

DDoS Attacks, Booter Services & DDoS Mitigation at IXPs

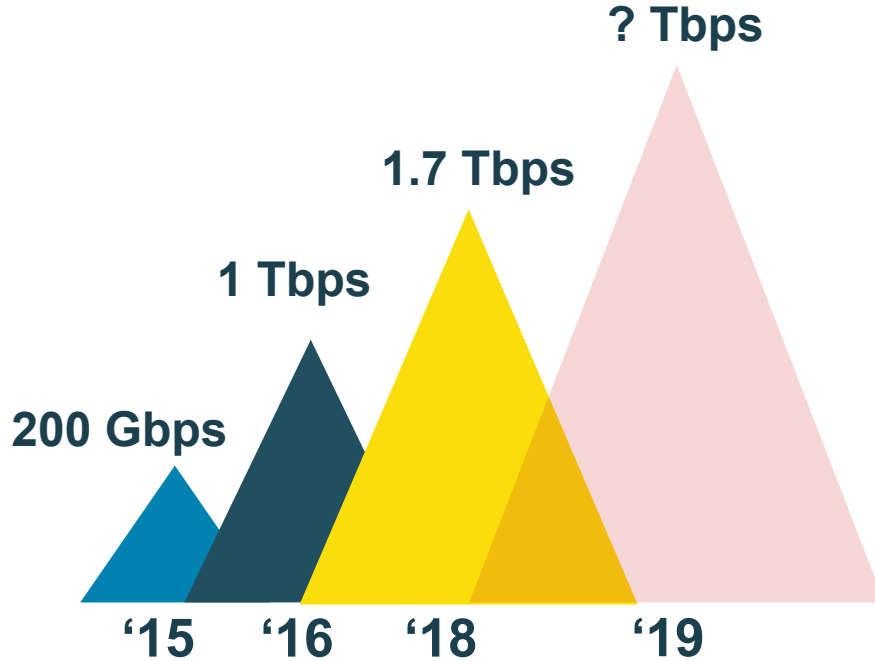


Where networks meet

*Daniel Kopp
Products & Research*

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

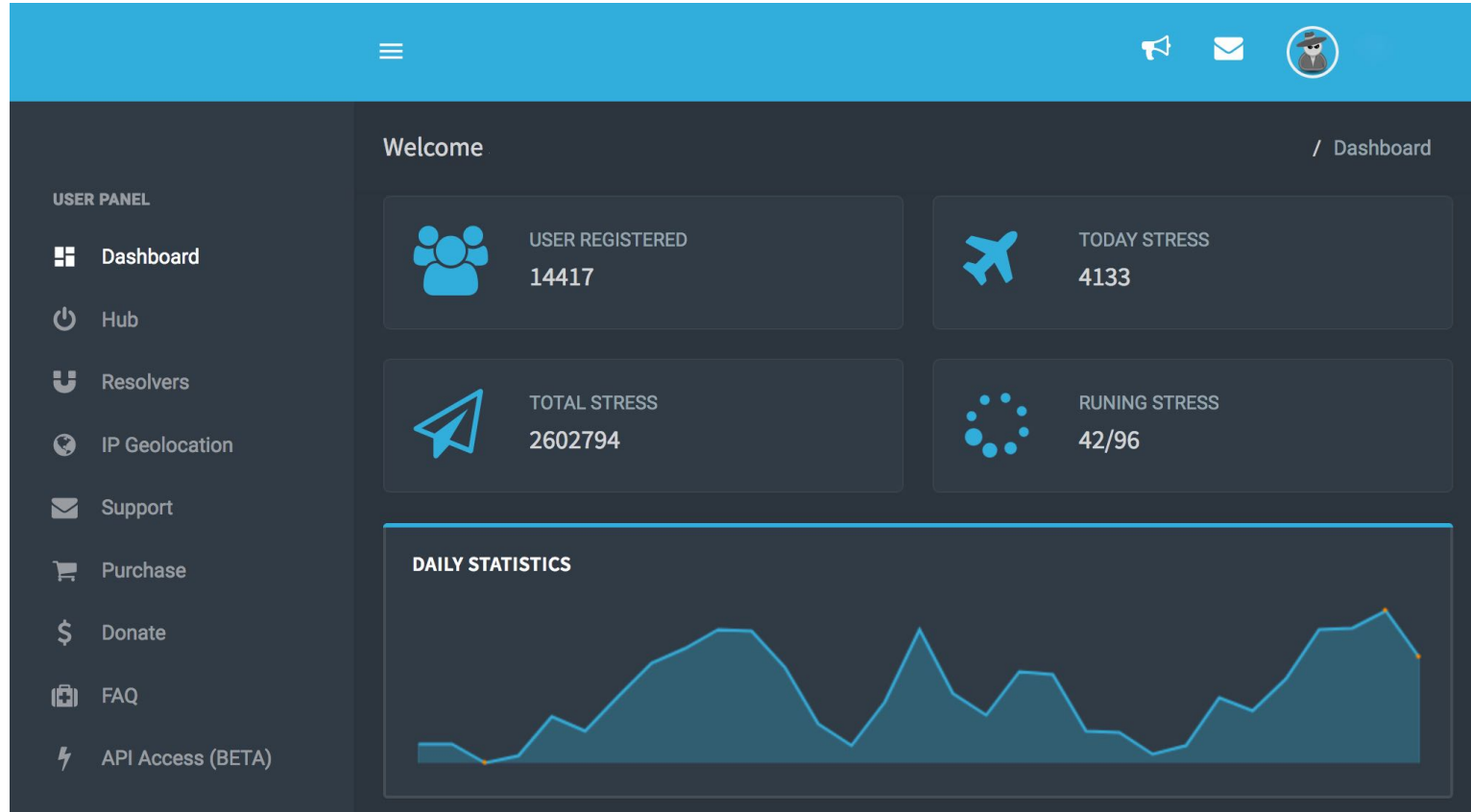
Security

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

- f 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.
- tw
- in



DDoS for Hire - Booter Services



Serviceplans

Welcome **John**
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 All methods 1 concurrent 30 days Instant delivery	1200 seconds boot time All methods 1 concurrent 30 days Instant delivery	1800 seconds boot time All methods 1 concurrent 30 days Instant delivery
PURCHASE	PURCHASE	PURCHASE

