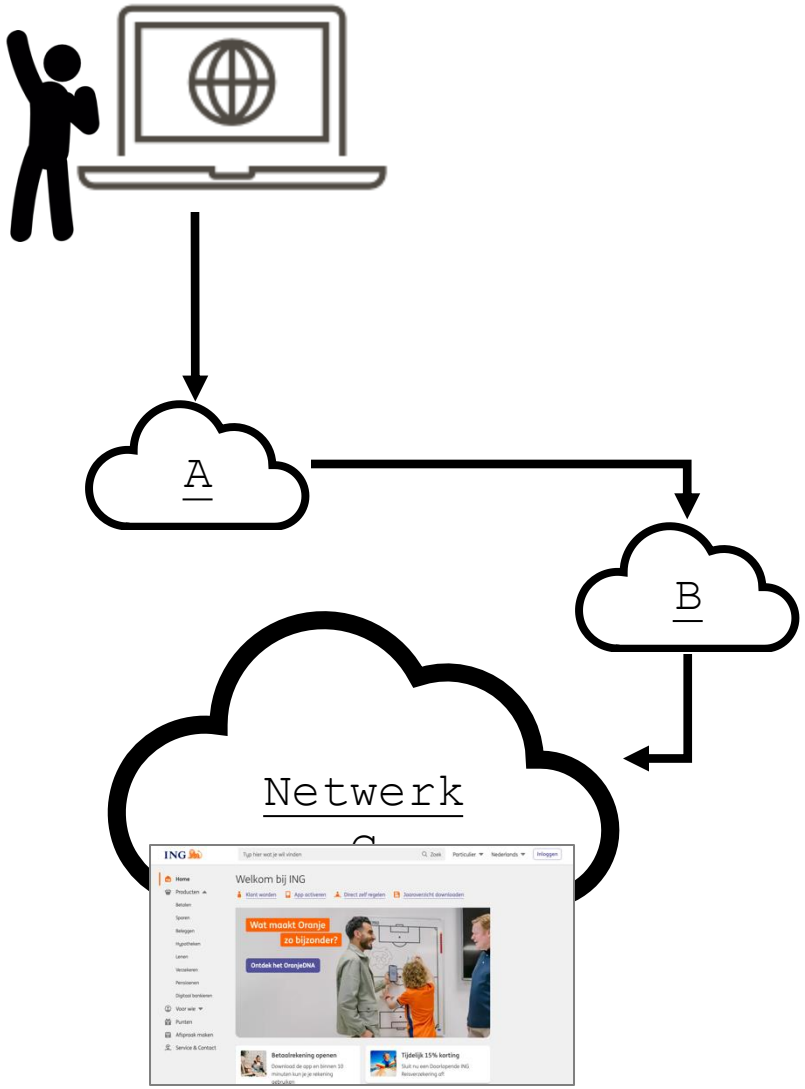
Routing Security bij Labs

Moritz Müller

Arnhem, 8 october 2024

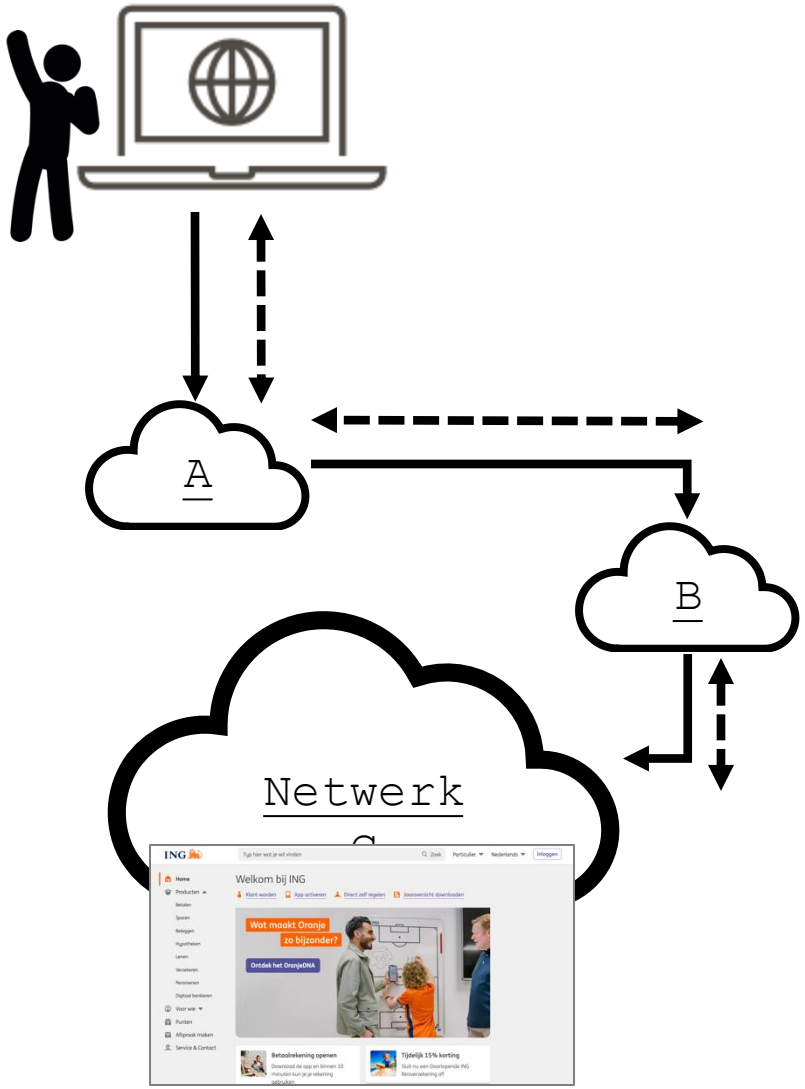
Risico: aanvallen op het routeringsysteem

