

Practical Solutions for Amplification Attacks

Damian Menscher, Google



\$ whoami

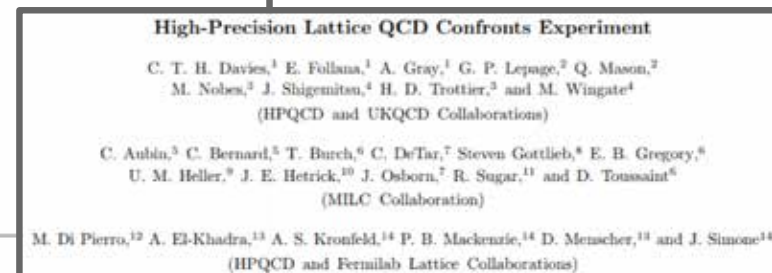
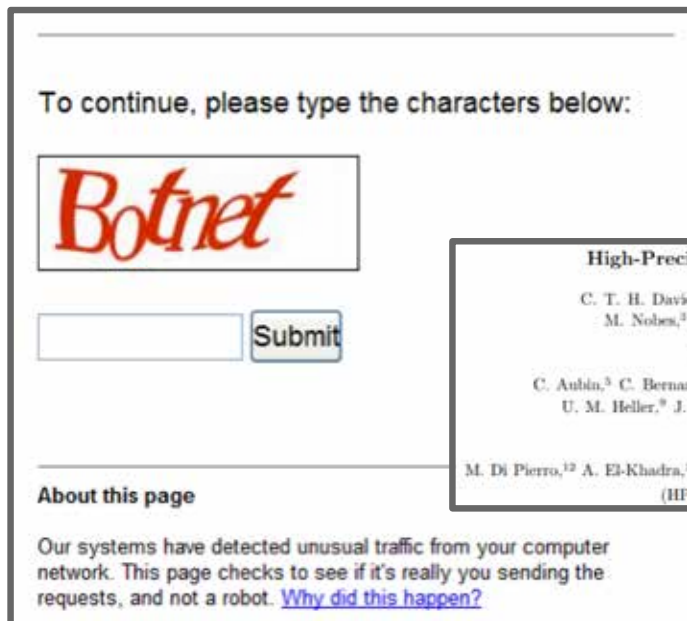
Security Reliability Engineer

DDoS focus for 10+ years

- author of that pesky captcha page

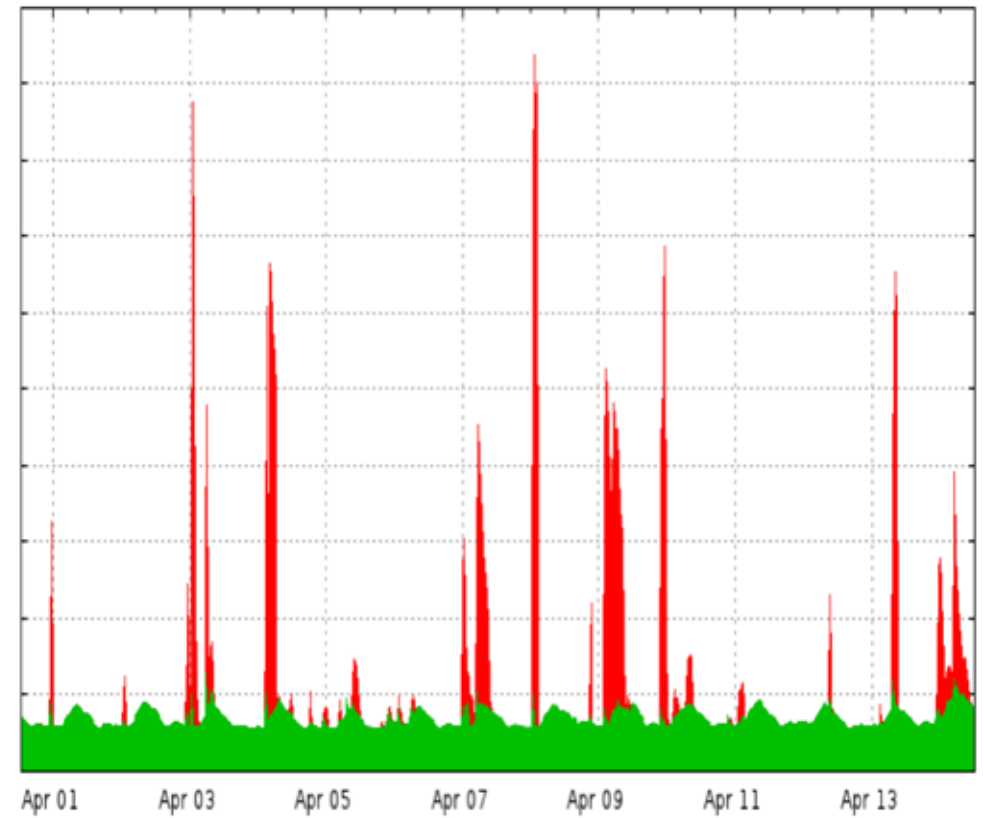
Scientific background

NOT a network engineer!



Agenda

1. Review of DDoS attacks
2. Failed approaches
3. Designing a solution



The Growing DDoS Threat



Biggest DDoS attack in history slows Internet, breaks record at 300 Gbps

GitHub hit with the largest DDoS attack ever seen

DDoS attackers have found a new way of magnifying their attacks, with experts warning that bigger attacks are likely.

Sample headlines

#	Method Name	Method Type	Target Type	Target Syntax
1	GET-HTTP	Layer 7	Websites, WebServers, etc .	URL: http://target.com
2	HEAD-HTTP	Layer 7	Websites, WebServers, etc .	URL: http://target.com
3	POST-HTTP	Layer 7	Websites, WebServers, etc .	URL: http://target.com
4	JSBYPASS-HTTP	Layer 7	Websites, WebServers, etc .	URL: http://target.com
5	JOOMLA	Layer 7	Websites, WebServers, etc .	URL: http://target.com
6	SNMP	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
7	SSDP	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
8	DNS	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
9	CHARGEN	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
10	NTP	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
11	TS3	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
12	SSYN	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
13	DOMINATE	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
14	ACK	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
15	NGSSYN	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
16	OVX	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
17	TCPACK	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
18	TCPSYN	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
19	TCPRST	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
20	TCPURG	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
21	TCPPUSH	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
22	TCPECE	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
23	TCPCWR	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
24	ICMP	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
25	MUDP	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
26	VSE	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337
27	ATCP	Layer 4	Home / Peoples, Servers, Custom IPs, etc .	IP: 1337

