DDoS Attacks, Booter Services & DDoS Mitigation at IXPs

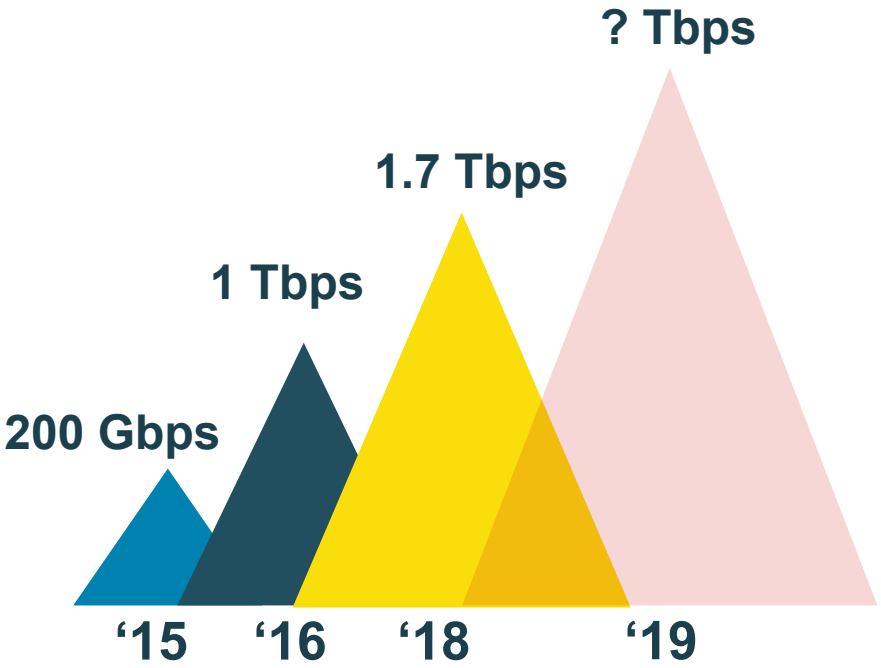
Daniel Kopp
Products & Research

DE-CIX

Where networks meet

www.de-cix.net

DDoS Attacks



NETSCOUT

Attack Map | Archives | About

BLOG HOME | CORPORATE SITE | RSS

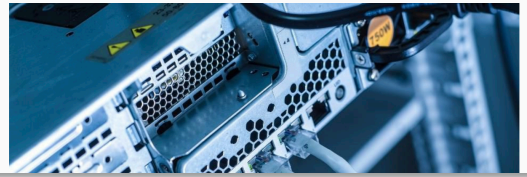
NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us

Carlos Morales on March 5, 2018.

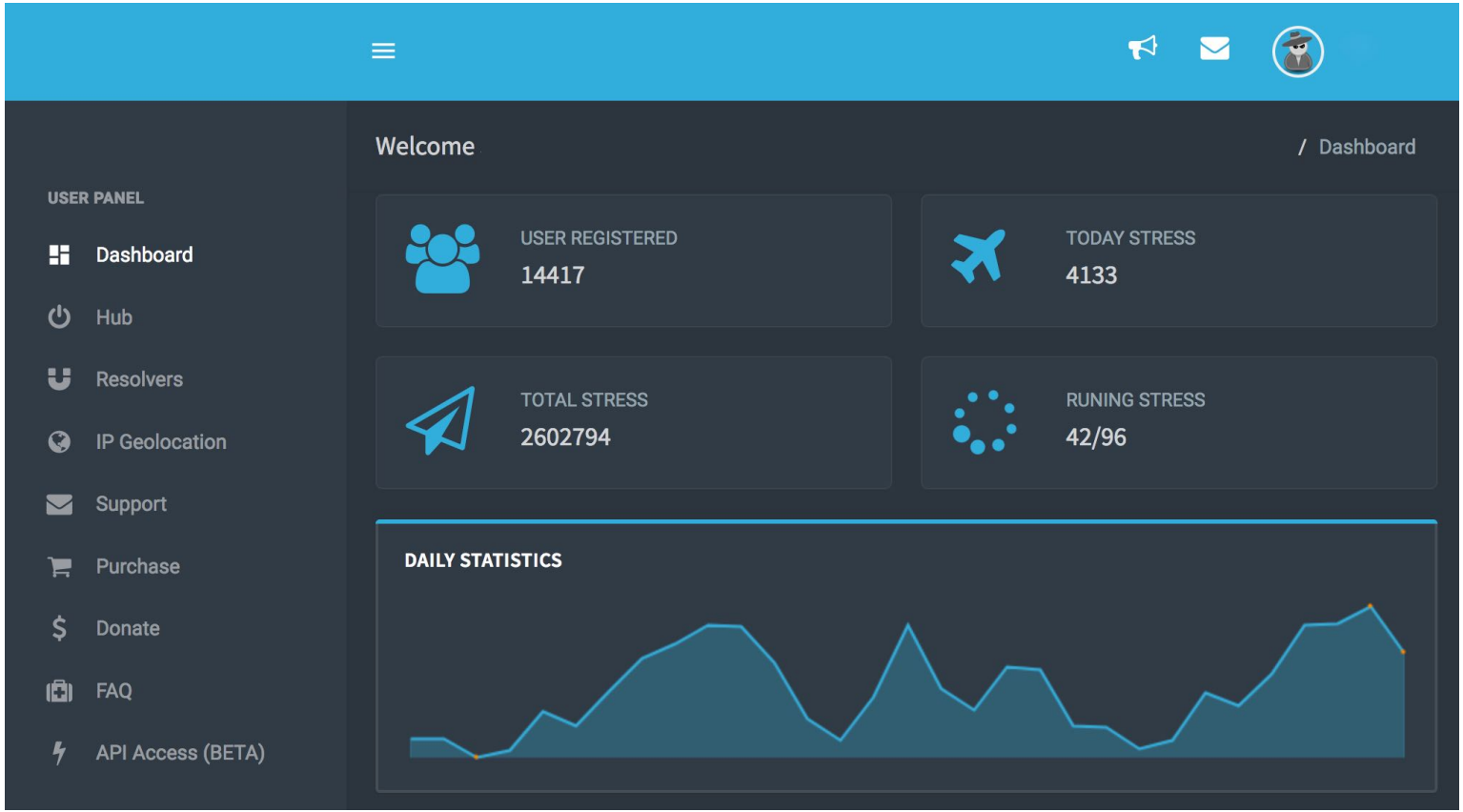
A Frightening New Kind Of DDoS Attack Is Breaking Records

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.