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

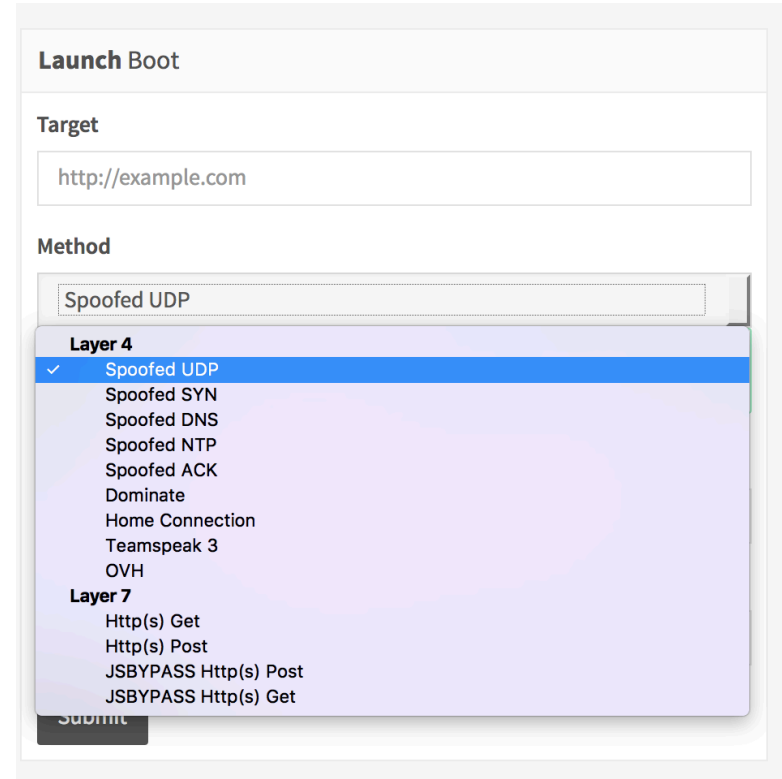
→ **Flat rate** for DDoS attacks

- 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**



The image shows a web interface for configuring a DDoS attack. The main heading is "Launch Boot". Below it, there is a "Target" field containing "http://example.com". Underneath is a "Method" dropdown menu currently set to "Spoofed UDP". A dropdown menu is open, showing a list of attack types categorized by layer. "Layer 4" is expanded, showing options like "Spoofed UDP" (which is selected with a checkmark), "Spoofed SYN", "Spoofed DNS", "Spoofed NTP", "Spoofed ACK", "Dominate", "Home Connection", "Teamspeak 3", and "OVH". Below "Layer 4" is "Layer 7", with options "Http(s) Get", "Http(s) Post", "JSBYPASS Http(s) Post", and "JSBYPASS Http(s) Get". A "Submit" button is visible at the bottom of the form.

Launch Boot

Target
http://example.com

Method
Spoofed UDP

Layer 4

- ✓ Spoofed UDP
- Spoofed SYN
- Spoofed DNS
- Spoofed NTP
- Spoofed ACK
- Dominate
- Home Connection
- Teamspeak 3
- OVH

Layer 7

- Http(s) Get
- Http(s) Post
- JSBYPASS Http(s) Post
- JSBYPASS Http(s) Get

Submit

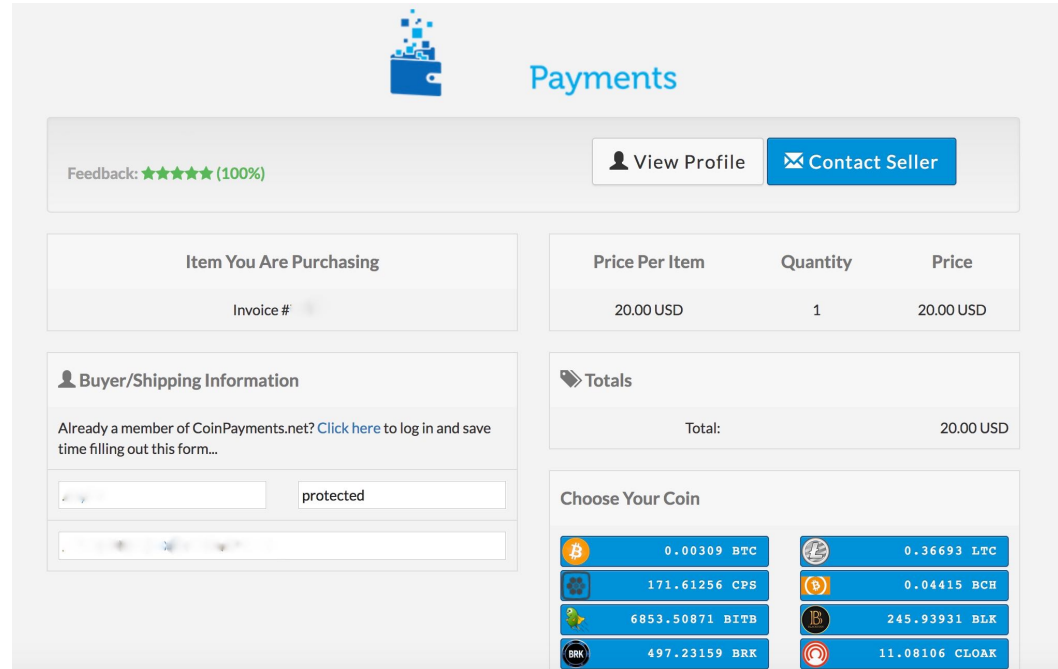
Payment

→ Fake services exist

→ Payment with **crypto currency**

→ Payment and activation takes
time

→ Prices **\$20 - \$200**



The screenshot shows a payment interface for a transaction. At the top, there is a blue icon of a wallet with a 'c' and the word 'Payments' in blue. Below this, there is a feedback section showing a 5-star rating (100%) and two buttons: 'View Profile' and 'Contact Seller'. The main transaction details are presented in a table with three columns: 'Item You Are Purchasing', 'Price Per Item', 'Quantity', and 'Price'. The item is 'Invoice #', the price is '20.00 USD', and the quantity is '1'. Below the table, there is a section for 'Buyer/Shipping Information' with a note about logging in and a form with a 'protected' label. To the right, there is a 'Totals' section showing a total of '20.00 USD'. At the bottom, there is a 'Choose Your Coin' section with a grid of buttons for different cryptocurrencies: BTC (0.00309), LTC (0.36693), CPS (171.61256), BCH (0.04415), BITB (6853.50871), BLK (245.93931), BRK (497.23159), and CLOAK (11.08106).

