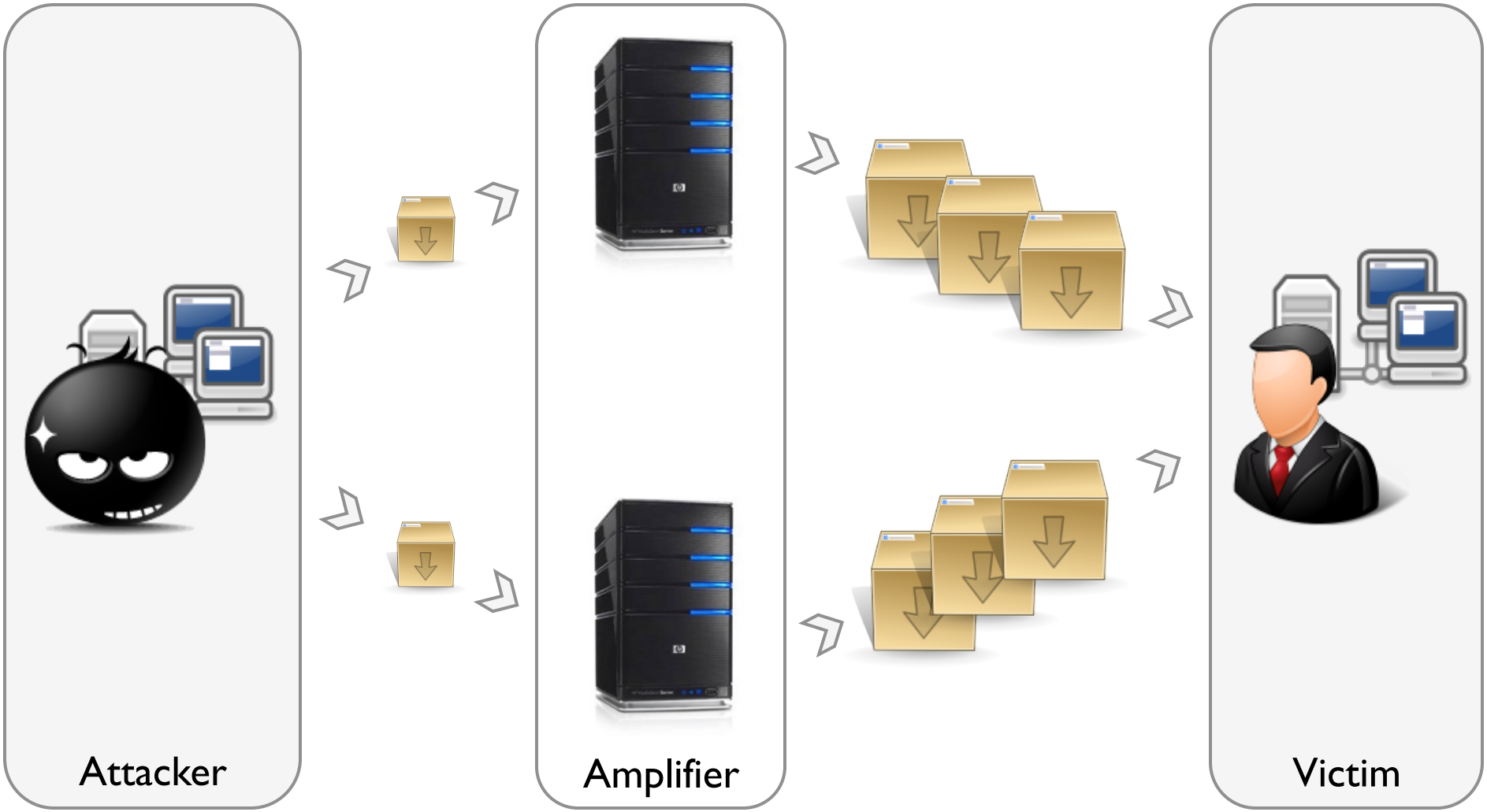
Amplification DDoS Attacks – Defenses for Vulnerable Protocols

Christian Rossow
VU University Amsterdam / Ruhr-University Bochum

RIPE 68, May 2014, Warsaw

Amplification DDoS Attacks



Amplification Attacks in Practice

Cloudflare Blog post, February 2014

Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

Published on February 13, 2014 01:00AM by Matthew Prince.