DDoS for Hire - Booter Services



Serviceplans

Dashboard
Boot
Tickets
Help
Purchase with BTC
Purchase with ETH

Welcome
Your reliable stresser.

Warning
You cannot purchase a new membership right now. Note: You already have a membership. You can buy when your current membership expire.

Available Packages - **Instant Delivery**

Silver	Gold	Platinum
$14/month	$19/month	$29/month
600 seconds boot time	1200 seconds boot time	1800 seconds boot time
All methods	All methods	All methods
1 concurrent	1 concurrent	1 concurrent
30 days	30 days	30 days
Instant delivery	Instant delivery	Instant delivery
PURCHASE	PURCHASE	PURCHASE

VIP Silver	VIP Gold	VIP Platinum
$79/month	$89/month	$119/month
4800 seconds boot time	7200 seconds boot time	10800 seconds boot time
All methods	All methods	All methods
1 concurrent	1 concurrent	1 concurrent
30 days	30 days	30 days
Instant delivery	Instant delivery	Instant delivery
PURCHASE	PURCHASE	PURCHASE

Order Confirmation

Description: Add Service access

Seconds: 1200 (20 Minutes)
Concurrents: 1 (Simultaneous Running Floods)
Targets per Day: 40 (Resets every day at midnight, our server time)
Length: 1 Months
VIP Access: ✖
API Access: ✖
Price: $22.80 USD
Crypto Price: $19.38 USD

PROCEED TO CHECKOUT

Order Confirmation

Description: Add Service access

Seconds: 1200 (20 Minutes)
Concurrents: 1 (Simultaneous Running Floods)
Targets per Day: 40 (Resets every day at midnight, our server time)
Length: 1 Months
VIP Access: ✔
API Access: ✖
Price: Cannot exceed $75.00 USD, crypto checkout available only!
Crypto Price: $178.84 USD

PROCEED TO CHECKOUT

DDoS Order

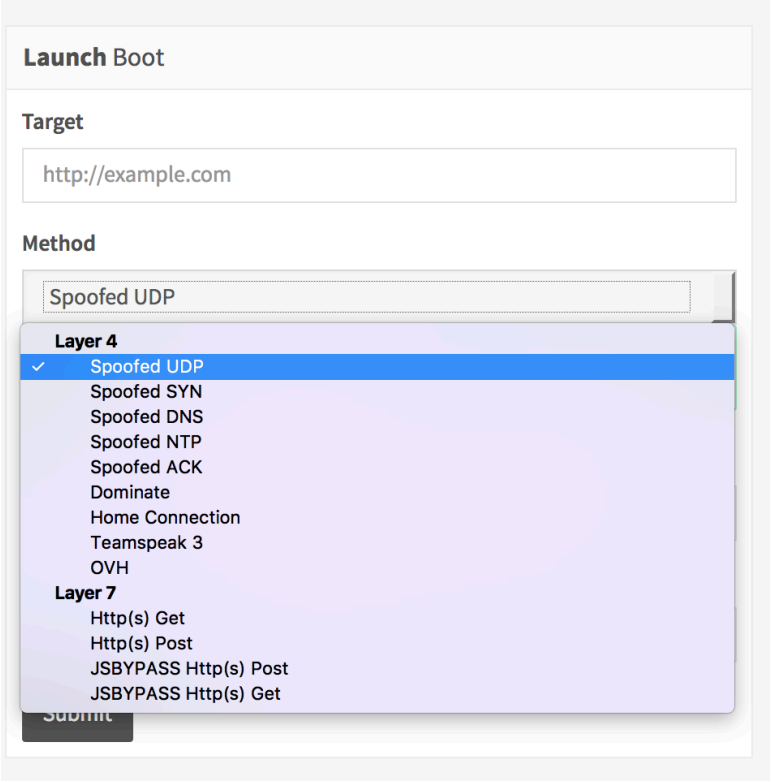
→ **Flat rate** for DDoS attacks

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

→ 10 - 20 **different types**

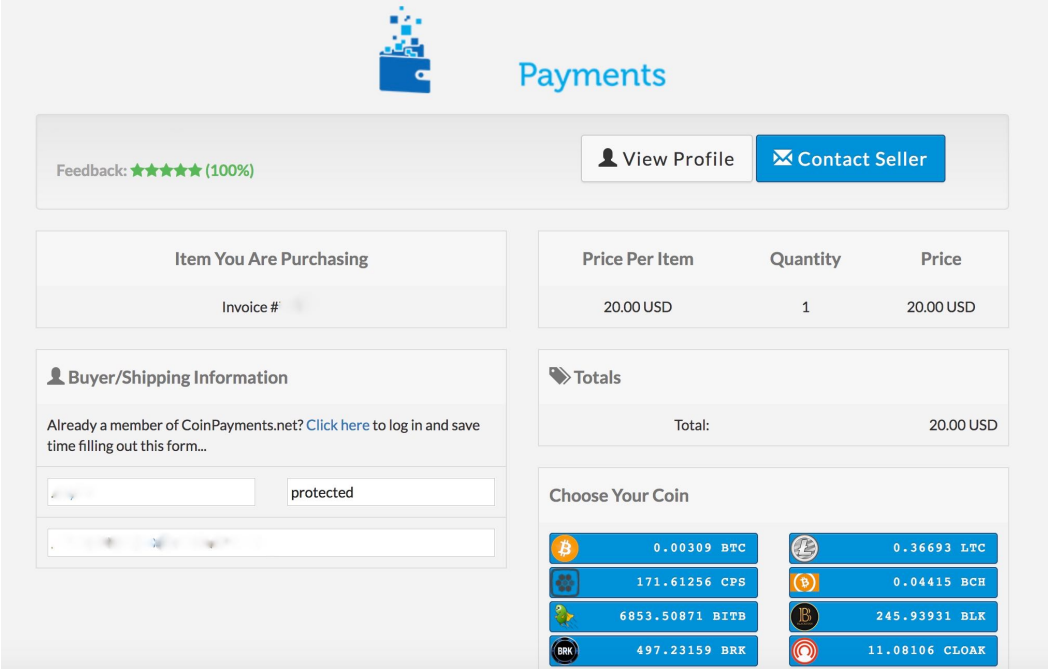
- Application → high pps
- Amplification → high bandwidth

