

Routing Under Siege: How Traffic Engineering Decisions Facilitate Prefix Hijackings

Renan Barreto, Leandro Bertholdo, Pedro Marcos

renan.barreto@furg.br

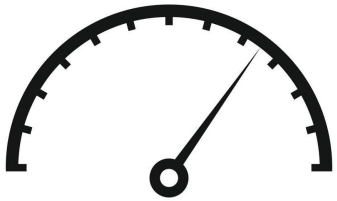
May 2026

FURG
UNIVERSIDADE FEDERAL
DO RIO GRANDE

UFRGS
UNIVERSIDADE FEDERAL
DO RIO GRANDE DO SUL

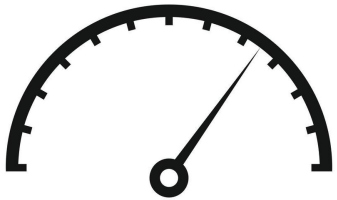
Traffic delivery is key for Internet operations

Traffic delivery is key for Internet operations

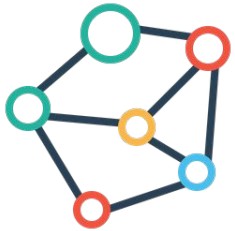


Application requirements and performance

Traffic delivery is key for Internet operations

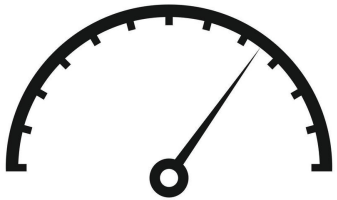


Application requirements and performance

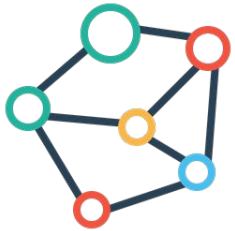


Increasing connectivity

Traffic delivery is key for Internet operations



Application requirements and performance

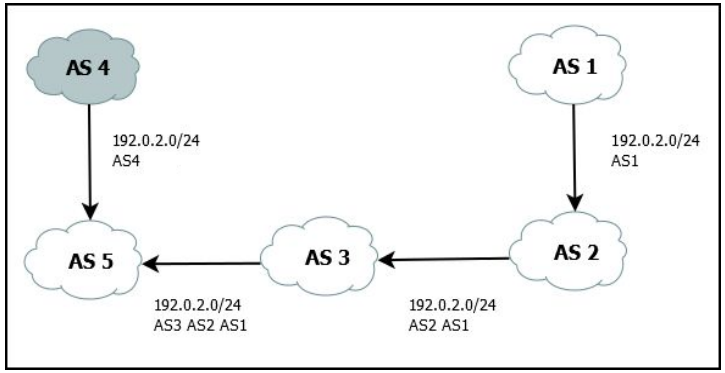


Increasing connectivity

ASes use traffic engineering techniques to improve performance and resilience

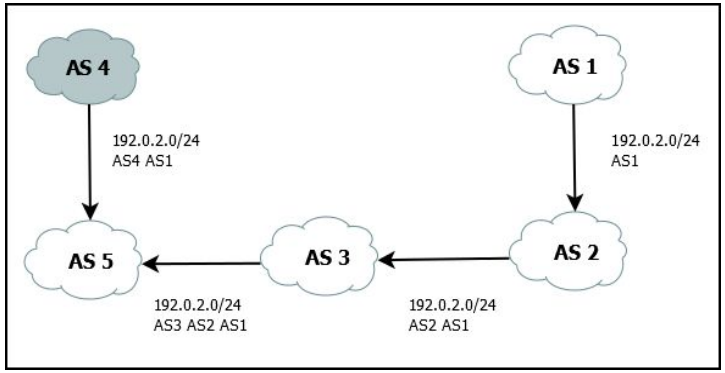
Prefix Hijack events affects the Internet

Prefix Hijack events affects the Internet



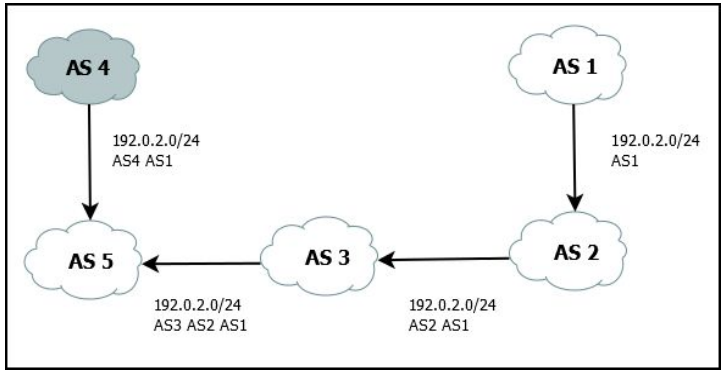
These occur when an AS announces a prefix that it does not own

Prefix Hijack events affects the Internet



These occur when an AS announces a prefix that it does not own, or a path to another AS, which it does not possess

Prefix Hijack events affects the Internet

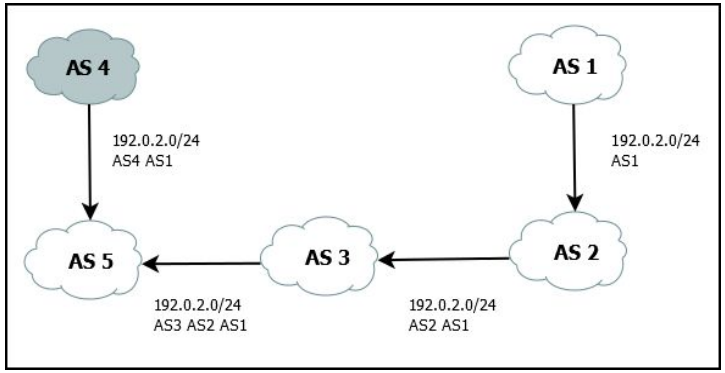


Cloudflare 1.1.1.1 incident on June 27, 2024

2024-07-04

These occur when an AS announces a prefix that it does not own, or a path to another AS, which it does not possess

Prefix Hijack events affects the Internet



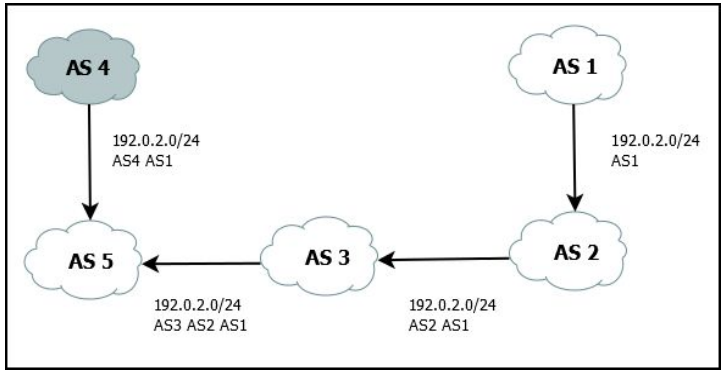
Cloudflare 1.1.1.1 incident on

ROUTING SECURITY | ROUTING SECURITY INCIDENTS

Not just another BGP Hijack

These occur when an AS announces a prefix that it does not own, or a path to another AS, which it does not possess

Prefix Hijack events affects the Internet



Cloudflare 1.1.1.1 incident on

ROUTING SECURITY | ROUTING SECURITY INCIDENTS

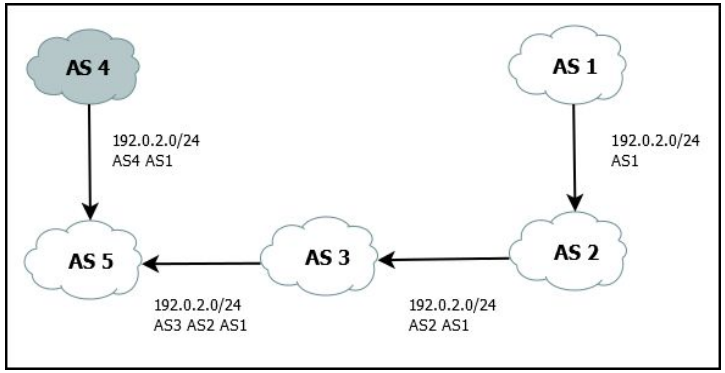
Not just another BGP Hijack

ROUTING SECURITY | ROUTING SECURITY INCIDENTS

KlaySwap – Another BGP Hijack Targeting Crypto Wallets

These occur when an AS announces a prefix that it does not own, or a path to another AS, which it does not possess

Prefix Hijack events affects the Internet



These occur when an AS announces a prefix that it does not own, or a path to another AS, which it does not possess

Cloudflare 1.1.1.1 incident on

ROUTING SECURITY | ROUTING SECURITY INCIDENTS

Not just another BGP Hijack

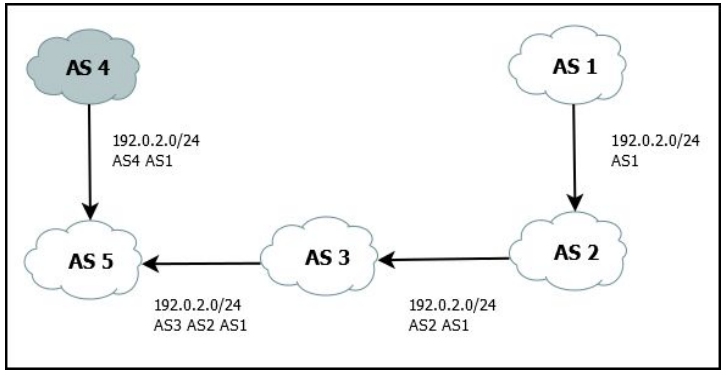
ROUTING SECURITY | ROUTING SECURITY INCIDENTS

KlaySwap – Another BGP Hijack

NEWS AND ANNOUNCEMENTS | ROUTING SECURITY | ROUTING SECURITY INCIDENTS

Did Ukraine suffer a BGP hijack and how can networks protect themselves?

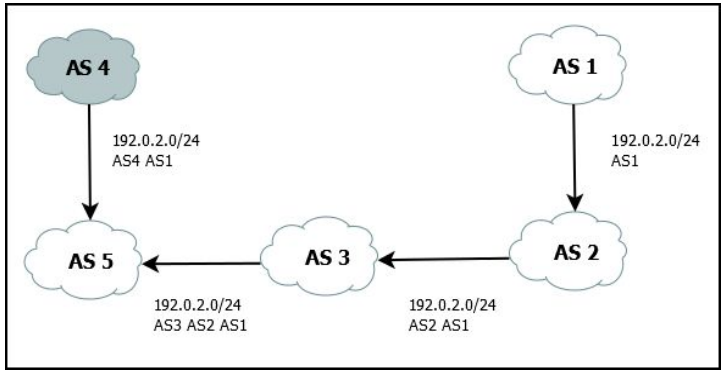
Prefix Hijack events affects the Internet



These occur when an AS announces a prefix that it does not own, or a path to another AS, which it does not possess



Prefix Hijack events affects the Internet





These occur when an AS announces a prefix that it does not own, or a path to another AS, which it does not possess

Malicious ASes can delay, discard, or intercept data

Our goal is to understand how traffic engineering decisions affect routing security

Our goal is to understand how traffic engineering decisions affect routing security



How do different techniques affect the impact of a hijack?

Our goal is to understand how traffic engineering decisions affect routing security



How do different techniques affect the impact of a hijack?



What is the current state of ITE usage and its potential impact on security?

Our goal is to understand how traffic engineering decisions affect routing security



How do different techniques affect the impact of a hijack?



What is the current state of ITE usage and its potential impact on security?



What leads an AS to accept a hijacked route announcement?

Our goal is to understand how traffic engineering decisions affect routing security



How do different techniques affect the impact of a hijack?



What is the current state of ITE usage and its potential impact on security?



What leads an AS to accept a hijacked route announcement?



Which characteristics of the victim and the attacker influence the outcome of a hijack?

Our goal is to understand how traffic engineering decisions affect routing security



How do different techniques affect the impact of a hijack?



What is the current state of ITE usage and its potential impact on security?



What leads an AS to accept a hijacked route announcement?



Which characteristics of the victim and the attacker influence the outcome of a hijack?

Our goal is to understand how traffic engineering decisions affect routing security



How do different techniques affect the impact of a hijack?



What is the current state of ITE usage and its potential impact on security?



What leads an AS to accept a hijacked route announcement?

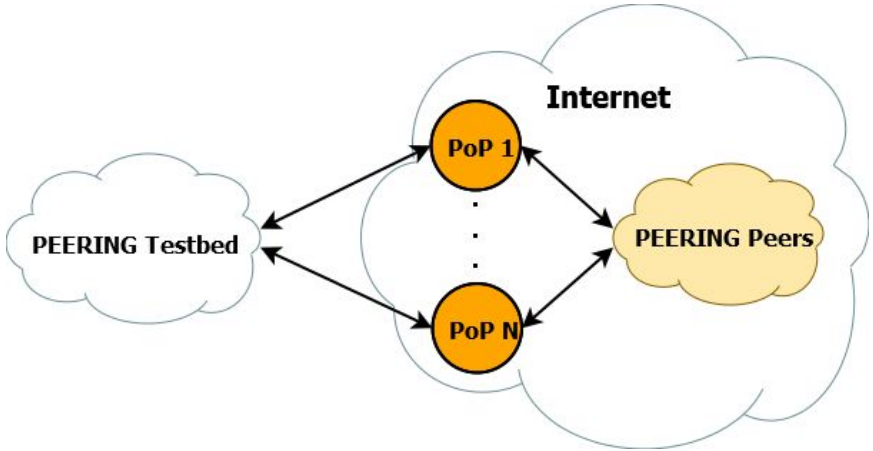


Which characteristics of the victim and the attacker influence the outcome of a hijack?

