Next steps in routing security

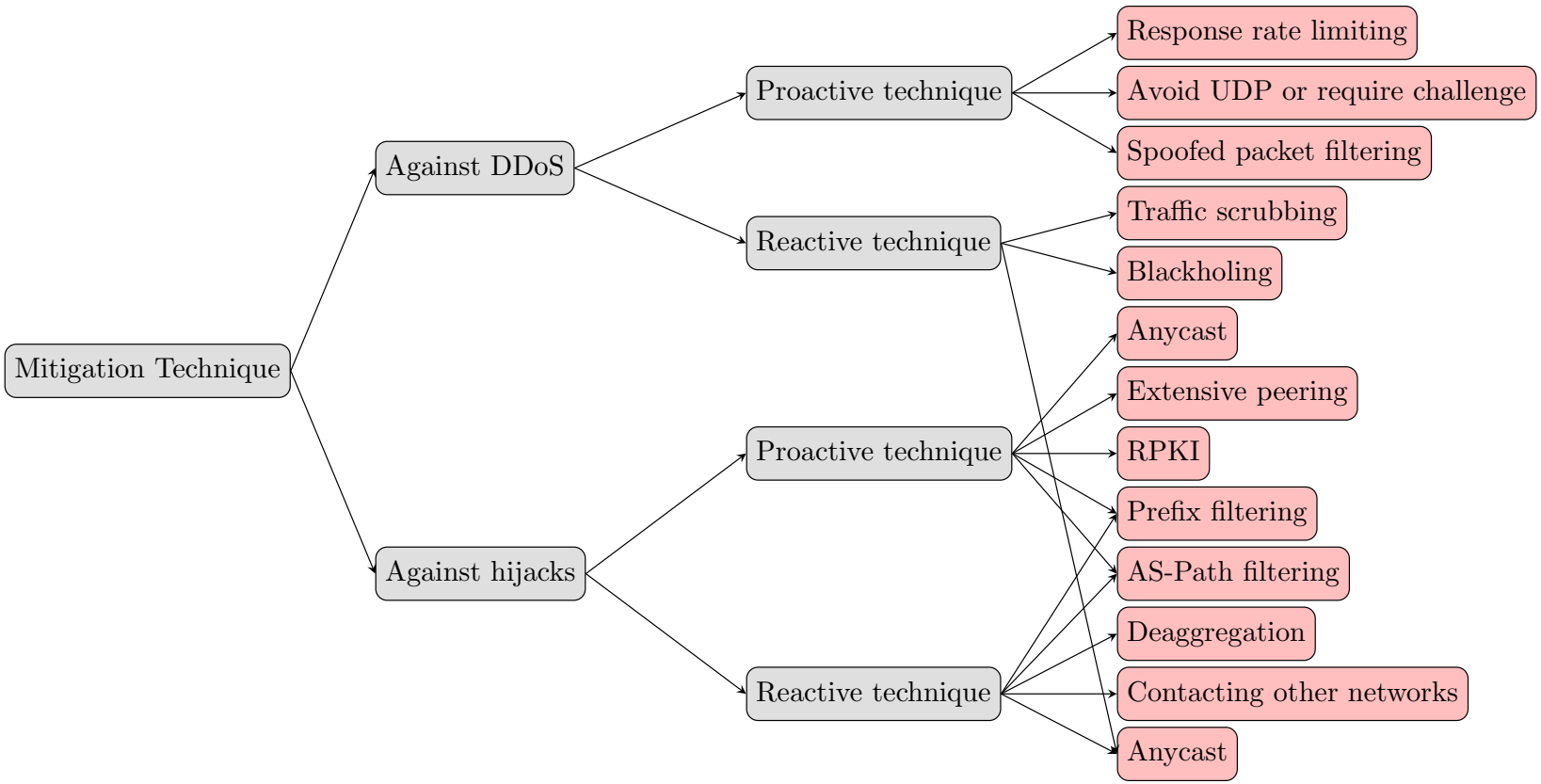
Cristel Pelsser

April, 2018

Network Research Group
ICube / University of Strasbourg

- **Secure mitigation**
- Data-plane path verification