**PRICING PACKAGES** / perfect price

MONTHLY BRONZE

19.99\$

XyZ Public Network

150-200Gbps Network Capacity

26 Attack Methods

1800(s) Stress Time

1 Months Membership

1 Parallel attacks

REGISTER

MONTHLY SILVER

24.99\$

XyZ Public Network

150-200Gbps Network Capacity

26 Attack Methods

2400(s) Stress Time

1 Months Membership

1 Parallel attacks

REGISTER

MONTHLY DIAMOND

29.99\$

XyZ Public Network

150-200Gbps Network Capacity

26 Attack Methods

3600(s) Stress Time

1 Months Membership

1 Parallel attacks

REGISTER

Example of a booter / stresser service

Bypassing Resource Constraints

Asymmetric cost

Use others' compute

Use others' bandwidth



DNS

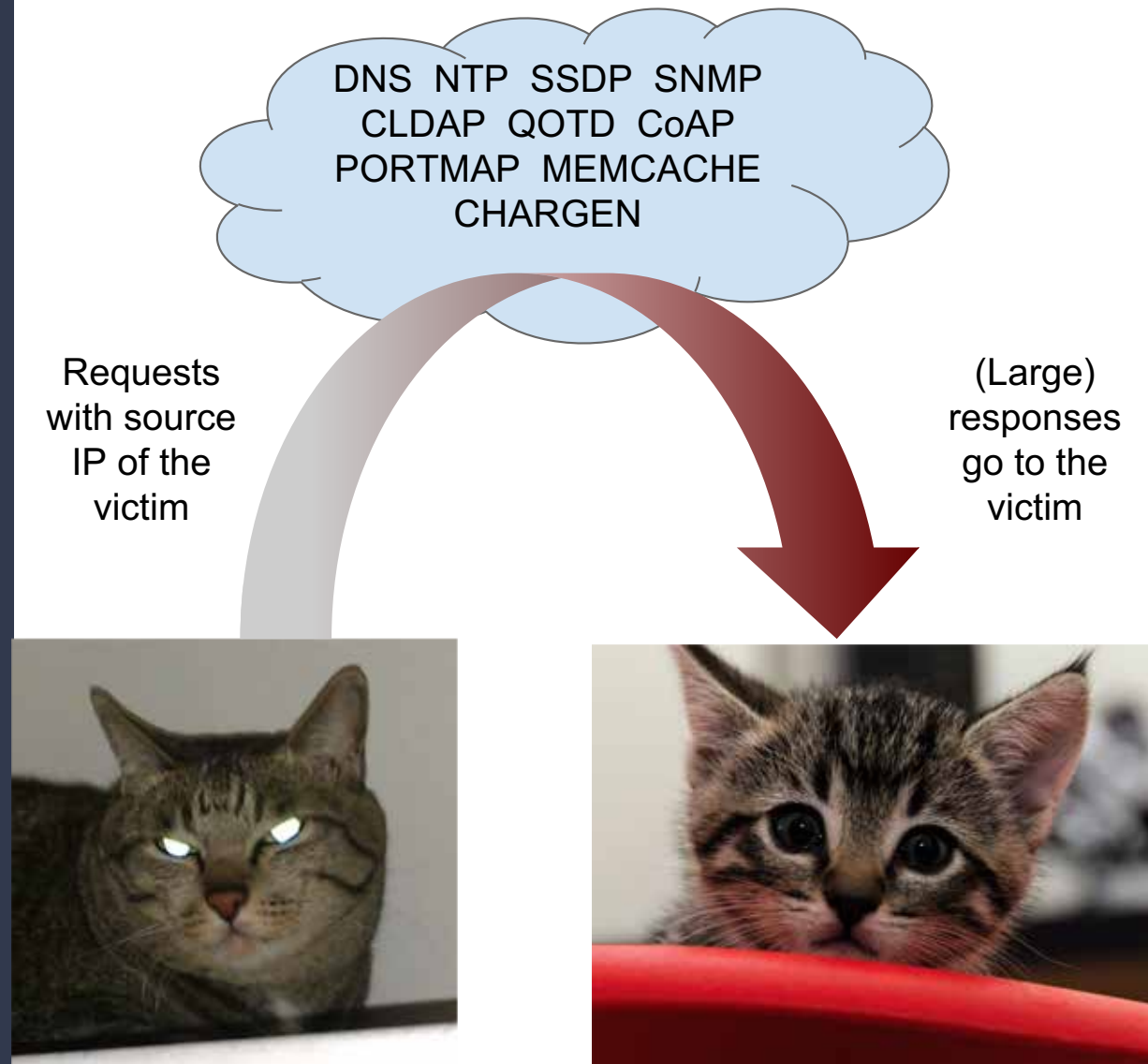
? cpsec.gov./ANY

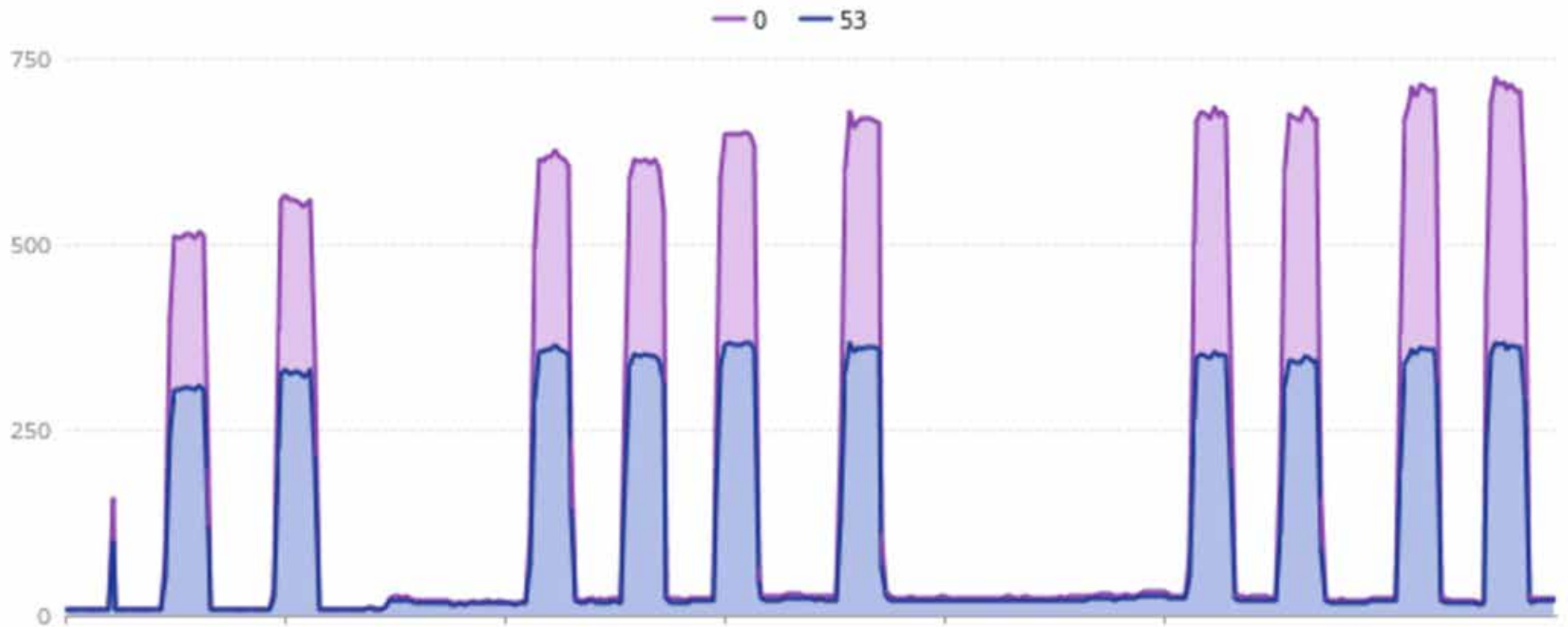
cpsec.gov.	15880	IN	MX	U
hormel.cpsec.gov.				
cpsec.gov.	15880	IN	RRSIG	MX 8 2 21600
20190515095424 20190512085424 35763 cpsec.gov. Pw8uxFtJ6bFXqCKhh+C4EQvzMoAfY6HydLyy9Oog/nFpfvopqGqfGUwV				
olQDf0lxz6bPhxpZtOafCZWQIDMUGk/CAXac82Ol2sV6PTydL20jA7lg YgUy8/06U8LmaU7M/E2kRt5Va+qdgXJ84sSENV8Ji4OkOc44QXmQ7ujv Ekw=				
cpsec.gov.	1480	IN	DNSKEY	256 3 8
AwEAApTN+Q/AWyqJuGr9cNbFLIVB2NLeIbMib3HbOdZBnJr/2GiZPoX OUbRpLd7xvltj9gsOjY7SuqcX3KF2YUq2UuPsEVUREi0BtZmhd5nRbK				
KCHzsPgYjBckZyhy2j4BCHN9xiWT5isx0S322HXlXhOVTm/GWat59BW7 ey5IkKbX				
cpsec.gov.	1480	IN	DNSKEY	256 3 8
AwEAAeFVM04Xf7Y2etYKzgWuaOrwLgsndqpac3qo2UMclH3m87mCvpPw lHajpTEA6CEiGOq2thrxqDgpZqa81RgtXU2NAXaAX+cuCTDrDZrJ+AU5				
ID1vpVwDYKIBy59M+Q0B7KgWLNEX3uSrHXo56wAUuFDloGosxobz2BGC NX1VbKDL				
cpsec.gov.	1480	IN	DNSKEY	257 3 8
AwEAAARzvvqE80pdmC3yXSdhUluHHdLBjpaGOB4ZGQ6xVH+S5x7R+QHUp QQ13hLIWjj1PFb1lahZH4jDiPV3KJfJSi/3FZE33wUg+kF/hdR5UqHel				
IRgvucNnJnSpehc7CRNvBNEraSqpvmlHRp3qSJ85plGpqexUPtee2BbN 7mFgvtPXOM9lQCxA5cLA8xFQdjSe7+WmeM3uEHcybTNGyJFV9IEeliKs				
rx5TTXtCacRZIXG0ib+hLMUFzItHw4YyRbmso00w0eNRhOZOG80tG+Zq QXe+zKhJn7VZJ3DosJ4CY5iPuebZPyPe7AHjpZkrJS7co8+zE5AcohzV				
J4RiFxr85rU=				
cpsec.gov.	1480	IN	RRSIG	DNSKEY 8 2 7200
20190515095424 20190512085424 40399 cpsec.gov. oTRqoVkvZDAQV4obh9Fa+Qm1BW0sJpr16zwpHDlmdlwOyTNJtnwcv/nXl				
6Zlr2SUPf0bsB6Z+65z3x2bJqcX1NArckdLWTwEjAWJ1W7dPcDPePZ51 TPGZ+bi13E3hrsmZhe9fUSg77jLOV2qERx4kPSSvyKpNtSi1R5K/OMZG				
gCOB8guNjRT7D3jNUPyy1R2lBzMmq1fEdbrikSJ5gpaLYlzfMoM0yMz 4xdU8rLDGOrfE/ASGH3yB26xLgmtNdhLVsK176dOso6bJGUyDB5mVjby				
