Freie Universität Berlin

Impactful Measurement Research: Lessons from Analyzing Mitigations of Prefix Hijacking and DDoS

Matthias Wählisch

<m.waehlisch@fu-berlinde>

The Internet core suffers

Hijacking

The problem!

RPKI

The solution?

DDoS

The problem!

Blackholing

The solution?

The Internet core suffers

Hijacking

The problem!

RPKI

The solution?

DDoS

The problem!

Blackholing

The solution?

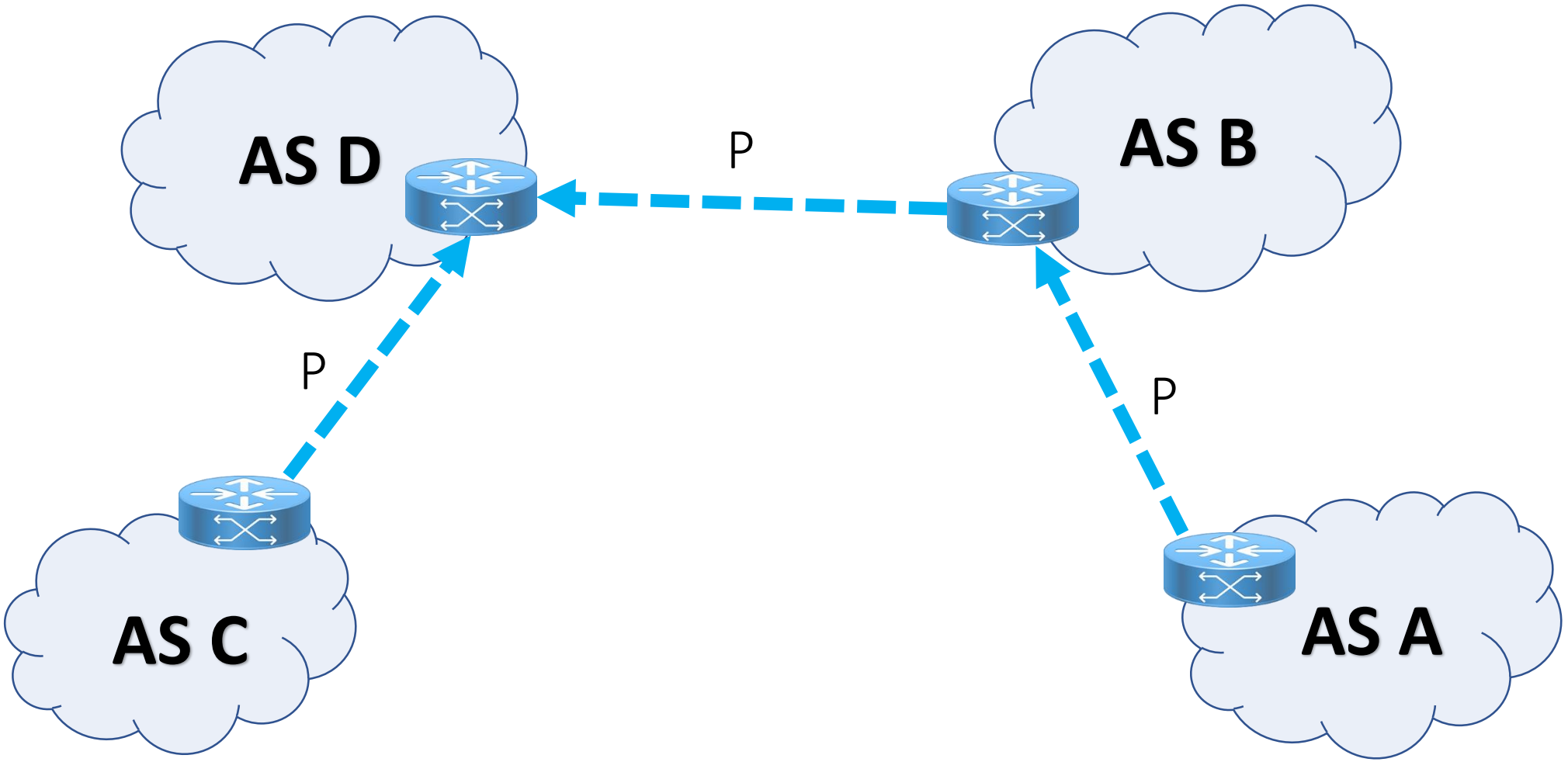
References

Matthias Wählisch, Olaf Maennel, Thomas C. Schmidt,
Towards Detecting BGP Route Hijacking using the RPKI,
ACM Computer Communication Review, Vol. 42, No. 4, pp. 103-104, 2012.

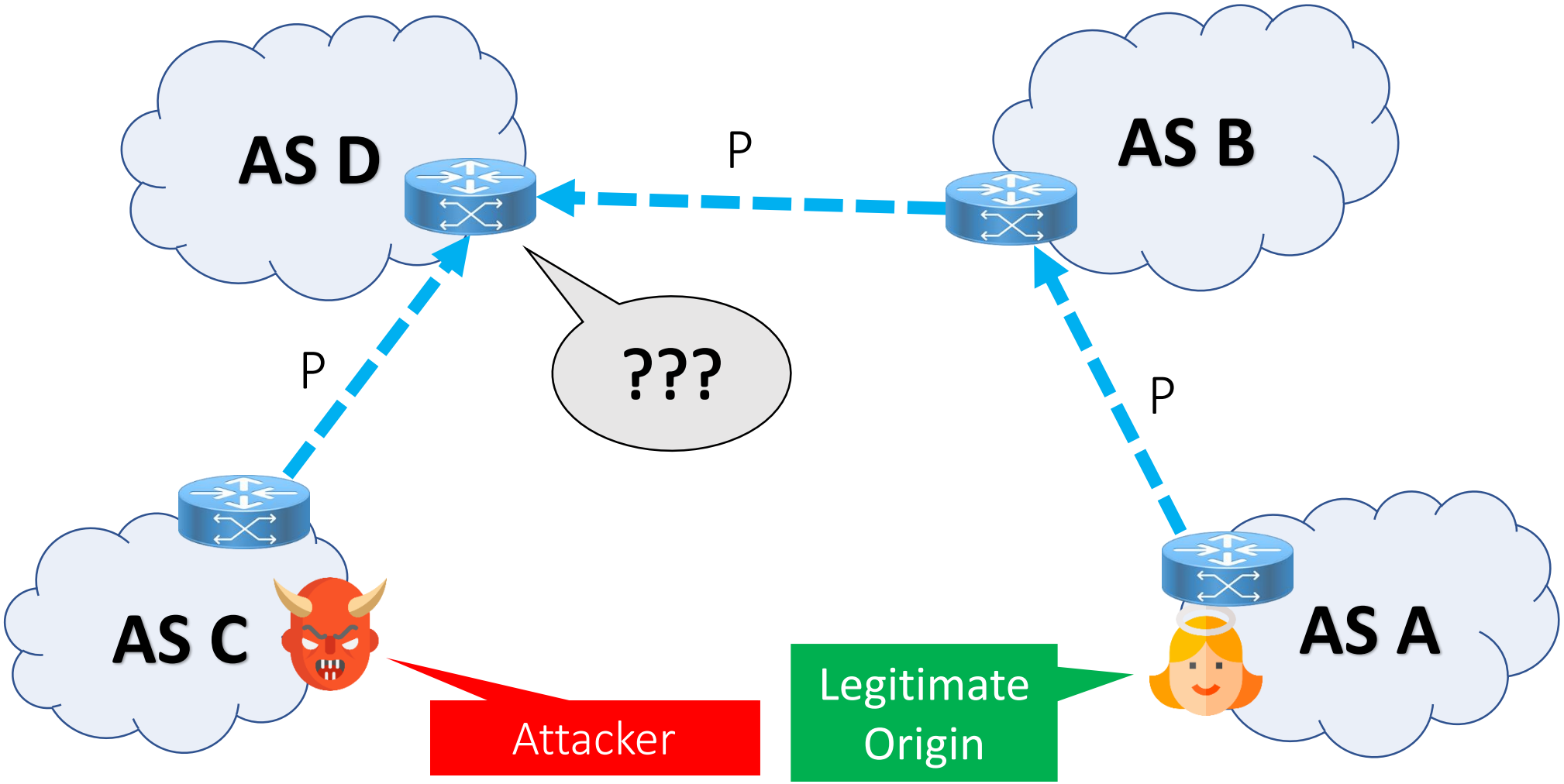
Matthias Wählisch, Robert Schmidt, Thomas C. Schmidt, Olaf Maennel, Steve Uhlig, Gareth Tyson,
RiPKI: The Tragic Story of RPKI Deployment in the Web Ecosystem, **In:** *Proc. of 14th ACM Workshop on Hot Topics in Networks (HotNets),* New York: ACM, 2015.

Andreas Reuter, Randy Bush, Italo Cunha, Ethan Katz-Bassett, Thomas C. Schmidt, Matthias Wählisch,
Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering, *ACM Computer Communication Review,* Vol. 48, No. 1, pp. 19-27, 2018.