→ Claim to offer **5 - 100 Gbit/s**



Payment

- → **Fake services** exist
- → Payment with **crypto currency**
- → Payment and activation takes time
- → Prices **$20 - $200**

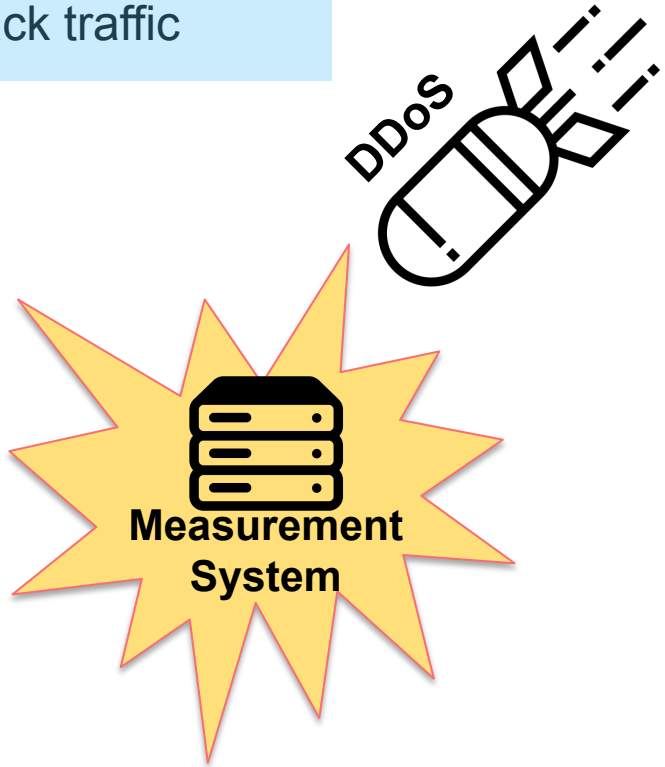


Measurement System Motivation

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



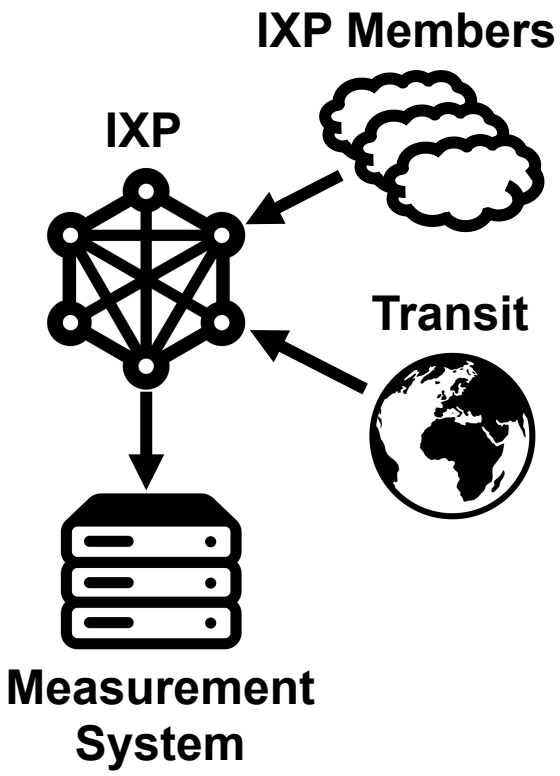
