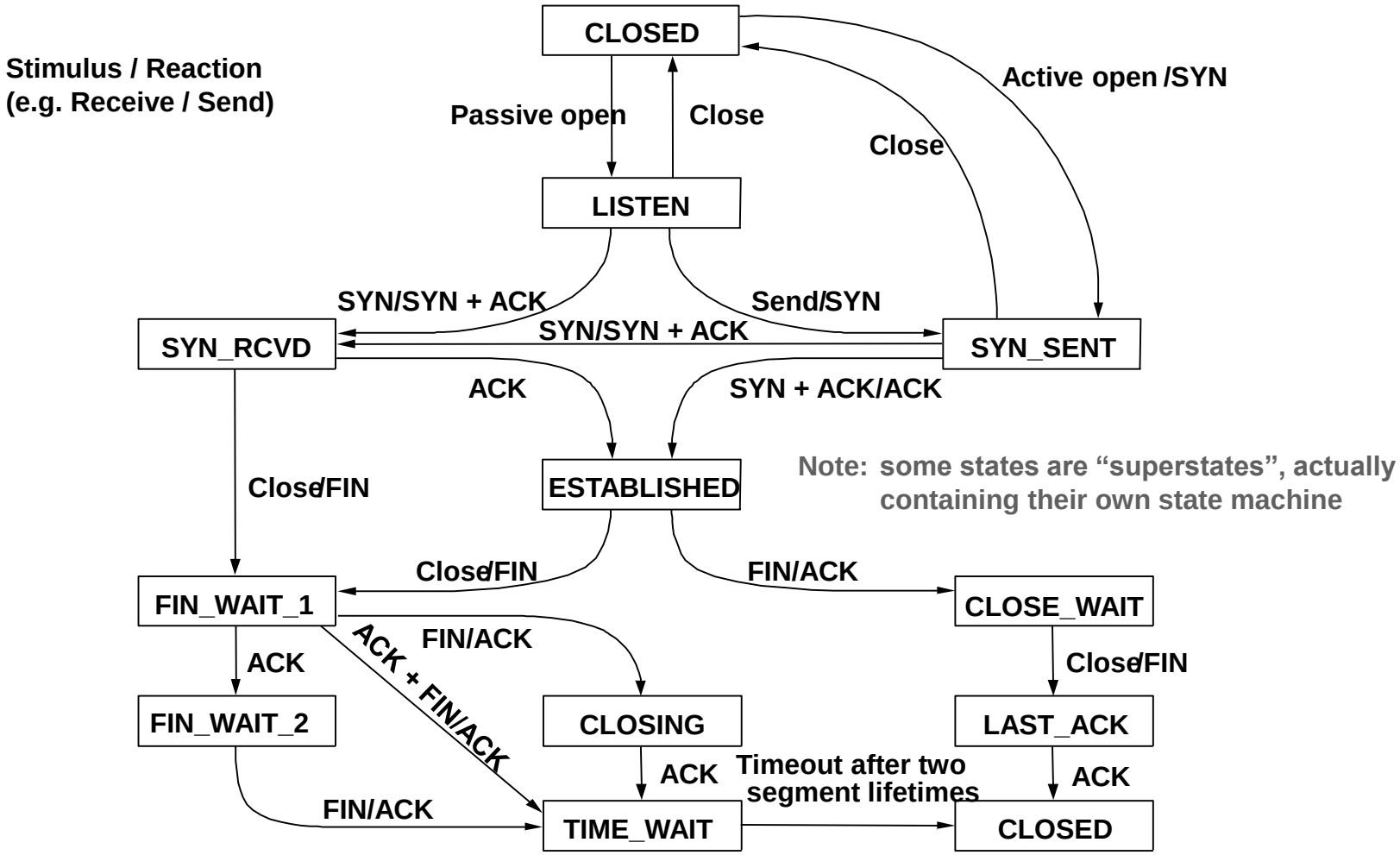
Depleting Memory: TCP's Three-Way-Handshake

- The *Transmission Control Protocol (TCP):*
  - provides a connection-oriented, reliable transport service
  - uses IP for transport of its PDUs
- TCP connection establishment is realized with handshake:



- After handshake, data can be exchanged in both directions
- Both peers may initiate termination of the connection (two-way-handshake)