Item You Are Purchasing	Price Per Item	Quantity	Price
Invoice #	20.00 USD	1	20.00 USD

Feedback: ★★★★★ (100%)

[View Profile](#) [Contact Seller](#)

Buyer/Shipping Information

Already a member of CoinPayments.net? [Click here](#) to log in and save time filling out this form...

protected

Totals

Total: 20.00 USD

Choose Your Coin

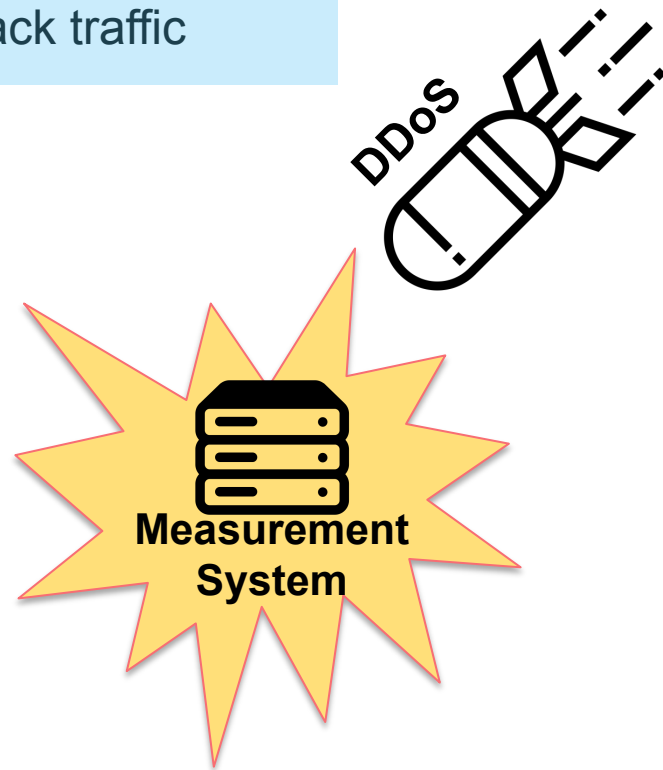
0.00309 BTC	0.36693 LTC
171.61256 CPS	0.04415 BCH
6853.50871 BITB	245.93931 BLK
497.23159 BRK	11.08106 CLOAK