Measurement System and Setup

→ **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



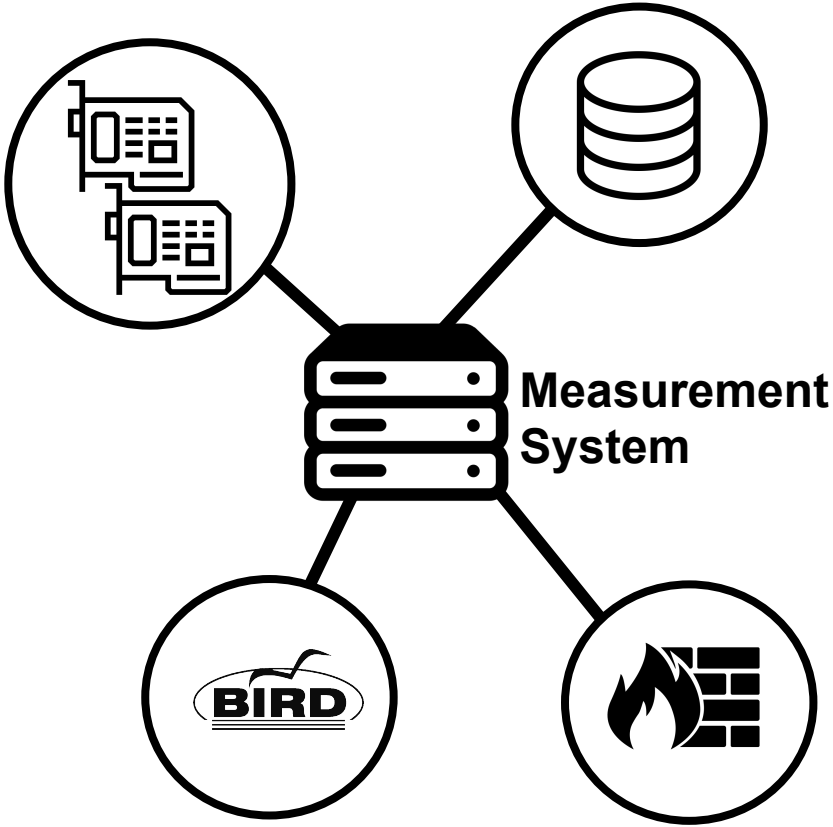
Measurement System and Setup

→ **Hardware**

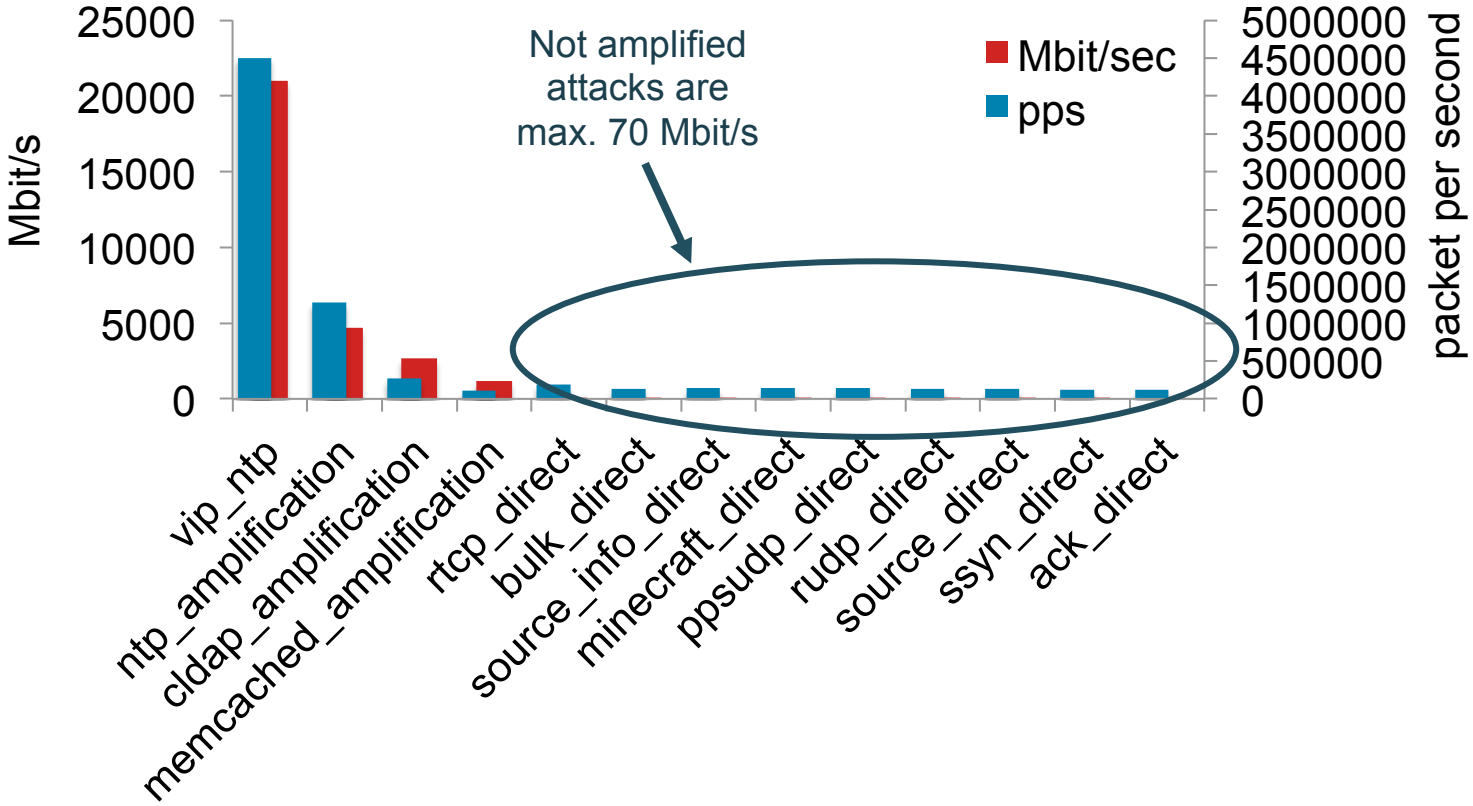
- Dedicated second NIC as mirror
- Fast write speed: SAS RAID-0
- Dedicated Raid Controller
- Singe core performance

