Lecture 27: Network Security

CS 105   Spring 2021

Networking Stack

7 - Application	Deliver content	HTTP
6 - Presentation	Manage encoding	
5 - Session	Manage sessions	TLS/SSL
4 - Transport	Deliver (un)reliably	TCP/UDP
3 - Network	Deliver globally	IP
2 - Data Link	Deliver locally	Ethernet
1 - Physical	Deliver signals	0s and 1s
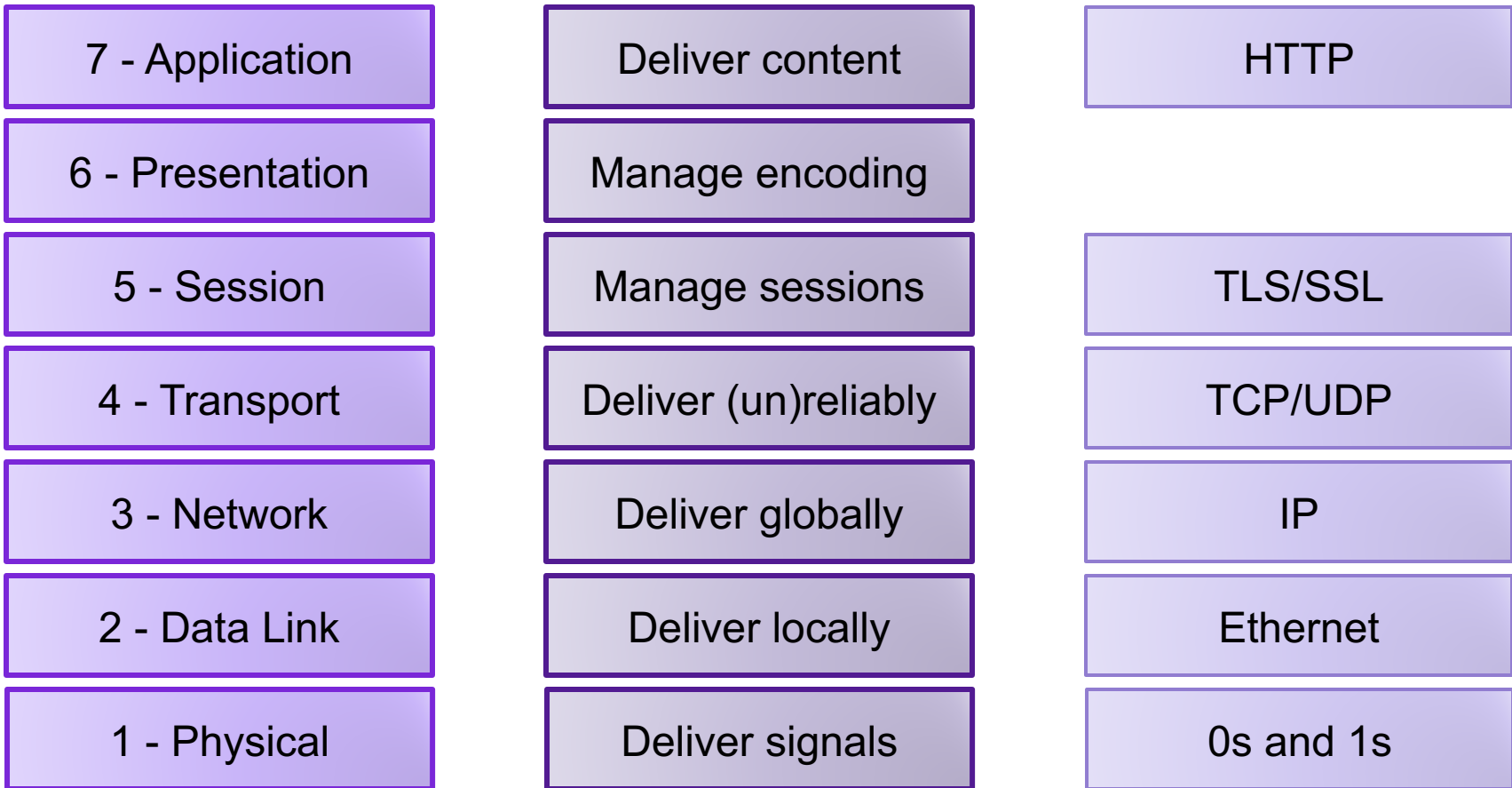
# Denial of Service Attacks

- Goal: violate availability by making system unable to respond to requests from legitimate users

  1. Resource-saturation attacks
 2. Vulnerability-based attacks

Ping

- The **Internet Control Message Protocol (ICMP)** is an network-layer support protocol used to pass operational information and error messages

