UNIVERSITÄT DES SAARLANDES

Unpacking Internet Ossification: A Large-Scale Study of Path-Impairing Middleboxes Across IPv4 and IPv6

Fahad Hilal, Taha Albakour, Oliver Gasser, Kevin Vermeulen

PAM 2026

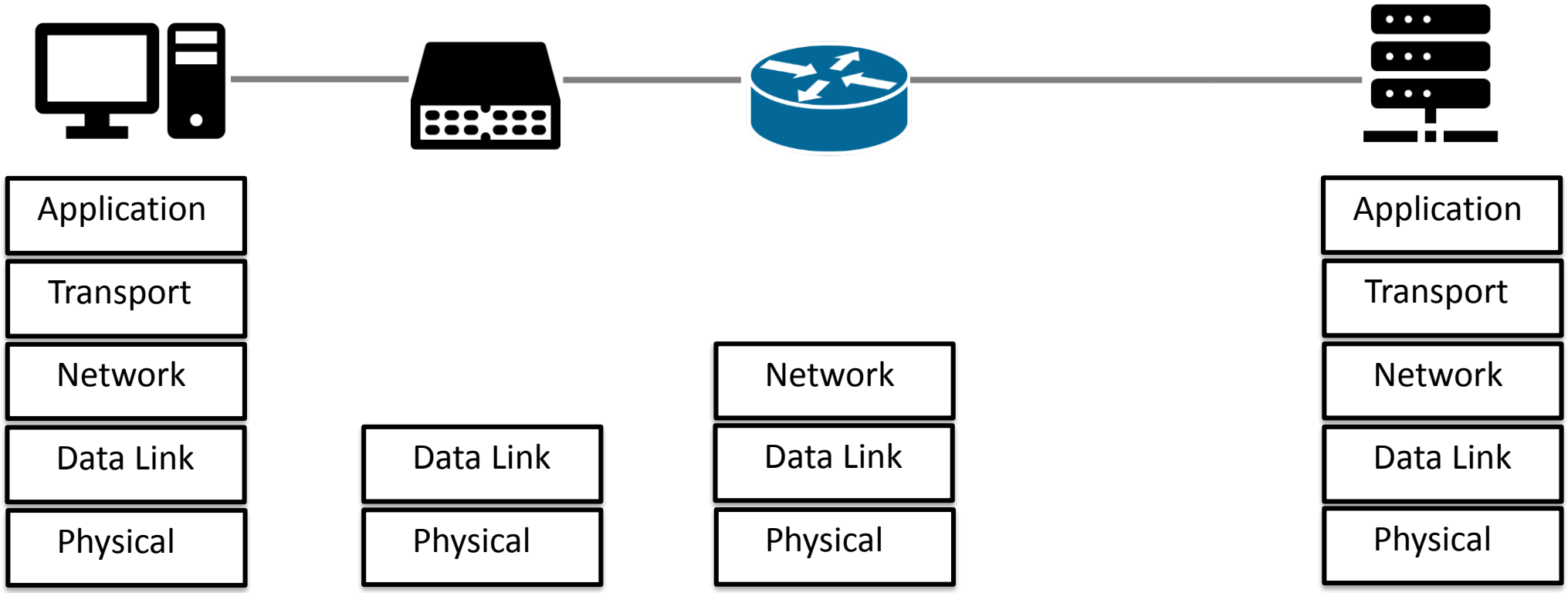
MAX PLANCK INSTITUTE FOR INFORMATICS

IPinfo

ÉCOLE POLYTECHNIQUE

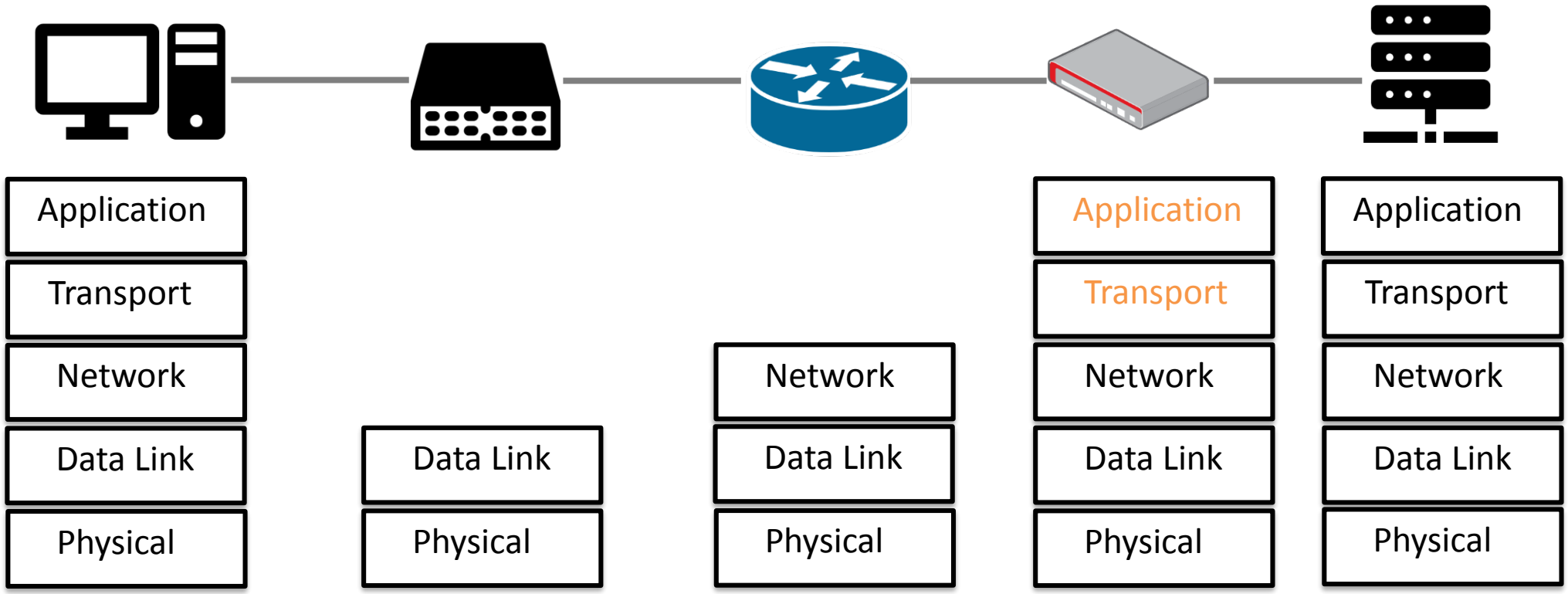
The Traditional Internet-End-to-End Principle

- Simplicity in middle, intelligence at ends



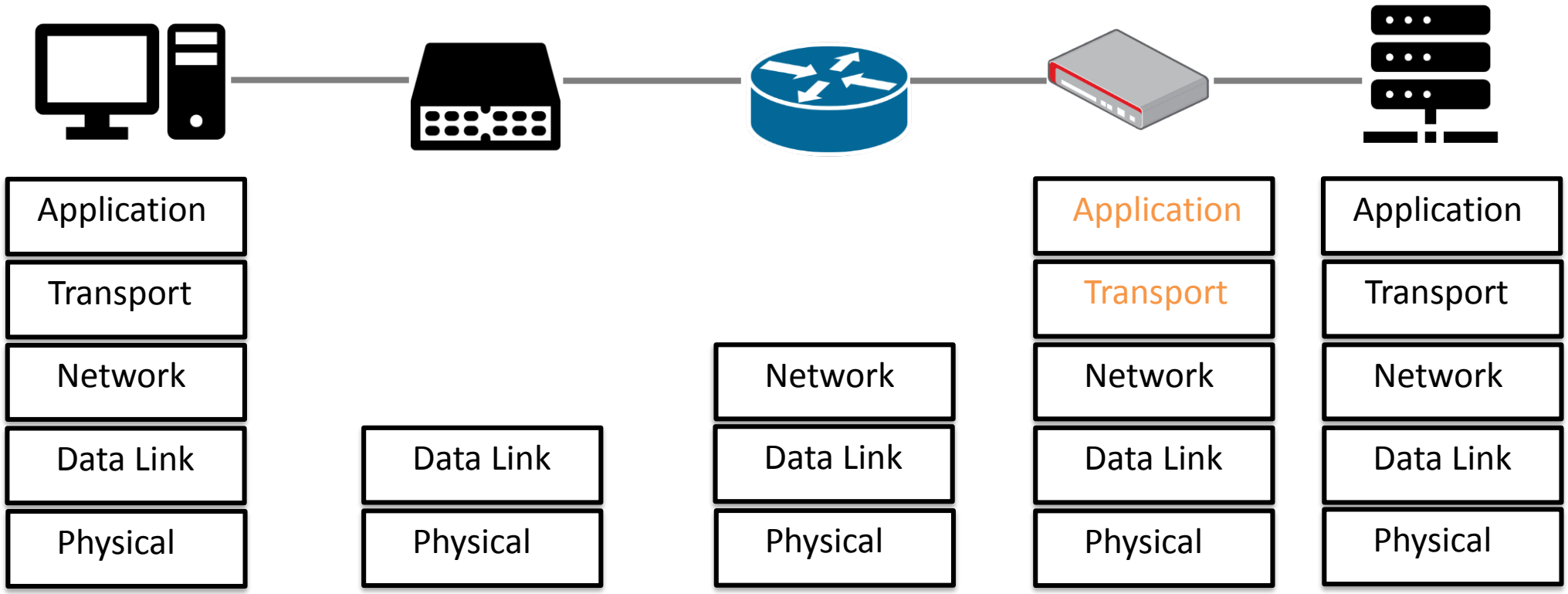
Growing Complexity-Middleboxes

- Internet as ***deployed***, no longer as ***designed***



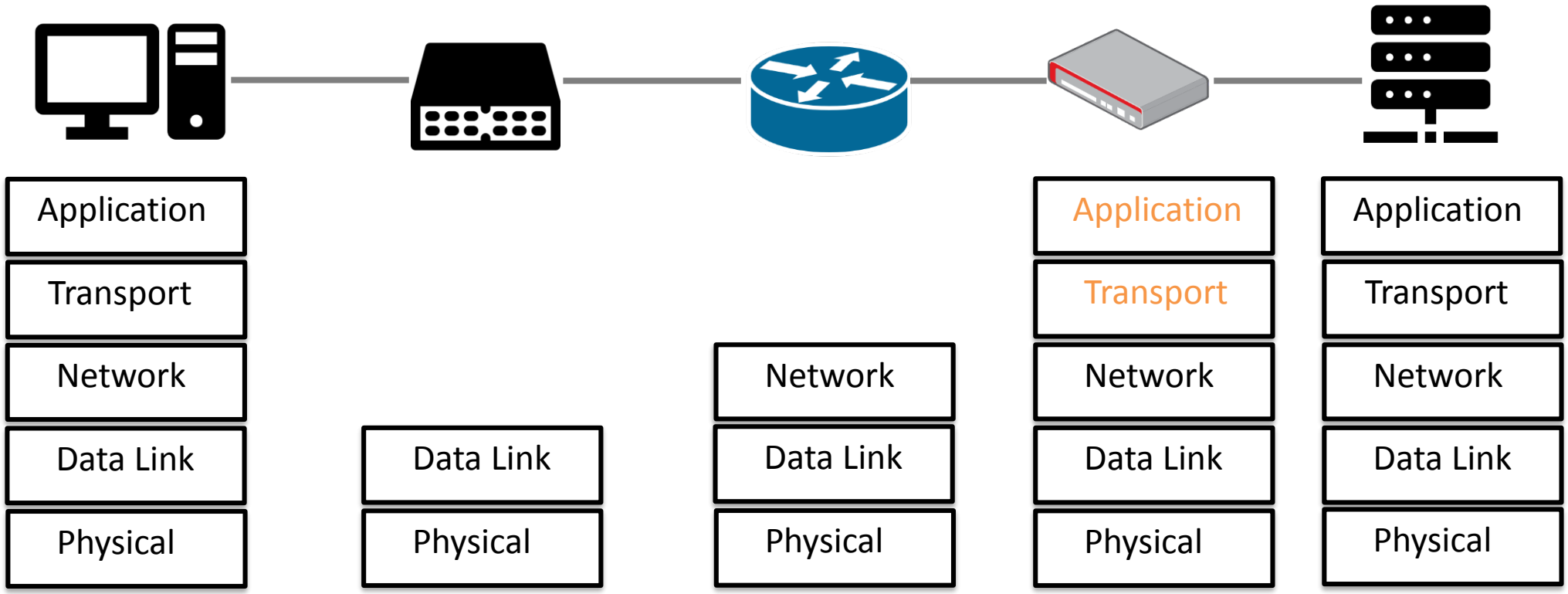
Growing Complexity-Middleboxes

- Internet as ***deployed***, no longer as ***designed***
- ***Invasion*** of ***middleboxes***



