Beyond 400 Gbps: Abusing NTP and Other Protocols for DDoS

Christian Rossow
VU University Amsterdam

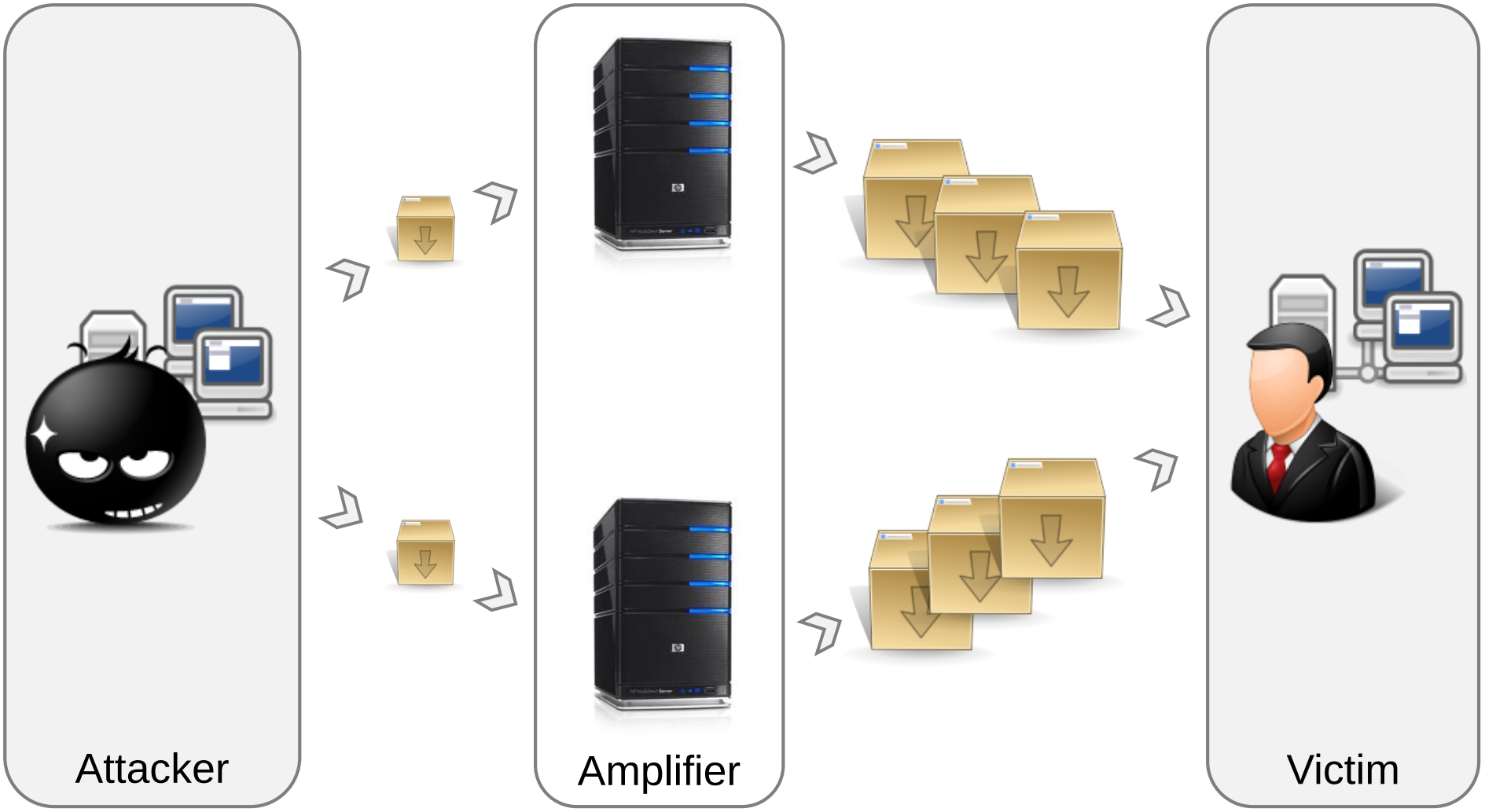
FIRST TC, April 2014, Amsterdam

About me: Christian Rossow

- PostDoc at VU Amsterdam
  - Syssec group of Herbert Bos
- PostDoc at Ruhr University Bochum
  - Syssec group of Thorsten Holz