- **traceroute:** display path to a host in an IP network
- **ping:** test reachability of a host in an IP network
  - sends ICMP echo request packet to target host and waits for ICMP echo reply
  - Uses CPU, network bandwidth
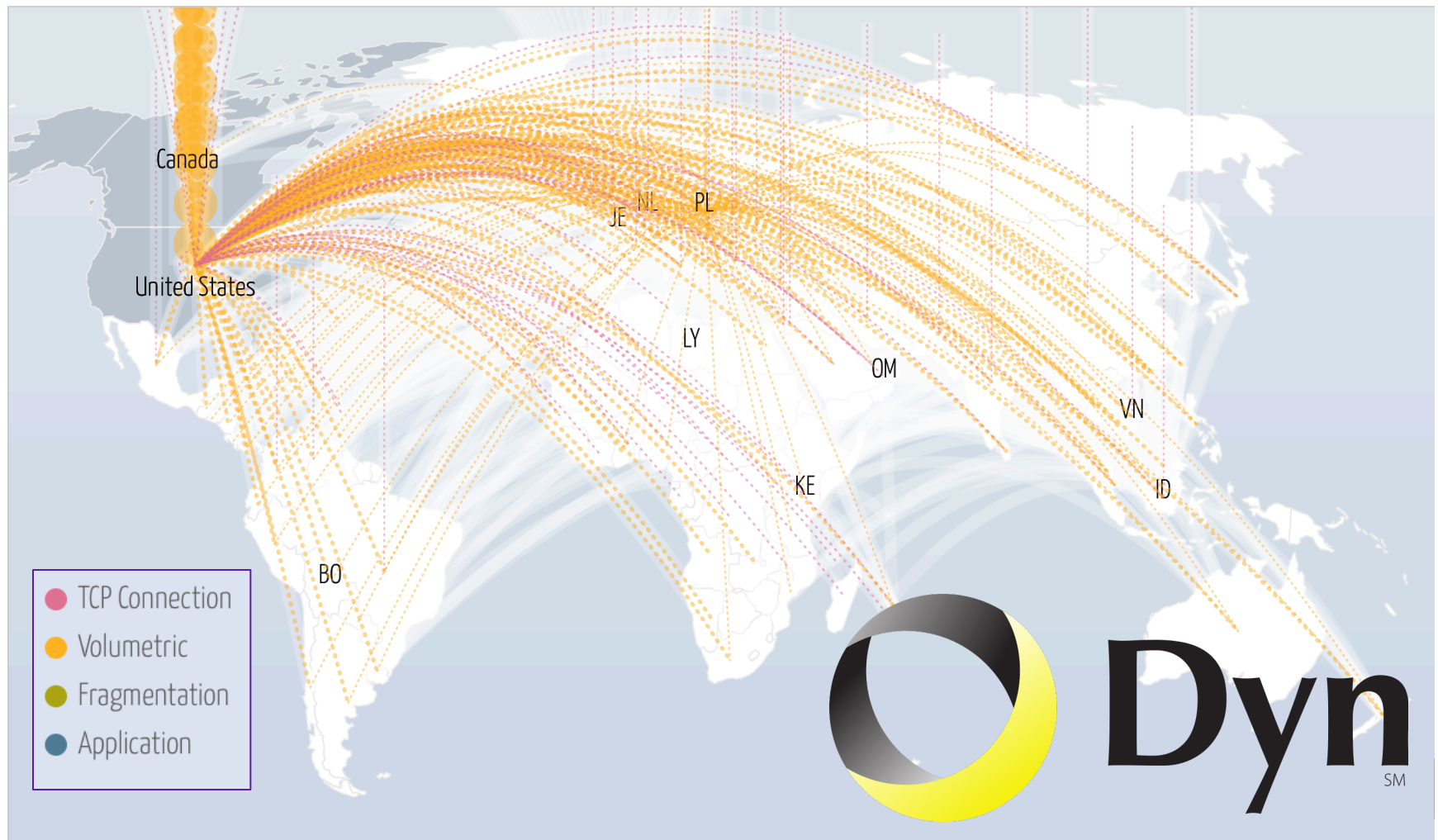
Ping Flood