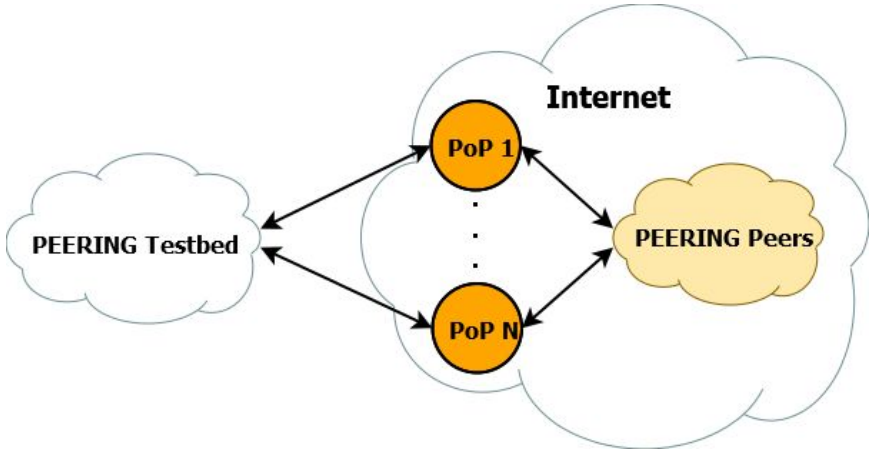
To analyze the impact of ITE, we will use PEERING

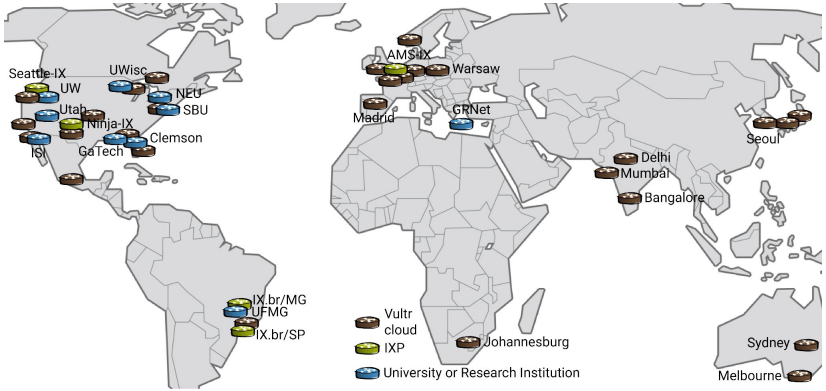
To analyze the impact of ITE, we will use PEERING

To analyze the impact of ITE, we will use PEERING

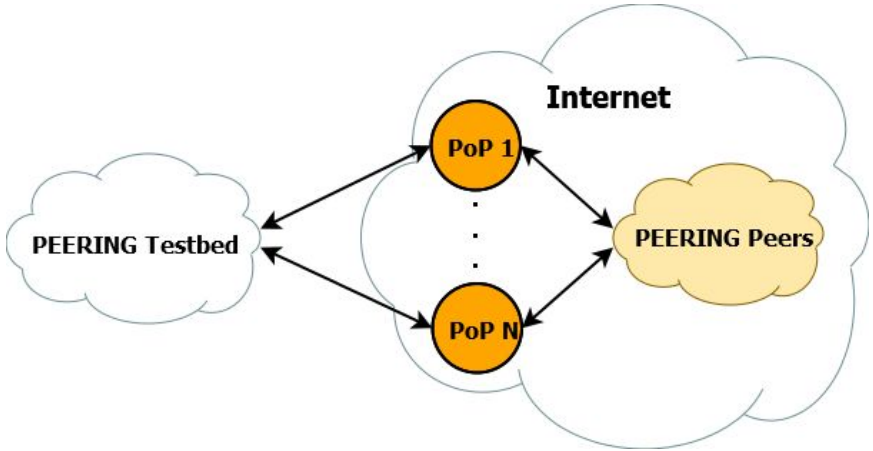


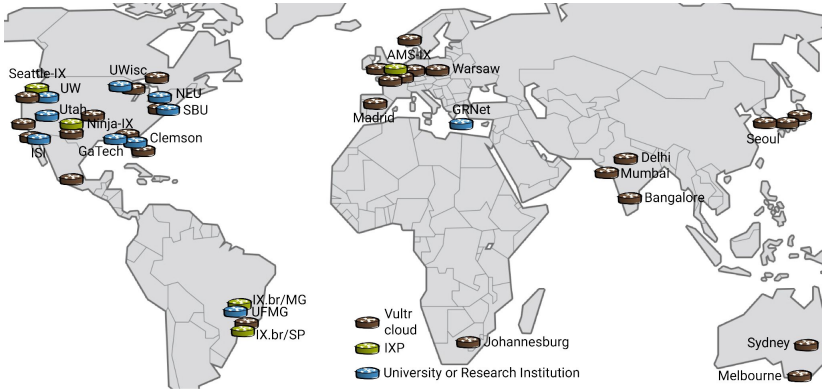
To analyze the impact of ITE, we will use PEERING





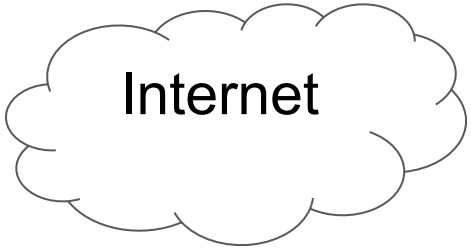
To analyze the impact of ITE, we will use PEERING





