Progress Yet to Be Fulfilled: Measuring Collateral Damage in RPKI ROV

Weitong Li, Yuze Li, and Tijay Chung

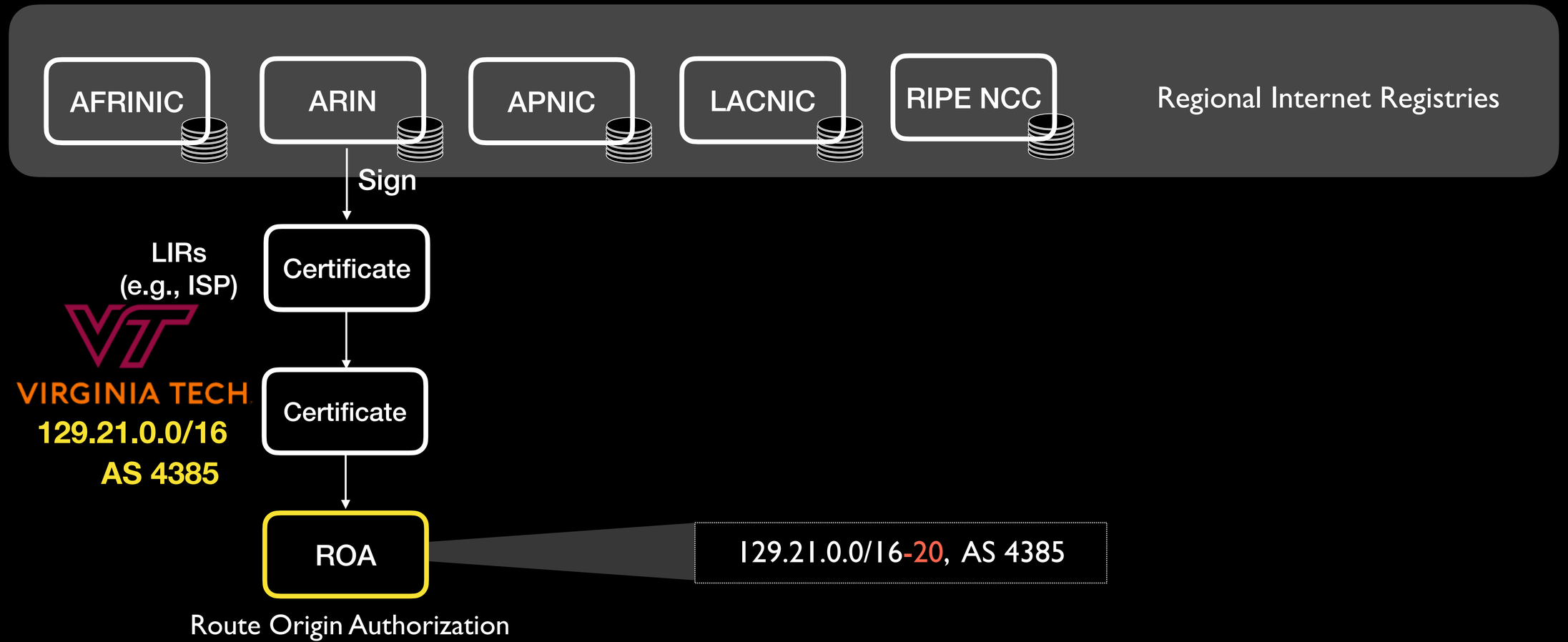
Virginia Tech

VIRGINIA TECH

BGP and RPKI

- Resource Public Key Infrastructure (RPKI) framework designed to secure Internet's routing structure; specifically BGP (developed starting in 2008)
- Currently more than 50% of IP spaces are verifiable with RPKI