- Other affiliations
  - 2006 – 2013: Institute for Internet Security
  - Internships at ICSI (Berkeley), TU Vienna, Symantec
  - Symantec fellowship award 2013

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

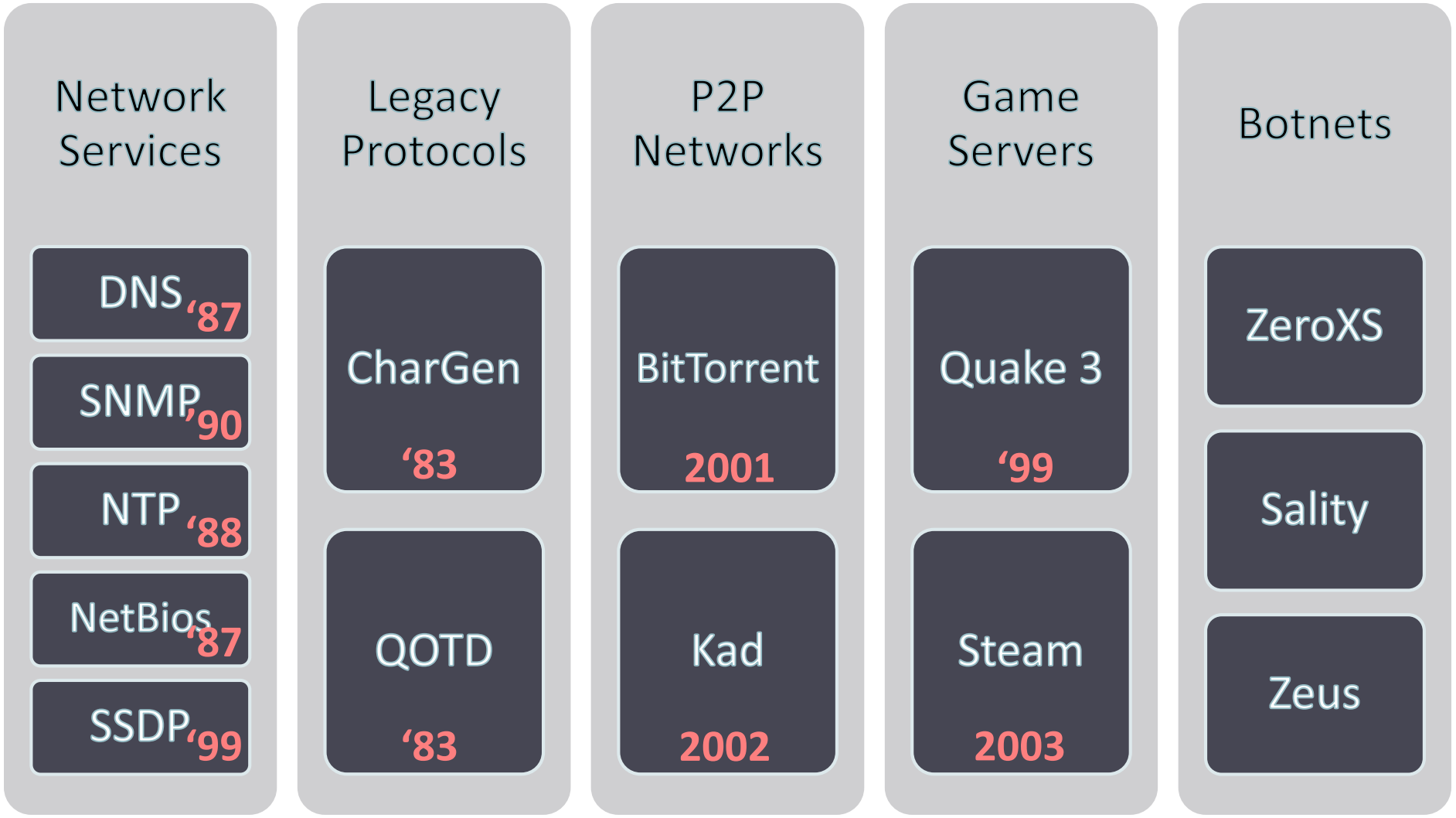
At the bottom of this attack we once again find the problem of open DNS recursors. The attackers were able to generate more than 300Gbps of traffic likely with a network of their own that only had access 1/100th of that amount of traffic themselves. We've written about how these mis-configured DNS recursors 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)