On Monday we mitigated a large DDoS that targeted one of our customers. The attack peaked just shy of 400Gbps. We've seen a handful of other attacks at this scale, but this is the largest attack we've seen that uses NTP amplification. This style of attacks has grown dramatically over the last six months and poses a significant new threat to the web. Monday's attack serves as a good case study to examine how these attacks work.

The Full Problem

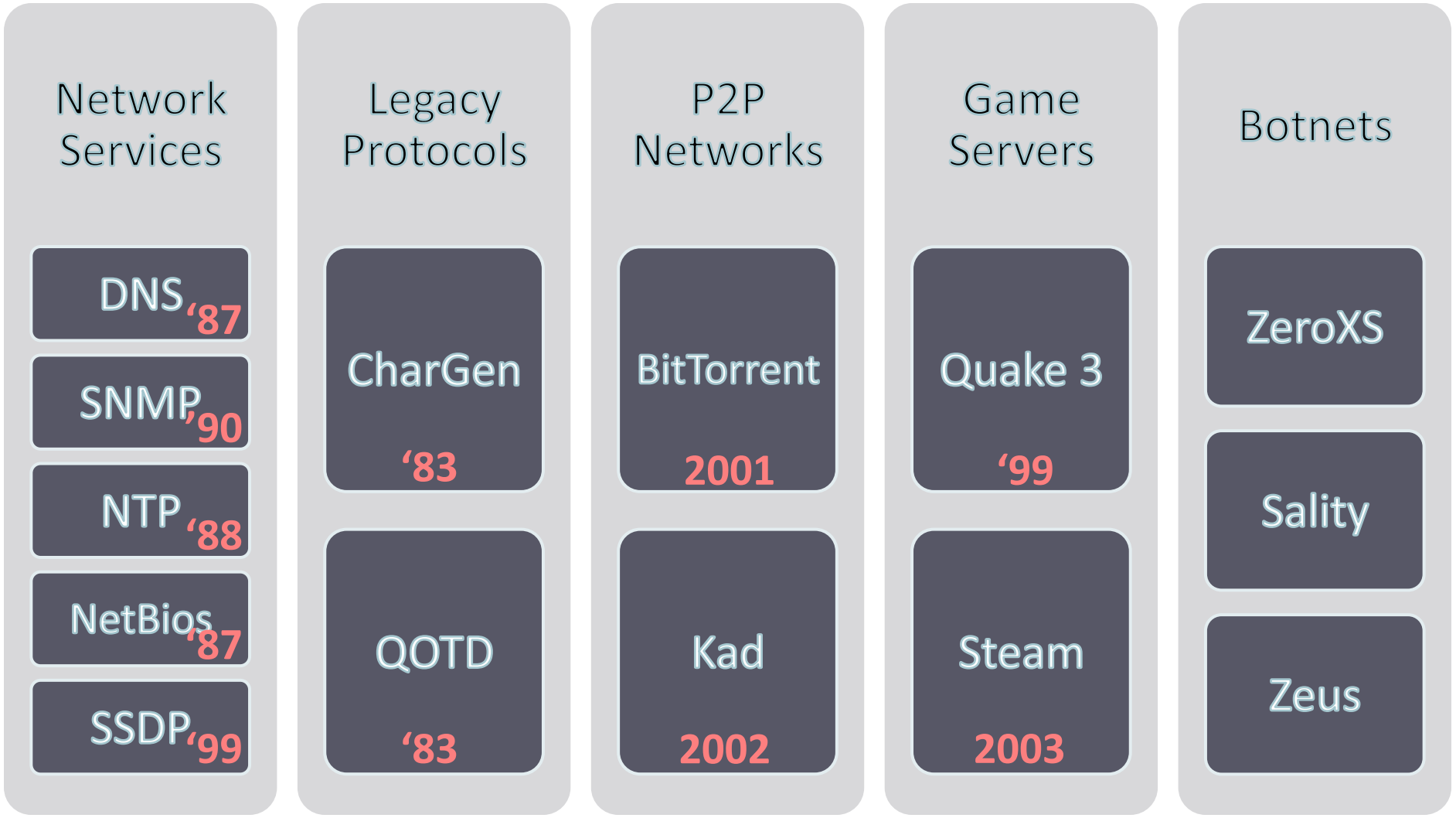
At the bottom of this attack we once again find the problem of open DNS recursors. The attackers were able to generate more than 300Gbps of traffic likely with a network of their own that only had access 1/100th of that amount of traffic themselves. We've written about how these mis-configured DNS recursors as a bomb waiting to go off that literally threatens the stability of the Internet itself. We've now seen an attack that begins to illustrate the full extent of the problem.