RPKI Structure: ROA



VIRGINIA TECH

RPKI Structure: ROV

ROV Router

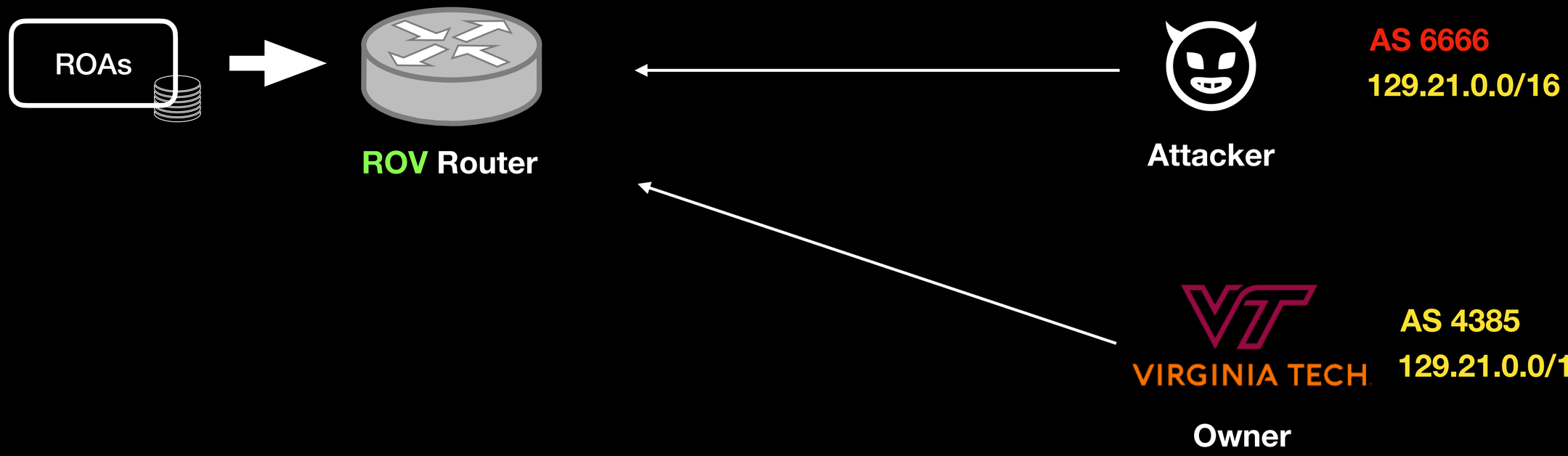
Attacker

AS 6666
129.21.0.0/16

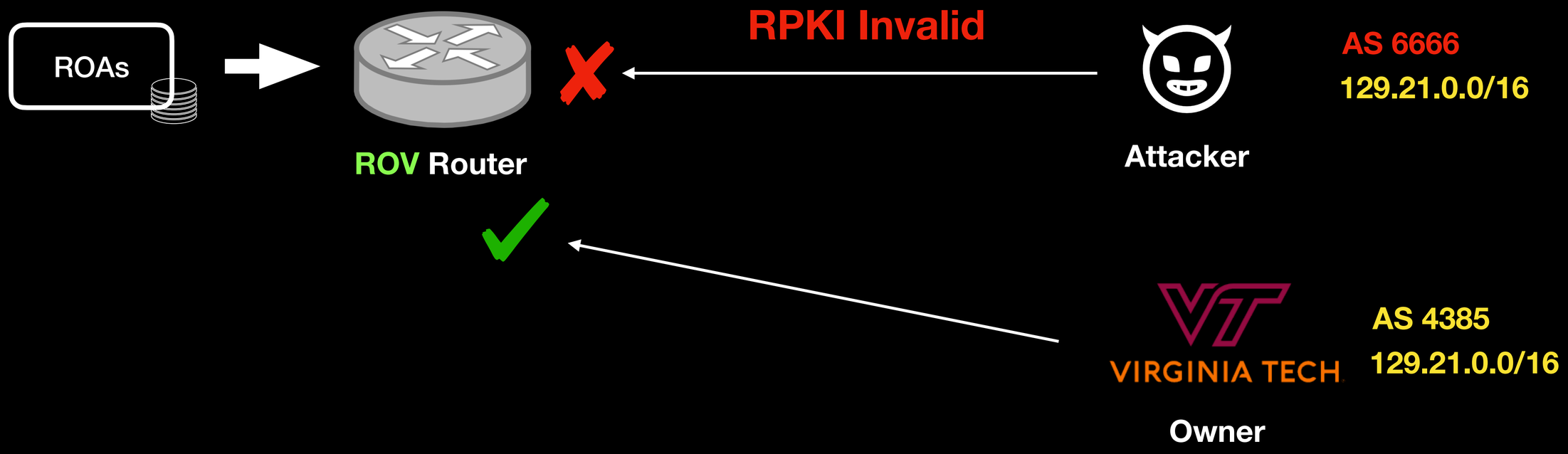
Owner

AS 4385