eQ46c5Zswya+CWkx46SsrBXf9f5VNx652IGSoJGss7dUbk5ulXX74EW3 +Metwg==				
cpsec.gov.	15880	IN	NS	a1-85.akam.net.
cpsec.gov.	15880	IN	NS	a13-64.akam.net.
cpsec.gov.	15880	IN	NS	a3-67.akam.net.
cpsec.gov.	15880	IN	NS	a20-65.akam.net.
cpsec.gov.	15880	IN	NS	a4-64.akam.net.
cpsec.gov.	15880	IN	NS	a28-66.akam.net.
cpsec.gov.	15880	IN	RRSIG	NS 8 2 21600
20190515095424 20190512085424 35763 cpsec.gov. i8UkkKujjJiySKg+j59Mu9vl3qujlzHpAUzdRdPhSfZ1vpmWqv+F/7Yy				
NPLDDrtajHVMKpjEBcVw4rLTa/1/otM6OjPXY6n5nP9CbnFXftrplW1K 8rJZ9bbM044HeOTU0+OamfMKQwZ4Es4FLTGPliHCl9lIOnTdOzgDdSk6 oyM=				
cpsec.gov.	15880	IN	TXT	
"da5eeb81385047fcb72043e2fcb34ac8"				
cpsec.gov.	15880	IN	TXT	"v=spf1
ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.25 ip4:63.74.109.20 mx a:list.cpsec.gov -all"				
cpsec.gov.	15880	IN	TXT	
"2y97jj9vwr9ctt9v1yqdy88nyh39vmrk"				
cpsec.gov.	15880	IN	TXT	
"MS=ms34764123"				
cpsec.gov.	15880	IN	RRSIG	TXT 8 2 21600
20190515095424 20190512085424 35763 cpsec.gov. xQsbl3stF/Wk8TBo3zXvbJ0OfvkEWWSCIYYgonTb0gxEYEzmqV34ioBV				
w44Xw9tCrQA2/MUnfTUKyUsVfRyU8ZqEu6BN/W8L1miX67cCiO7XO+3c YL/9eWnhKMwFQXTPExpPpnQStGgBQVlXheDFtF0Hxsc9T8Bw8F7XLDI YFA=				
cpsec.gov.	15880	IN	NSEC3PARAM 1 0 1 A14CB8E2EAF3B5A2	
cpsec.gov.	15880	IN	RRSIG	NSEC3PARAM 8 2
21600 20190515095424 20190512085424 35763 cpsec.gov. Q7TA+3SJw/1lGHH/cuRB7sUMwQ6LjKcZ7TtLKdsBN4sCskV59v3bT3yda				
evn6d3izOdTdoSE4EX8NSqtq8PrbVmV/OzqeGS4Bu9zhqnnsuVeBld7t mtmPBw1H0cgonkRz1quQmKzyMksmclDJ1kvHe4p8qV5rs/diYZ66Q0Va otQ=				
cpsec.gov.	15880	IN	SOA	a1-85.akam.net.
hostmaster.akamai.net. 1554486850 21600 3600 1728000 21600				
cpsec.gov.	15880	IN	RRSIG	SOA 8 2 21600
20190515095424 20190512085424 35763 cpsec.gov. eSJ0Dt/U4lpuNhIV7bXyWw9ZUrLA9pPfBaIF2tdw01pKycbY0glagHny				
qyC+uKCKmV1M2ahQGUiqfH56TpQ72lIKbtowAl2aEGloSPlwrPzFiA 0LGIRWHh7GbIaGwWfWEYw8O8cWok12UMsuDZYTkwQUKfIbGY9VPfTqA asM=				
cpsec.gov.	15880	IN	A	63.74.109.48
cpsec.gov.	15880	IN	RRSIG	A 8 2 21600
20190515095424 20190512085424 35763 cpsec.gov. owQZV2pTlCpYQg7VjoKlwHYWVR9KvXRl70lBk8E/eBFpY2MI0mKfSJsA				
Y08kj54NZYOabaz6P/zRWW/nXxRqU/cw43DwlWwVvtlFe3DPk6Uw1lx SXiG5r2R9J9ll/zYrw7NDIT/N9KaVVYkHgHhgOQRWwaXIWtfW84gqX2 j6w=				
cpsec.gov.	15880	IN	AAAA	2600:803:240::2
cpsec.gov.	15880	IN	RRSIG	AAAA 8 2 21600