→ **System Setup**

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

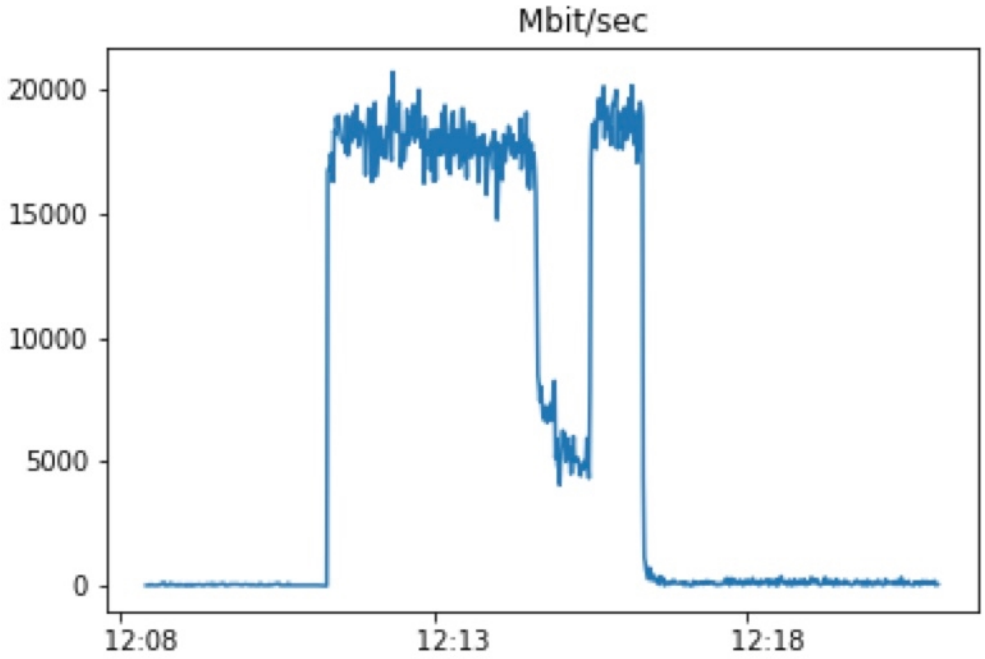


DDoS Attacks - Overview



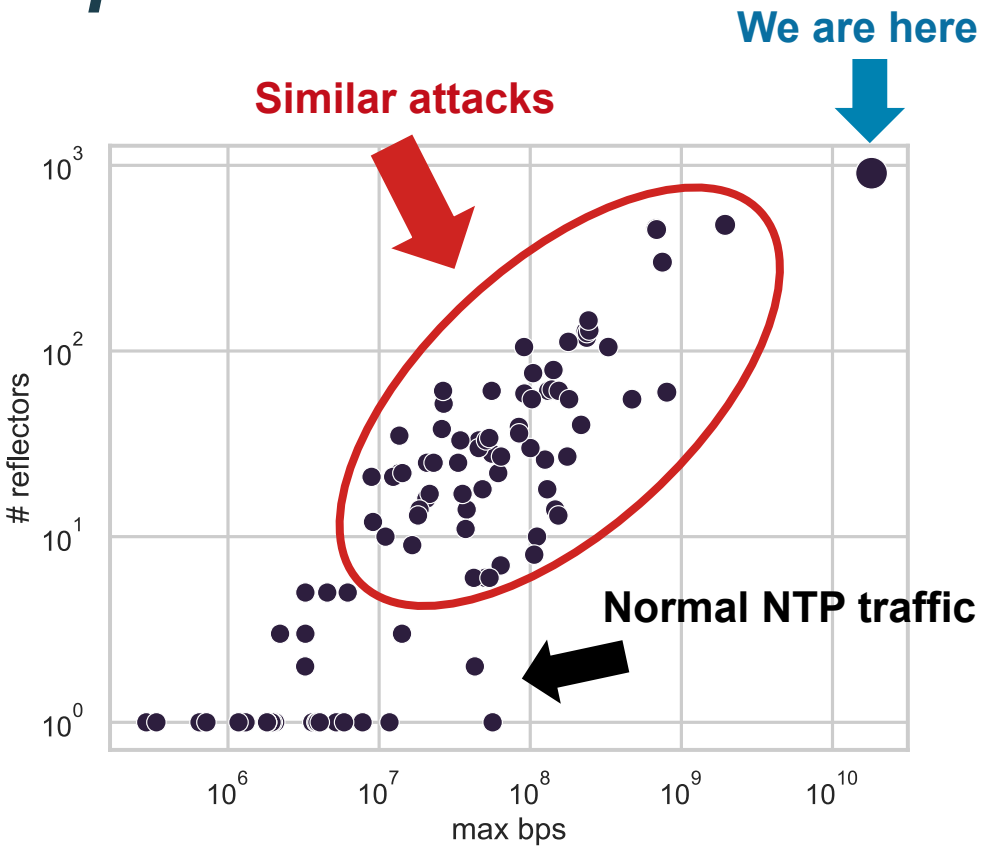
DDoS - NTP Reflection

- → 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 Attack Landscape

- ➔ We profile our attack traffic
  - Number of reflectors
  - Max bytes per second
- ➔ Map it to all other NTP traffic at the same time
- ➔ At least 60 possible similar attacks



Booter Services vs. FBI

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

THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT | OUR AGENCY | PRIORITIES | NEWS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Thursday, December 20, 2018

Criminal Charges Filed in Los Angeles and Alaska in Conjunction with Seizures Of 15 Websites Offering DDoS-For-Hire Services

The Justice Department announced today the seizure of 15 internet domains associated with DDoS-for-hire services, as well as criminal charges against three defendants who facilitated the computer attack platforms.

The sites, which offered what are often called "booter" or "stresser" services, allowed paying users to launch powerful

DE-CIX Product Development - Next Generation Blackholing

Where networks meet

www.de-cix.net

ISP DDoS Defense Toolbox

ACL

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

TSS

(Traffic Scrubbing Services)

