Countering DDoS Attacks with Comprehensive ACLs learnt from Blackholing Traffic

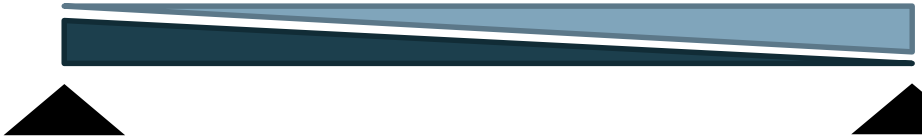
Matthias Wichtlhuber* | Alina Rubina* | Eric Strehle+ | Oliver Hohlfeld+

*DE-CIX | +Brandenburg University of Technology, Cottbus

matthias.wichtlhuber@de-cix.net

Motivation

- → Distributed Denial of Service is an ongoing threat to critical network infrastructure
- → Operator‘s toolbox:



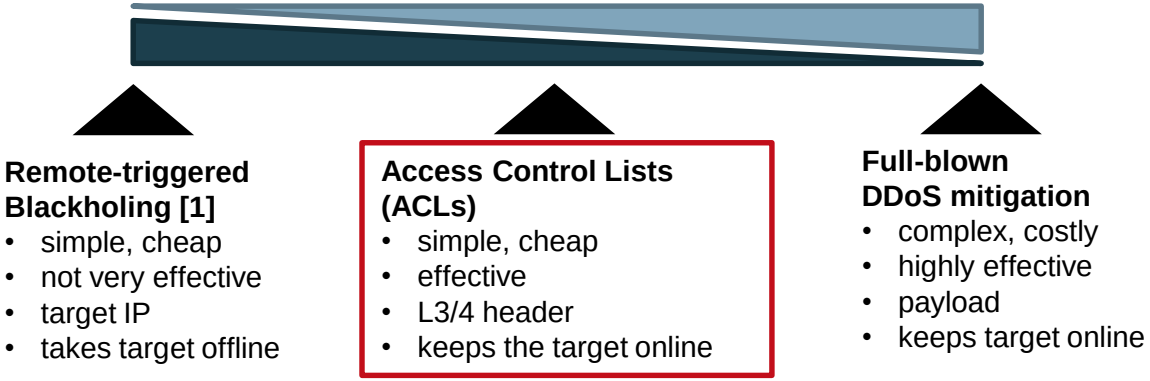
Remote-triggered Blackholing [1]
- simple, cheap
- not very effective
- target IP
- takes target offline

Full-blown DDoS mitigation
- complex, costly
- highly effective
- payload
- keeps target online

[1] T. King, C. Dietzel, J. Snijders et al.: „RFC7999: BLACKHOLE Community“, 2016.

Motivation

- → Distributed Denial of Service is an ongoing threat to critical network infrastructure
- → Operator‘s toolbox:



- → We are missing a validated, comprehensive list of ACLs covering the most relevant DDoS vectors

[1] T. King, C. Dietzel, J. Snijders et al.: „RFC7999: BLACKHOLE Community“, 2016.

