DoS, Scanning, Firewalls

CMSC 23200, Spring 2025, Lecture 10

Grant Ho

University of Chicago, 04/24/2025
(Slides adapted from Blasé Ur, Peyrin Kao, Vern Paxson, and Zakir Durumeric)

Logistics

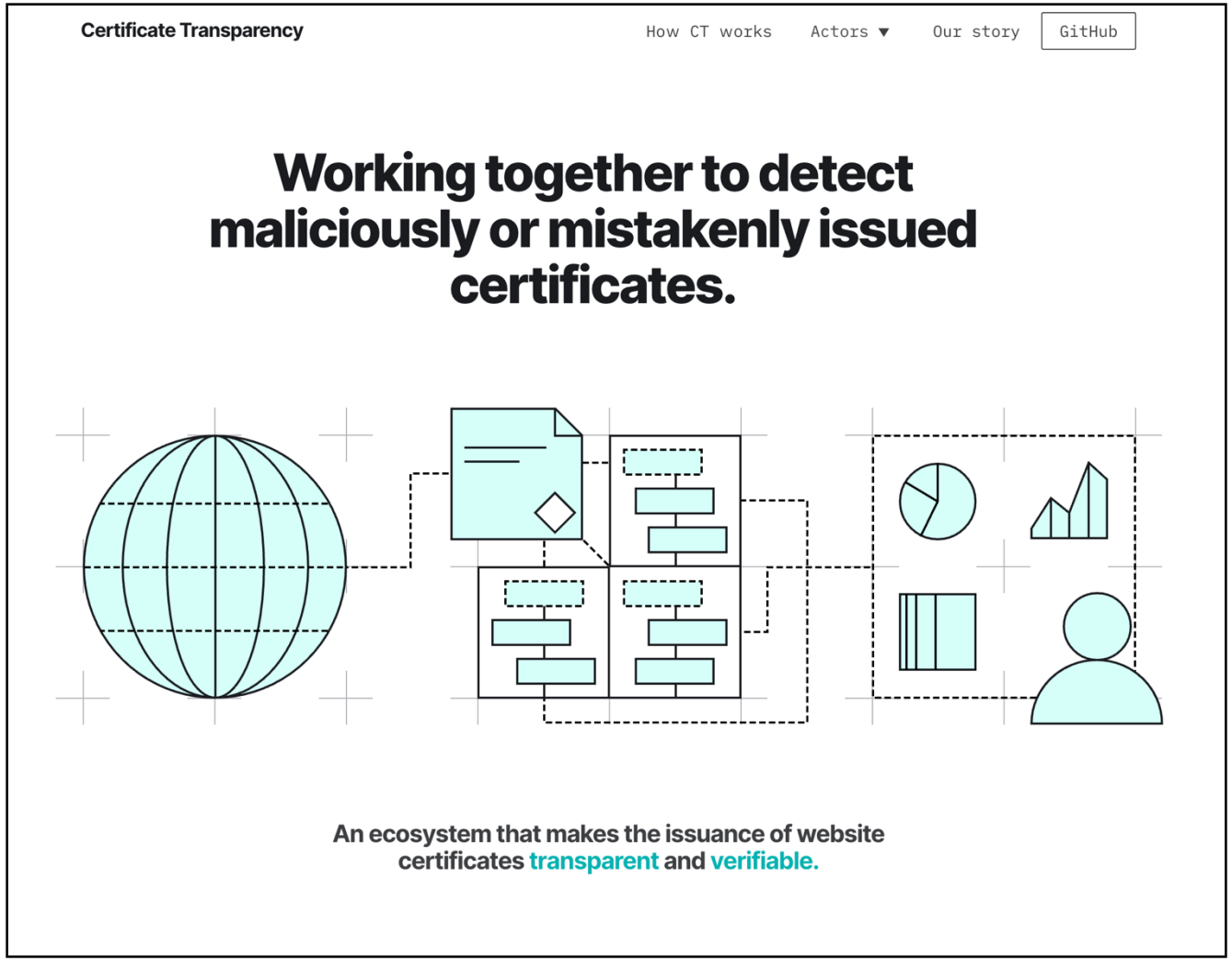
- Assignment 2 grades released
  - Regrades open until next Friday (May 2) at noon

- Assignment 4 released tomorrow

Outline

- Certificates & TLS
- Denial of Service
- Network Scanning & Firewalls

Certificate Transparency (CT): How do we find rogue certs?



Scenario: Attackers compromise a CA and create rogue certs for `google.com` that have
(1) attacker's public keys and
(2) valid CA signature

How does Google or the CA discover these rogue certs were issued or in use?

Cert Transparency:

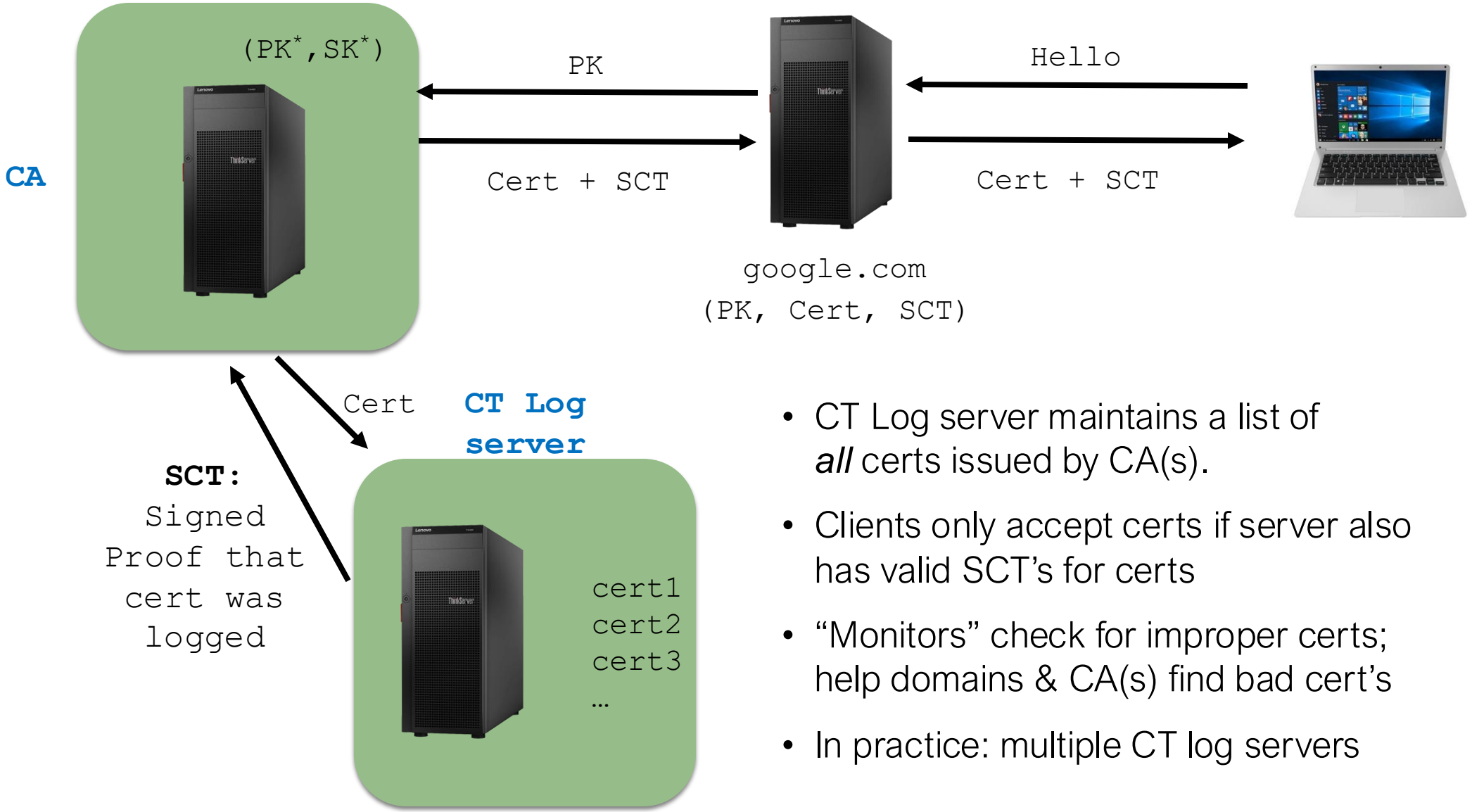
- Require all cert's added to public audit logs
- Domains & CA's can check audit logs for rogue certs & revoke them

Certificate Transparency (CT)

Simplified strategy to find certificates we should revoke:

- An auditor maintains a list (log) of every certificate ever issued
- Whenever a CA issues a cert, they submit (add) cert to this log
- Clients only accept a server's cert if it appears on the log
- Each server (domain) can now monitor the logs to see if anyone (and who) issued a rogue certificate for them
  - If so, add the rogue cert to revocation lists
  - If CA has pattern of issuing rogue cert's, ban them

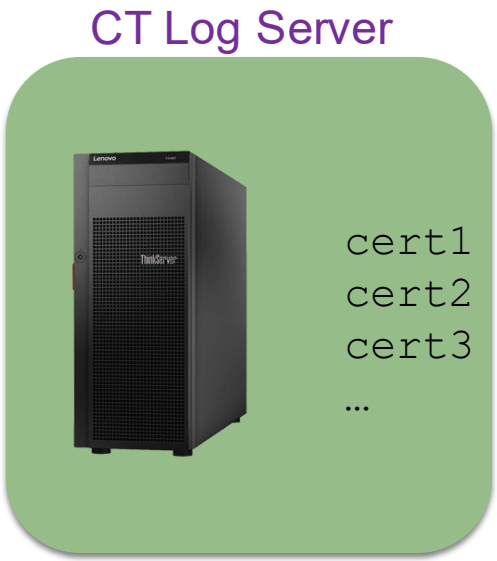
Certificate Transparency (CT)



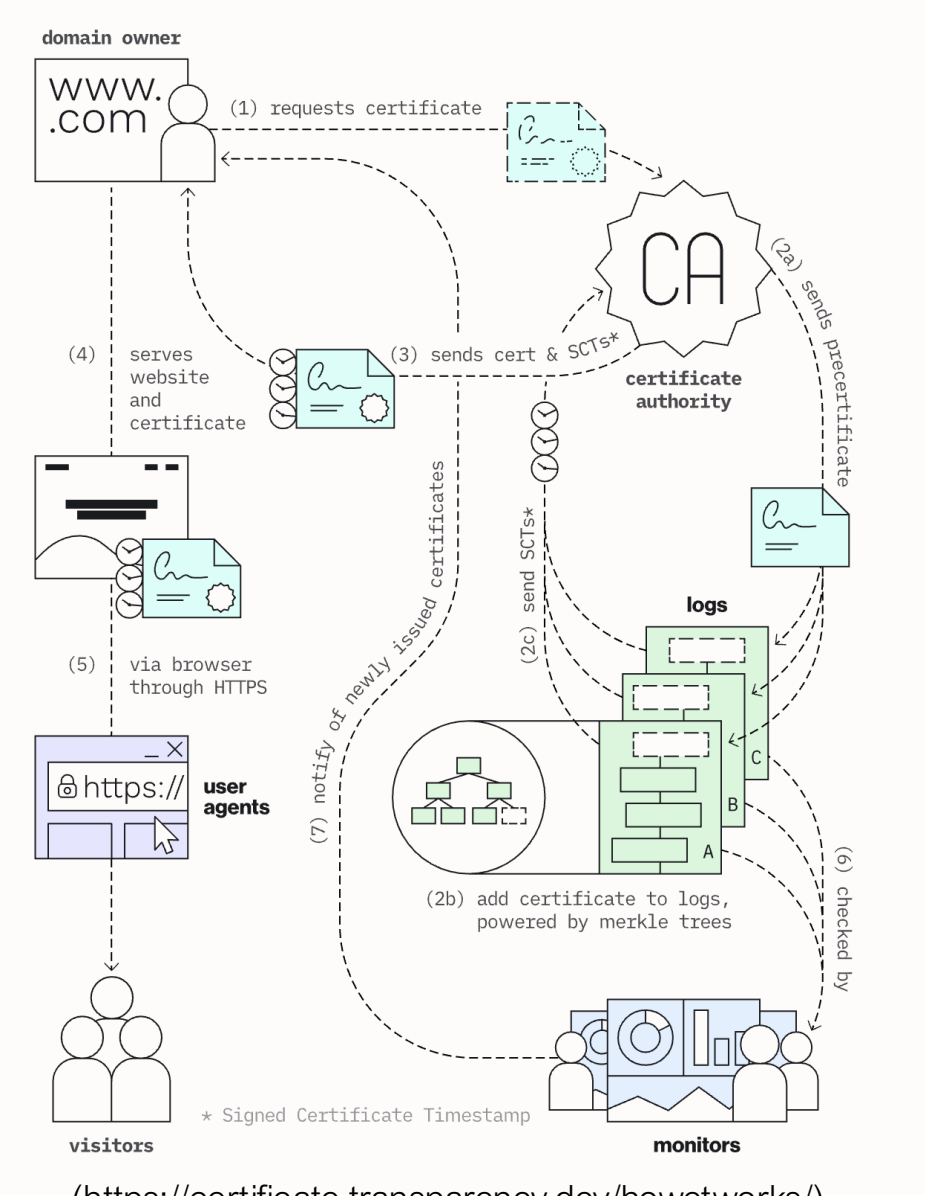
- CT Log server maintains a list of *all* certs issued by CA(s).
- Clients only accept certs if server also has valid SCT's for certs
- "Monitors" check for improper certs; help domains & CA(s) find bad cert's
- In practice: multiple CT log servers