Categorization of existing protection and mitigation solutions

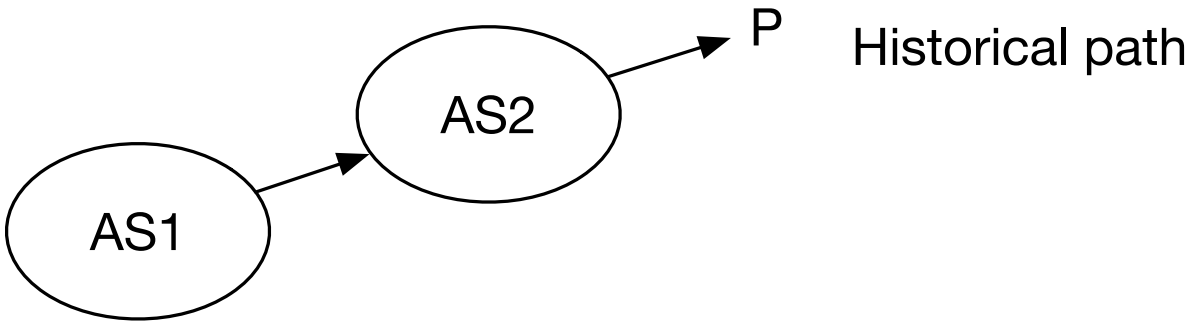


Signaling mitigation to other operators

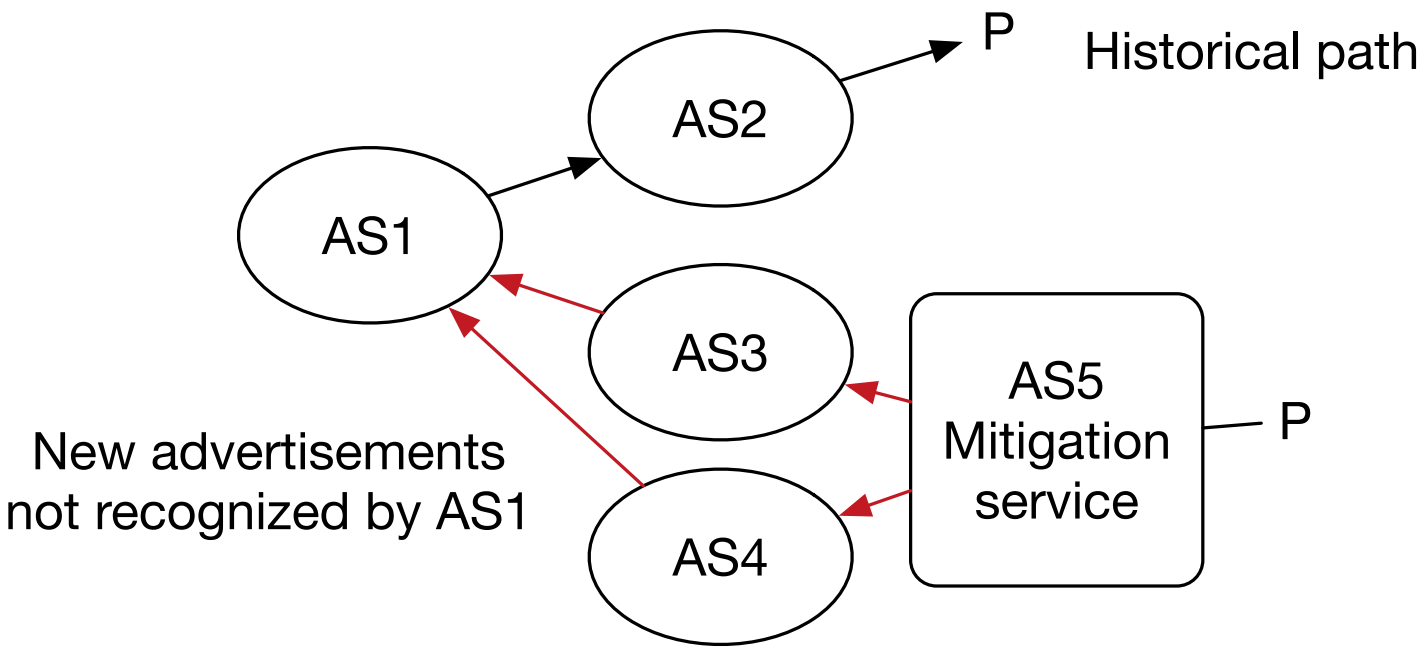
Needs to be attributed **even if done in BGP**.
(authentication and integrity)