Het pad naar
2.18.157.132
(ing.nl)
is
A → B → C

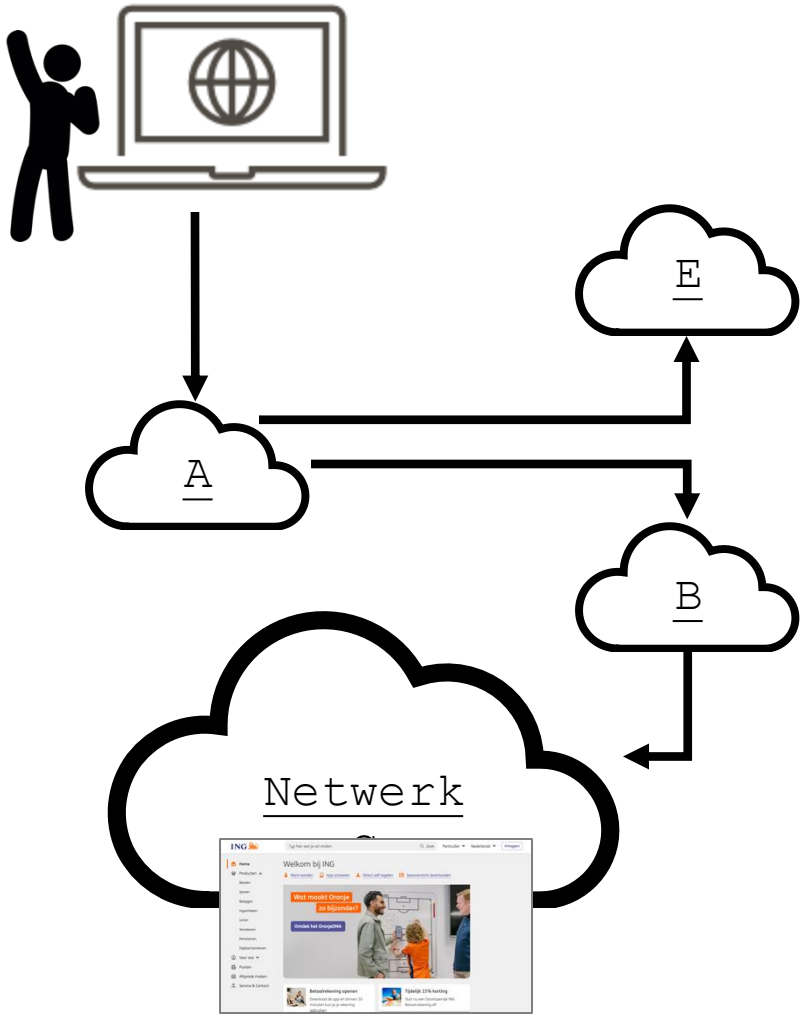


Risico: aanvallen op het routeringsysteem

Het pad naar
2.18.157.132
(ing.nl)
is
A → B → C

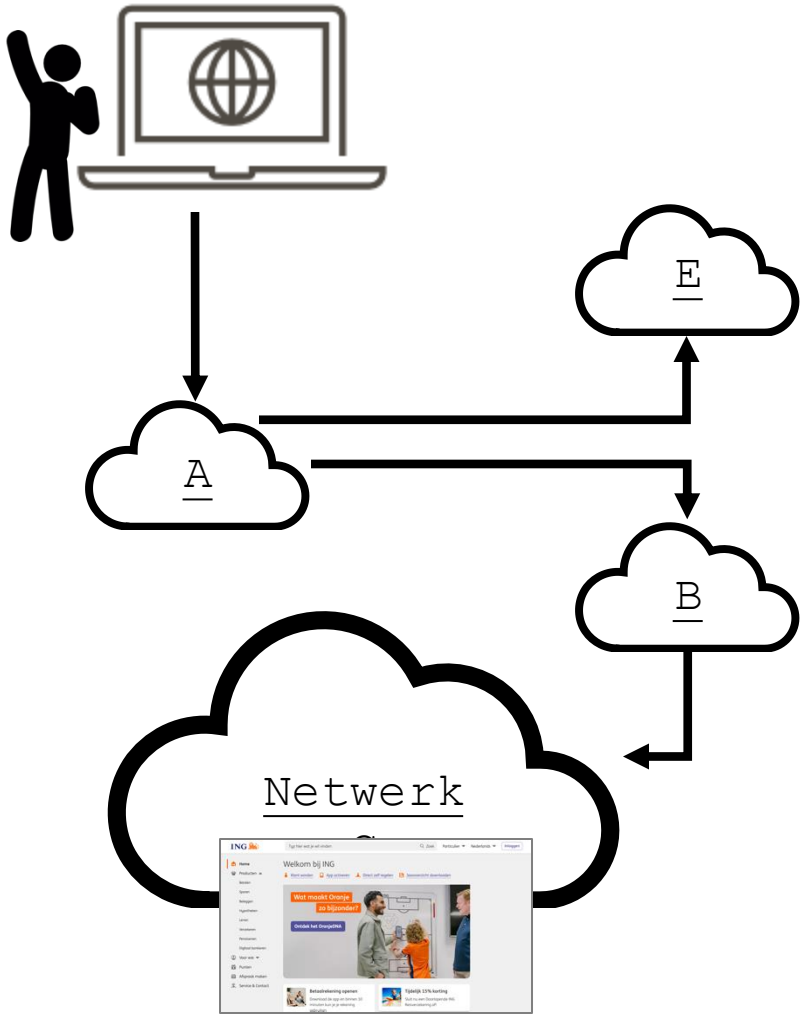