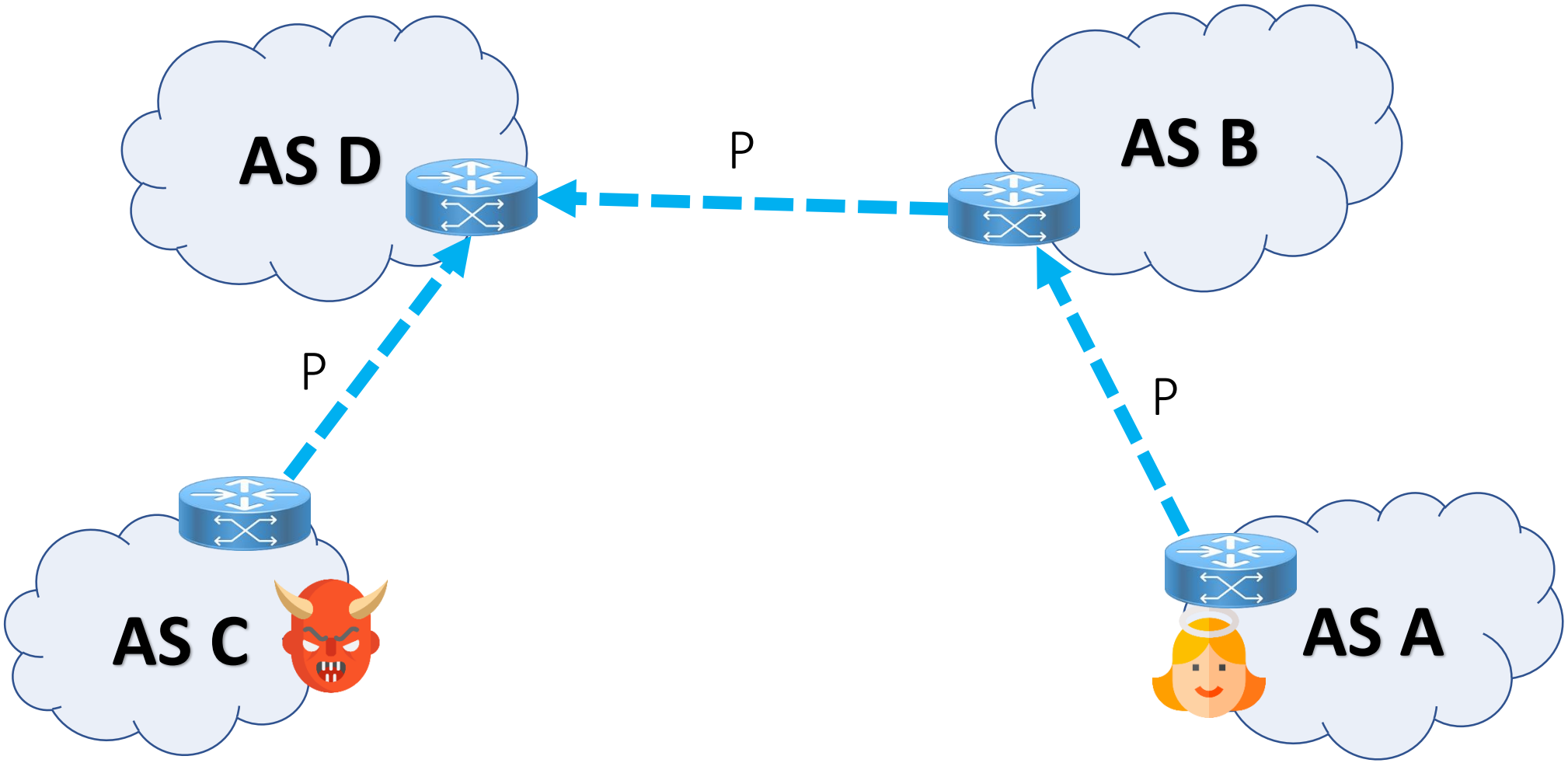
The problem: Prefix hijacking



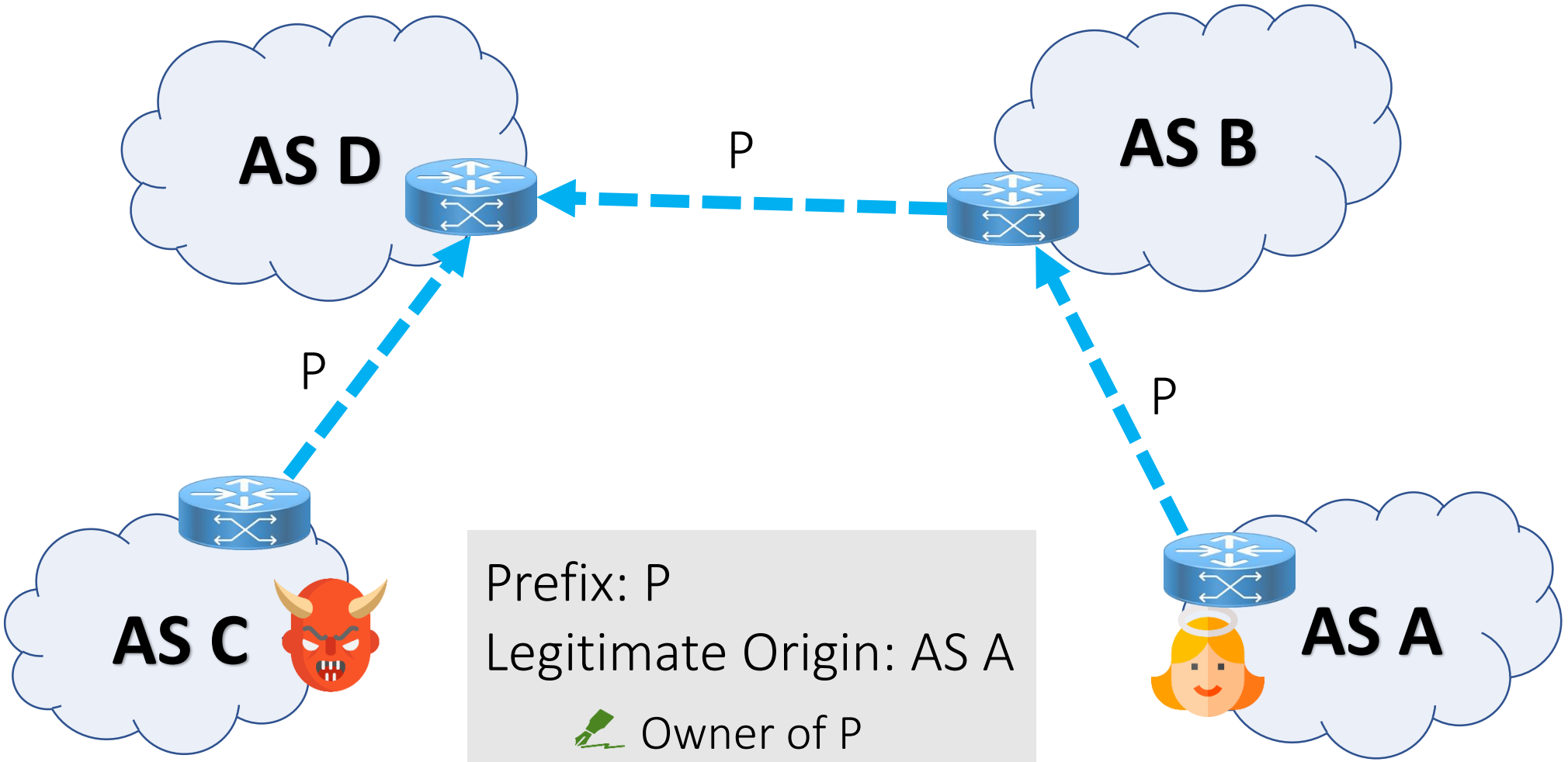
The problem: Prefix hijacking



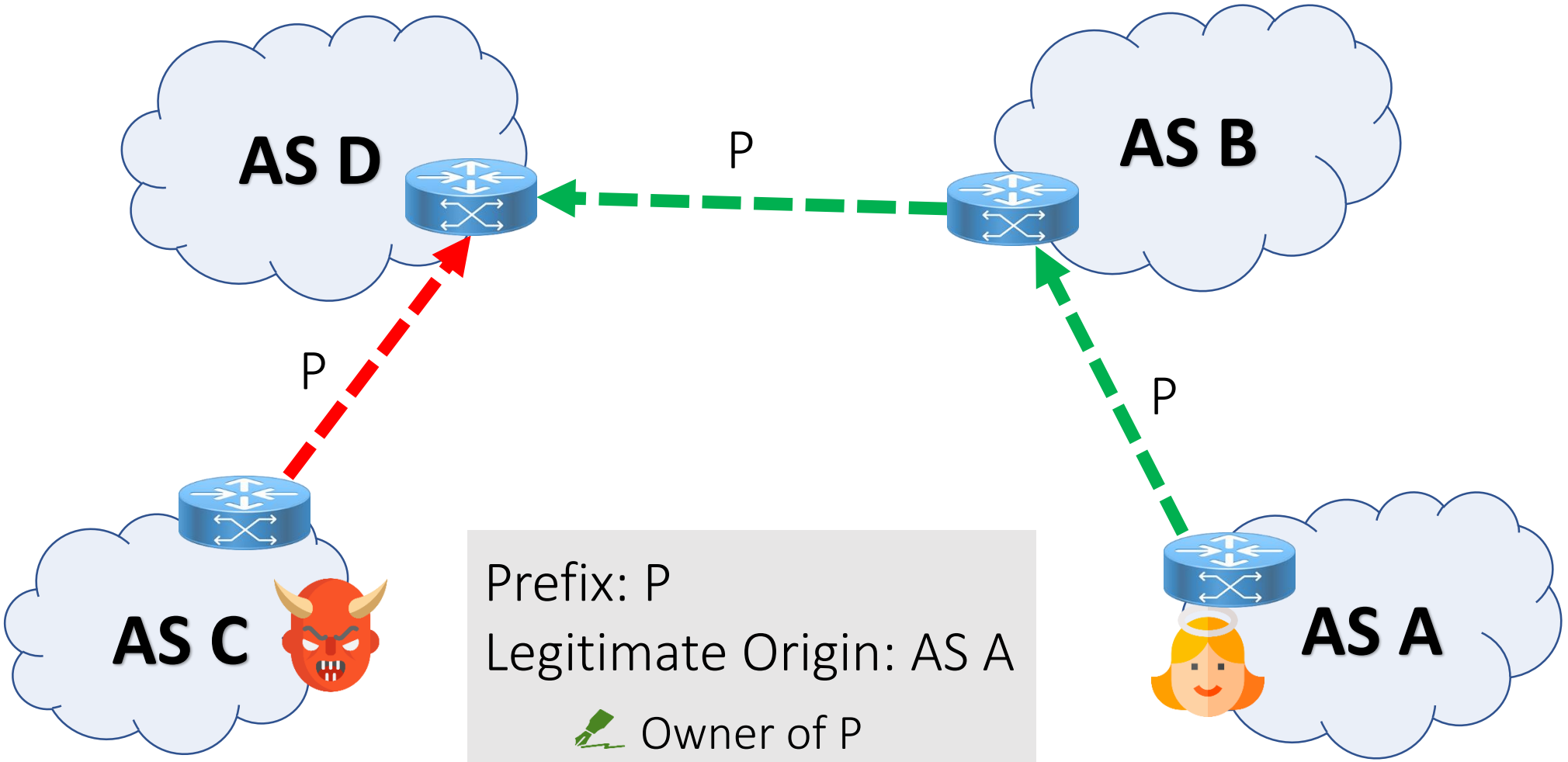
The solution: RPKI in a nutshell



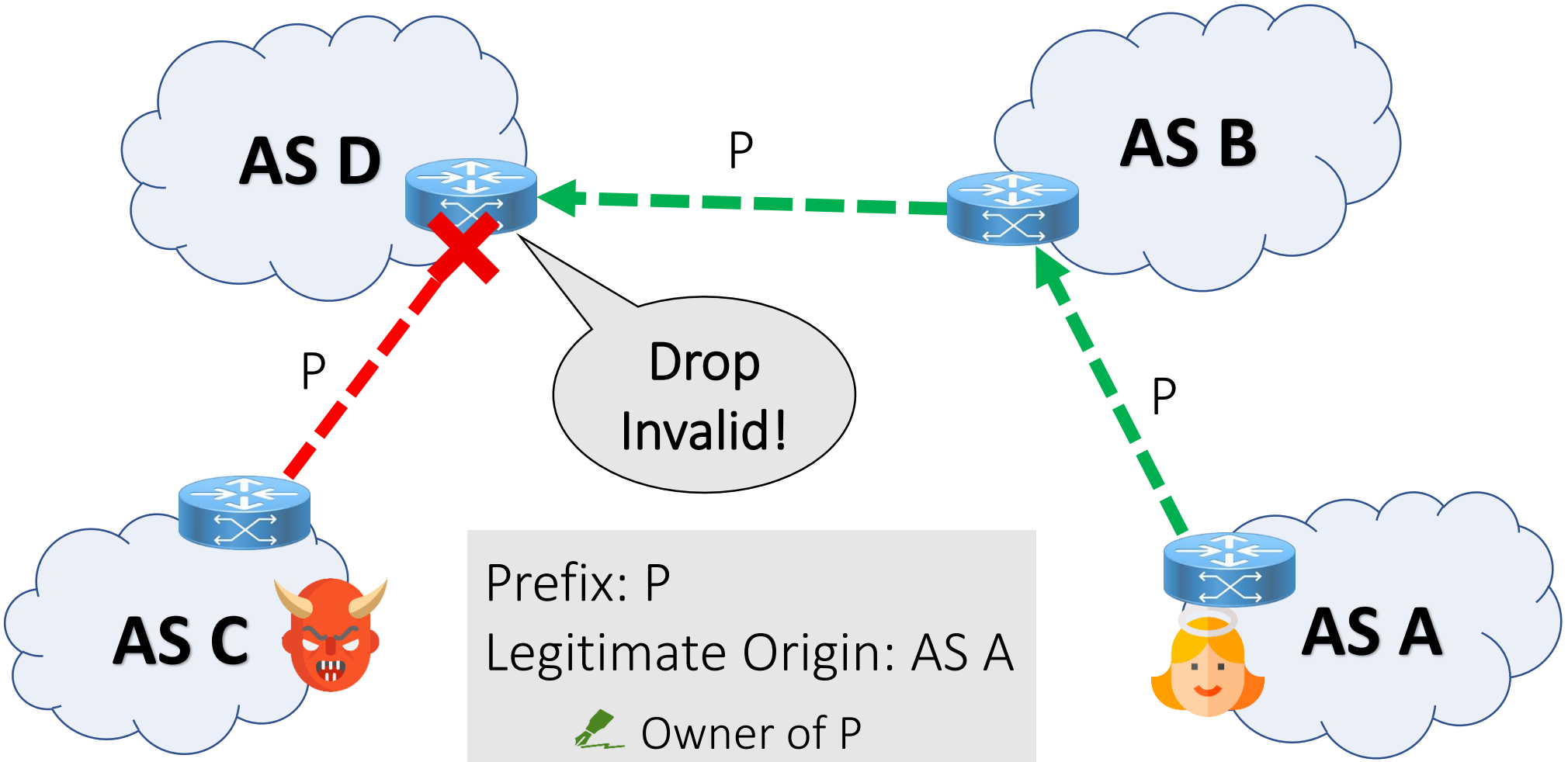
The solution: RPKI in a nutshell