Blackholing involves advertising a community in BGP.
How does the recipient trust that the community is not advertised maliciously?

Reactive prefix advertising



Reactive prefix advertising



Anycasting and advertising from additional peers break protection solutions relying on history.
(prefix filtering, AS-path filtering, primary path, . . .)
$\rightarrow$ The mitigation ressembles an attack.

Mitigation using BGP has the same weaknesses as BGP

Attributes can be added, modified

- **Communities**, AS-paths, Origins, ...

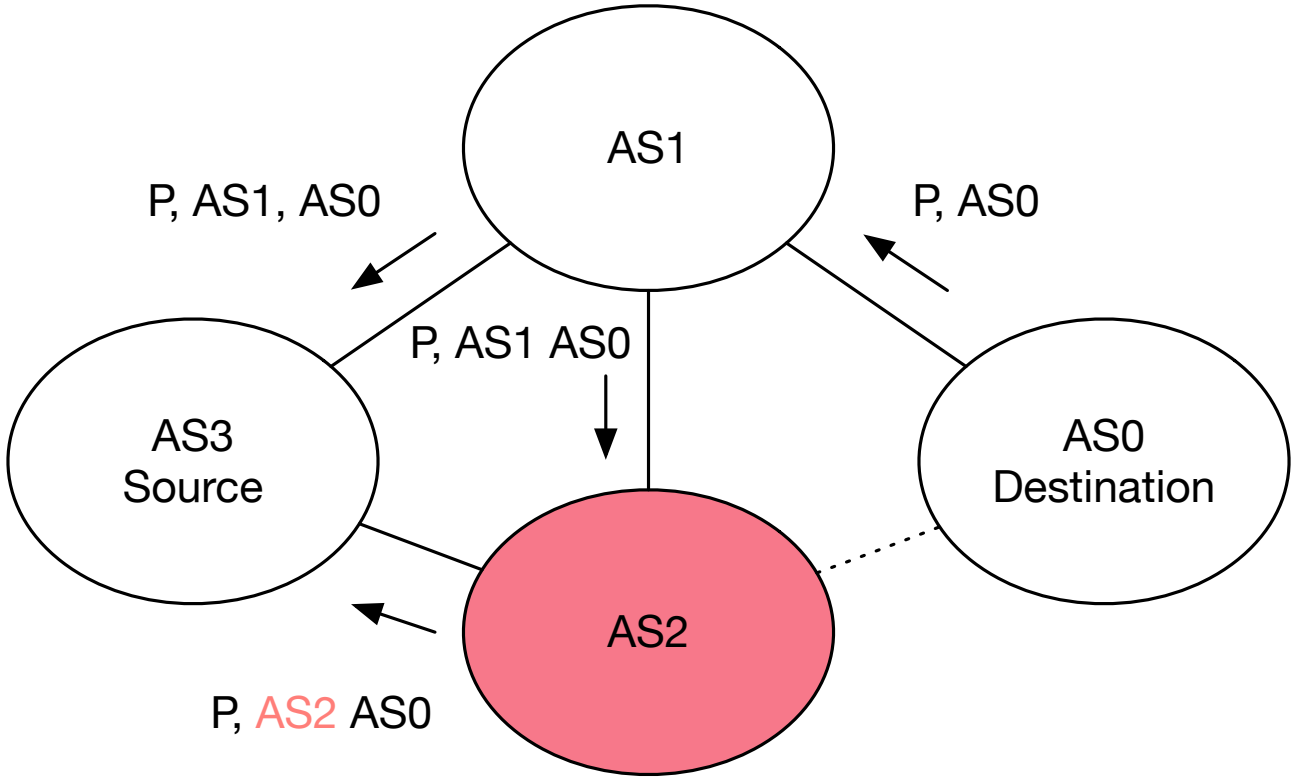
The solution for Route Origin Validation exists.