Challenges with CT

- List is huuuuge (every issued cert… solution: temporal sharding)
- Trust the CT Log?
- (Monitors) Who checks the logs?
- Privacy (e.g., enterprise has private servers)?



Cert Transparency & OCSP



(https://certificate.transparency.dev/howctworks/)

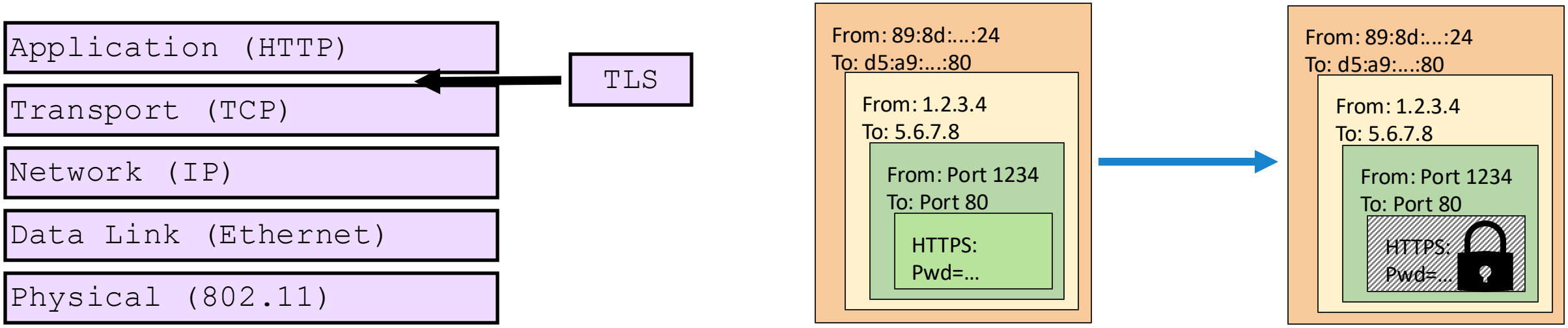
How do CT and OCSP compare?

- OCSP: Allows *clients* to determine if a cert is valid
- CT: Allows *domains* (cert owners) and *CA's* to find malicious cert's

Outline

- Certificates & TLS
- Denial of Service
- Network Scanning & Firewalls

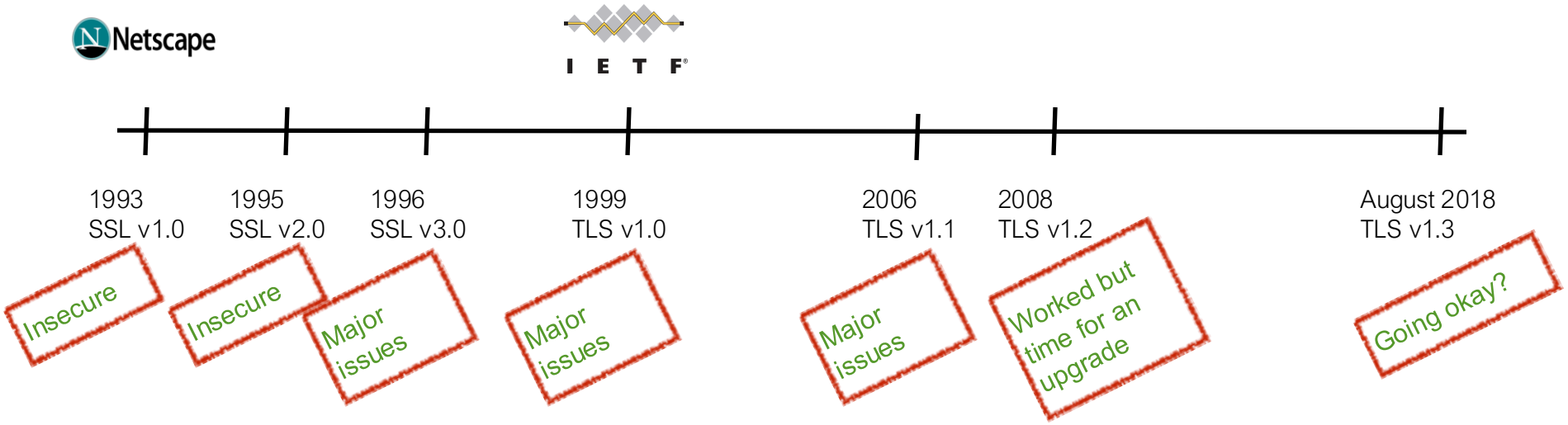
TLS: Transport Layer Security Protocol



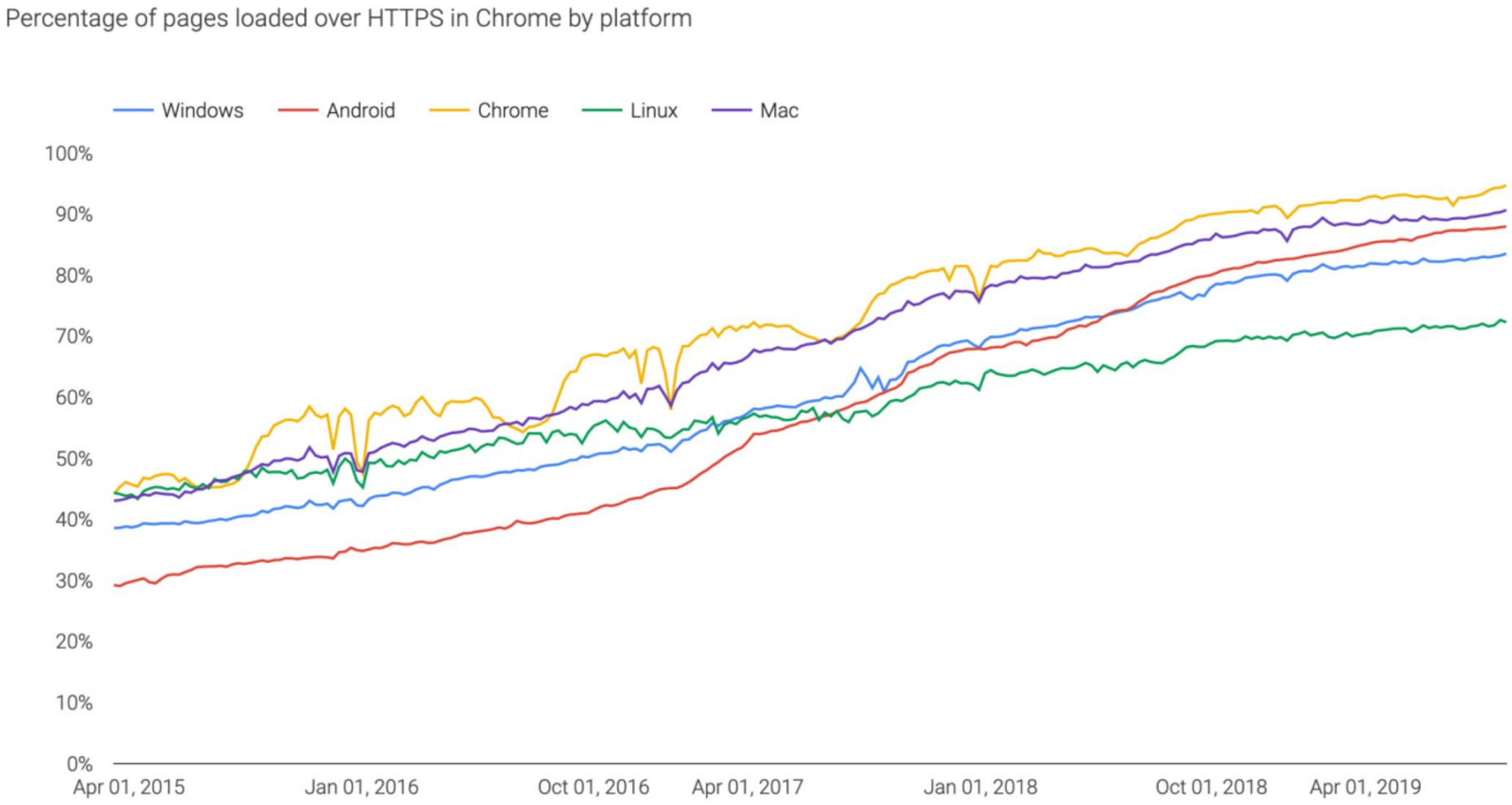
- **Goal:** Allow any application using TCP to transmit data with E2E security
- TLS takes requests from applications (e.g. browser speaking HTTP) and transmits them securely to another host on the Internet

History: SSL/TLS

- SSL = “Secure Sockets Layer”
- TLS = “Transport Layer Security” (renaming of SSL)