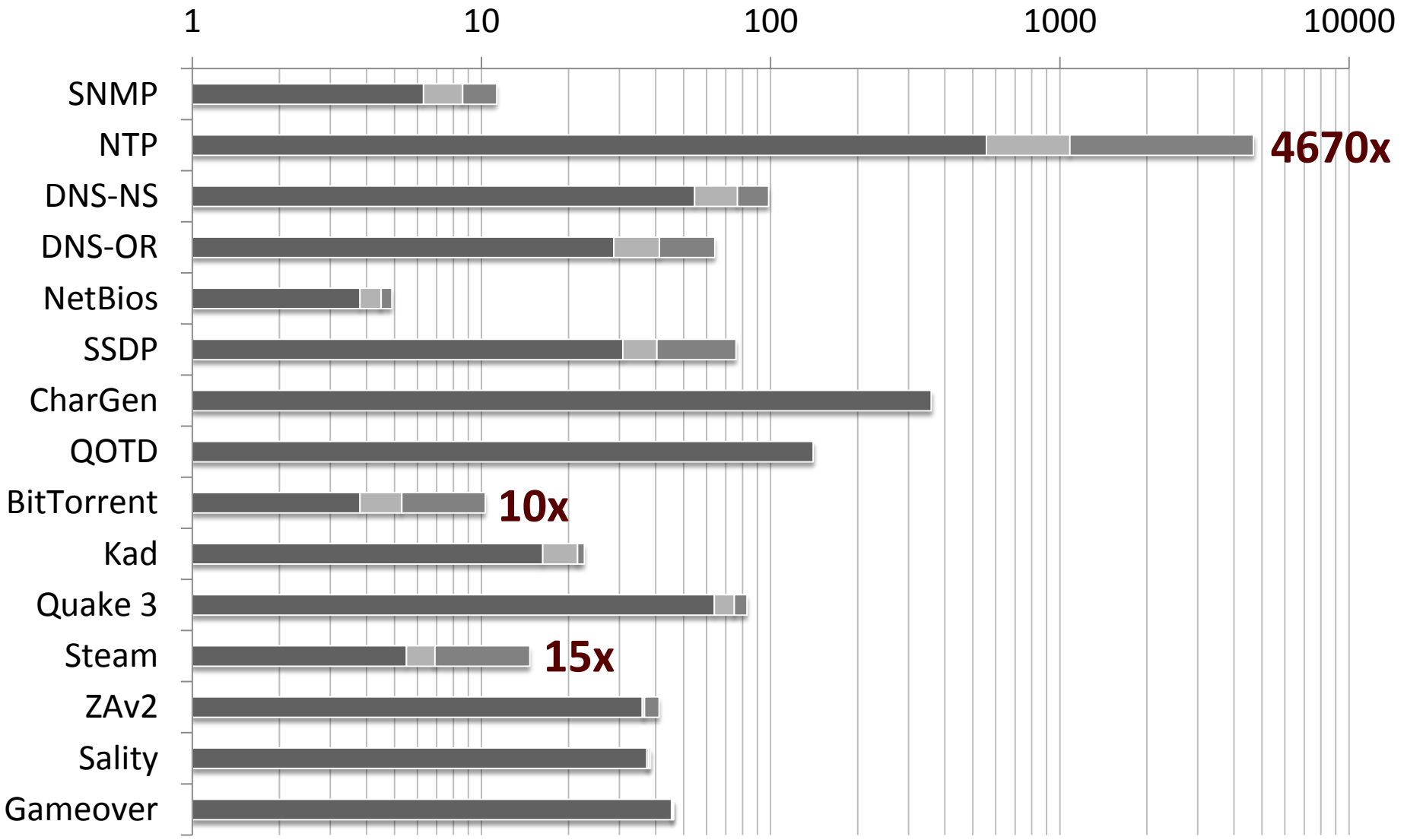
- Bandwidth Amplification Factor (BAF)

