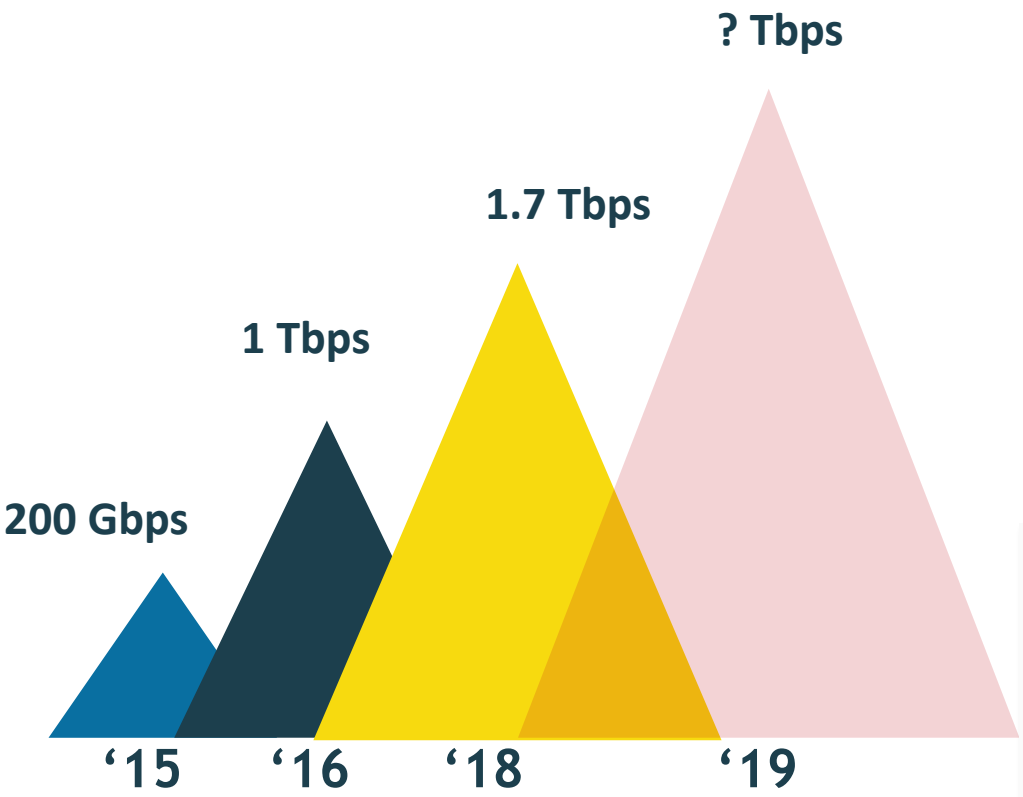
DDoS Attacks, Booter Services & DDoS Mitigation at IXPs

Daniel Kopp
DE-CIX Products & Research

DE-CIX

DDoS Attacks



NETSCOUT

Attack Map Archives

BLOG HOME CORPORATE SITE

NETSCOUT Arbor Confirm 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon

Carlos Morales on March 5, 2018.

Peak Attack Sizes Through March 2018

A Frightening New Kind Of DDoS Attack Is Breaking Records

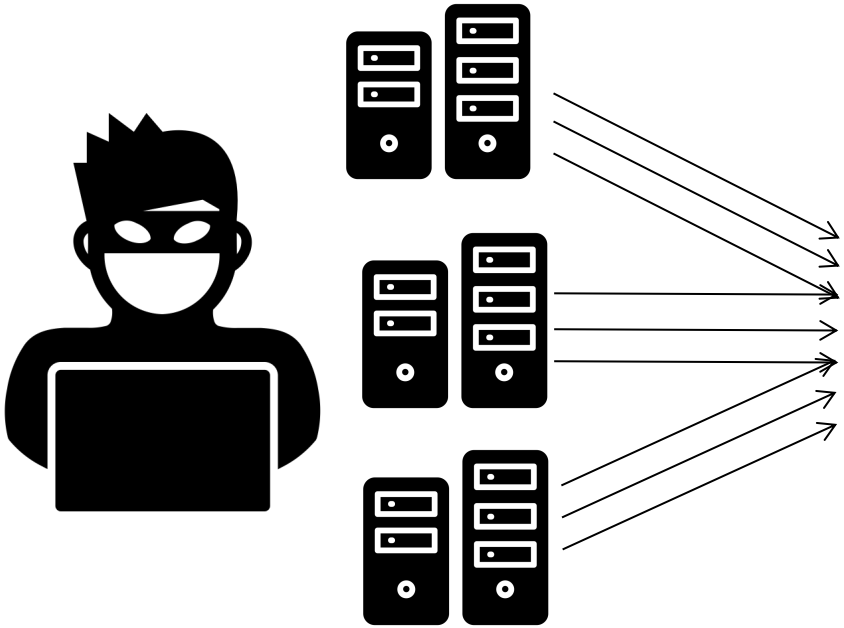
Lee Mathews Contributor

Security

Observing, pondering, and writing about tech. Generally in that order.

Back in October of 2016, a denial-of-service attack against a service provider called Dyn crippled Americans' Internet access on the east coast. Its servers were bombarded with a jaw-dropping amount of traffic. Some estimates believed the data rate of the attack peaked at around 1.2Tbps, which was unheard of at the time.

Performing a DDoS Attack

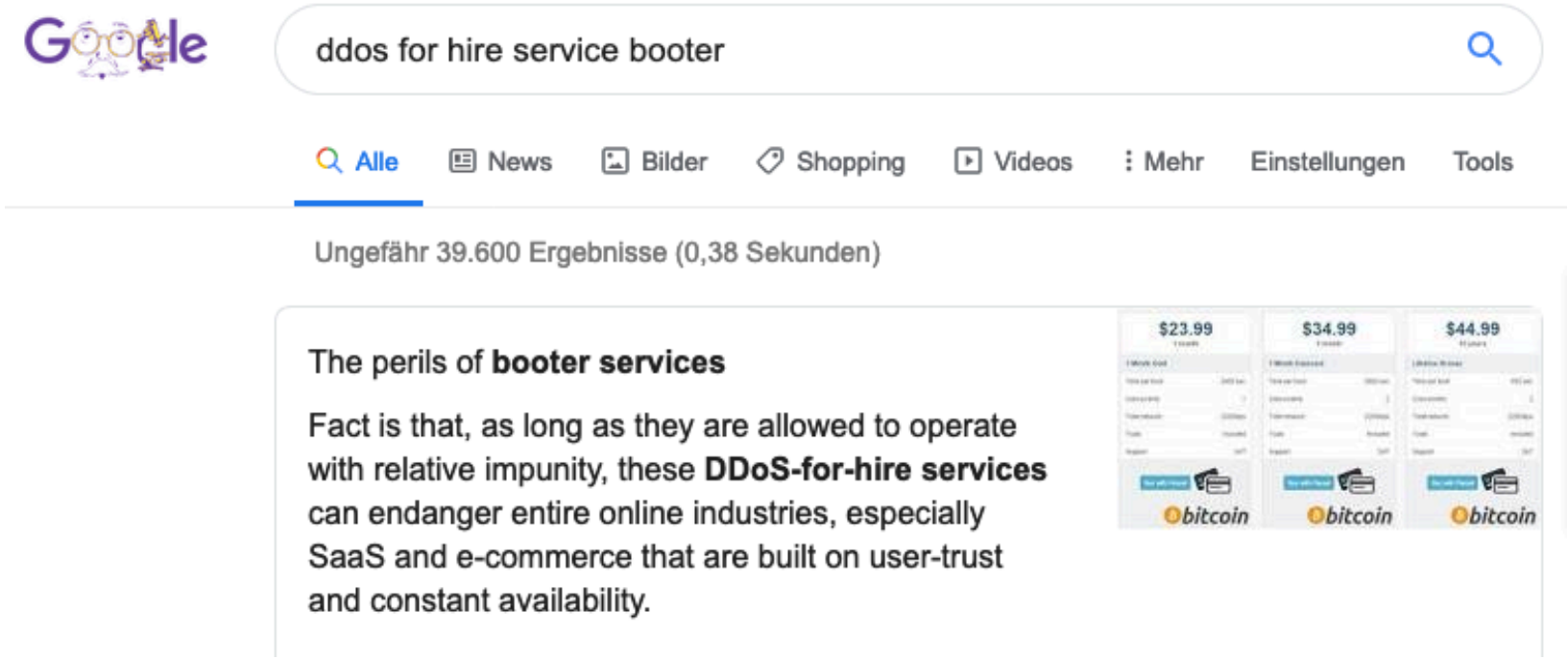


→**Requirements**

→**Techincal expertise**

→ **Infrastructure (**Use somebody else's infrastructure protocol flaws, unprotected systems, ...**)**

DDoS for Hire - Booter Services




DEFCON.PRO
HOME
FEATURES
SERVICES
ABOUT
PRICING
PAYMENTS
CONTACT
REGISTER
LOGIN
DEFCON PRO - Best Stresser / Booter
Finding New Ways to Fix Old Problems!
Login
Register

Advantages:

Below are our advantages.