The solution: RPKI in a nutshell



The solution: RPKI in a nutshell



Easy. Right?

What can possibly go wrong?

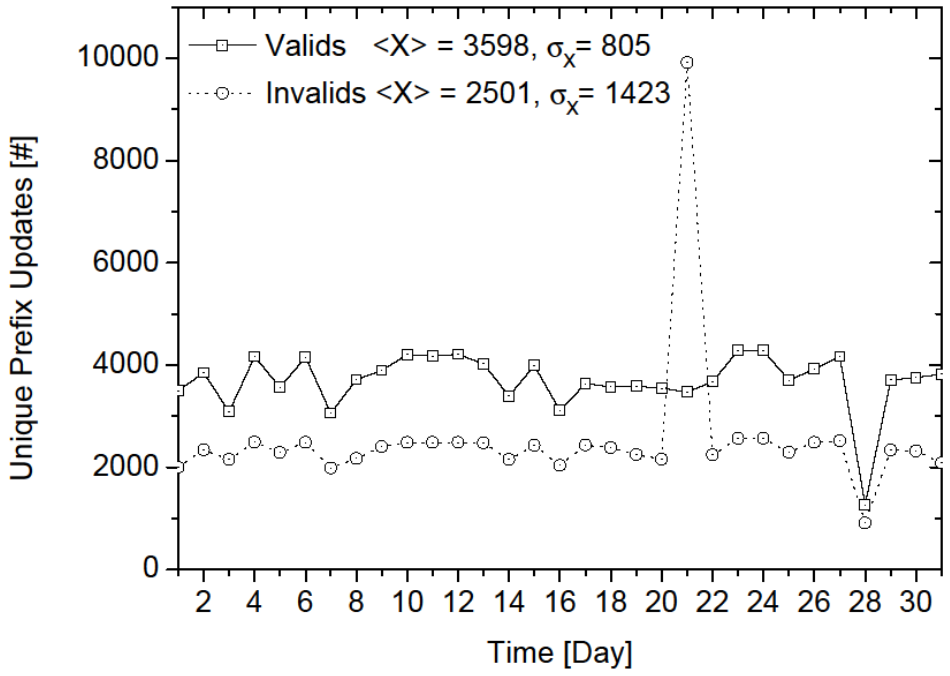
Easy. Right?

What can possibly go wrong?

Incorrectly configured RPKI attestation objects.

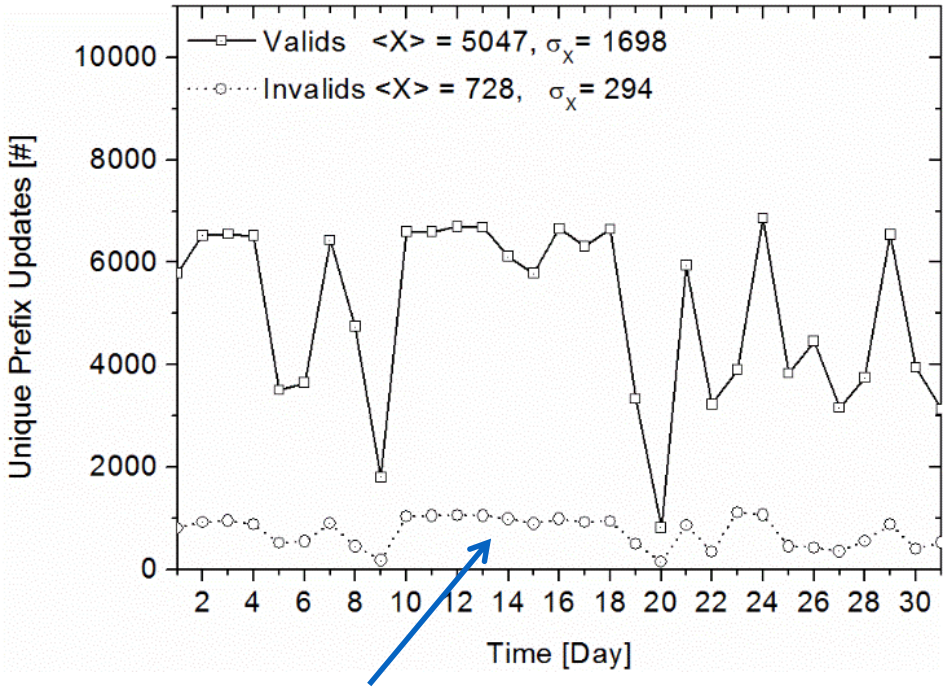
Invalid = Invalid?