PEERING enables real-world BGP announcements on the Internet

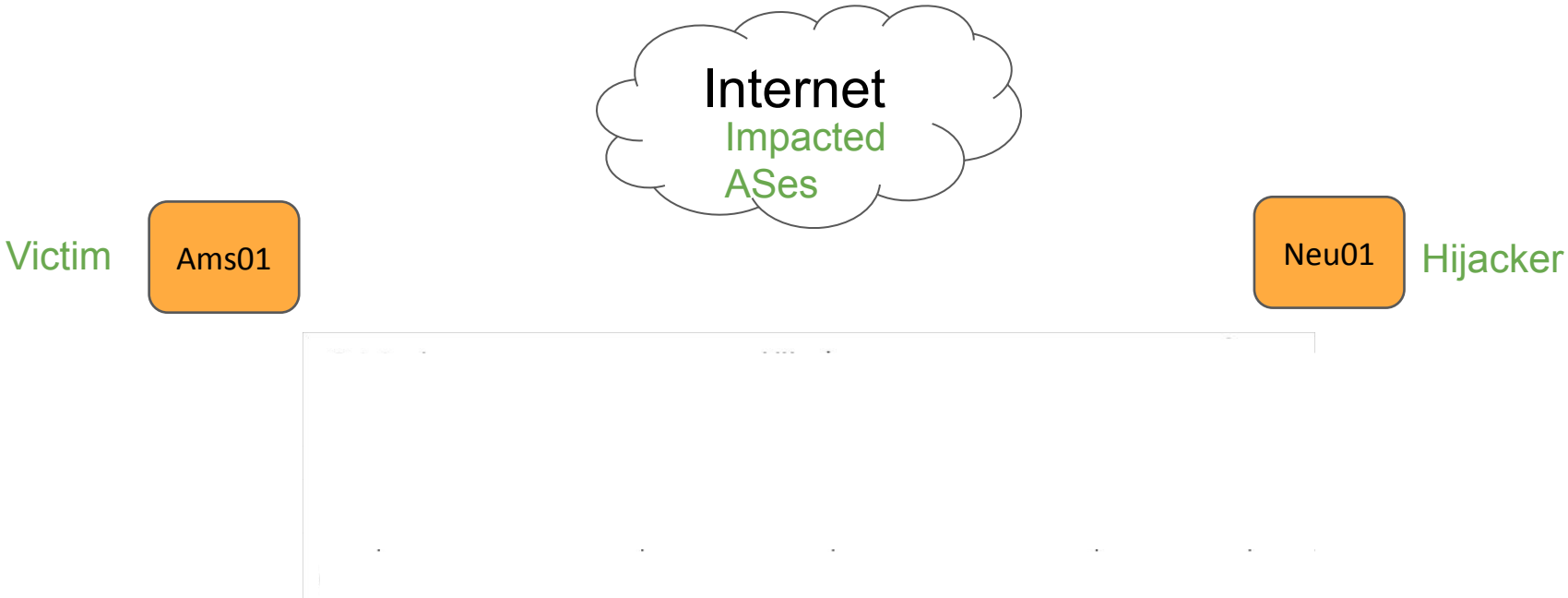
Example of configuration



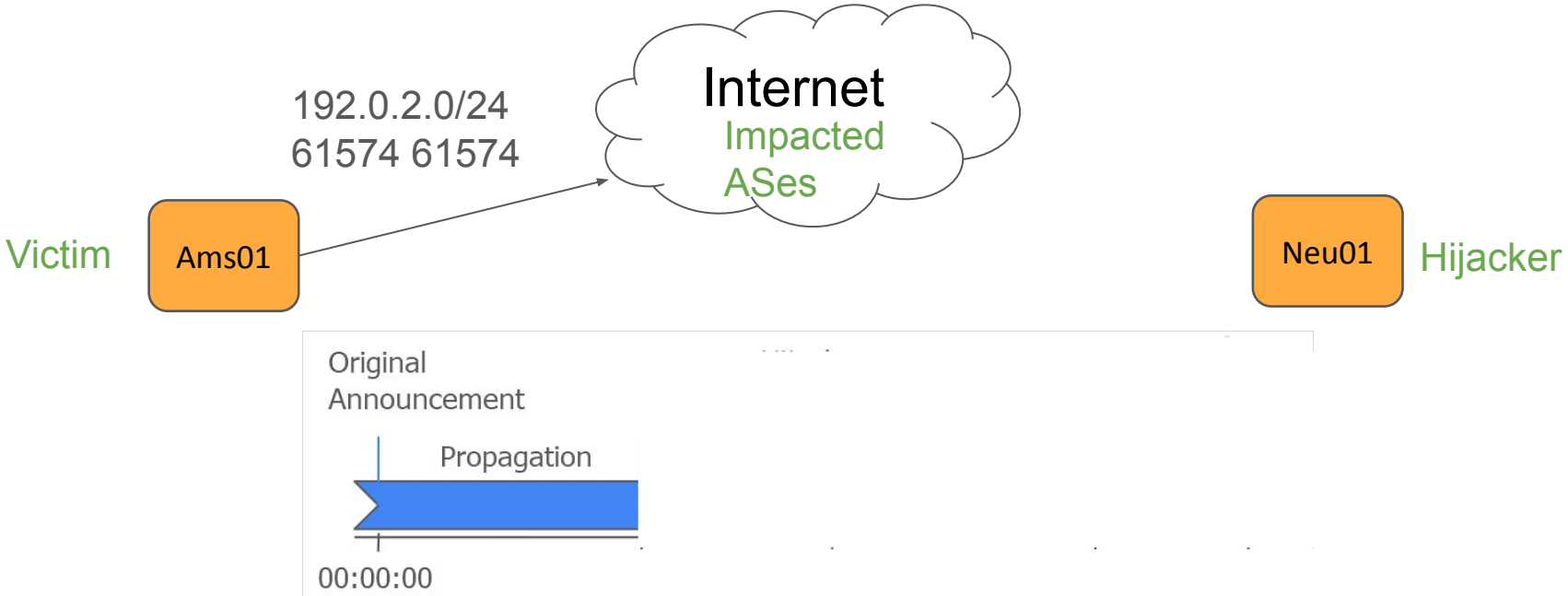
Example of configuration



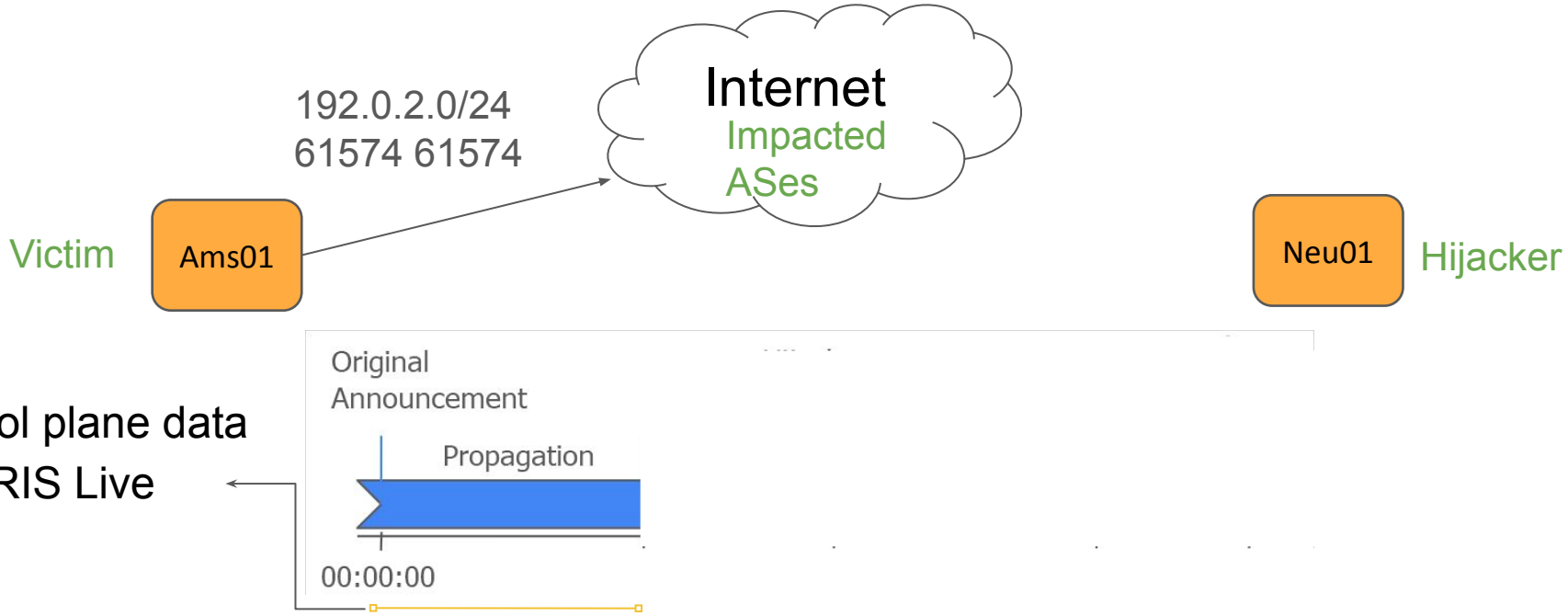
Example of configuration



Example of configuration

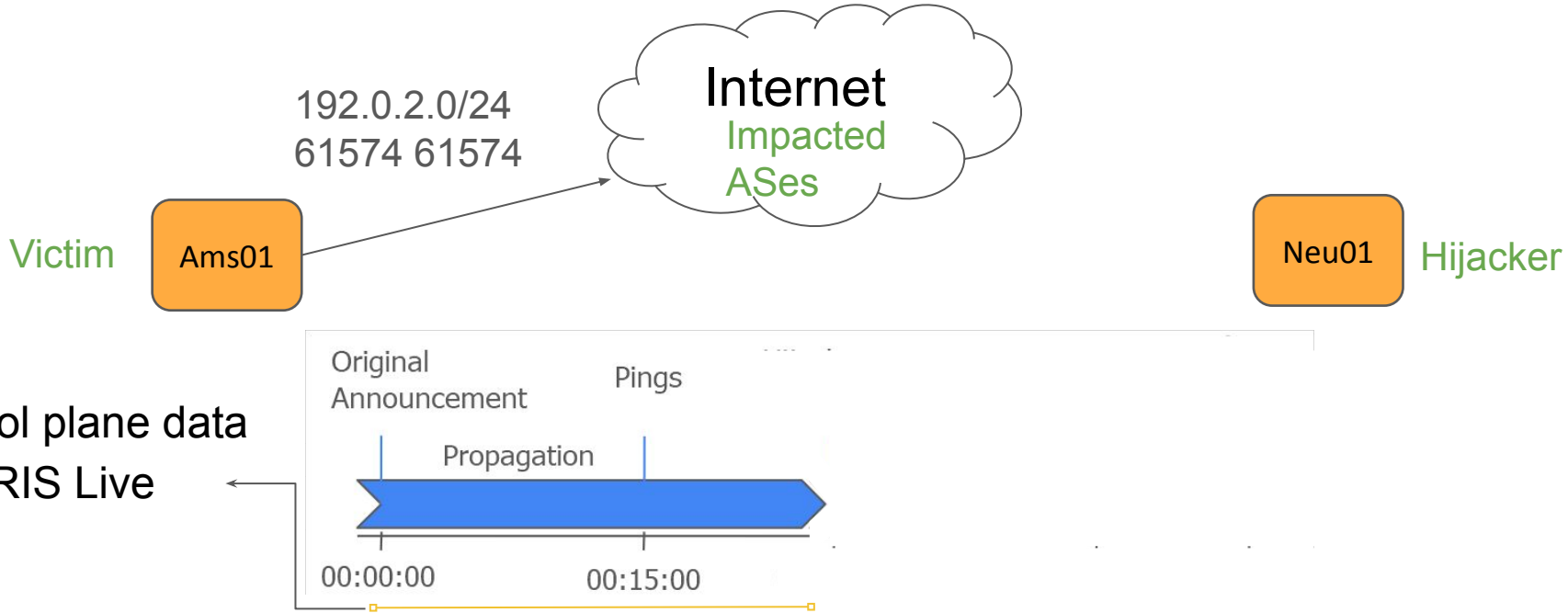


Example of configuration



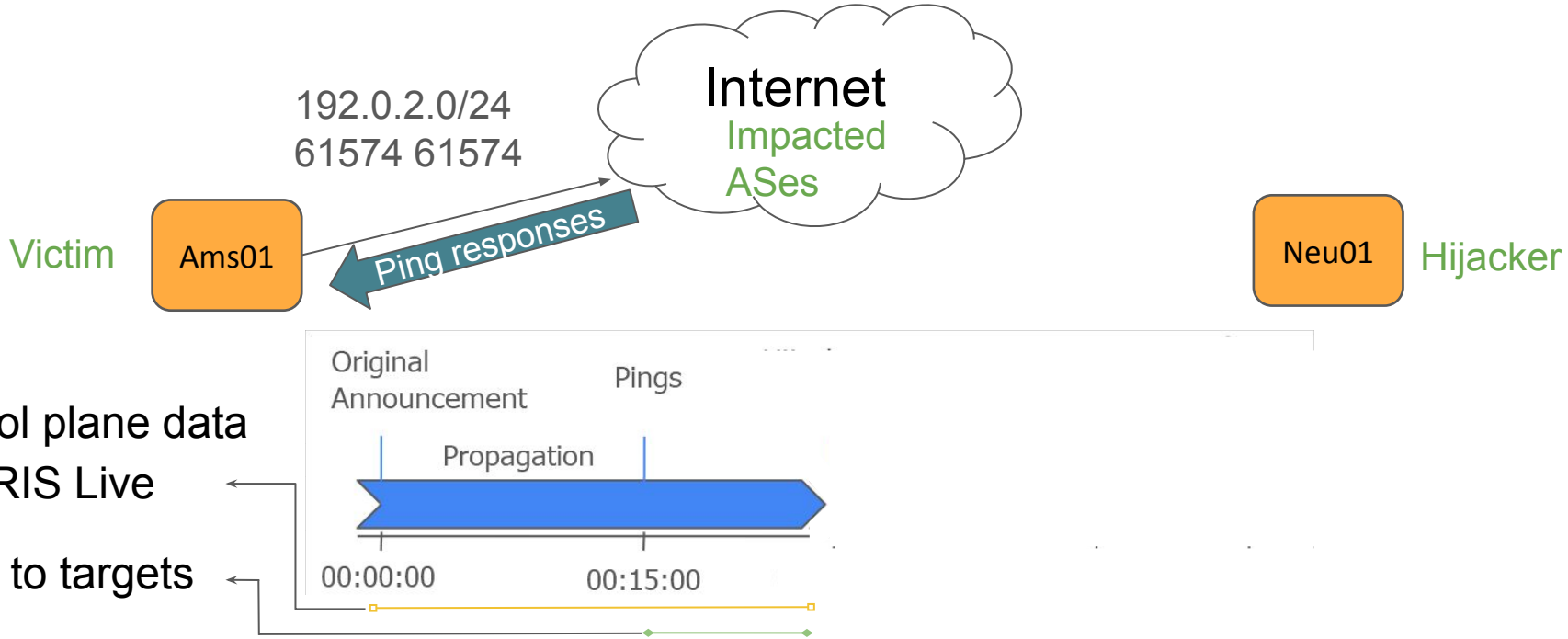
Control plane data
from RIS Live

Example of configuration



Control plane data
from RIS Live

Example of configuration

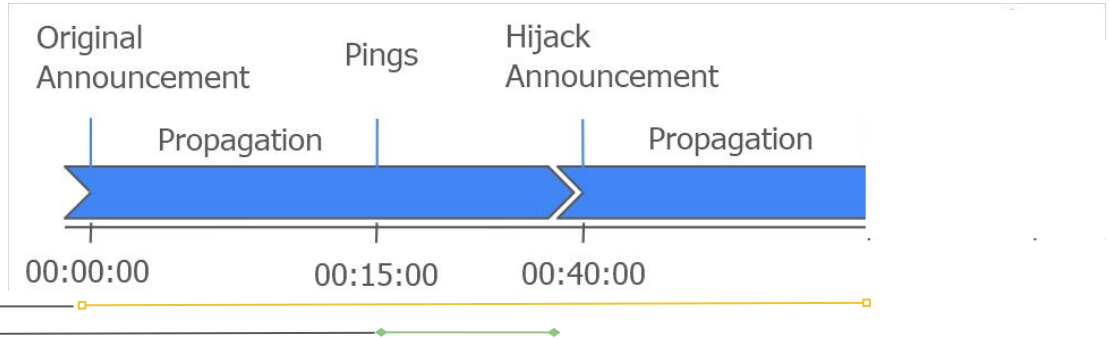


Example of configuration

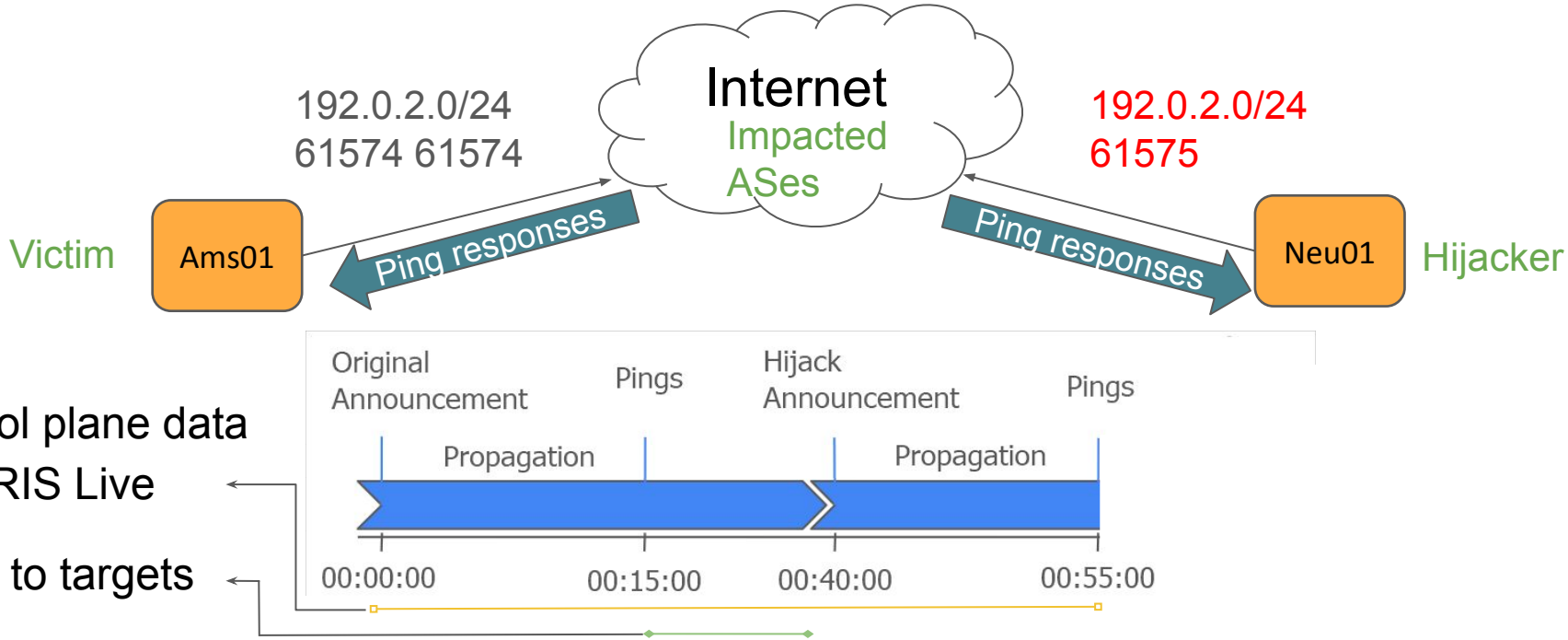


Control plane data from RIS Live

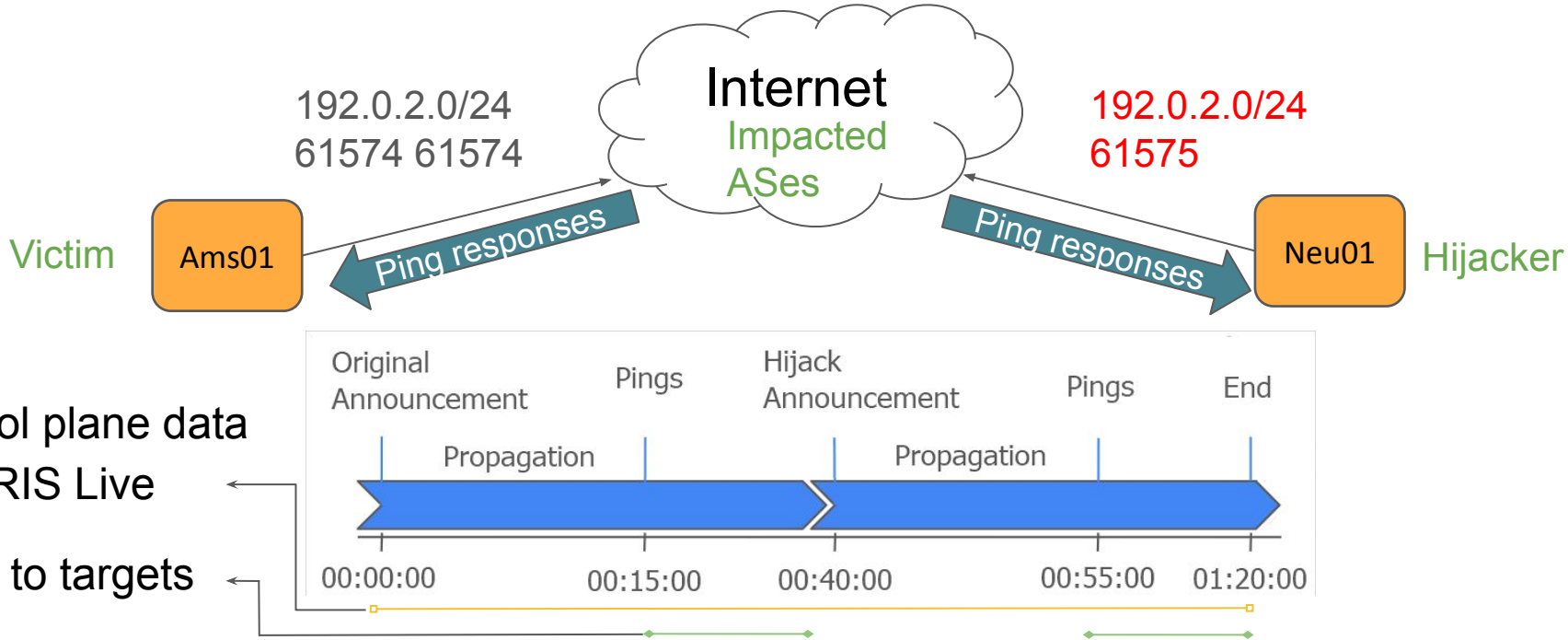
Pings to targets



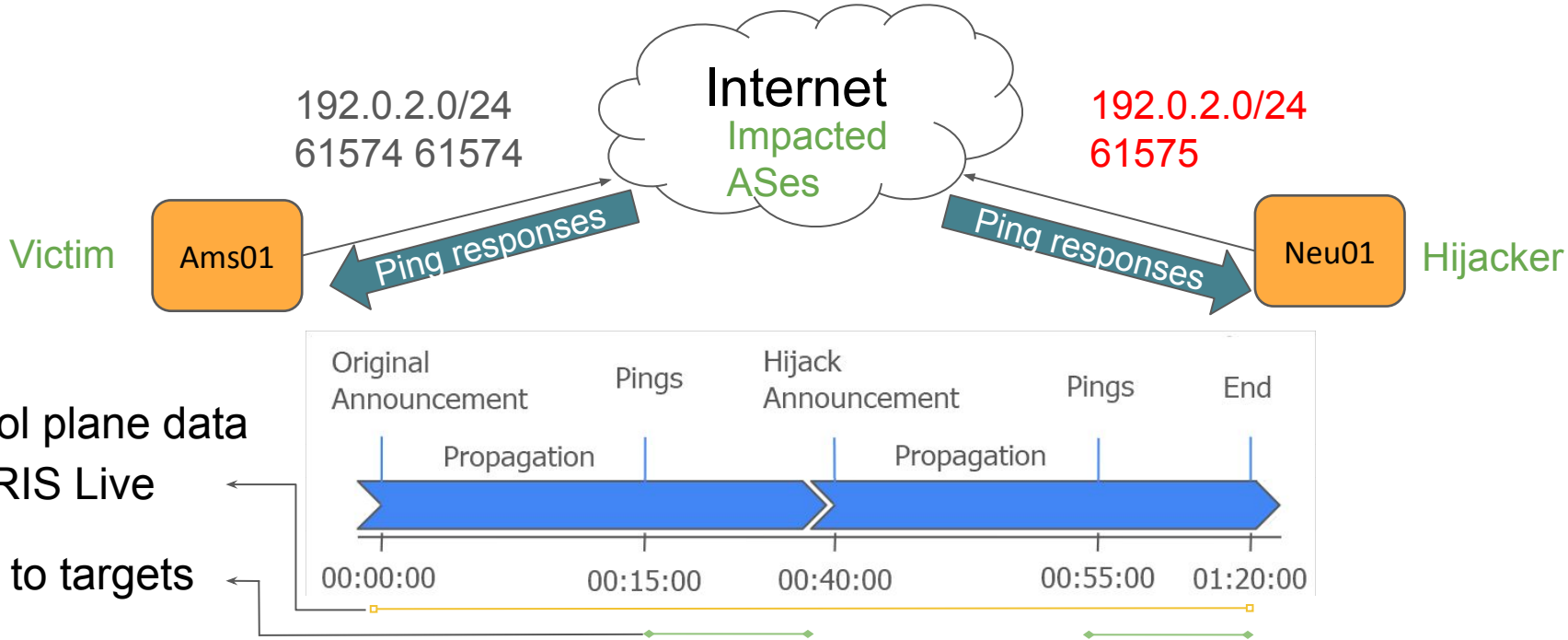
Example of configuration



Example of configuration



Example of configuration



In each iteration, we will vary the techniques employed, AS locations, and connectivity

Details of experiments

Details of experiments

PoP

PoPs/Muxes were selected considering quality, stability and geographical diversity: *amsterdam01*, *ufmg01*, *neu01*, *vtrjohannesburg*, and *vtrseoul*

Details of experiments



PoPs/Muxes were selected considering quality, stability and geographical diversity: *amsterdam01*, *ufmg01*, *neu01*, *vtrjohannesburg*, and *vtrseoul*



Data plane targets are based on the ANT IP list where:

- Only responsive targets were used;
- Hosts with unavailable geolocation data (Per MaxMind DB) where discarded;
- Maximum 5 entries per AS.

In total, 127,421 responsive targets across 45,462 ASes

Details of experiments



PoPs/Muxes were selected considering quality, stability and geographical diversity: *amsterdam01*, *ufmg01*, *neu01*, *vtrjohannesburg*, and *vtrseoul*



