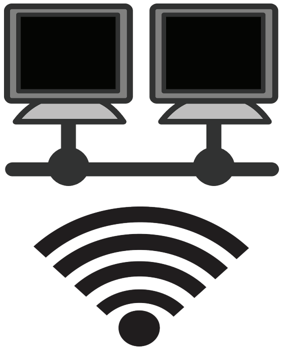
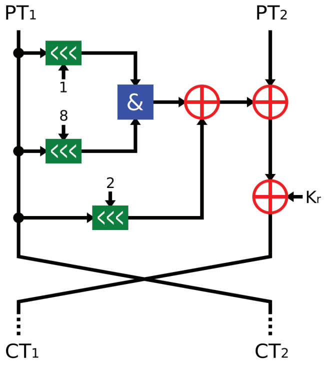
CSE 40567 / 60567: Computer Security





Network Security 4

Homework #6 is due tonight at 11:59PM (your timezone)

See **Assignments Page** on the course website for details

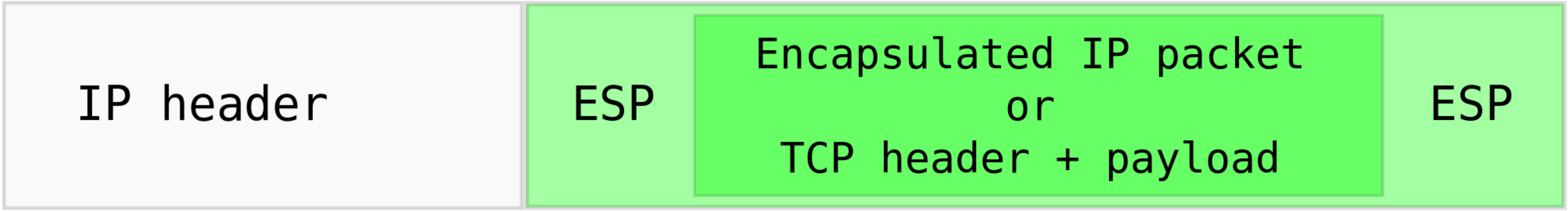
Guest Lecture 4/23: Stephen Watt on hacking, prison, and what came after

Live on zoom!

Covert Channels

Overt vs. Covert Secure Channels

IPSEC is an overt protection mechanism



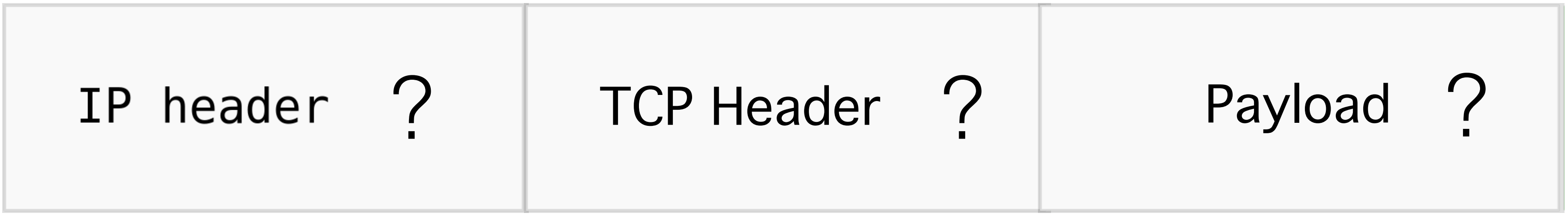
IP header

ESP

Encapsulated IP packet
or
TCP header + payload

ESP

Covert channels hide data in a non-obvious way



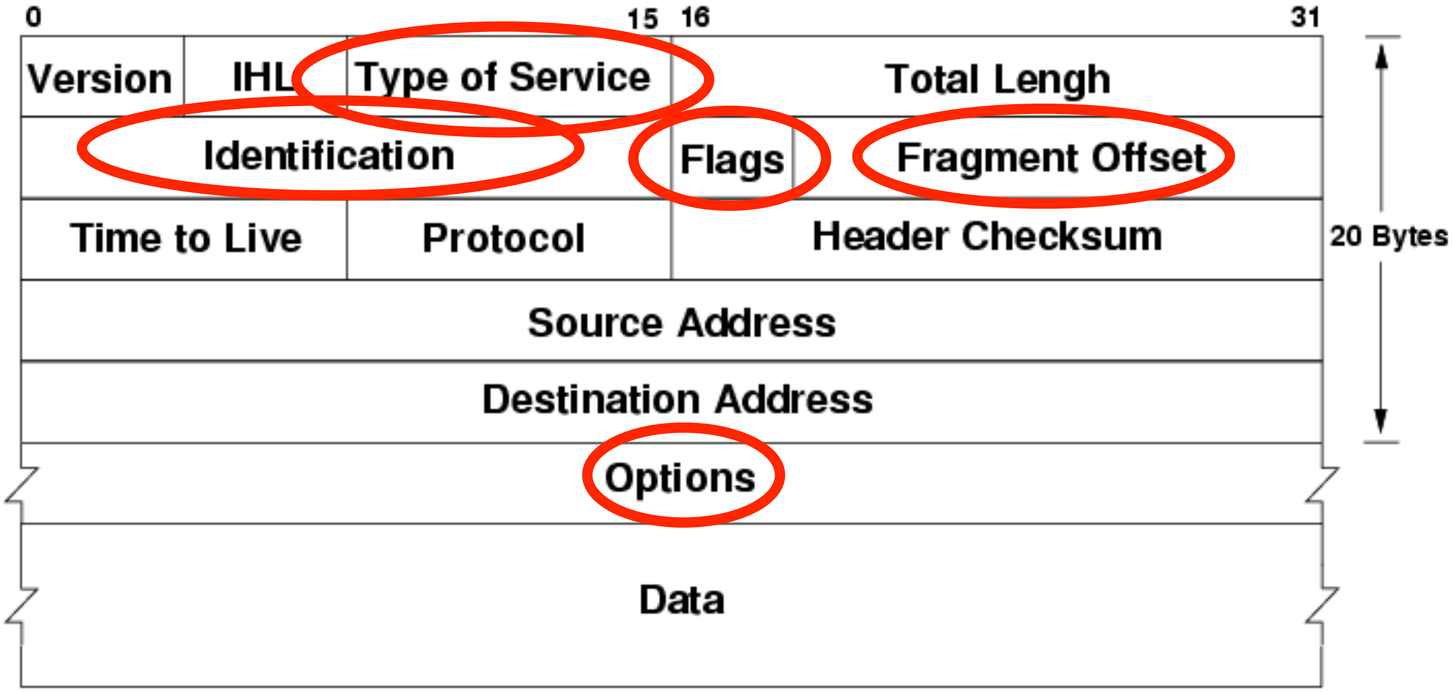
IP header ?