Risico: aanvallen op het routeringsysteem



Risico: aanvallen op het routeringsysteem

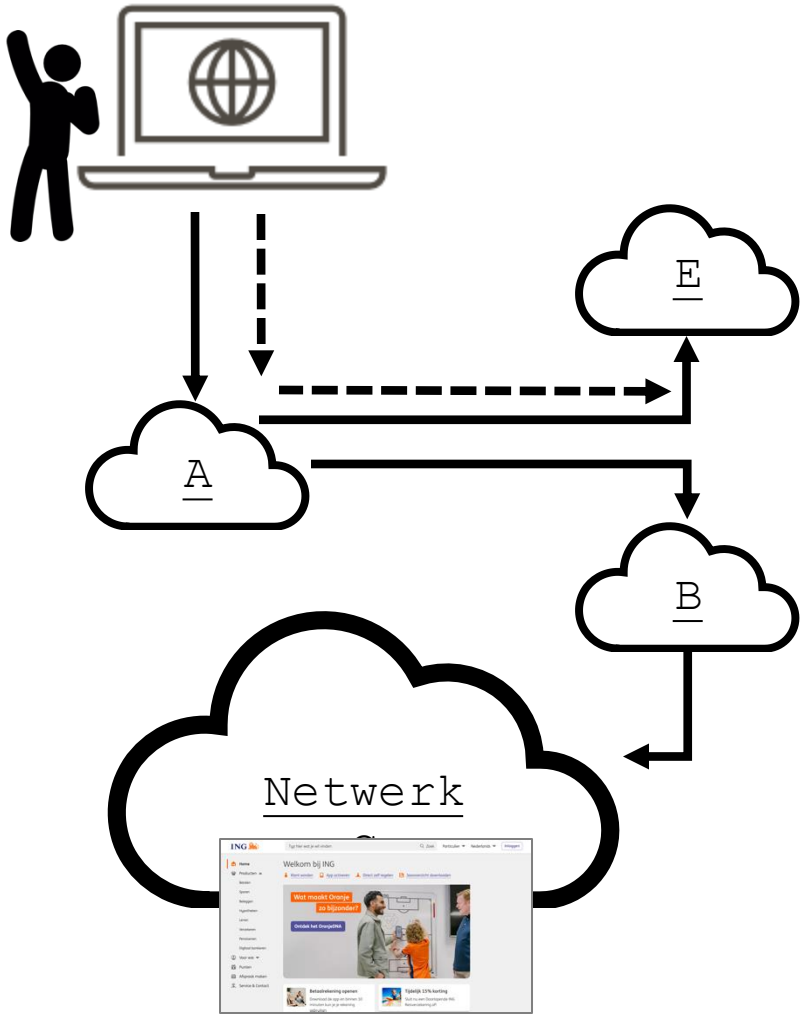
Het pad naar
2.18.157.132
is
A → E



2.18.157.132