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

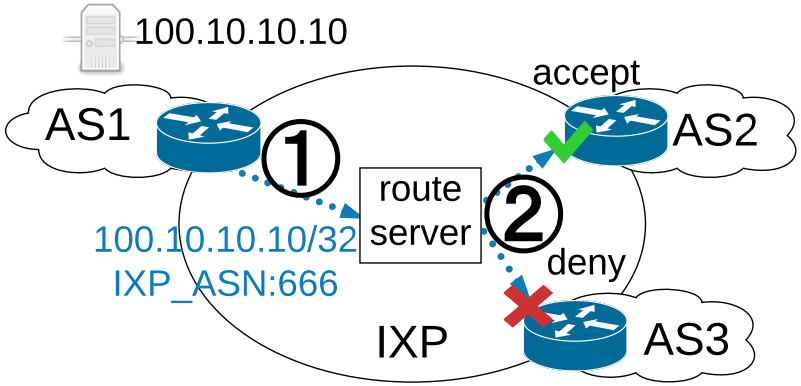
Flowspec

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

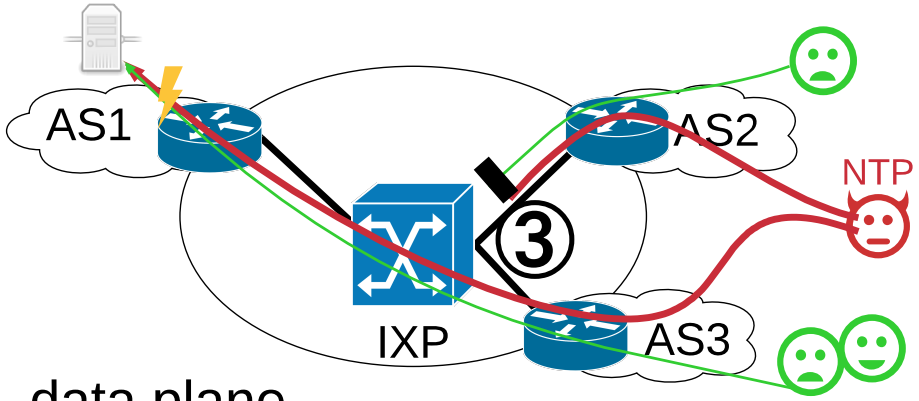
RTBH

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

Traditional Blackholing at IXPs



control plane



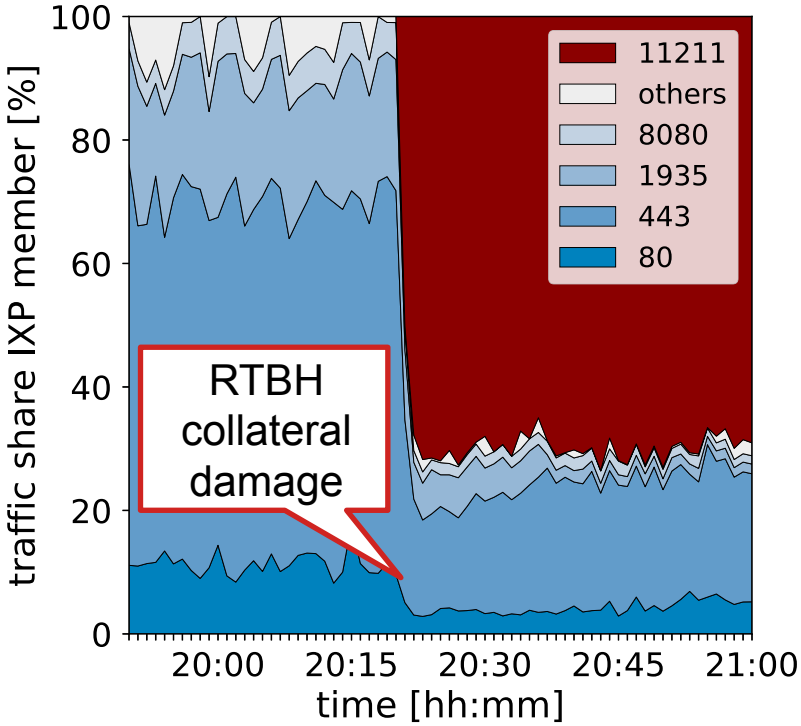
data plane

Blackholing – Limitations

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

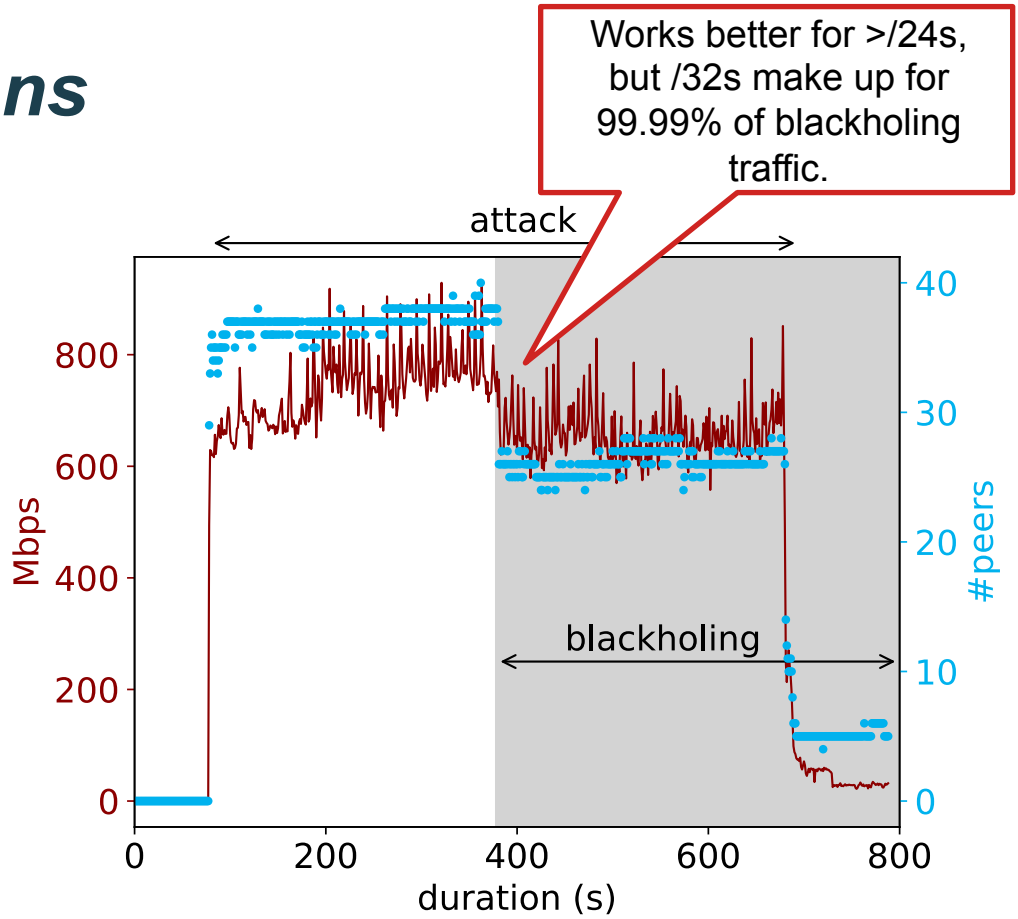
→**Collateral damage!**

→**Granularity too coarse!**



Blackholing – Limitations

- → How “ineffective“ can it be?
  - NTP DDoS attack
  - AS at IXP via ML peering
  - Attacks for 10 min to /32
- → Drop all traffic to /32
- → Traffic: 800 to 600 Mbps
- → Peers: 38 to 26
- → **Signaling too complex!**