January 2012



Number of invalids
decreased over time, but …

May 2012



Are all these updates really hijacks?? No!

Common pitfalls

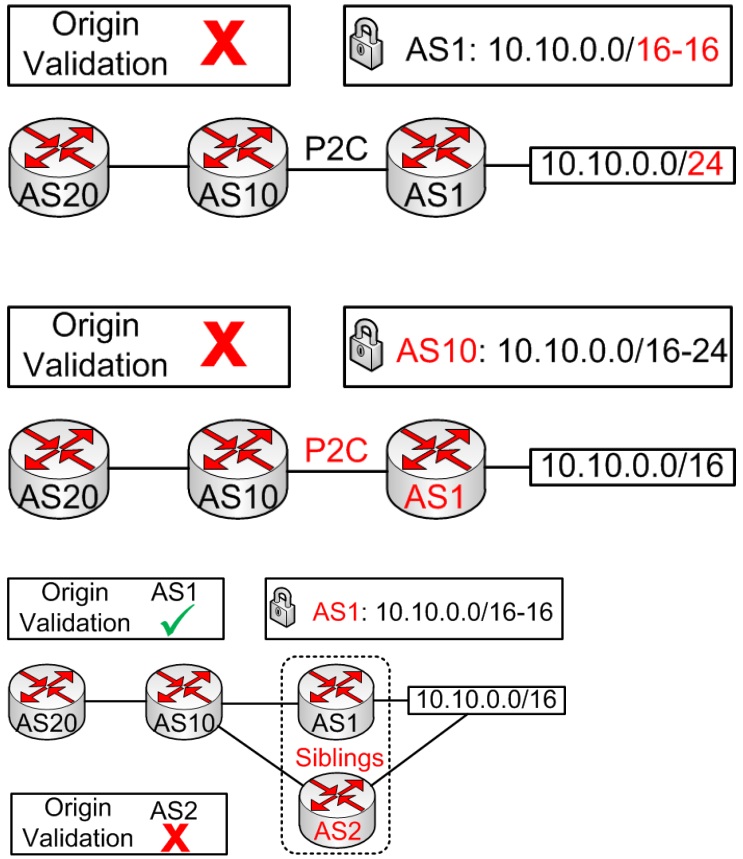
Case 1: Missing Customer (or Sibling) Legitimation
ROA created: 12.0.0.0/8-9 -> AS 7018
AS 27487 announces 12.0.19.0/24
AS 2386 announces 12.1.216.0/24
⇒ Consider sub-allocations, start most specific

Both announcements are invalid if no RPKI object exists.

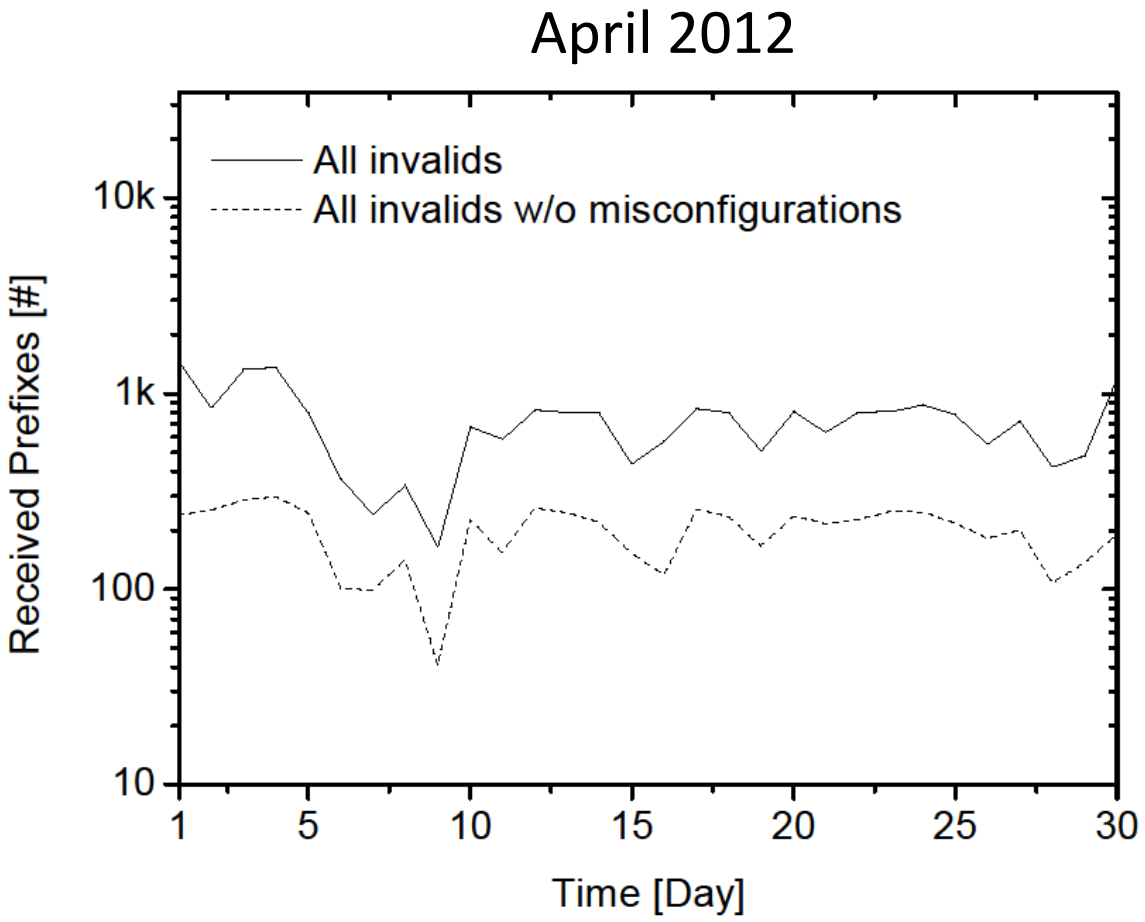
Case 2: (De-)Aggregation
ROA created: 78.192.0.0/10-10 -> AS 12322
Usual announcement: 78.192.0.0/10
For 30 minutes: 78.192.10.0/24 …
⇒ Configure the max ROA prefix length explicitly

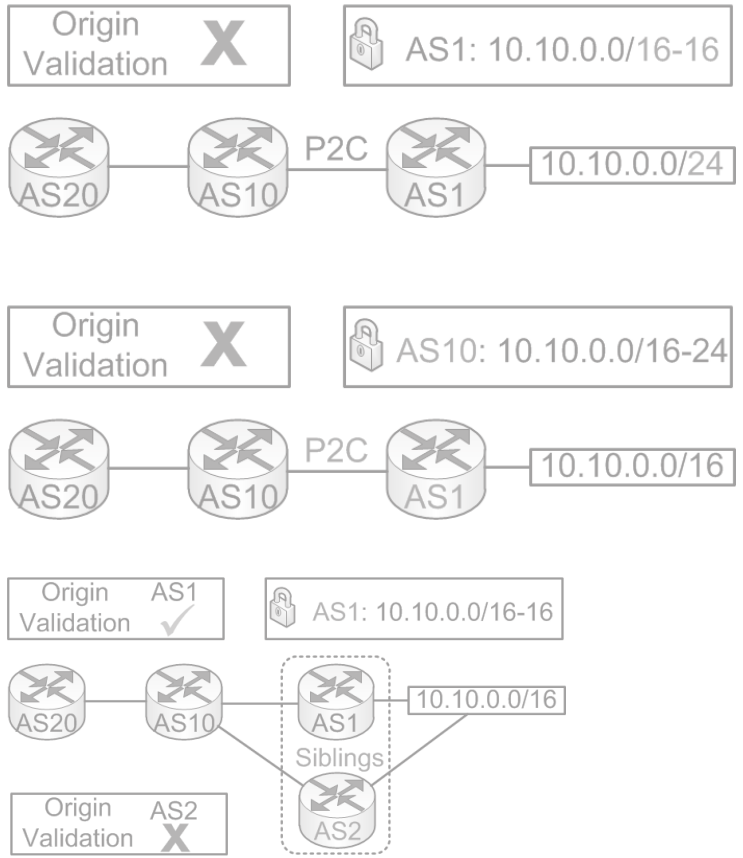
Methodology to discover potential misconfigurations [CCR'12]

1. Valid origin, announced prefix is more specific
2. Provider does not consider customer
3. Additional ASes of a company are not authorized



Methodology to discover potential misconfigurations [CCR'12]





What else?

When we started measuring in

2015 [HotNets'15], no CDN was involved in RPKI

Now Cloudflare, Google … are pushing

2018 [CCR'18], few ASes deployed RPKI filtering

Now many ASes (e.g., AT&T) deploy RPKI filtering

Since beginning of RPKI in 2012

Measurements were one important building block to understand RPKI deployment better, identify pitfalls, train operators.

It required sound measurement methodologies.

Your research may have impact, if you interact with operators.

The Internet core suffers

Hijacking

The problem!

RPKI

The solution?

DDoS

The problem!

Blackholing

The solution?