Risico: aanvallen op het routeringsysteem

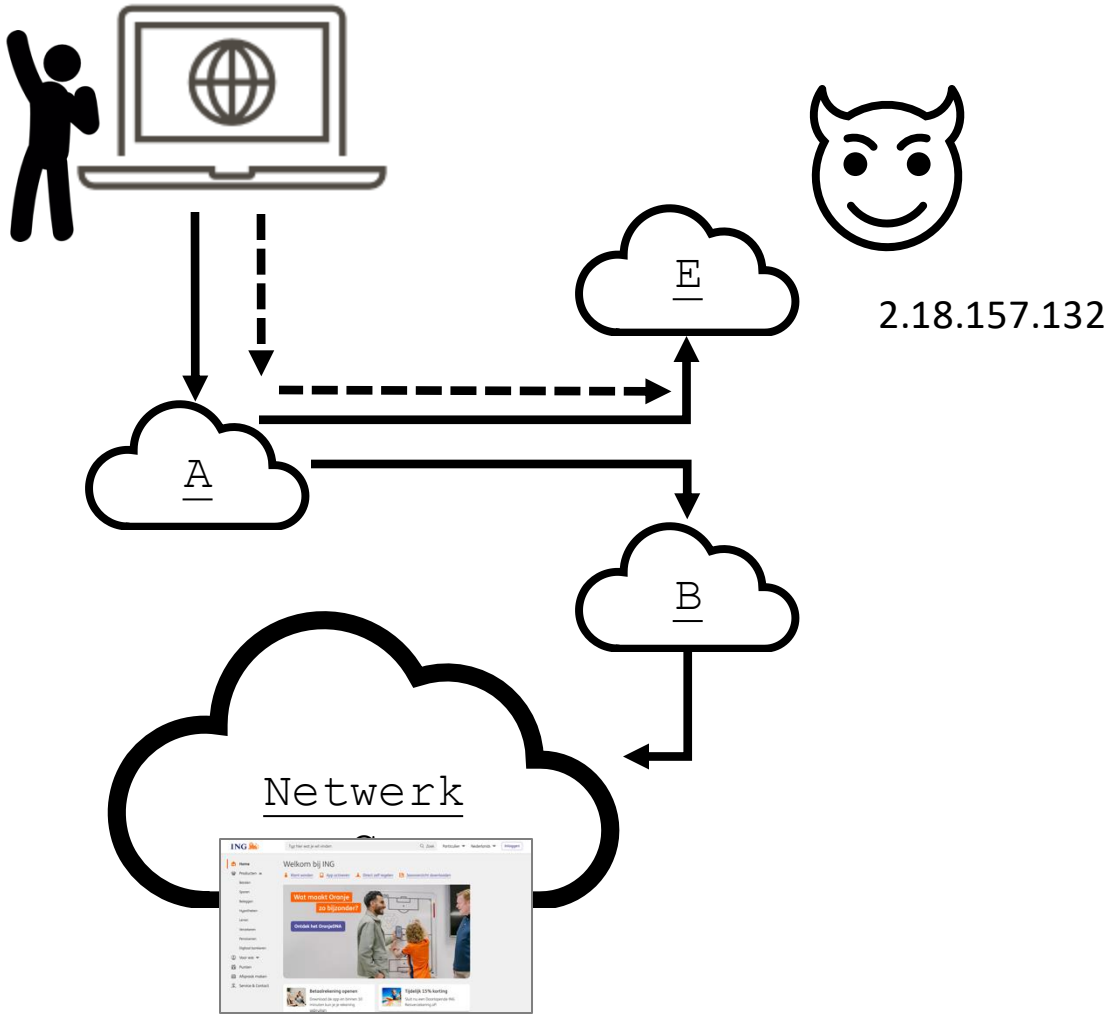
Het pad naar
2.18.157.132
is
A → E



2.18.157.132

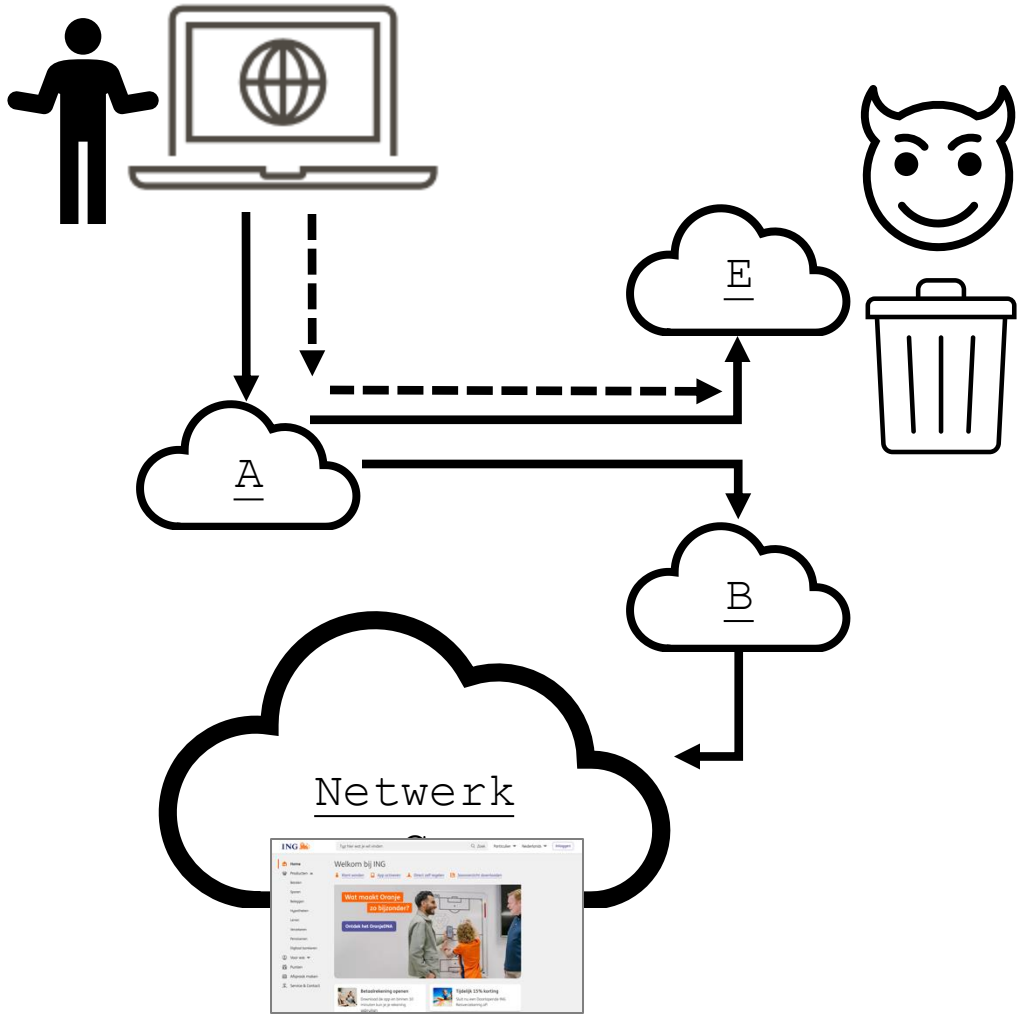
Risico: aanvallen op het routeringsysteem