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



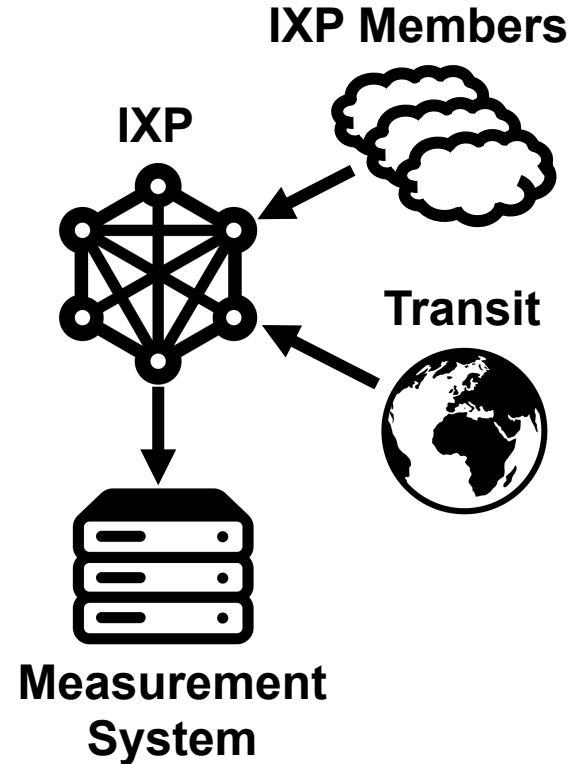
Measurement System and Setup

→ Internet Connectivity

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

→ Measurement Limitations

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



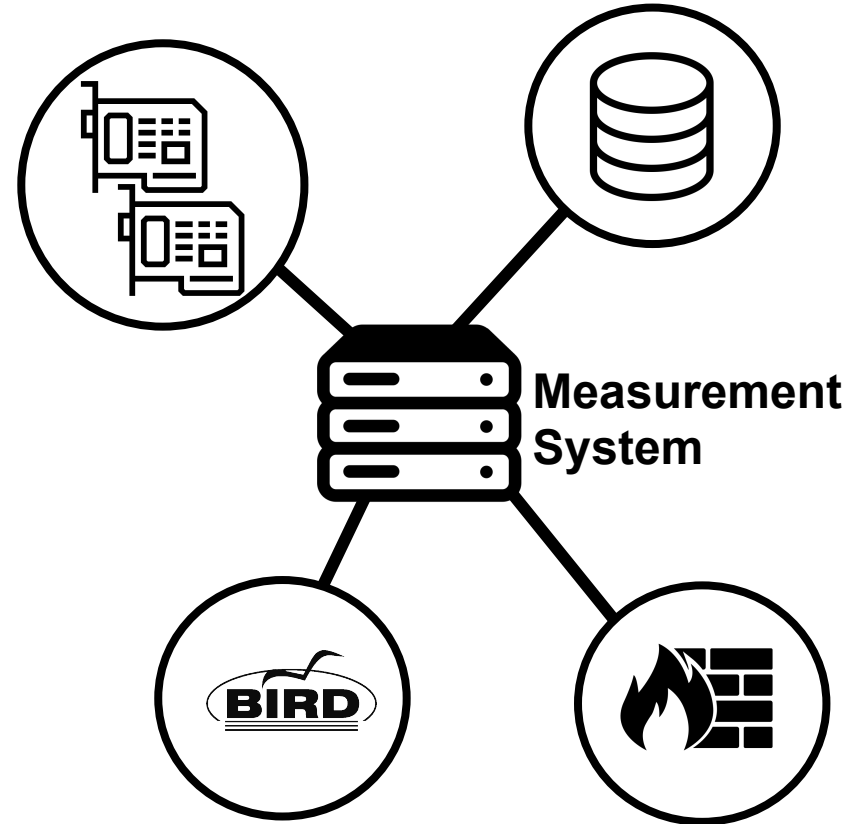
Measurement System and Setup

→ Hardware

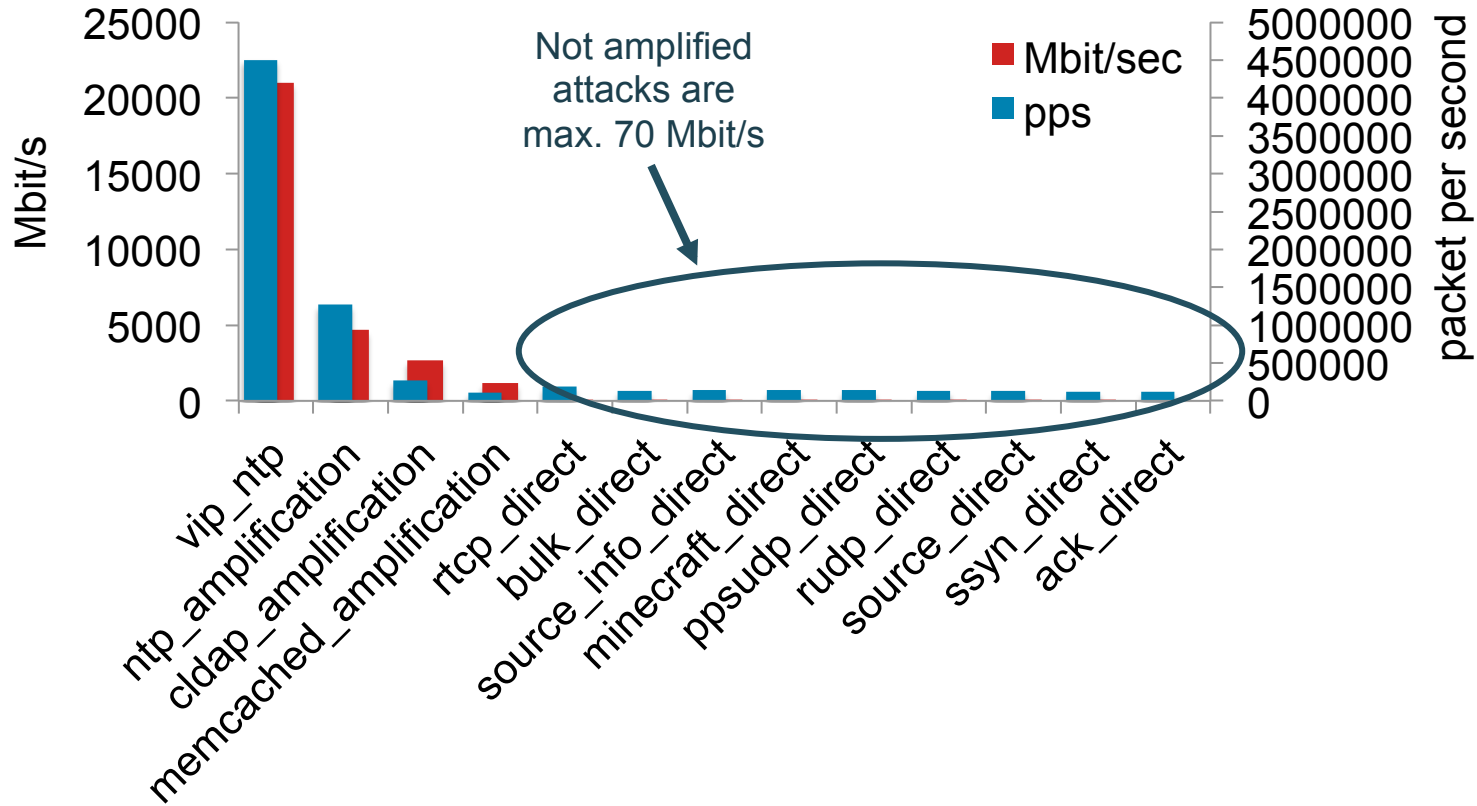
- Dedicated second NIC as mirror
- Fast write speed: SAS RAID-0
- Dedicated Raid Controller
- Single core performance