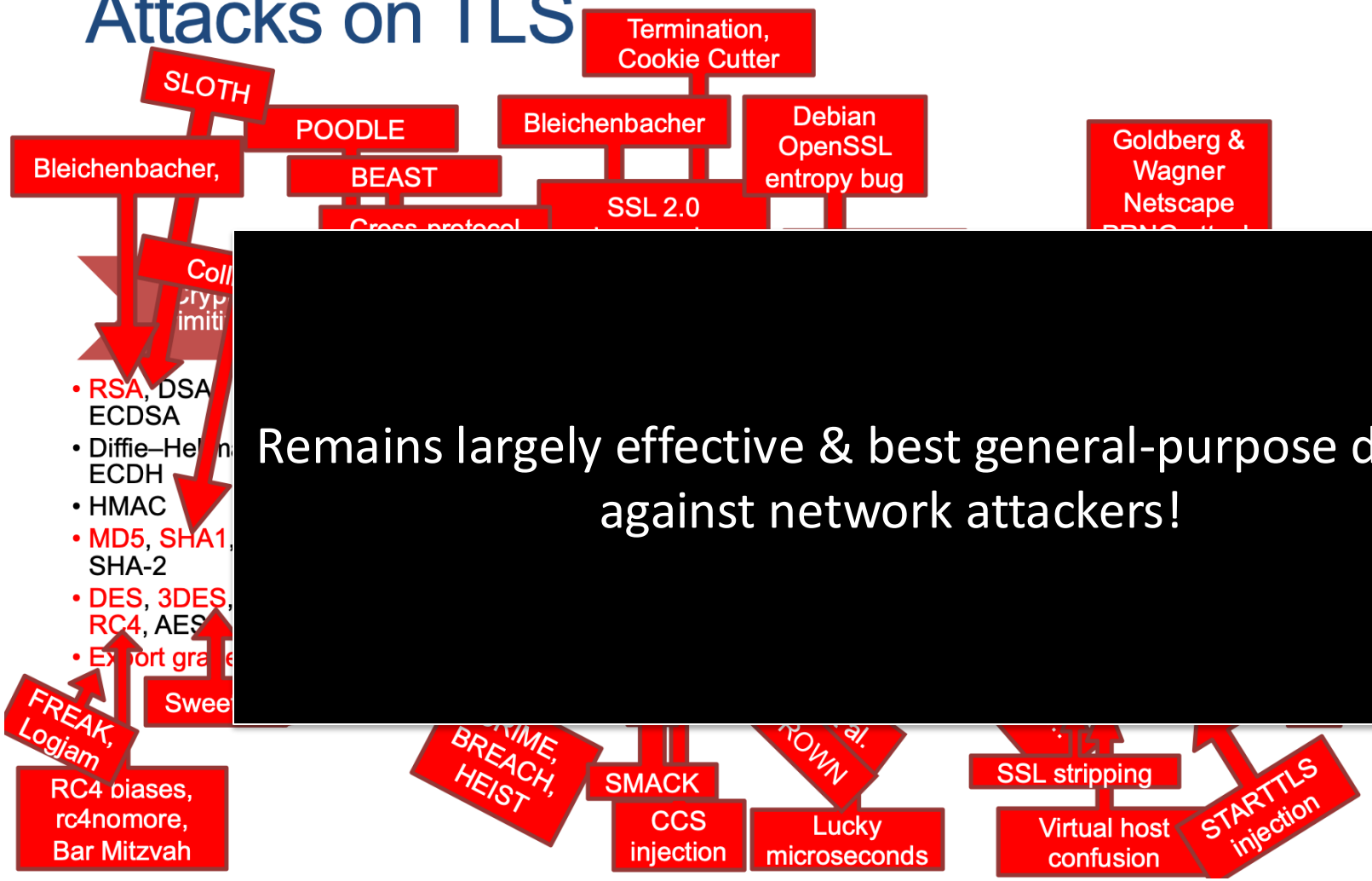


TLS Adoption (HTTPS)

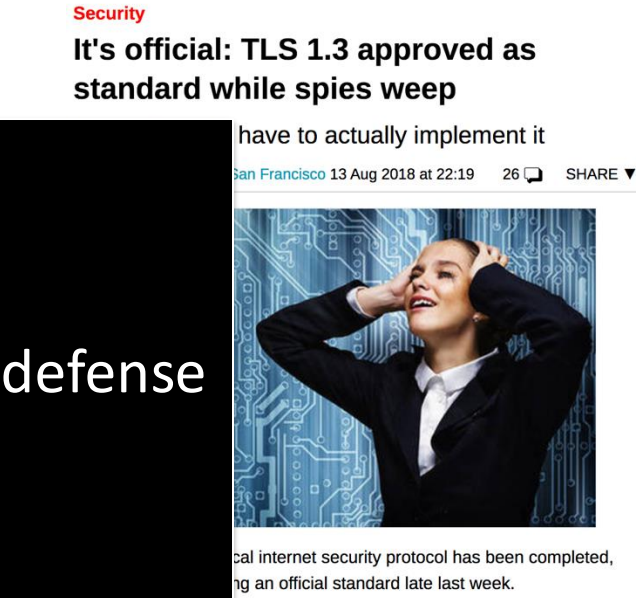


(Source: transparencyreport.google.com, via Matt Green)

Attacks on TLS



Remains largely effective & best general-purpose defense against network attackers!



TLS Protocol: Very Similar to Our Template

- Is cert for Bob?
- Is cert in CT logs and has it been revoked?
- Does the certificate *chain* have valid signatures?

PK, SK ← Keygen

Alice

Hello [Protocols & Init]

cert=[PK,"Bob",σ]

C = Enc(PK, K)

Verify Integrity & Keys
(MAC(K, Dialogue))

Bob

Pick random key K

K

K←Dec(SK,C)

K

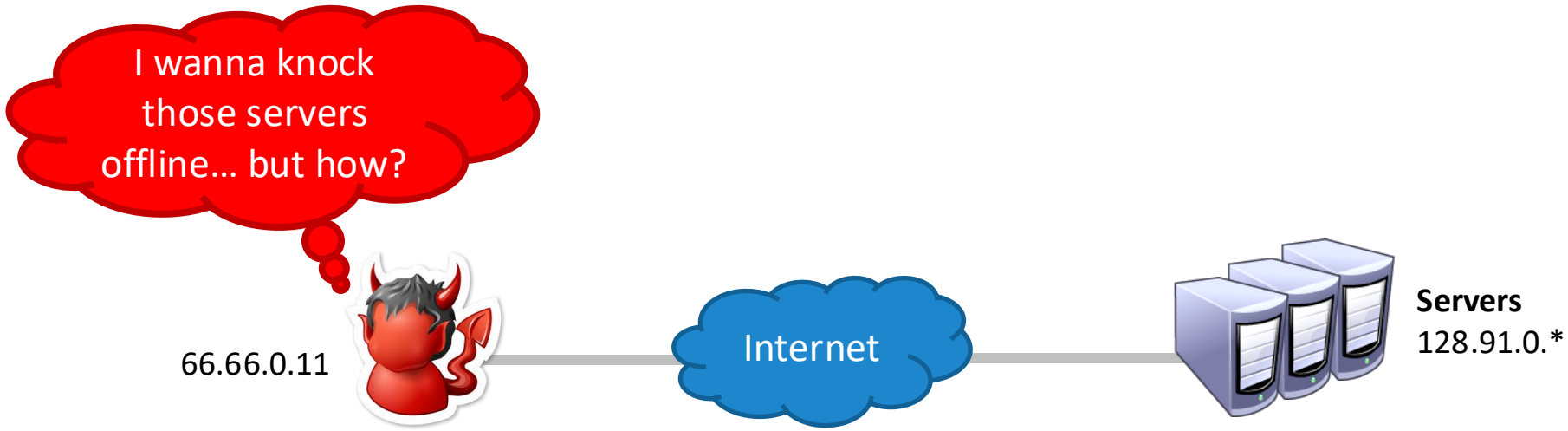
AES-GCM(K,Mi)

Outline

- Certificates & TLS
- Denial of Service (Availability Attacks)
- Network Scanning & Firewalls

Denial of Service (DoS) Attacks

- **Goal:** Prevent users from being able to access a target: specific computer, service, or piece of data (Disrupt Availability)
- **Threat Model:** Active attacker who can freely send packets to target



Attacker Motivations for DoS

- Showing off / entertainment / ego
- Competitive advantage
  - Maybe commercial, maybe just to win
- Vendetta / denial-of-money
- Extortion
- Impair defenses
- Political statements / manipulation
- Warfare

Botnets Beat Spartan Laser on *Halo 3*

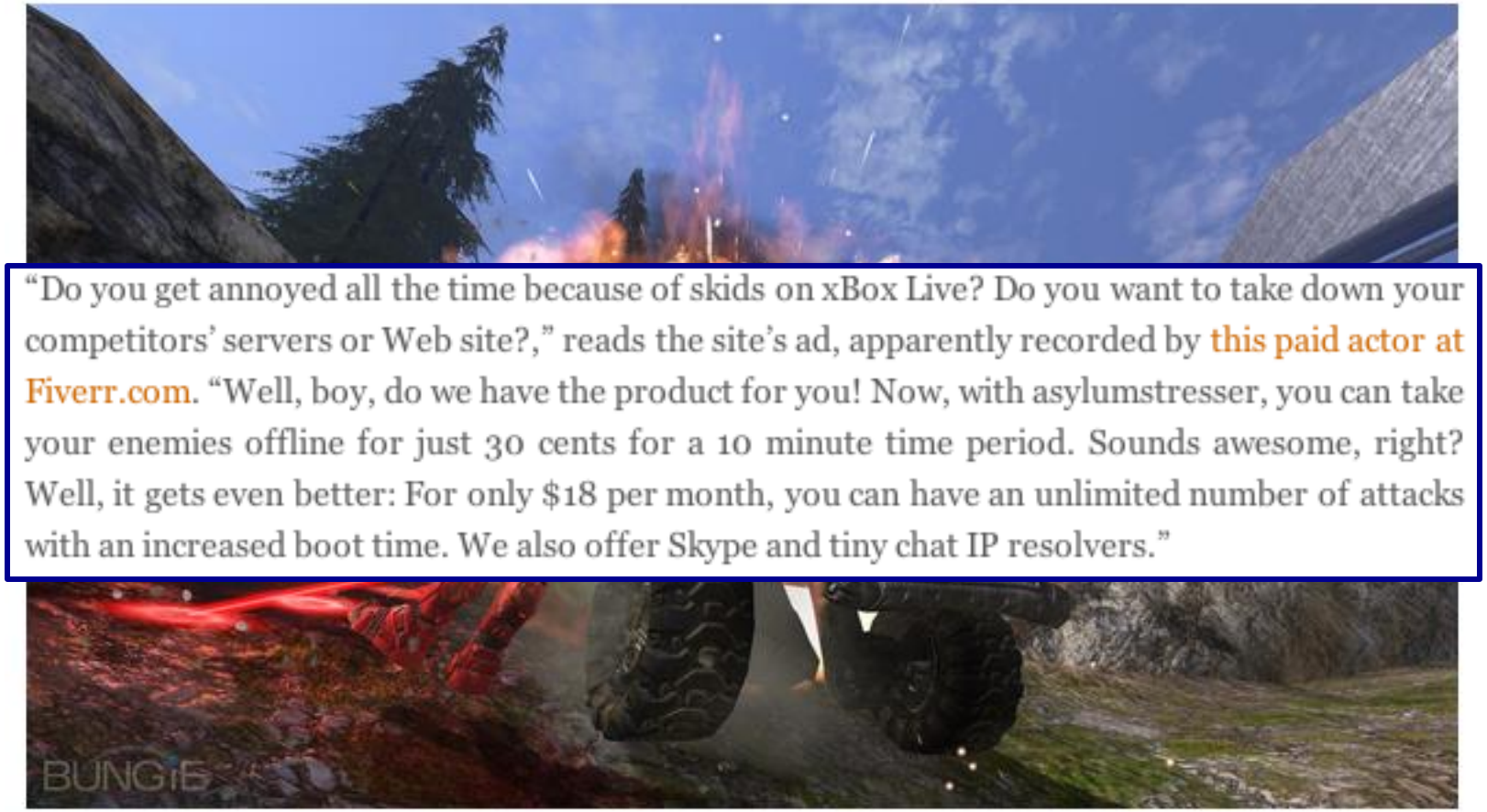
By Kevin Poulsen ✉ February 4, 2009 | 12:13 pm | Categories: Cybarmageddon!

What's the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.

Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen ✉ February 4, 2009 | 12:13 pm | Categories: Cybarmageddon!



"Do you get annoyed all the time because of skids on xBox Live? Do you want to take down your competitors' servers or Web site?," reads the site's ad, apparently recorded by this paid actor at Fiverr.com. "Well, boy, do we have the product for you! Now, with asylumstresser, you can take your enemies offline for just 30 cents for a 10 minute time period. Sounds awesome, right? Well, it gets even better: For only $18 per month, you can have an unlimited number of attacks with an increased boot time. We also offer Skype and tiny chat IP resolvers."