Data plane targets are based on the ANT IP list where:

- Only responsive targets were used;
- Hosts with unavailable geolocation data (Per MaxMind DB) where discarded;
- Maximum 5 entries per AS.

In total, 127,421 responsive targets across 45,462 ASes

ASNs used: 61574 and 61575

Prefix used:187.164.226.0/23 and its sub-prefixes

Details of experiments



Prefix length experiments were run between 16/11/2024 and 22/11/2024.
ASPP were run between 24/01/2025 and 05/02/2025.
Selective announcement experiments were run 17/02/2025 and 18/02/2025.

Details of experiments



Prefix length experiments were run between 16/11/2024 and 22/11/2024.
ASPP were run between 24/01/2025 and 05/02/2025.
Selective announcement experiments were run 17/02/2025 and 18/02/2025.



We measure the impact in the control plane and data plane as:

$$\textit{Impact Percentage} = \frac{\textit{Monitors/Hosts Hijacker}}{\textit{Monitors/Hosts Victim}} \times 100$$

Details of experiments



Prefix length experiments were run between 16/11/2024 and 22/11/2024.
ASPP were run between 24/01/2025 and 05/02/2025.
Selective announcement experiments were run 17/02/2025 and 18/02/2025.



We measure the impact in the control plane and data plane as:

$$\textit{Impact Percentage} = \frac{\textit{Monitors/Hosts Hijacker}}{\textit{Monitors/Hosts Victim}} \times 100$$

Due to limitations, we restrict our experiments to IPv4 and type-0 hijacks. No ROAs were created or modified

Our goal is to understand the how traffic engineering decisions affect routing security



How do different techniques affect the impact of a hijack?

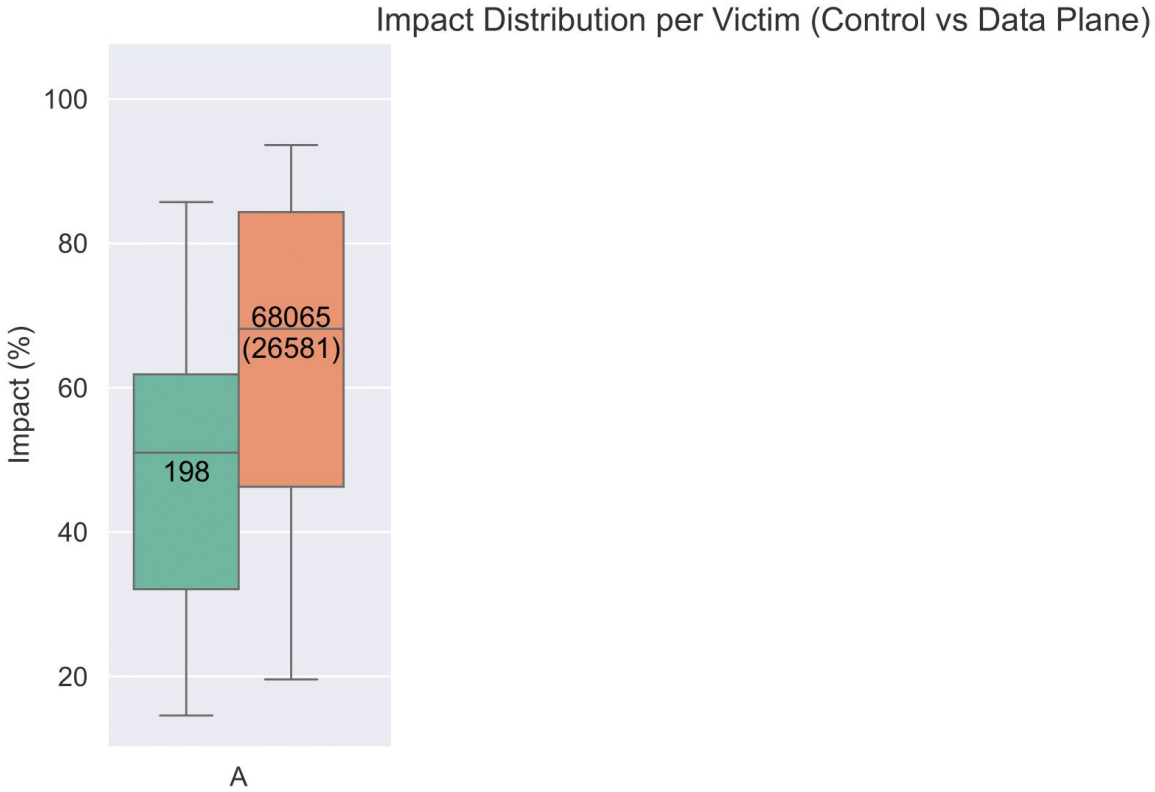


What is the current state of ITE usage and its potential impact on security?