129.21.0.0/16

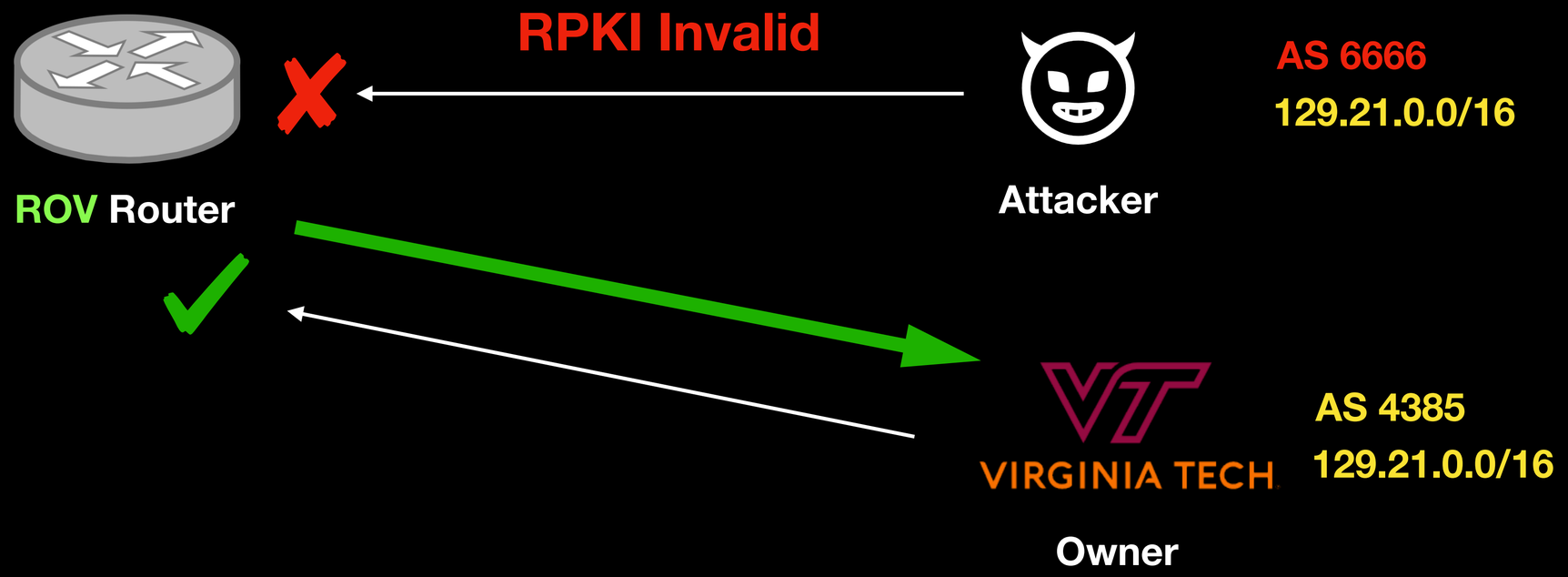
RPKI Structure: ROV



RPKI Structure: ROV

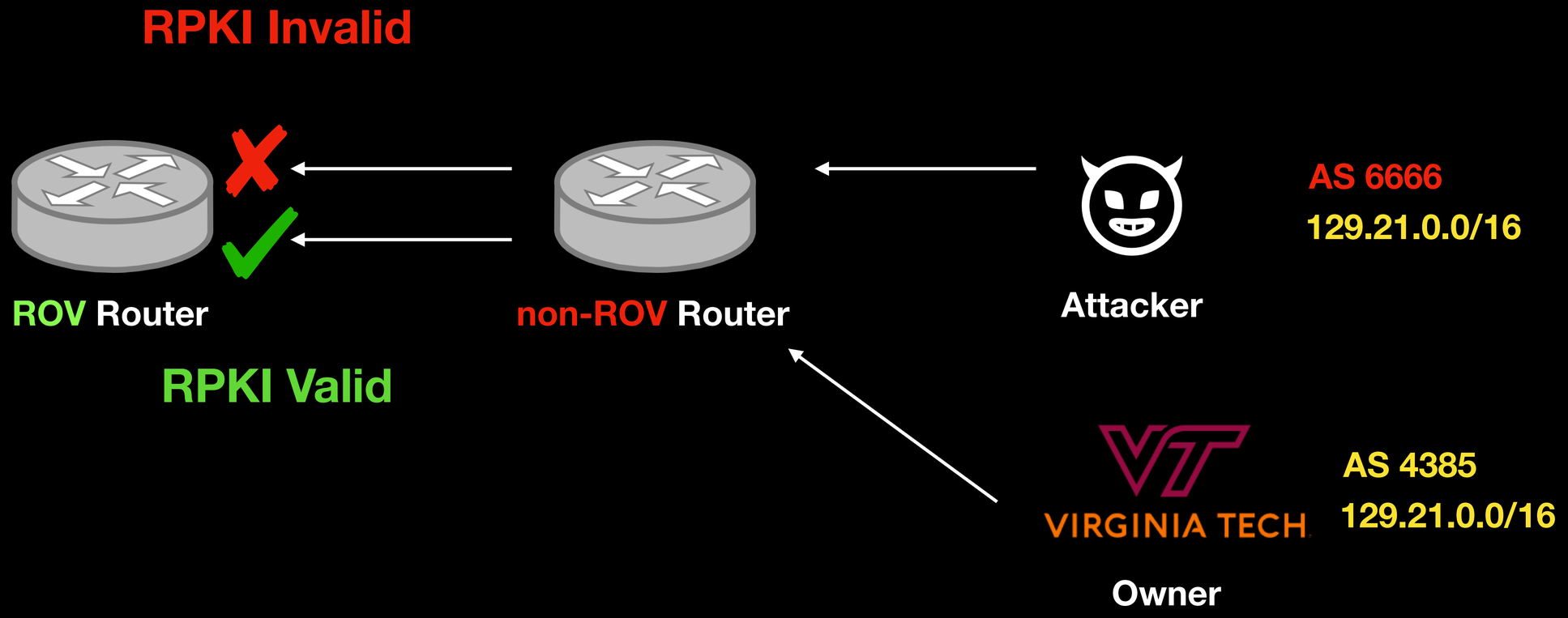


RPKI Structure: ROV

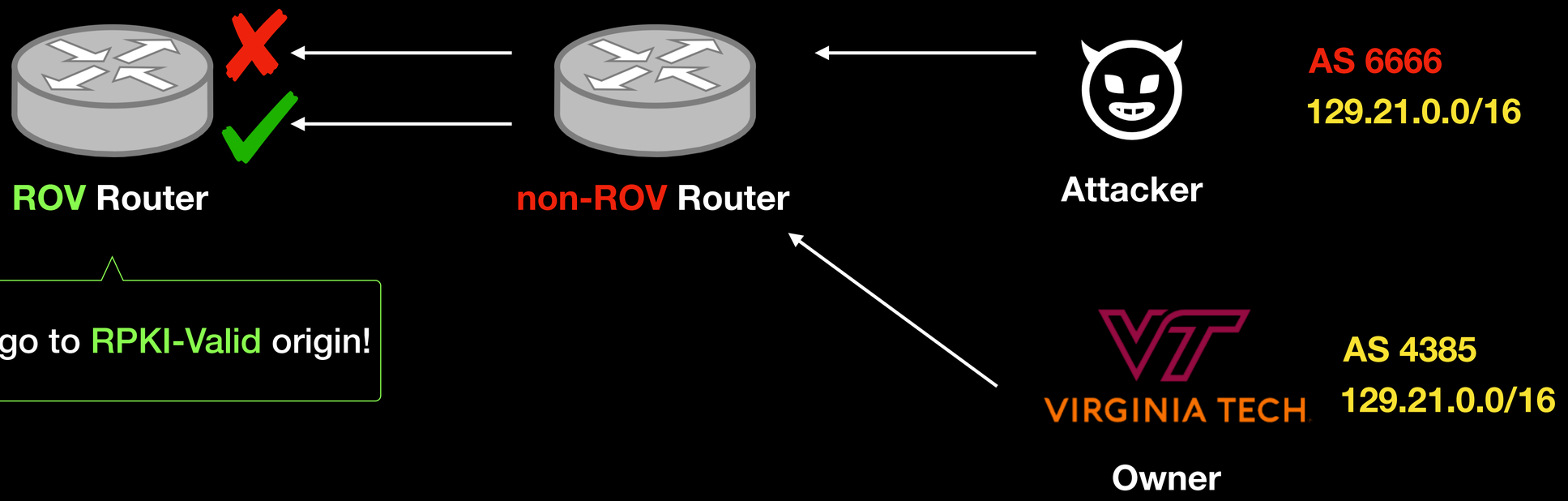