While lists of open recursors have been passed around on network security lists for the last few years, on Monday the full extent of the problem was, for the first time, made public. The Open Resolver Project made available the full list of the 21.7 million open resolvers online in an effort to shut them down.

Cloudflare Blog post, March 2013

Attack

14 Network Protocols Vulnerable to Amplificatioon



Measuring Amplification Rates (1/2)

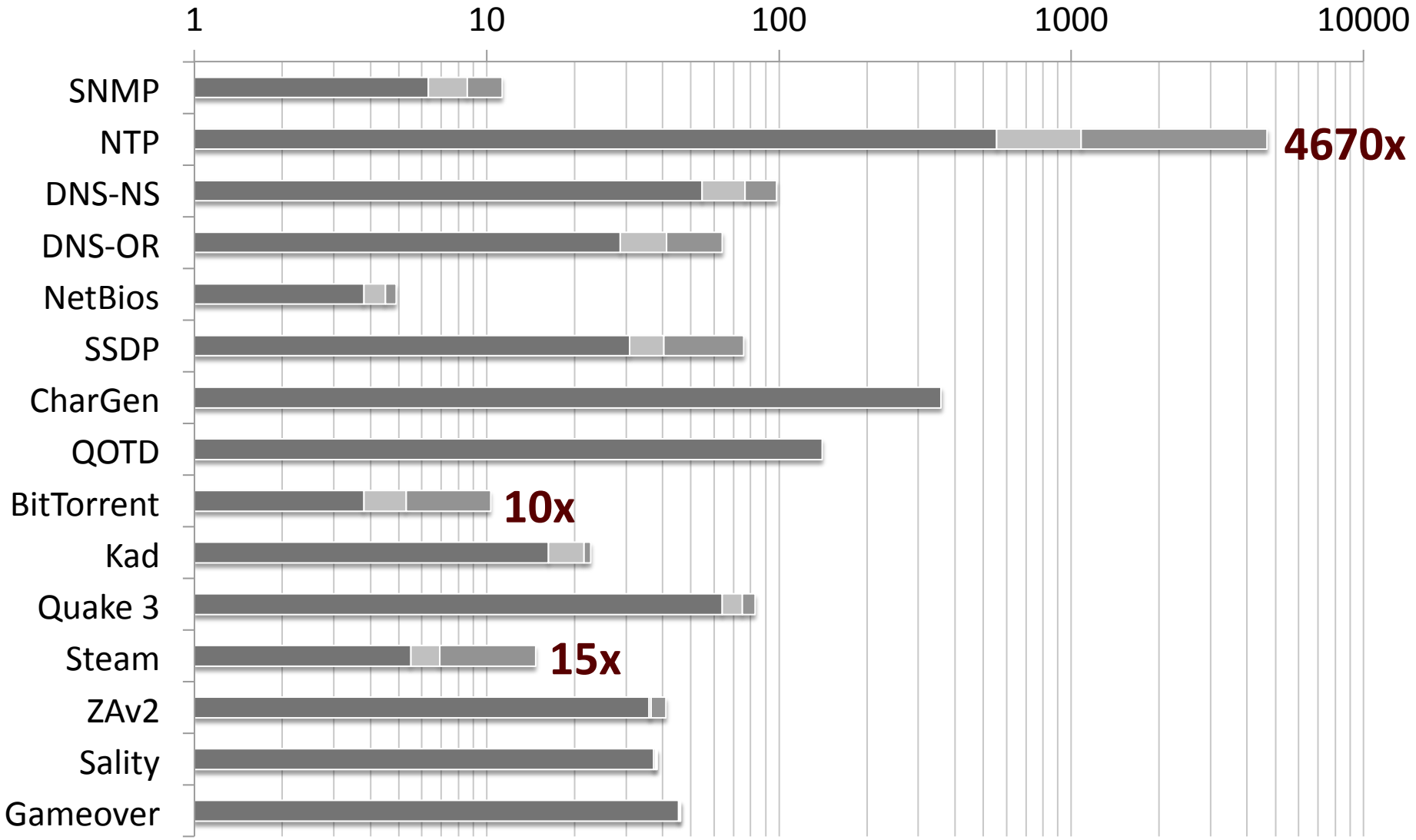
- Bandwidth Amplification Factor (BAF)

$$\frac{\text{UDP payload bytes at victim}}{\text{UDP payload bytes from attacker}}$$