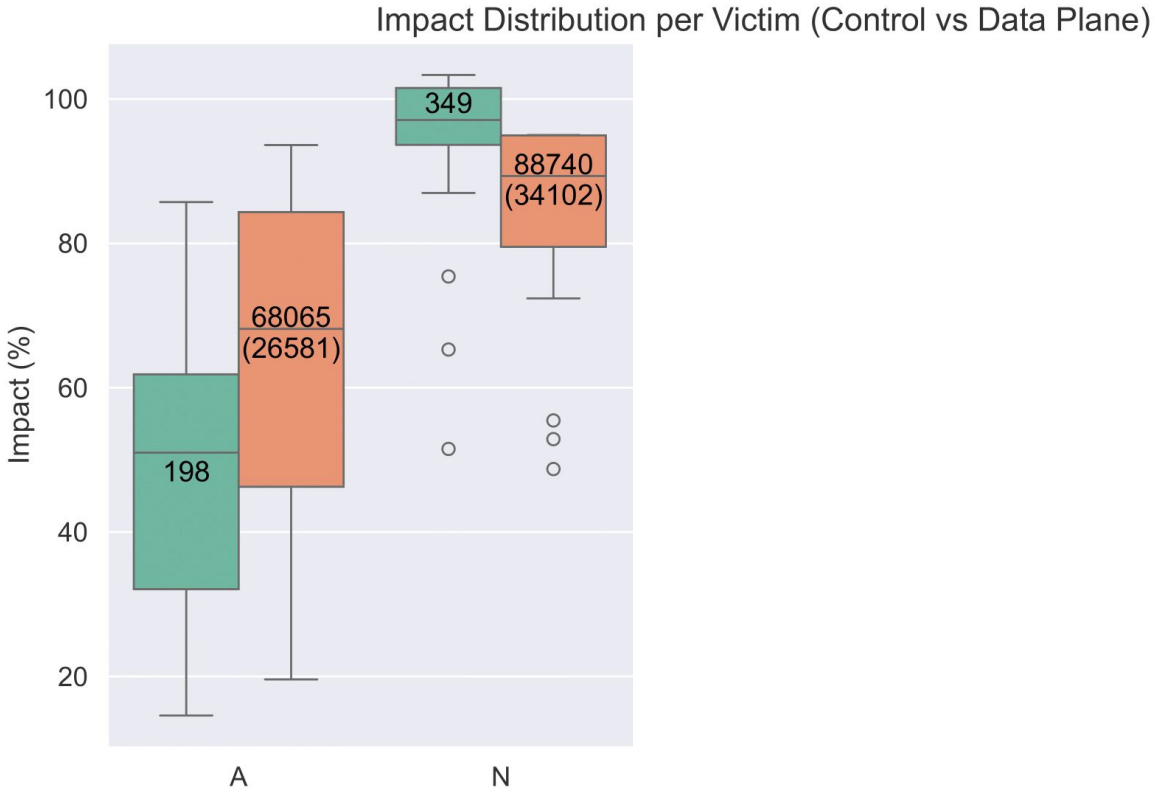
ITE Impact - Prepend



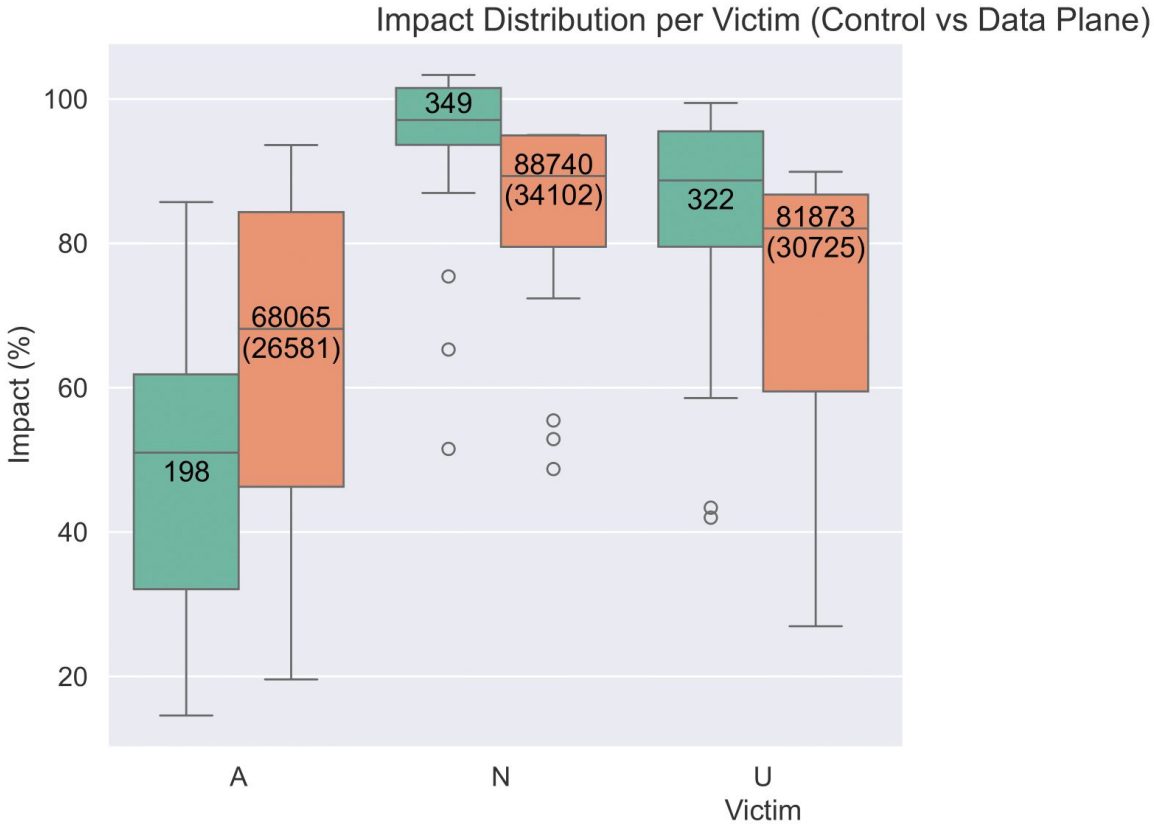
ITE Impact - Prepend



ITE Impact - Prepend



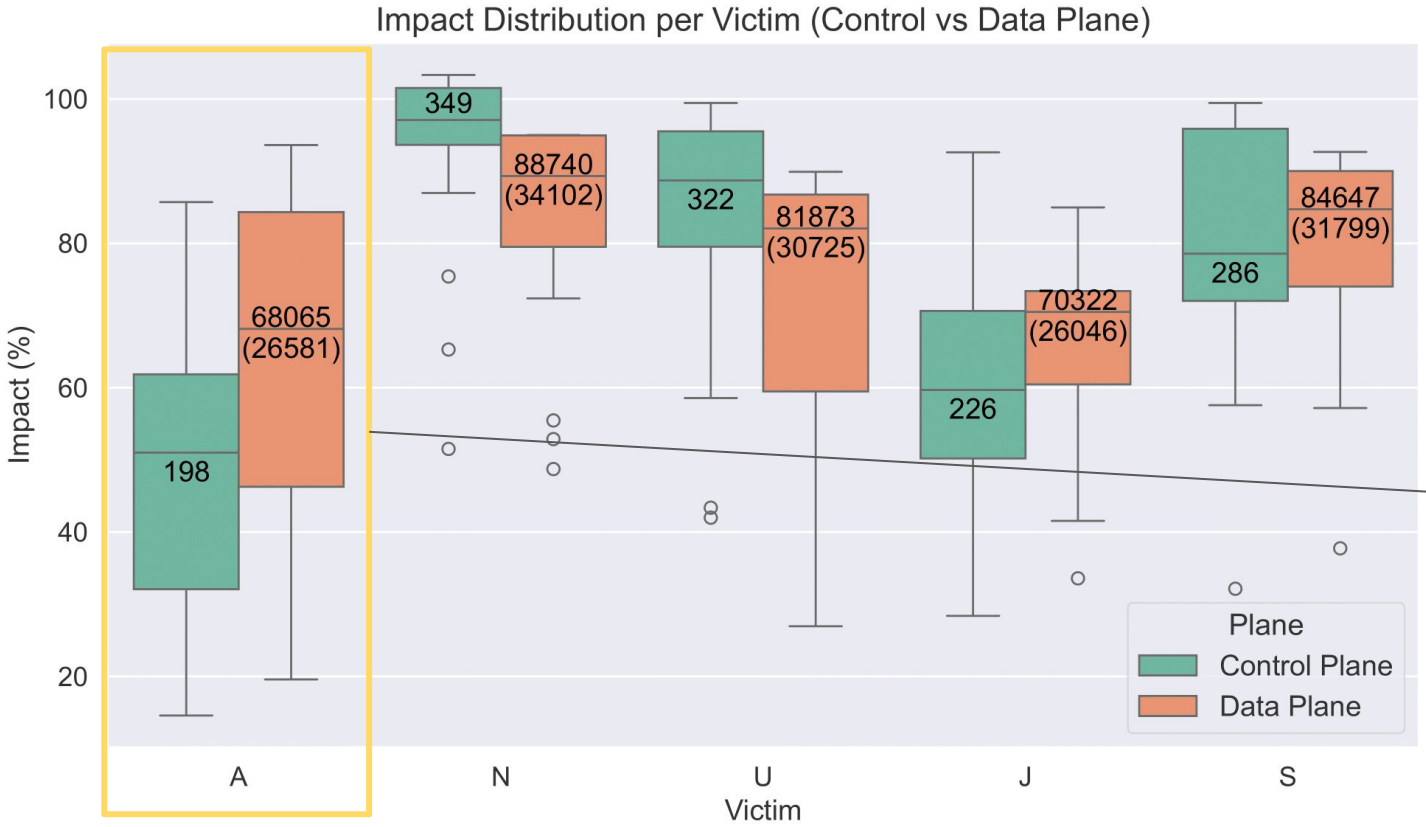
ITE Impact - Prepend



ITE Impact - Prepend

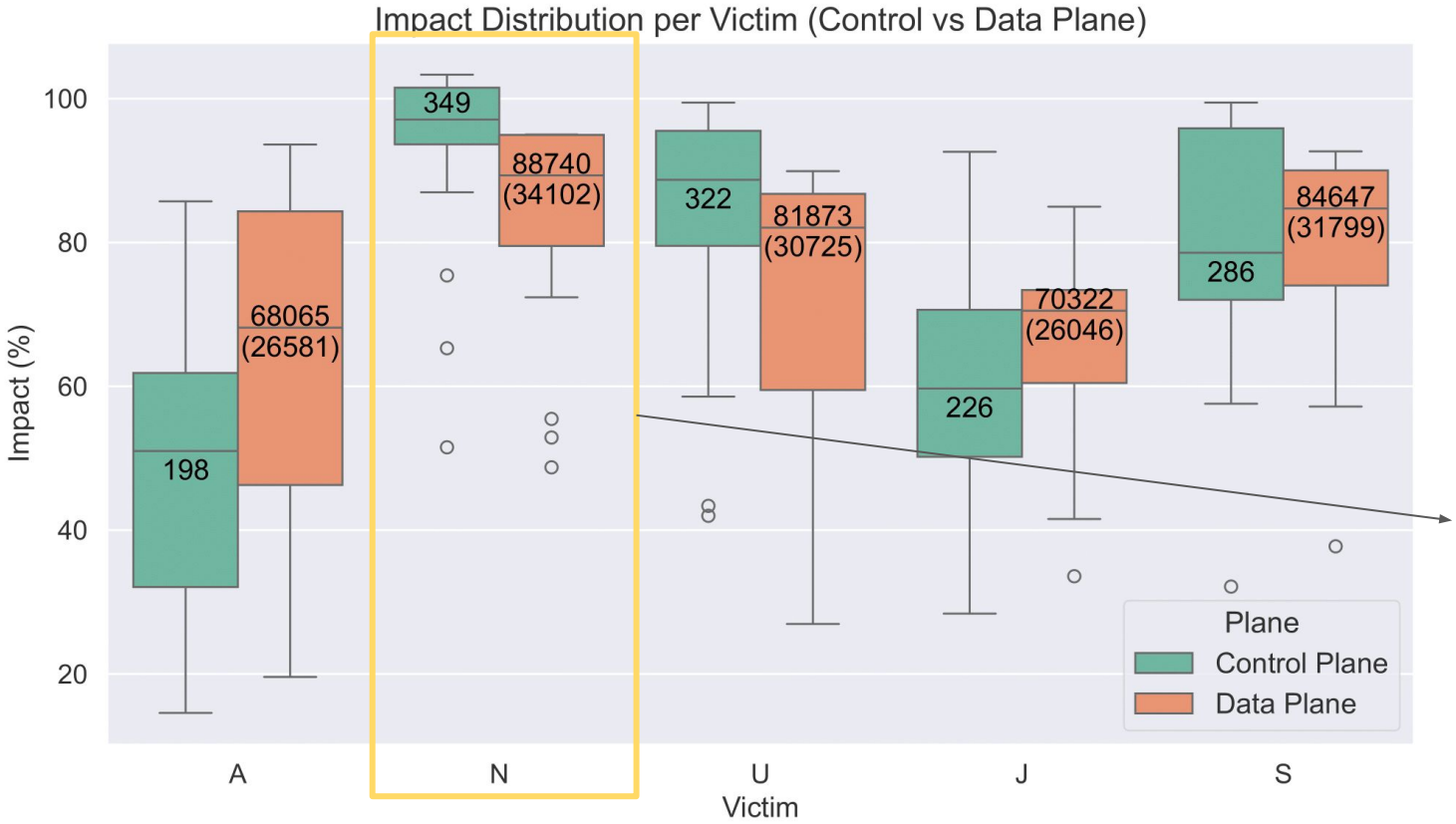


ITE Impact - Prepend



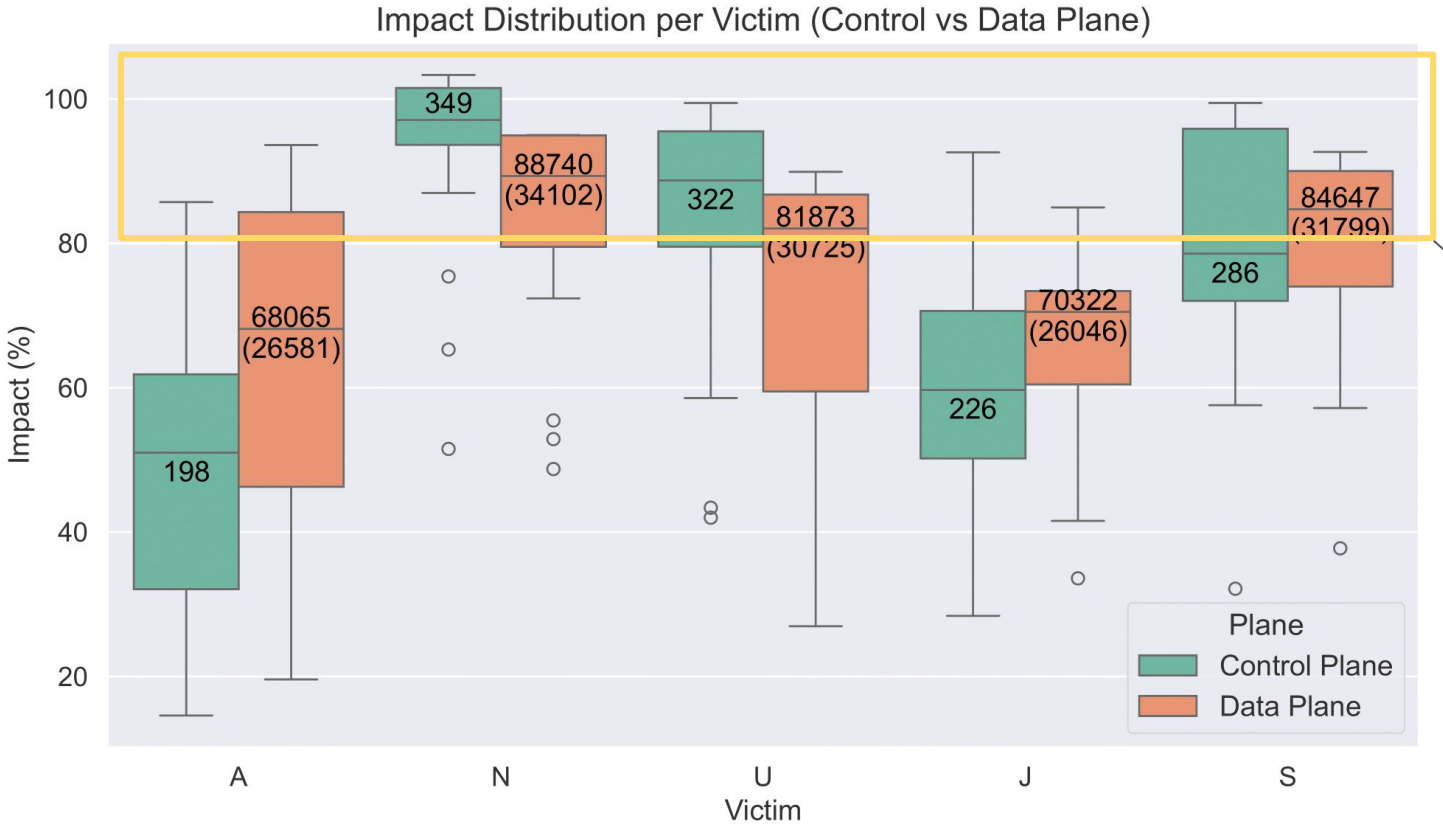
Amsterdam is less impacted in some scenarios

ITE Impact - Prepend



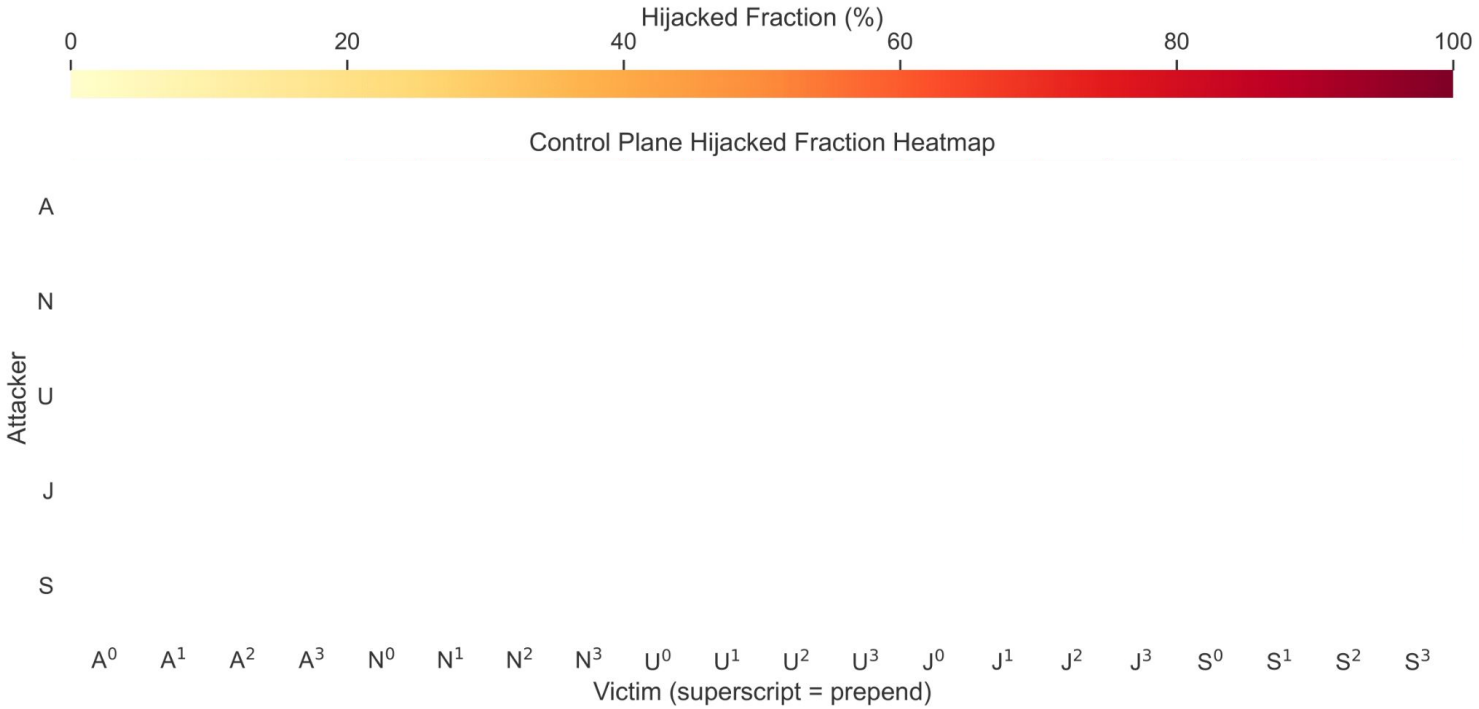
Neu01 experiences more significant impact