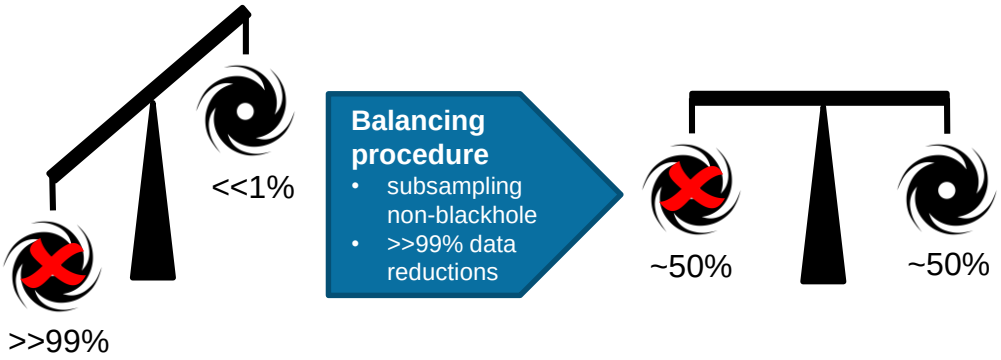
Our Approach

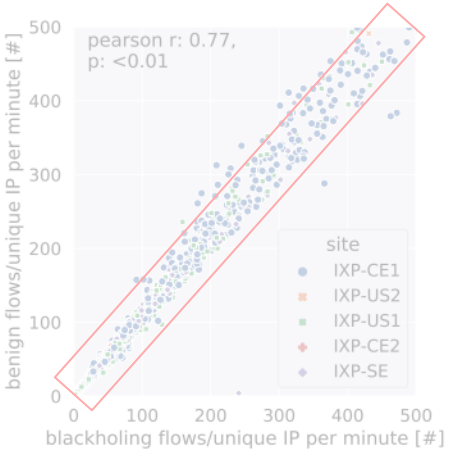
IXPs have a good visibility of RTBH traffic

- → DE-CIX sees around 3‘500 announced blackholes on average on route servers
- → Most of this is DDoS and signalled to be unwanted by customers

1. Collect sampled flow data (e.g. IPFIX) of RTBH traffic
2. Prepocess data and apply data mining algorithms
3. Generate a comprehensive (>300) list of ACLs for packet headers typically sent to a blackhole by IXP customers
4. Publish ACLs on GitHub

Preprocessing: Balancing



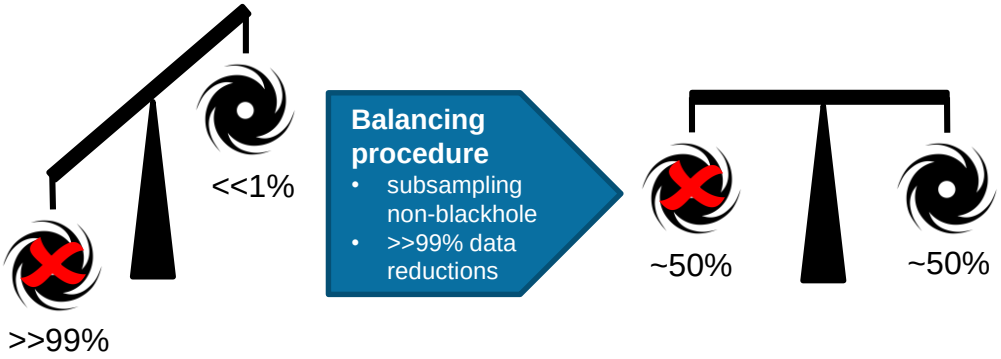


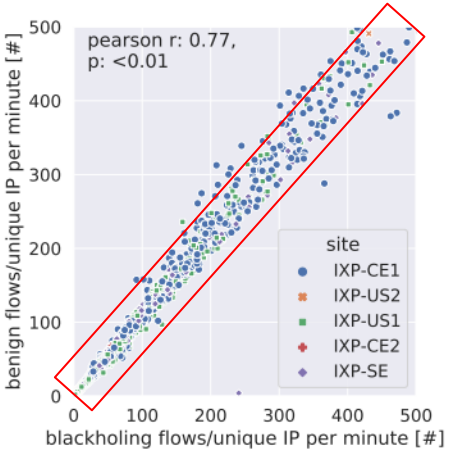
- Blackholing flows are highly underrepresented in overall flow export (<<1%)
- We balance by subsampling non-blackholing flows

→ Balanced flow export is <<1% of total flow export

→ Personal data like IPs is not needed and removed (GDPR compliance)

Preprocessing: Balancing





- Blackholing flows are highly underrepresented in overall flow export (<<1%)
- We balance by subsampling non-blackholing flows

→ Balanced flow export is <<1% of total flow export

→ Personal data like IPs is not needed and removed (GDPR compliance)

Background: Association Rule Mining (ARM)

- **Example:** Brian and Markus are shopping online

Buyer	Obscenely large TV	Wall mount	Drilling machine
Brian	Yes	Yes	Yes
Markus	Yes	Yes	No