- 24/7 Support
- Private Methods
- Skype Resolver
- 99% UPTIME
- Dedicated Servers
- Crypto, BitCoin and more
- Stop Button
- IP Geolocation
- Cloudfare resolver
- Domain resolver
- Amazing Power
- Easy to use interface

Our services

Below the services which you can use on our network.

Stress testing

You are not sure about the capabilities of our Stresser? Buy a trial and check our power!

Great Support

Our employees watch over the company 24/7. You can contact via ticketing system.

99% Uptime

Our network is working all the time, technical breaks occur very rarely. The network is stable.

Easy panel

Our panel is easy to use and graphically clear. It has all the necessary options.

Helpful Tools

We have useful tools such as IP geolocation, teamspeak, domain and CloudFare resolver.

Cheap price

You don't have enough money to feel a hacker? Redemption at our low-cost service with high power.

About Us

In this section you will learn some information about us and our business.

Our Company

Our organization is engaged in stress testing and DDoS Protection from Feb 2016. Mainly interested in the industry DDoS attacks.

We had some popular stresser's have been praised by customers. Our team consists of some very experienced people involved in hacking from az.

DEFCON network was created for a large project strong stresser which would break the existing market.

DDoS Order

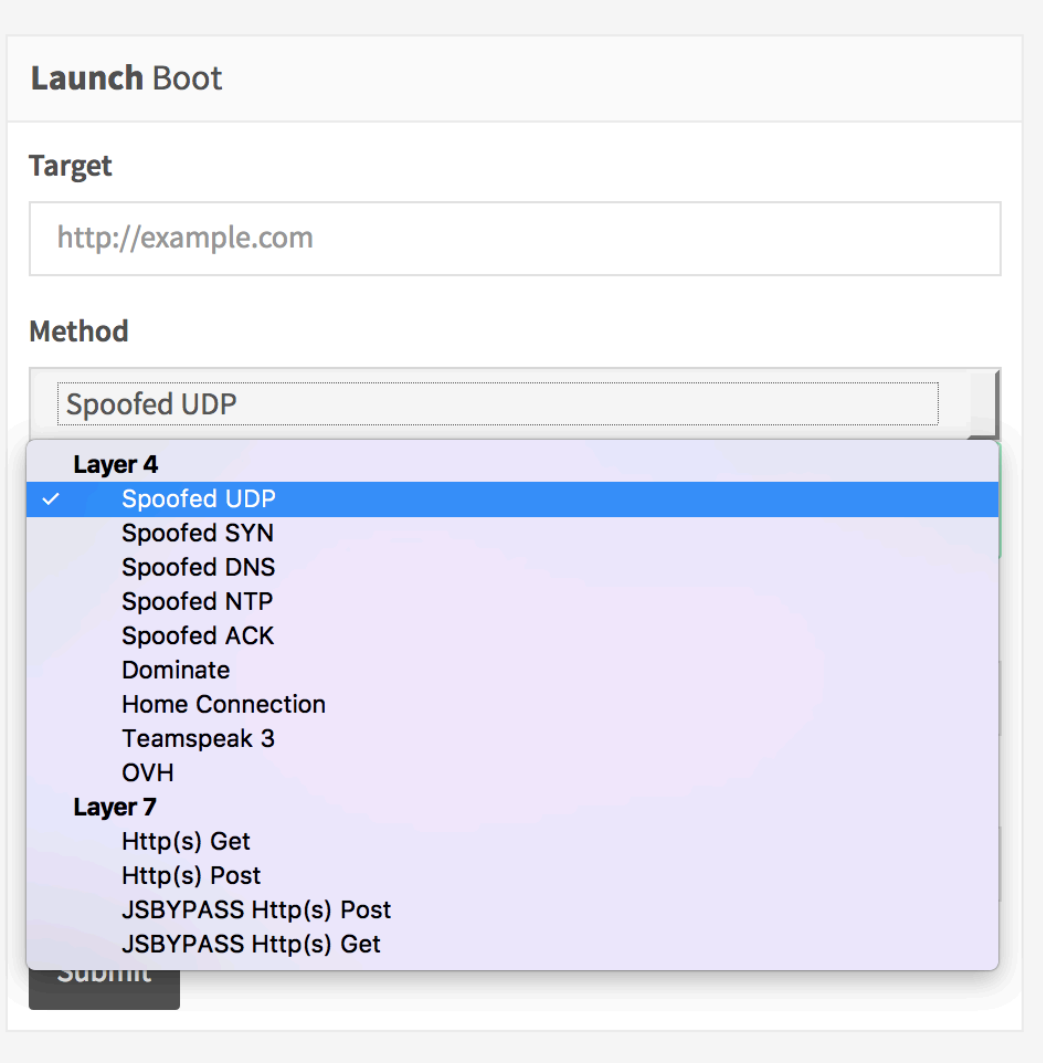
→ **Flat rate** for DDoS attacks

- x attacks a day
- x concurrent
- Usually 30 days

→ 10 - 20 **different types**

- Application → high pps
- Amplification → high bandwidth

→ Claim to offer **5 - 100 Gbit/s**

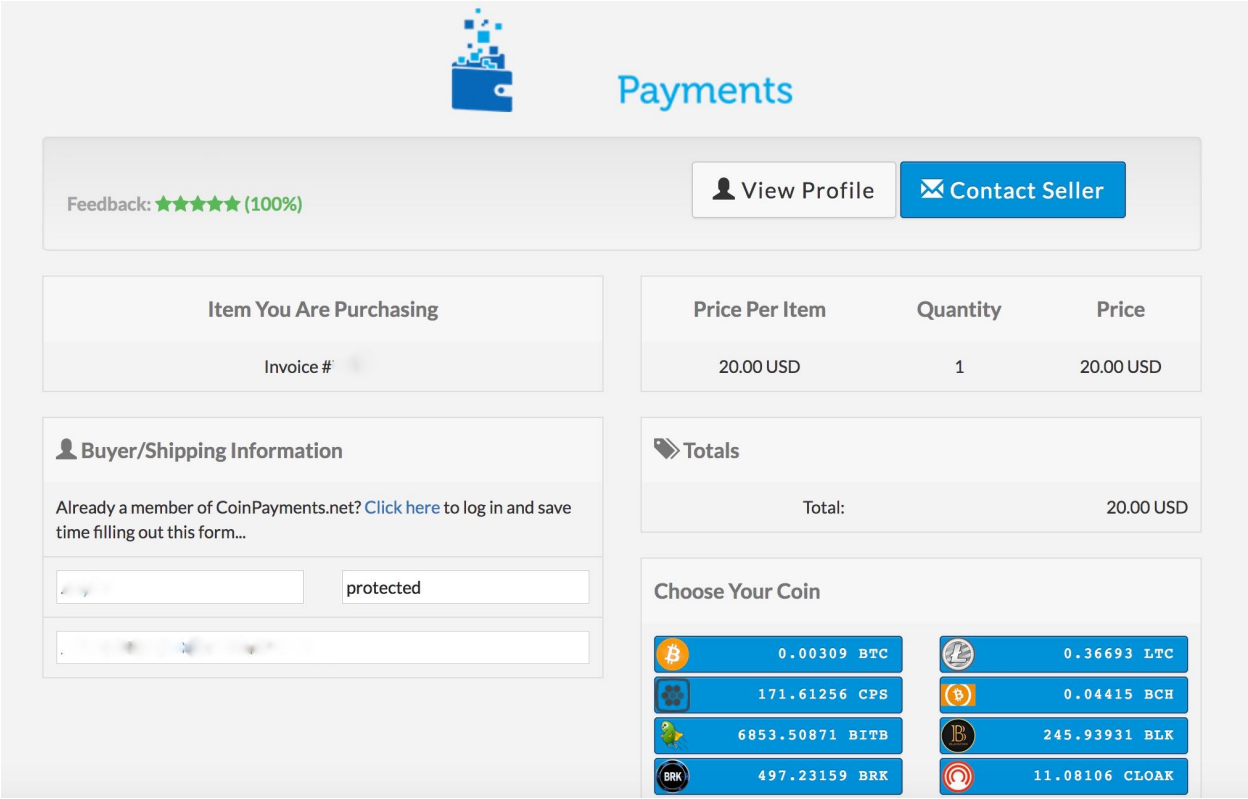


Payment

→ Payment with **crypto currency**

→ Prices **$20 - $200**

→ **Fake services** exist

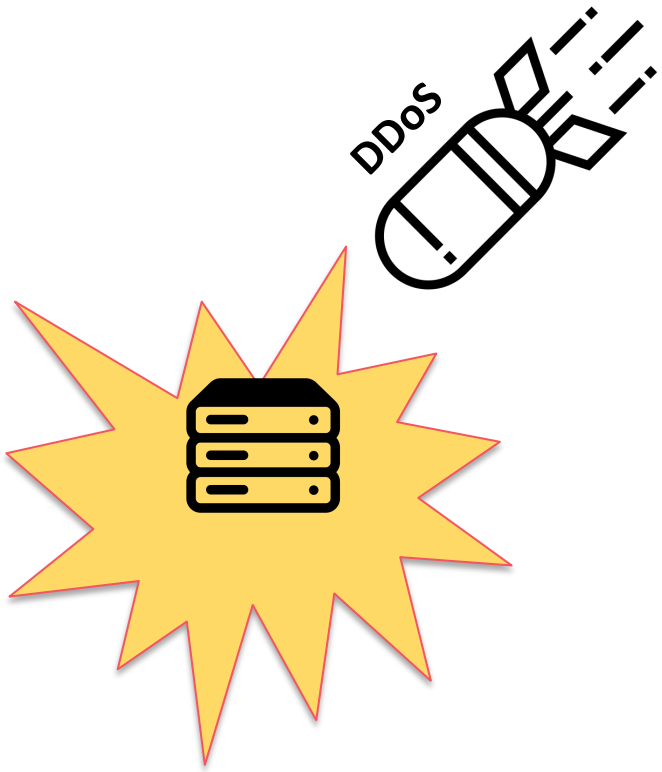


Measurement System Motivation

We built a server and network setup to attack ourselves and record the attack traffic

→ **Requirements**

- Minimal impact during DDoS
- Record 10 Gbit/sec to disc
- Record at least continuous 30min
- Global reachability
- Direct connection to many ASNs
- Keep costs low



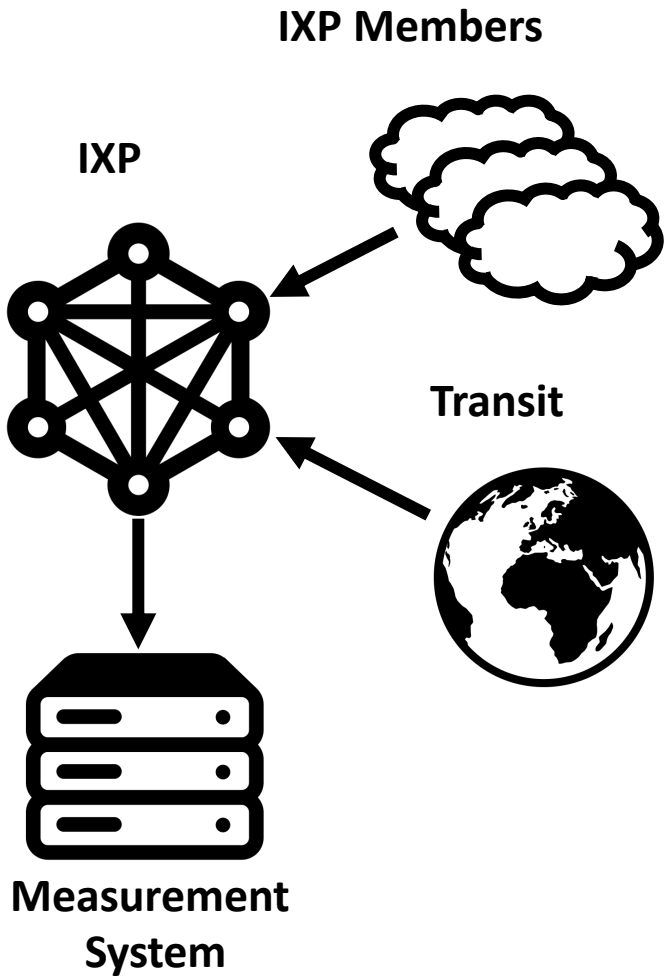
Measurement System and Setup

→ Internet Connectivity

- 10G Peering
- 10G Transit
- Own ASN and IPv4 Space

→ Mesurement Limitations

- Tcpdump → up to 10 Gbits/sec
- sFlow → up to 10 Gbits/sec
- IPFIX → over 100 GBit/sec



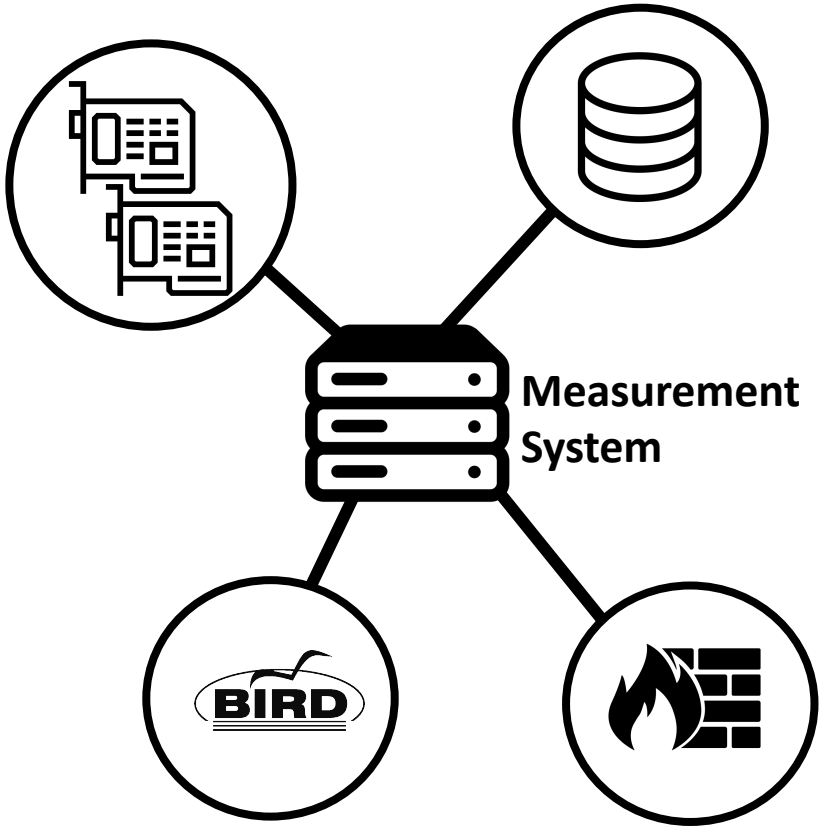
Measurement System and Setup

→ Hardware

- Dedicated second NIC as mirror
- Fast write speed: SAS RAID-0
- Dedicated Raid Controller
- Singe core performance