Het pad naar
2.18.157.132
is
A → E



Risico: aanvallen op het routeringsysteem

Het pad naar
2.18.157.132
is
A → E



Risico: aanvallen op het routeringsysteem

- Prefix hijacks
  - Exact match
  - More specifc
- Path hijack

- Heel vaak misconfiguratie, soms malafide

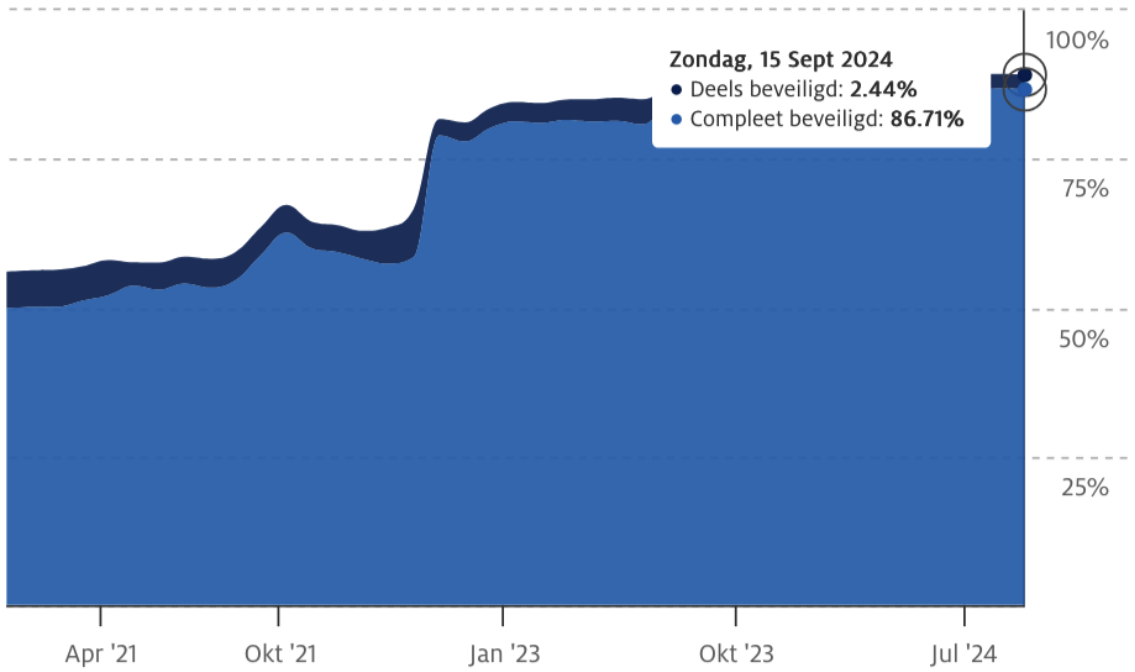
Routing security: Relevant voor .nl

- Invloed op de beschibkaarheid van onze diensten
- Invloed op de beschikbaarheid van diensten gekoppeld aan domeinnamen
- Kan het vertrouwen in het internet in zijn geheel verlagen

Stap 1: RPKI

- Resource Public Key Infrastructure (RPKI)

- Toepassingen:
  - Geverifieerde informatie over welk IP-adresruimte vanuit welk netwerk bereikbaar is (ROA)
  - Geverifieerde informatie over welk netwerk via welk netwerk bereikbaar is (ASPA)
  - …



.nl Domeinnamen met een VRP
Bron: https://stats.sidnlabs.nl/nl/web.html#secure%20routing%20(rpki)

Uitdagingen van RPKI

- **Kwestbaar**: Een storing van de RPKI kan grote gevolgen hebben voor de veiligheid en beschikbaarheid van het internet.

- **Onvoldoende:** De informatie die op dit moment in de RPKI staat is niet voldoende om tegen alle aanvallen op het routeringsysteem te beschermen.

- **Onduidelijk:** Niet alle aanvallen op het routeringsysteem hebben even veel impact. Voor netwerkbeheerders is niet altijd duidelijk hoe ze moeten omgaan met aanvallen.

SIDN LABS

Onze aanpak

1. Onderzoeksfocus bepalen

2. Samenwerken

3. Zelf draaien

Onze aanpak

1. Onderzoeksfocus bepalen

2. Samenwerken

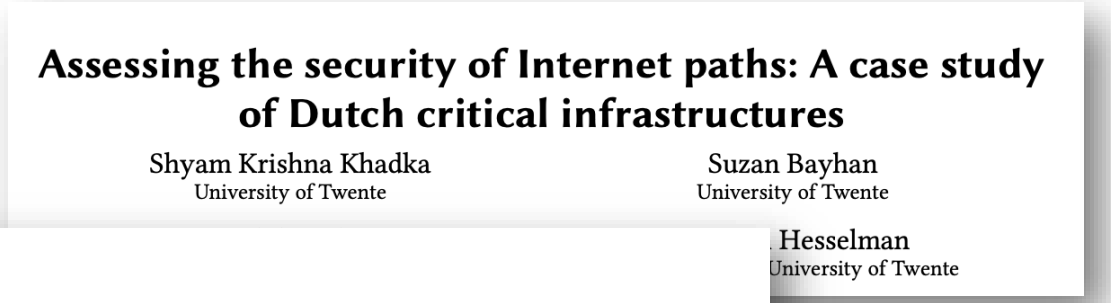
3. Zelf draaien

https://www.sidnlabs.nl/nieuws-en-blogs/onze-onderzoeksagenda-voor-veiligere-routering