BGPsec enables to protect the AS-path.

$\rightarrow$ also applicable to mitigation.

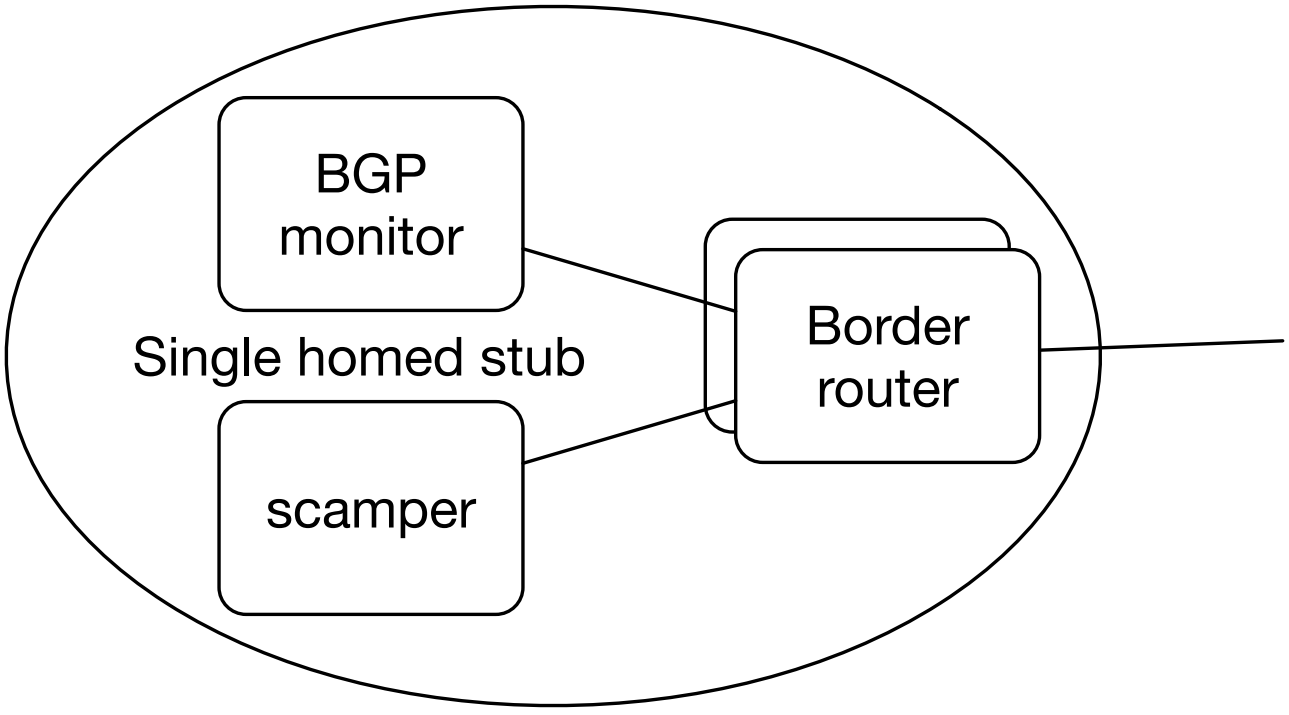
- Secure mitigation
- **Data-plane path verification**