TCP Header ?

Payload ?

Many places to squirrel away data

IP Header



0 15 16 31

Version | IHL | Type of Service | Total Lengh

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

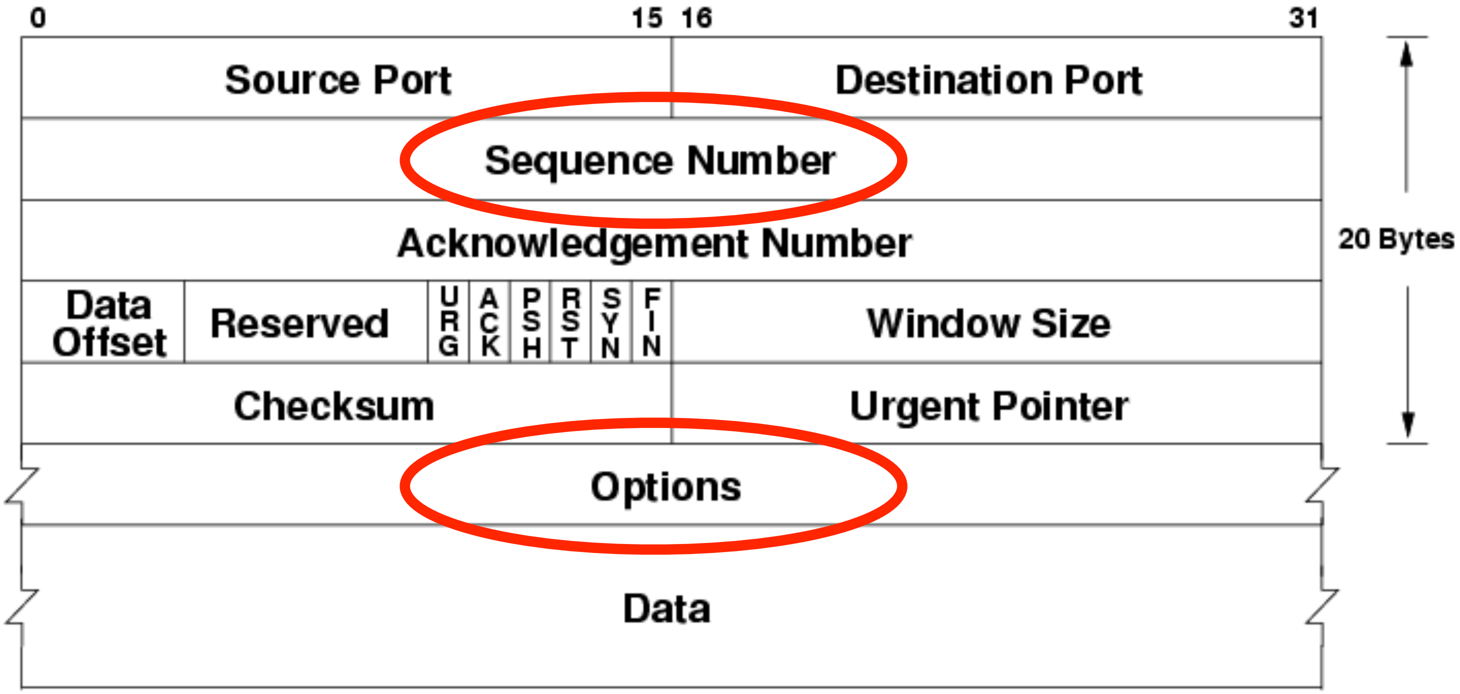
Options

Data

20 Bytes

Many places to squirrel away data

TCP Header



0 15 16 31

Source Port | Destination Port

Sequence Number

Acknowledgement Number