But ROV is still partially-deployed

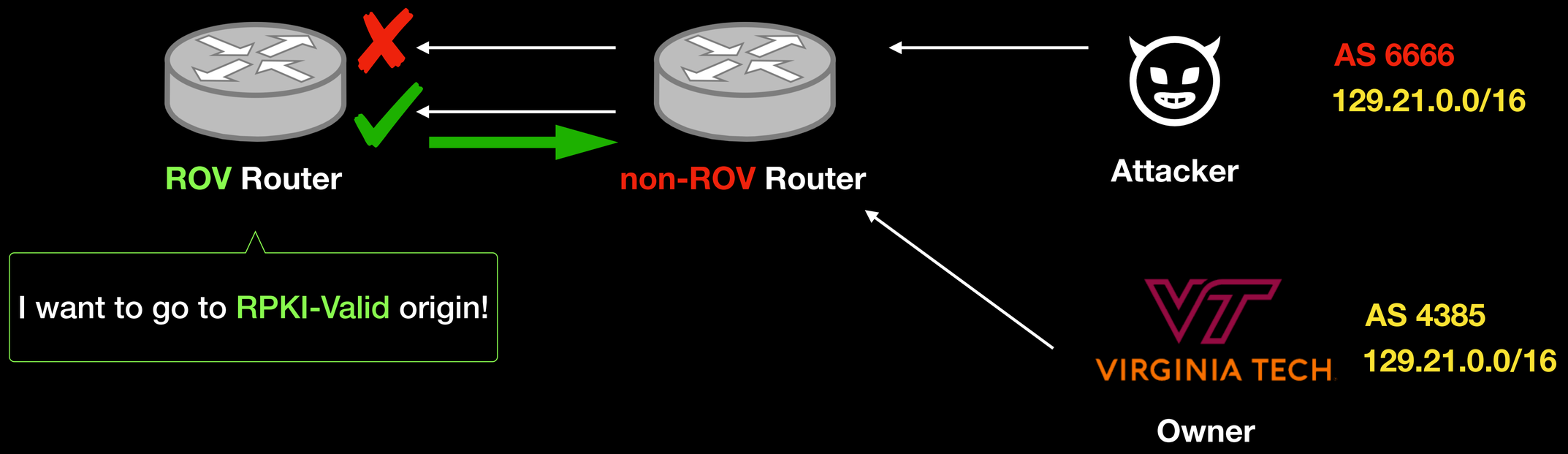
ROV can prevent hijack, but …



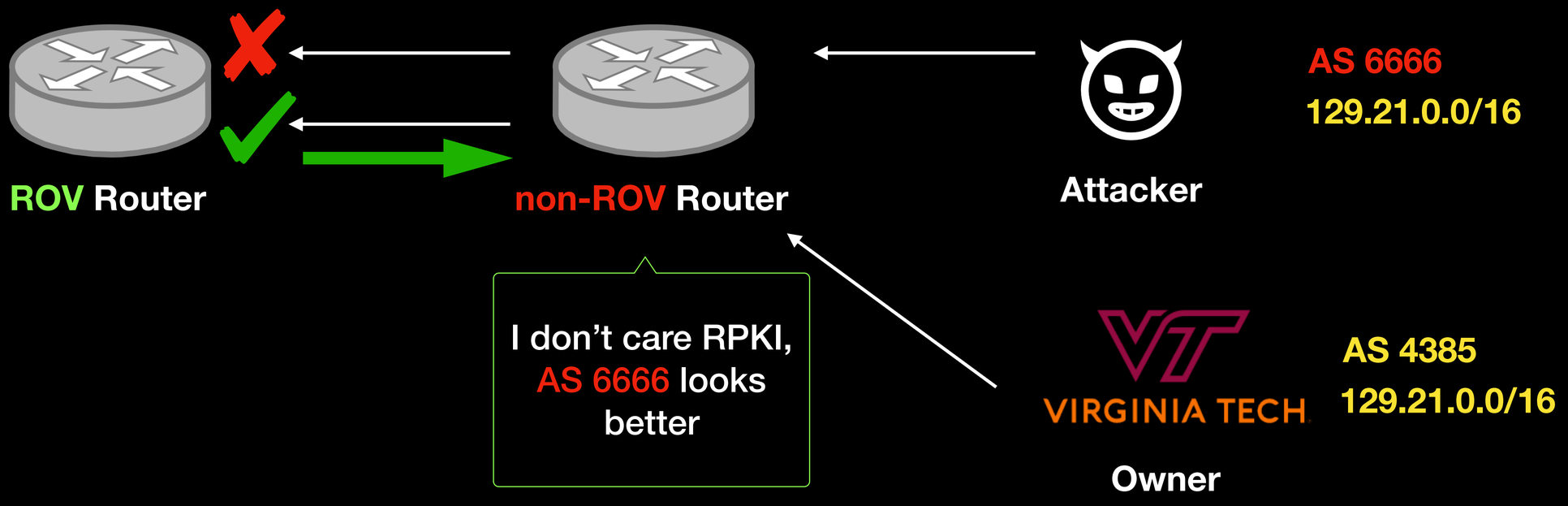
ROV can prevent hijack, but …