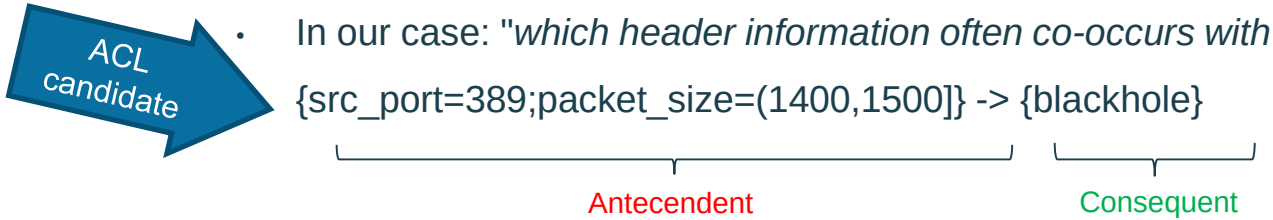
- Recommendations for Matthias shopping online
  - {large TV} → {wall mount} 100% of all baskets 
  - {large TV, drilling machine} → {wall mount} 100% of all baskets 
  - {drilling machine} → {large TV} 50% of all baskets 

→ Rules like these are **called association rules**

→ This is a way to identify **clusters of co-occurring items in the data**

Applying ARM to Traffic Data

- Association rule mining to identify (filterable) headers in the data
  - In our case: "*which header information often co-occurs with blackhole?*"

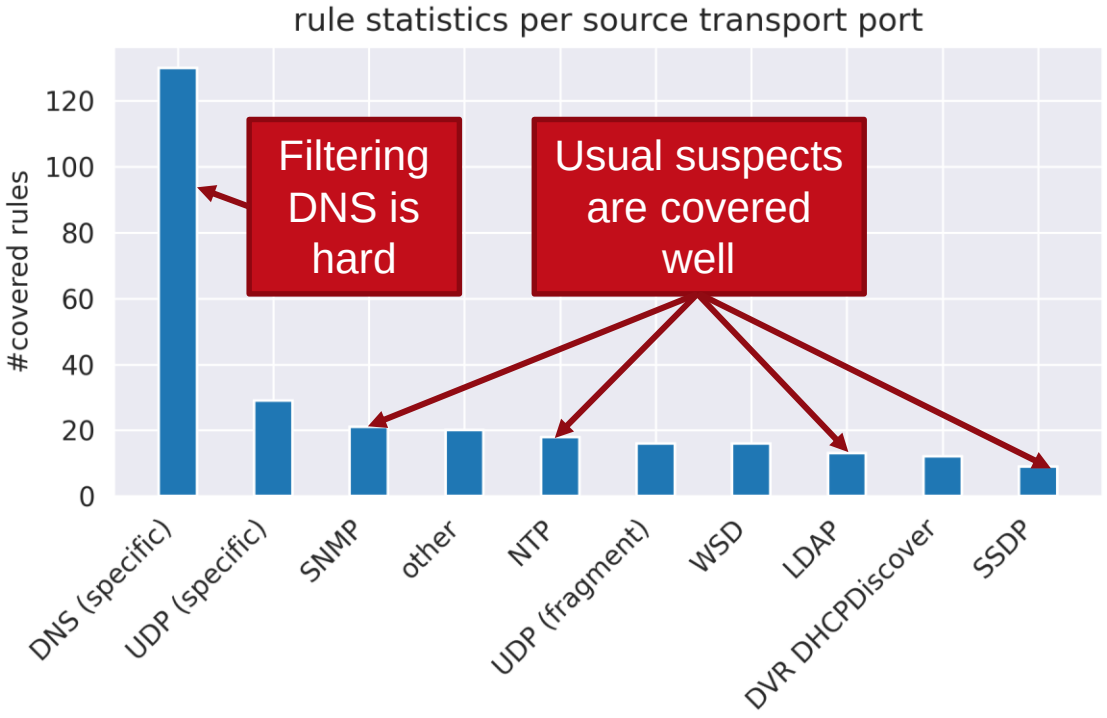


- Important metrics:
  - *antecendent support:* how often is the antecendent found in the training set?
    - relevance of attack vector
  - *confidence:* how often did the antecendent appear together with the consequent?
    - quality of classification (with 1.0 as the highest confidence)