Data Offset | Reserved | URG | ACK | PSH | RST | SYN | FIN | Window Size

Checksum | Urgent Pointer

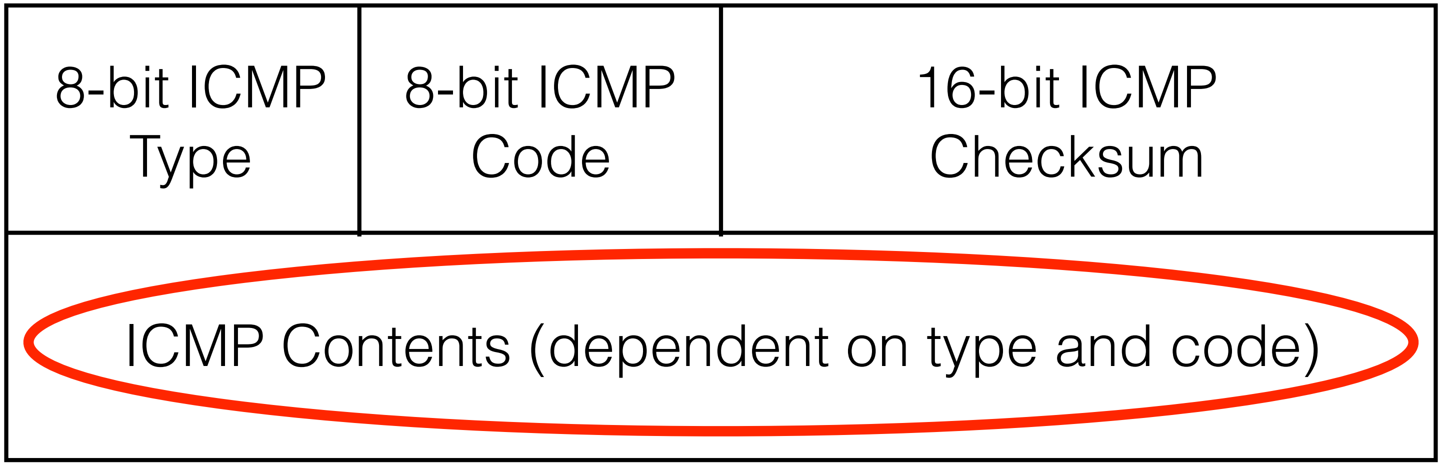
Options

Data

20 Bytes

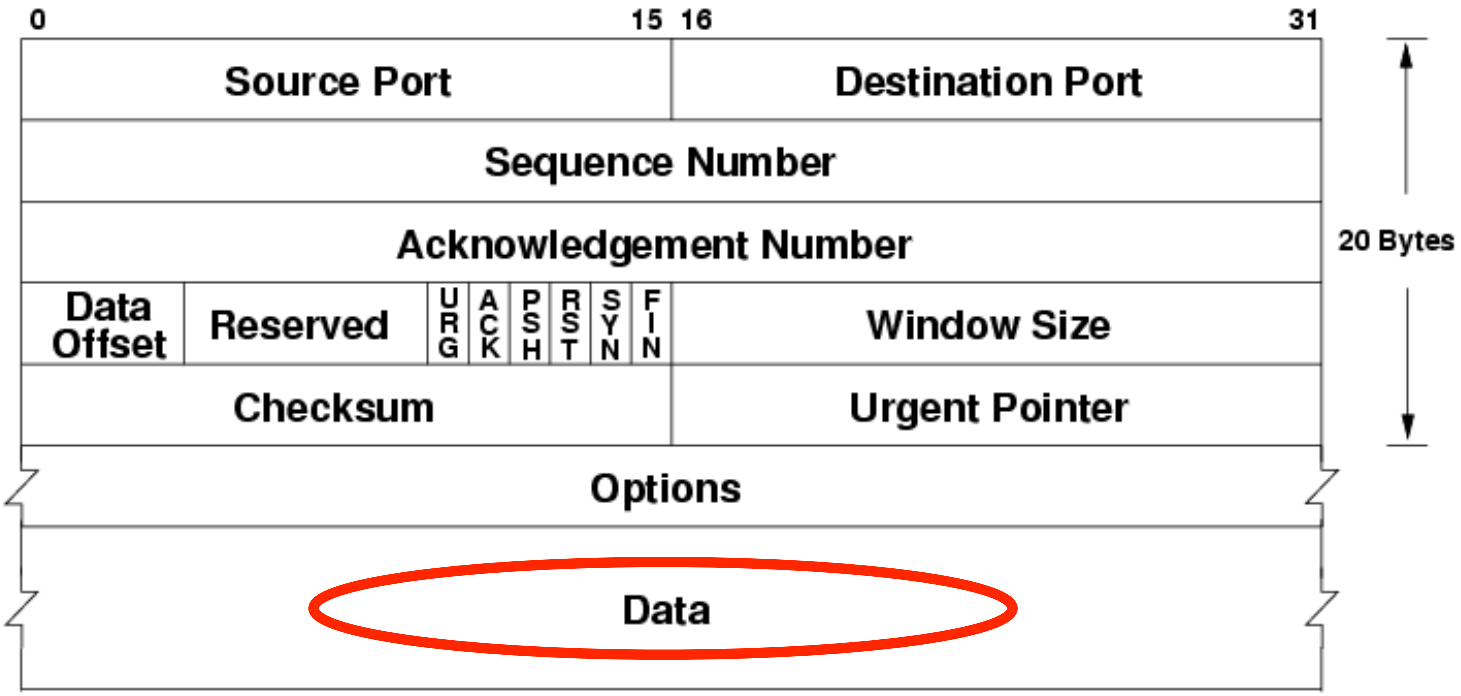
Many places to squirrel away data

Create a tunnel with ping requests and responses

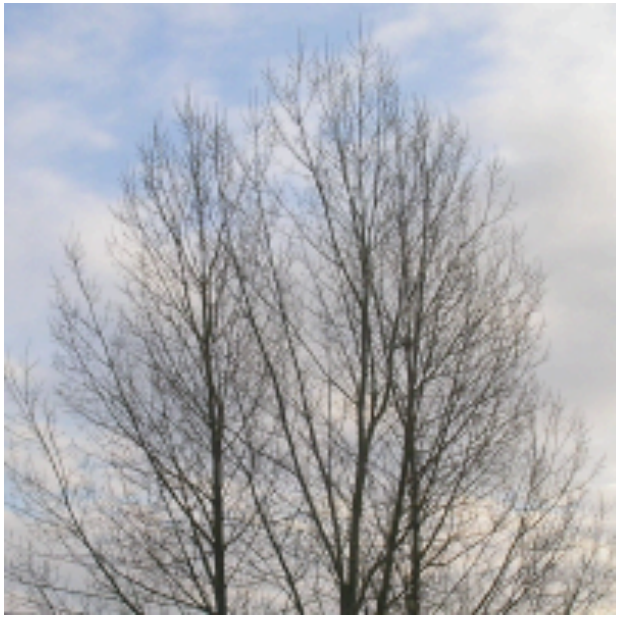


8-bit ICMP Type	8-bit ICMP Code	16-bit ICMP Checksum
ICMP Contents (dependent on type and code)		