Reflection / Amplification Attacks

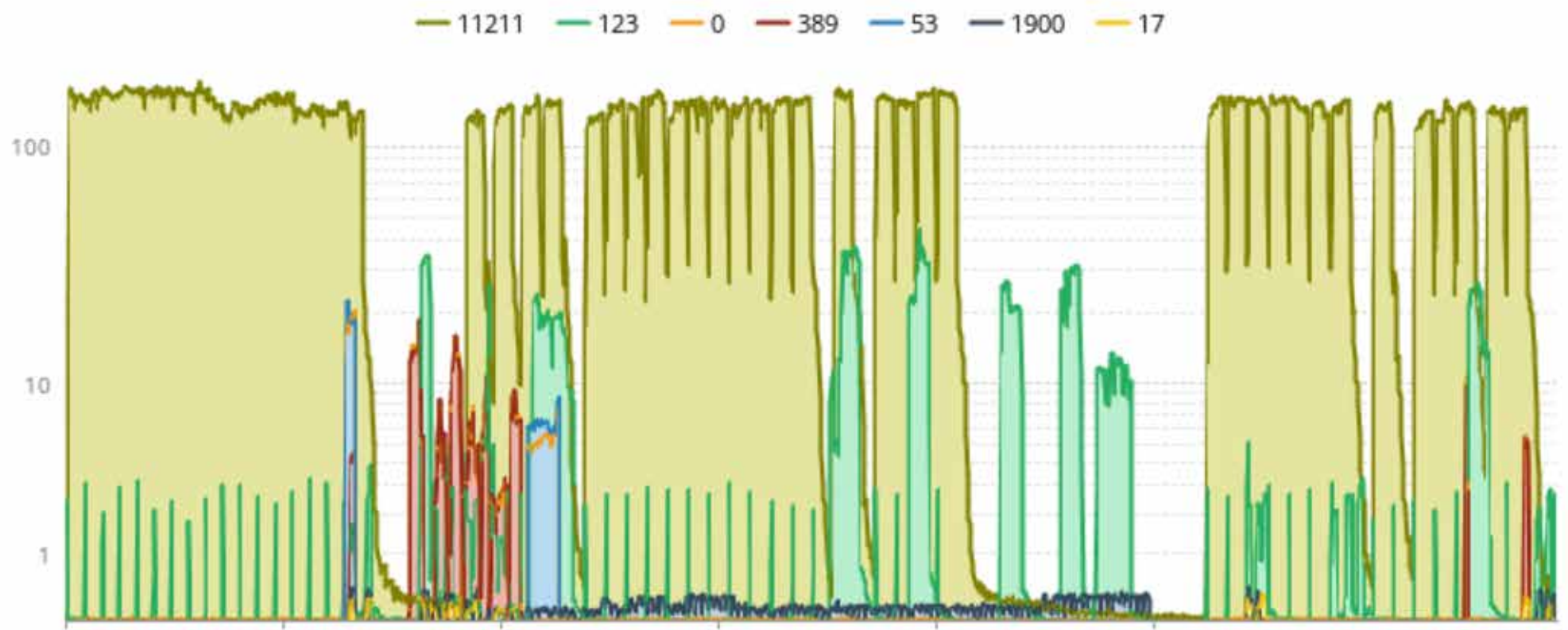
Amplification of

- bandwidth
- packets





Victim's view of a series of DNS amplification attacks in August 2017



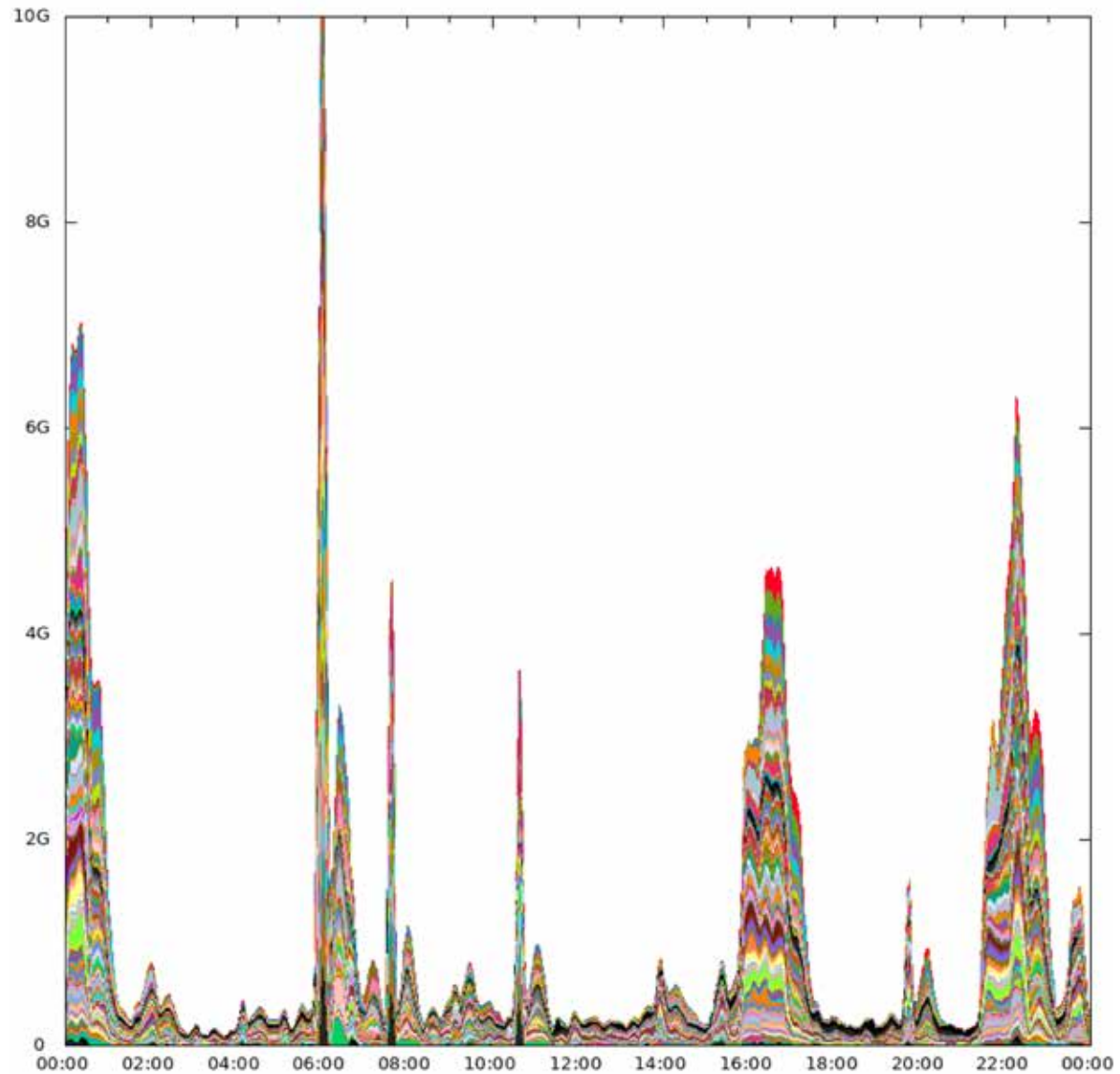
Victim's view of a blend of amplification attacks in April 2019

Defense

Fat pipes