→ System Setup

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

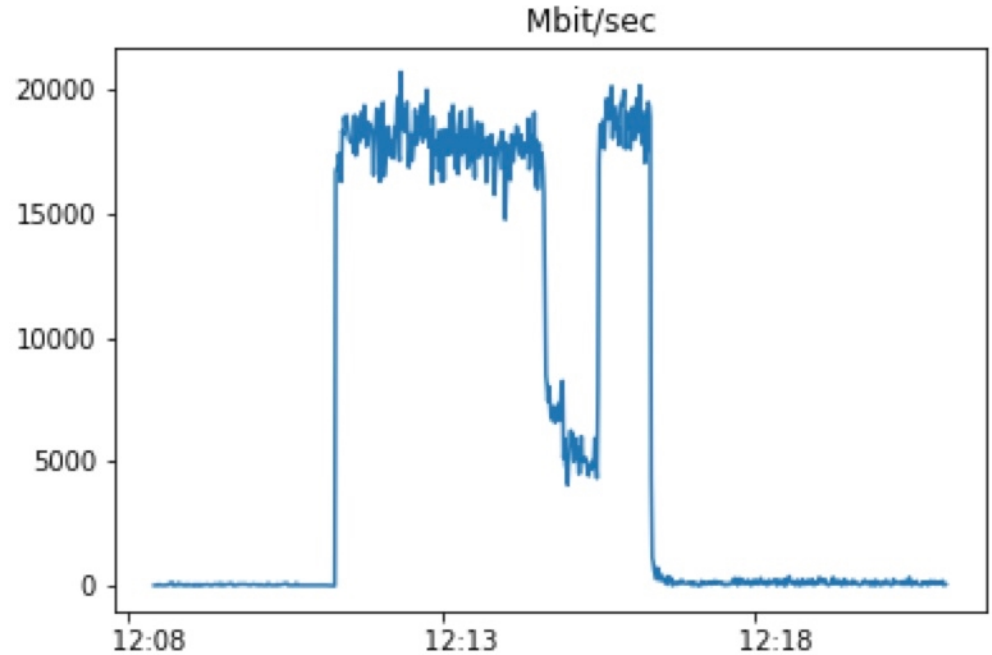


DDoS Attacks - Overview



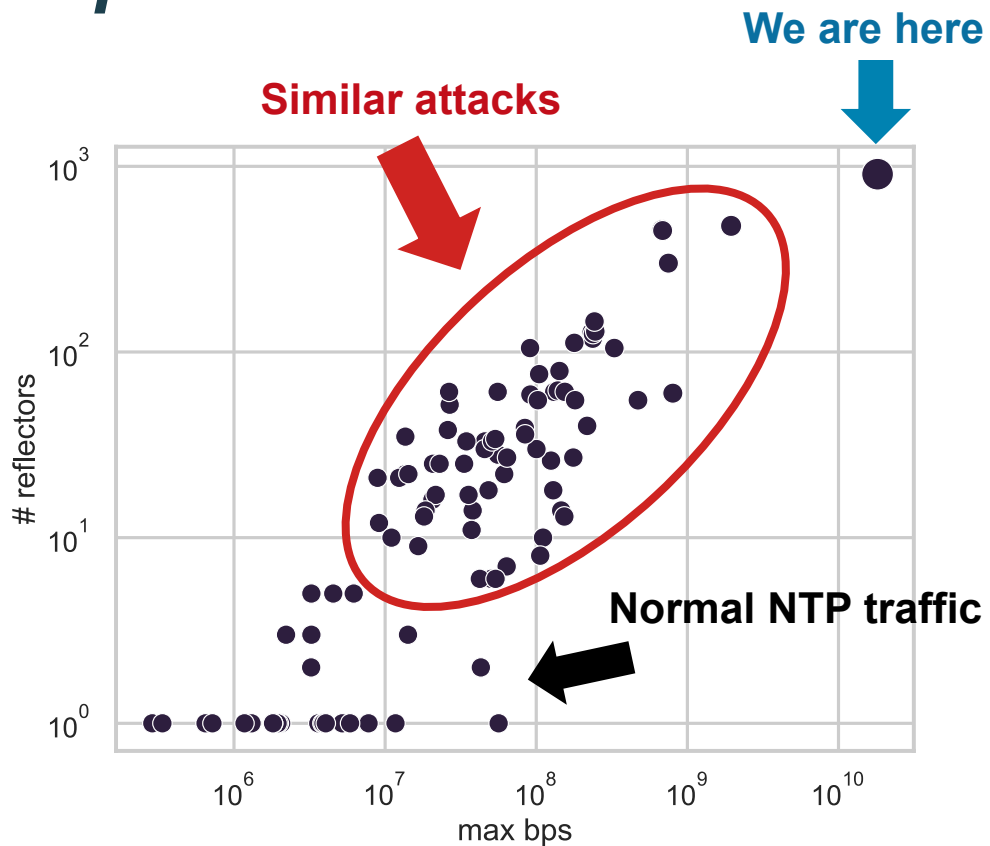
DDoS - NTP Reflection

- 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 screenshot shows the top portion of the Department of Justice website. At the top left is the official seal of the Department of Justice. To its right, the text reads "THE UNITED STATES DEPARTMENT of JUSTICE". Below this is a navigation bar with four links: "ABOUT", "OUR AGENCY", "PRIORITIES", and "NEWS". Underneath the navigation bar, there is a breadcrumb trail: "Home » Office of Public Affairs » News". A black banner with the text "JUSTICE NEWS" is visible. At the bottom of the screenshot, the text "Department of Justice" and "Office of Public Affairs" is displayed.



The screenshot shows a website seizure notice. At the top, a red banner with white text reads "THIS WEBSITE HAS BEEN SEIZED". Below this, the text states: "This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Central District of California under the authority of 18 U.S.C. §1030(i)(1)(A) as part of coordinated law enforcement action taken against illegal DDoS-for-hire services." It further mentions that the action was taken in coordination with the United States Attorney's Office of the District of Alaska, the Department of Justice Computer Crime and Intellectual Property Section, and the National Crime Agency (NCA). The notice also features the logos of the NCA, the FBI, and the Dutch police (Politie). At the bottom, it provides a link for more information: "For additional information, see the FBI Public Service Announcement I-101717b-PSA, <https://www.ic3.gov/media/2017/171017-2.aspx>".