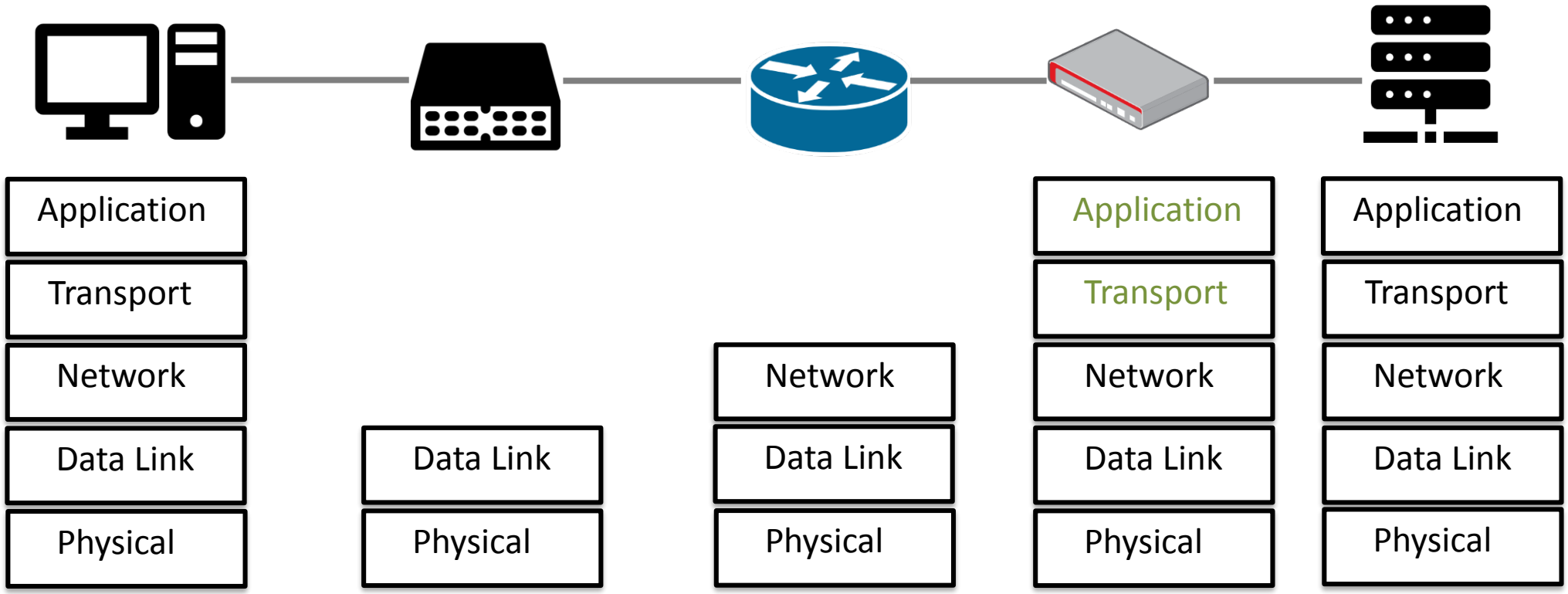
Growing Complexity-Middleboxes

- Internet as ***deployed***, no longer as ***designed***
- ***Invasion*** of ***middleboxes***
  - Inspect, filter, modify



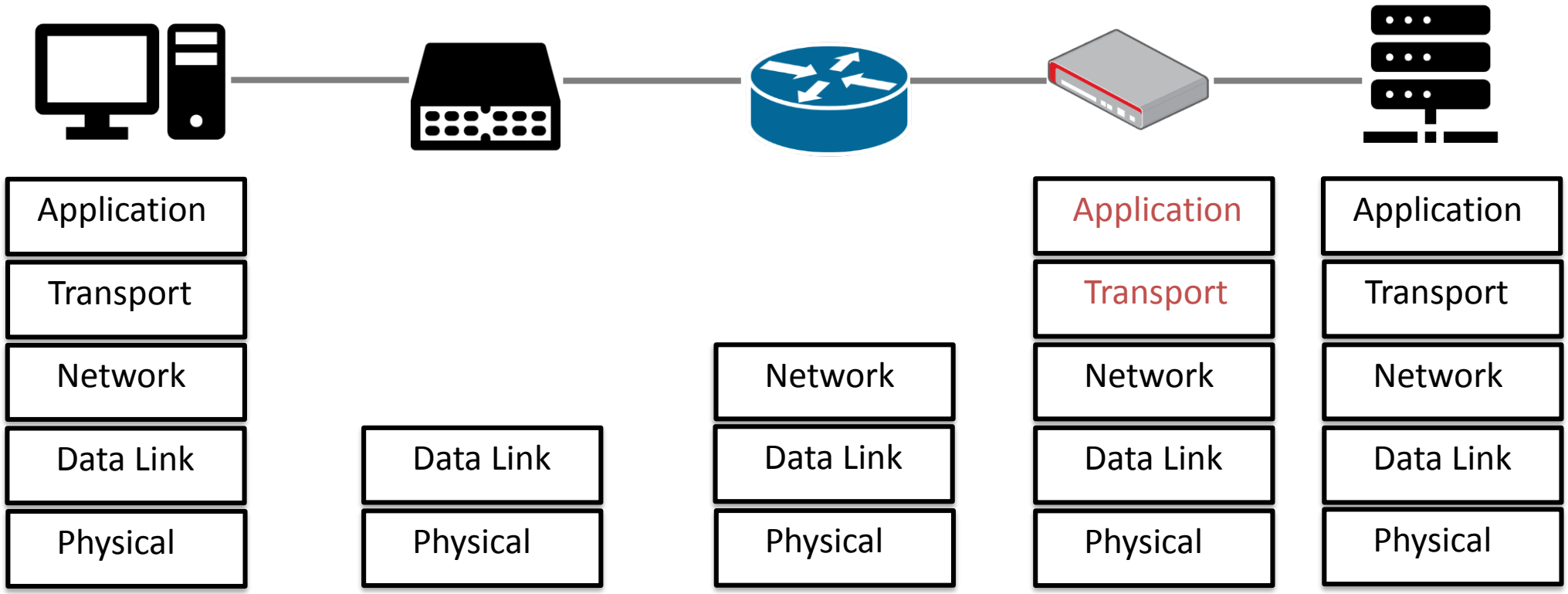
Growing Complexity-Middleboxes

- Internet as ***deployed***, no longer as ***designed***
- ***Invasion*** of ***middleboxes***
  - Inspect, filter, modify
  - Thwart attacks, expand address space, balance resources



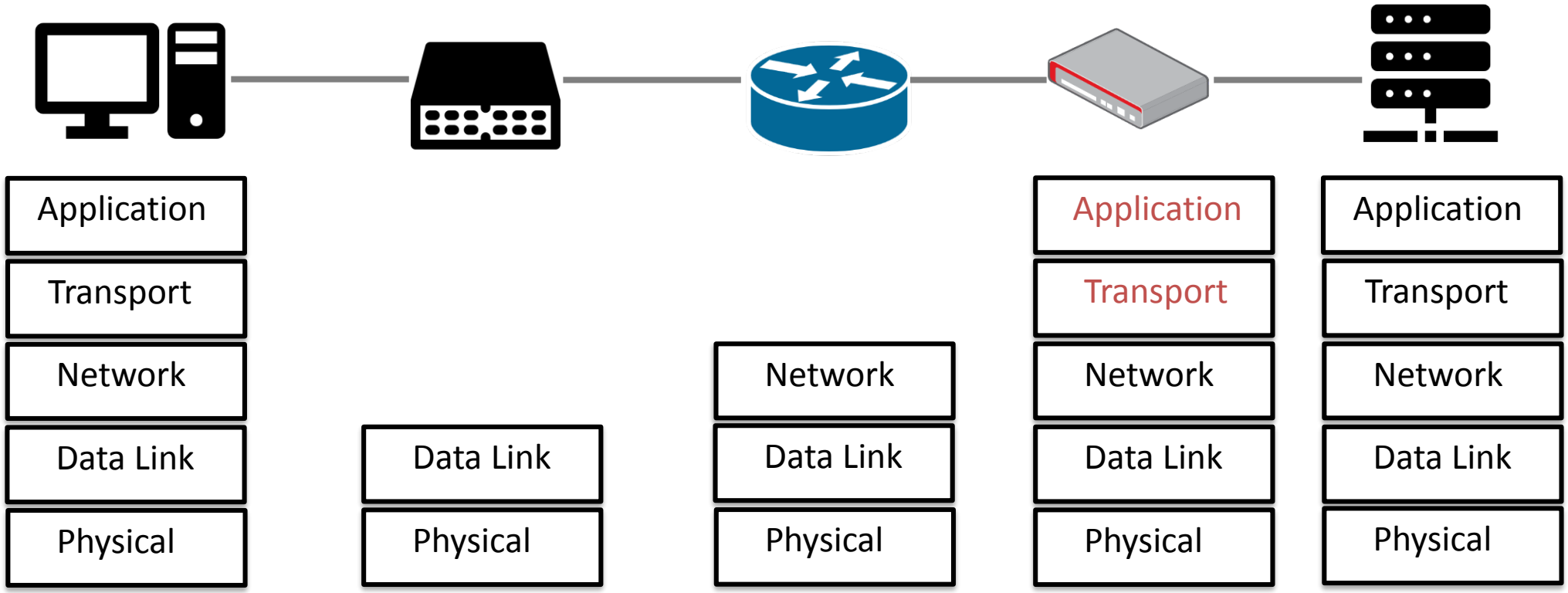
Growing Complexity-Middleboxes

- Internet as ***deployed***, no longer as ***designed***
- ***Invasion*** of ***middleboxes***
  - Ossification



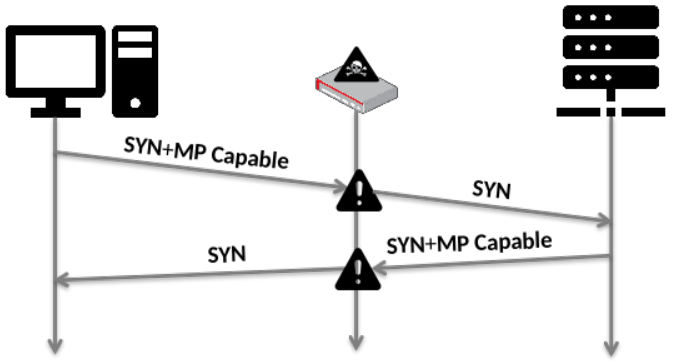
Growing Complexity-Middleboxes

- Internet as ***deployed***, no longer as ***designed***
- ***Invasion*** of ***middleboxes***
  - Ossification
    - DCCP, SCTP standardized,
    - ***Failed*** to be deployed at large scale



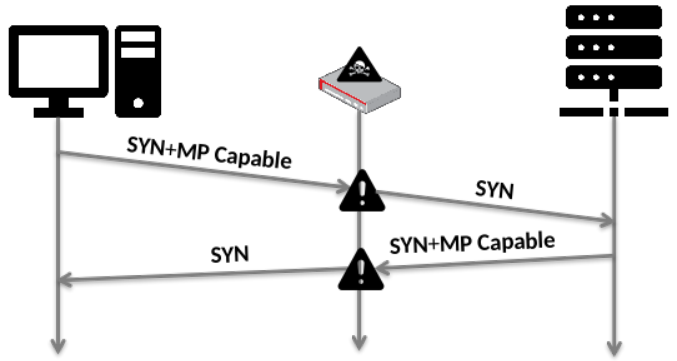
Contributions

- Path-Impairing middleboxes (MBs)
  - Unexpected alterations ***(impairments)*** to TCP/IP packet headers
    - e.g., TCP option removals



Contributions

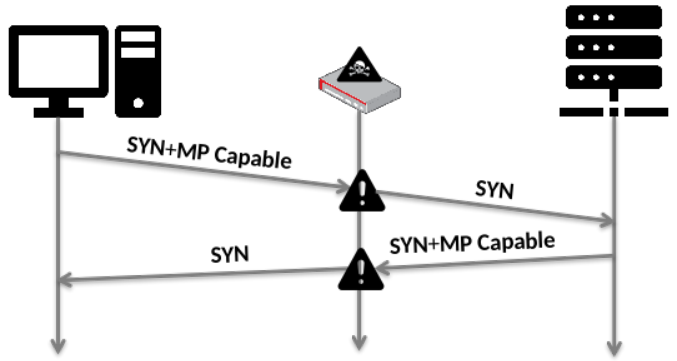
- Path-Impairing middleboxes (MBs)
  - Unexpected alterations ***(impairments)*** to TCP/IP packet headers
    - e.g., TCP option removals
  - Prior work
    - One-off snapshots [1, 2, 3], small-scale [2, 3], IPv4 only [2, 3]



[1] Hilal, Fahad, and Oliver Gasser. "Yarrpbox: Detecting middleboxes at Internet-scale." ACM CoNEXT 2023.
[2] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.
[3] Detal, Gregory, et al. "Revealing middlebox interference with tracebox." ACM IMC 2013.

Contributions

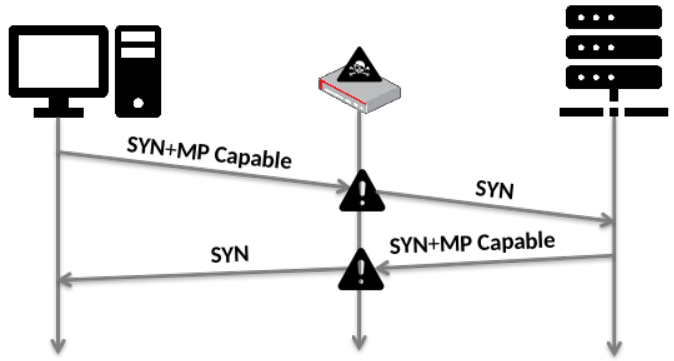
- Path-Impairing middleboxes (MBs)
  - Unexpected alterations ***(impairments)*** to TCP/IP packet headers
    - e.g., TCP option removals
  - Prior work
    - One-off snapshots [1, 2, 3], small-scale [2, 3], IPv4 only [2, 3]
      - Internet-scale view of ***prevalence*** and ***impact***?



[1] Hilal, Fahad, and Oliver Gasser. "Yarrpbox: Detecting middleboxes at Internet-scale." ACM CoNEXT 2023.
[2] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.
[3] Detal, Gregory, et al. "Revealing middlebox interference with tracebox." ACM IMC 2013.

Contributions

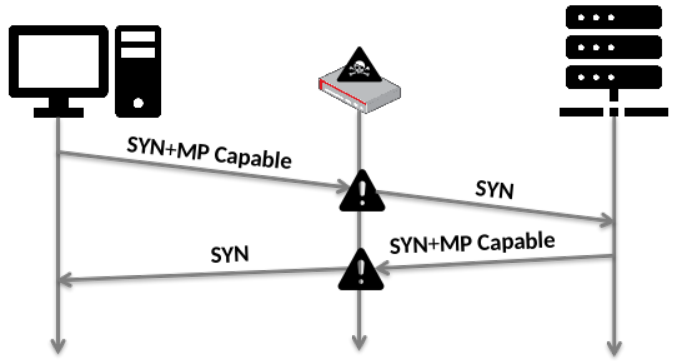
- Path-Impairing middleboxes (MBs)
  - Unexpected alterations ***(impairments)*** to TCP/IP packet headers
    - e.g., TCP option removals
  - Prior work
    - One-off snapshots [1, 2, 3], small-scale [2, 3], IPv4 only [2, 3]
      - Internet-scale view of ***prevalence*** and ***impact***?
      - ***IPv6*** less impaired?



[1] Hilal, Fahad, and Oliver Gasser. "Yarrpbox: Detecting middleboxes at Internet-scale." ACM CoNEXT 2023.
[2] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.
[3] Detal, Gregory, et al. "Revealing middlebox interference with tracebox." ACM IMC 2013.