Onze aanpak

1. Onderzoeksfocus bepalen

ACM/IRTF Applied Networking Research Workshop 2024



2. Samenwerken

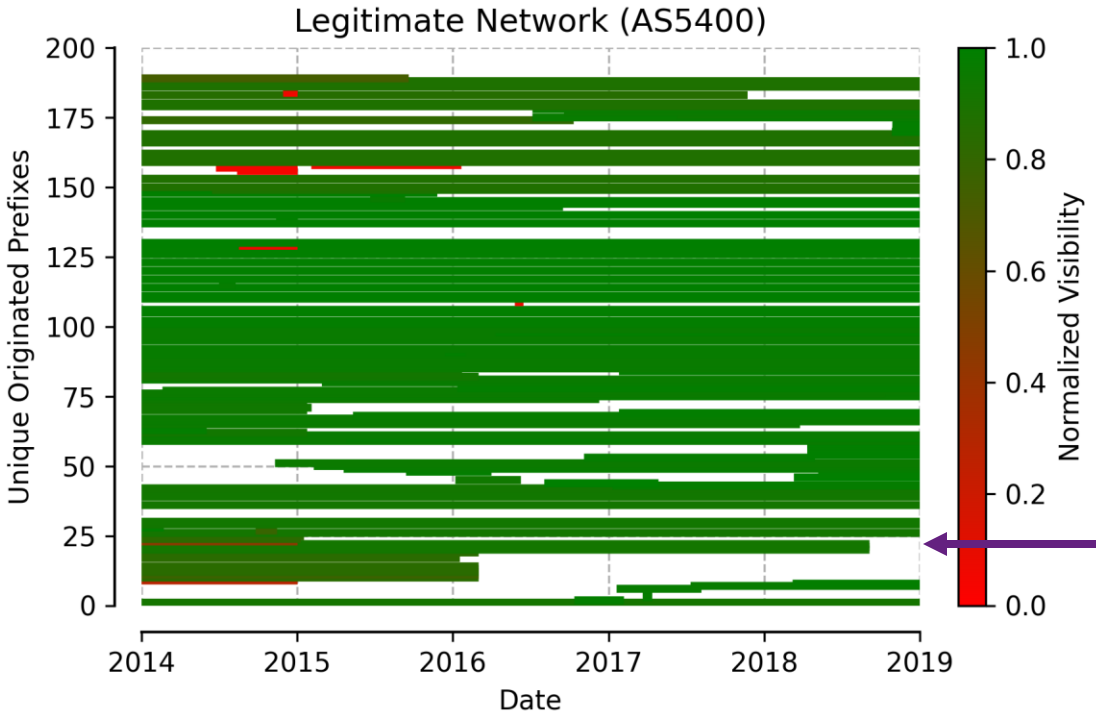
Network Traffic Measurement and Analysis Conference 2024

3. Zelf draaien

Serial BGP Hijackers: A Reproducibility Study and Assessment of Current Dynamics

Ebrima Jaw[†], Moritz Müller[†*], Cristian Hesselman[†*], Lambert Nieuwenhuis[†]
[†]University of Twente, Enschede, The Netherlands
[*]SIDN Labs, Arnhem, The Netherlands

- *Serial hijacker* = AS dat regelmatig en lang routing hijacks veroorzaakt

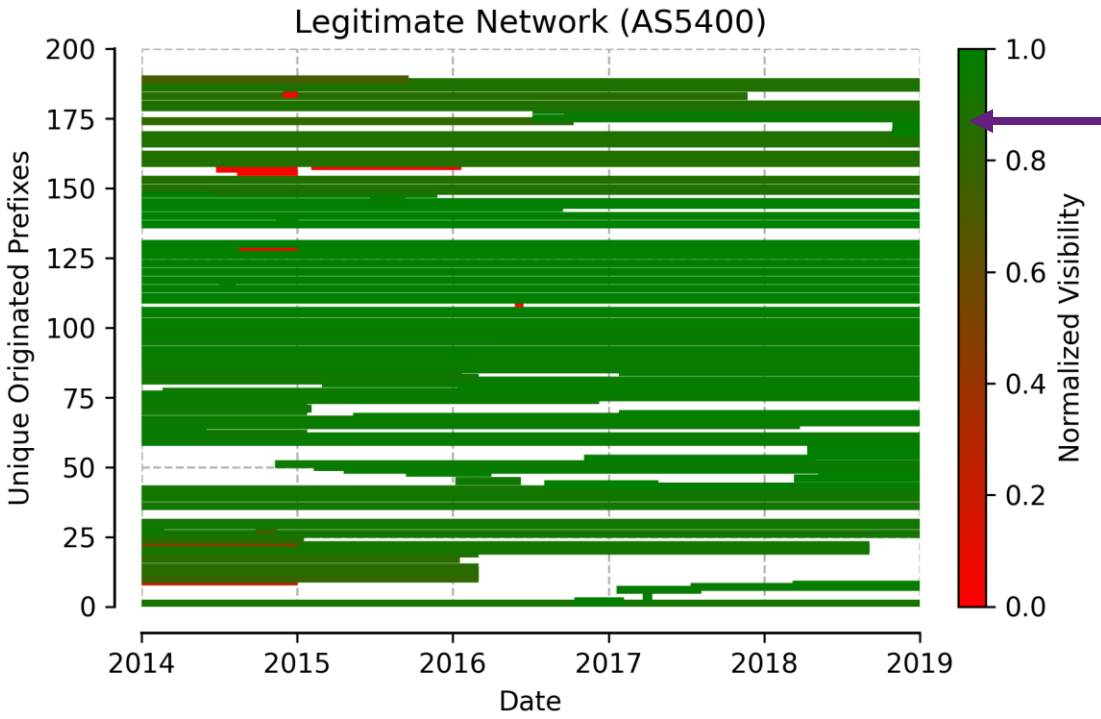


Een lijn = een prefix

Serial BGP Hijackers: A Reproducibility Study and Assessment of Current Dynamics

Ebrima Jaw[†], Moritz Müller[†*], Cristian Hesselman[†*], Lambert Nieuwenhuis[†]
[†]University of Twente, Enschede, The Netherlands
[*]SIDN Labs, Arnhem, The Netherlands