Global peering

Router ACLs to *throttle large* UDP
packets sourced from *known*
amplification ports

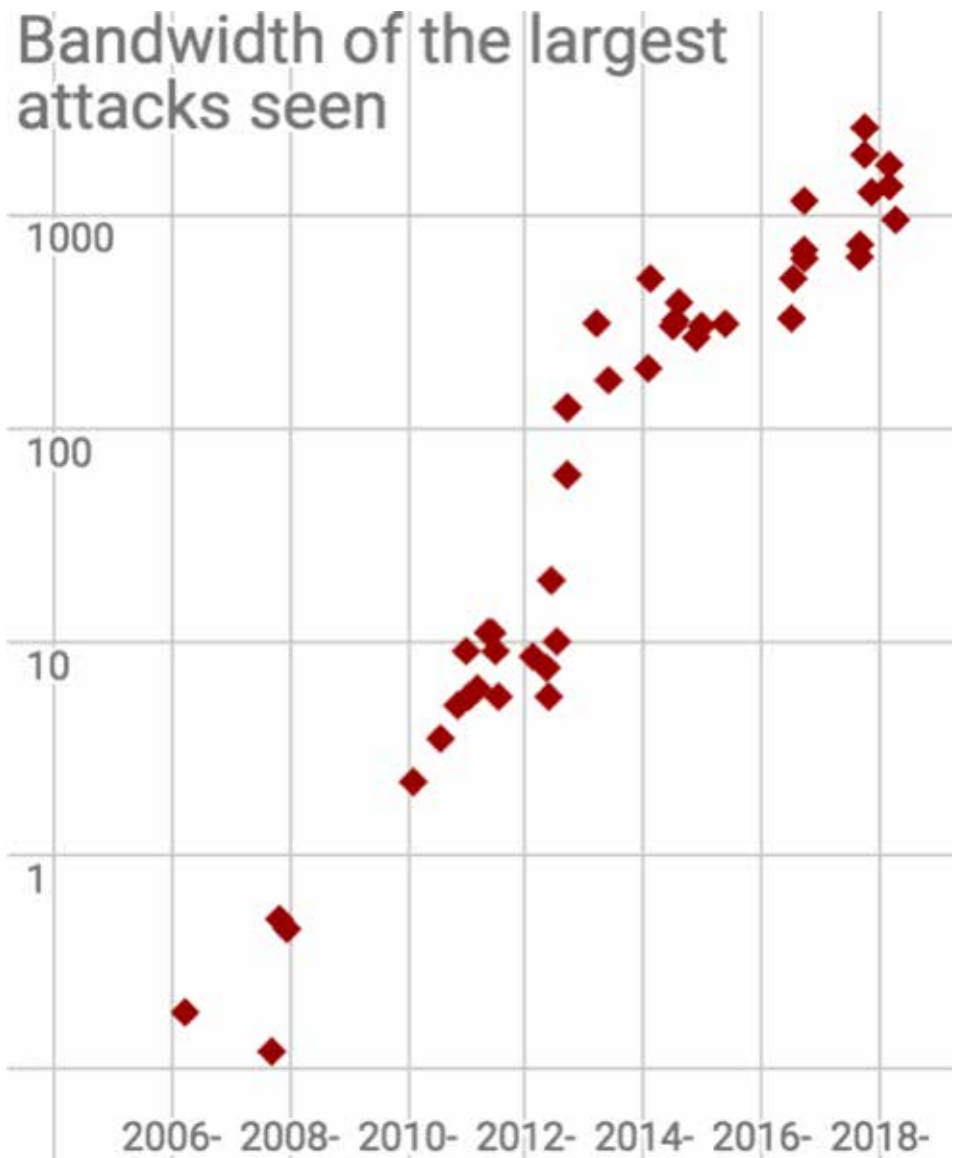


Exponential Growth

Moore's Law

More devices

→ 5 Tbps attacks this year



Failed Approaches



Block / Throttle UDP

Harms existing protocols

What about DNS, QUIC, games?