- ping -f
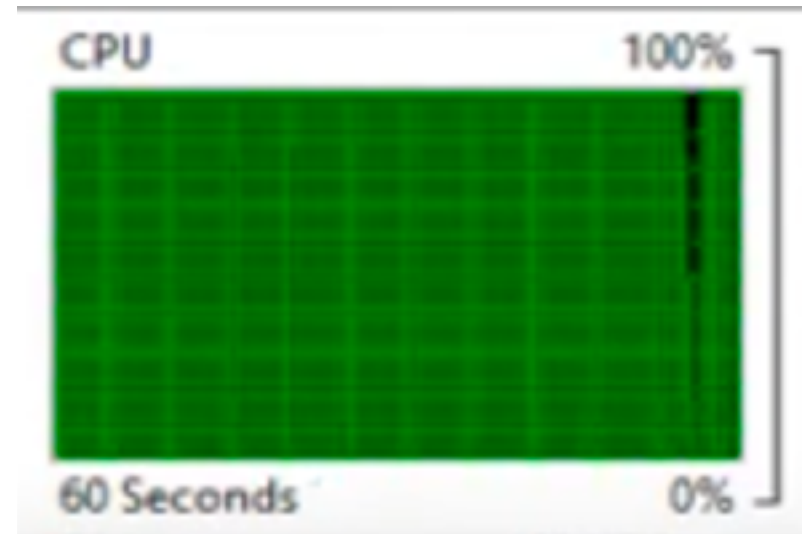
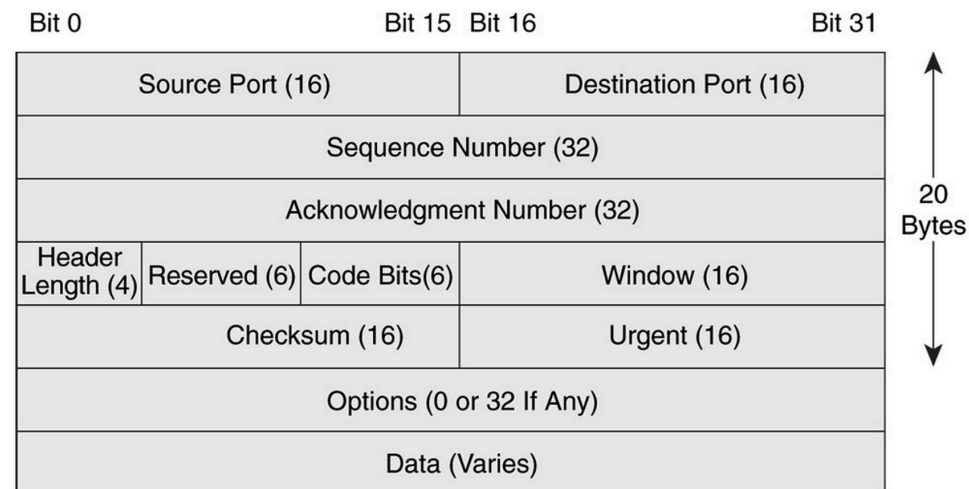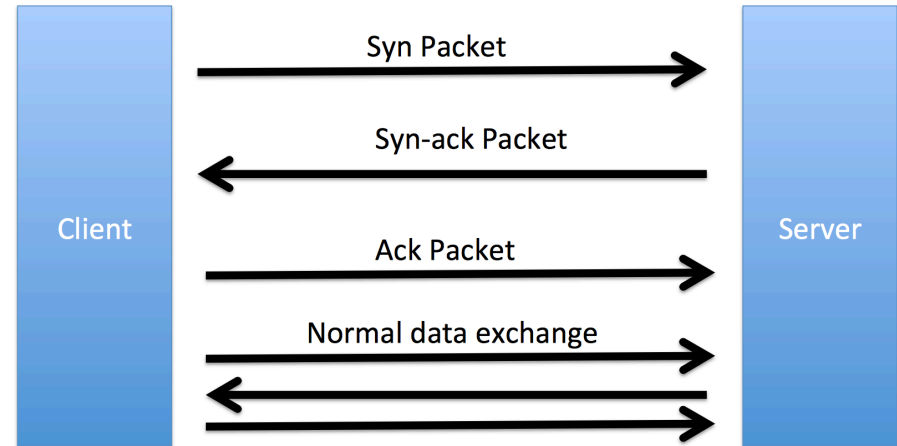# Ping Flood
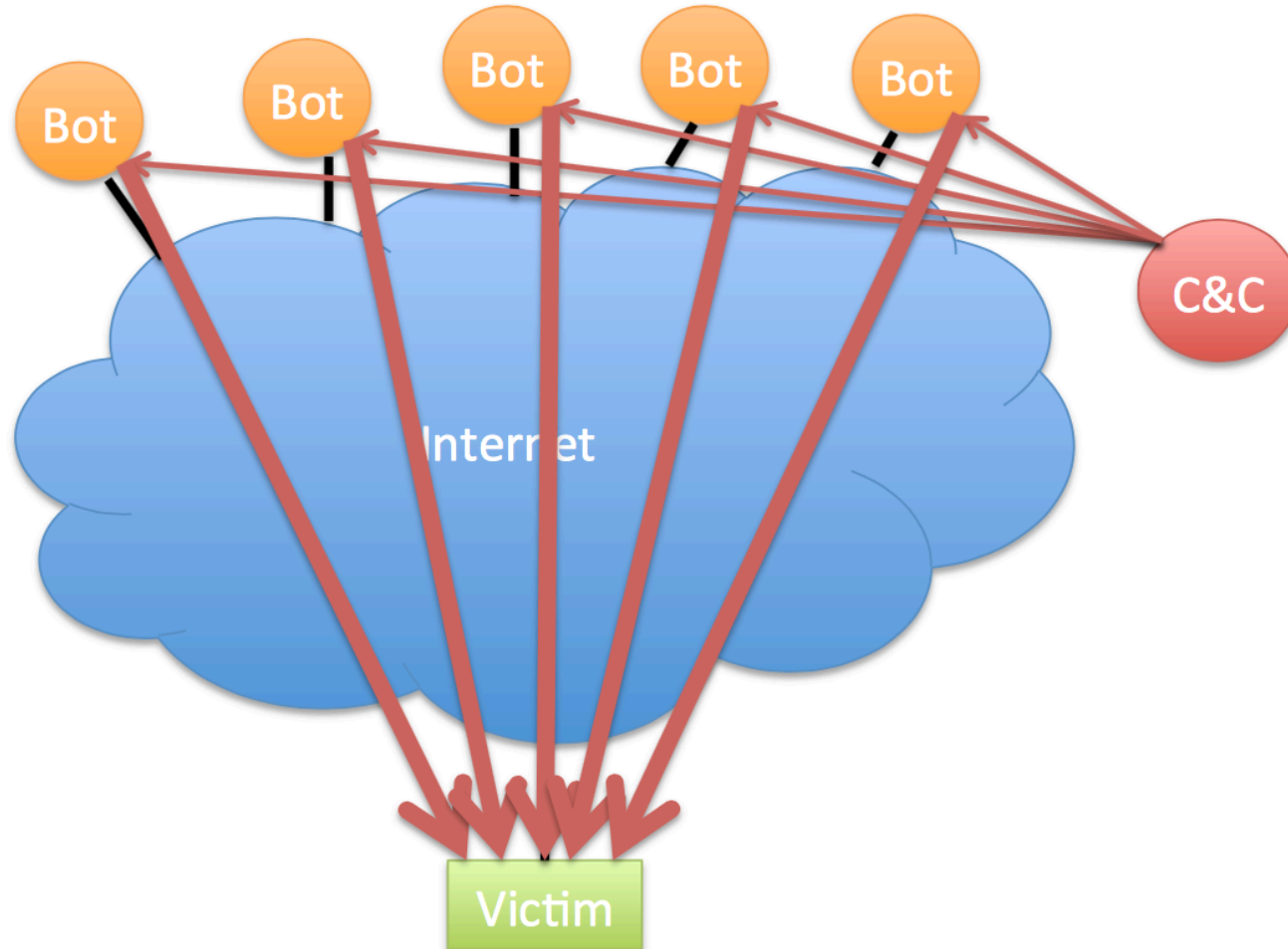
Defenses against Ping Floods