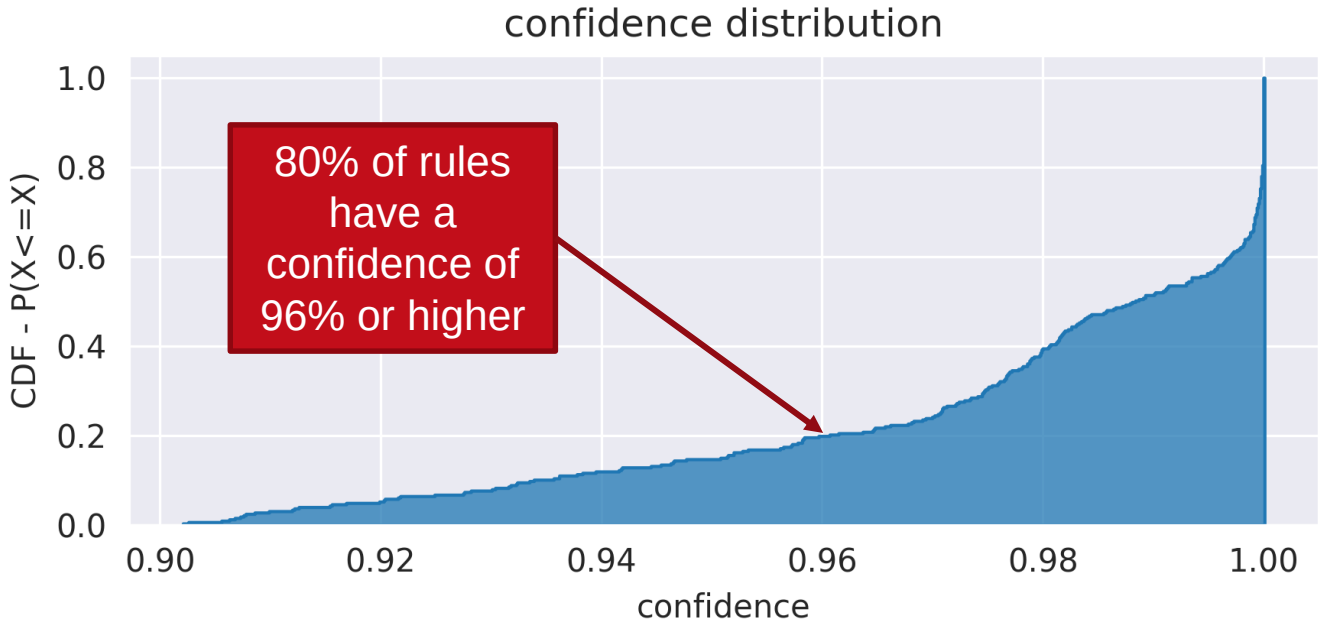
ACL Definition: Properties

```
"0a42ee90": {                    # ID of the filtering rule
  "protocol":17,                 # Protocol (UDP)
  "port_src":123,                # Source port (NTP)
  "port_dst":28960,              # Destination port (Call of Duty)
  "packet_size":"(400,500]",     # Packet size 400-500 Bytes
  "confidence":0.99,             # 99% of these flow were blackholed
  "antecedent support":1021,     # We have seen 1021 of these flows
}
```

Analysis of generated ACLs (1/2)



Analysis of generated ACLs (2/2)



DE CIX

How to use this …

➔The ACLs are hosted as JSON on github

- https://github.com/DE-CIX/ripe84-learning-acls

➔Convert the list into a suitable config format for your networking gear

- Anybody here that wants to contribute a script? → Pull Request

➔Deploy and apply to a prefix whenever neccessary

- Use as an additional escalatory step before blackholing/scrubbing

DE CIX

Thank You for Your attention!

DE-CIX Management GmbH | Lindleystr. 12 | 60314 Frankfurt | Germany
Phone + 49 69 1730 902 0 | sales@de-cix.net | www.de-cix.net