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

- 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

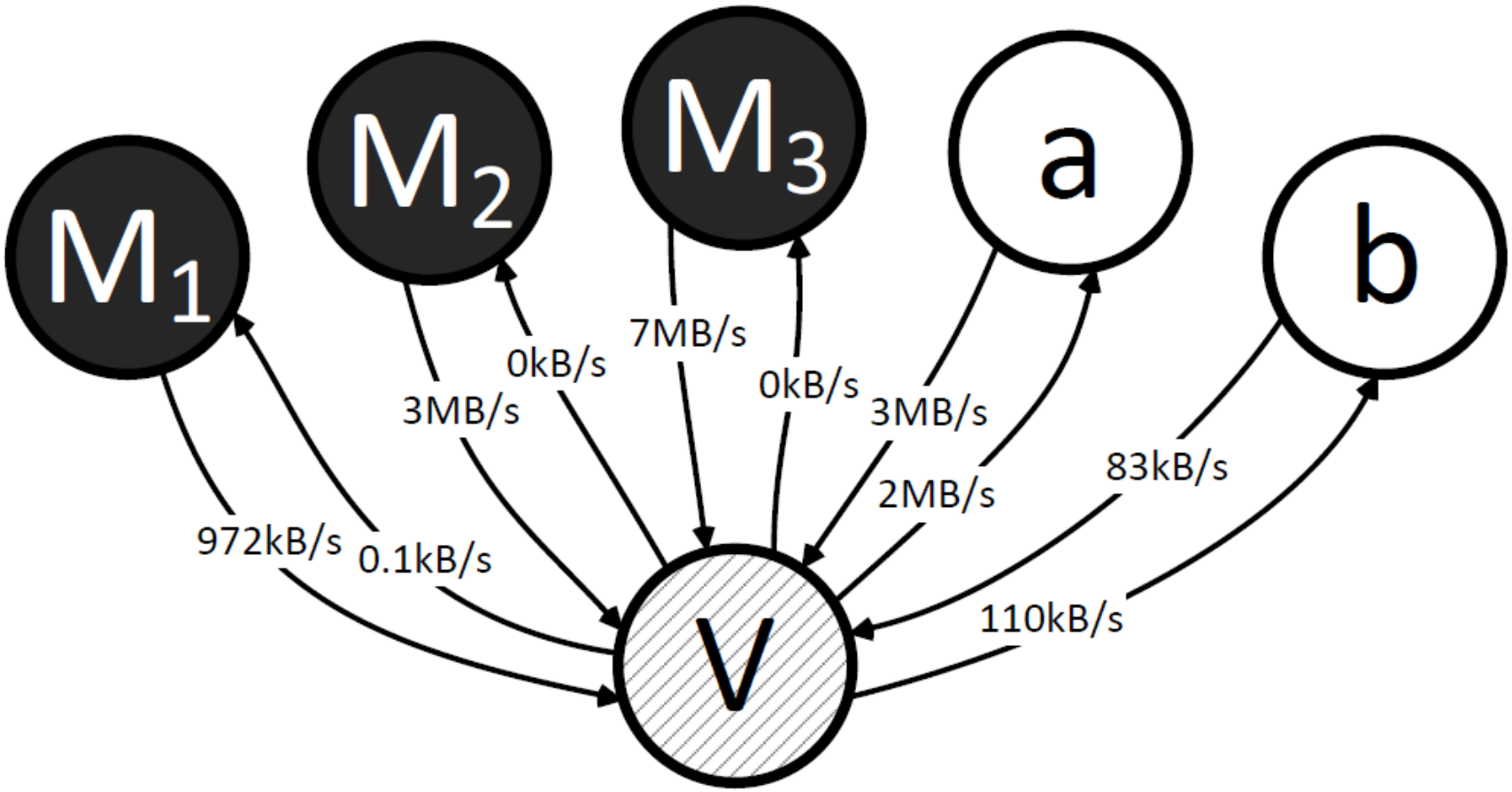
Protocol	Amplifiers	Tech.	t_{1k}	t_{100k}
SNMP v2	4,832,000	Scan	1.5s	148.9s
NTP	1,451,000	Scan	2.0s	195.1s
DNS_{NS}	255,819	Crawl	35.3s	3530.0s
DNS_{OR}	7,782,000	Scan	0.9s	92.5s
NetBios	2,108,000	Scan	3.4s	341.5s
SSDP	3,704,000	Scan	1.9s	193.5s
CharGen	89,000	Scan	80.6s	n/a
QOTD	32,000	Scan	228.2s	n/a
BitTorrent	5,066,635	Crawl	0.9s	63.6s
Kad	232,012	Crawl	0.9s	108.0s
Quake 3	1,059	Master	0.6s	n/a
Steam	167,886	Master	1.3s	137.1s
ZAv2	27,939	Crawl	1.5s	n/a
Sality	12,714	Crawl	4.7s	n/a
Gameover	2,023	Crawl	168.5s	n/a