Contributions

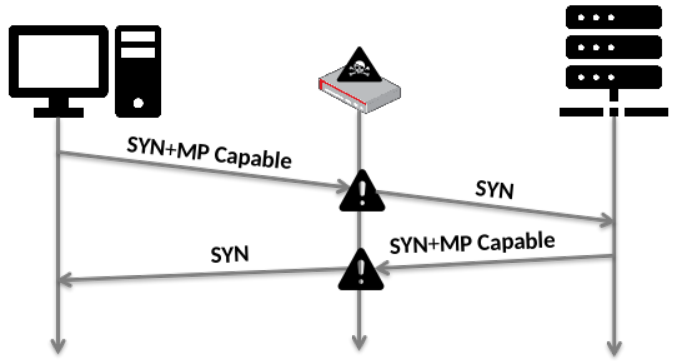
- Path-Impairing middleboxes (MBs)
  - Unexpected alterations ***(impairments)*** to TCP/IP packet headers
    - e.g., TCP option removals
  - Prior work
    - One-off snapshots [1, 2, 3], small-scale [2, 3], IPv4 only [2, 3]
      - Internet-scale view of ***prevalence*** and ***impact***?
      - ***IPv6*** less impaired?
      - Root ***causes***?



[1] Hilal, Fahad, and Oliver Gasser. "Yarrpbox: Detecting middleboxes at Internet-scale." ACM CoNEXT 2023.
[2] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.
[3] Detal, Gregory, et al. "Revealing middlebox interference with tracebox." ACM IMC 2013.

Contributions

- Path-Impairing middleboxes (MBs)
  - Unexpected alterations ***(impairments)*** to TCP/IP packet headers
    - e.g., TCP option removals
  - Prior work
    - One-off snapshots [1, 2, 3], small-scale [2, 3], IPv4 only [2, 3]
      - Internet-scale view of ***prevalence*** and ***impact***?
      - ***IPv6*** less impaired?
      - Root ***causes***?
      - Stability?



[1] Hilal, Fahad, and Oliver Gasser. "Yarrpbox: Detecting middleboxes at Internet-scale." ACM CoNEXT 2023.
[2] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.
[3] Detal, Gregory, et al. "Revealing middlebox interference with tracebox." ACM IMC 2013.

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?
- How are announced prefixes and popular domains ***affected***?

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?
- How are announced prefixes and popular domains ***affected***?
- Are path-impairing MBs ***stable*** over short and long periods?

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?
- How are announced prefixes and popular domains ***affected***?
- Are path-impairing MBs ***stable*** over short and long periods?
- How can we engage with network ***operators*** to aid de-ossification?

Measurement Setup-Yarrpbox

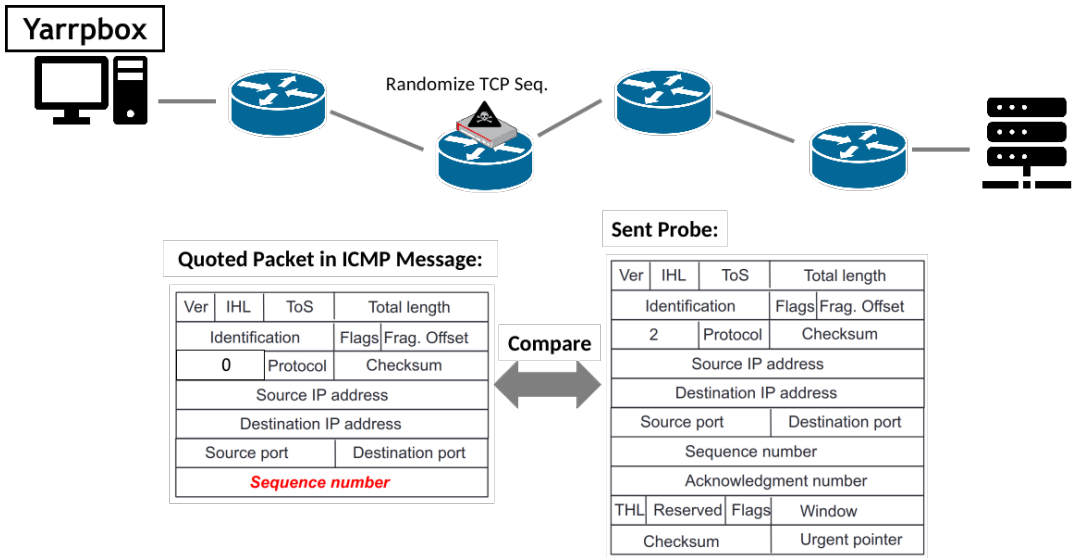
UNIVERSITÄT DES SAARLANDES

- **Features**
  - Internet-scale path-impairing MB detector [1]
    - On-path Impairments
    - ***Approx. topl.*** position of path-impairing MB

[1] Hilal, Fahad, and Oliver Gasser. "Yarrpbox: Detecting middleboxes at Internet-scale." ACM CoNEXT 2023.

Measurement Setup-Yarrpbox

- **Features**
  - Internet-scale path-impairing MB detector [1]
    - On-path Impairments
    - ***Approx. topl.*** position of path-impairing MB
- **Operation**
  - TTL-limited probes -> ICMP msgs -> packet state on Internet paths



[1] Hilal, Fahad, and Oliver Gasser. "Yarrpbox: Detecting middleboxes at Internet-scale." ACM CoNEXT 2023.

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?

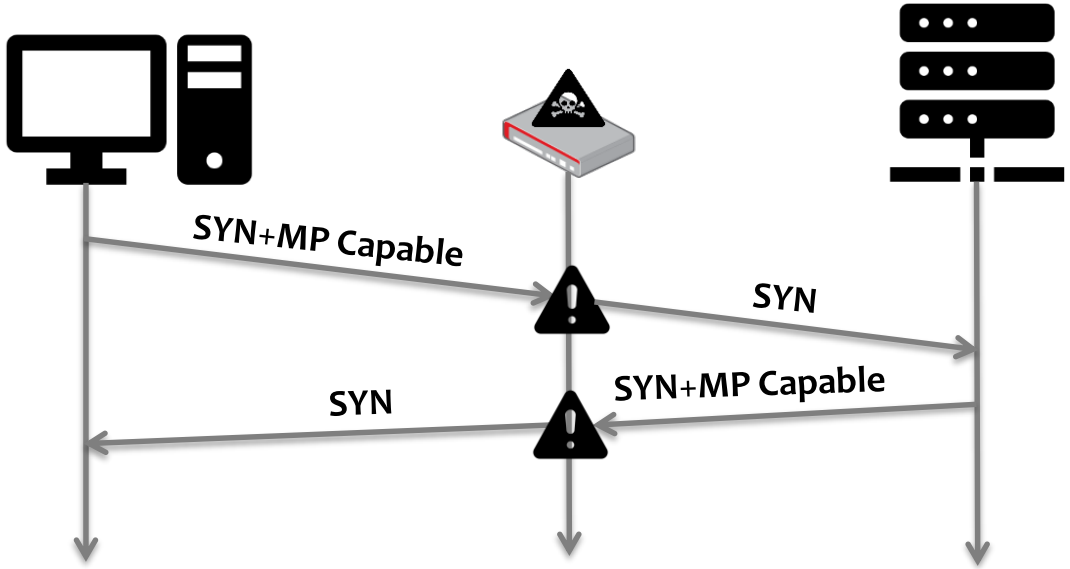
Analysis Heuristic-Path Impairing MB Behavior Taxonomy

UNIVERSITÄT DES SAARLANDES

- **Categories**
  - Feature Disabling (DF), Disrupted Traffic (DT), Negotiation Disruption (ND) [1]

[1] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.

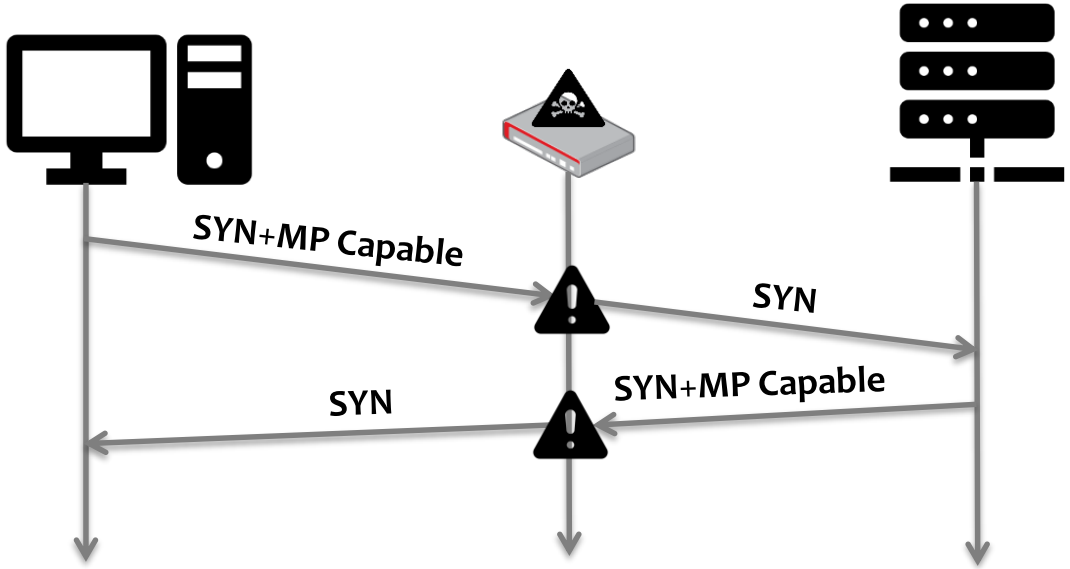
Analysis Heuristic-Path Impairing MB Behavior Taxonomy



- **Disabling Features (DF)** [1]

[1] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.

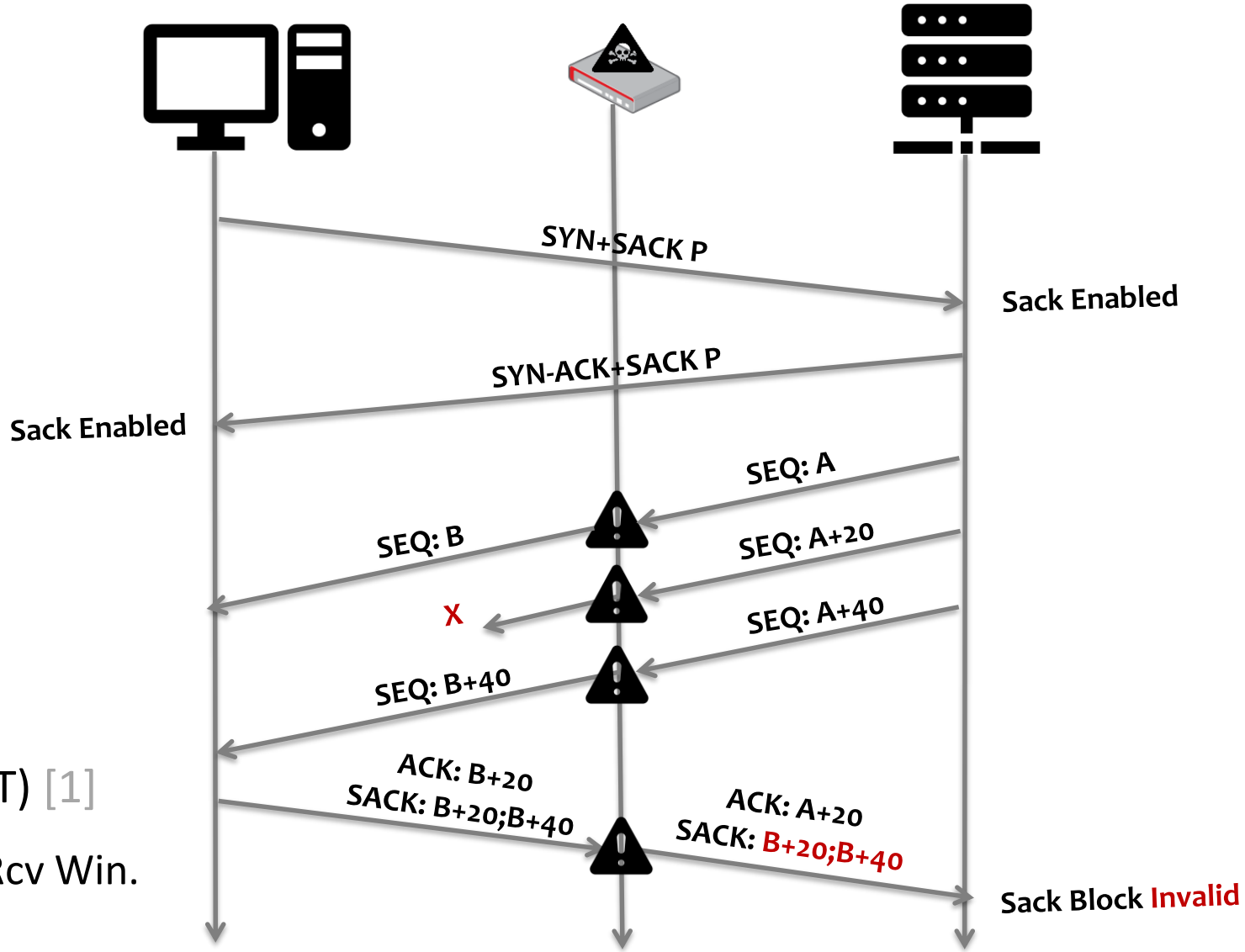
Analysis Heuristic-Path Impairing MB Behavior Taxonomy



- **Disabling Features (DF)** [1]
  - TCP opts. removal, ECN disable

[1] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.