FOR IMMEDIATE RELEASE

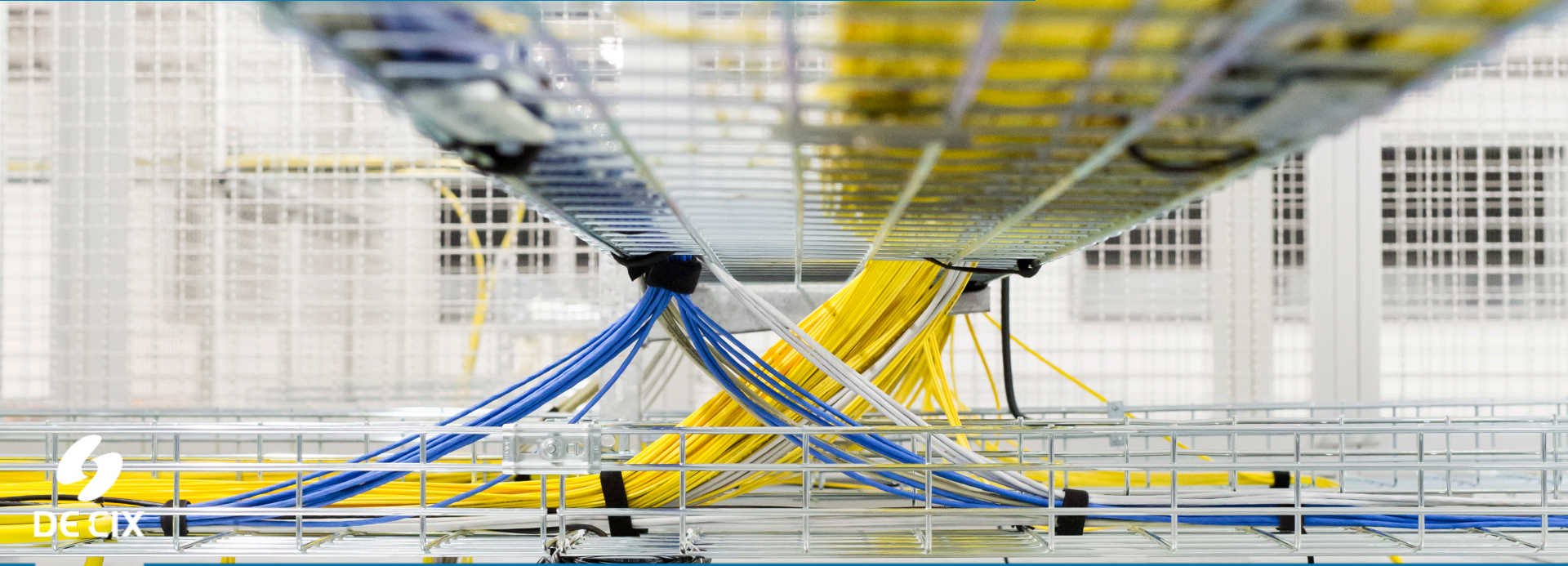
Thursday, December 20, 2018

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



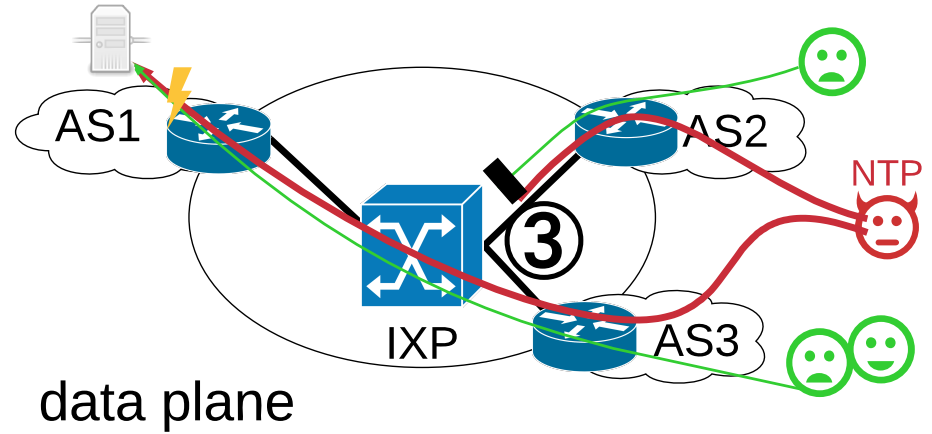
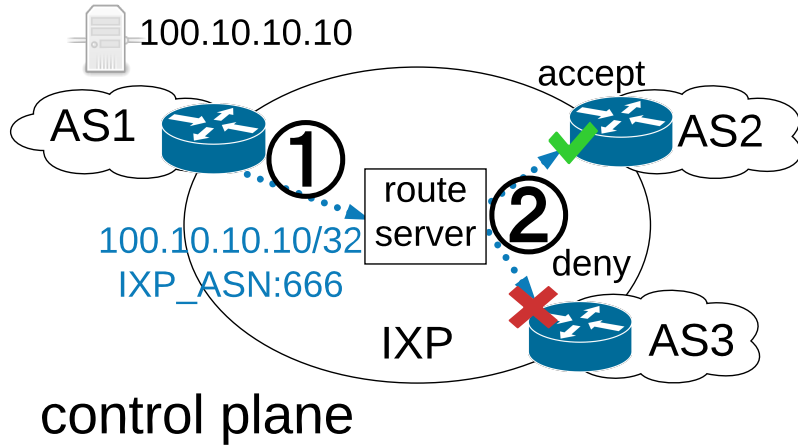
- Filters at arbitrary granularity
- Vendor- specific
- Per device config