Defense

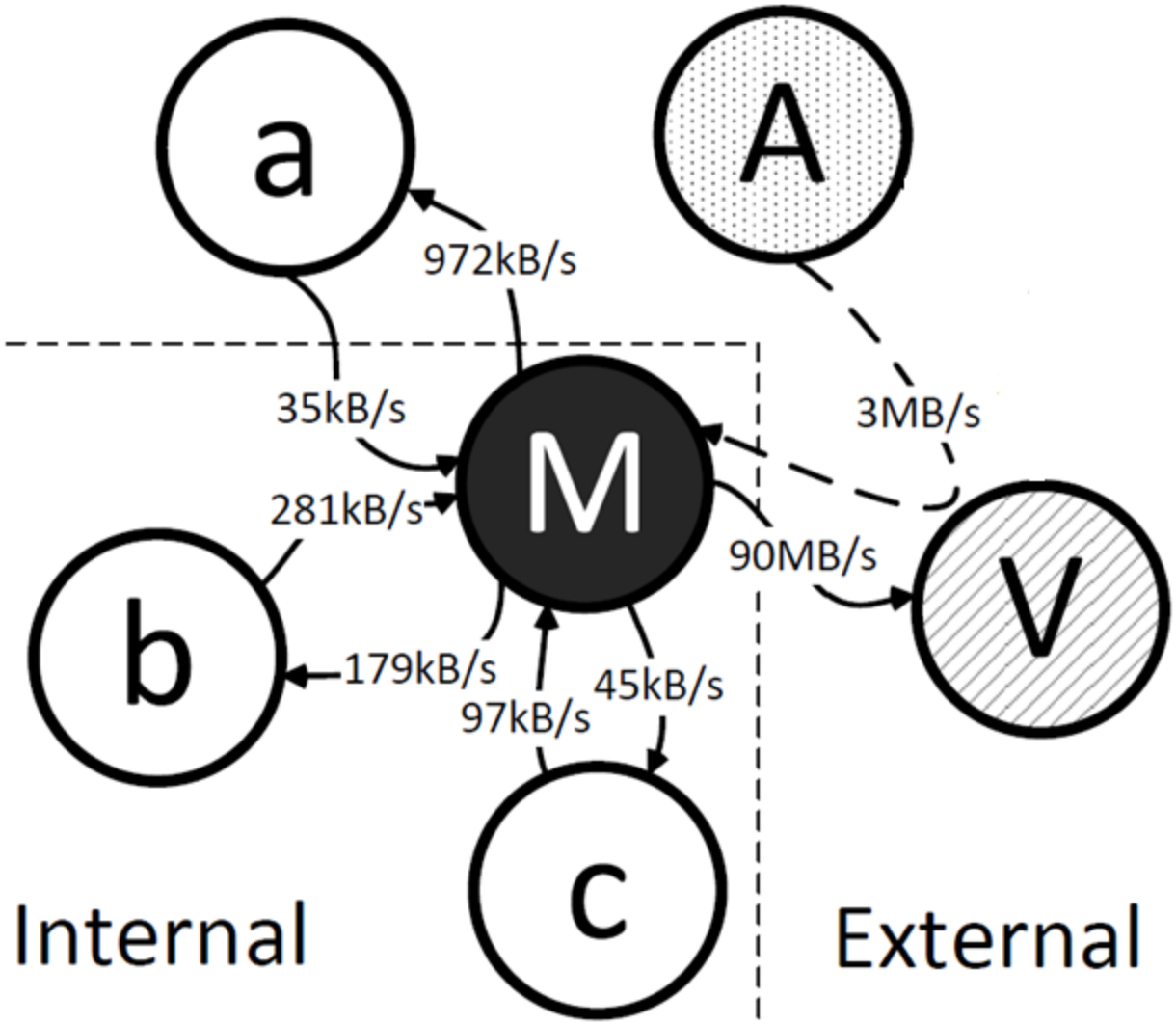
Let's Play Defense

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

Attack Detection at the Victim



Attack Detection at the Amplifier



Attack traffic filtering

Protocol	(ii) UDP ports		(iii) Resp len		(iv) PL	Detection Port	Detection len	Detection PL
SNMP	1	100.0%	239	14.9%	+9B	✓		✓
NTP	1	100.0%	90	26.1%	>100B	✓		✓
DNS_{NS}	—	—	875	2.1%	+7B			✓
DNS_{OR}	> 1000	41.3%	70	24.7%	+7B			✓
NetBios	6	97.9%	21	29.1%	+55B	✓		✓
SSDP	1	100.0%	96	36.0%	+17B	✓		✓
CharGen	1	100.0%	5	76.5%	+36B	✓	✓	✓
QOTD	1	100.0%	10	16.7%	+1B	✓		
BitTorrent	> 1000	12.4%	128	24.1%	+12B			✓
Kad	> 1000	17.2%	54	54.8%	2B			
Quake 3	174	41.7%	462	0.8%	+19B			✓
Steam	> 1000	8.9%	856	19.9%	+8B			✓
ZAv2	84	98.6%	13	98.3%	+12B	✓	✓	✓
Sality	> 1000	2.1%	33	3.7%	none			
Gameover	> 1000	0.3%	201	3.3%	none			

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

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)

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!
- S.A.V.E. would kill the problem at its root

Acknowledgements

- Thanks to
  - SURFnet, DFN-CERT, CERT/CC
  - John Kristoff (Team Cymru)
  - Jared Mauch (Open*XXX*Project.org)
  - Harlan Stenn (NTF)
  - Alfred Reynolds (Valve Software)
  - Marc Kührer (Ruhr-University Bochum)
  - *And many others.*

Beyond 400 Gbps: Abusing NTP and Other Protocols for DDoS

Christian Rossow
VU University Amsterdam

FIRST TC, April 2014, Amsterdam