What's the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.


DDOS EM'
WHEN IN DOUBT KNOCK EM' OUT!
Features
Resolvers
Skype
Steam
Cloudflare
IP Tools
Geolocation
IP Logger
Host to IP
MAX BOOT TIME OF
3600
UDP, SSYN, RUDY, UDP-LAG, ARME, GET, POST

Extortion via DDoS on the rise

By Denise Pappalardo and Ellen Messmer, Network World, 05/16/05

Criminals are increasingly targeting corporations with distributed denial-of-service attacks designed not to disrupt business networks but to extort thousands of dollars from the companies.

Ivan Maksakov, Alexander Petrov and Denis Stepanov were accused of receiving $4 million from firms that they threatened with cyberattacks.

The trio concentrated on U.K. Internet gambling sites, according to the prosecution. One bookmaker, which refused to pay a demand for $10,000, was attacked and brought offline--which reportedly cost it more than $200,000 a day in lost business.

December 8, 2010, 4:18 PM

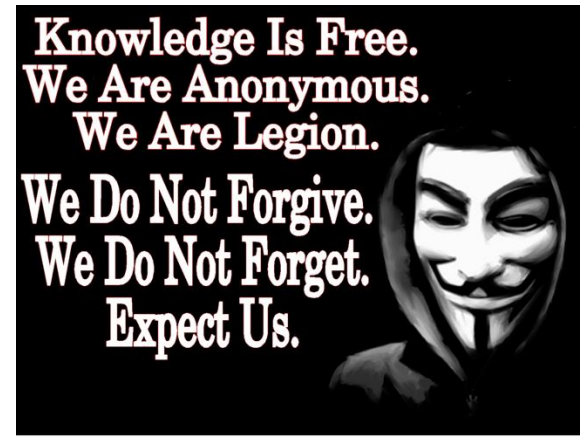
‘Operation Payback’ Attacks Fell Visa.com

By ROBERT MACKEY

A message posted on Twitter by a group of Internet activists announcing the start of an attack on Visa’s Web site, in retaliation for the company’s actions against WikiLeaks.

Last Updated | 6:54 p.m. A group of Internet activists took credit for crashing the Visa.com Web site on Wednesday afternoon, hours after they launched a similar attack on MasterCard. The cyber attacks, by activists who call themselves Anonymous, are aimed at punishing companies that have acted to stop the flow of donations to WikiLeaks in recent days.

The group explained that its distributed denial of service attacks — in which they essentially flood Web sites site with traffic to slow them down or knock them offline — were part of a broader effort called Operation Payback, which



Denial of Service (DoS): Availability

Two main DoS Strategies:

1. Exploit program flaws (e.g., bug that crashes the target)
2. Exhaust the target's resources (CPU, memory, bandwidth, etc.)

Often very easy to perform… but difficult to mitigate ☹

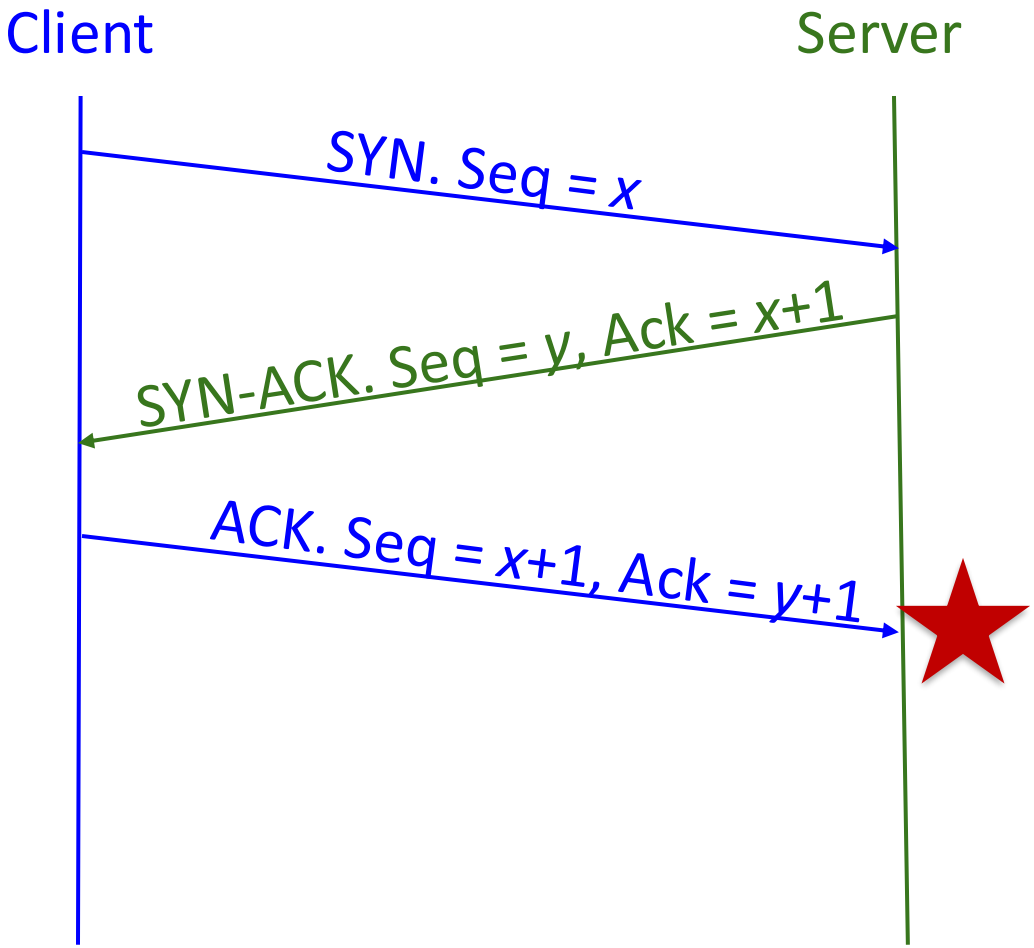
DoS from program flaws = fairly straightforward

– Most attacks we'll discuss focus on resource exhaustion

DoS Attack Parameters

- Asymmetric Attack:
  - Attacker either generates a much larger cost at the target, or has much more resources (e.g., bandwidth) than the target
- What kind of packets does the attacker send to the victim?
  - Minimize effort and risk of detection for attacker
  - While also maximizing damage to the target

TCP SYN Flooding



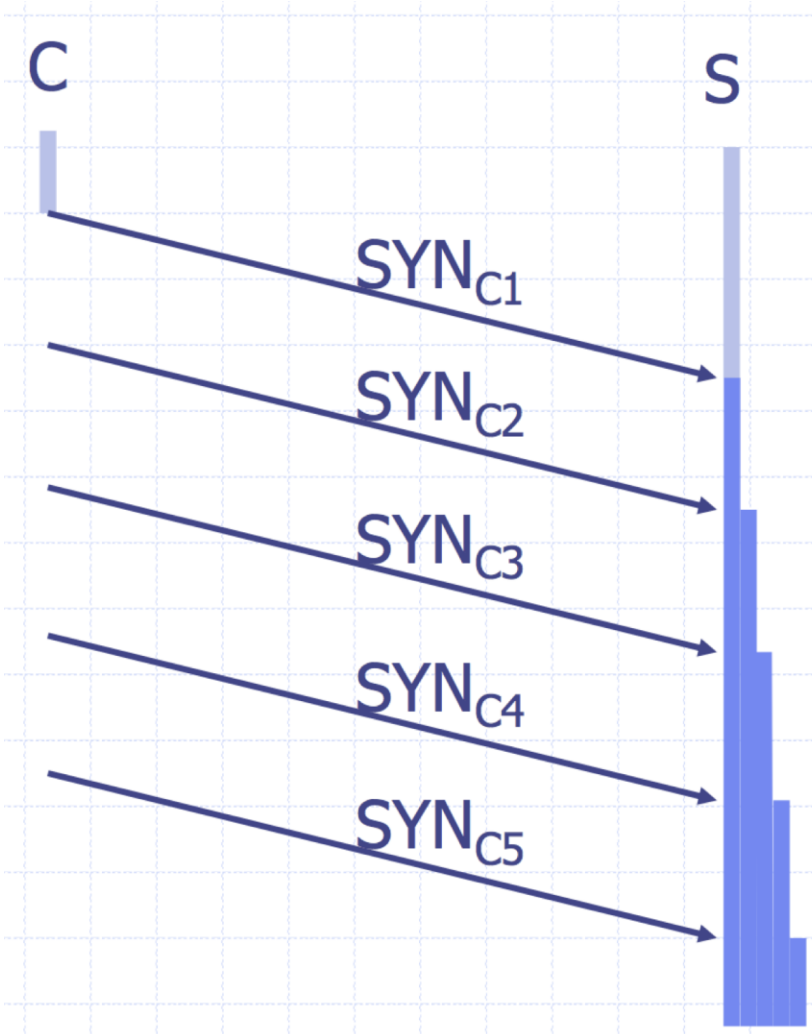
Server stores state during TCP handshake:

- Allocates memory to validate that client's ACK number is correct

Attack: Flood the target with SYN packets

- Exhausts available memory for target: no more connections
- Asymmetry: Easy to Spoof many SYN packets & attacker doesn't need state

TCP SYN Flooding



Single machine:

- SYN Packets with **random source IP addresses**
- Fills up backlog queue on server
- No further connections possible

SYN Flooding Defenses

- **Core Problem:** Server commits resources without confirming client's identity or requiring them to commit resources

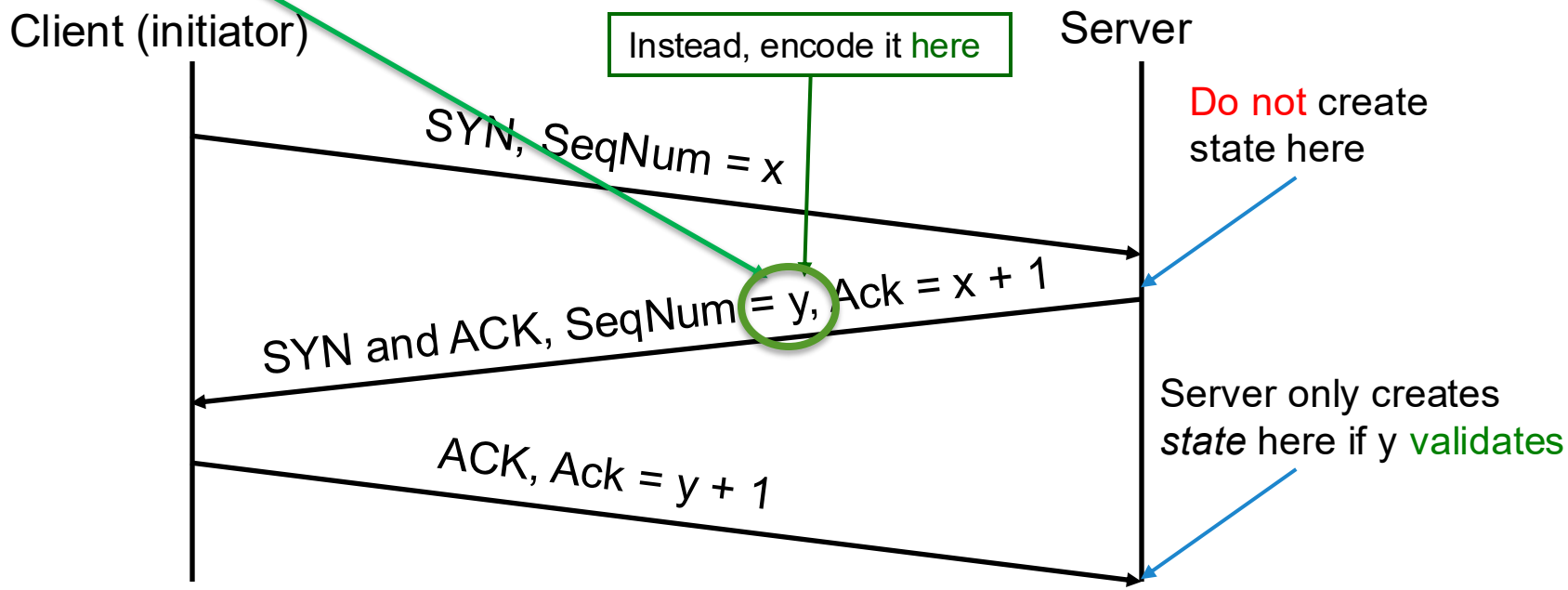
- **Defense Approach #1:** Overprovision
  - Have lots of servers with lots of memory
  - Drawbacks: expensive + target server might not be able to acquire sufficient resources vs. motivated attacker