Reference

Marcin Nawrocki, Jeremias Blendin, Christoph Dietzel, Thomas C. Schmidt, Matthias Wählisch, **Down the Black Hole: Dismantling Operational Practices of BGP Blackholing at IXPs**, **In:** *Proc. of ACM Internet Measurement Conference (IMC),* New York: ACM, 2019.

Common belief

Blackholing is an effective measure to mitigate DDoS

Common (mis) belief

?

Blackholing is an effective measure

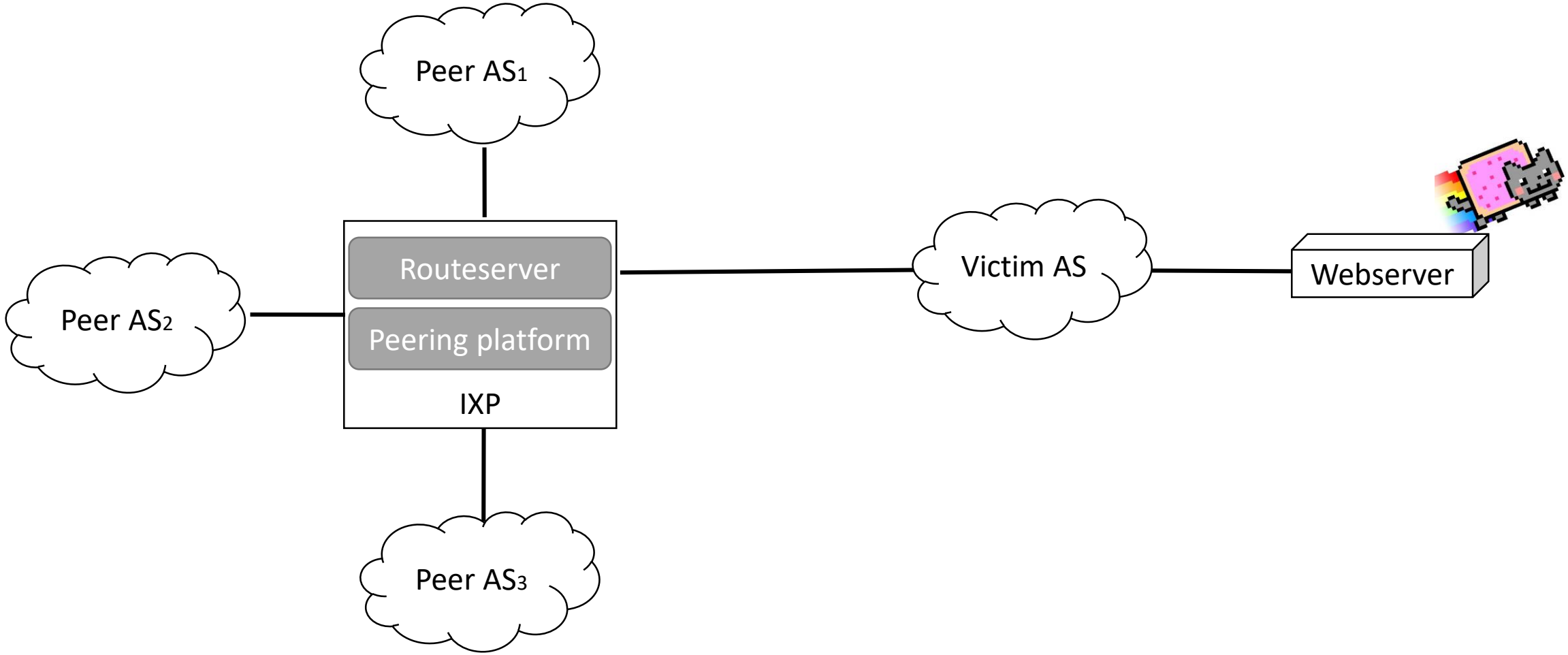
to mitigate DDoS

?

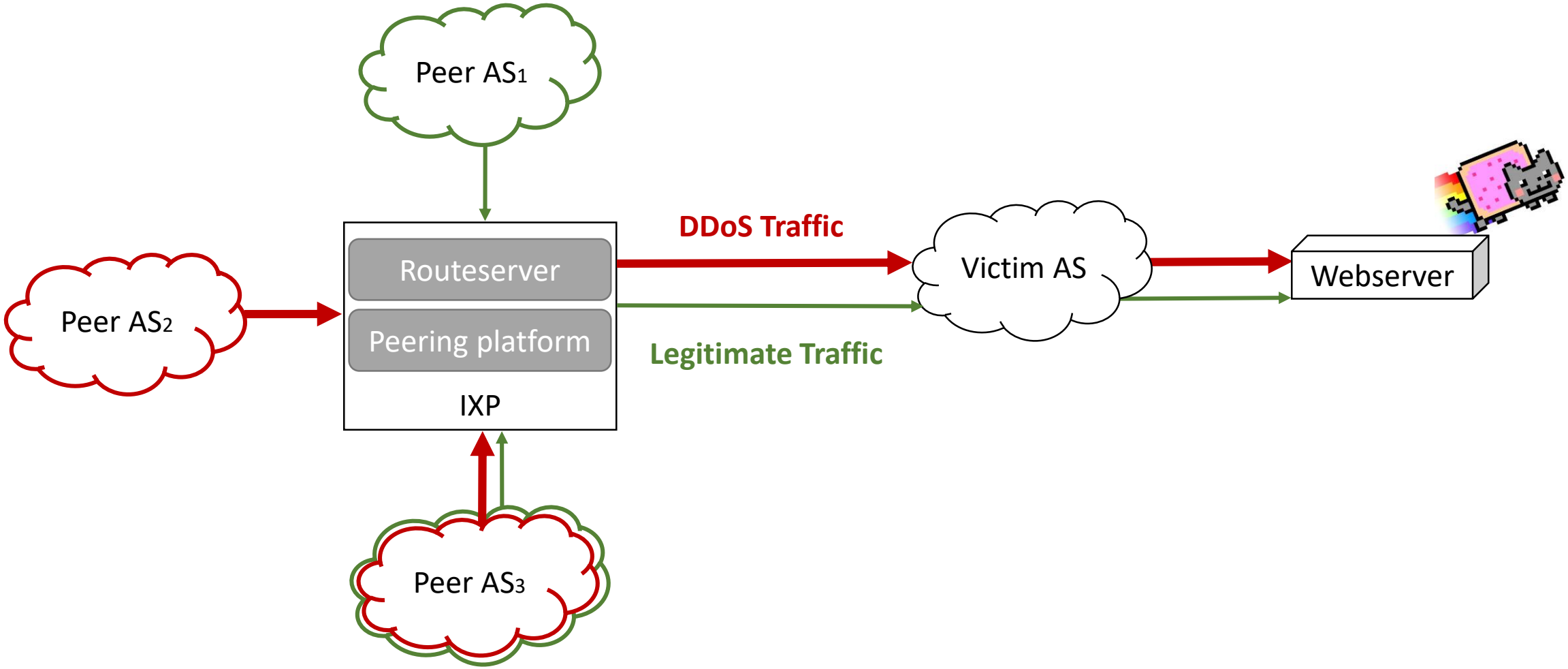
https://en.wikipedia.org/wiki/Black_hole#/media/File:Black_hole_-_Messier_87_crop_max_res.jpg