→ System Setup

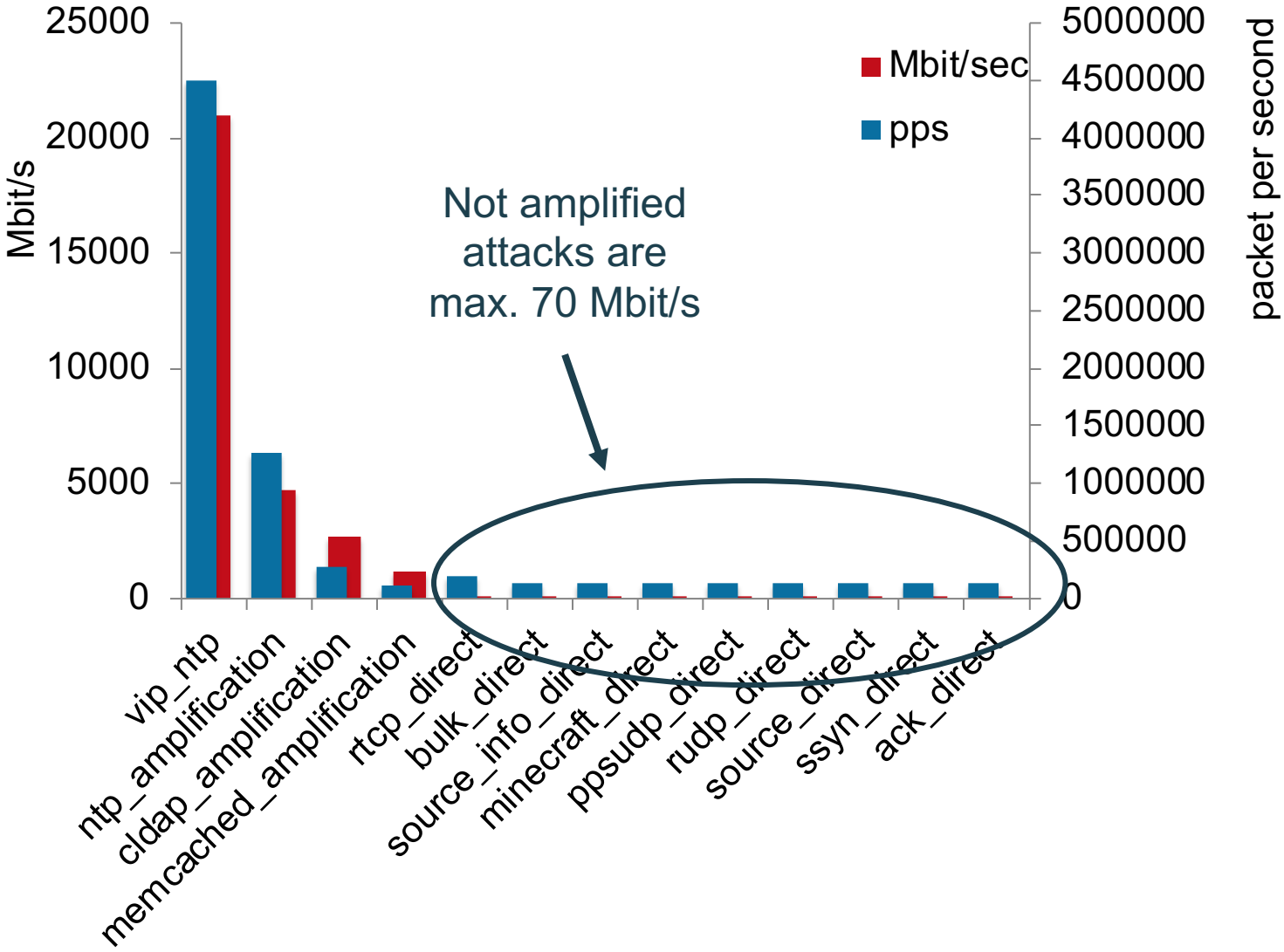
- Linux as a BGP Router and Network
- Bird & Docker
- ARP! → ARP tables and IP tables



Sample of Booter Service Prices

Booter	Seized	Time	NTP	DNS	CLDAP	mcache	non-VIP	VIP
A	✓	Apr, Aug	✓	✓	✓	✓	**$8.00**	$250
B	✓	Jun-Sep	✓	✓	✓	✓	**$19.83**	**$178.84**
C		Apr-May	✓	✓			**$14.00**	$89
D		May	✓	✓			**$19.99**	$149.99

DDoS Attacks - Overview



DDoS – Attack Traffic

NTP:

→Up to 20 Gbit/s

→ 4 million pps

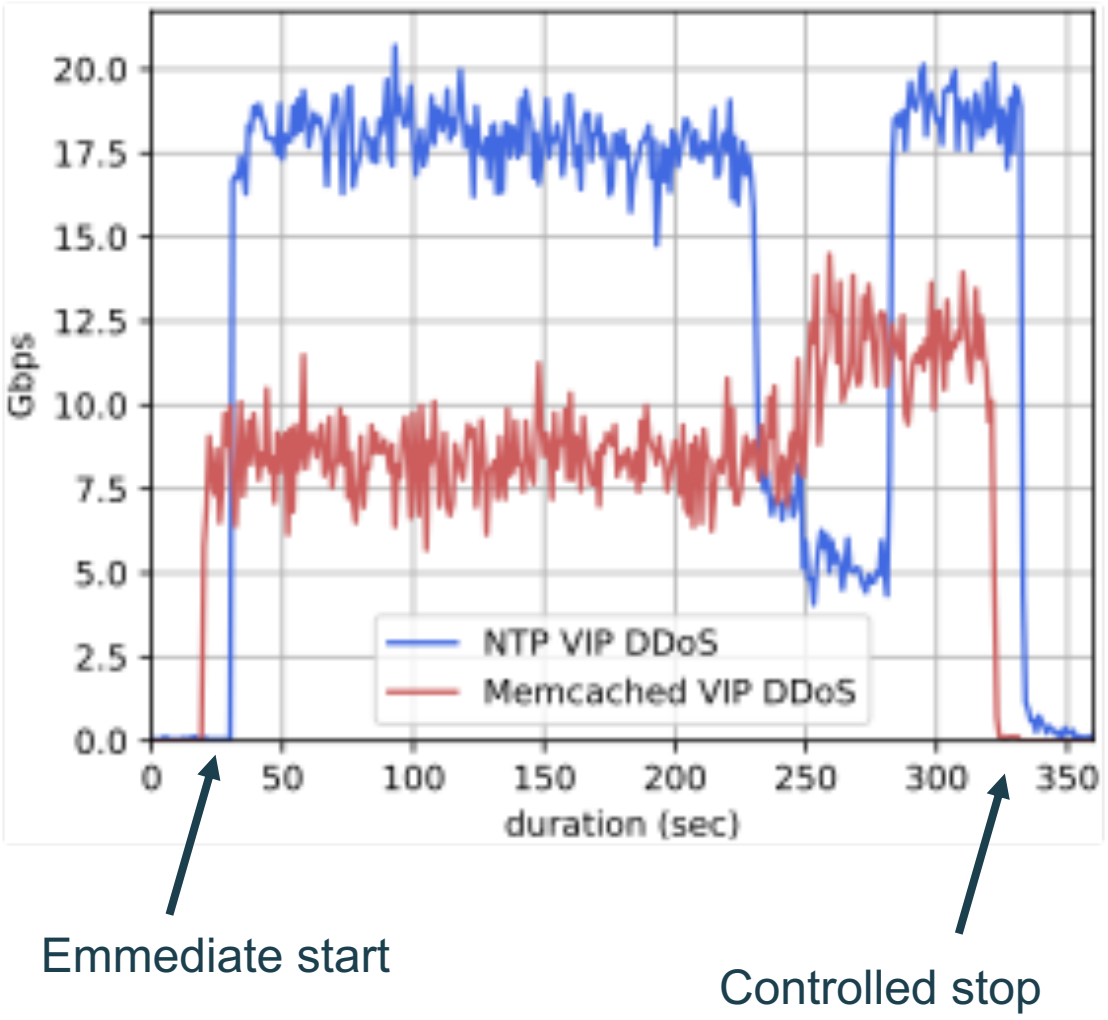
→ 930 source IPs (reflectors)

→ 350 source ASNs (networks)