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

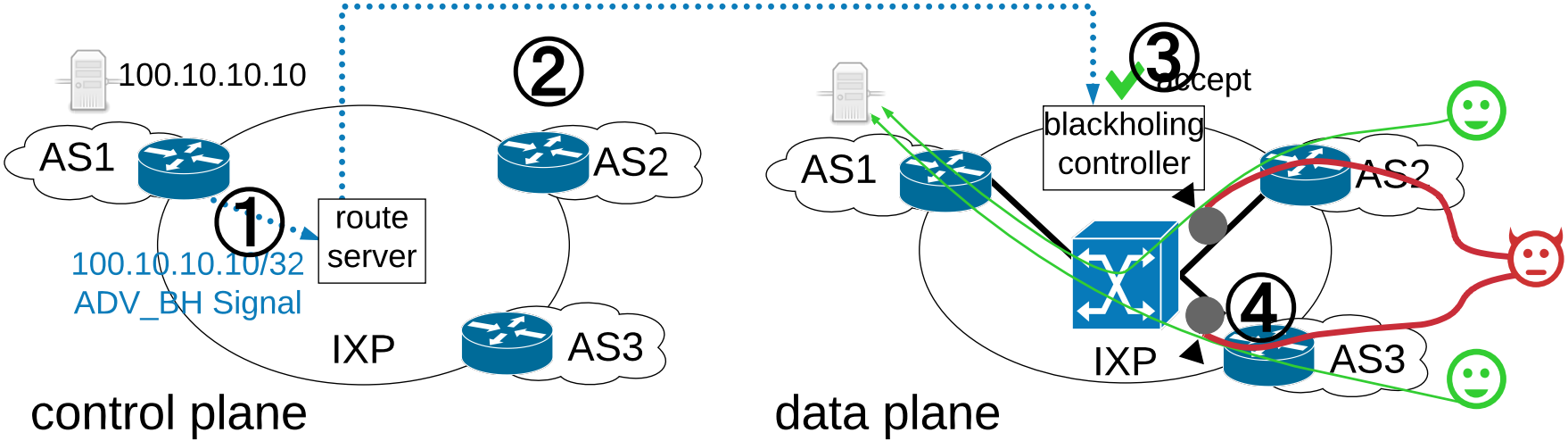
→Scalability

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

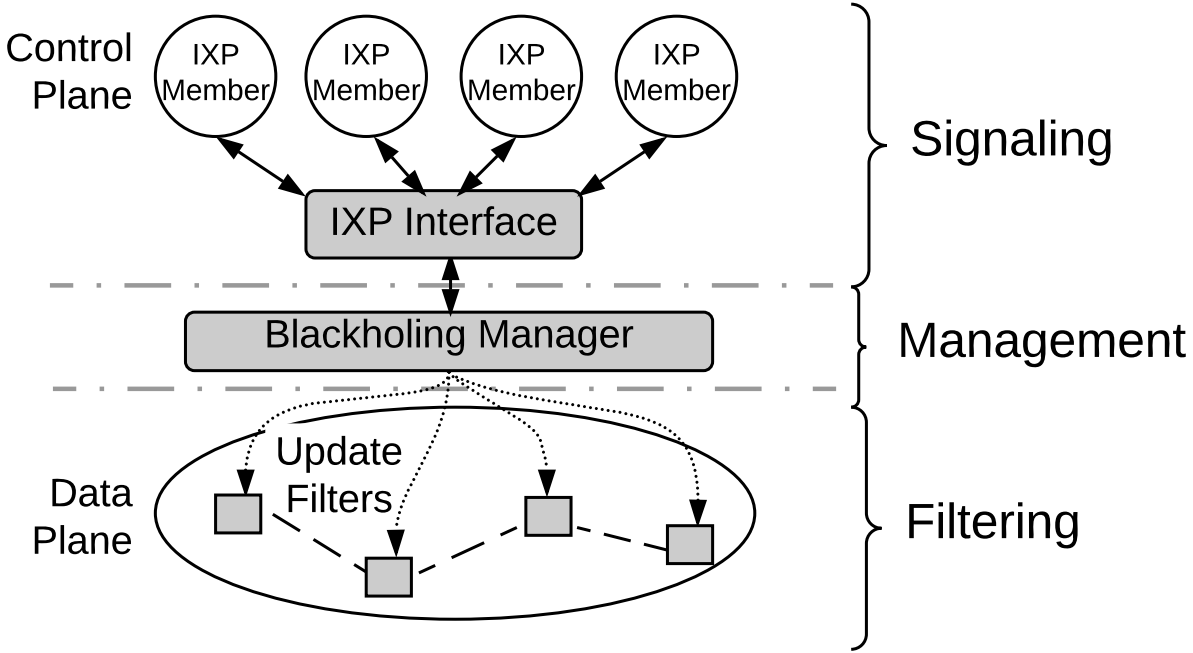
→ Cost

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

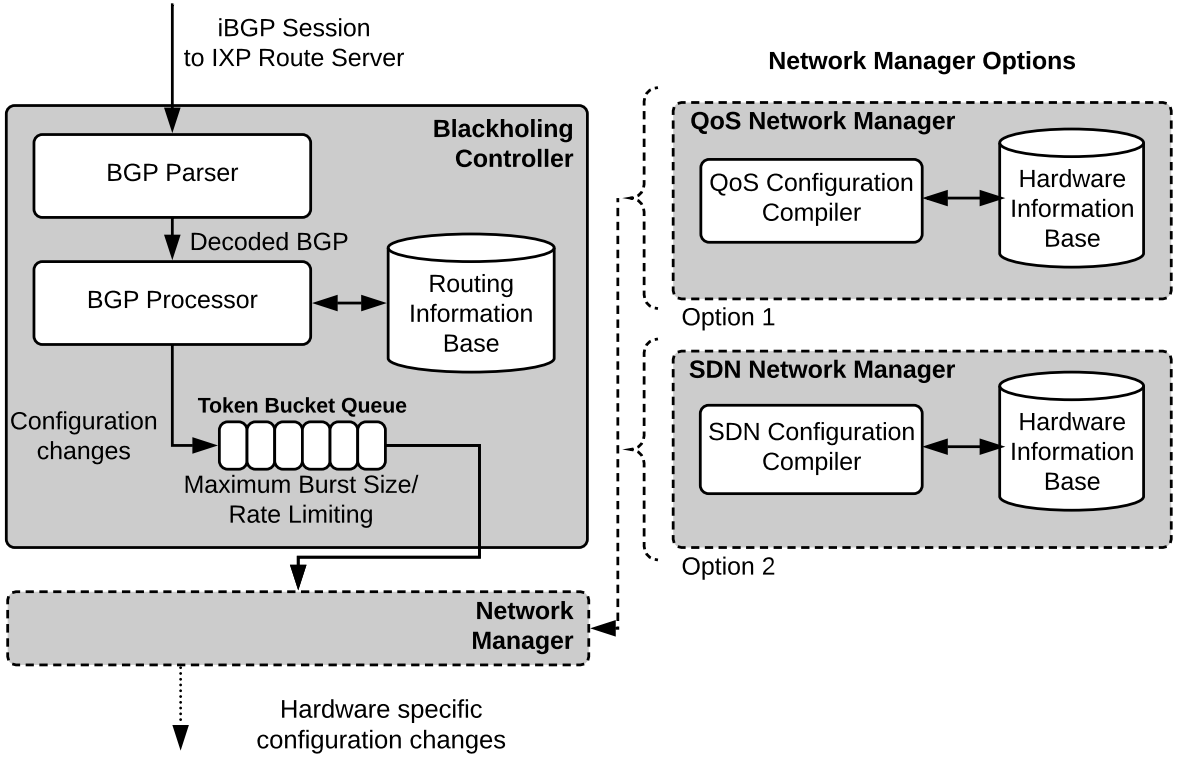
Advanced Blackholing System



Advanced Blackholing System



Advanced Blackholing Signaling (BGP part)



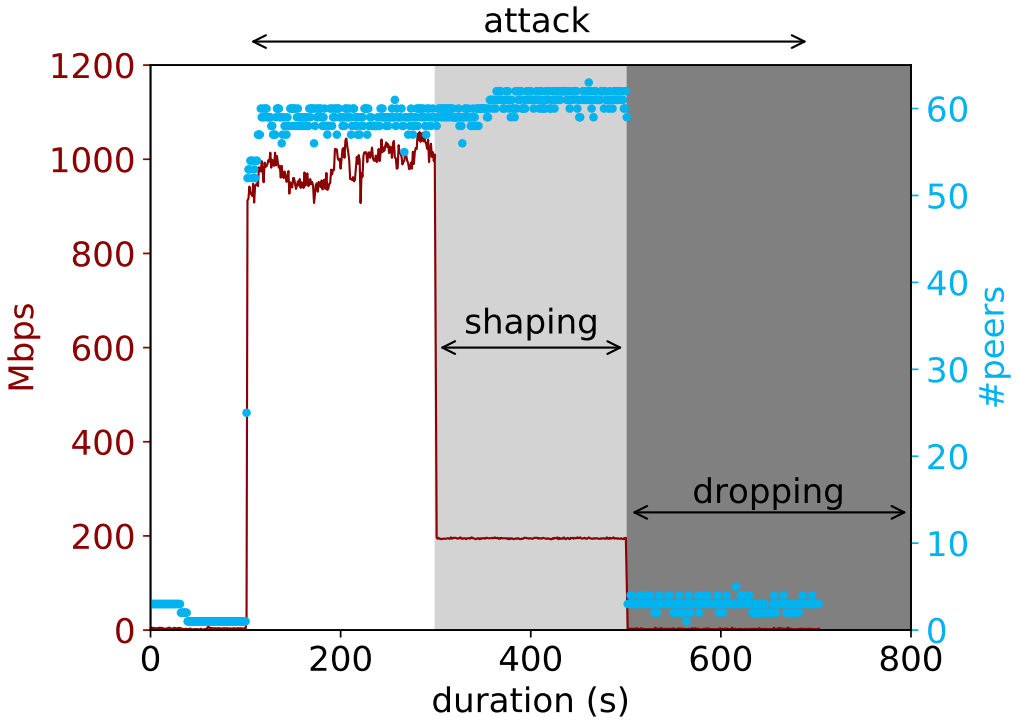
Building Blocks

- ✓ → Granularity
  - UDP, TCP, Ports, …
- ✓ → Signaling complexity
  - BGP communities or API
- ✓ → Cooperation
  - Enforced by IXP
- ✓ → Telemetry
  - Monitoring with statistics
- ✓ → Scalability
  - Line-rate in hardware
- ✓ → Cost
  - Implemented in existing hardware

Measurement Experiment

- ➔ How “effective“ is it?
  - NTP DDoS attack
  - AS at IXP via ML peering
  - Attacks for 10 min to /32

- ➔ Drop / shape UDP NTP
- ➔ Traffic: 1000 to 200 to 0 Mbps
- ➔ Peers: 60 to (almost) 0



Takeaways

→ **Booter Services**

- Popular on demand, **DDoS for hire for anybody**
- Usually max. 5 - 20 Gbit/sec

→**Traditional DDoS Mitigation at IXPs (Blackholing)**

- Limited effectiveness for common /32 announcements
- **Last resort** at the event of DDoS attacks

→ **Next Generation Blackholing**

- Meaningful addition to the IXP DDoS mitigation options
- Fine-grained and **effective DDoS mitigation**

Q&A - Discussion - Feedback