Can we detect AS-path cheating in BGP? (Without waiting for BGPsec)



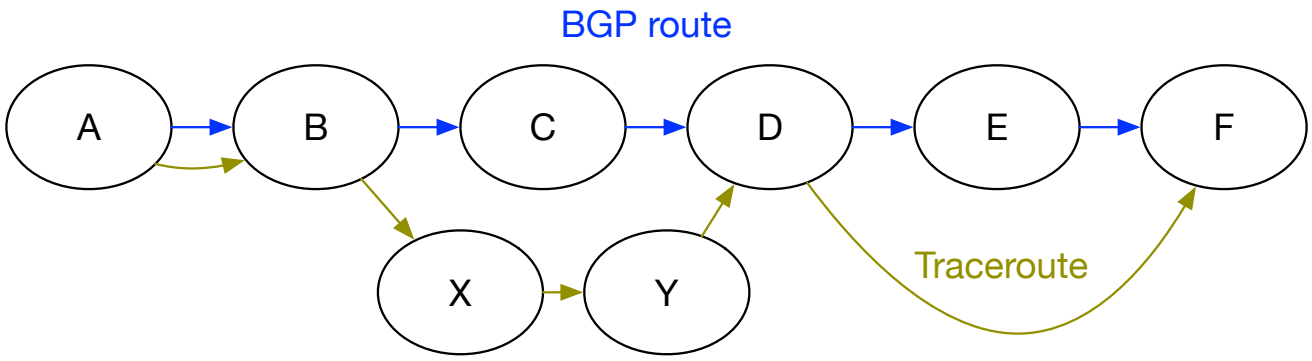
1. AS2 pretends he is directly connected to AS0.
2. AS3 chooses this path while it may have preferred the direct path from AS1 if AS2 had not cheated.

Experiment



Compare AS-path of BGP route to AS-level path obtained with traceroute

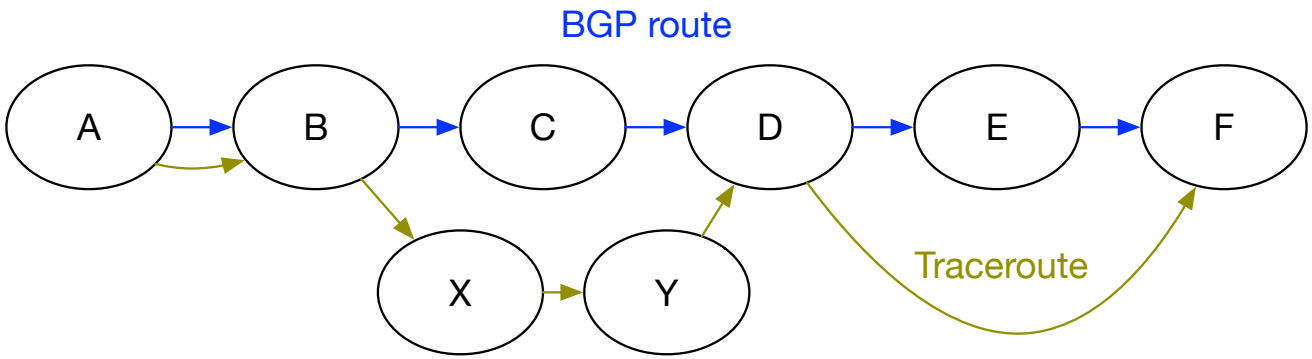
One observation



AS C in BGP is replaced by XY in the traceroute.

AS E is missing from the traceroute.

Who is cheating?



AS B advertises a route it does not use to our BGP monitor?

Is it cheating or some unpredicted interactions between routing protocols?

Take away questions

How to secure mitigation techniques?

How to attribute mismatches between BGP and traceroute AS-level paths?

Thank you

The team

- Julián Del Fiore
- Loïc Miller
- Cristel Pelsser
- Pascal Mérindol
- Jean-Jacques Pansiot
- Stéphane Cateloin