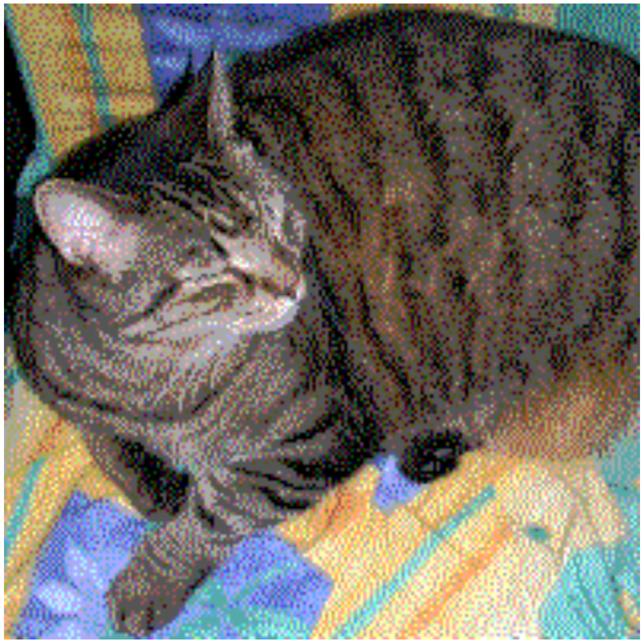
Many places to squirrel away data



Steganography



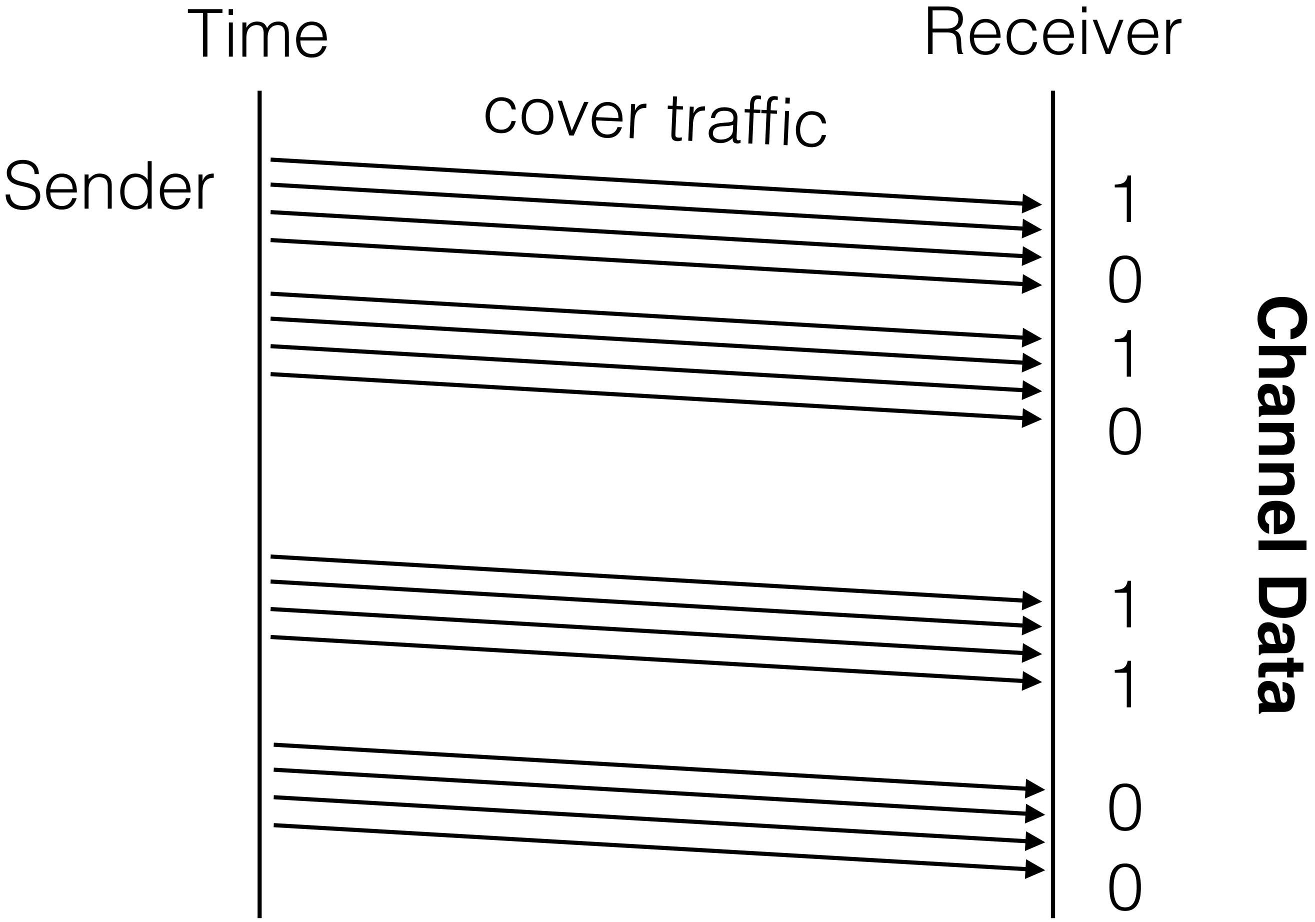
Steganography original cc BY-SA 3.0 Cyp



Steganography recovered cc BY-SA 3.0 Cyp

Timing channels

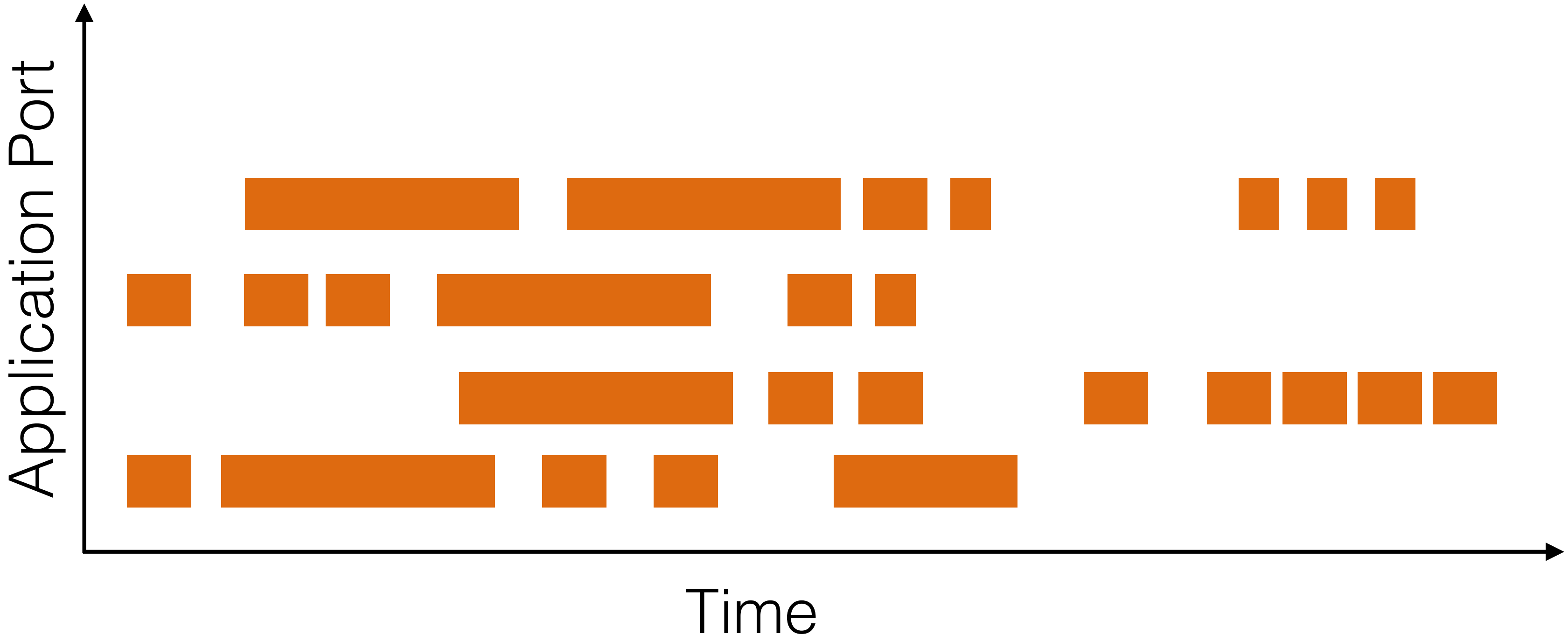
Convey information by triggering or delaying events at set time intervals