TCP Amplification??



© Rudy and Peter Skitterians

Clean up amplifiers

Requires too many participants

99.9% success rate → Failure

- 16M DNS
- 4M NTP
- 8M SNMP
- 80M SSDP



© 2011 Damian Menscher
Used with permission

BCP 38

No incentive

Helps others, not self → priority?

Network Working Group
Request for Comments: 2827
Obsoletes: [2267](#)
BCP: 38
Category: Best Current Practice

P. Ferguson
Cisco Systems, Inc.
D. Senie
Amaranth Networks Inc.
May 2000

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

Abstract

Recent occurrences of various Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point.

Table of Contents

1.	Introduction	2
2.	Background	3
3.	Restricting forged traffic	5
4.	Further capabilities for networking equipment.	6
5.	Liabilities.	6
6.	Summary.	7
7.	Security Considerations.	8
8.	Acknowledgments	8
9.	References	8
10.	Authors' Addresses	9
11.	Full Copyright Statement	10

Solution by Design



$$P_{\text{Success}} = \frac{\text{Incentive}}{\text{Participants}}$$

Identification of Problem ASNs



Bait Servers

Attacker requires thousands of amplification servers

Some are on your network



Router Counters

Simple real-time monitoring

Look for UDP to known amp ports

Easier as you get closer to source

Consider repeating for SYN packets to catch spoofed synfloods

```
term potential_udp_amp {  
  from {  
    protocol udp;  
    destination-port [ 17  
                      19  
                      53  
                      69  
                      111  
                      123  
                      137-139  
                      161  
                      389  
                      1900  
                      3702  
                      11211  
                    ]  
  } then {  
    count potential_udp_amp;  
  }  
}
```

Netflow / Sflow

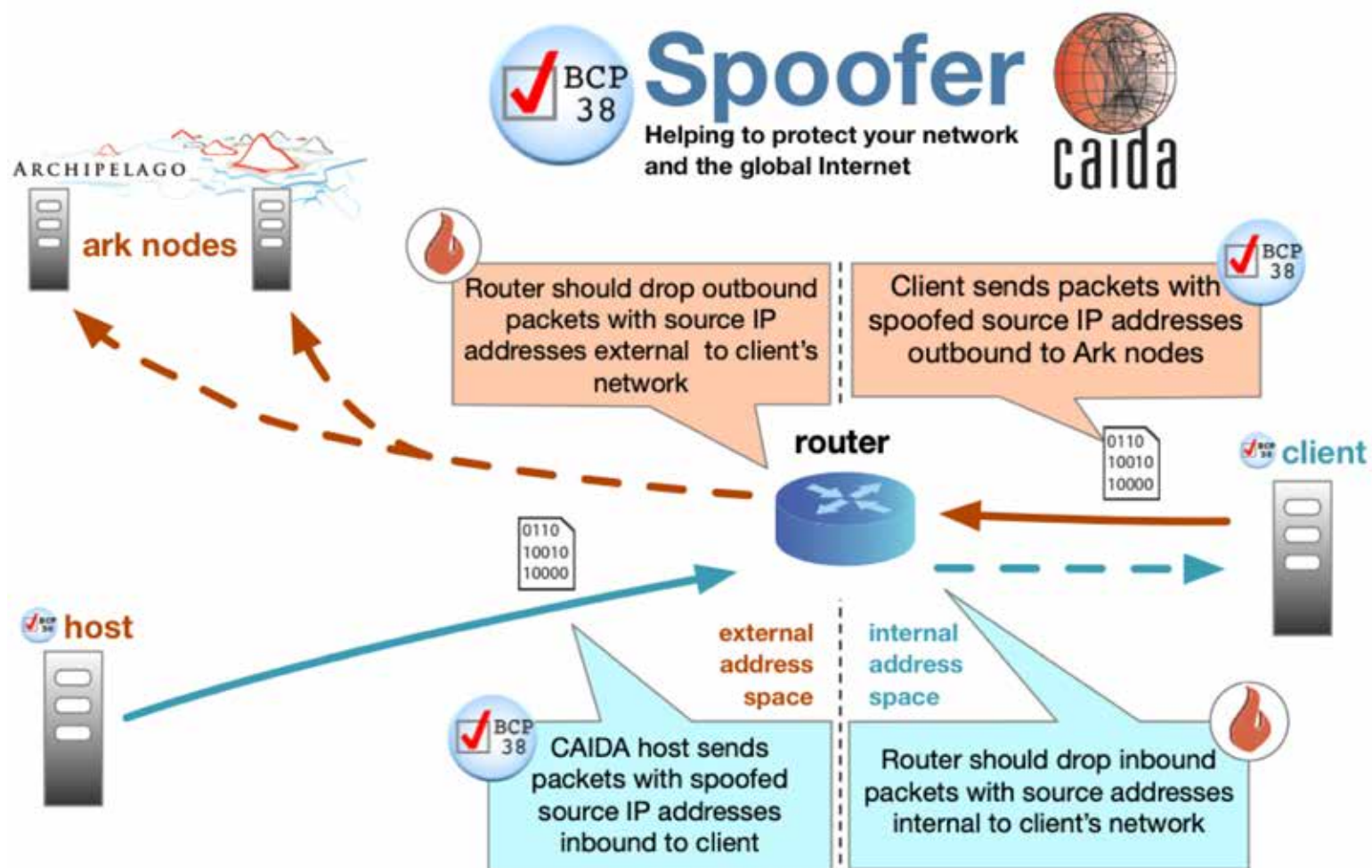
Look for lots of ASNs ingressing a single link

Common concerns

- Size: 1:64k sampling rate
- Privacy: 2 week retention
- Analysis: SQL database

```
dremel> select count(distinct source_ASN),  
               iface from netflow;
```