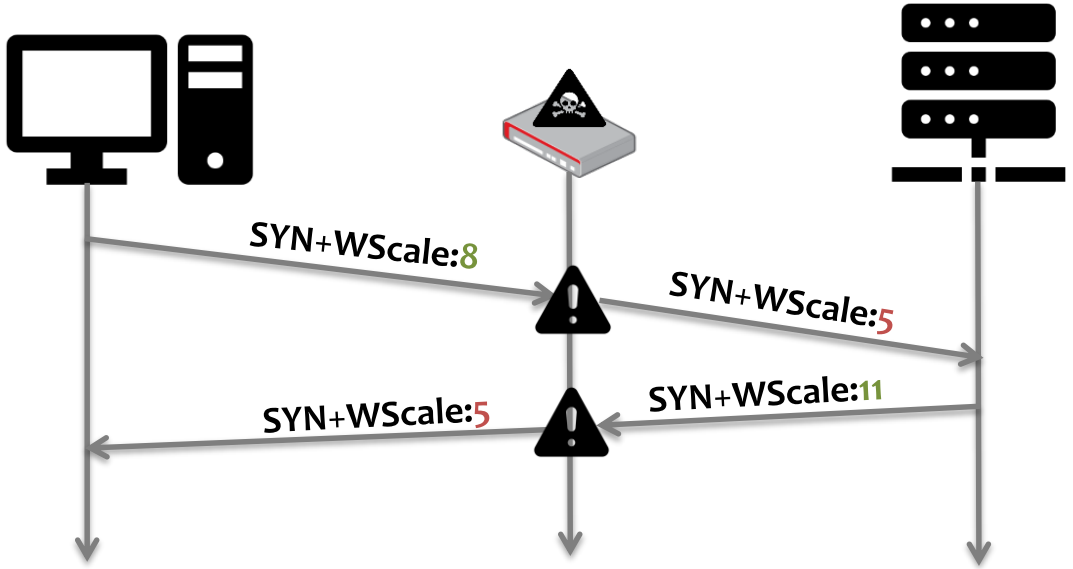
Analysis Heuristic-Path Impairing MB Behavior Taxonomy



- **Disrupted Traffic** (DT) [1]
  - TCP Seq No., TCP Rcv Win.

[1] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.

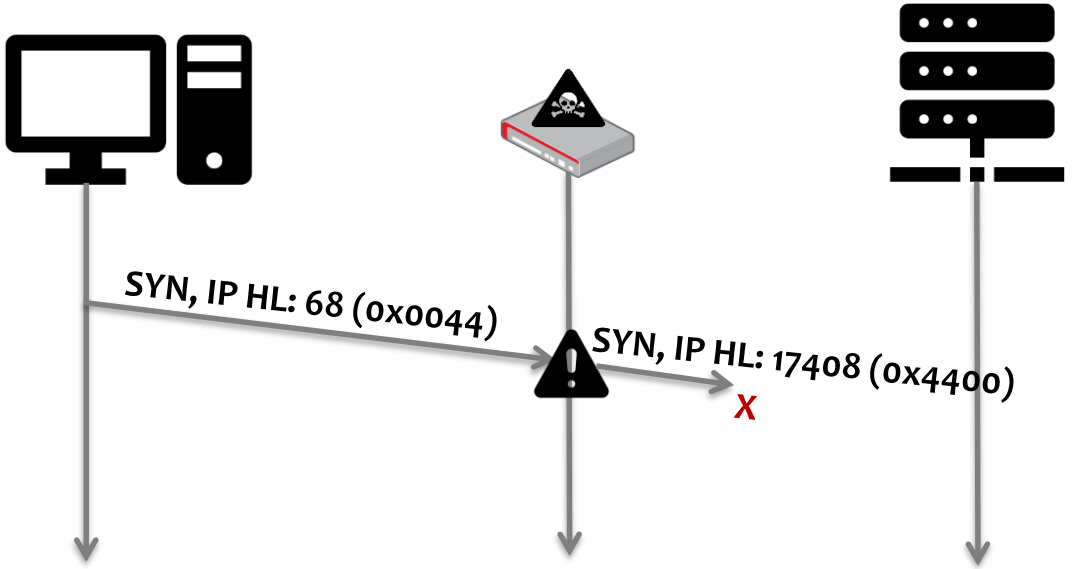
Analysis Heuristic-Path Impairing MB Behavior Taxonomy



- **Negotiation Disruption (ND)** [1]
  - TCP WScale, SACK P.

[1] Edeline, Korian, and Benoit Donnet. "A bottom-up investigation of the transport-layer ossification." TMA 2019.

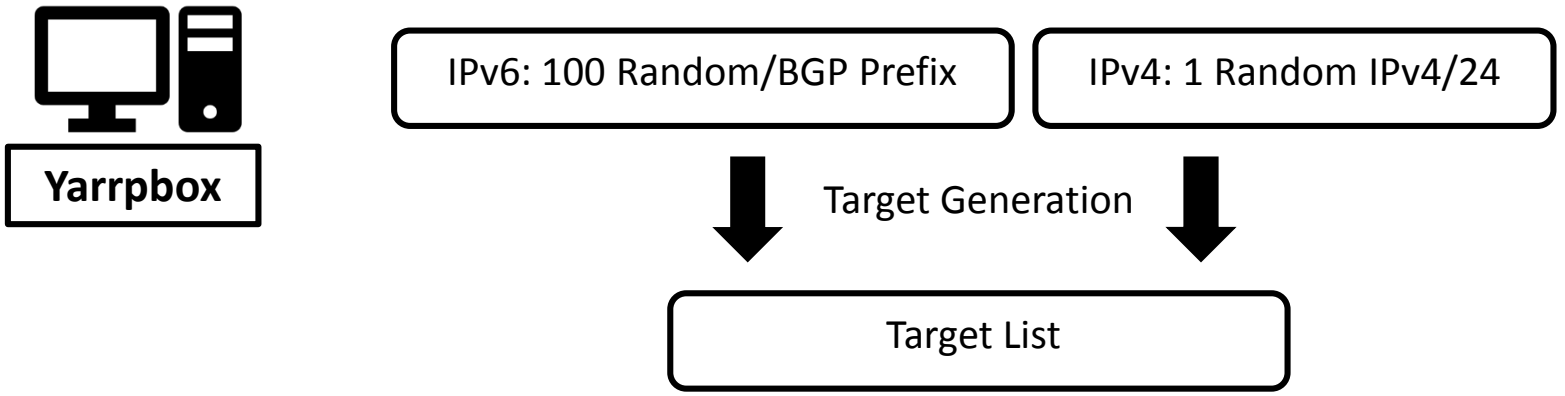
Analysis Heuristic-Path Impairing MB Behavior Taxonomy



- **Potential for blocks (PB)**
  - Sole IP HL alterations
    - Often byte order flips

Measurements and Results

Measurements

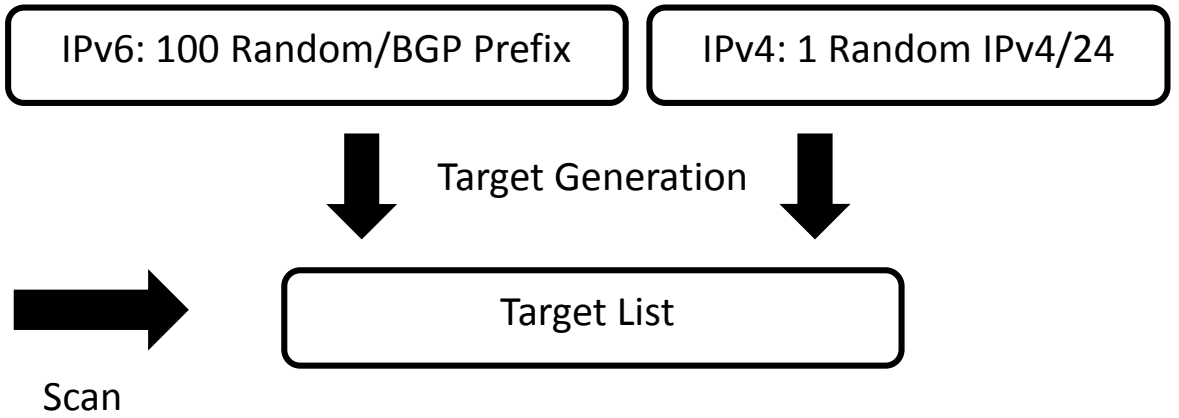


Measurements

Yarrpbox

Ver	HL	TOS	Total Length
Identification		Fl.	Frag. Offset
TTL	Protocol	Checksum	
Source IP			
Destination IP			

Source Port	Dest. Port (80,443)
Sequence Number	
Acknowledgement Number	
DO / RSVD / SYN,ECE, CWR	Window Size
Checksum	Urgent Pointer
TCP Options (MSS, SACK P, MP CAPABLE, TMSP)	



Measurements

Yarrpbox

Ver	HL	TOS	Total Length
Identification		Fl.	Frag. Offset
TTL	Protocol	Checksum	
Source IP			
Destination IP			

Source Port	Dest. Port (80,443)
Sequence Number	
Acknowledgement Number	
DO / RSVD / SYN,ECE, CWR	Window Size
Checksum	Urgent Pointer
TCP Options (MSS, SACK P, MP CAPABLE, TMSP)	

IPv6: 100 Random/BGP Prefix

IPv4: 1 Random IPv4/24

Target Generation

Scan

Target List

Analysis

Path-Impairments

Path-Impairing MBs

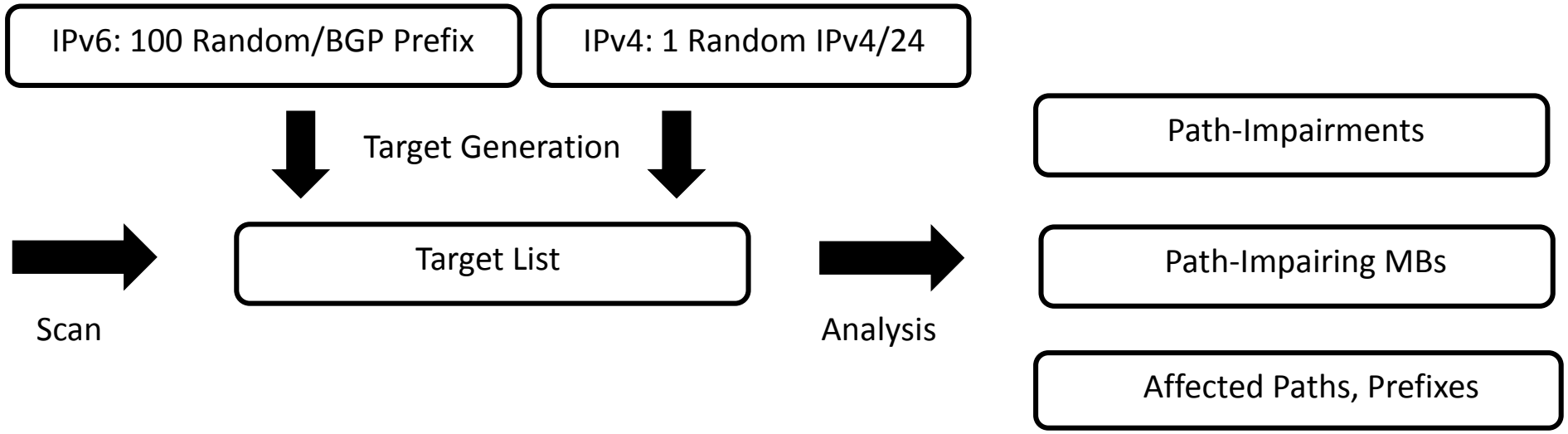
Affected Paths, Prefixes

Measurements

Yarrpbox

Ver	HL	TOS	Total Length
Identification		Fl.	Frag. Offset
TTL	Protocol	Checksum	
Source IP			
Destination IP			

Source Port	Dest. Port (80,443)
Sequence Number	
Acknowledgement Number	
DO / RSVD / SYN,ECE, CWR	Window Size
Checksum	Urgent Pointer
TCP Options (MSS, SACK P, MP CAPABLE, TMSP)	



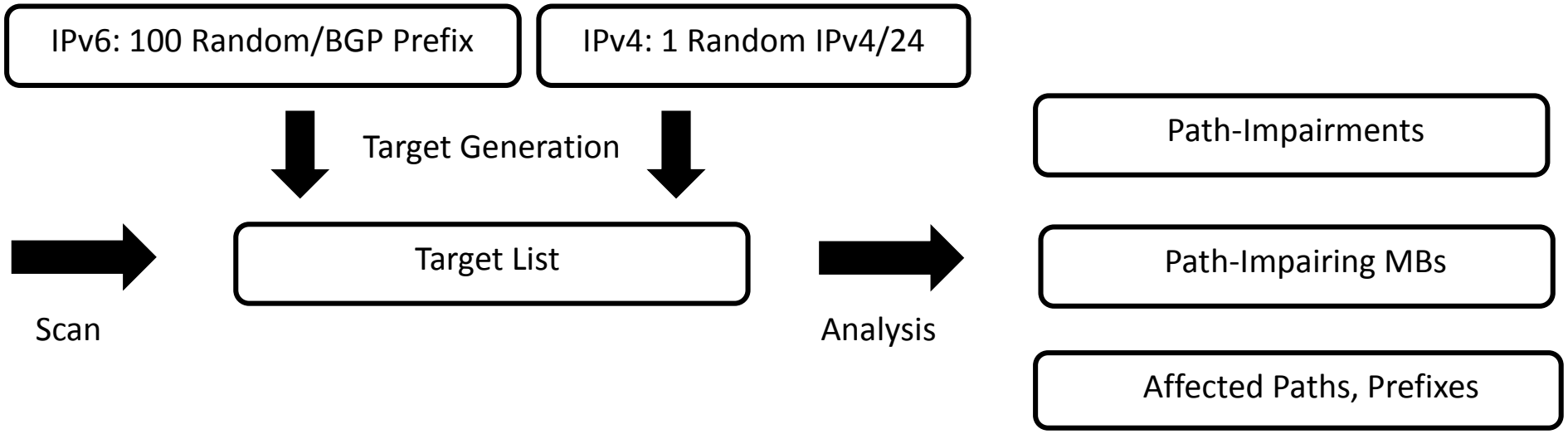
- **Tested paths**
  - IPv6: 251.6M, IPv4:156.9M
  - 3x paths, 10x more on-path ASes

Measurements

Yarrpbox

Ver	HL	TOS	Total Length
Identification		Fl.	Frag. Offset
TTL	Protocol	Checksum	
Source IP			
Destination IP			

Source Port	Dest. Port (80,443)
Sequence Number	
Acknowledgement Number	
DO / RSVD / SYN,ECE,CWR	Window Size
Checksum	Urgent Pointer
TCP Options (MSS, SACK P, MP CAPABLE, TMSP)	