ITE Impact - Prepend

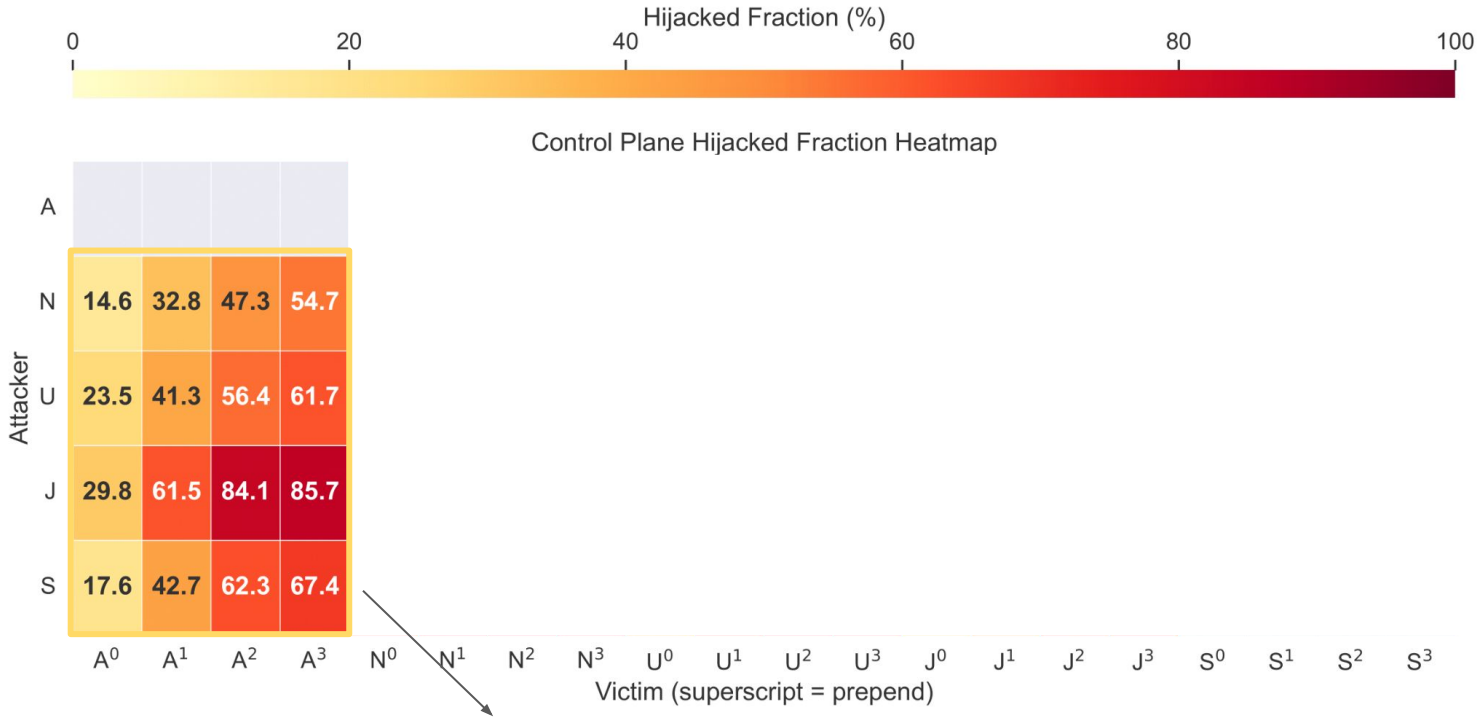


All muxes have scenarios with significant impact

ITE Impact - Prepend

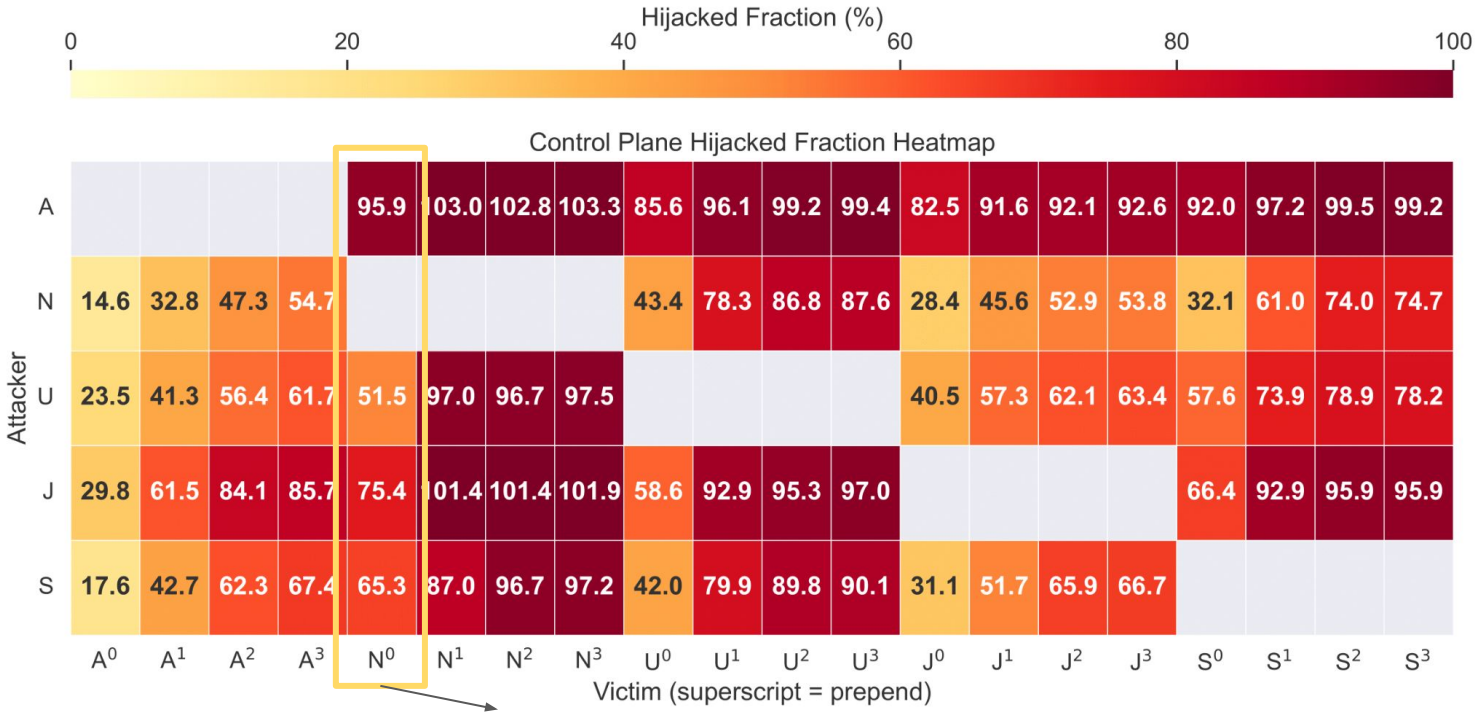


ITE Impact - Prepend



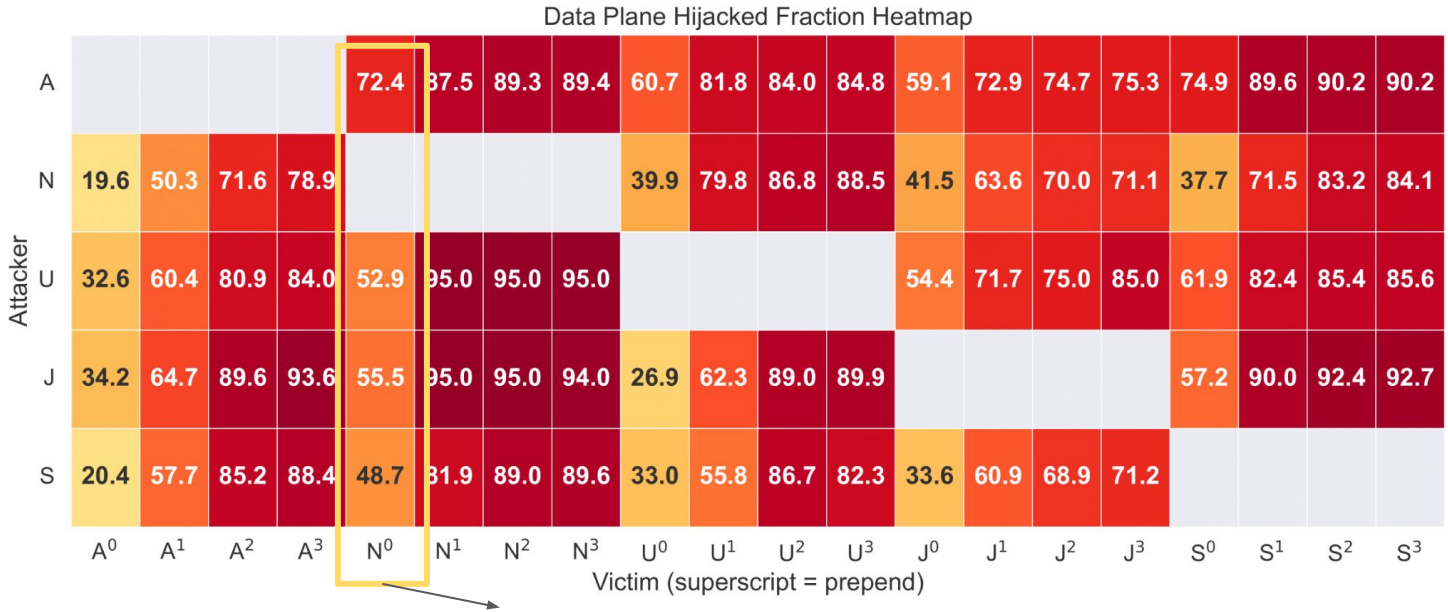
Increasing the number of prepends increases the impact of a hijack