- *Serial hijacker* = AS dat regelmatig en lang routing hijacks veroorzaakt

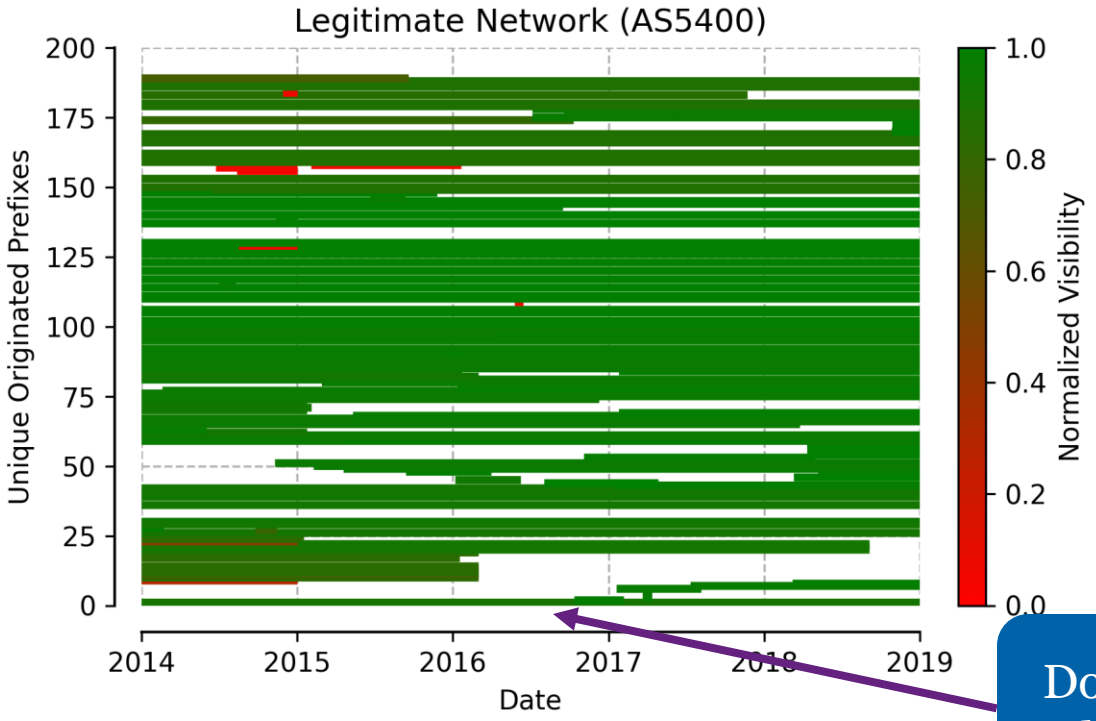


Groen = prefix bereikbaar op het hele internet

Serial BGP Hijackers: A Reproducibility Study and Assessment of Current Dynamics

Ebrima Jaw[†], Moritz Müller[†*], Cristian Hesselman[†*], Lambert Nieuwenhuis[†]
[†]University of Twente, Enschede, The Netherlands
[*]SIDN Labs, Arnhem, The Netherlands