I. How does BGP Blackholing work at IXPs?

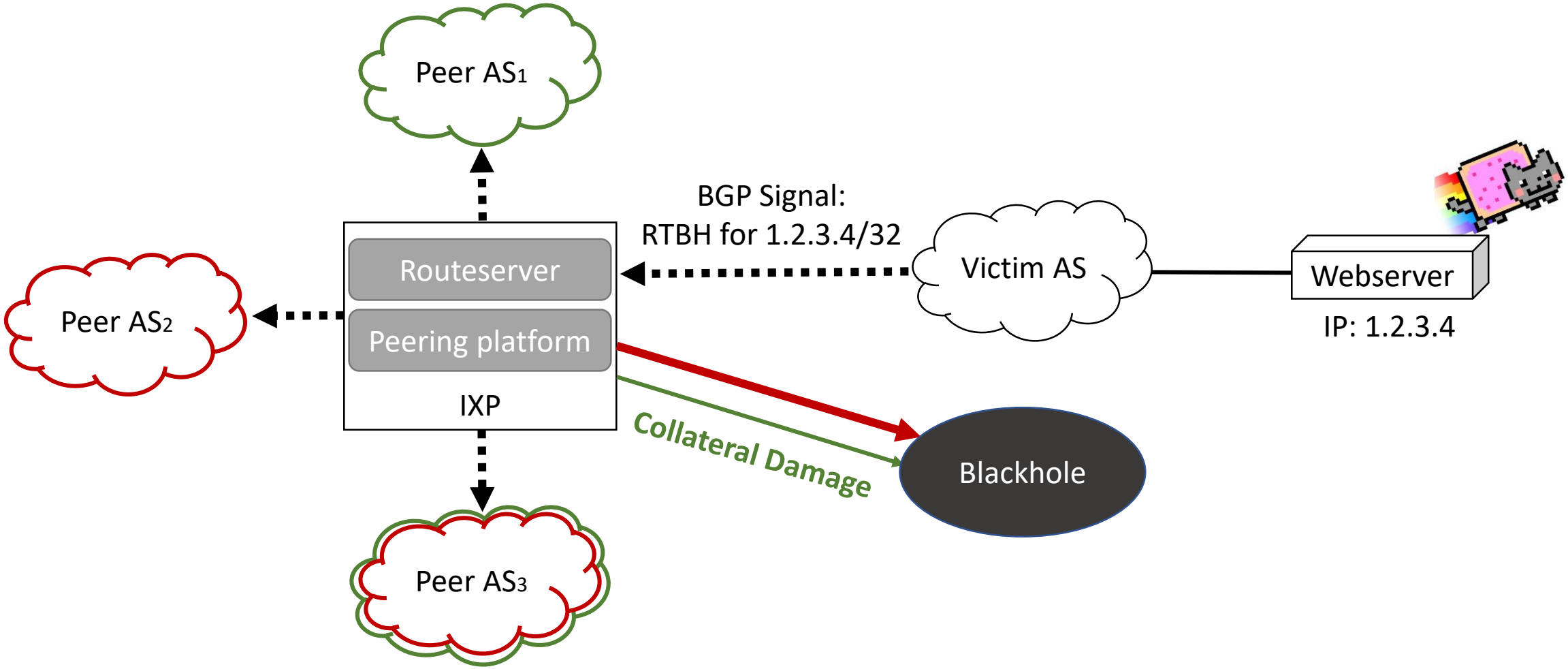
Remotely-Triggered Blackholing at IXPs



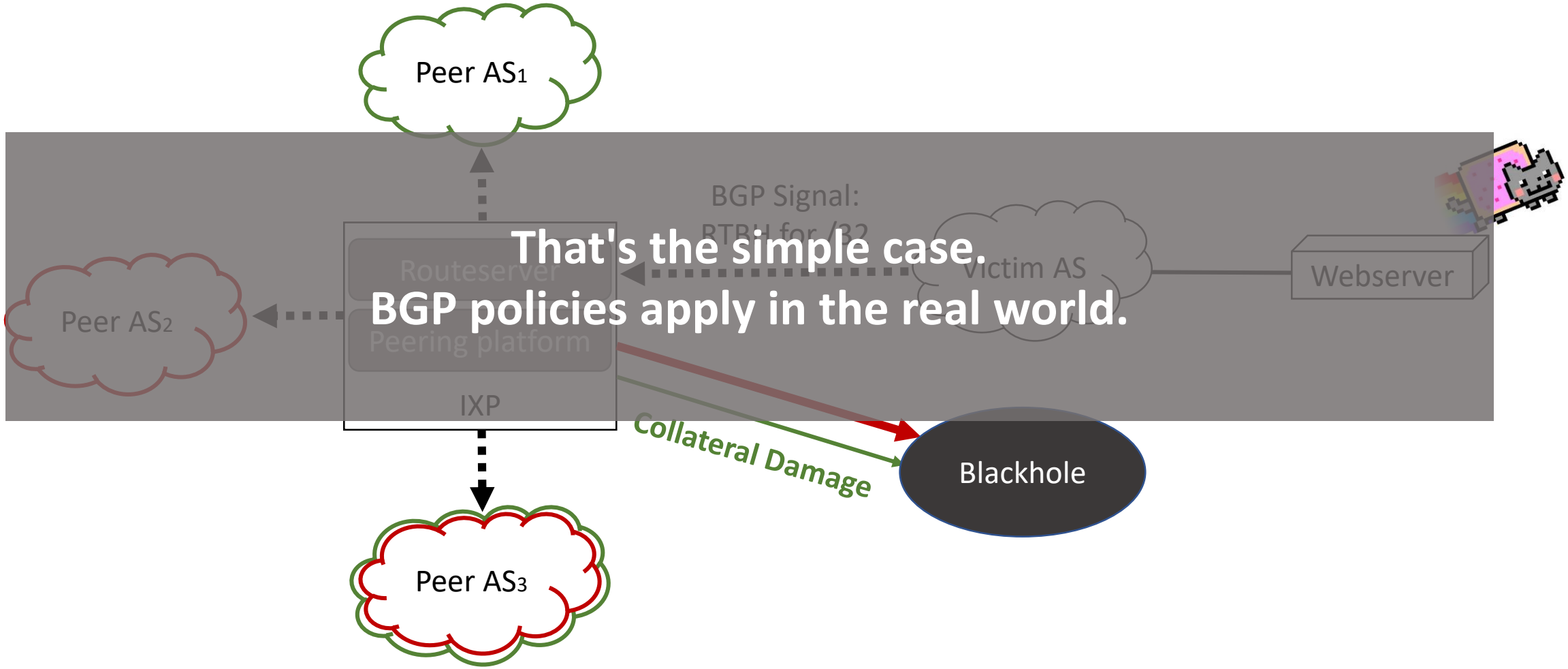
Remotely-Triggered Blackholing at IXPs



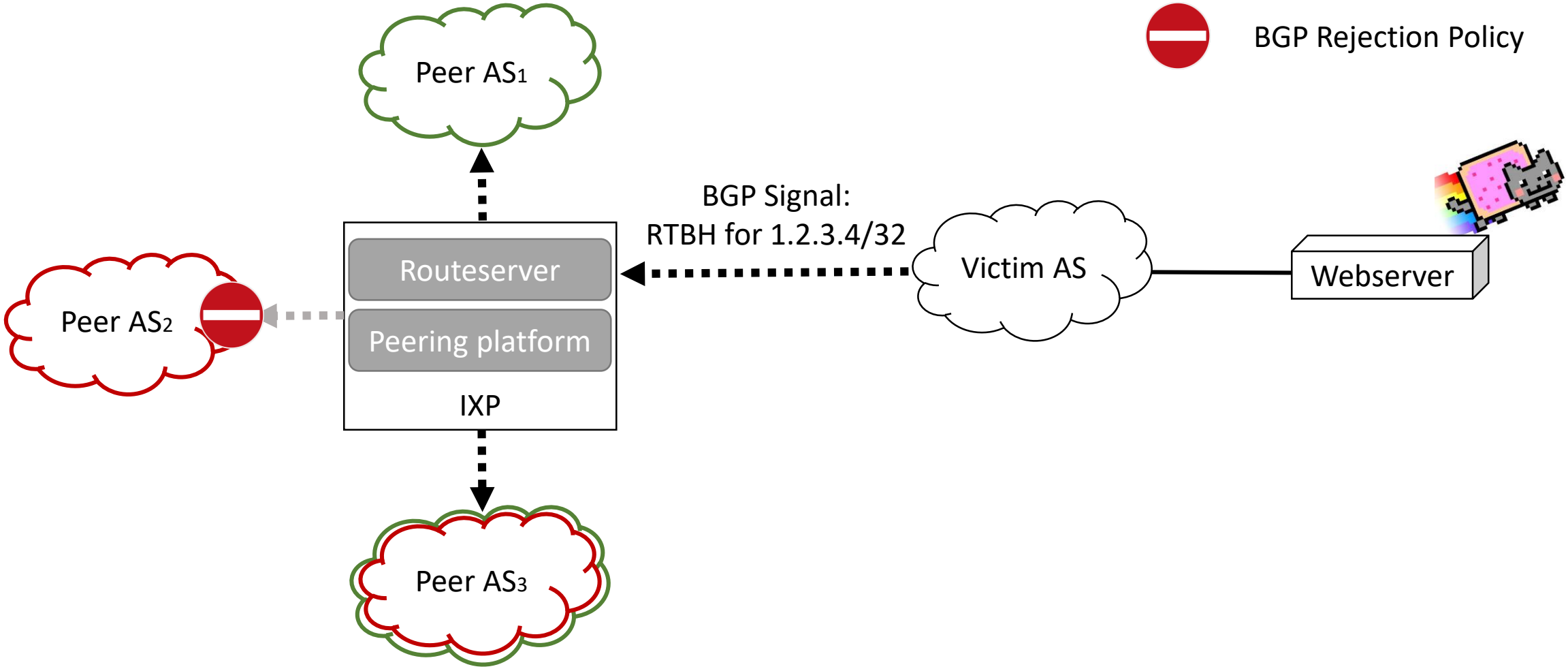
Remotely-Triggered Blackholing at IXPs



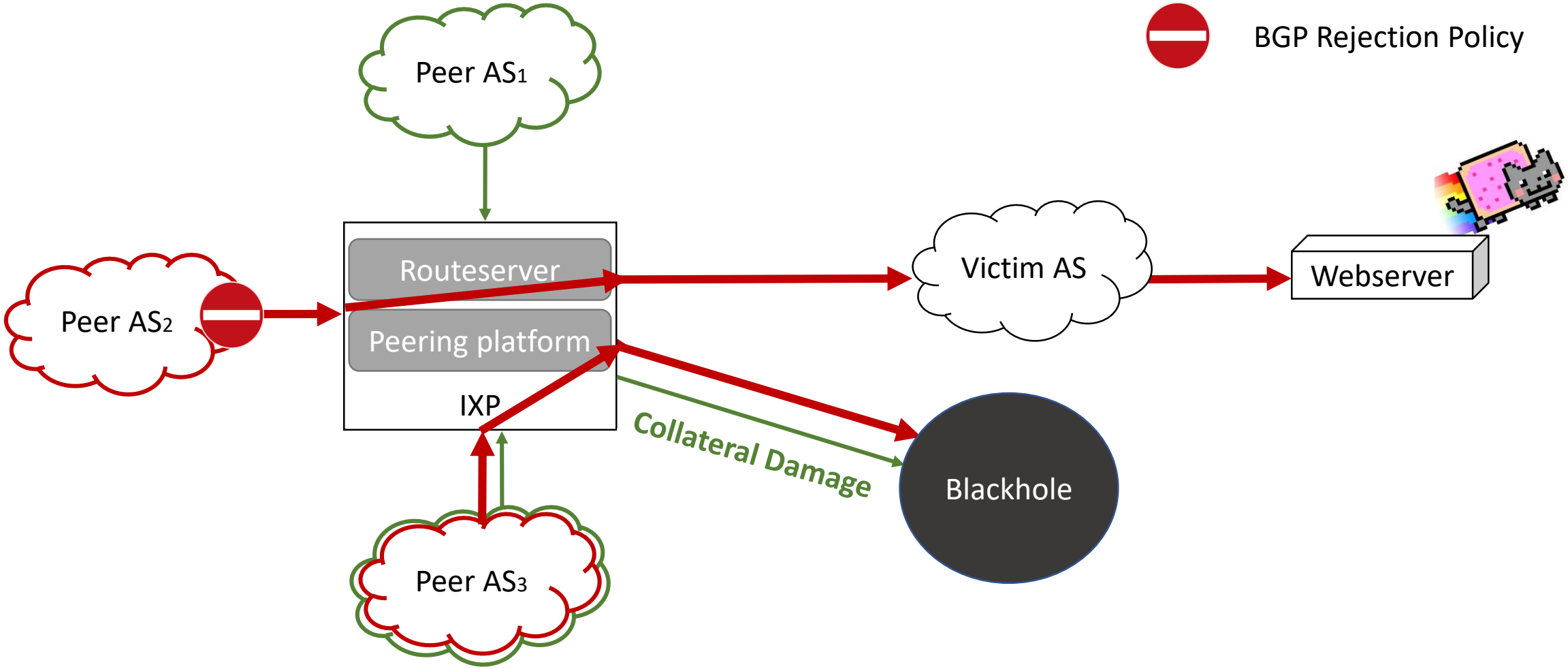
Remotely-Triggered Blackholing at IXPs



Remotely-Triggered Blackholing and BGP Policies



Remotely-Triggered Blackholing and BGP Policies



II. How well deployed is BGP Blackholing in the real world?

Our measurement approach