- 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

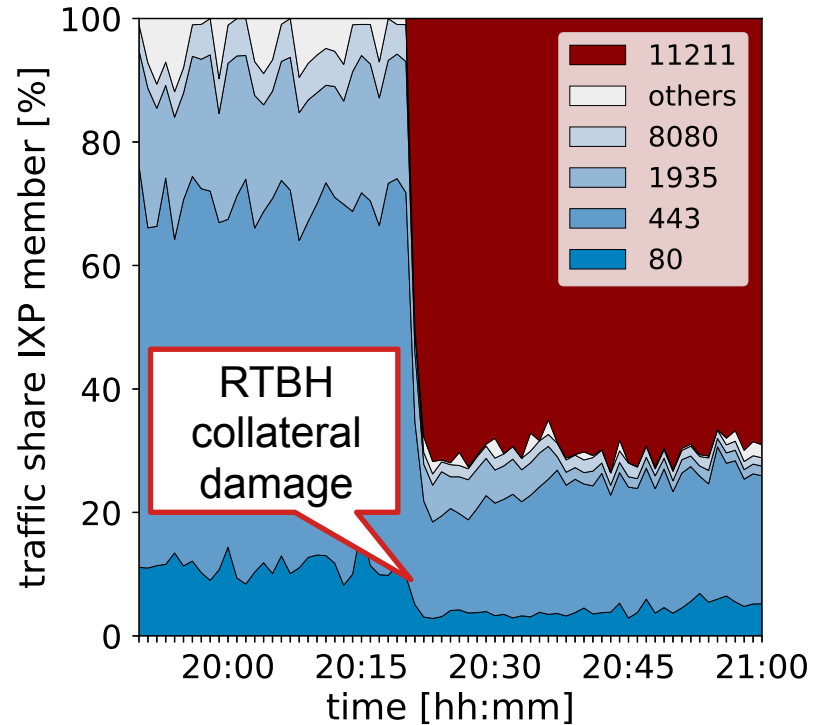
Traditional Blackholing at IXPs



Blackholing – Limitations

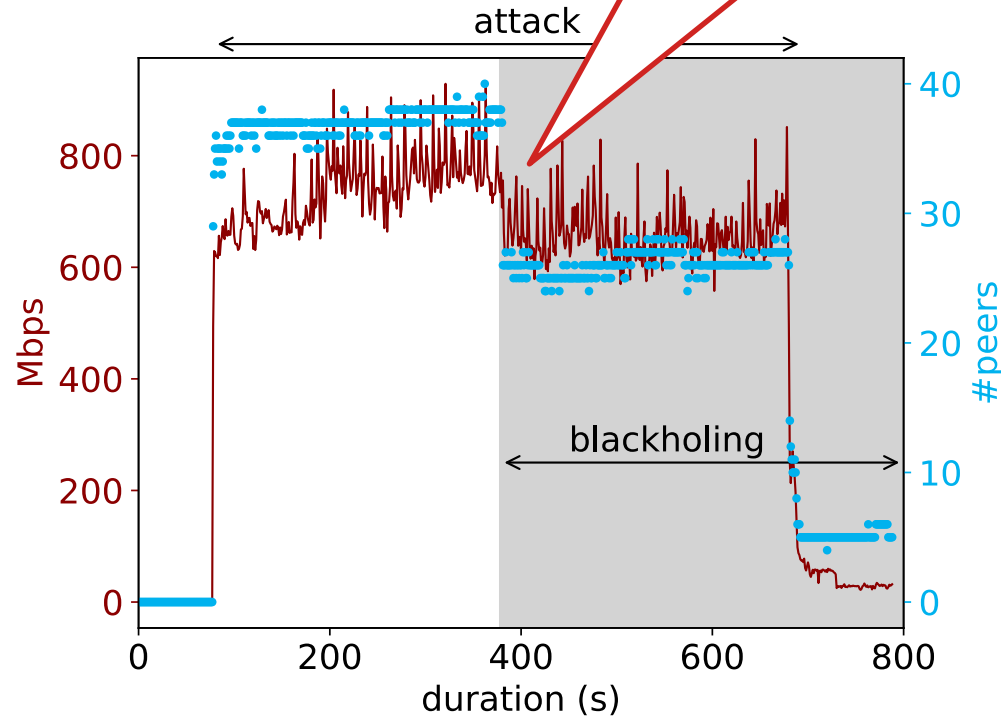
- Relative traffic of 40GE IXP port
- Mostly web traffic (80, 443, ...)
- Attack 70% memcached traffic
- Still significant share of web traffic

- **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

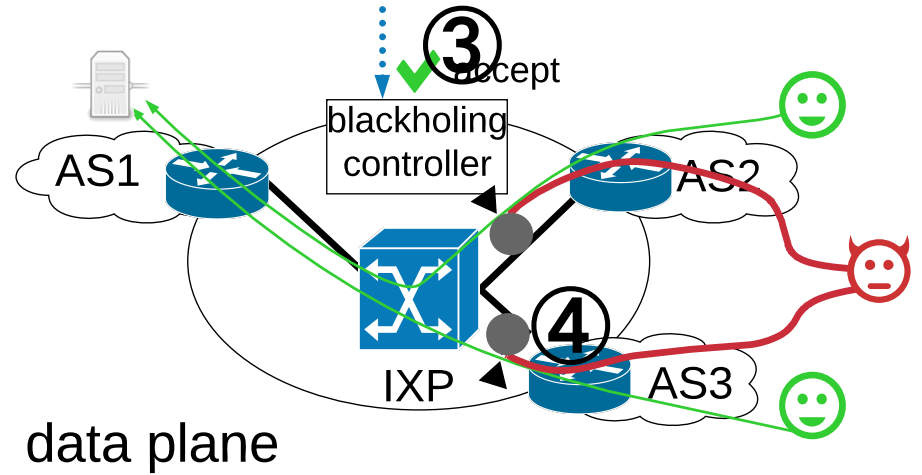
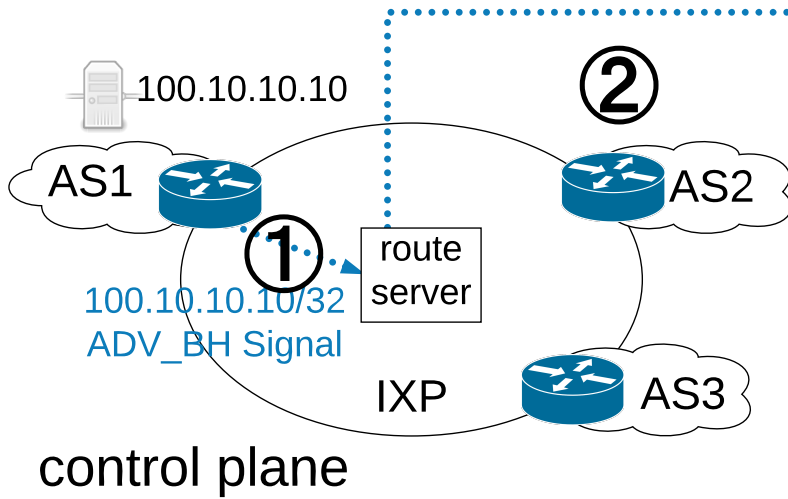
→ Scalability