Frequency-based channels

Convey information by triggering or delaying events at set time intervals

The ordering or combination of cover channel activity encodes the secret



Software packages

Tunnelshell: https://packetstormsecurity.com/search/files/?q=Tunnelshell

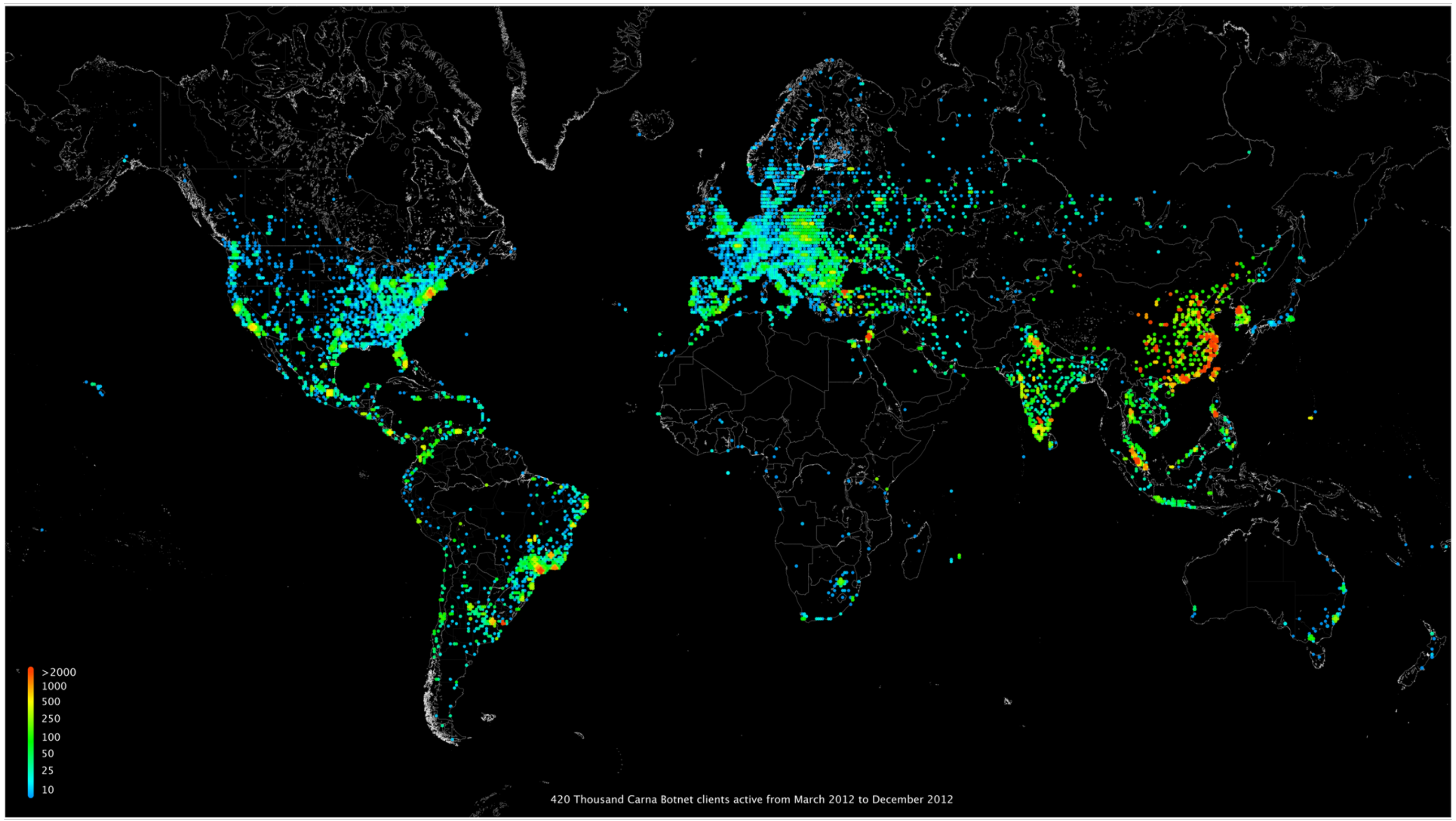
RECUB: http://mir-os.sourceforge.net/recub.htm

ptunnel: http://www.mit.edu/afs.new/sipb/user/golem/tmp/ptunnel-0.61.orig/web/

dns2tcp: in apt

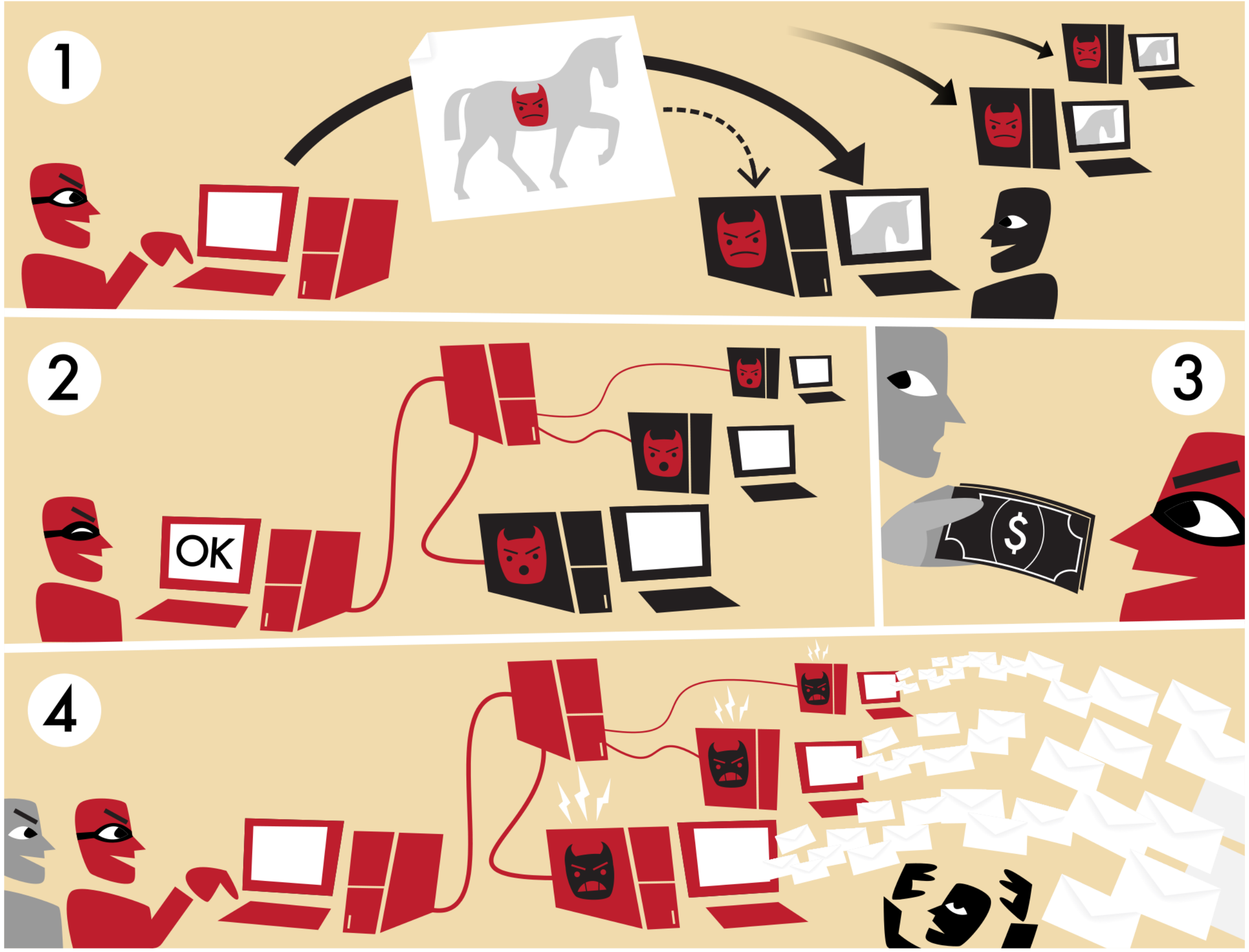
Distributed Denial of Service Attacks

Botnets


>2000
1000
500
250
100
50
25
10
420 Thousand Carna Botnet clients active from March 2012 to December 2012

Carna Botnet March–December 2012 (cc) BY-SA 4.0 Cyp

Distributed Denial of Service Attacks



How a botnet works 🅭 BY-SA 3.0 Uploaded by Tom-b~commonswiki

What does DDoS traffic look like?