One of the worlds-largest IXPs as a central vantage point

Wholistic view: >100 days, all related data - **no exceptions!**

BGP data

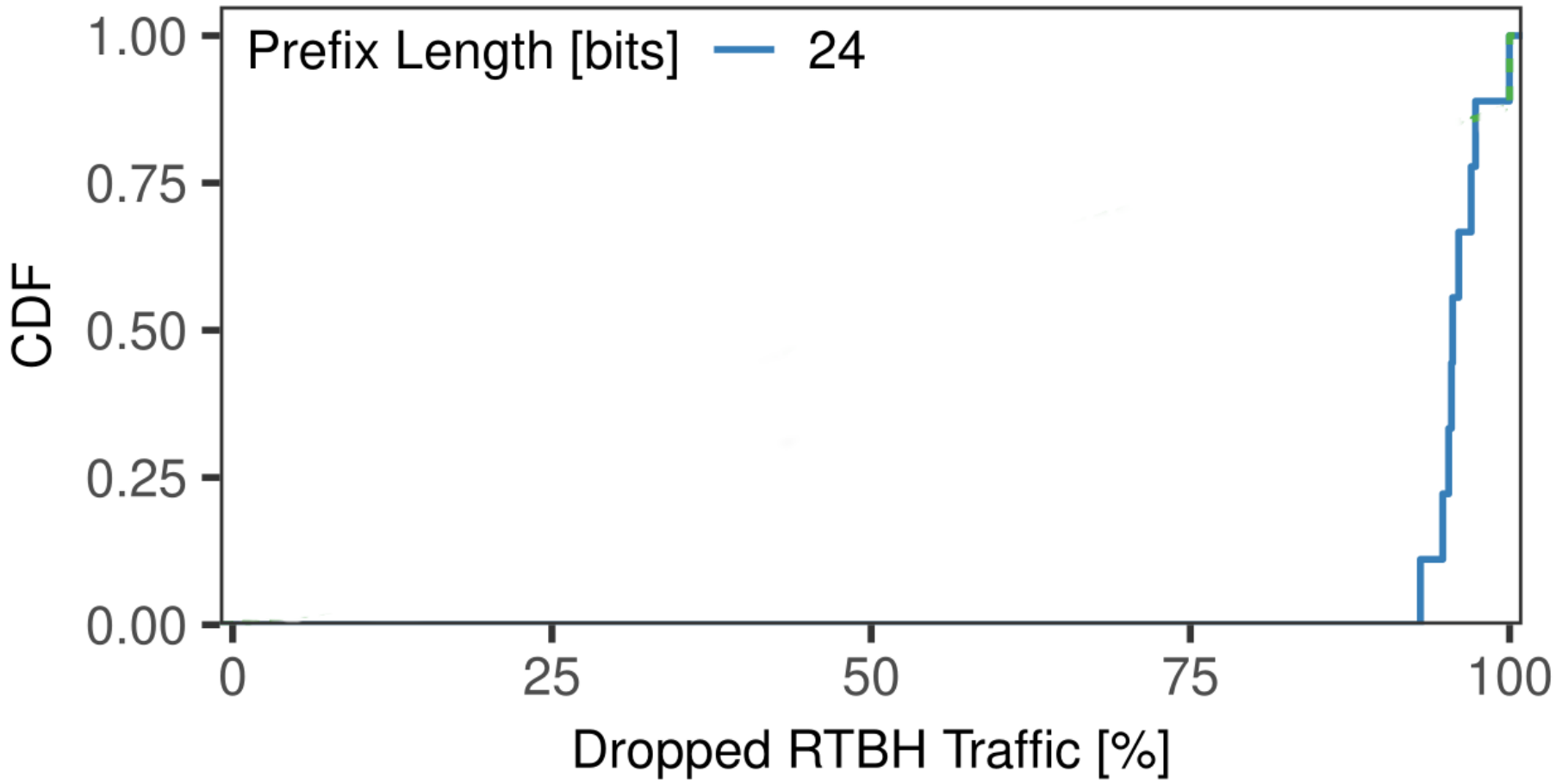
- All RTBH messages from all route-servers
- RTBH announcements identifiable by BGP community and next-hop-IP

Flow data

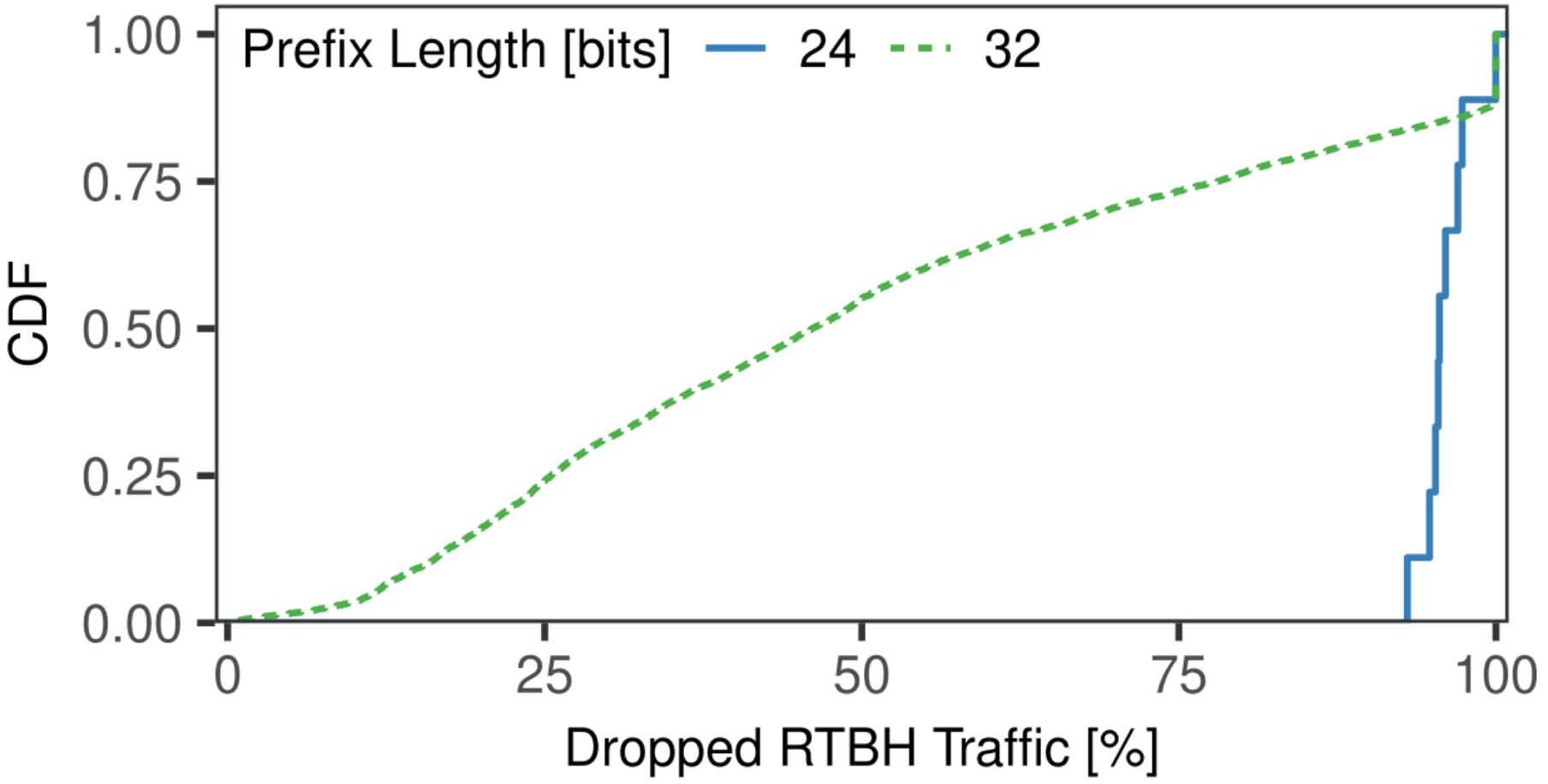
- All packets from/to prefixes, which have been blackholed at least once
- All packets which traverse the public switch-fabric (Sampling: 1/10000)
- *Dropped* packets identifiable by special MAC-address

Do all IXP member accept RTBH announcements ?