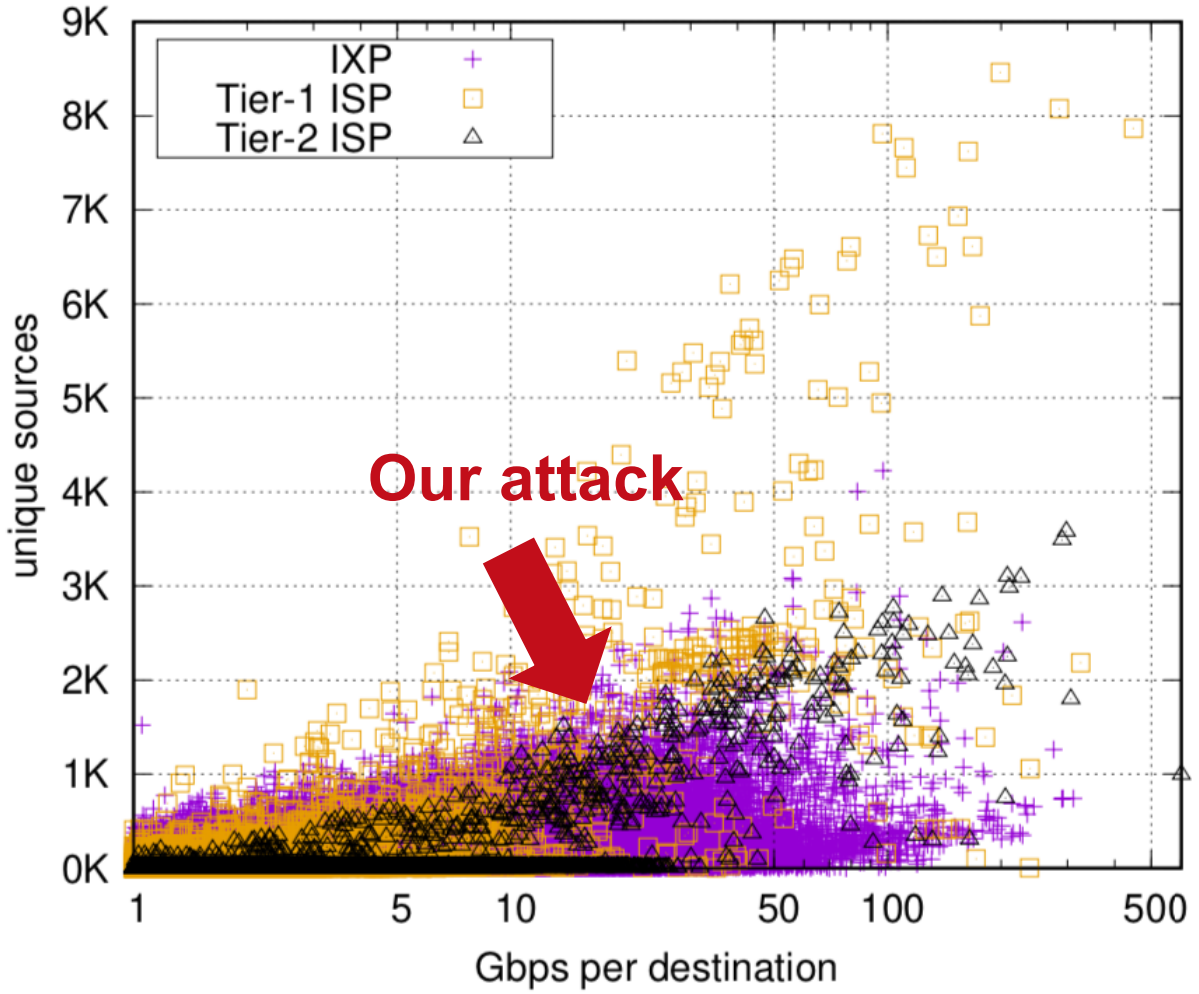
→ Top 3 ASNs 23% of traffic

- China, Taiwan, Hungary

→ Majority of traffic via transit



NTP DDoS Attacks Landscape



➔ 311K destinations | 224 victims > 100 Gbps | 5 > 300 Gbps | 1 > 600 Gbps

Booter Services vs. FBI

→ FBI operation took down prox. 15
DDoS for hire services end of last year

More Details...

DDoS Hide & Seek: On the Effectiveness of a Booter Services Takedown

Daniel Kopp
DE-CIX

Matthias Wichtlhuber
DE-CIX

Ingmar Poese
BENOCS

Jair Santanna
University of Twente

Oliver Hohlfeld
Brandenburg University of Technology

Christoph Dietzel
DE-CIX / MPI for Informatics

ABSTRACT

Booter services continue to provide popular DDoS-as-a-service platforms and enable anyone irrespective of their technical ability, to execute DDoS attacks with devastating impact. Since booters are a serious threat to Internet operations and can cause significant financial and reputational damage, they also draw the attention of law enforcement agencies and related counter activities. In this paper, we investigate booter-based DDoS attacks in the wild and the impact of an FBI takedown targeting 15 booter websites in December 2018 from the perspective of a major IXP and two ISPs. We study and compare attack properties of multiple booter services by launching Gbps-level attacks against our own infrastructure. To understand spatial and temporal trends of the DDoS traffic originating from booters we scrutinize 5 months, worth of inter-domain traffic. We observe that the takedown only leads to a temporary

Hohlfeld, and Christoph Dietzel. 2019. DDoS Hide & Seek: On the Effectiveness of a Booter Services Takedown. In *Internet Measurement Conference (IMC '19), October 21–23, 2019, Amsterdam, Netherlands.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3355369.3355590

available, e.g., computing power or network bandwidth. Beyond the web, modern DDoS attacks can overwhelm cloud services [50] or congest backbone peering links [48]. The motivation for launching attacks ranges from financial [9, 53], to political [4, 35], cyber warfare [19, 54], smoke screen for other attack types [33], and even teenagers attacking their schools [47]. To scale, DDoS amplification attacks [42, 43] abuse protocol design (flaws)—e.g., NTP, DNS, SNMP, and Memcached [2, 14, 37, 42]—where a relatively small request can trigger a significantly larger response (up to ×50 000). Spoofed source IP addresses [5, 6, 34, 36] allow traffic to be reflected to the target [55]. Thus, attacks are increasing in size and sophistication [1]. A few years back, the largest reported attacks peaked just below 300 Gbps [39, 40], whereas DDoS attacks have now reached the Tbps level [3, 26, 37, 58].

Booters as DDoS tool. DDoS-as-a-service providers, also referred

stand the booter market [45], (9) ethical and legal aspects related to booters [16, 18], and the impact of law enforcement operations on booters from a commercial perspective [7, 13].

Our contribution. In this first of its kind study, we shed light on

ISP DDoS Defense Toolbox

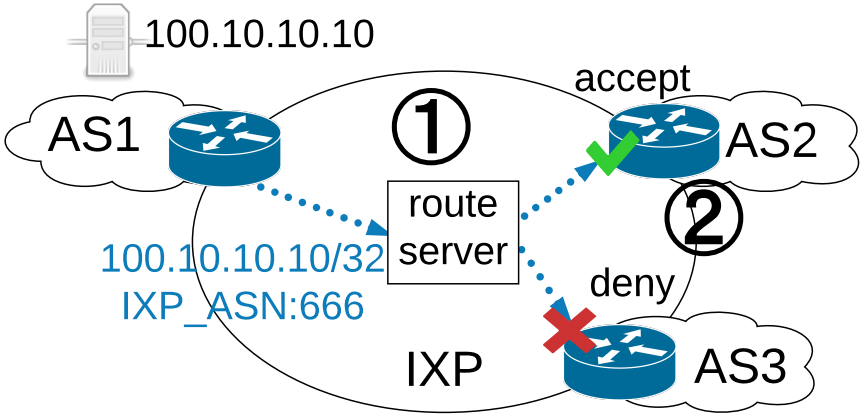
- Filters at arbitrary granularity
- Vendor-specific
- Per device config

- Carefree service
- Redirects traffic to scrubbing centers
- On-demand vs. always on

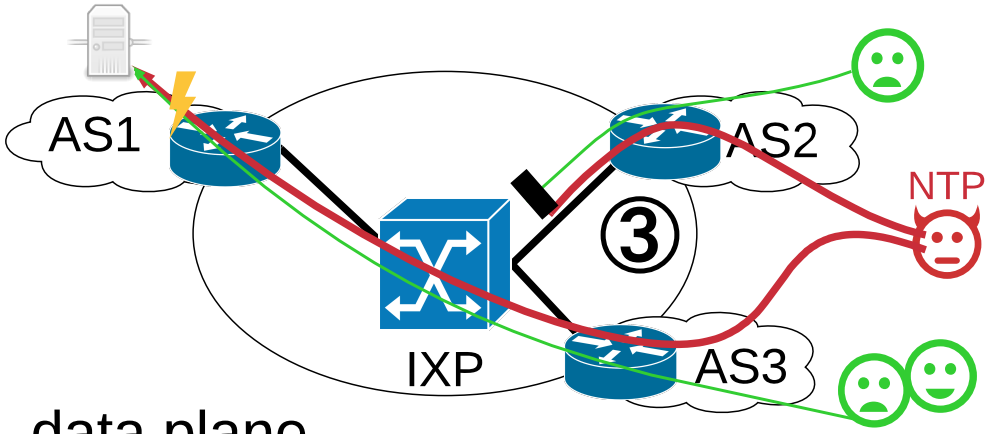
- Configures rules at neighbor network
- Filters at arbitrary granularity
- Cooperation required

- Configures rules at neighbor network
- Filters at IP granularity
- Cooperation required