- *Serial hijacker* = AS dat regelmatig en lang routing hijacks veroorzaakt

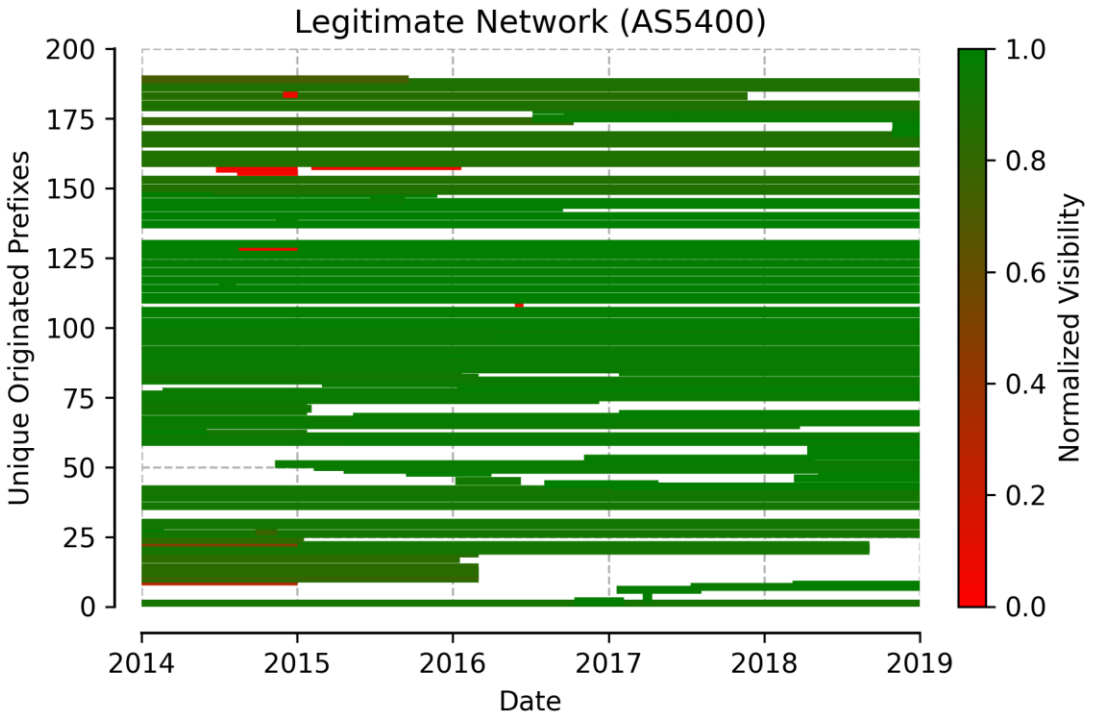


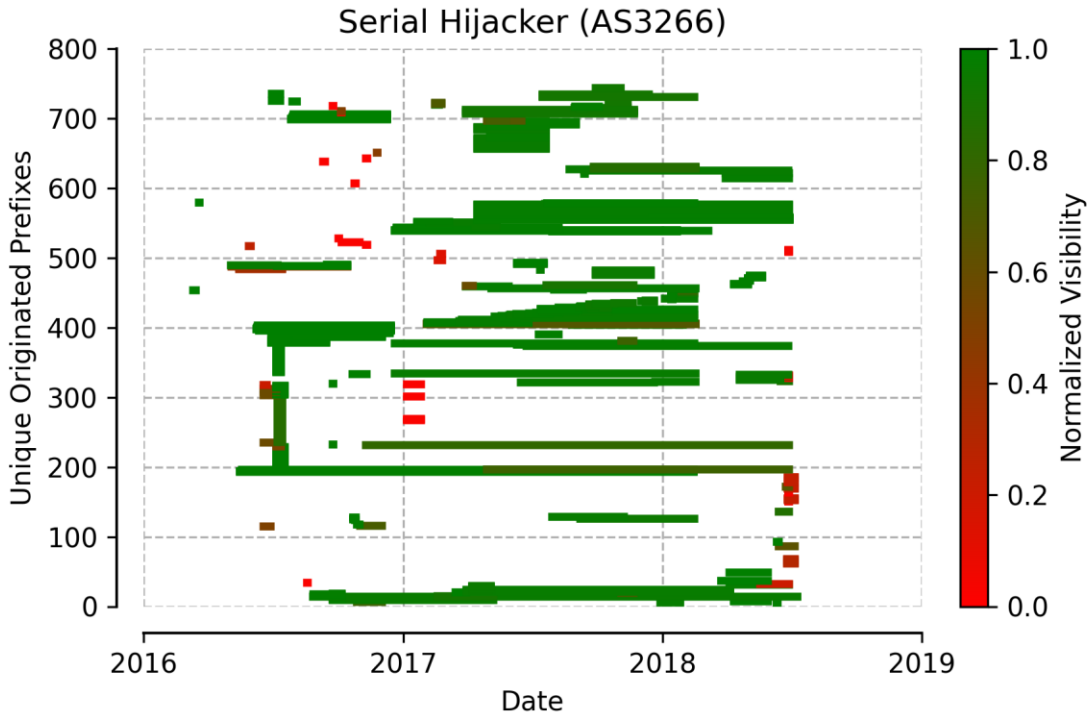
Doorlopende lijn = Prefix bereikbaar 5 jaar lang

Serial BGP Hijackers: A Reproducibility Study and Assessment of Current Dynamics

Ebrima Jaw[†], Moritz Müller[†*], Cristian Hesselman[†*], Lambert Nieuwenhuis[†]
[†]University of Twente, Enschede, The Netherlands
[*]SIDN Labs, Arnhem, The Netherlands

- *Serial hijacker* = AS dat regelmatig en lang routing hijacks veroorzaakt



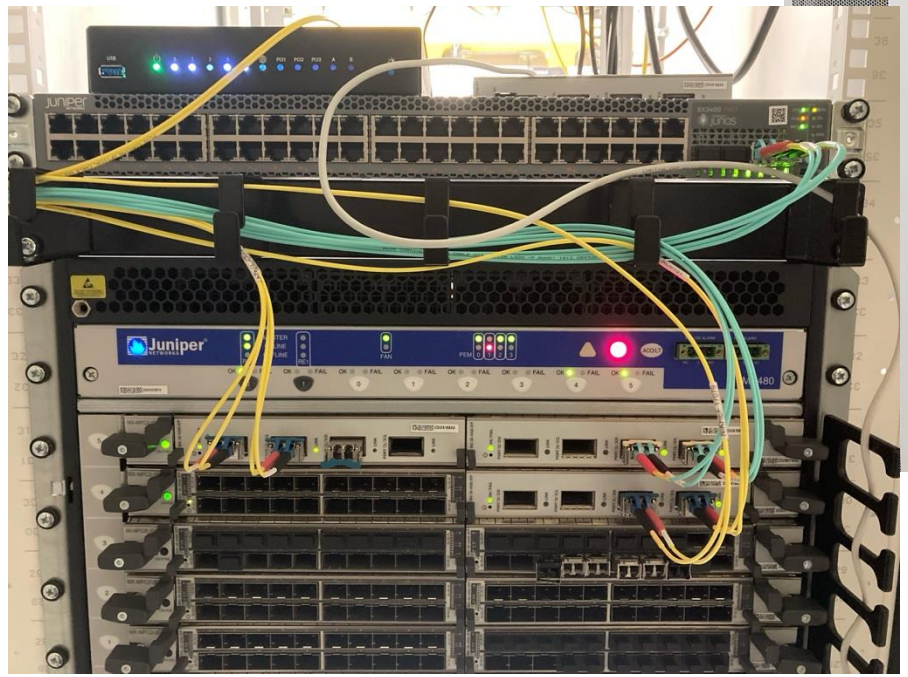


Onze aanpak

1. Onderzoeksfocus bepalen

2. Samenwerken

3. Zelf draaien



Doelen voor 2025

- Meer focus op BGPsec
  - het missende puzzelstukje in routing beveiliging
  - Veel uitdagingen
  - Aanpak: Praktijk ervaring verzamelen

- Weerbaarheid van RPKI
  - De RPKI raakt meer een meer gefragmenteerd
  - Tegelijkertijd stoppen we meer en meer in de RPKI
  - Aanpak: Metingen van de RPKI infrastructuur

Vragen, feedback
en verdere discussie