- Packet Amplification Factor (PAF)

$$\frac{\text{\# of IP packets at victim}}{\text{\# of IP packets from attacker}}$$

Measuring Amplification Rates (2/2)



Number of Amplifiers

Protocol	Amplifiers	Tech.
SNMP v2	4,832,000	Scan
NTP	1,451,000	Scan
DNS_{NS}	255,819	Crawl
DNS_{OR}	7,782,000	Scan
NetBios	2,108,000	Scan
SSDP	3,704,000	Scan
CharGen	89,000	Scan
QOTD	32,000	Scan
BitTorrent	5,066,635	Crawl
Kad	232,012	Crawl
Quake 3	1,059	Master
Steam	167,886	Master
ZAv2	27,939	Crawl
Sality	12,714	Crawl
Gameover	2,023	Crawl

Defense

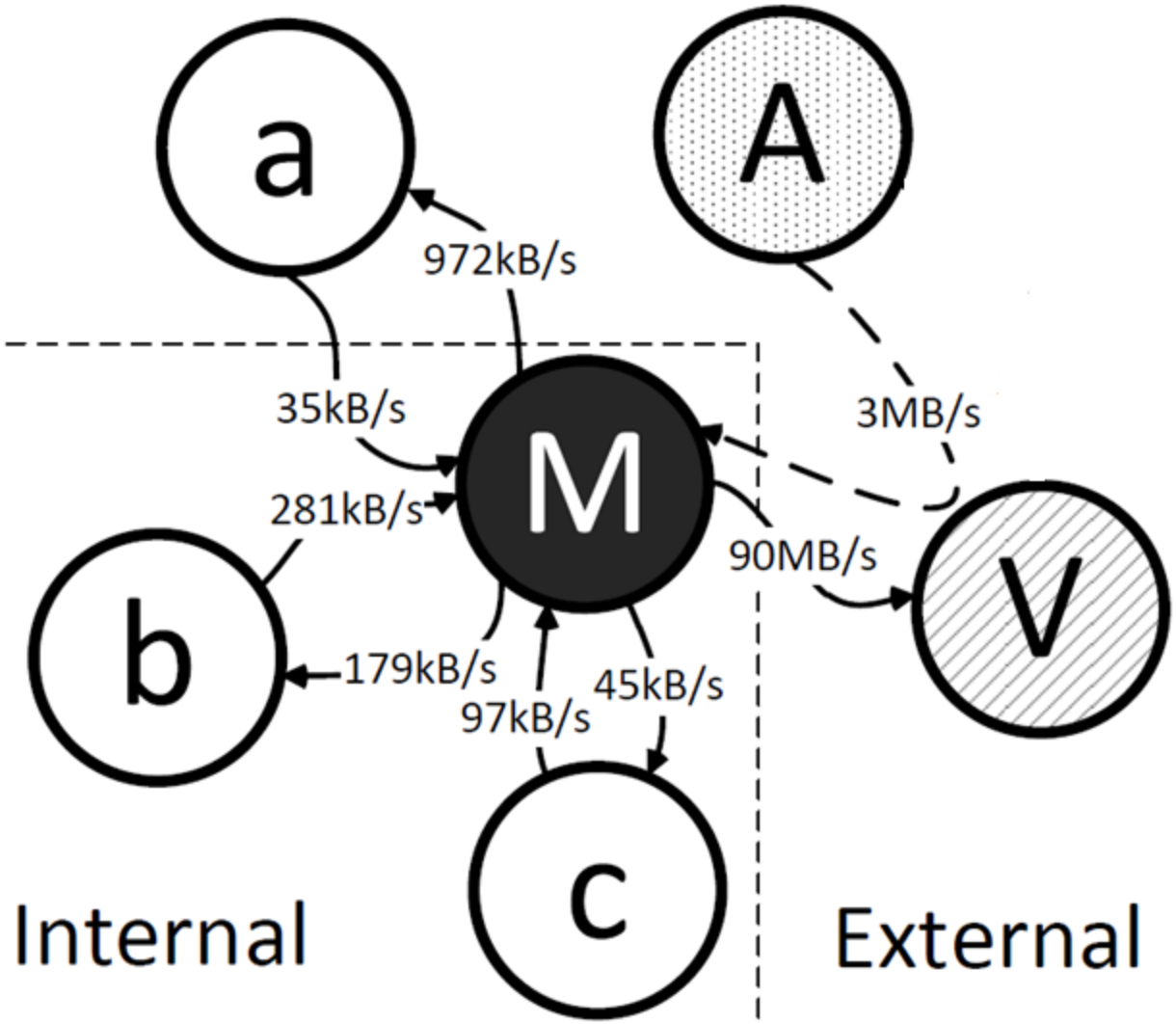
Let's Play Defense

- Defensive Countermeasures
  - Attack Detection
  - Attack Filtering
  - Hardening Protocols
  - etc.

Further Countermeasures

- S.A.V.E. – Source Address Verification Everywhere
  - a.k.a. BCP38
  - Spoofing is the root cause for amplification attack
- Implement proper handshakes in protocols
  - Switch to TCP
  - Re-implement such a handshake in UDP
- Rate limiting (with limited success)

Attack Detection at the Amplifier / Victim



Protocol Hardening: DNS

- Secure your open recursive resolvers
  - Restrict resolver access to your customers
  - See: http://www.team-cymru.org/Services/Resolvers/instructions.html
  - Check your network(s) at http://openresolverproject.org/
- Rate-limit at authoritative name servers
  - Response Rate Limiting (RRL) – now also in `bind`.

    See: http://www.redbarn.org/dns/ratelimits

Protocol Hardening: NTP

- Disable `monlist` at your NTP servers
  - Add to your ntp.conf: `restrict default noquery`
  - `monlist` is optional and not necessary for time sync