- Disable ICMP functionality
- Non-centralized firewalls
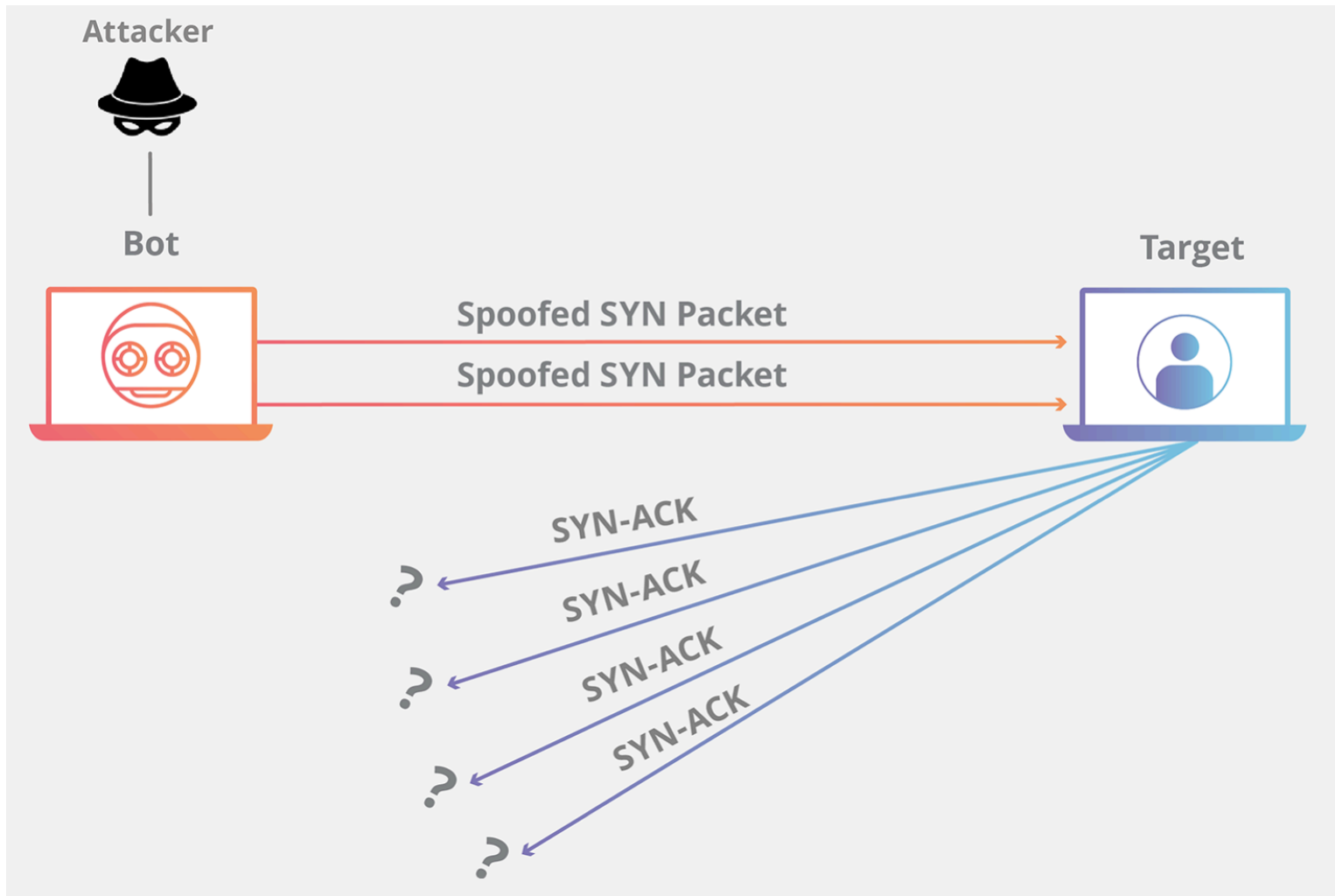
DNS Flood

TCP

- Reliable
  - acknowledgement
  - checksum
  - sequence number
- In-order
  - sequence number
- Congestion control
  - slow start
  - congestion avoidance
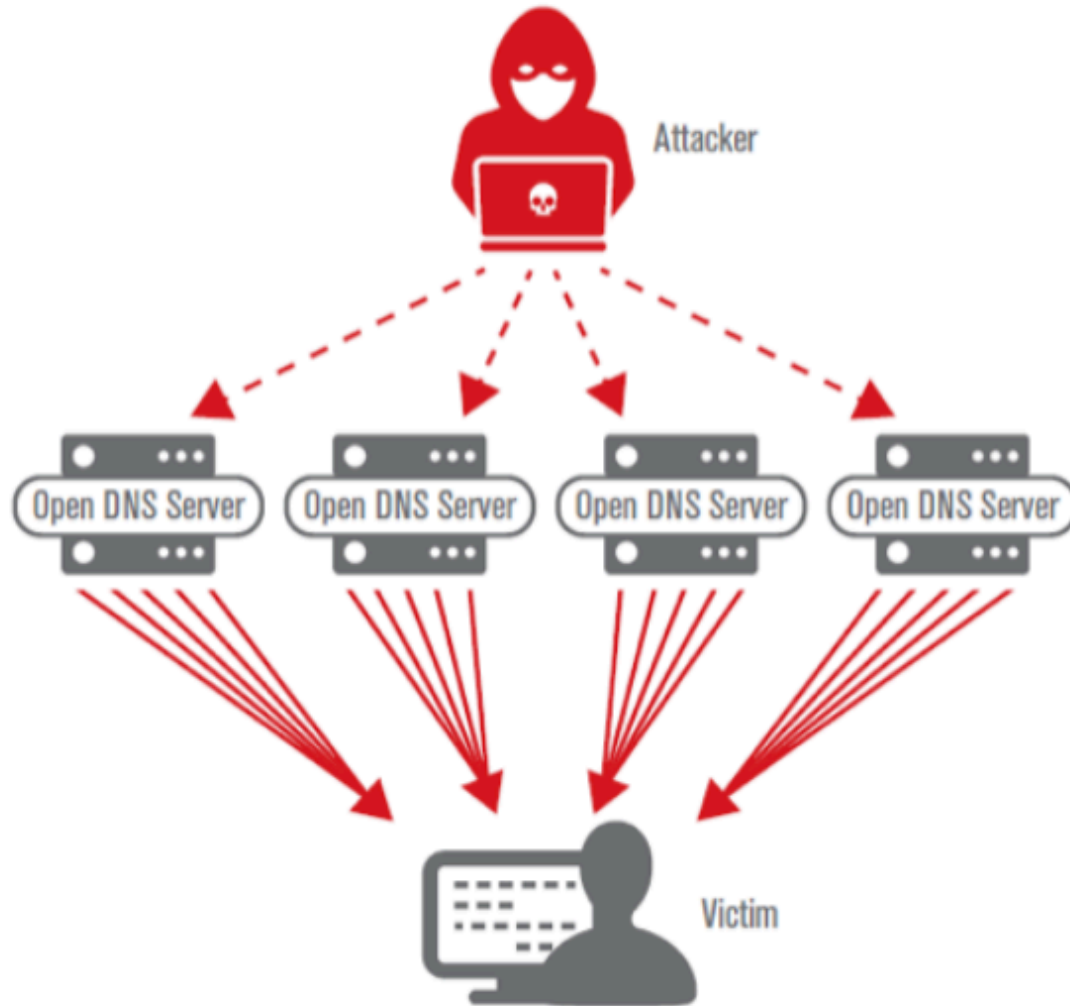 - fast retransmit
  - fast recovery