Traditional Blackholing at IXPs



control plane



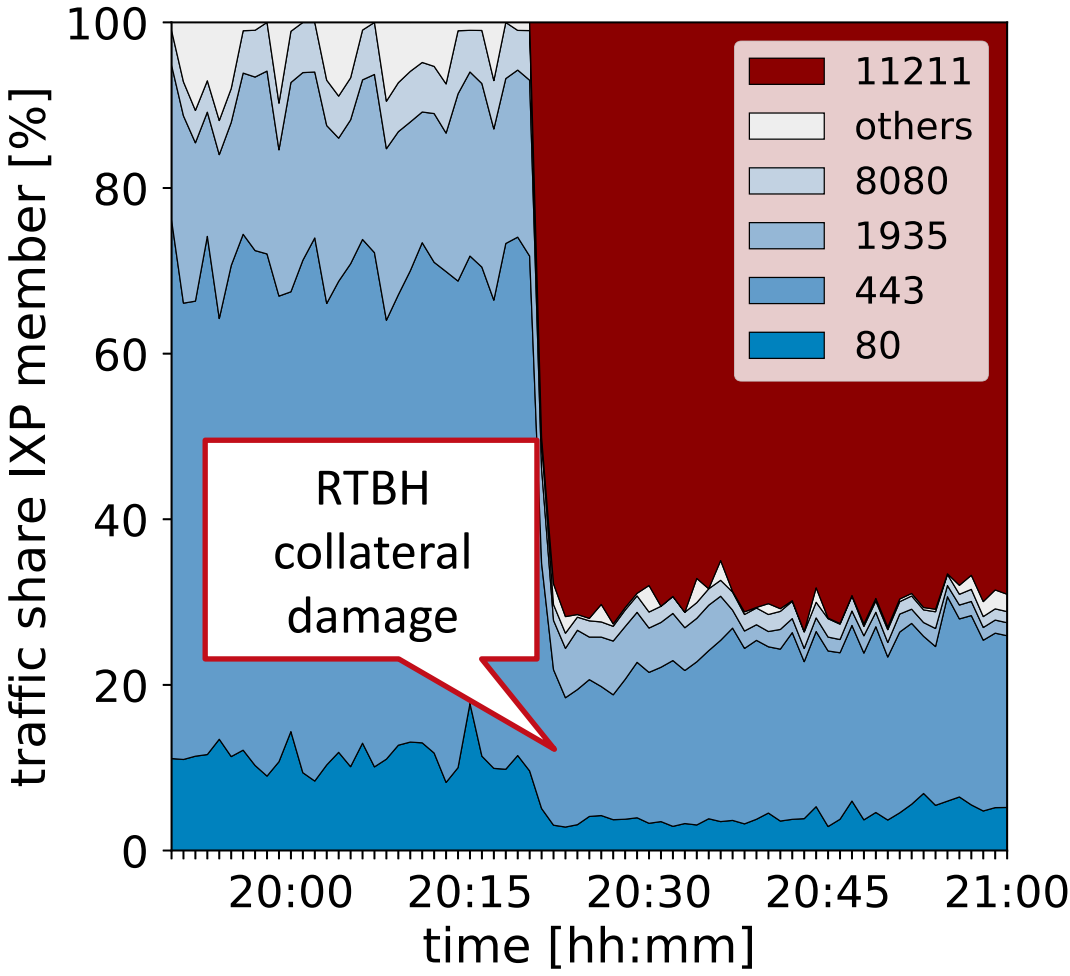
data plane

Traditional Blackholing – Limitations

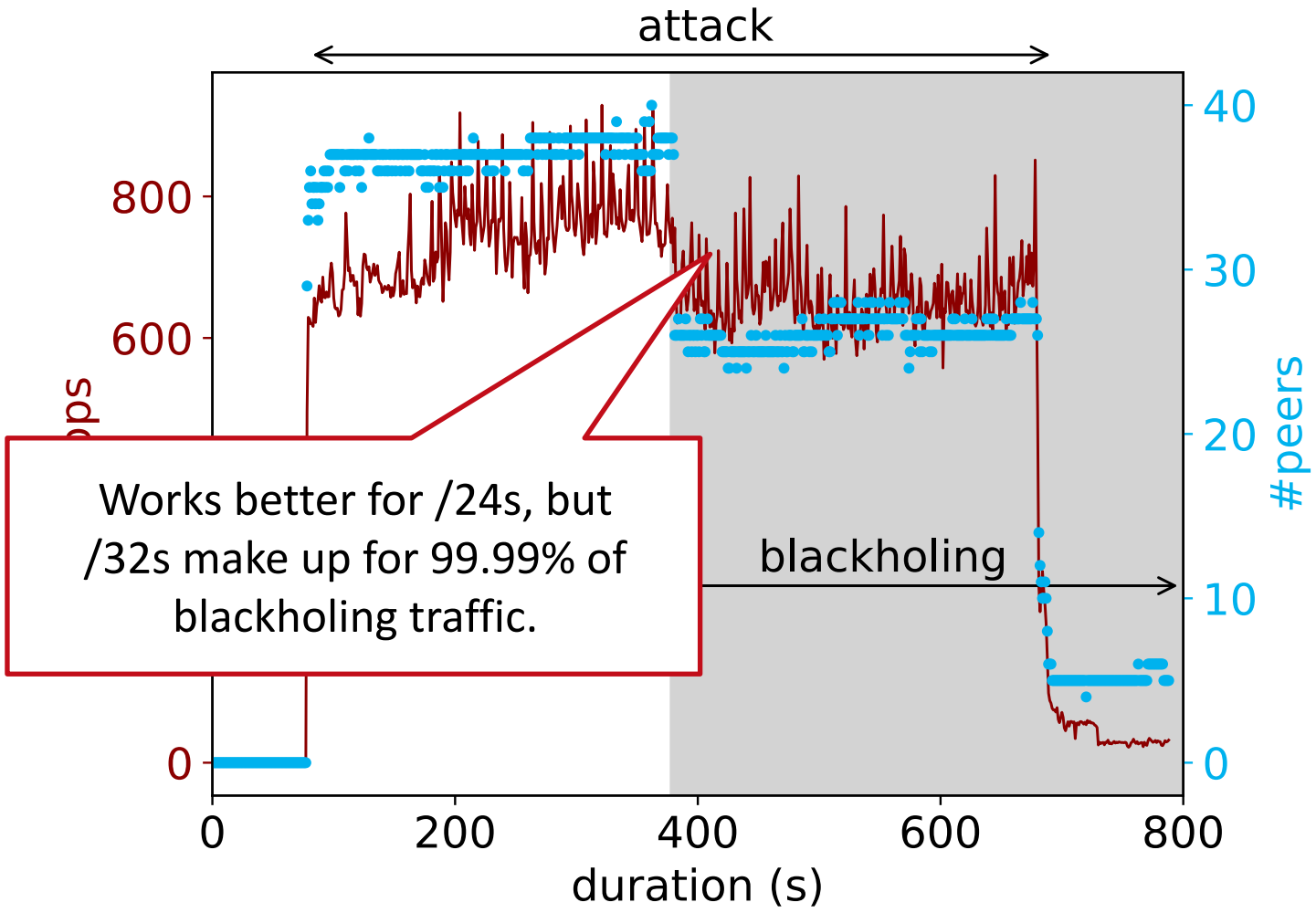
- → Relative traffic of 40GE IXP port
- → Mostly web traffic (80, 443, …)
- → Attack 70% memcached traffic
- → Still significant share of web traffic

→**Collateral damage!**

→**Granularity too coarse!**



Blackholing – Limitations



Blackhole for /32 → Traffic drops from 800 to 600 Mbps → Peers: 38 to 26

Advanced Blackholing Requirements

→ Granularity

- Fine-grained filtering (src/dst header fields)