ITE Impact - Prepend



However, ASes may experience impact even without using prepending

ITE Impact - Prepend

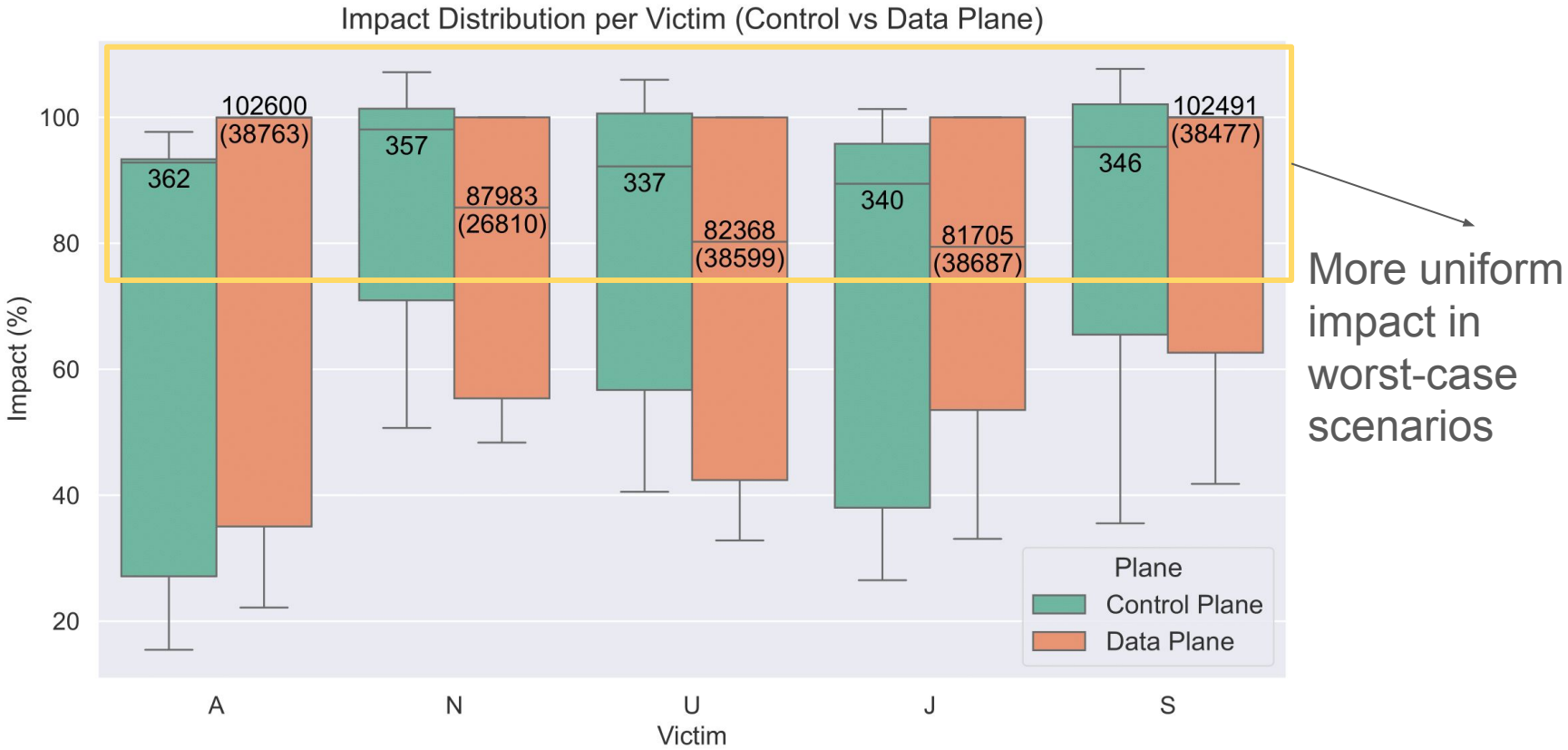


However, ASes may experience impact even without using prepending



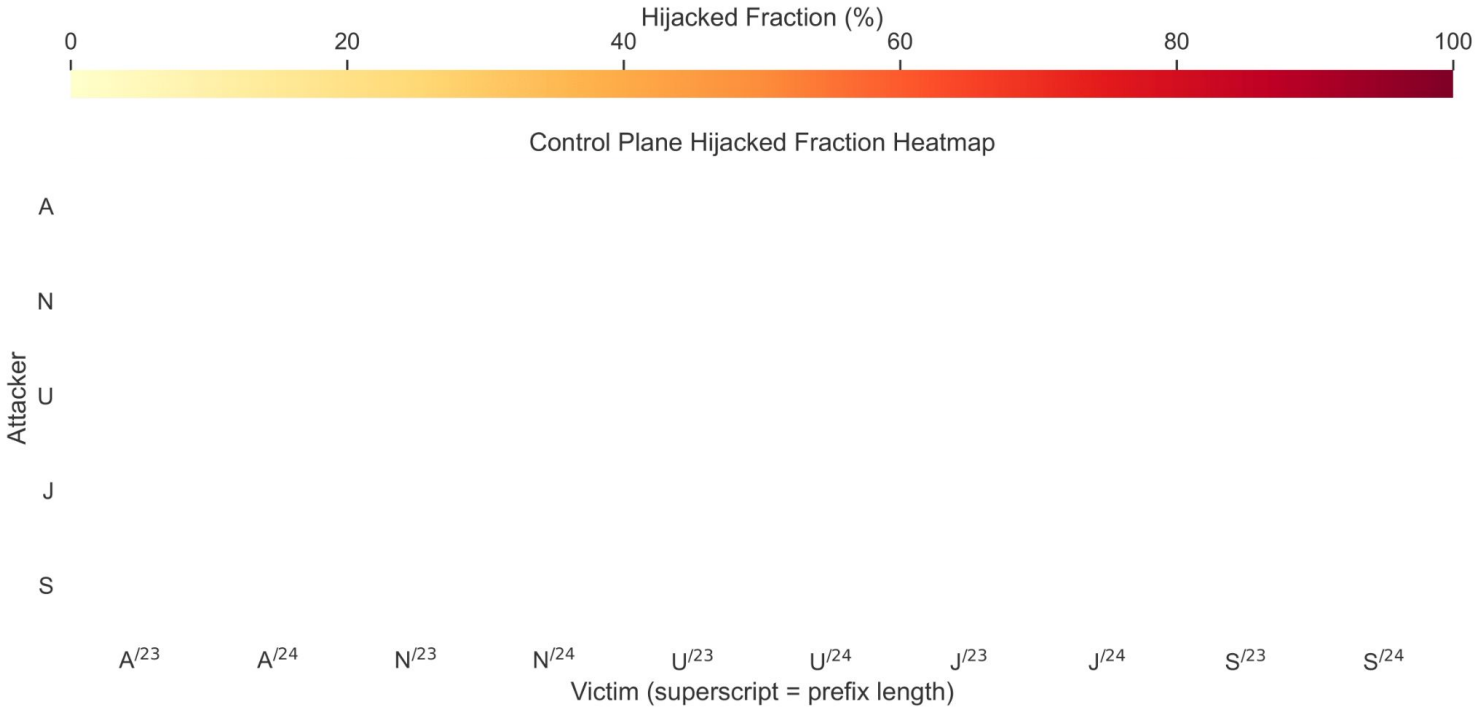
ITE Impact - Prefix Length

ITE Impact - Prefix Length

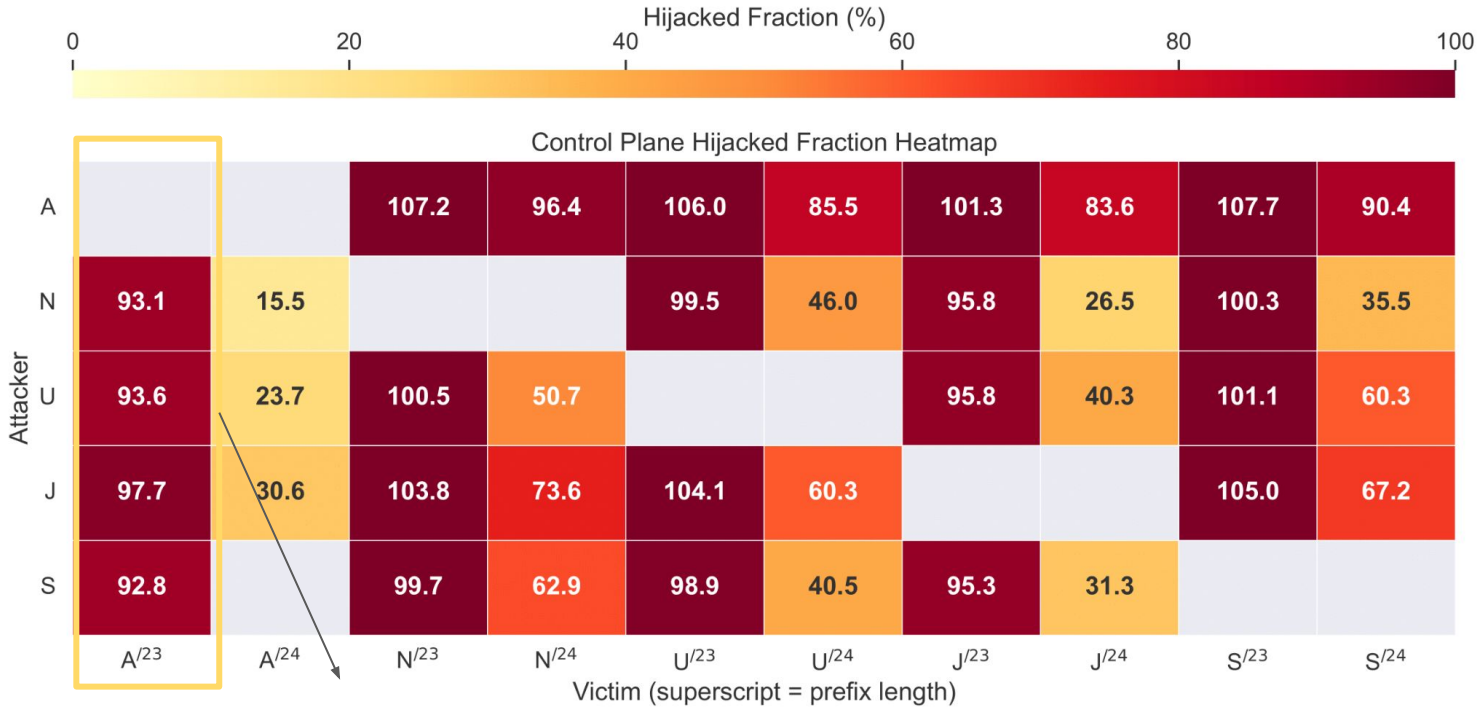


More uniform impact in worst-case scenarios

ITE Impact - Prefix Length

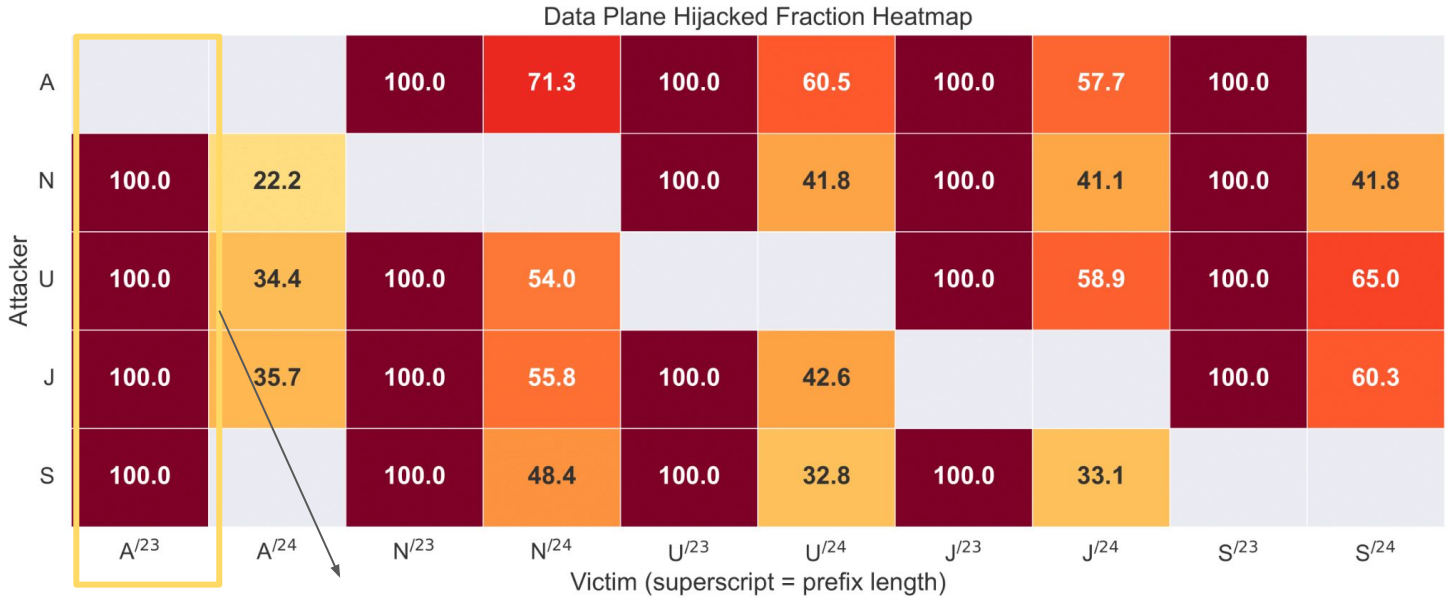


ITE Impact - Prefix Length



Even well-connected ASes can be affected by attacks using more specific prefixes

ITE Impact - Prefix Length



Even well-connected ASes can be affected by attacks using more specific prefixes

ITE Impact - Selective

Experiment Configuration			Control Plane Monitors		Data Plane Targets	
Origin	Hijacker	Peers/IX	Total	Hijacked	Total	Hijacked

ITE Impact - Selective

Experiment Configuration			Control Plane Monitors		Data Plane Targets	
Origin	Hijacker	Peers/IX	Total	Hijacked	Total	Hijacked
amsterdam01	neu01	AMS-IX	18	345 (1,916%)	1165	98252 (84.34%)
amsterdam01	neu01	Bit BV	371	65 (17.52%)	98872	21726 (21.97%)
amsterdam01	neu01	AMS-IX, Bit BV	371	65 (17.52%)	98939	21853 (22.08%)
amsterdam01	neu01	Coloclue, Bit BV	386	63 (16.32%)	98794	21681 (21.94%)
amsterdam01	neu01	AMS-IX, Coloclue, Bit BV	386	65 (16.83%)	98779	21818 (22.08%)

Similar impact across different configurations

ITE Impact - Selective

Experiment Configuration			Control Plane Monitors		Data Plane Targets	
Origin	Hijacker	Peers/IX	Total	Hijacked	Total	Hijacked
amsterdam01	neu01	AMS-IX	18	345 (1,916%)	1165	98252 (84.34%)
amsterdam01	neu01	Bit BV	371	65 (17.52%)	98872	21726 (21.97%)
amsterdam01	neu01	AMS-IX, Bit BV	371	65 (17.52%)	98939	21853 (22.08%)
amsterdam01	neu01	Coloclue, Bit BV	386	63 (16.32%)	98794	21681 (21.94%)
amsterdam01	neu01	AMS-IX, Coloclue, Bit BV	386	65 (16.83%)	98779	21818 (22.08%)
amsterdam01	neu01	Coloclue	391	39 (9.97%)	98884	20967 (21.20%)
amsterdam01	neu01	AMS-IX, Coloclue	391	39 (9.97%)	98716	20980 (21.25%)

Not announcing to a specific neighbor leads to a lower impact

Our goal is to understand the how traffic engineering decisions affect routing security



How do different techniques affect the impact of a hijack?



What is the current state of ITE usage and its potential impact on security?



Current Scenario

Current Scenario

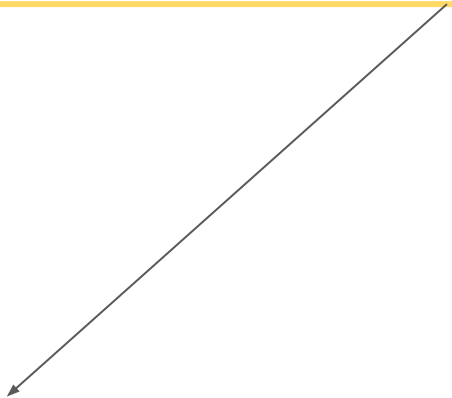
- Prepend usage
  - 0-1: Safe
  - 2: At Risk
  - 3 or More: Not Safe

Characteristic	Safe	At Risk	Not Safe

Current Scenario

- Prepend usage
  - 0-1: Safe
  - 2: At Risk
  - 3 or More: Not Safe

Characteristic	Safe	At Risk	Not Safe
ASPP	90.65%	3.48%	5.87%



Most of the address space does not use prepending or uses it only once