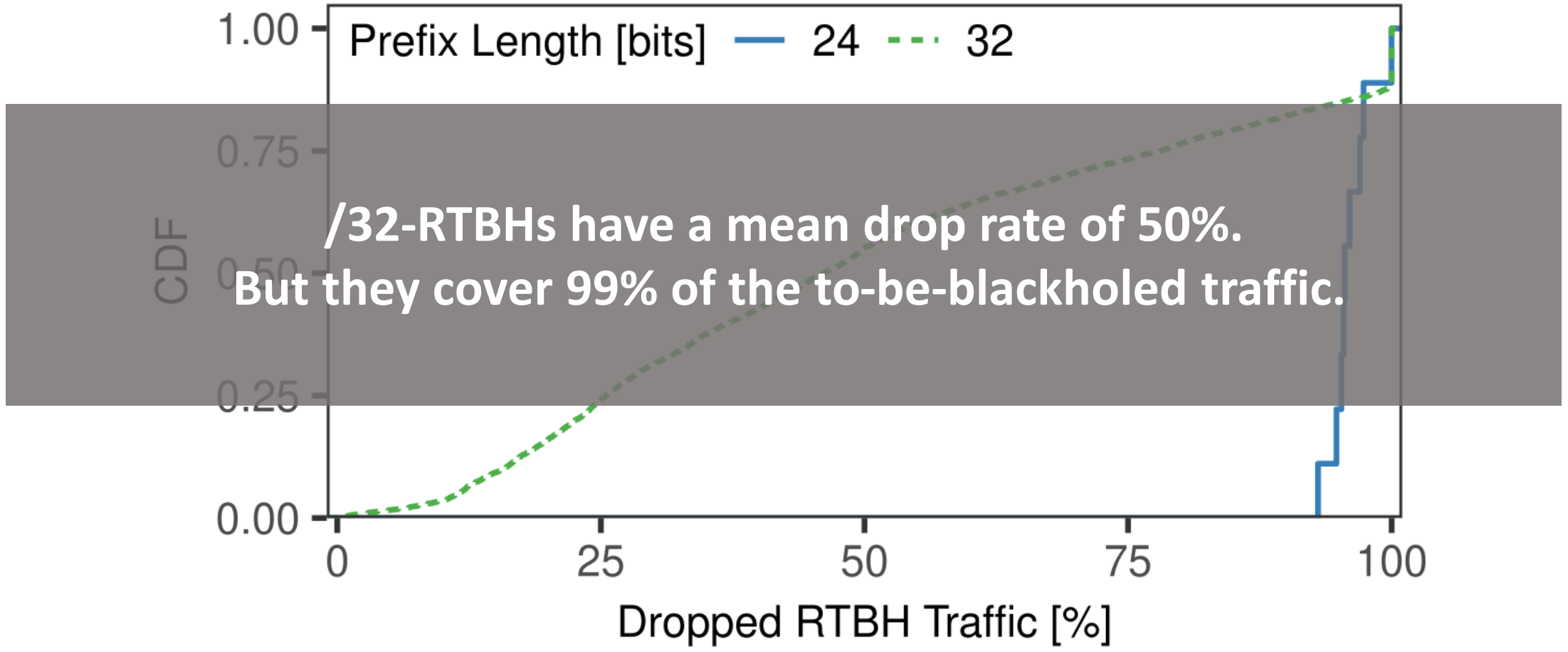
Successful mitigation depends on the announced RTBH prefix length



Successful mitigation depends on the announced RTBH prefix length

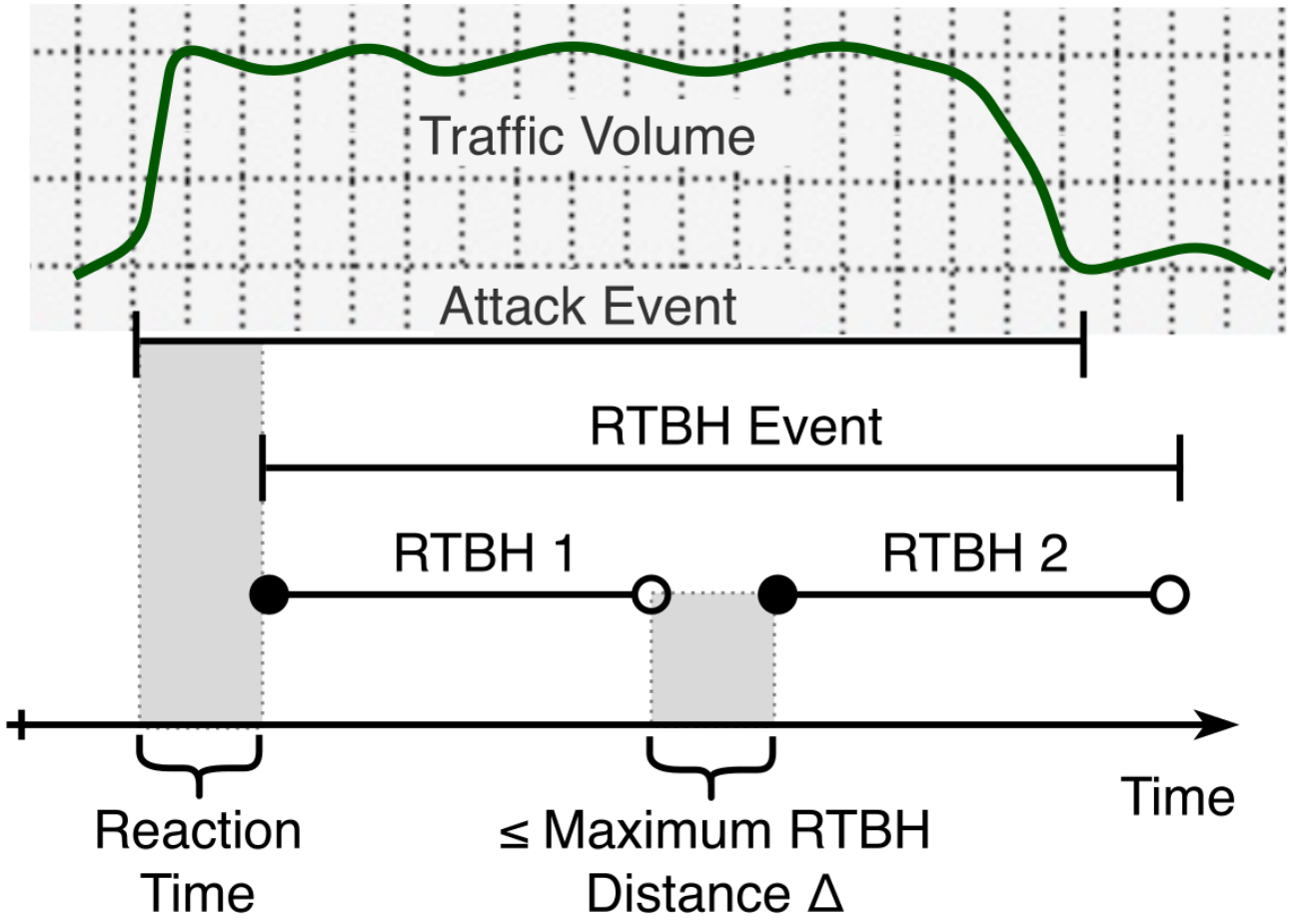


Successful mitigation depends on the announced RTBH prefix length



How much DDoS traffic do we actually see?

Measurement challenge
Multiple RTBHs cover the same attack



Data Plane (IPFIX)

Control Plane (BGP)

RTBH Announcement

RTBH Withdrawal

Analysis of 72 hours before an RTBH Event

Use a sliding window algorithm (EWMA) to infer whether one of the **monitored features** exhibits an anomalous peak:

Amplification Attacks	i. number of packets
	ii. number of unique destination ports
TCP SYN Attacks	iii. number of flows
	iv. number of unique source IP addresses
GRE Floods	v. number of non-TCP flows

But: Anomalies before RTBH are uncommon!

Traffic ≤ 72 hours	Anomaly ≤ 10 min	% RTBH Events
✓	✓	27%
✓	X	27%
X	-	46%

Vantage Point Bias?

Packet sampling might hide low-intensity attacks

A central vantage-point introduces location bias

Large ASs might use blackholing on all their peering links when there is a DDoS at only a single location

Related work using distributed measurements reached similar results

Jonker, Mattijs, et al. "A First Joint Look at DoS Attacks and BGP Blackholing in the Wild." Proceedings of the Internet Measurement Conference 2018. ACM, 2018.

Vantage Point Bias?

Packet sampling might hide low-intensity attacks

A central vantage-point introduces location bias

Large ASs might use blackholing on all their peering links when there is a DDoS at only a single location

Related work using distributed measurements reached similar results

IXPs have limitations to study DDoS attacks.

Jonker, Mattijs, et al. "A First Joint Look at DoS Attacks and BGP Blackholing in the Wild." Proceedings of the Internet Measurement Conference 2018. ACM, 2018.

Summary

The Internet is utterly complex and easily vulnerable.

If you think you don’t understand the Internet. You are probably right.

If you think all operators understand the Internet. Your are wrong.

Not all protection approaches work as expected.

Sound Internet measurements help.

Research and operator community benefit from each other.

Give something back to the Internet.

Talk to operators about your research.