General strategy: blast target with as many packets as possible

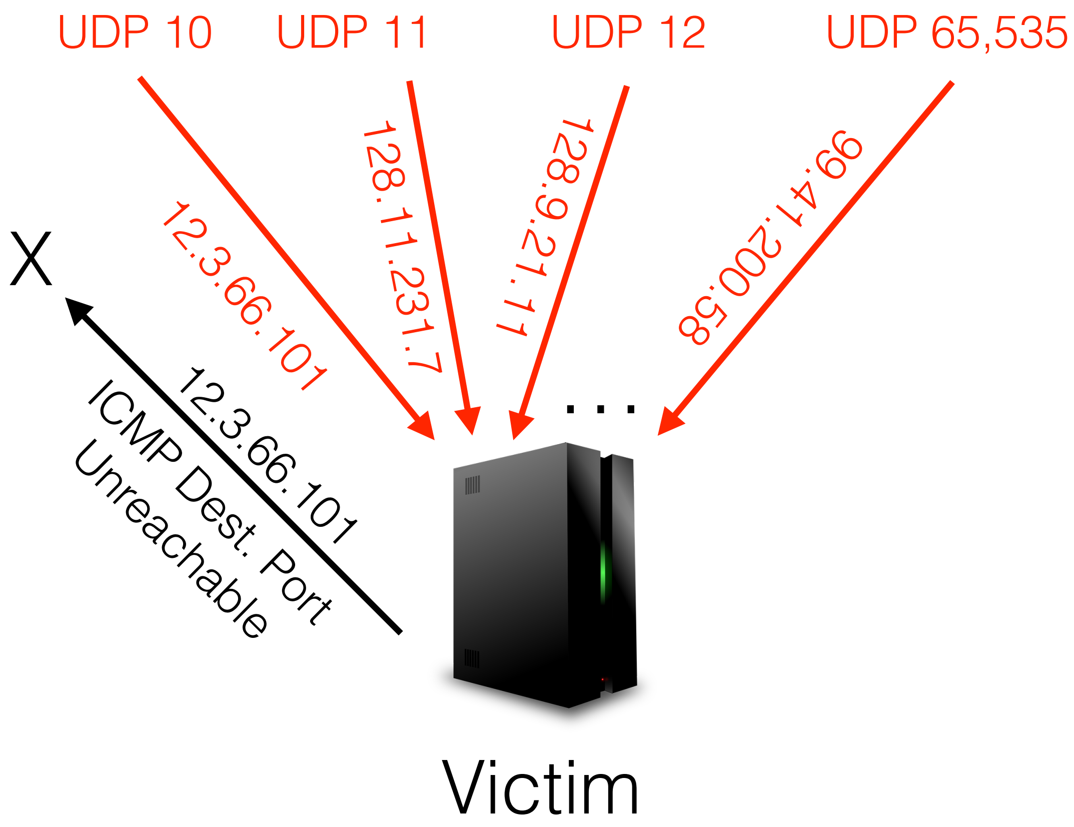
- ‣ Saturates bandwidth
- ‣ May crash OS

- Flood attacks
- Amplification attacks
- Resource depletion attacks

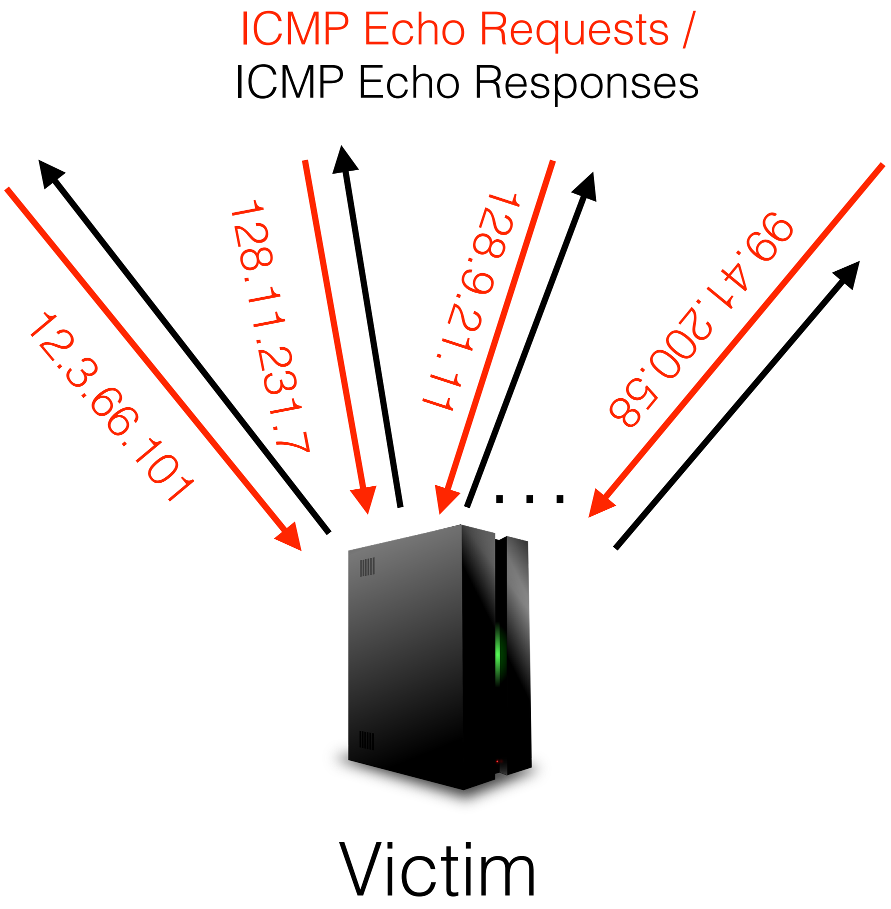
S. Specht and R. Lee, “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures”, 2004