- **Path-impairing MBs**
  - IPv6: 778 in 241 ASes, IPv4: 5.8k in 1.8k ASes

Measurements

Yarrpbox

Ver	HL	TOS	Total Length
Identification		Fl.	Frag. Offset
TTL	Protocol	Checksum	
Source IP			
Destination IP			

Source Port	Dest. Port (80,443)
Sequence Number	
Acknowledgement Number	
DO RSVD SYN,ECE, CWR	Window Size
Checksum	Urgent Pointer
TCP Options (MSS, SACK P, MP CAPABLE, TMSP)	

Scan

Target List

Measurements

MassDNS

Tranco Top 1M Domains

Resolve

IPv6 addresses

IPv4 addresses

Target List

Scan

Analysis

Yarrpbox

Ver	HL	TOS	Total Length
Identification	Fl.	Frag. Offset	
TTL	Protocol	Checksum	
Source IP			
Destination IP			

Source Port	Dest. Port (80,443)
Sequence Number	
Acknowledgement Number	
DO RSVD SYN,ECE, CWR	Window Size
Checksum	Urgent Pointer
TCP Options (MSS, SACK P, MP CAPABLE, TMSP)	

Measurements

MassDNS

Tranco Top 1M Domains

Resolve

IPv6 addresses

IPv4 addresses

Target List

Scan

Analysis

Path-Impairments

Path-Impairing MBs

Affected Paths, Domains, Targets

Yarrpbox

Ver	HL	TOS	Total Length
Identification		Fl.	Frag. Offset
TTL	Protocol		Checksum
Source IP			
Destination IP			

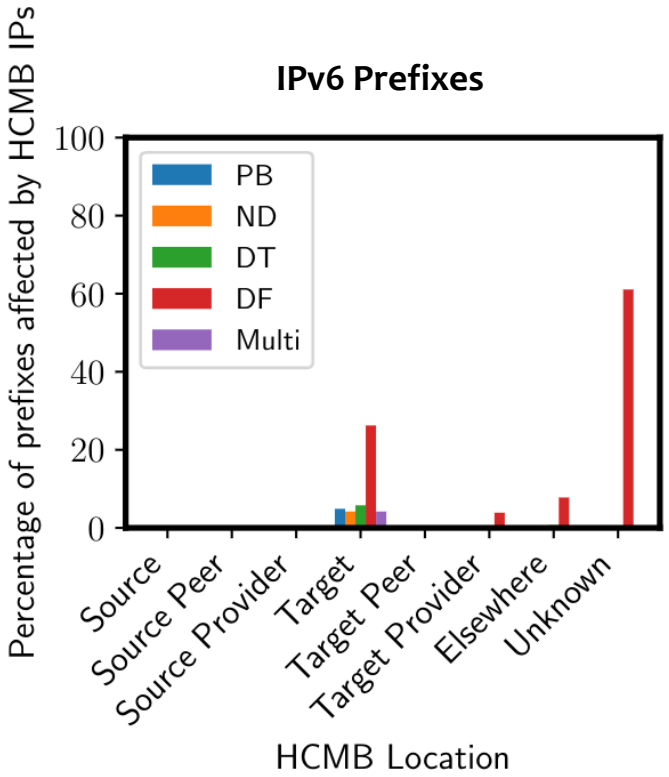
Source Port	Dest. Port (80,443)
Sequence Number	
Acknowledgement Number	
DO RSVD SYN,ECE,CWR	Window Size
Checksum	Urgent Pointer
TCP Options (MSS, SACK P, MP CAPABLE, TMSP)	

Research Questions

UNIVERSITÄT DES SAARLANDES

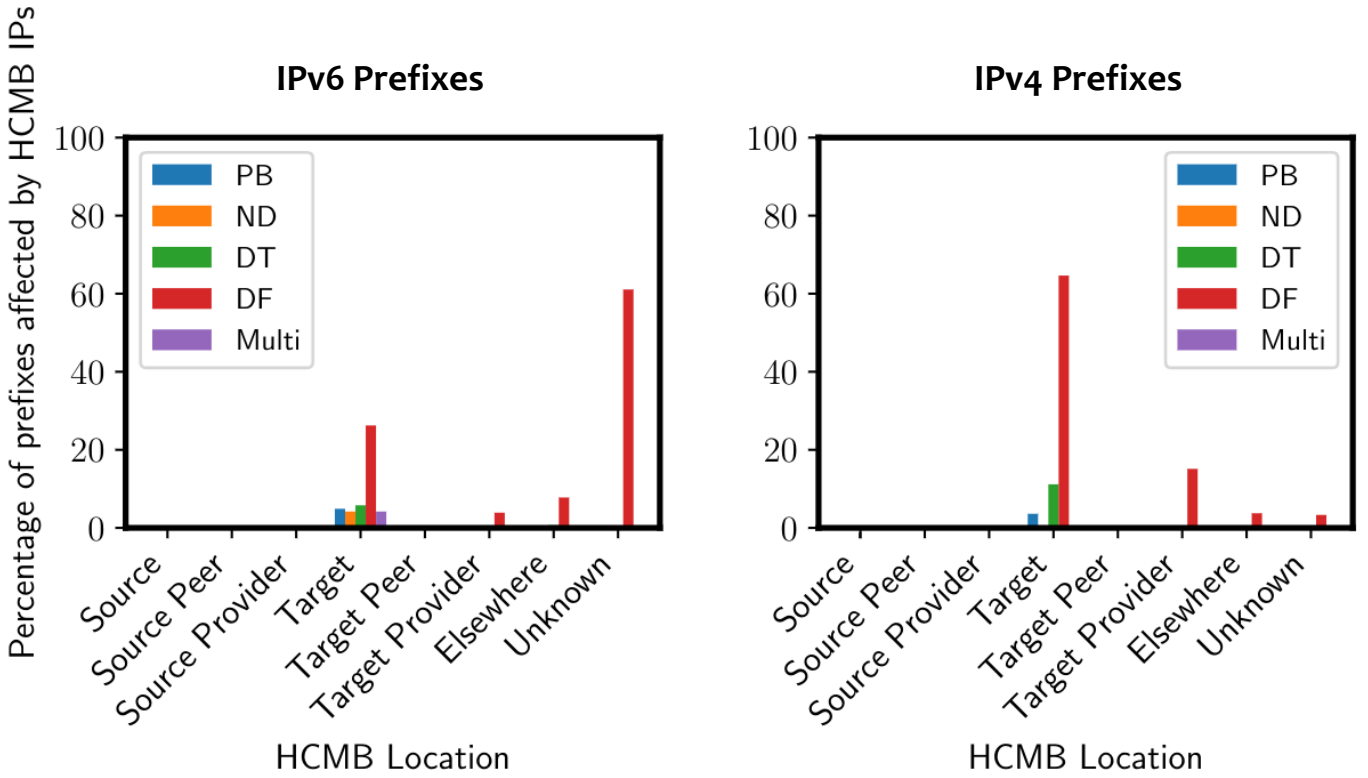
- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?

Results-Path Impairing MB Behaviors and Positioning



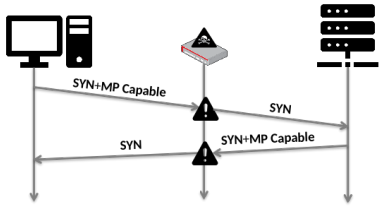
- **Topl. position**
  - Extracted from CAIDA AS Relationship

Results-Path Impairing MB Behaviors and Positioning

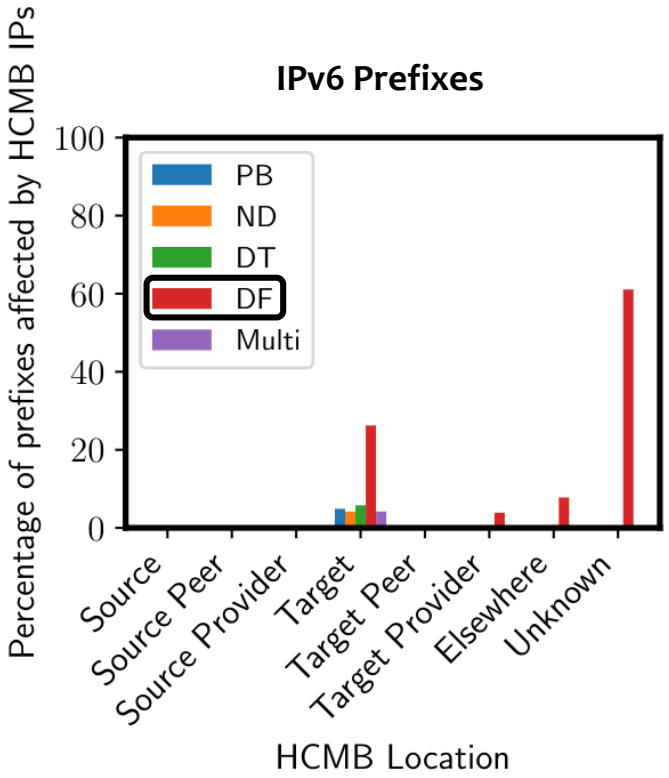


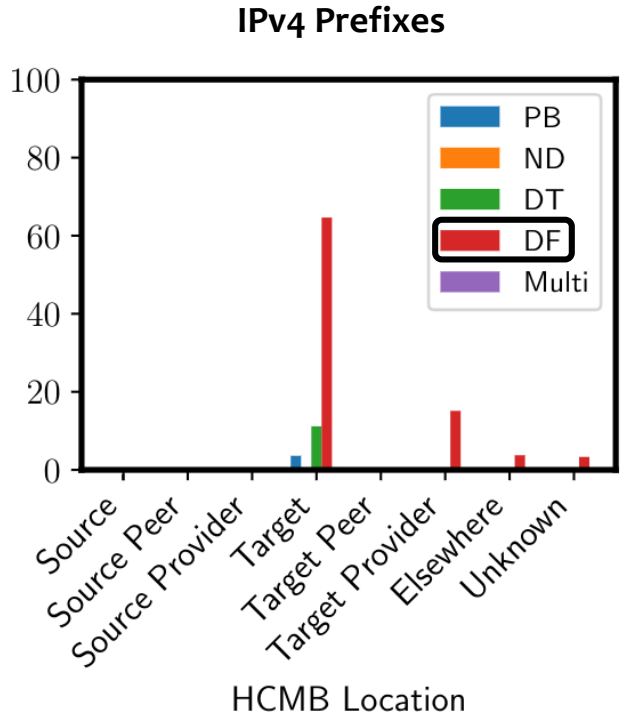
- **Topl. position**
  - Extracted from CAIDA AS Relationship