Bit 0		Bit 15	Bit 16		Bit 31
Source Port (16)			Destination Port (16)		
Sequence Number (32)					
Acknowledgment Number (32)					
Header Length (4)	Reserved (6)	Code Bits(6)	Window (16)		
Checksum (16)			Urgent (16)		
Options (0 or 32 If Any)					
Data (Varies)					

20 Bytes

SYN Flood

Defending Against SYN Floods

- Increase RECV queue size
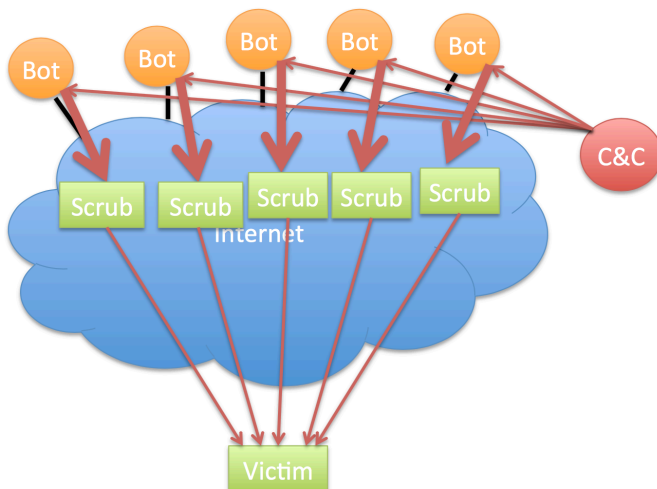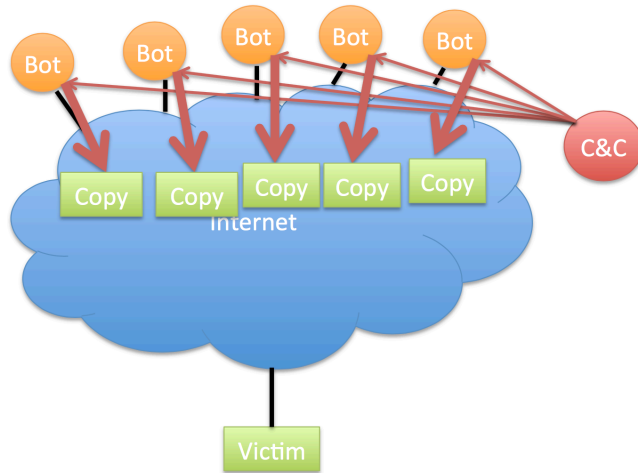- Recycle oldest half-open connections
- SYN cookies

DNS Reflection Attacks

DDOS Attacks

Mitigating DoS Attacks

Mitigating DoS Attacks

	Gold Award (IMPERVA INCAPSULA)	2 (f5)	3 (ARBOR NETWORKS)	4	5 (VERISIGN)	6 (neustar)	7 (Akamai)	8 (DOS arrest)	9 (CLOUDFLARE)	10 (radware)
	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes	Compare Quotes
Web Application Firewall (?)	✓	✓		✓			✓	✓	✓	✓
Rate Limiting (?)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Automatic Bot Discernment (?)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP Blocking (?)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
BGP (?)	✓	✓	✓	✓	✓	✓		✓	✓	N/A
DNS (?)	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A
Web Proxy (?)	✓	✓		✓	✓	✓	✓	✓	✓	N/A
Real Time Monitoring (?)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Deep Packet Inspection (?)	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A