  - Check your network(s) at http://openntpproject.org/

- Filter `monlist` response packets
  - UDP source port 123 with IP packet length 468
  - Only very few (non-killer) `monlist` legitimate use cases

Conclusion

Conclusion

- 14+ UDP-based protocols are vulnerable to ampl.
- We can mitigate individual amplification vectors
  - NTP: Down to 8% of vulnerable servers in 7 weeks
  - DNS: Still 25M open resolvers – let's close them!

Amplification DDoS Attacks – Defenses for Vulnerable Protocols

Christian Rossow
VU University Amsterdam / Ruhr-University Bochum

RIPE 68, May 2014, Warsaw

More Slides

Detailed BAF and PAF per Protocol

Protocol	BAF *all*	BAF 50%	BAF 10%	PAF *all*	Scenario
SNMP v2	6.3	8.6	11.3	1.00	*GetBulk* request
NTP	556.9	1083.2	4670.0	10.61	Request "monlist" statistics
DNS_{NS}	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS_{OR}	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	*SEARCH* request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Sality	37.3	37.9	38.4	1.00	URL list exchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

Measuring Amplification Rates (2/2)

	BAF			PAF
Protocol	*all*	50%	10%	*all*
SNMP v2	6.3	8.6	11.3	1.00
NTP	556.9	1083.2	4670.0	10.61
DNS_{NS}	54.6	76.7	98.3	2.08
DNS_{OR}	28.7	41.2	64.1	1.32
NetBios	3.8	4.5	4.9	1.00
SSDP	30.8	40.4	75.9	9.92
CharGen	358.8	n/a	n/a	1.00
QOTD	140.3	n/a	n/a	1.00
BitTorrent	3.8	5.3	10.3	1.58
Kad	16.3	21.5	22.7	1.00
Quake 3	63.9	74.9	82.8	1.01
Steam	5.5	6.9	14.7	1.12
ZAv2	36.0	36.6	41.1	1.02
Sality	37.3	37.9	38.4	1.00
Gameover	45.4	45.9	46.2	5.39