Results-Path Impairing MB Behaviors and Positioning



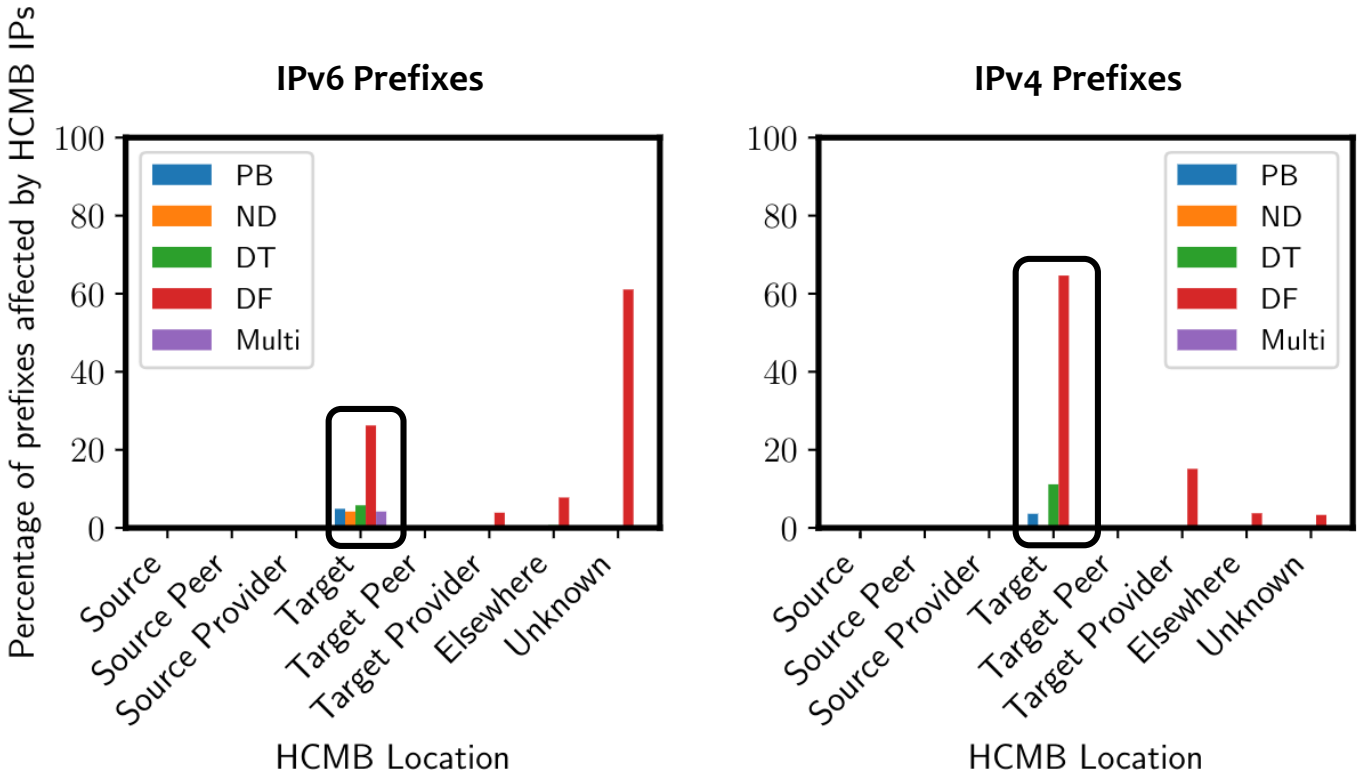
Disabling Features





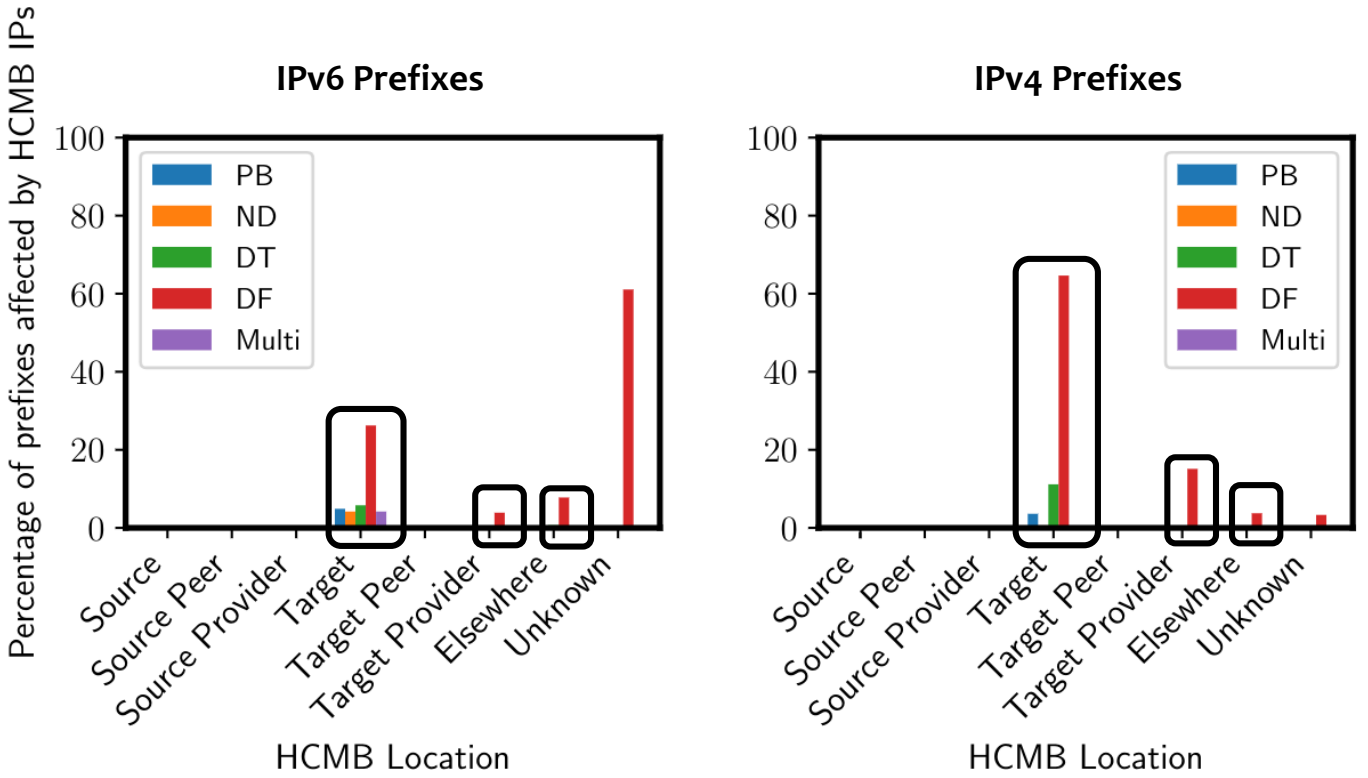
- **Topl. position**
  - Extracted from CAIDA AS Relationship
- **Impairments**
  - ***MP Capable*** (DF) removals dominate (NOP-based overwriting)

Results-Path Impairing MB Behaviors and Positioning



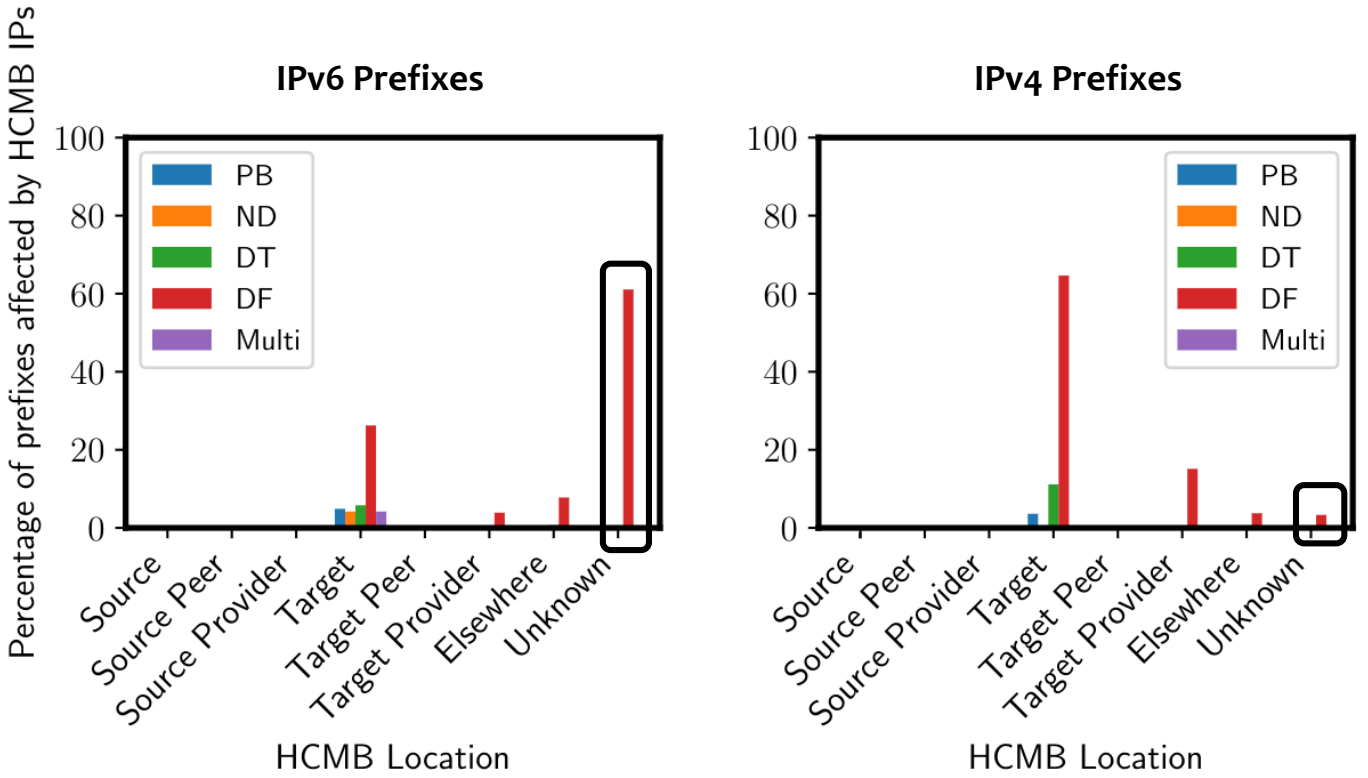
- **Topl. position**
  - Extracted from CAIDA AS Relationship
- **Impairments**
  - ***MP Capable*** (DF) removals dominate (NOP-based overwriting)

Results-Path Impairing MB Behaviors and Positioning



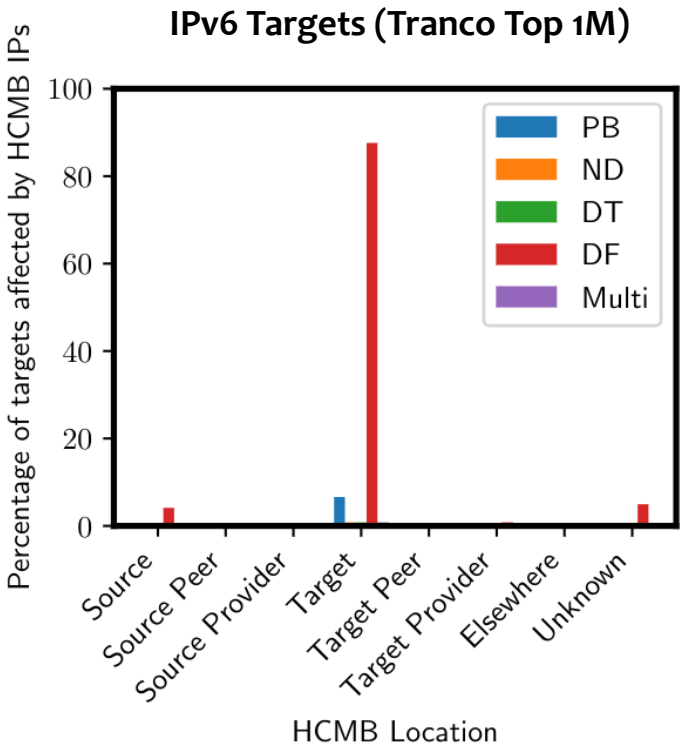
- **Topl. position**
  - Extracted from CAIDA AS Relationship
- **Impairments**
  - ***MP Capable*** (DF) removals dominate (NOP-based overwriting)

Results-Path Impairing MB Behaviors and Positioning



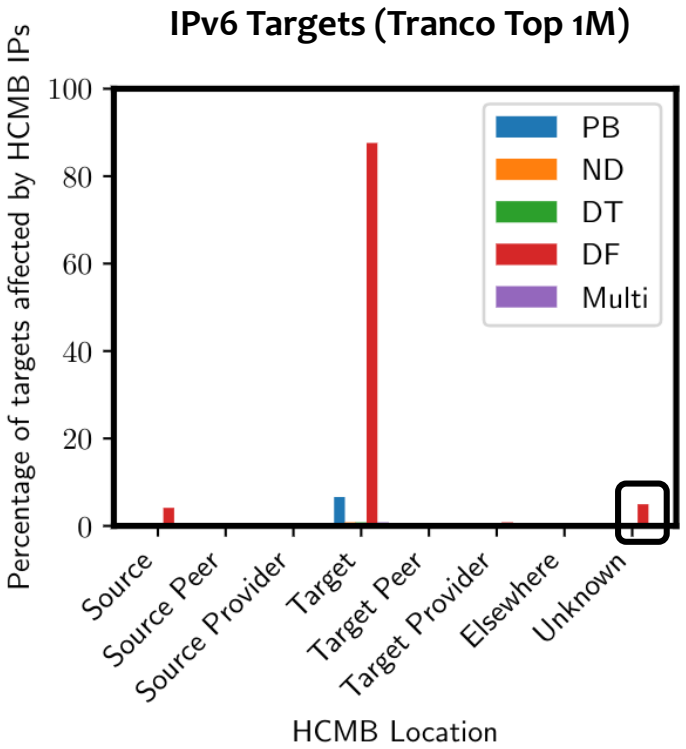
- **Topl. position**
  - Extracted from CAIDA AS Relationship
- **Impairments**
  - ***MP Capable*** (DF) removals dominate (NOP-based overwriting)

Results-Path Impairing MB Behaviors and Positioning



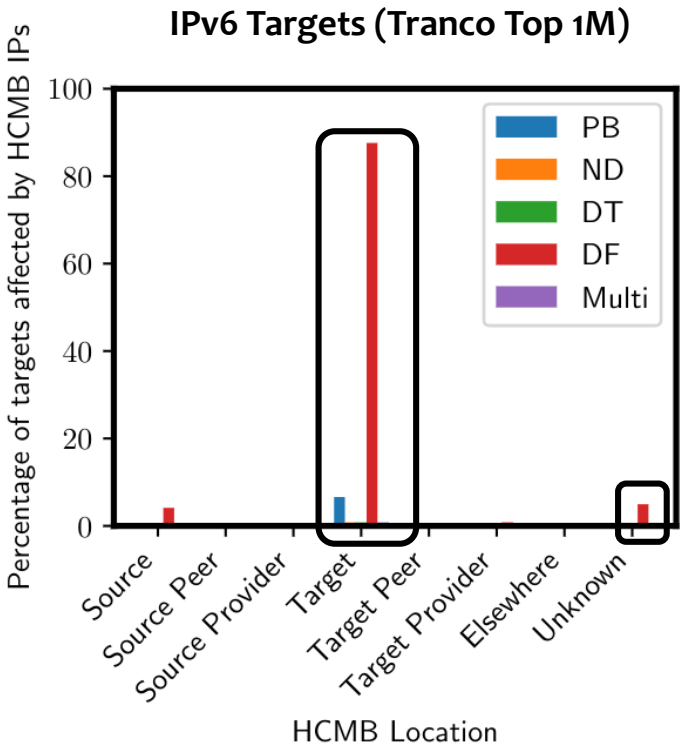
- **Impairments**
  - ***MP Capable*** (DF) removals dominate (NOP-based overwriting)

Results-Path Impairing MB Behaviors and Positioning



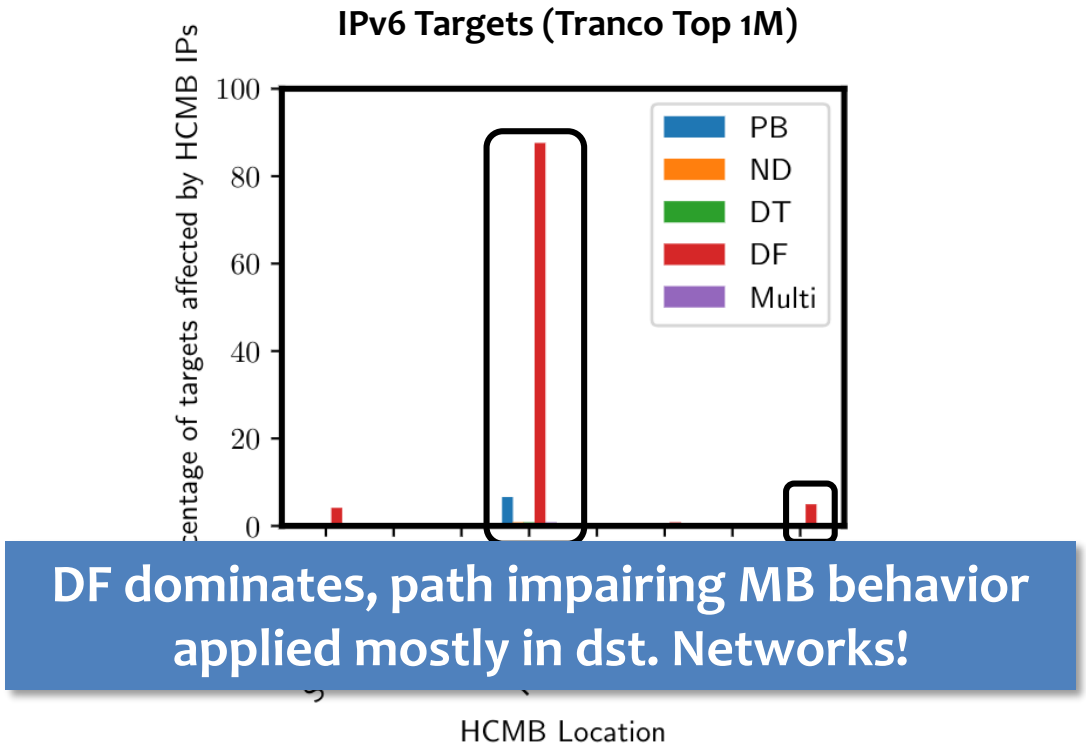
- **Impairments**
  - ***MP Capable*** (DF) removals dominate (NOP-based overwriting)

Results-Path Impairing MB Behaviors and Positioning



- **Impairments**
  - ***MP Capable*** (DF) removals dominate (NOP-based overwriting)

Results-Path Impairing MB Behaviors and Positioning



DF dominates, path impairing MB behavior applied mostly in dst. Networks!