→ Signaling complexity

- Easy to use, short setup time

→ Cooperation

- Lower levels of cooperation among the involved parties

→Telemetry

→ Feedback on the state of the attack at any time

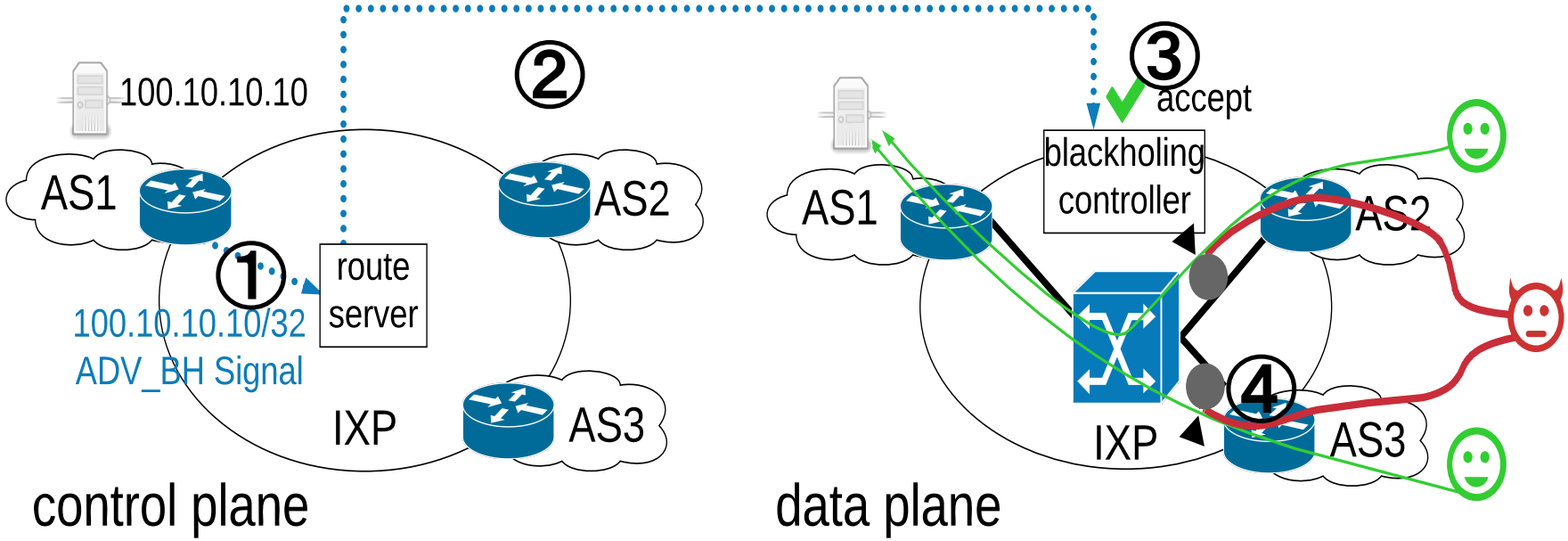
→Scalability

→ Scale in terms of performance, filters, reaction time, config complexity

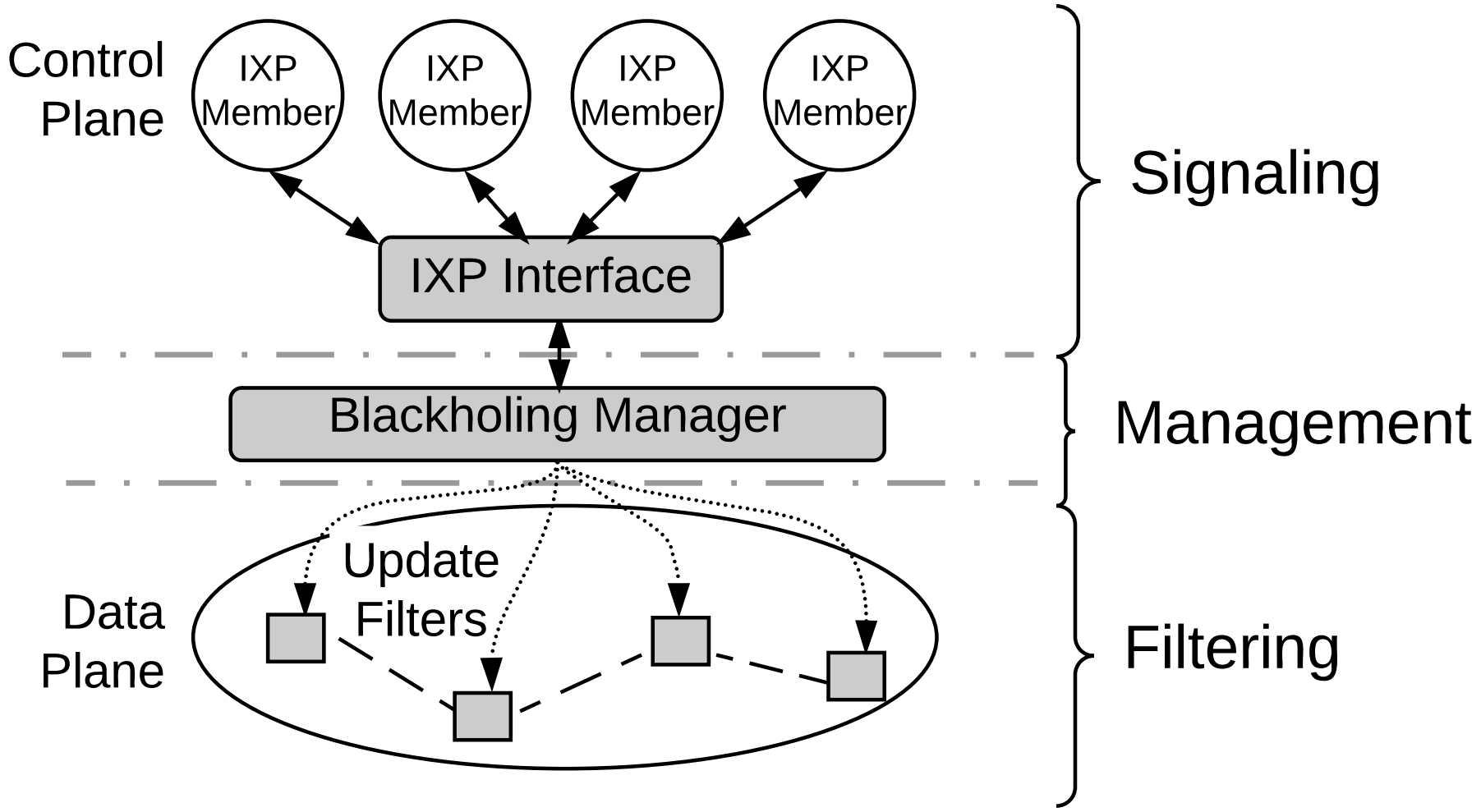
→ Cost

→ Meeting all requirements with min. invest (CAPEX & OPEX)

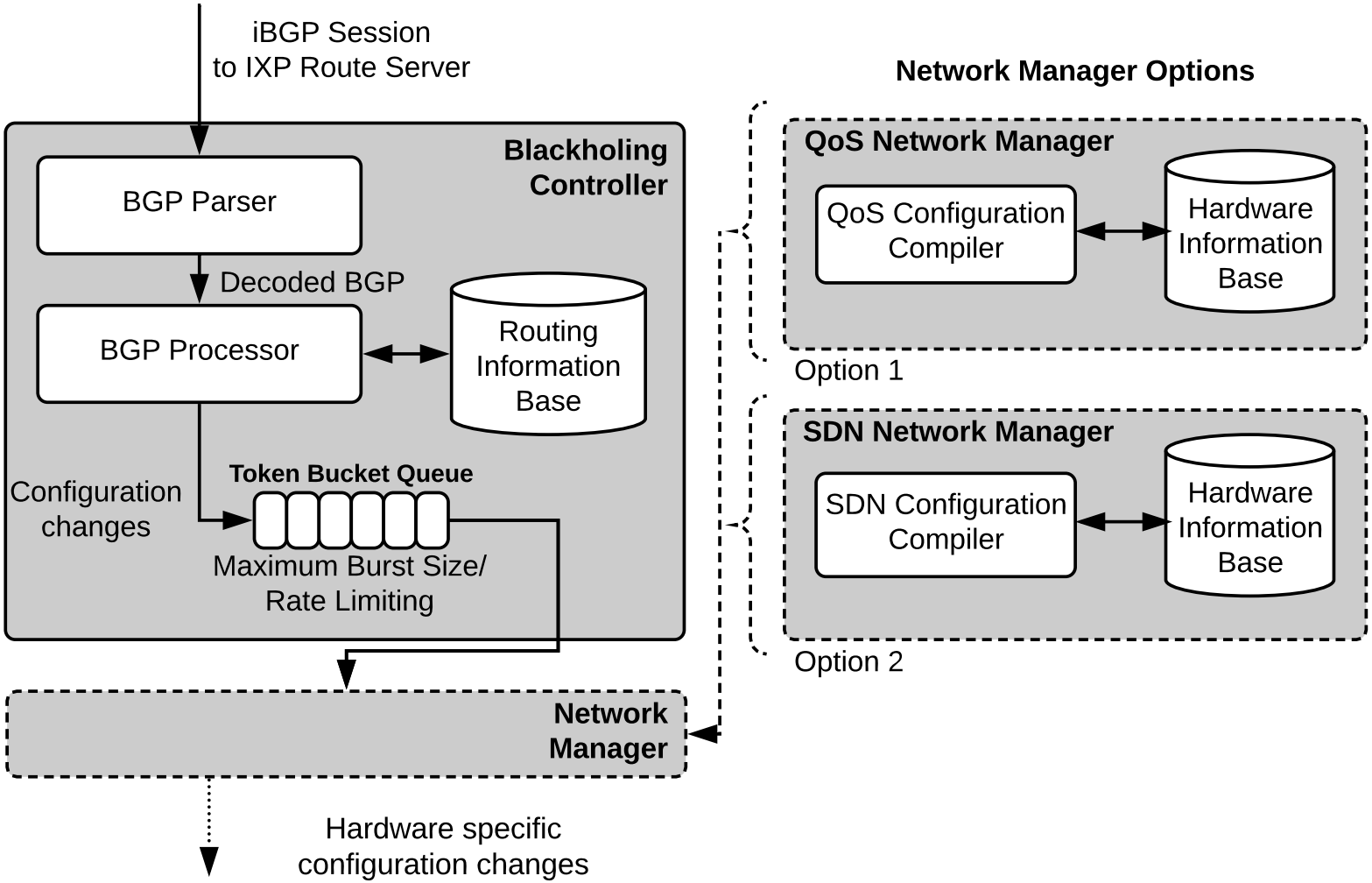
Advanced Blackholing System



Advanced Blackholing System



Advanced Blackholing Signaling (BGP part)