Botnets

DDoS as a Service

DDoS as a Service
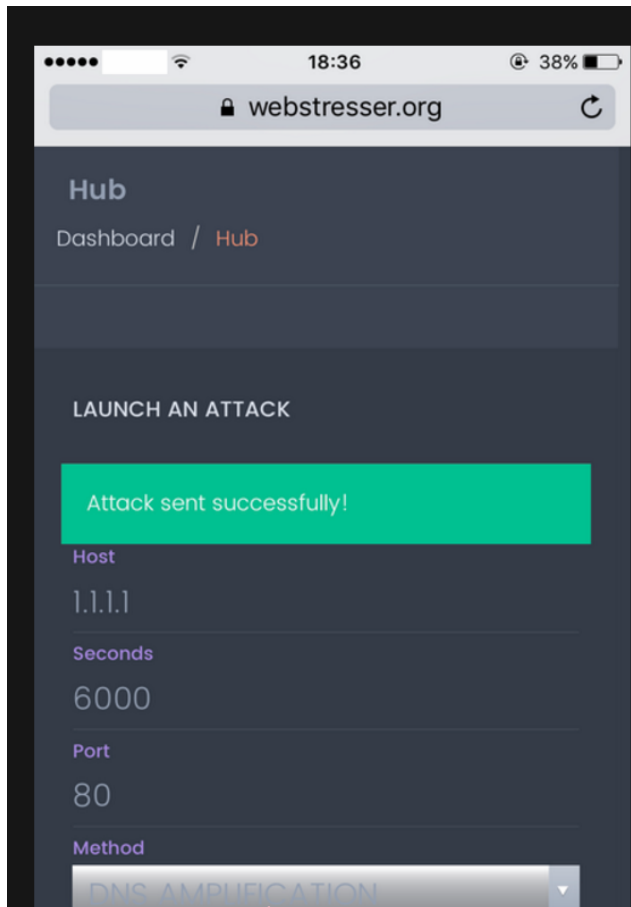
CRAZY FEATURES

Our high performance dedicated servers ensures only strong stress tests. With spoofed and amplified stress tests we take care of your privacy online.

— — —

Our custom coded attack scripts, IP Logger, 24/7 customer service, 37 backend servers, Layer4 and Layer7 stress tests, Paypal and Bitcoin autobuy.

Purchase using Paypal

We believe in huge potential of Paypal with paying online. Many other booters / IP Stressers doesnt have paypal enabled because they are scamming their customers.

Purchase with Bitcoin

By purchasing with bitcoin you automatically grant yourself a 15% discount. This beautifull crypto currency ensures complete privacy while paying online.

Remote Requests

Port Open
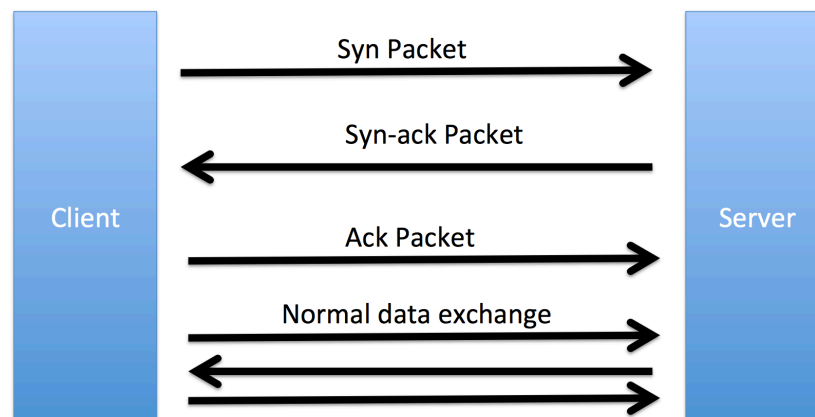
Initial seq # for server to client bytes

Ack of client -> server ISN **+1**

Bit 0		Bit 15	Bit 16		Bit 31
Source Port (16)			Destination Port (16)		
Sequence Number (32)					
Acknowledgment Number (32)					
Header Length (4)	Reserved (6)	Code Bits(6)	Window (16)		
	Checksum (16)		Urgent (16)		
Options (0 or 32 If Any)					
Data (Varies)					

20 Bytes

S (0x02) | A (0x10) set

Typically none
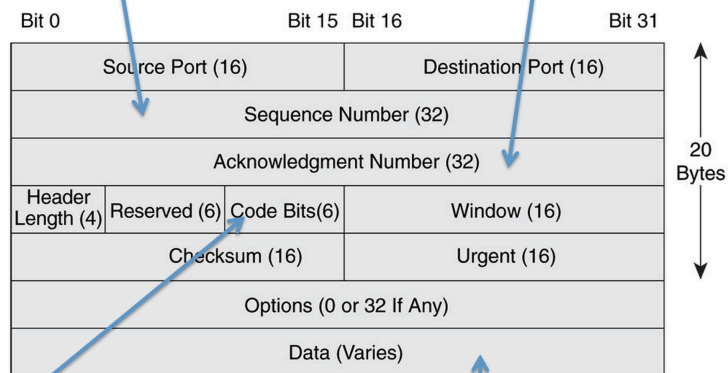
Port Closed

- No machine
  - ICMP response from router
- Machine but port closed
  - TCP reset packet
- Intercepted
  - Silence (depends on config)

Port Scanning

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-18 21:43 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed ports

PORT        STATE SERVICE     VERSION
21/tcp      open  ftp
22/tcp      open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp      open  http        Apache httpd 2.4.7 ((Ubuntu))
554/tcp     open  rtsp
7070/tcp    open  realserver
9929/tcp    open  nping-echo Nping echo
31337/tcp open  Elite