- **Impairments**
  - ***MP Capable*** (DF) removals dominate (NOP-based overwriting)

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?
- How are announced prefixes and popular domains ***affected***?

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?
- How are announced prefixes and popular domains ***affected***?

Results-Path Impairing MB Affected Domains

UNIVERSITÄT DES SAARLANDES

Address Family	Affected Domains	Affected Paths
IPv6	**150 (0.05%)**	0.24%
IPv4	8.9k (1%)	1%

- Domain affected from any VP -> Affected domain

Results-Path Impairing MB Affected Domains

UNIVERSITÄT DES SAARLANDES

Address Family	Affected Domains	Affected Paths
IPv6	**150 (0.05%)**	0.24%
IPv4	8.9k (1%)	1%

- Domain affected from any VP -> Affected domain
- ~35% (IPv6), ~20% (IPv4) -> ***Top 100k***
- 13x more MP Capable, 67x more ECN, impaired ***IPv4*** paths

Results-Path Impairing MB Affected Domains

UNIVERSITÄT DES SAARLANDES

Address Family	Affected Domains	Affected Paths
IPv6	**150 (0.05%)**	0.24%
IPv4	8.9k (1%)	1%

- Domain affected from any VP -> Affected domain
- ~35% (IPv6), ~20% (IPv4) -> ***Top 100k***
- 13x more MP Capable, 67x more ECN, impaired ***IPv4*** paths
- 99.4% only IPv4 affected,
  - ***6.1%*** have ***AAAA***

Results-Path Impairing MB Affected Domains

UNIVERSITÄT DES SAARLANDES

Address Family	Affected Domains	Affected Paths
IPv6	**150 (0.05%)**	0.24%
IPv4	8.9k (1%)	1%

Switching addr. families could allow impairment-free paths!

- Domain affected from any VP -> Affected domain
- ~35% (IPv6), ~20% (IPv4) -> ***Top 100k***
- 13x more MP Capable, 67x more ECN, impaired ***IPv4*** paths
- 99.4% only IPv4 affected,
  - ***6.1%*** have ***AAAA***

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?
- How are announced prefixes and popular domains ***affected***?

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?
- How are announced prefixes and popular domains ***affected***?
- How can we engage with network ***operators*** to aid de-ossification?

Results-Causes of Path Impairments

UNIVERSITÄT DES SAARLANDES

- **Engagement with operators**
  - Opinion on TCP options, features (SACK Permitted, MP Capable, ECN),
  - Filtering policies configured?

Results-Causes of Path Impairments

UNIVERSITÄT DES SAARLANDES

- **Engagement with operators**
  - Opinion on TCP options, features (SACK Permitted, MP Capable, ECN),
  - Filtering policies configured?
- **Findings**
  - None claim any filtering
    - *"**transparent**" to TCP options ,"**essential** for good performance"*

Results-Causes of Path Impairments

UNIVERSITÄT DES SAARLANDES

- **Engagement with operators**
  - Opinion on TCP options, features (SACK Permitted, MP Capable, ECN),
  - Filtering policies configured?
- **Findings**
  - None claim any filtering
    - *"**transparent**" to TCP options ,"**essential** for good performance"*
  - Some IPv4 addrs. tied to MP Capable
    - Operators ***unaware*** of path-impairing MBs?

Results-Causes of Path Impairments

UNIVERSITÄT DES SAARLANDES

- **Engagement with operators**
  - Opinion on TCP options, features (SACK Permitted, MP Capable, ECN),
  - Filtering policies configured?
- **Findings**

Overly restrictive device defaults?

  - None claim any filtering
    - *"**transparent**" to TCP options ,"**essential** for good performance"*
  - Some IPv4 addrs. tied to MP Capable
    - Operators ***unaware*** of path-impairing MBs?

Results-Causes of Path Impairments

- **Examine vendor docs. (MPTCP handling)**

UNIVERSITÄT DES SAARLANDES

Results-Causes of Path Impairments

UNIVERSITÄT DES SAARLANDES

- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors ***allow*** TCP option filtering [1, 2, 3]

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.

Results-Causes of Path Impairments

UNIVERSITÄT DES SAARLANDES

- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors ***allow*** TCP option filtering [1, 2, 3]
    - Palo Alto [3], Cisco [4], Citrix [5], CheckPoint [6] ***defaults***
      - Remove/replace TCP options,
        - eg. MPTCP with ***NOPs*** [4]

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.
[4] www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
[5] support.citrix.com/external/article?articleUrl=CTX461232-tcp-option-lost-when-traffic-go-through-tcp-type-load-balancelb-vserver&language=en_US
[6] support.checkpoint.com/results/sk/sk114666

Results-Causes of Path Impairments

UNIVERSITÄT DES SAARLANDES

- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors ***allow*** TCP option filtering [1, 2, 3]
    - Palo Alto [3], Cisco [4], Citrix [5], CheckPoint [6] ***defaults***
      - Remove/replace TCP options,
        - eg. MPTCP with ***NOPs*** [4]
- **Vendor identif.**
  - Nmap, SNMPv3, Censys -> MB vendors
    - Cisco, Palo Alto, Check Point -> ***Top 5***!

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.
[4] www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
[5] support.citrix.com/external/article?articleUrl=CTX461232-tcp-option-lost-when-traffic-go-through-tcp-type-load-balancelb-vserver&language=en_US
[6] support.checkpoint.com/results/sk/sk114666

Results-Causes of Path Impairments

UNIVERSITÄT DES SAARLANDES

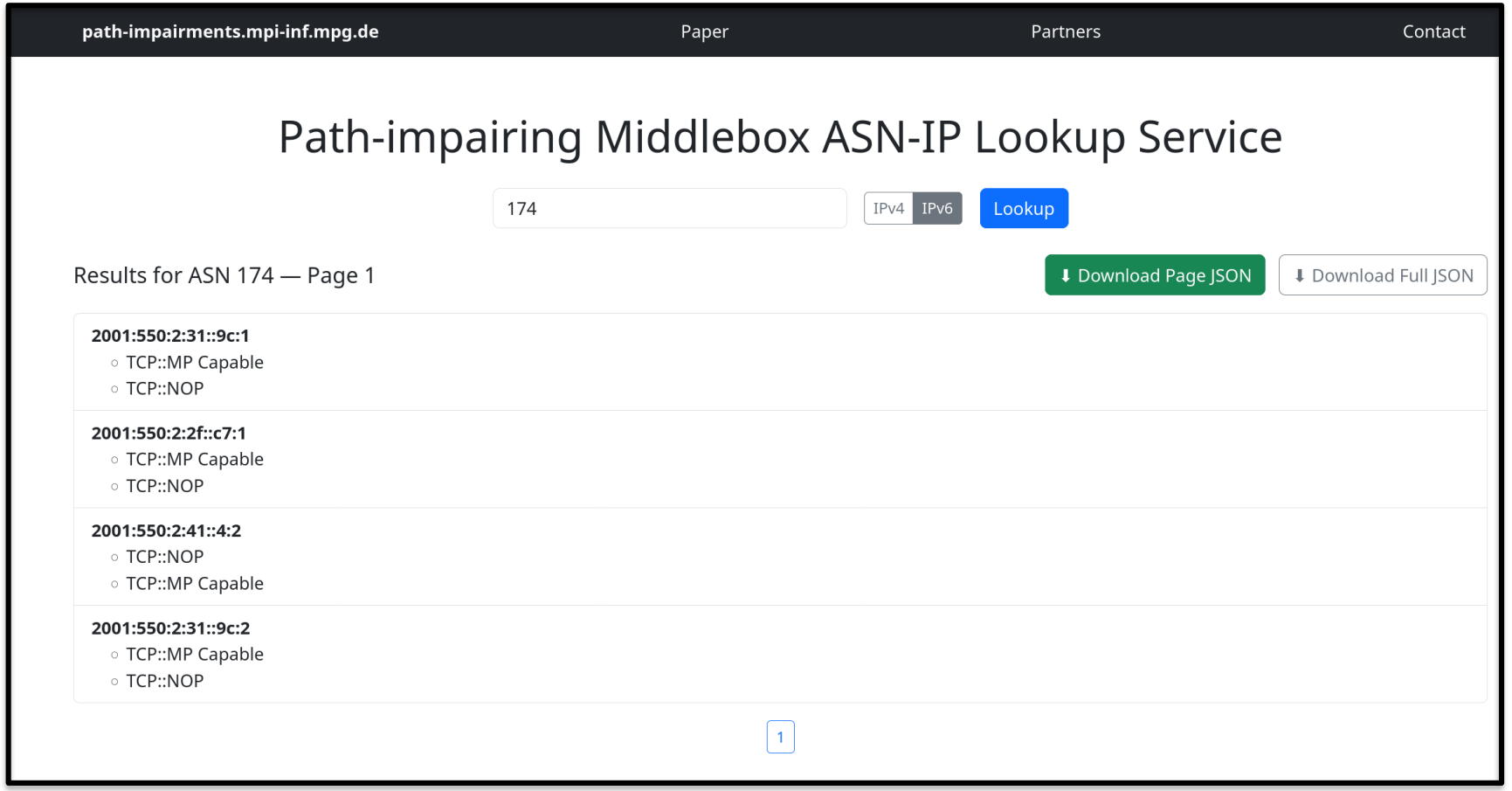
- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors ***allow*** TCP option filtering [1, 2, 3]
    - Palo Alto [3], Cisco [4], Citrix [5], CheckPoint [6] ***defaults***
      - Remove/replace TCP options,
        - eg. MPTCP with ***NOPs*** [4]
- **Vendor identif.**
  - Nmap, SNMPv3, Censys -> MB vendors
    - Cisco, Palo Alto, Check Point -> ***Top 5***!

Device defaults potentially one (unintended) cause of impairments!

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.
[4] www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
[5] support.citrix.com/external/article?articleUrl=CTX461232-tcp-option-lost-when-traffic-go-through-tcp-type-load-balancelb-vserver&language=en_US
[6] support.checkpoint.com/results/sk/sk114666

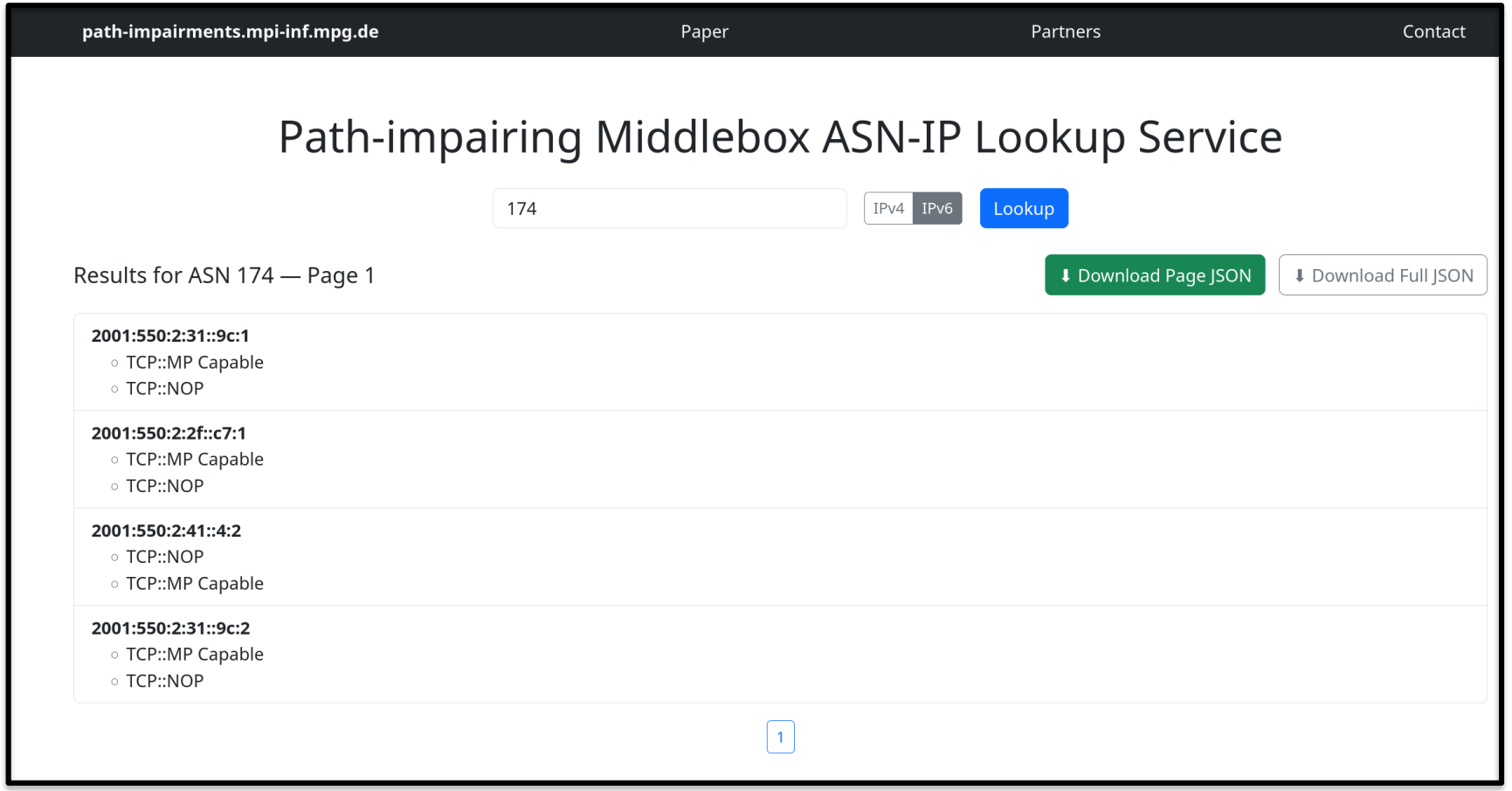
Towards Deossification

- ASN -> Path-impairing MB ***look-up service***



Towards Deossification

- ASN -> Path-impairing MB ***look-up service***



Research Questions

UNIVERSITÄT DES SAARLANDES

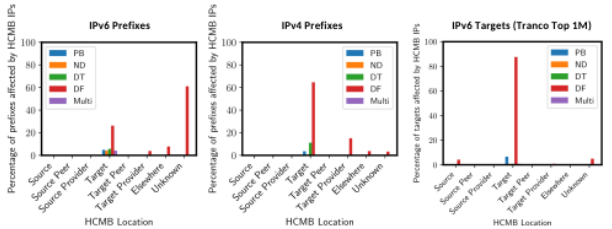
- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?
- How are announced prefixes and popular domains ***affected***?
- How can we engage with network ***operators*** to aid de-ossification?
- Are path-impairing MBs ***stable*** over short and long periods?