SYN Flooding Defenses

- **Approach #2:** Detect & Filter
  - Server can try to identify packets that are SYN Flooding & ignore them
  - Drawbacks: hard to identify them
    - Only have src IP address in packets
    - But the attacker can spoof these src IP addresses!
- **Approach #3:** Change the ACK validation so the server doesn't have to store state!
  - Practical Defense: SYN cookies

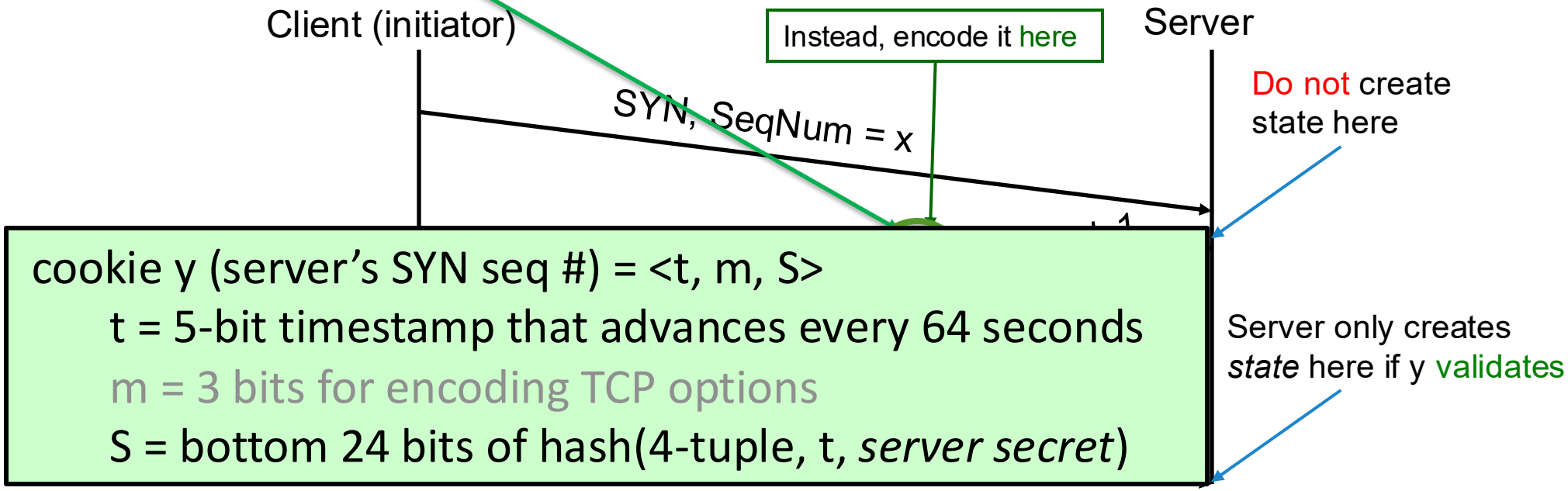
Practical Defense: *SYN Cookies*

- Server: when SYN arrives, encode critical state entirely within SYN-ACK's sequence # y !
  - y = *encoding* of necessary state, using server secret
- When ACK of SYN-ACK arrives, server only creates state ***if*** value of **y** from it agrees w/ secret



Practical Defense: *SYN Cookies*

- Server: when SYN arrives, encode critical state entirely within SYN-ACK's sequence # y !
  - y = *encoding* of necessary state, using server secret
- When ACK of SYN-ACK arrives, server only creates state *if* value of **y** from it agrees w/ secret



Reflection & Amplification Attacks

SYN Flooding: exhaust *memory* of server

Network DoS: exhaust *network bandwidth* of server / client

- Amplification Attacks: Exploit asymmetry in protocols, where a network request packet generates much greater response traffic
- Reflection Attacks: Use third-party machines (not controlled by attacker) to flood the target
- Amplification + Reflection often used together

Ping (ICMP) Protocol

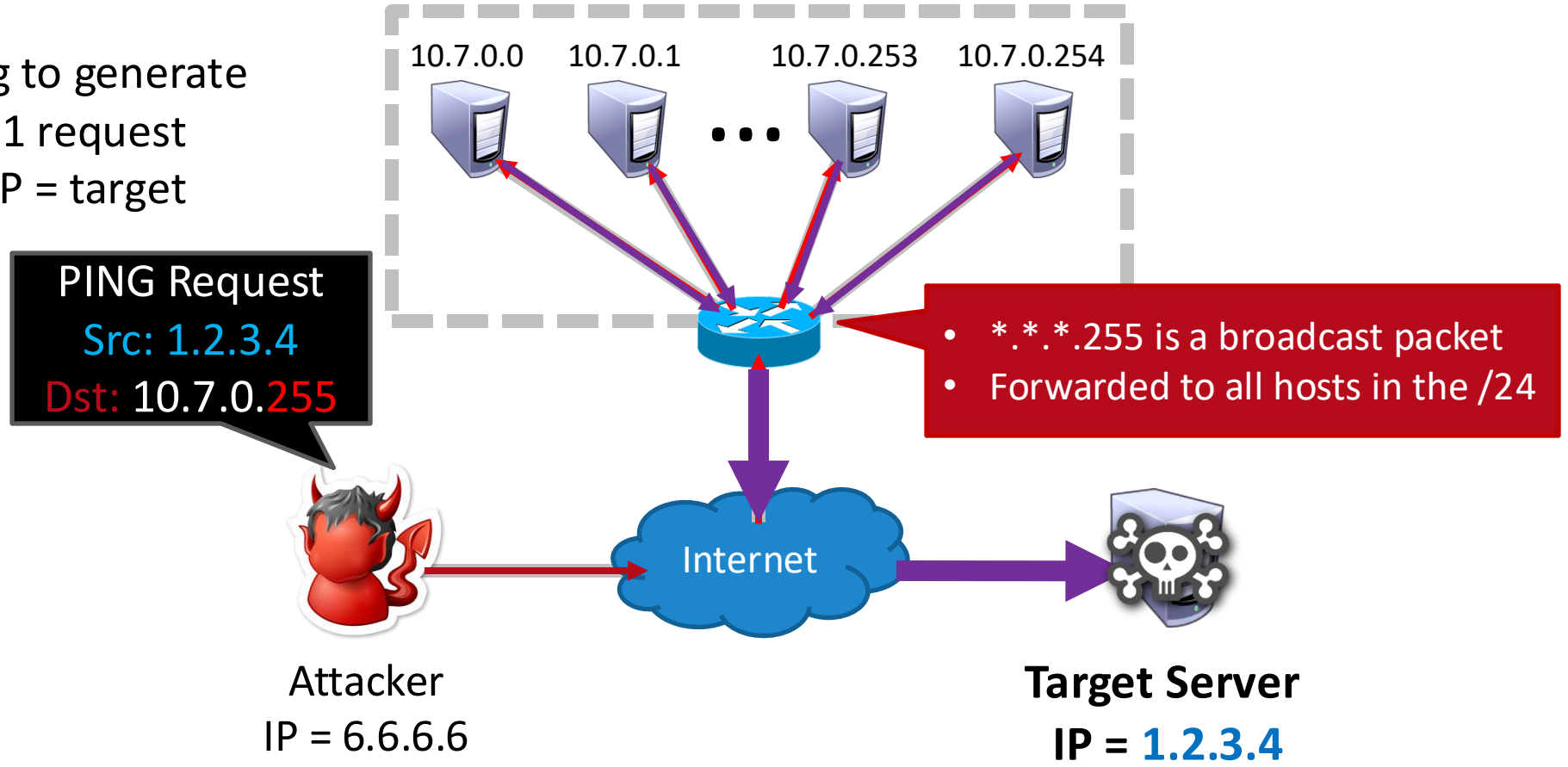
- Essential, low-level network utility (status/liveliness check)
- Sends a “ping” ICMP message to a host on the internet

```
$ ping 66.66.0.255
PING 66.66.0.255 (66.66.0.255) 56(84) bytes of data.
64 bytes from 66.66.0.255: icmp_seq=1 ttl=58 time=41.2 ms
```

- Destination host is supposed to respond with a “pong” indicating that it can receive packets
- By default, ping messages are 56 bytes long (+ some header bytes)

The Smurf Attack: ICMP Flooding

- Abuses broadcasting to generate many responses for 1 request
- Attacker spoofs src IP = target



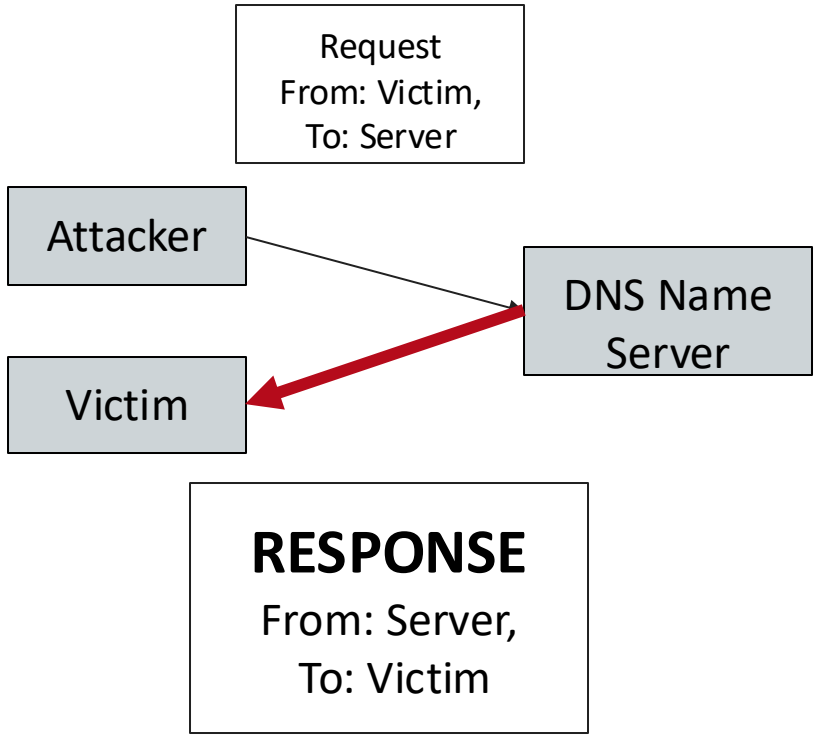
Why Does Smurfing Work?