Device type: general purpose
Running (JUST GUESSING): Linux 3.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:3.13
Aggressive OS guesses: Linux 3.13 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 20.31 seconds
```
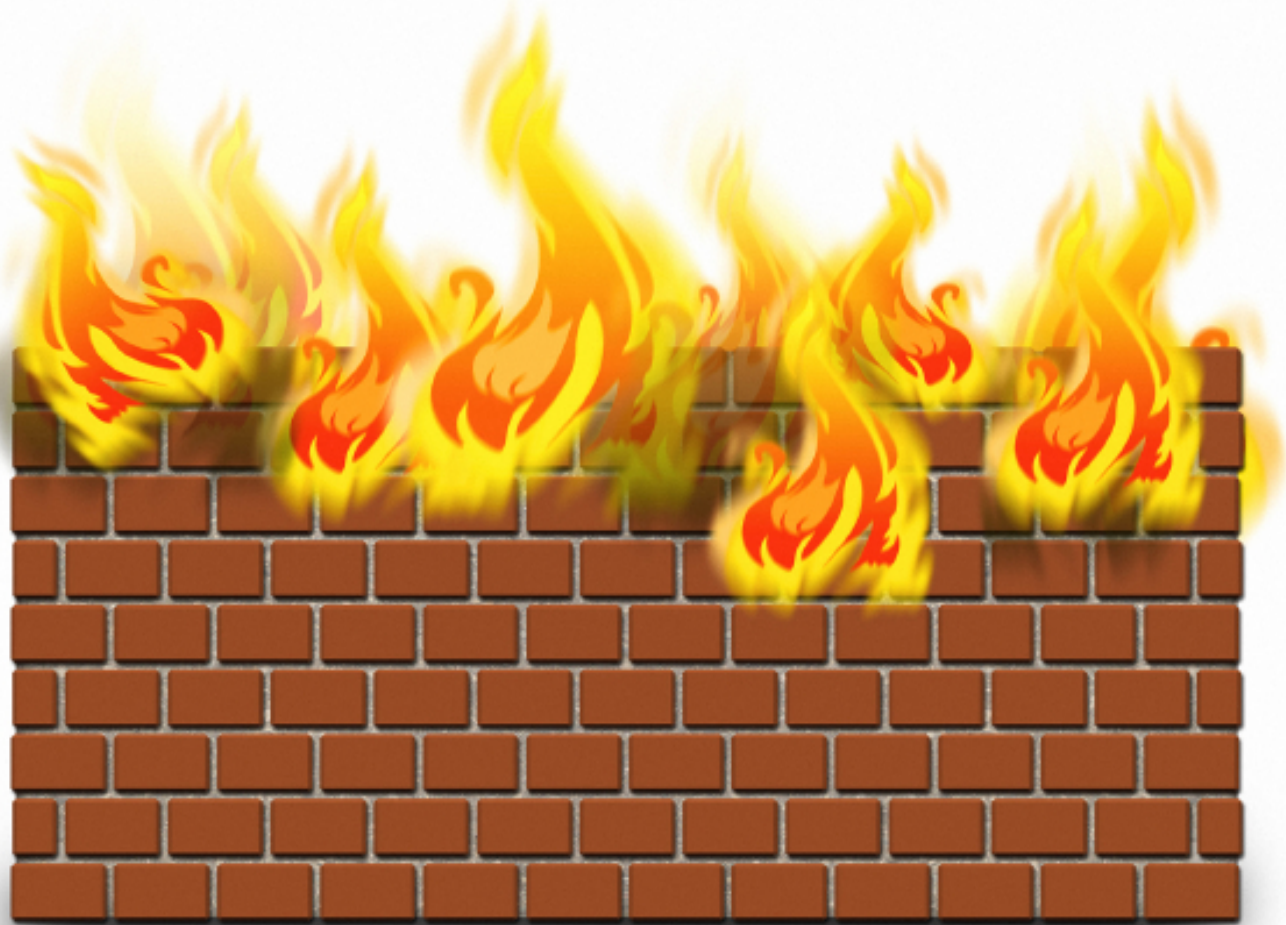
Firewalls
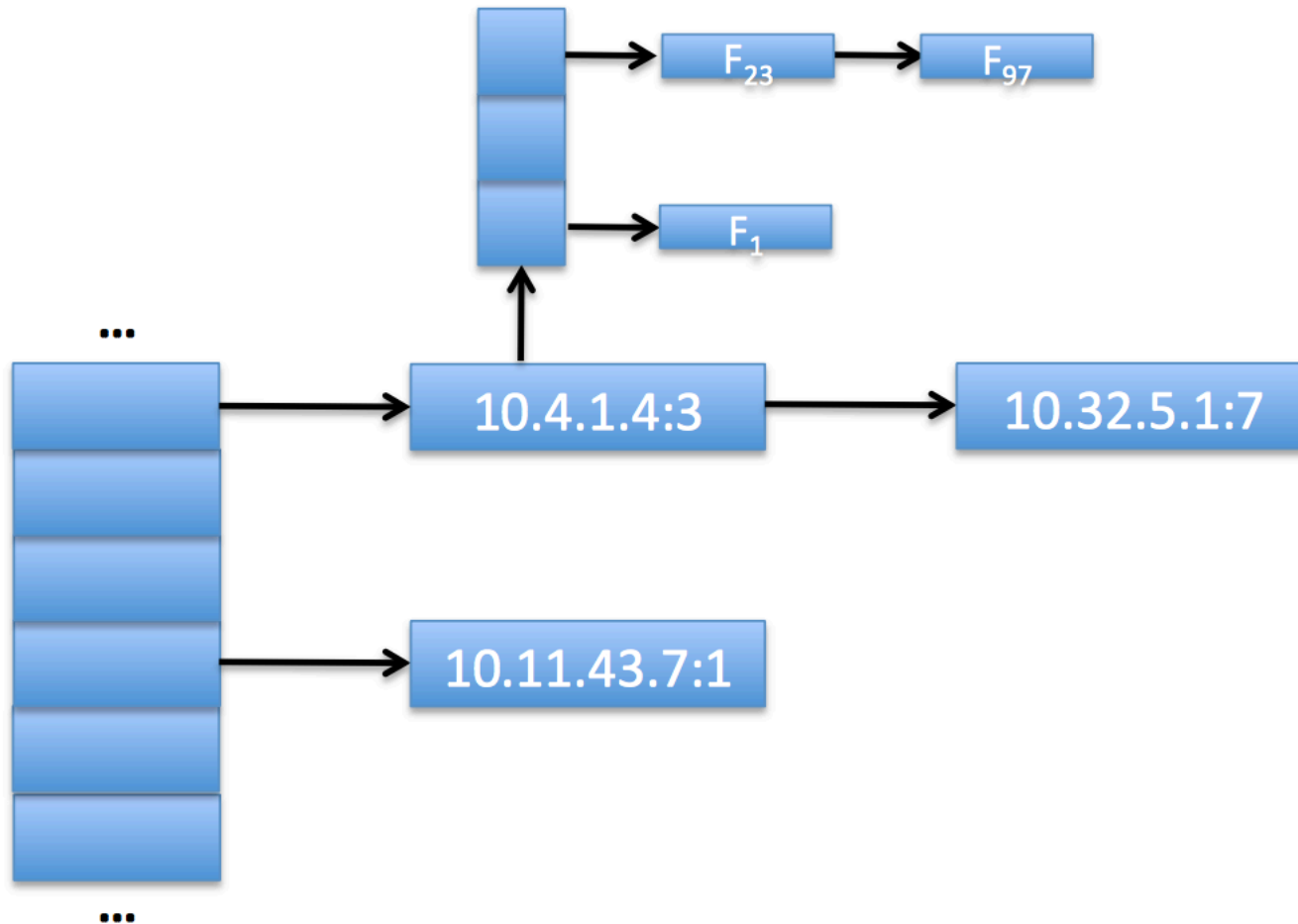
Packet Filtering

| Protocol	Source IP	Dest. IP	Dest. Port	Action
TCP	*	192.168.1.*	25	Permit
UDP	*	192.168.1.*	69	Permit
TCP	192.168.1.*	*	80	Permit
TCP	*	192.168.1.18	80	Permit
TCP	*	192.168.1.*	*	Deny
TCP	*	192.168.1.*	*	Deny

Stateful Inspection

Deep-Packet Inspection