Research Questions

UNIVERSITÄT DES SAARLANDES

- ***Which*** path-impairing middlebox ***behaviors*** are dominant?
- Where ***on path*** are path-impairing middlebox behaviors applied?
- How are announced prefixes and popular domains ***affected***?
- How can we engage with network ***operators*** to aid de-ossification?
- Are path-impairing MBs stable over short and long periods?

Results-Path-Impairing MB Behaviors and Positioning



- **Topl. position**
  - Extracted from CAIDA AS Relationship
- **Impaired paths**
  - IPv6: DF (88%) PB (9%), IPv4: DF (95%)
    - *MP Capable* (DF) removals dominate (*NOP-based* overwriting)

Results-Path-Impairing MB Affected Domains

Address Family	Affected Domains	Affected Paths
IPv6	150 (0.05%)	0.24%
IPv4	8.9k (1%)	1%

- Domain affected from any VP -> Affected domain
- ~35% (IPv6), ~20% (IPv4) -> *Top 100k*
- 13x more MP Capable, 67x more ECN, impaired *IPv4* paths
- 99.4% only IPv4 affected,
  - *6.1%* have *AAAA*,

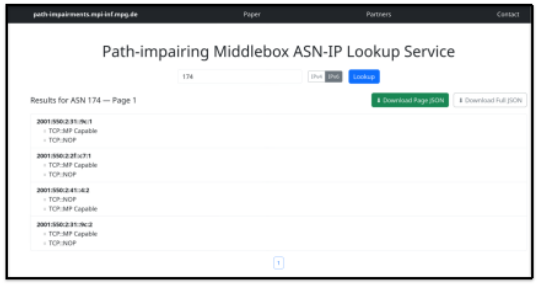
Results-Causes of Path-Impairments

- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors *allow* TCP option filtering [1, 2, 3]
    - Palo Alto [3], Cisco [4], Citrix [5], CheckPoint [6] *defaults*
      - Remove/replace TCP options,
        - eg. MPTCP with *NOPs* [4]
- **Vendor identif.**
  - Nmap, SNMPv3, Censys -> MB vendors
    - Cisco, Palo Alto, Check Point -> *Top 5*!

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.
[4] www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
[5] support.citrix.com/external/article?articleUrl=CTX461232-tcp-option-lost-when-traffic-go-through-tcp-type-load-balancelb-vserver&language=en_US
[6] support.checkpoint.com/results/sk/sk114666

Towards Deossification

- ASN -> Path-impairing MB *look-up service*



Results-Path-Impairing MB Behaviors and Positioning

DF dominates, path-impairments applied mostly in dst. networks!

- Extracted from CAIDA AS Relationship
- **Impaired paths**
  - IPv6: DF (88%) PB (9%), IPv4: DF (95%)
    - *MP Capable* (DF) removals dominate (*NOP-based* overwriting)

Results-Path-Impairing MB Affected Domains

Address Family	Affected Domains	Affected Paths
IPv6	150 (0.05%)	0.24%
IPv4	8.9k (1%)	1%

- Domain affected from any VP -> Affected domain
- ~35% (IPv6), ~20% (IPv4) -> *Top 100k*
- 13x more MP Capable, 67x more ECN, impaired *IPv4* paths
- 99.4% only IPv4 affected,
  - *6.1%* have *AAAA*,

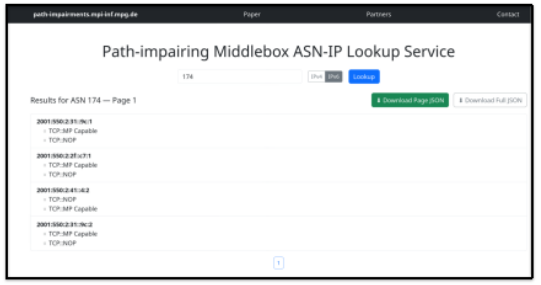
Results-Causes of Path-Impairments

- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors *allow* TCP option filtering [1, 2, 3]
    - Palo Alto [3], Cisco [4], Citrix [5], CheckPoint [6] *defaults*
      - Remove/replace TCP options,
        - eg. MPTCP with *NOPs* [4]
- **Vendor identif.**
  - Nmap, SNMPv3, Censys -> MB vendors
    - Cisco, Palo Alto, Check Point -> *Top 5*!

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.
[4] www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
[5] support.citrix.com/external/article?articleUrl=CTX461232-tcp-option-lost-when-traffic-go-through-tcp-type-load-balancelb-vserver&language=en_US
[6] support.checkpoint.com/results/sk/sk114666

Towards Deossification

- ASN -> Path-impairing MB *look-up service*



Results-Path-Impairing MB Behaviors and Positioning

DF dominates, path-impairments applied mostly in dst. networks!

- Extracted from CAIDA AS Relationship
- **Impaired paths**
  - IPv6: DF (88%) PB (9%), IPv4: DF (95%)
    - *MP Capable* (DF) removals dominate (*NOP-based* overwriting)

Results-Path-Impairing MB Affected Domains

Address Family	Affected Domains	Affected Paths
IPv6	150 (0.05%)	0.24%
IPv4	8.9k (1%)	1%

Switching addr. families could allow impairment-free paths!

- 99.4% only IPv4 affected,
  - *6.1%* have *AAAA*,

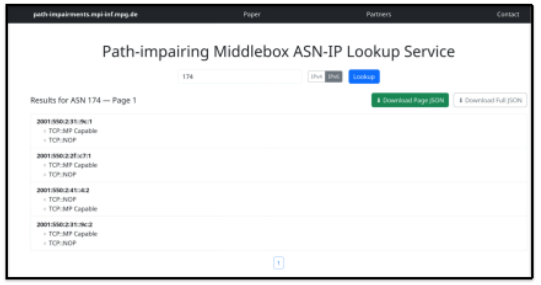
Results-Causes of Path-Impairments

- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors *allow* TCP option filtering [1, 2, 3]
    - Palo Alto [3], Cisco [4], Citrix [5], CheckPoint [6] *defaults*
      - Remove/replace TCP options,
        - eg. MPTCP with *NOPs* [4]
- **Vendor identif.**
  - Nmap, SNMPv3, Censys -> MB vendors
    - Cisco, Palo Alto, Check Point -> *Top 5*!

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.
[4] www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
[5] support.citrix.com/external/article?articleUrl=CTX461232-tcp-option-lost-when-traffic-go-through-tcp-type-load-balancelb-vserver&language=en_US
[6] support.checkpoint.com/results/sk/sk114666

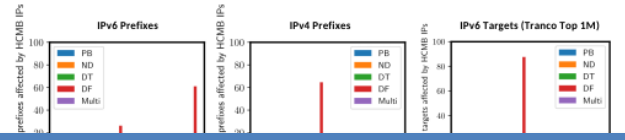
Towards Deossification

- ASN -> Path-impairing MB *look-up service*



UNIVERSITÄT DES SAARLANDES

Results-Path-Impairing MB Behaviors and Positioning



- Extracted from CAIDA AS Relationship
- **Impaired paths**
  - IPv6: DF (88%) PB (9%), IPv4: DF (95%)
    - *MP Capable* (DF) removals dominate (*NOP-based* overwriting)

DF dominates, path-impairments applied mostly in dst. networks!

Results-Path-Impairing MB Affected Domains

Address Family	Affected Domains	Affected Paths
IPv6	150 (0.05%)	0.24%
IPv4	8.9k (1%)	1%

- 99.4% only IPv4 affected,
  - *6.1%* have *AAAA*,

Switching addr. families could allow impairment-free paths!

Results-Causes of Path-Impairments

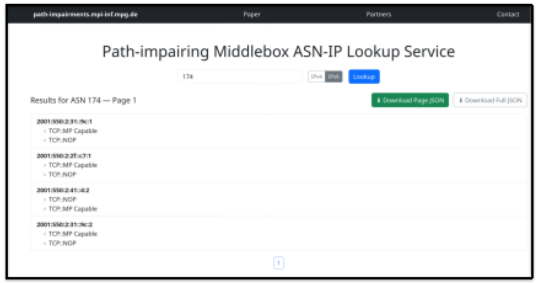
- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors *allow* TCP option filtering [1, 2, 3]
    - Palo Alto [3], Cisco [4], Citrix [5], CheckPoint [6] *defaults*
      - Remove/replace TCP options,
        - eg. MPTCP with *NOPs* [4]

Device defaults potentially one (unintended) cause of impairments!

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.
[4] www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
[5] support.citrix.com/external/article?articleUrl=CTX461232-tcp-option-lost-when-traffic-go-through-tcp-type-load-balancelb-vserver&language=en_US
[6] support.checkpoint.com/results/sk/sk114666

Towards Deossification

- ASN -> Path-impairing MB *look-up service*



UNIVERSITÄT DES SAARLANDES

Results-Path-Impairing MB Behaviors and Positioning

- Extracted from CAIDA AS Relationship
- **Impaired paths**
  - IPv6: DF (88%) PB (9%), IPv4: DF (95%)
    - *MP Capable* (DF) removals dominate (*NOP-based* overwriting)

DF dominates, path-impairments applied mostly in dst. networks!

Results-Path-Impairing MB Affected Domains

Address Family	Affected Domains	Affected Paths
IPv6	150 (0.05%)	0.24%
IPv4	8.9k (1%)	1%

- 99.4% only IPv4 affected,
  - *6.1%* have *AAAA*,

Switching addr. families could allow impairment-free paths!

Results-Causes of Path-Impairments

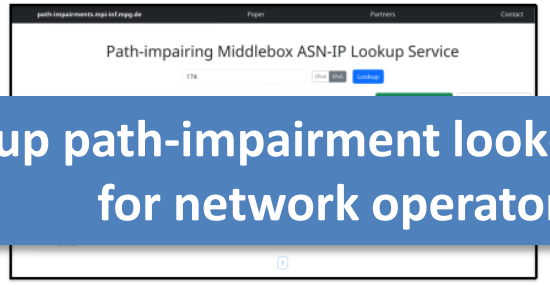
- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors *allow* TCP option filtering [1, 2, 3]
    - Palo Alto [3], Cisco [4], Citrix [5], CheckPoint [6] *defaults*
      - Remove/replace TCP options,
        - eg. MPTCP with *NOPs* [4]

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.
[4] www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
[5] support.citrix.com/external/article?articleUrl=CTX461232-tcp-option-lost-when-traffic-go-through-tcp-type-load-balancelb-vserver&language=en_US
[6] support.checkpoint.com/results/sk/sk114666

Device defaults potentially one (unintended) cause of impairments!

Towards Deossification

- ASN -> Path-impairing MB *look-up service*



Set up path-impairment look-up service for network operators!

UNIVERSITÄT DES SAARLANDES

Questions?

Results-Path-Impairing MB Behaviors and Positioning

- Extracted from CAIDA AS Relationship
- **Impaired paths**
  - IPv6: DF (88%) PB (9%), IPv4: DF (95%)
    - *MP Capable* (DF) removals dominate (*NOP-based* overwriting)

DF dominates, path-impairments applied mostly in dst. networks!

Results-Path-Impairing MB Affected Domains

Address Family	Affected Domains	Affected Paths
IPv6	150 (0.05%)	0.24%
IPv4	8.9k (1%)	1%

- 99.4% only IPv4 affected,
  - *6.1%* have *AAAA*,

Switching addr. families could allow impairment-free paths!

Results-Causes of Path-Impairments

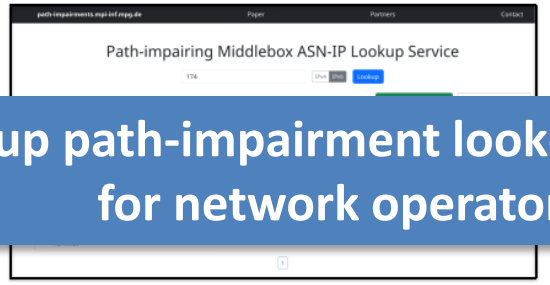
- **Examine vendor docs. (MPTCP handling)**
  - Firewall vendors *allow* TCP option filtering [1, 2, 3]
    - Palo Alto [3], Cisco [4], Citrix [5], CheckPoint [6] *defaults*
      - Remove/replace TCP options,
        - eg. MPTCP with *NOPs* [4]

[1] www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/security-edit-tcp-options.html
[2] www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/firewall/asdm-78-firewall-config/conns-connlimits.html
[3] docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/device/device-setup-session/tcp-settings.
[4] www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/116519-technote-mptcp-00.html
[5] support.citrix.com/external/article?articleUrl=CTX461232-tcp-option-lost-when-traffic-go-through-tcp-type-load-balancelb-vserver&language=en_US
[6] support.checkpoint.com/results/sk/sk114666

Device defaults potentially one (unintended) cause of impairments!

Towards Deossification

- ASN -> Path-impairing MB *look-up service*



Set up path-impairment look-up service for network operators!