1. Internet Control Message Protocol (ICMP) does not include authentication
   - Receivers accept messages without verifying the source
   - Enables attackers to spoof the src IP addr of messages
2. Attacker benefits from an amplification factor

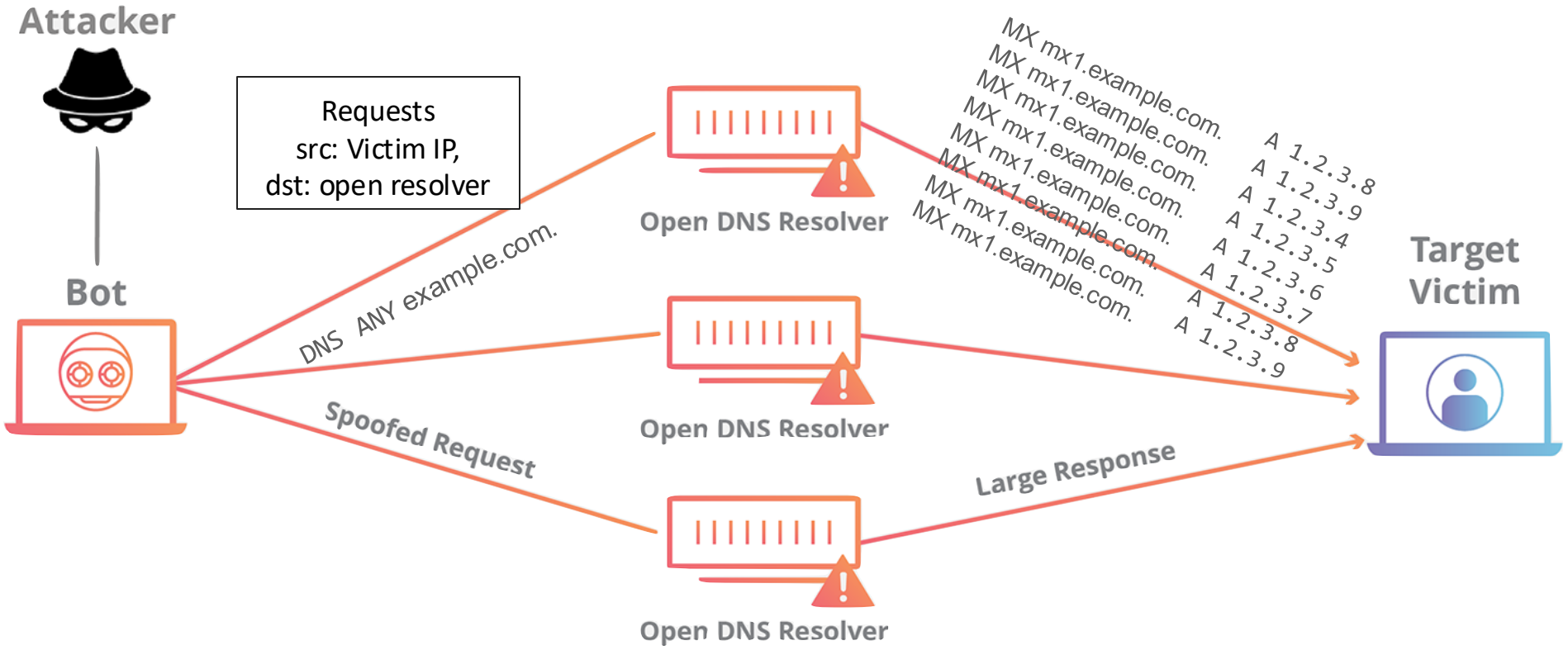
$$amp\ factor = \frac{total\ response\ size}{request\ size}$$

UDP Amplification & Reflection

- Some protocols / commands generate large responses for a single (small) request
  - DNS: Query type "*ANY*" returns all records server has about a domain
  - NTP: MONLIST returns list of last 600 clients who asked for the time recently
- Attack: Spoof requests from target machine's src IP address to other services
  - Typically use UDP-based protocols: Why?



DNS Reflection (+ Amplification) Attack



Spoof DNS requests from victim src IP addr to many **open** DNS resolvers

- Open resolvers accept requests from any client, e.g. 8.8.8.8, 8.8.4.4, 1.1.1.1, 1.0.0.1
- February 2014 – 25 million open DNS resolvers on the internet

Image: Cloudflare

Preventing Spoofing: Ingress & Egress Filtering

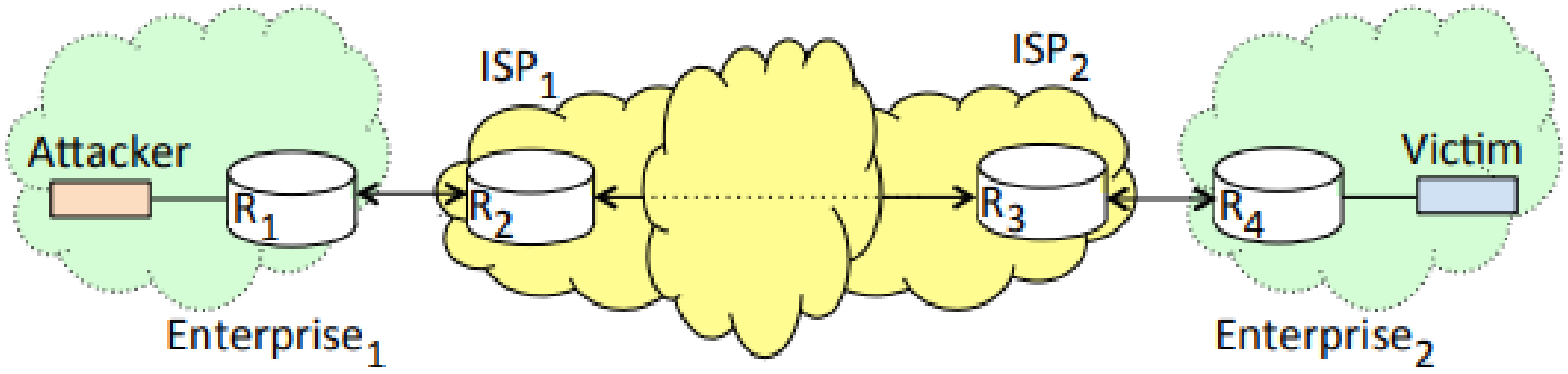
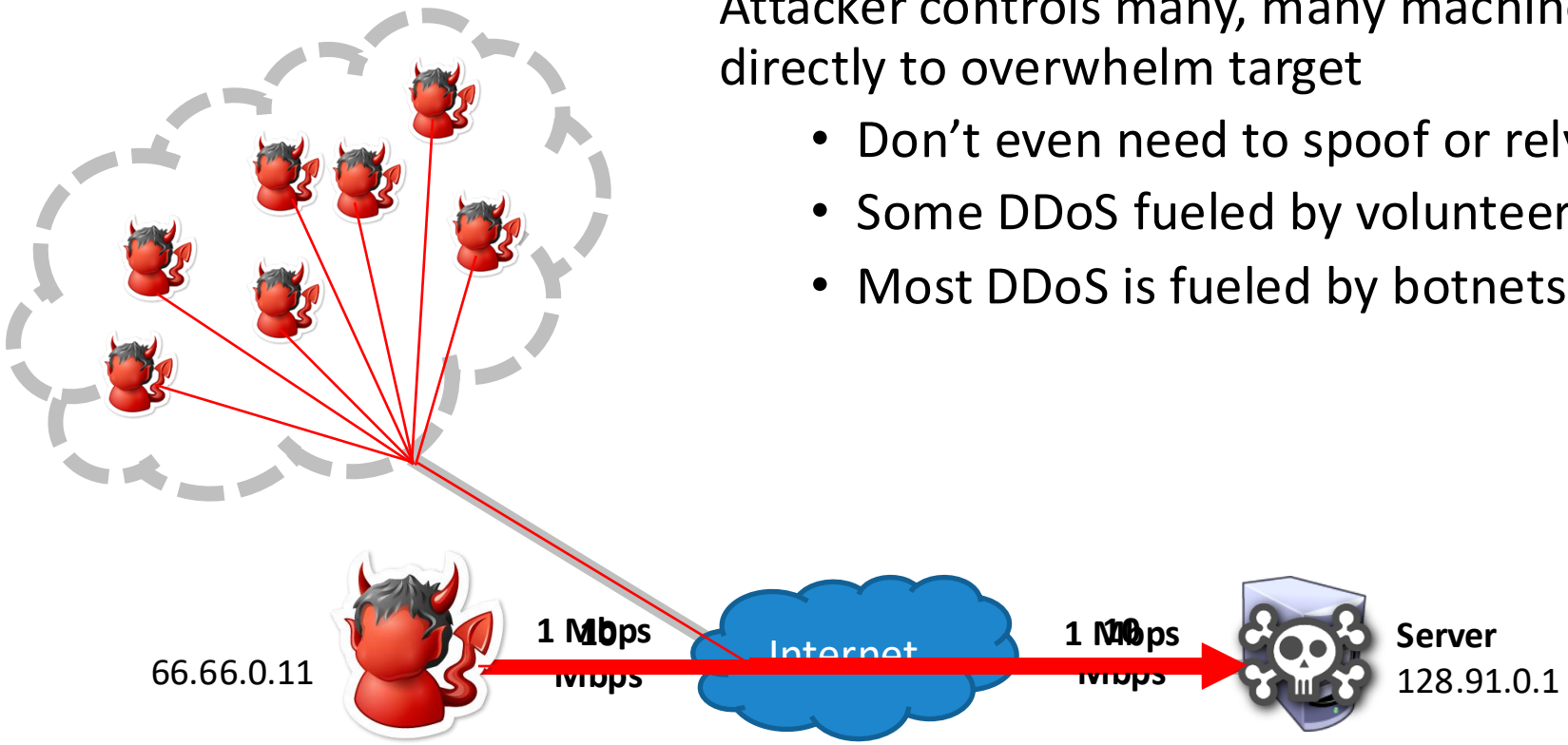


Figure 11.6: Ingress and egress filtering. An attacker may use a spoofed source IP address in traffic sent to a victim. ISP_1 does ingress filtering at R_2 for traffic entering from $Enterprise_1$. $Enterprise_1$ does egress filtering at R_1 for traffic leaving to ISP_1. For firewall rules to implement ingress and egress filtering, see Table 10.1 in Section 10.1.

- Networks know which IP addresses belong to them and
- ISPs/ASNs know which IP addresses they've given to sub-networks

Distributed Denial of Service (DDoS) Attacks



Attacker controls many, many machines and uses them directly to overwhelm target

- Don’t even need to spoof or rely on UDP protocols
- Some DDoS fueled by volunteers (e.g. Anonymous)
- Most DDoS is fueled by botnets (e.g., Mirari)

THE WALL STREET JOURNAL.