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

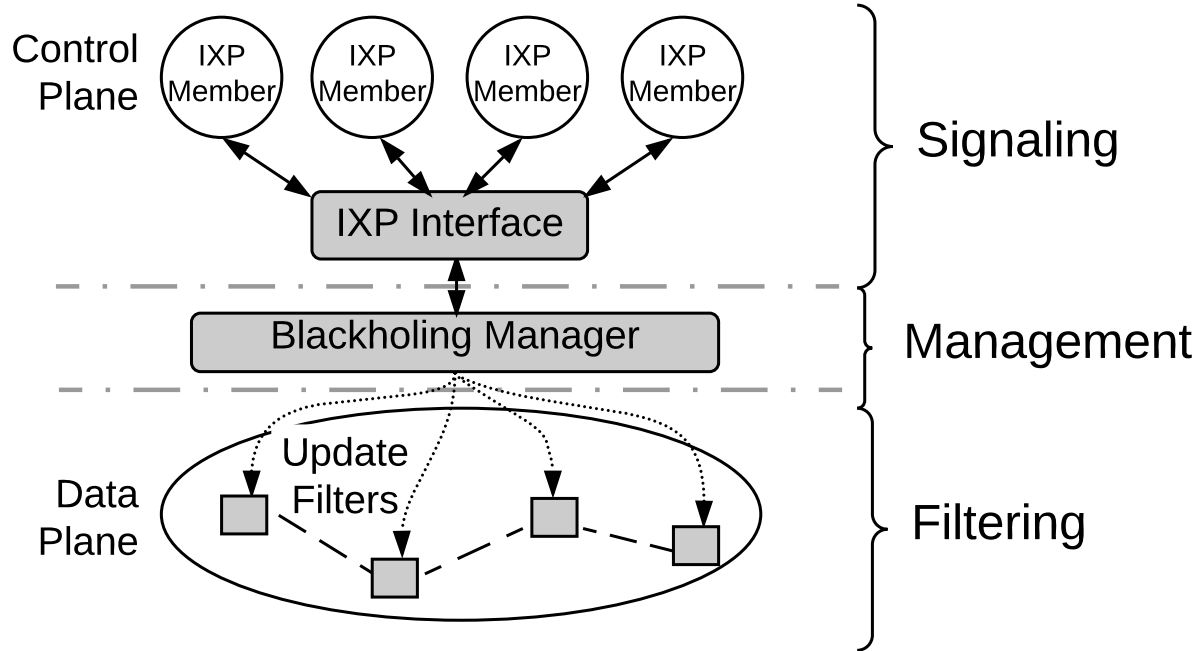
→ Cost

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

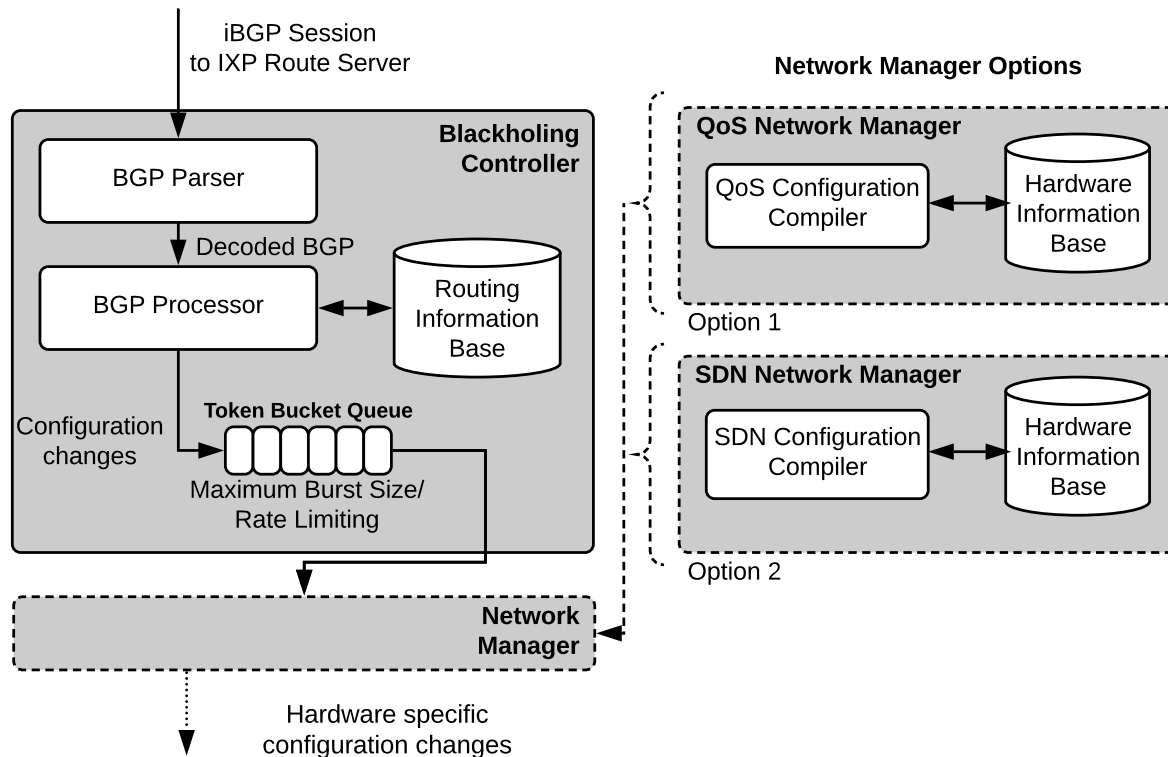
Advanced Blackholing System



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

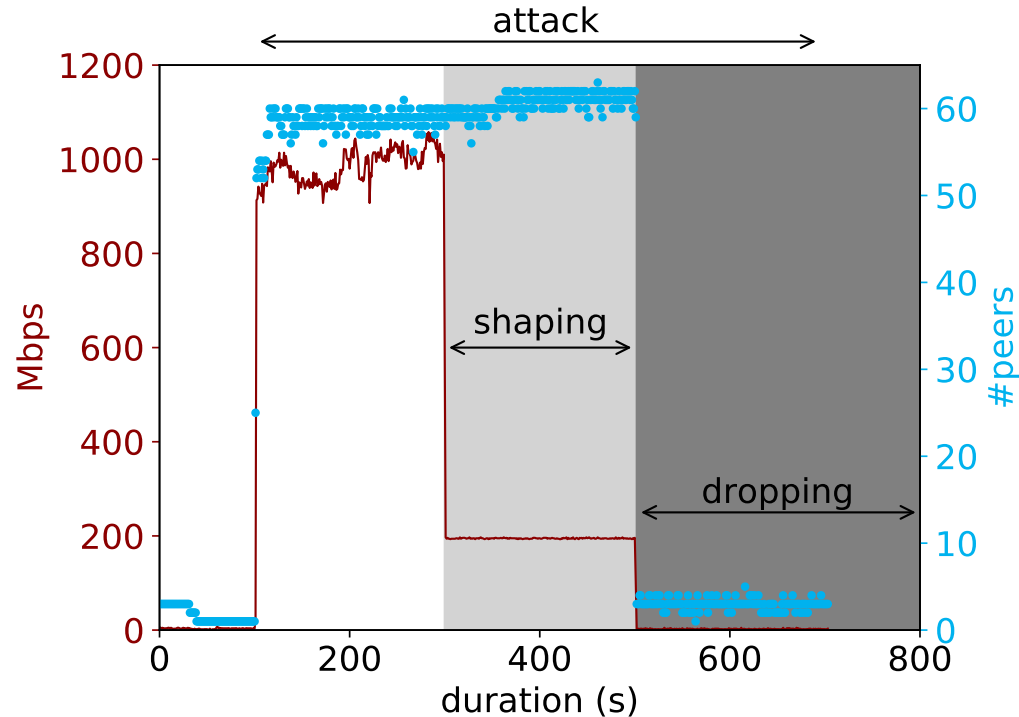
✓ → Cost

- 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**



A person is holding a globe of the Earth in front of a wall covered in newspaper clippings. The globe is the central focus, showing continents and oceans. The text 'Q&A - Discussion - Feedback' is overlaid in white, bold, italicized font across the center of the image.

Q&A - Discussion - Feedback



Where networks meet

www.de-cix.net