Current Scenario

- Prepend usage
  - 0-1: Safe
  - 2: At Risk
  - 3 or More: Not Safe

- Peers/Providers
  - 1: Unsafe
  - 2 or More: Safe

Characteristic	Safe	At Risk	Not Safe
ASPP	90.65%	3.48%	5.87%
Peers/Providers	82.46%	N/A	17.54%

Most of the address space is announced by ASes with at least two Peers/Providers

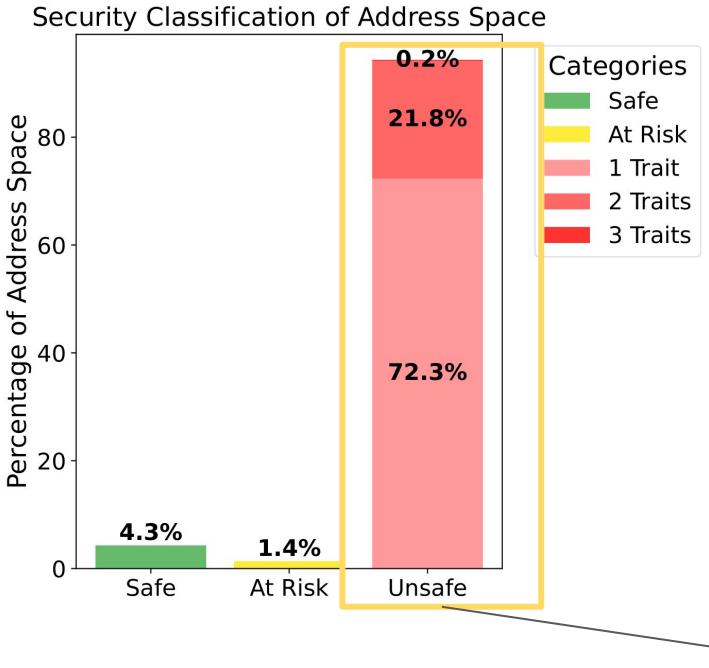
Current Scenario

- Prepend usage
  - 0-1: Safe
  - 2: At Risk
  - 3 or More: Not Safe
- Peers/Providers
  - 1: Unsafe
  - 2 or More: Safe
- Prefix length
  - /24: Safe
  - /23: At Risk
  - /22 or Shorter: Not Safe

Characteristic	Safe	At Risk	Not Safe
ASPP	90.65%	3.48%	5.87%
Peers/Providers	82.46%	N/A	17.54%
Prefix Length	5.34%	1.45%	93.21%

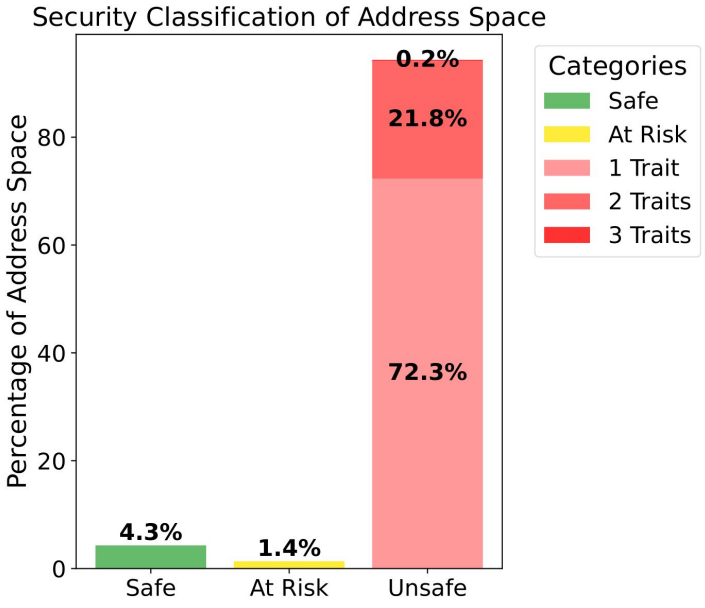
Most of the address space is announced in prefixes shorter than /23

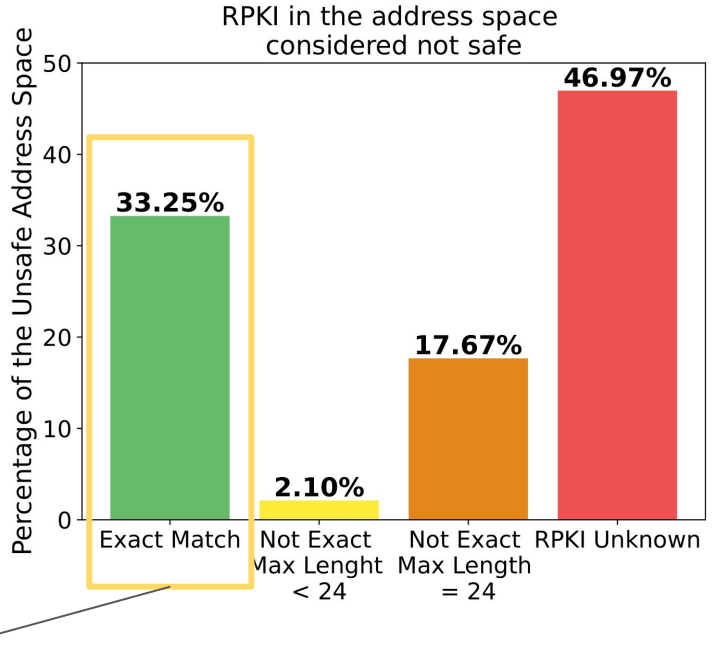
Current Scenario



By combining the three analyses, most of the address space exhibits characteristics that may facilitate the impact of a prefix hijack

Current Scenario





Of the address space we consider insecure, only 33.25% has ROAs with a max length equal to the announcement

In Summary…

In Summary…



RQ1:The techniques influence the likelihood of a hijack. Attacks using longer prefixes are effective

In Summary…



RQ1:The techniques influence the likelihood of a hijack. Attacks using longer prefixes are effective



RQ2: 61.4% of the address space has security risks

In Summary…



RQ1:The techniques influence the likelihood of a hijack. Attacks using longer prefixes are effective



RQ2: 61.4% of the address space has security risks



Limit ASPP to only the necessary to achieve routing objectives.

In Summary…



RQ1:The techniques influence the likelihood of a hijack. Attacks using longer prefixes are effective



RQ2: 61.4% of the address space has security risks



Limit ASPP to only the necessary to achieve routing objectives.



Create and validate ROAs. If possible keep max length inline with current announcements.

In Summary…



RQ1:The techniques influence the likelihood of a hijack. Attacks using longer prefixes are effective



RQ2: 61.4% of the address space has security risks



Limit ASPP to only the necessary to achieve routing objectives.



Create and validate ROAs. If possible keep max length inline with current announcements.

In Summary…



RQ1:The techniques influence the likelihood of a hijack. Attacks using longer prefixes are effective



RQ2: 61.4% of the address space has security risks



Limit ASPP to only the necessary to achieve routing objectives.



Create and validate ROAs. If possible keep max length inline with current announcements.

Renan Barreto
renan.barreto@furg.br