TCP Connection Management: State Diagram



Background: Reaction According to Protocol

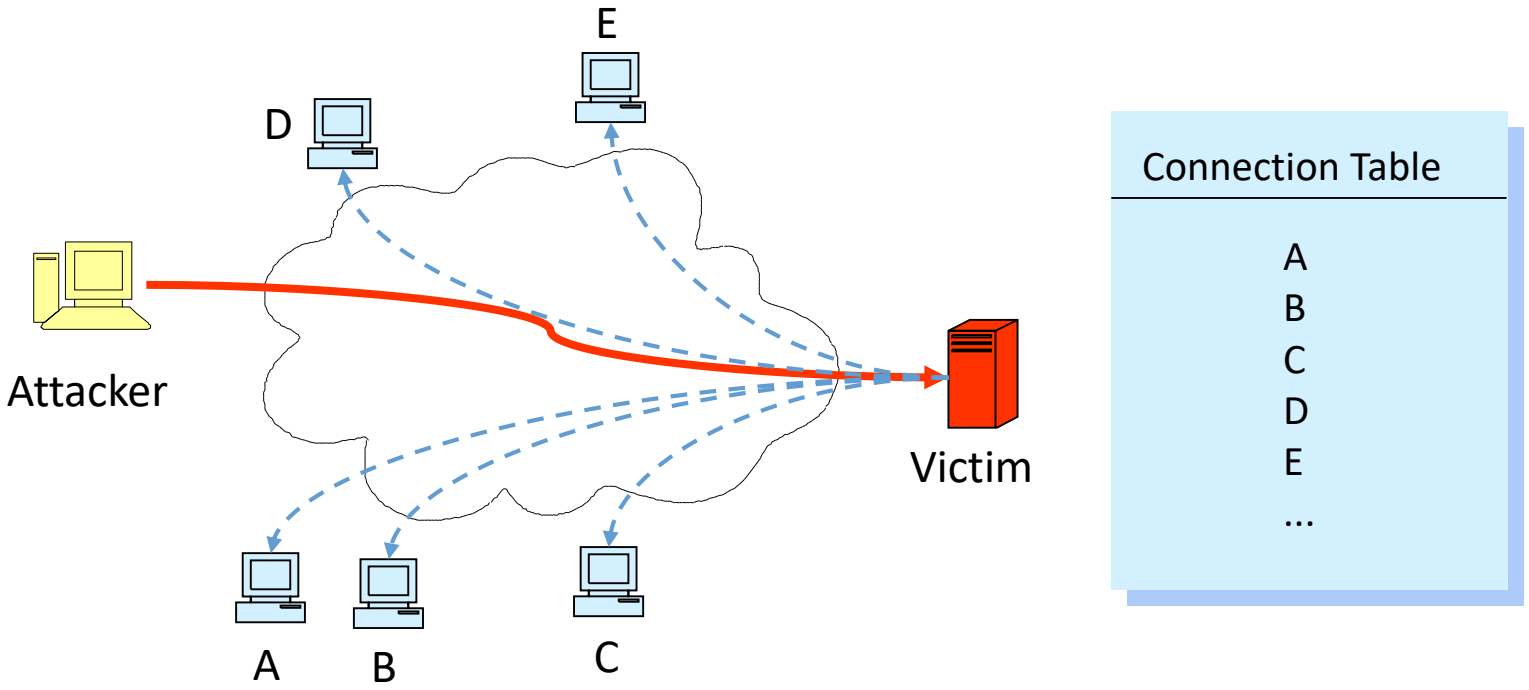
Karlsruhe Institute of Technology

Reply packets according to protocol specification if state not available

Packet Sent	Reaction of Receiver
TCP SYN (to open port)	TCP SYN ACK
TCP SYN (to closed port)	TCP RST (ACK)
TCP ACK	TCP RST (ACK)
TCP DATA	TCP RST (ACK)
TCP RST	no response
TCP NULL	TCP RST (ACK)
ICMP Echo Request	ICMP Echo Reply
ICMP TS Request	ICMP TS Reply
UDP Packet (to open port)	protocol dependent
UDP Packet (to closed port)	ICMP Port Unreachable
TCP SYN ACK (to closed port)	----

TCP SYN Flood: Memory Depletion

- Category *Storage of useless state information:*
  - Here: TCP-SYN flood attack



More recent Memory Depletion DoS Attacks

- Zip bombs (see above)
  - Exploit recursive/nested compression to create very large output
  - Recently also with overlapping files (non-recursive)

- „A billion laughs“
  - „XML bomb“
  - Exponential entity expansion attack on parsers

https://www.bamsoftware.com/hacks/zipbomb/