October 21, 2016

Cyberattack Knocks Out Access to Websites

Popular sites such as Twitter, Netflix and PayPal were unreachable for part of the day

twitter

amazon web services™

PayPal

NETFLIX

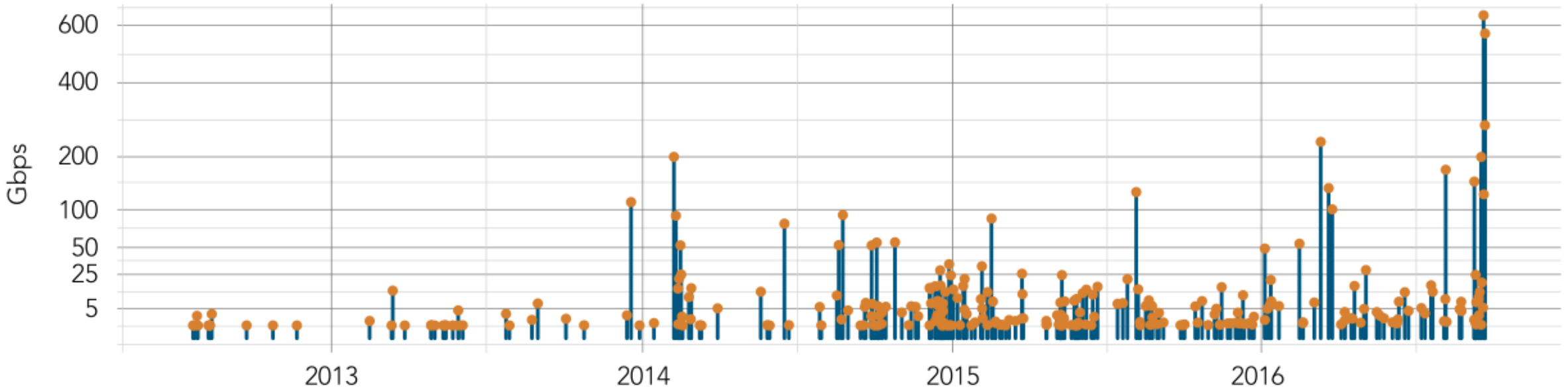
SOUNDCLOUD

Spotify

GitHub

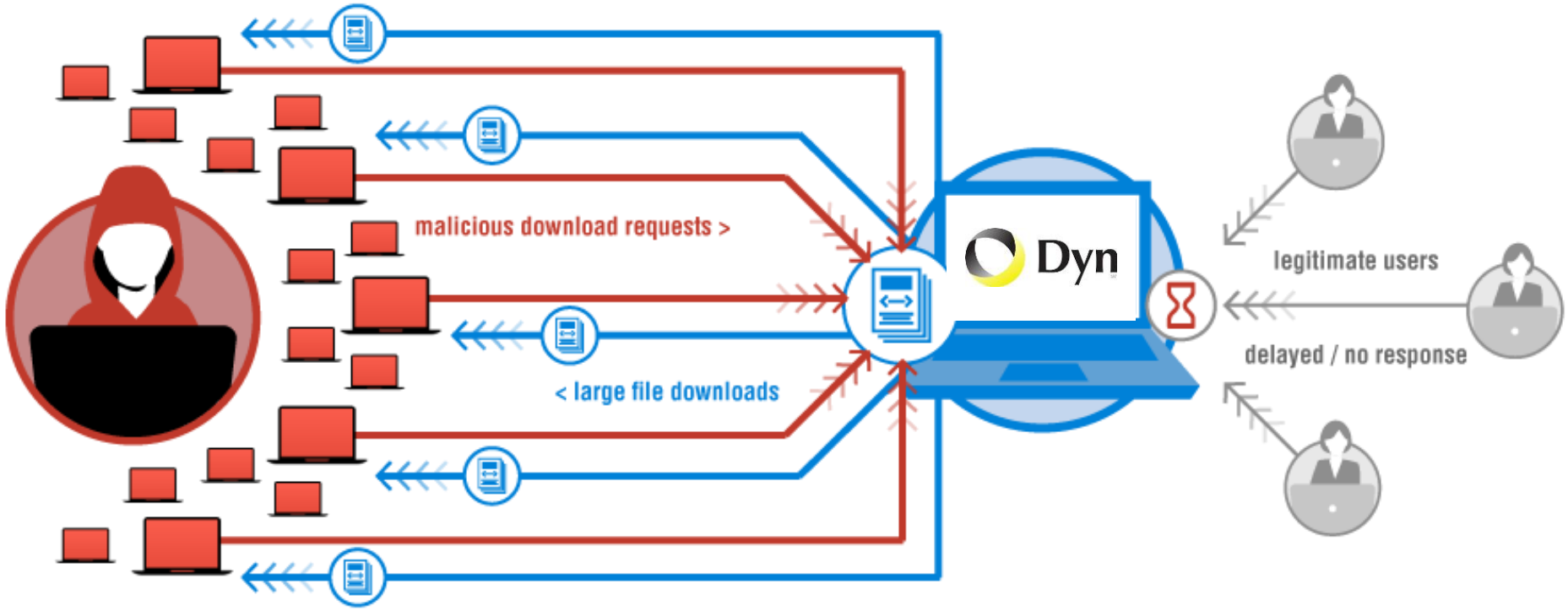
reddit

New York Times



"The magnitude of the attacks seen during the final week were significantly larger than the majority of attacks Akamai sees on a regular basis. […] In fact, while the attack on September 20 was the largest attack ever mitigated by Akamai, the attack on September 22 would have qualified for the record at any other time, peaking at 555 Gbps."

Source: 2017 Akamai State of the Internet



> “We are still working on analyzing the data but the estimate at the time of this report is up to 100,000 malicious endpoints. […] There have been some reports of a magnitude in the 1.2 Tbps range; at this time we are unable to verify that claim.”

Image: Verisign

A Botnet of IoT Devices (Mirai)

≈ ~~200K Hosts~~

200K IoT devices

Not Amplification.

Flood with SYN, ACK, UDP, and GRE packets

Password Guessing

Password	Device Type	Password	Device Type	Password	Device Type
123456	ACTi IP Camera	klv1234	HiSilicon IP Camera	1111	Xerox Printer
anko	ANKO Products DVR	jvbzd	HiSilicon IP Camera	Zte521	ZTE Router
pass	Axis IP Camera	admin	IPX-DDK Network Camera	1234	Unknown
888888	Dahua DVR	system	IQinVision Cameras	12345	Unknown
666666	Dahua DVR	meinsm	Mobotix Network Camera	admin1234	Unknown
vizxv	Dahua IP Camera	54321	Packet8 VOIP Phone	default	Unknown
7ujMko0vizxv	Dahua IP Camera	00000000	Panasonic Printer	fucker	Unknown
7ujMko0admin	Dahua IP Camera	realtek	RealTek Routers	guest	Unknown
666666	Dahua IP Camera	1111111	Samsung IP Camera	password	Unknown
dreambox	Dreambox TV Receiver	xmhdipc	Shenzhen Anran Camera	root	Unknown
juantech	Guangzhou Juan Optical	smcadmin	SMC Routers	service	Unknown
xc3511	H.264 Chinese DVR	ikwb	Toshiba Network Camera	support	Unknown
OxhlwSG8	HiSilicon IP Camera	ubnt	Ubiquiti AirOS Router	tech	Unknown
cat1029	HiSilicon IP Camera	supervisor	VideoIQ	user	Unknown
hi3518	HiSilicon IP Camera	<none>	Vivotek IP Camera	zlxx.	Unknown
klv123	HiSilicon IP Camera				

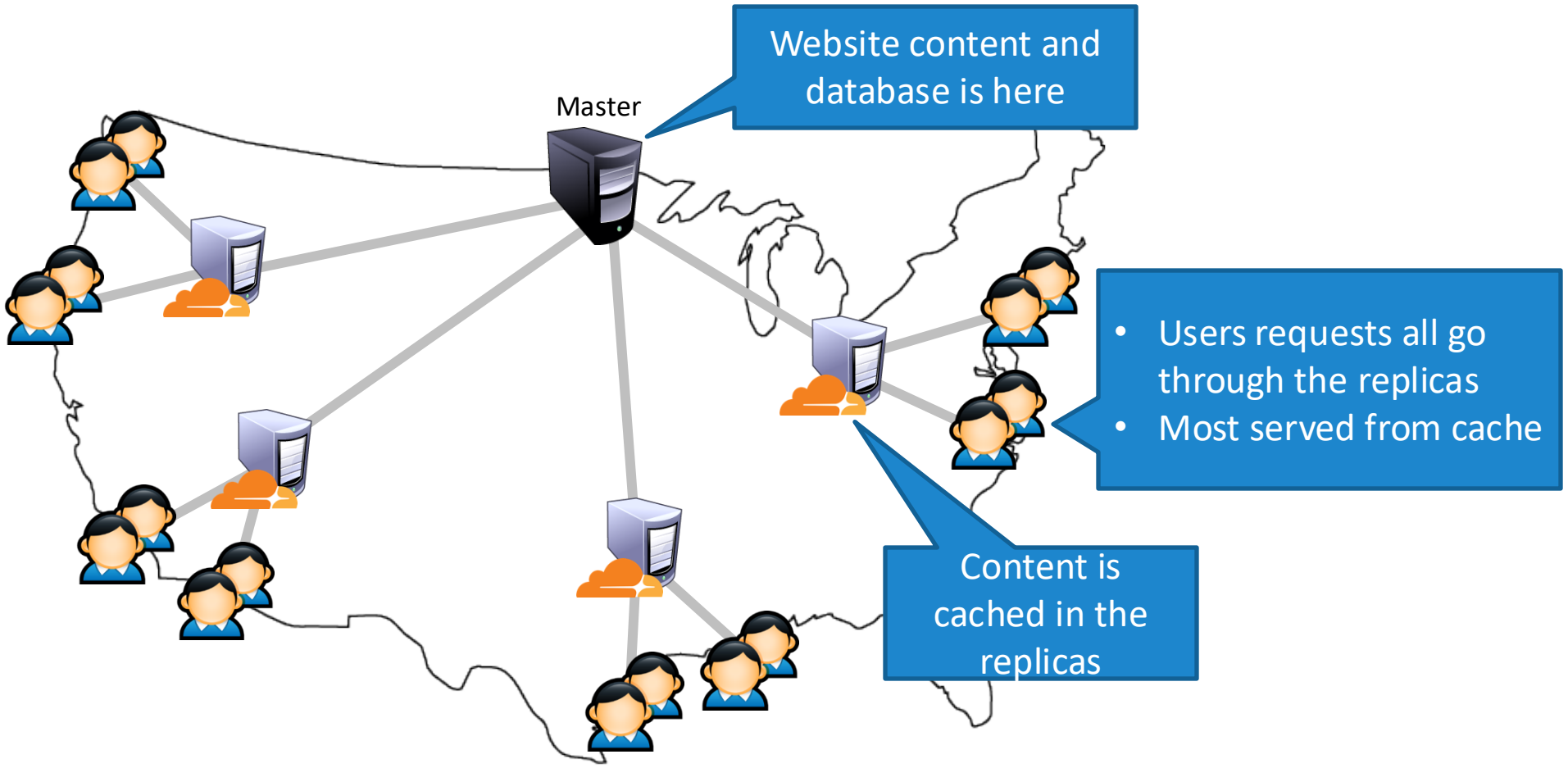
Infamous DDoS Attacks

When	Against Who	Size	How
March 2013	Spamhaus	120 Gbps	Botnet + DNS reflection
February 2014	Cloudflare	400 Gbps	Botnet + NTP reflection
September 2016	Krebs	620 Gbps	Mirai
October 2016	Dyn (major DNS provider)	1.2 Tbps	Mirai
March 2018	Github	1.35 Tbps	Botnet + memcached reflection