ASNs	metro	Link Description
44235	ams	Asteroid
32423	lga	NYIIX
16585	lax	AS 3491
15054	fra	InterLan
12814	mil	AS 3257
8730	fra	DE-CIX
8654	lis	GIGAPIX
8269	hkg	AS 4134
7032	maa	AS 55410
7026	lax	AS 3356
6204	ord	AS 6453
5905	svo	AS 12389
5828	mil	AS 6453
5828	svo	AS 12389
5739	lax	AS 3356
5693	svo	AS 12389
5336	ord	AS 6453
5036	gru	PTT.BR
4915	mct	AS 8529
4557	hkg	AS 4134



AMS-IX	EXTREME IX DELHI	SWISSIX
AMS-IX HONG KONG	FRANCEIX	TIE-ATLANTA
ANY2	Giganet	TORIX RS2
BBIX SINGAPORE	HKIX	UA-IX
BIX-BG	HORYZONT	W-IX
Dataline-IX	InterLan	
DE-CIX	IXPN	
DECIX	JPNAP TOKYO 1	
DE-CIX Hamburg	LONAP	
ECIX-Hamburg	MEGAPORT LOS ANGELES	
EQUINIX	MEGAPORT SINGAPORE	
Equinix Ashburn	MIX	
EQUINIX DALLAS	MSK-IX	
EQUINIX HONG KONG	MUMBAI-IX	
EQUINIX LOS ANGELES	PEERING.CZ-ROUTE-SERVERS	
EQUINIX PARIS	PTT.BR	
EQUINIX SAN JOSE	RoNIX	
EQUINIX SINGAPORE	SGIX	
EQUINIX SYDNEY	SIX	
Equinix Zurich	SPB-IX	

ASNs:

209 701 1239 1273 1299 2711 2914 3255
 3257 3267 3320 3356 3491 3741 3786 4134
 4230 4657 4755 4767 4766 4788 4826 4837
 5391 5650 6128 6453 6461 6762 7385 7418
 7497 7552 7922 8100 8151 8251 8473 8595
 8717 8881 8928 8966 9050 9121 9198 9299
 9304 9318 9381 9416 9498 9658 9829 10026
 10429 11014 12389 12552 12578 12670
 12714 12876 12956 13489 14259 16637
 16735 17451 17547 17557 17639 17917
 17922 18101 18207 18229 18403 18734
 18747 21859 23520 23930 24203 24961
 26613 27552 29049 29091 31133 33480
 33576 34772 34867 36351 36884 36944
 38193 40676 41798 44217 45194 45769
 45899 45903 52320 55352 55410 55818
 58453 58587 58601 58717 60294 132602
 132876 133840 134009 135834

Peers sending spoofed traffic to Google in a botnet attack on 2018-05-30

(Un)cooperative Remediation of Problem ASNs

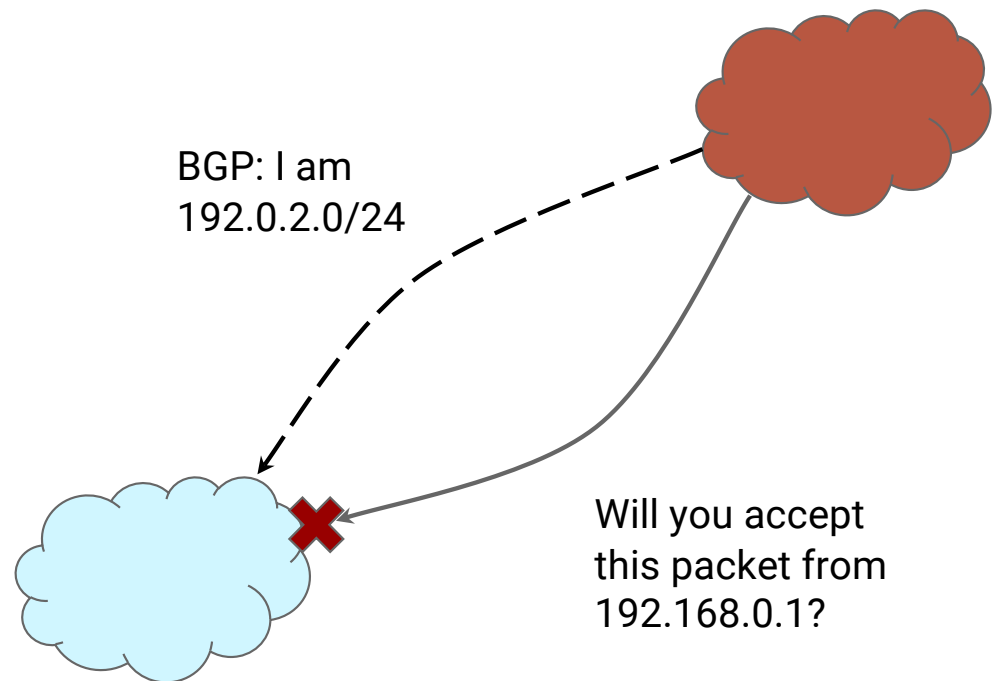


uRPF

Loose or strict?

Asymmetric routing?

Twice the route lookups??