Flood Attacks

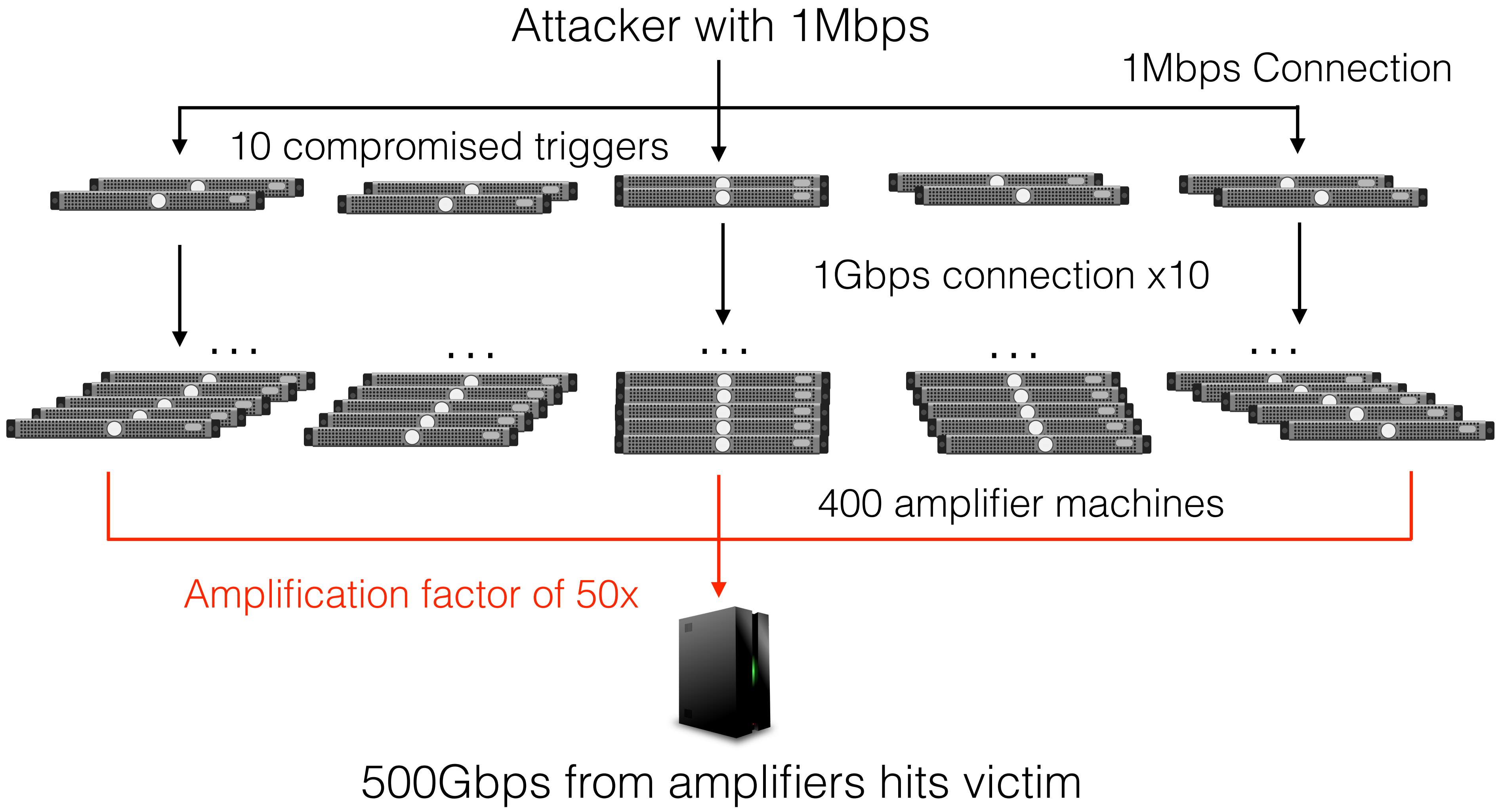
UDP Flood Attack



ICMP Flood Attack



Amplification Attacks

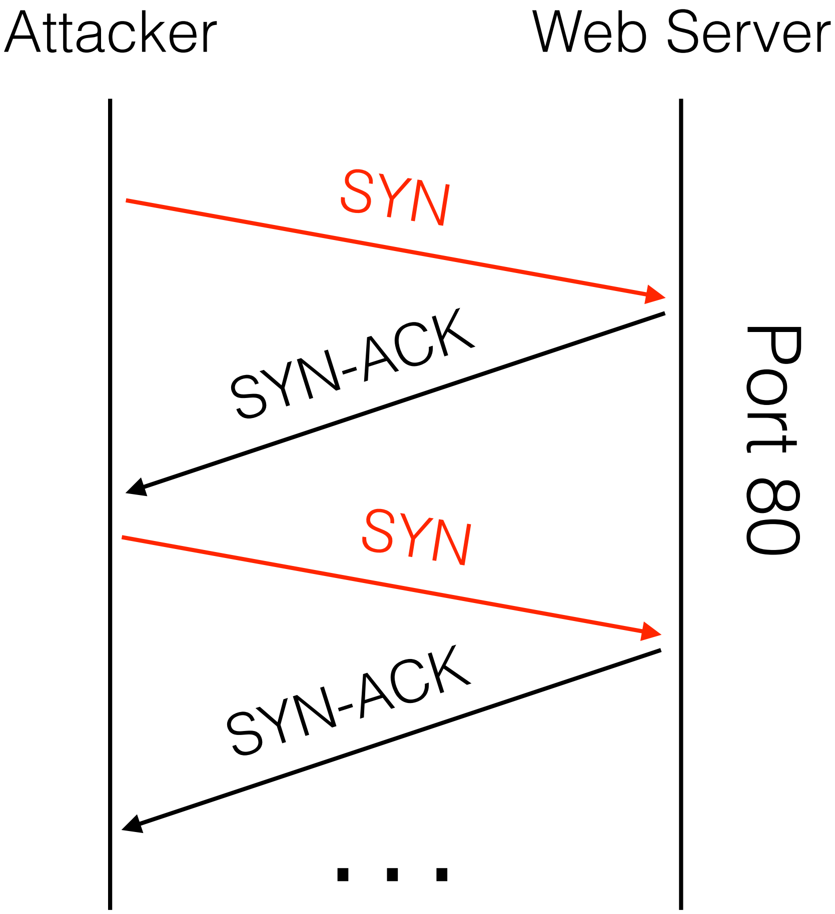


500Gbps from amplifiers hits victim

https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

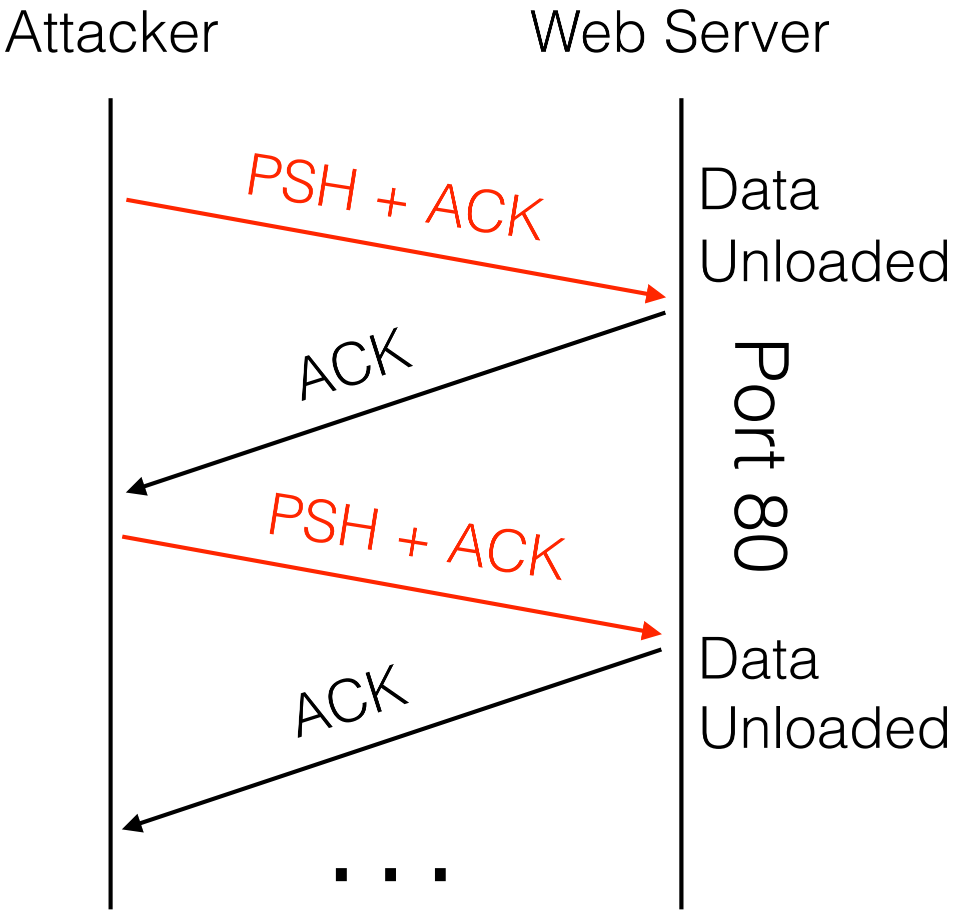
Resource Depletion Attacks

1. TCP SYN Attack



Send SYNs until no more connections can be established

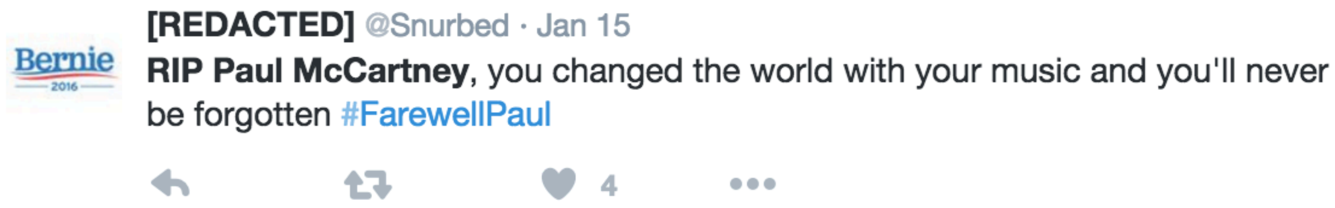
2. TCP PSH + ACK Attack



Send PSH + ACKs until target's resources are exhausted

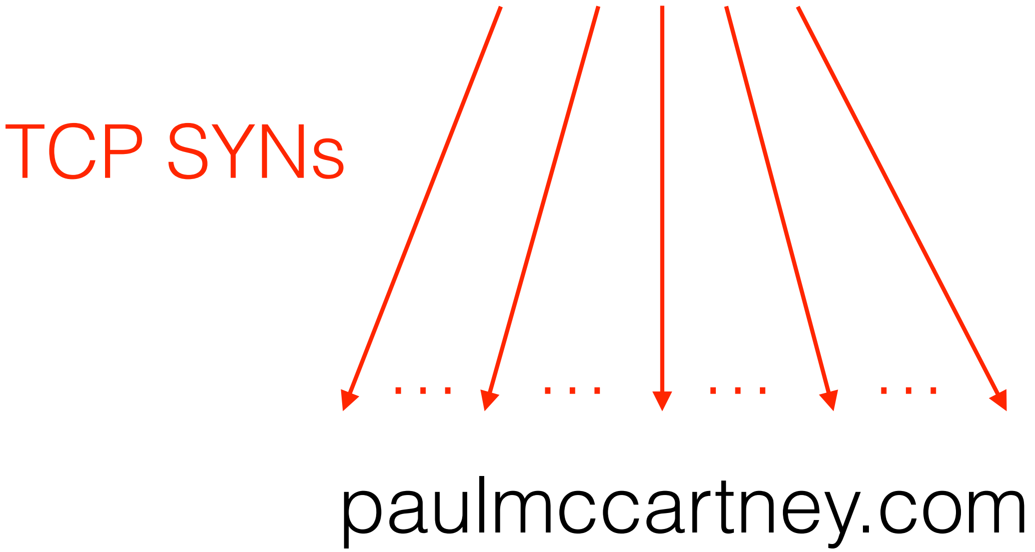
Insidious: direct lots of legitimate traffic to site

https://twitter.com/search?q=%22RIP%20Paul%20McCartney%22



[REDACTED] @Snurbed · Jan 15

RIP Paul McCartney, you changed the world with your music and you'll never be forgotten #FarewellPaul



TCP SYNs

paulmccartney.com

Defenses

- Attacks on the decline (?)
  - Reported peak in the early to mid-2000s (Kaspersky Lab)
- Technical countermeasures are now commonplace
  - Firewalls
  - Switches with rate-limiting and ACLs
  - Routers with rate-limiting and ACLs

http://www.kaspersky.com/internet-security-center/threats/ddos-attacks

Botnet DDoS Attacks: Q4 2015

Kaspersky Lab Report

- Resources in 69 countries were targeted by DDoS attacks.
- 94.9% of the targeted resources were located in 10 countries.
- Largest numbers of DDoS attacks targeted victims in China, the US and South Korea.
- Longest DDoS attack lasted for 371 hours (or 15.5 days).
- SYN DDoS, TCP DDoS and HTTP DDoS remain the most common attack scenarios.
- The proportion of DDoS attacks from Linux-based botnets was 54.8%.

https://securelist.com/analysis/quarterly-malware-reports/73414/kaspersky-ddos-intelligence-report-for-q4-2015/