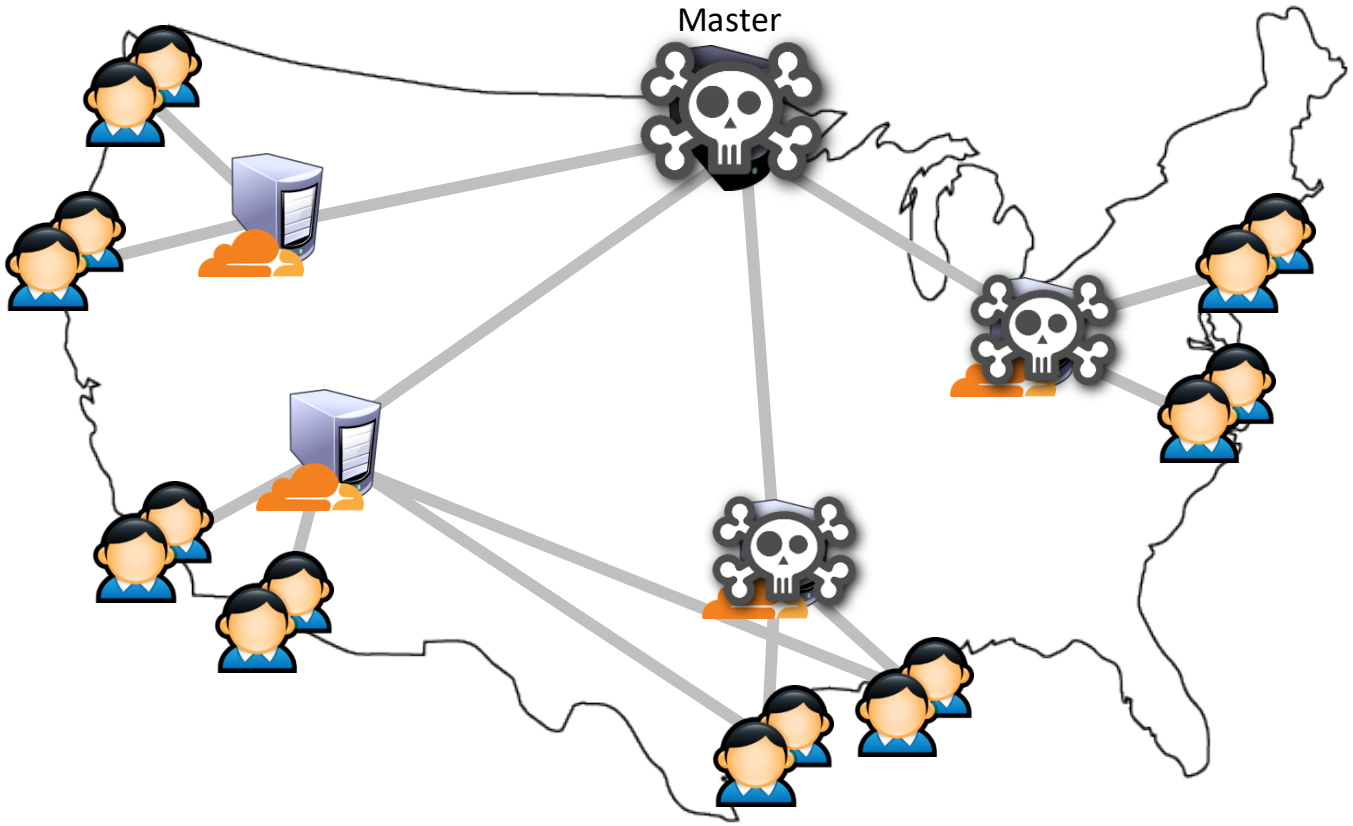
Content Delivery Networks (CDNs)

- CDNs help companies scale-up their websites
  - Cache customer content on many replica servers
  - Users access the website via the replicas
- Examples: Akamai, Cloudflare, Rackspace, Amazon Cloudfront, etc.
- Side-benefit: DDoS protection
  - CDNs have many servers, and a huge amount of bandwidth
  - Difficult to knock all the replicas offline
  - Difficult to saturate all available bandwidth
  - No direct access to the master server
- Cloudflare: 15 Tbps of bandwidth over 149 data centers

Content Delivery Networks (CDNs)



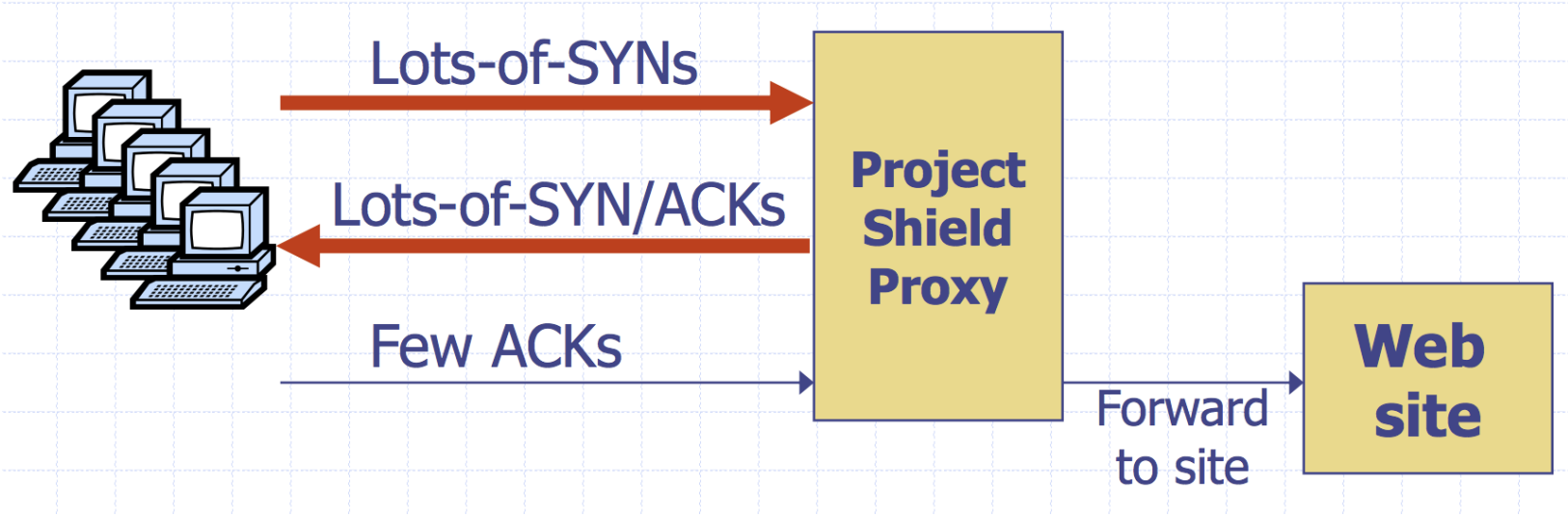
DDoS Defense via CDNs



- What if you DDoS the master replica?
  - Cached copies in the CDN still available
  - Easy to do ingress filtering at the master
- What if you DDoS the replicas?
  - Difficult to kill them all
  - Dynamic DNS can redirect users to live replicas

Google Project Shield

- DDoS Attacks are often used to censor content. In the case of Mirai, Brian Kreb's blog was under attack.
- Google Project shield uses Google bandwidth to shield vulnerable websites (e.g., news, blogs, human rights orgs)



Outline

- Certificates & TLS
- Denial of Service (Attacks on Availability)
- Network Scanning & Firewalls

Network Scanning

- Goals: Identify information about hosts on a network
  - Which IP addresses have assigned machines?
  - What services do those machines offer (SSH, HTTP, DNS, etc.)?
  - Is there a machine with known vulnerabilities at a particular IP address?

- Useful technique for both attackers & defenders

Network Scanning Tools: Traceroute

- ping (ICMP): check if host is responsive
- traceroute — hops between me and host
  - Sends repeated ICMP reqs w/ increasing TTL

```
thor Wed Oct 24(12:51am)[~]:-> traceroute www.slack.com
traceroute to www.slack.com (52.85.115.213), 64 hops max, 52 byte packets
 1  v11router (128.135.11.1)  1.265 ms  0.788 ms  0.778 ms
 2  a06-021-100-to-d19-07-200.p2p.uchicago.net (10.5.1.186)  1.292 ms  0.749 ms  0.833 ms
 3  d19-07-200-to-h01-391-300.p2p.uchicago.net (10.5.1.46)  2.124 ms  2.435 ms  2.072 ms
 4  192.170.192.34 (192.170.192.34)  0.755 ms
    192.170.192.32 (192.170.192.32)  0.810 ms  0.701 ms
 5  192.170.192.36 (192.170.192.36)  0.887 ms  0.918 ms  0.877 ms
 6  r-equinix-isp-ae2-2213.wiscnet.net (216.56.50.45)  1.625 ms  1.803 ms  1.866 ms
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  178.236.3.103 (178.236.3.103)  4.516 ms  4.326 ms  4.320 ms
12  * * *
13  * * *
14  * * *
15  server-52-85-115-213.ind6.r.cloudfront.net (52.85.115.213)  4.554 ms  4.398 ms  4.757 ms
thor Wed Oct 24(12:52am)[~]:->
```

Port Scanning

- What services are running on a server? Nmap

```
linux3 Wed Oct 24(12:54am)[~]:-> nmap www.cs.uchicago.edu

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-24 00:55 CDT
Nmap scan report for www.cs.uchicago.edu (34.203.108.171)
Host is up (0.019s latency).
Other addresses for www.cs.uchicago.edu (not scanned): 54.164.17.80 54.85.61.218
rDNS record for 34.203.108.171: ec2-34-203-108-171.compute-1.amazonaws.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
linux3 Wed Oct 24(12:55am)[~]:->
```

- 5 seconds to scan a single machine!!

SYN Scanning

Send only a SYN : only needs application to run TCP

Responses:

- SYN-ACK — port open
- RST — port closed
- Nothing — filtered (e.g., firewall)

Outline

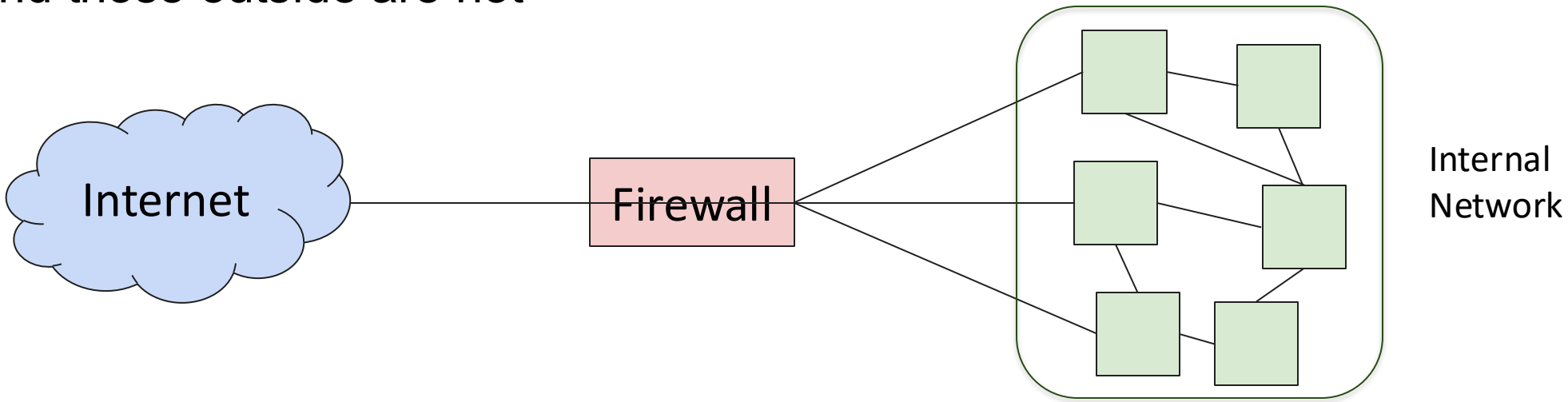
- Certificates & TLS
- Denial of Service (Attacks on Availability)
- Network Scanning & Firewalls

Firewalls

- How do you protect a set of systems against external attack?
  - Example: A company network with many servers and employee computers
- Observation: More network services = more risk
  - Each available service creates more opportunities for vulnerabilities
  - Turning off all network services is often infeasible (printing, SSH, etc.)
- Observation: More networked machines = more risk
  - What if you have to secure hundreds of systems?
  - What if the systems have different hardware, operating systems, and users?
  - What if there are some systems in the network that you aren't aware of?
- Instead of securing individual machines, we want to secure the entire network!

Firewalls and Security Policies

- Idea: Create single point of access in & out of network (chokepoint), with a monitor
  - “Ensure complete mediation”
  - Any traffic that could affect vulnerable systems must pass through the firewall
- Network access is controlled by a **policy** (based on threat model)
  - Defines what traffic is allowed to exit the network (**outbound policy**)
  - Defines what traffic is allowed to enter the network (**inbound policy**)
  - Traditional threat model: assume machines “inside” the network are trusted, and those outside are not



Firewalls and Security Policies

- What's the policy of a standard home network?
  - Outbound policy: Allow outbound traffic
    - Users inside the network can connect to any service
  - Inbound policy: Only some traffic is able to enter the network
    - Allow inbound traffic in response an outbound connection
    - Allow inbound traffic to certain, trusted services (e.g. SSH)
    - Deny all other inbound traffic