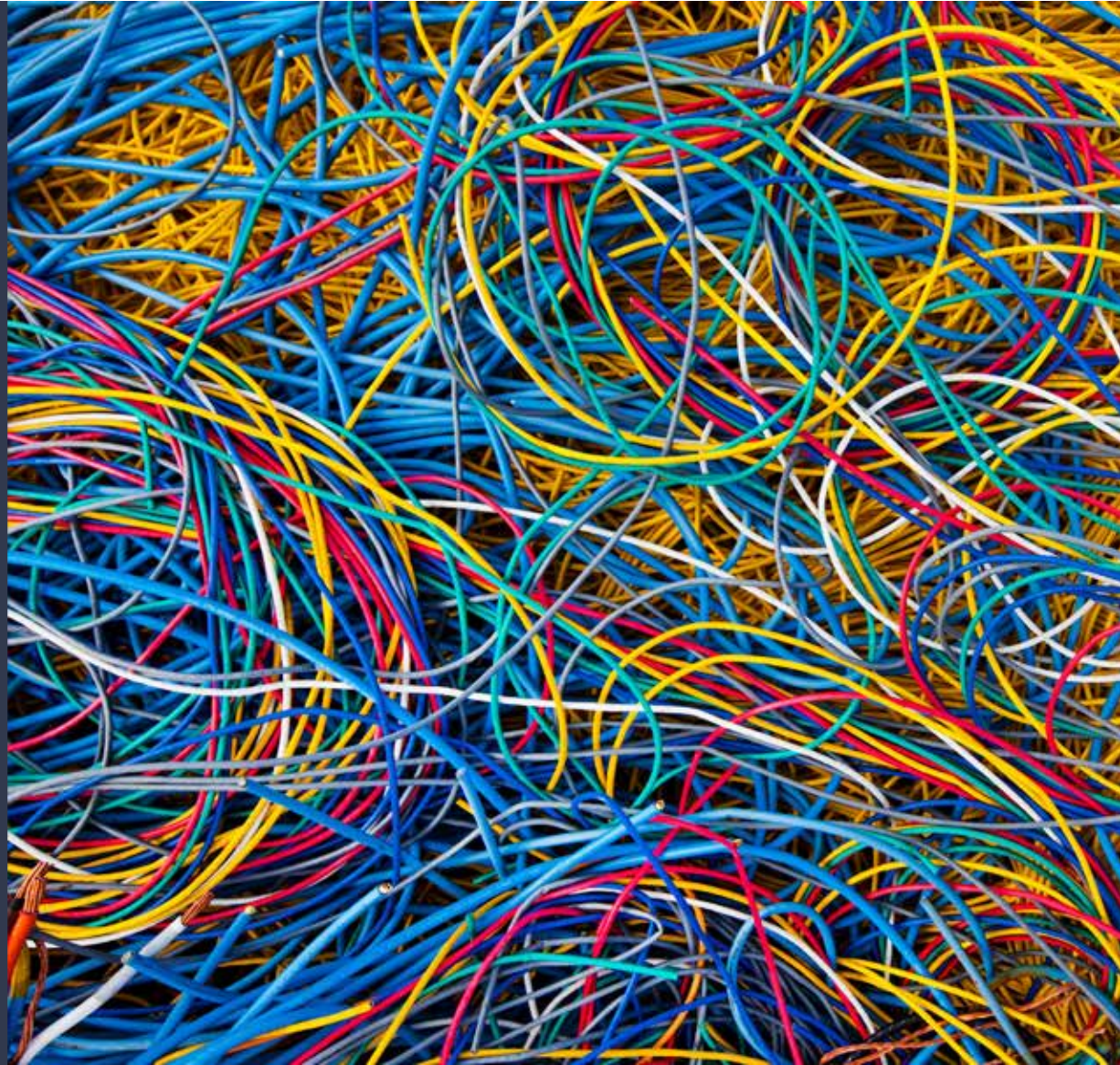
ACLs

Useful for problem customers

Automation to keep updated

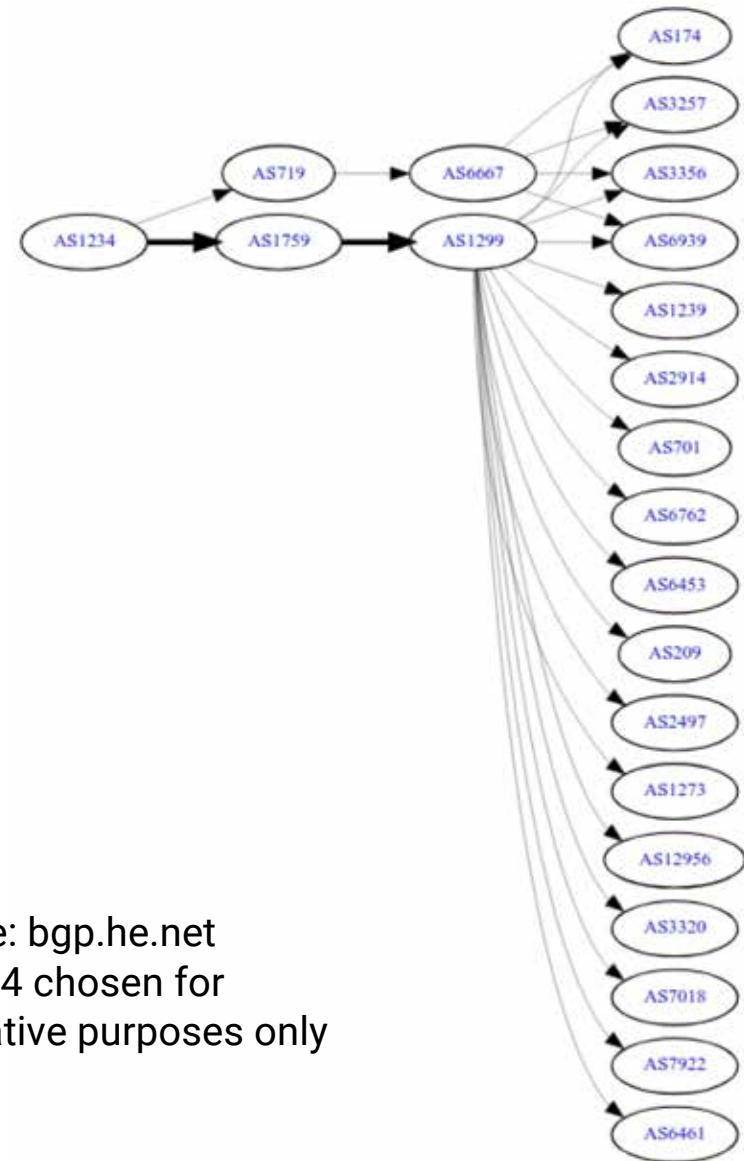
Router can only support 10k prefixes, though?

- 15169: 500
- 16509: 3,500
- 4134: 14,500 → 470



Enforcement Points

Attacker → Transit → Amplifier



Source: bgp.he.net
AS1234 chosen for
illustrative purposes only

Incentives for Transit Providers?

Transit providers are in a position to eliminate all UDP amplification attacks (and spoofed-source synfloods).

How can we encourage them?

Proactive: improve stability of the internet

Reactive: response to abuse complaints

Legal: law enforcement attack traceback requests

→ avoid the burden of responding by filtering spoofed attack traffic

Economic: customers prefer transit providers who filter spoofed packets

Regulatory: (threats of) government mandates

Other?

Call to Action

Software vendors:

- SHOULD minimize amplification to unverified sources

Network providers:

- are REQUIRED to **filter egress traffic** to prevent spoofing
- MAY request their transit providers trace the source of spoofed attacks

Transit providers:

- SHOULD use netflow or router counters to **identify sources of spoofed traffic**
- SHOULD **apply ACLs** to uncooperative customers

Questions / Discussion

Damian Menscher <damian@google.com>