```
alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"OS-LINUX
OS-LINUX x86 Linux overflow attempt";
flow:to_server,established; content:"1|C0 B0 02 CD 80 85
C0|uL|EB|L^|B0|"; metadata:ruleset community, service dns;
classtype:attempted-admin; sid:264; rev:13;)
```

Network Security
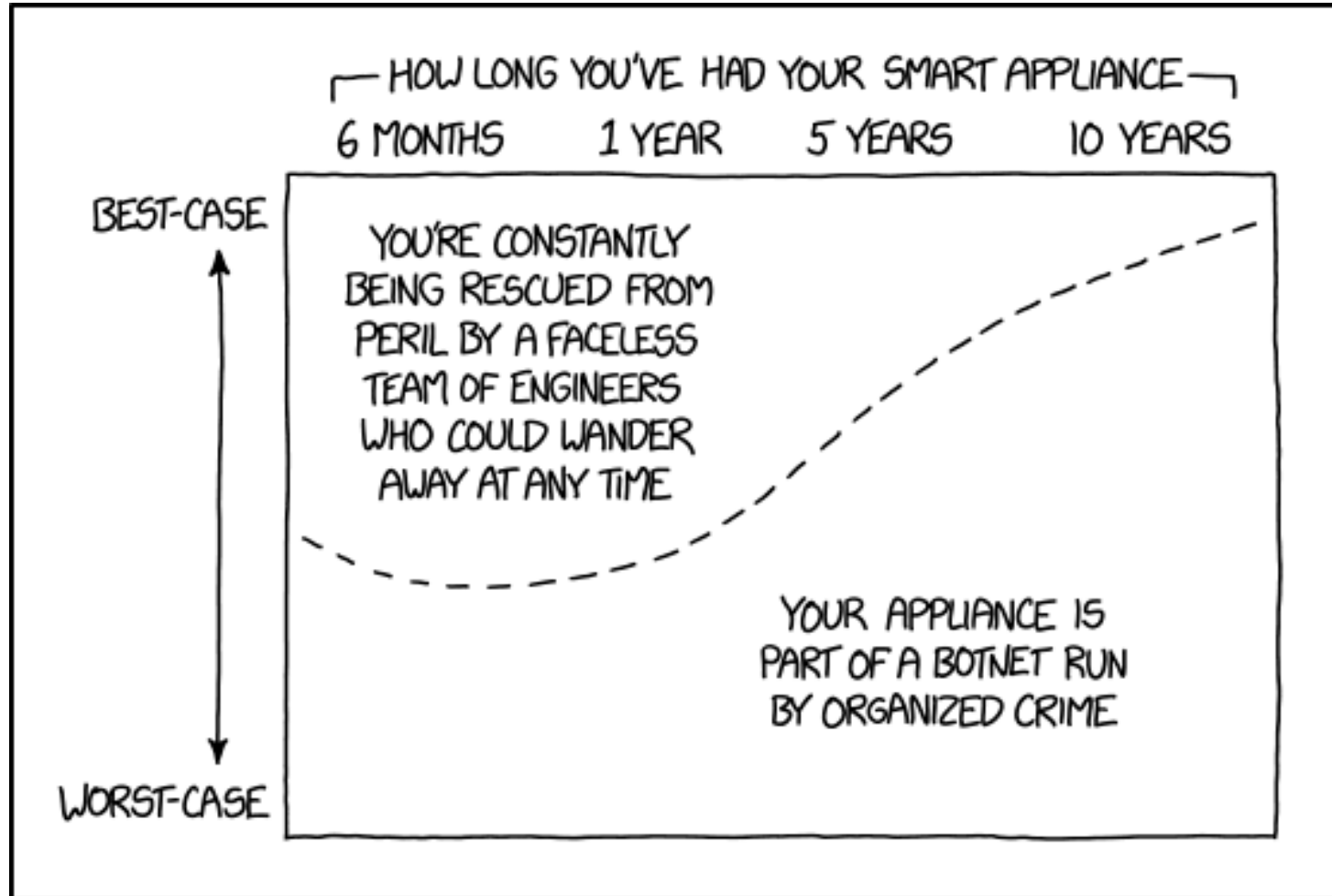
Feedback

1. Rate how well you think this recorded lecture worked
   1. Better than an in-person class
   2. About as well as an in-person class
   3. Less well than an in-person class, but you still learned something
   4. Total waste of time, you didn't learn anything

2. How much time did you spend on this video lecture?

3. Do you have particular questions you'd like me to address in class?

4. Do you have any other comments or feedback?