Building Blocks

✓ → **Granularity**

- UDP, TCP, Ports, …

✓ → **Telemetry**

- Monitoring with statistics

✓ → **Signaling complexity**

- BGP communities or API

✓ → **Scalability**

- Line-rate in hardware

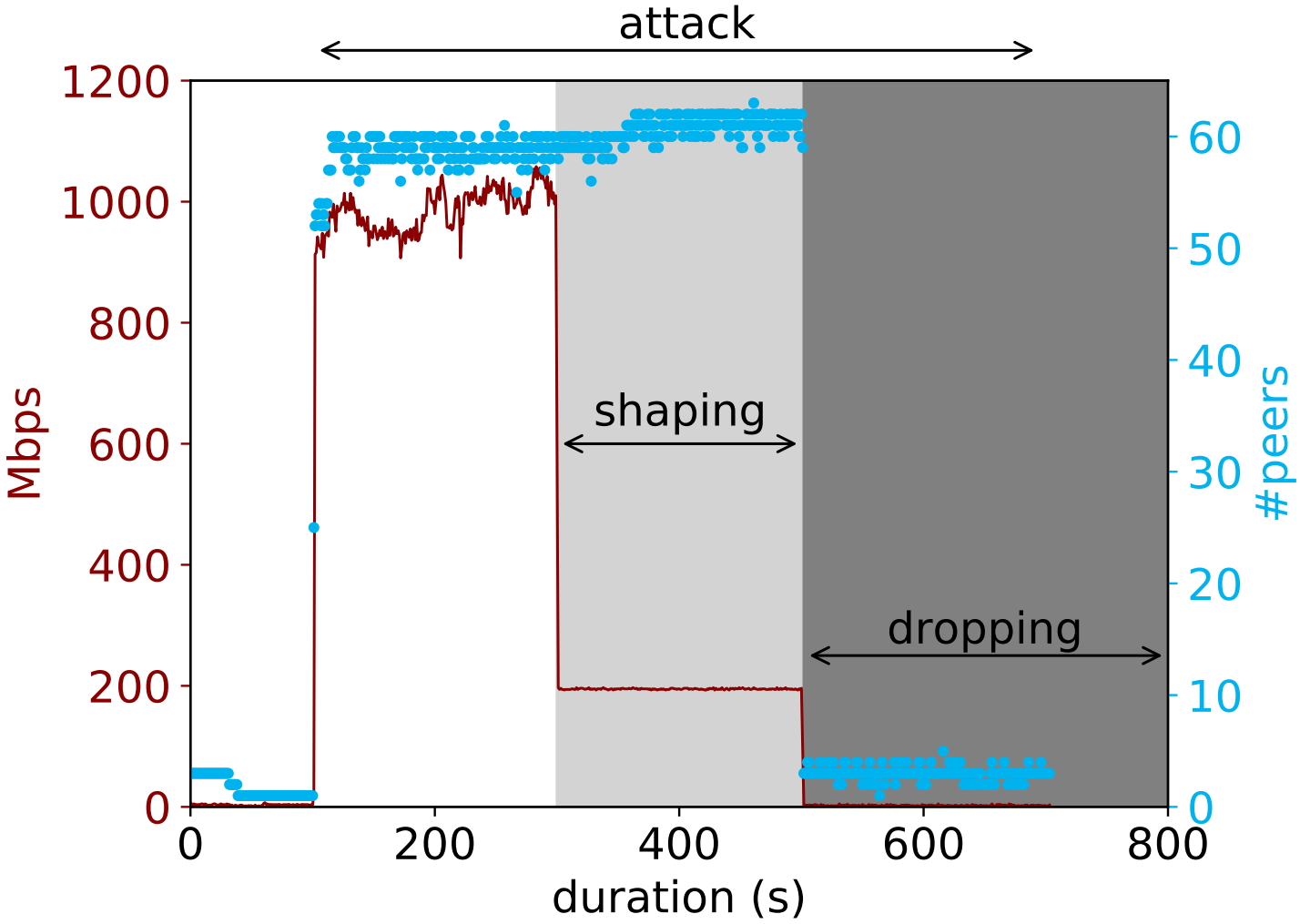
✓ → **Cooperation**

- Enforced by IXP

✓ → **Cost**

- Implemented in existing hardware

Advanced Blackholing how "effective" is it?



Drop / Shape UDP NTP → Traffic 1000 to 200 to 0 Mbps → Peers: 60 to 0

More Details...

Stellar: Network Attack Mitigation using Advanced Blackholing

Christoph Dietzel
TU Berlin/DE-CIX
christoph@inet.tu-berlin.de

Matthias Wichtlhuber
DE-CIX
matthias.wichtlhuber@rnd.de-cix.net

Georgios Smaragdakis
TU Berlin
georgios@inet.tu-berlin.de

Anja Feldmann
Max Planck Institute for Informatics
anja@mpi-inf.mpg.de

ABSTRACT

Network attacks, including Distributed Denial-of-Service (DDoS), continuously increase in terms of bandwidth along with damage (recent attacks exceed 1.7 Tbps) and have a devastating impact on the targeted companies/governments. Over the years, mitigation techniques, ranging from blackholing to policy-based filtering at routers, and on to traffic scrubbing, have been added to the network operator's toolbox. Even though these mitigation techniques provide some protection, they either yield severe collateral damage, e.g., dropping legitimate traffic (blackholing), are cost-intensive, or do not scale well for Tbps level attacks (ACL filtering, traffic scrubbing), or require cooperation and sharing of resources (Flowspec).

In this paper, we propose Advanced Blackholing and its system realization Stellar. Advanced blackholing builds upon the scalability of blackholing while limiting collateral damage by increasing its granularity. Moreover, Stellar reduces the required level of cooperation to enhance mitigation effectiveness. We show that fine-grained blackholing can be realized, e.g., at a major IXP, by combining available hardware filters with novel signaling mechanisms. We evaluate the scalability and performance of Stellar at a large IXP that interconnects more than 800 networks, exchanges more than 6 Tbps traffic, and witnesses many network attacks every day. Our results show that network attacks, e.g., DDoS amplification attacks, can be successfully mitigated while the networks and services under attack continue to operate untroubled.

is generated and steered towards a target service to make it unavailable. Once the network links to the target are congested due to the DDoS attack, legitimate traffic that traverses the same links is also affected.

DDoS threats are continuously increasing in terms of volume, frequency, and complexity. While the largest observed and publicly reported attacks were between 50 to 200 Gbps before 2015 [59, 60, 70], current peaks are an order of magnitude higher and exceeded 1 Tbps [9, 48] in 2016, and 1.7 Tbps [57] in early 2018. We also observe a massive rise in the number of DDoS attacks. Jonker et al. [41] report that a third of all active /24 networks were targeted by DDoS attacks between 2016 and 2017. Similar observations are reported by the security industry [3, 19]. A particularly prominent DDoS attack type is amplification attacks [64, 65]. They take advantage of protocol design flaws, whereby a relatively small request triggers a significantly larger response. With a spoofed source IP address [49] the response traffic is amplified and reflected to the target. Vulnerable protocols include classical protocols such as NTP, DNS, and/or SNMP [20, 64], as well as relatively new protocols, e.g., DNSSEC [74] and memcached [5, 57]. Amplification factors of up to 50,000× have been witnessed in the wild [73]. To exemplify, a request of 15 bytes can trigger a 750 Kbytes response.

1.1 DDoS Mitigation: State of the Art


Q&A - Discussion - Feedback