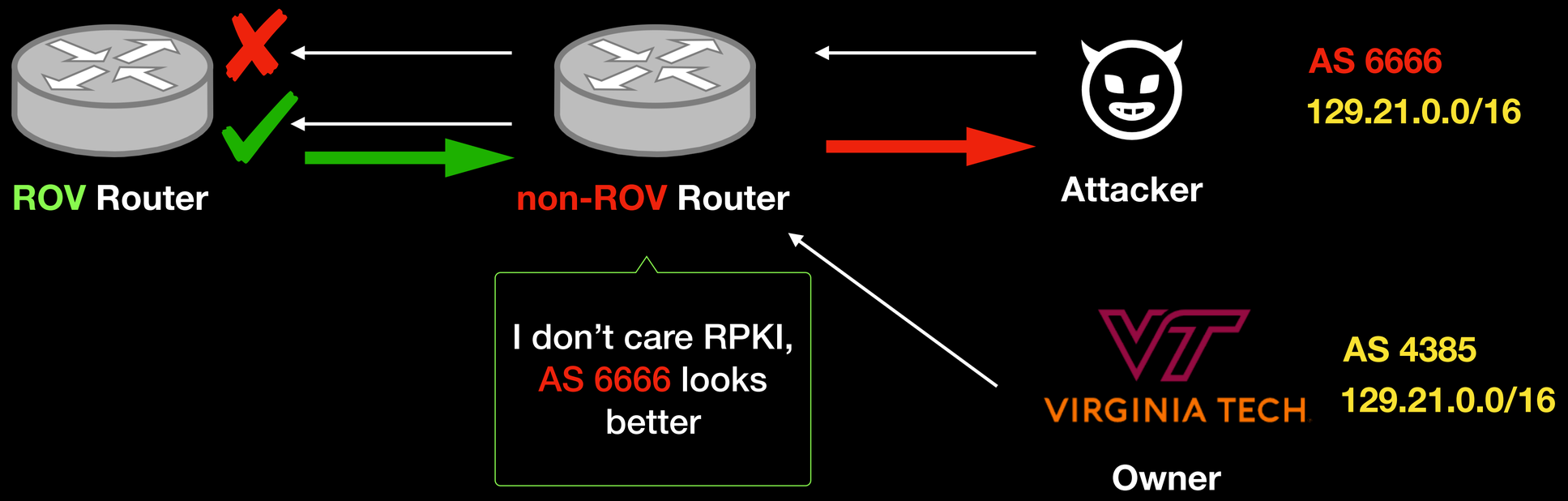
ROV can prevent hijack, but …



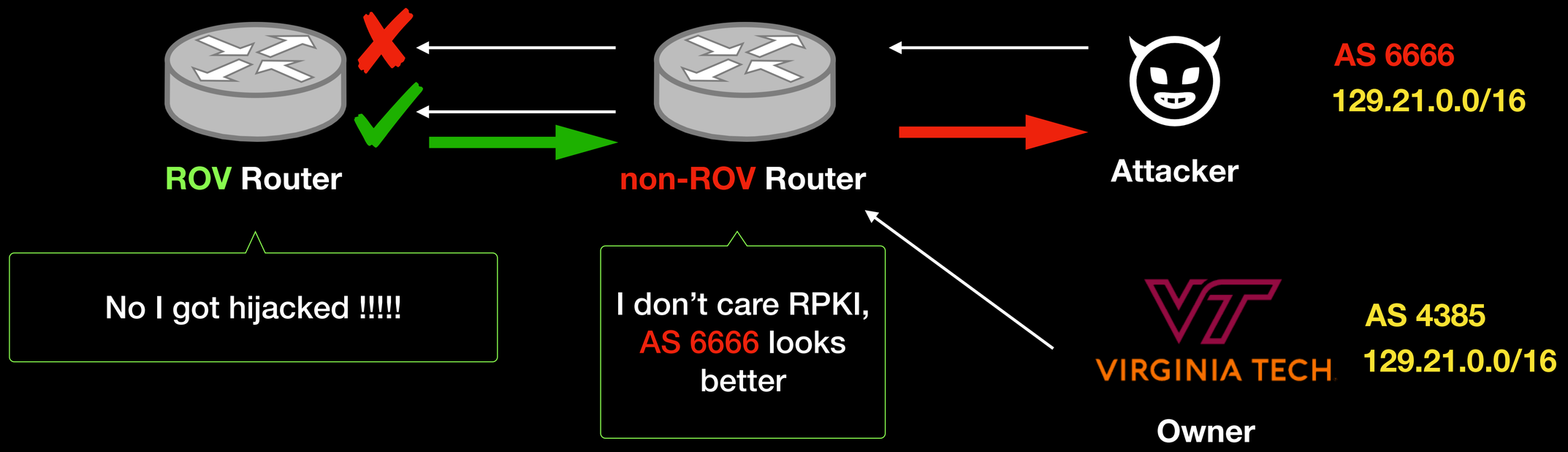
ROV can prevent hijack, but …



ROV can prevent hijack, but …



ROV can prevent hijack, but …



The Collateral Damage in ROV

- A ROV-enabled network can still be hijacked with RPKI-invalid announcements if any hops in-the-path are non-ROV

The Collateral Damage in ROV

- A ROV-enabled network can still be hijacked with RPKI-invalid announcements if any hops in-the-path are non-ROV
- ROV is still far from fully deployment, so collateral damage will be a long existing challenge.

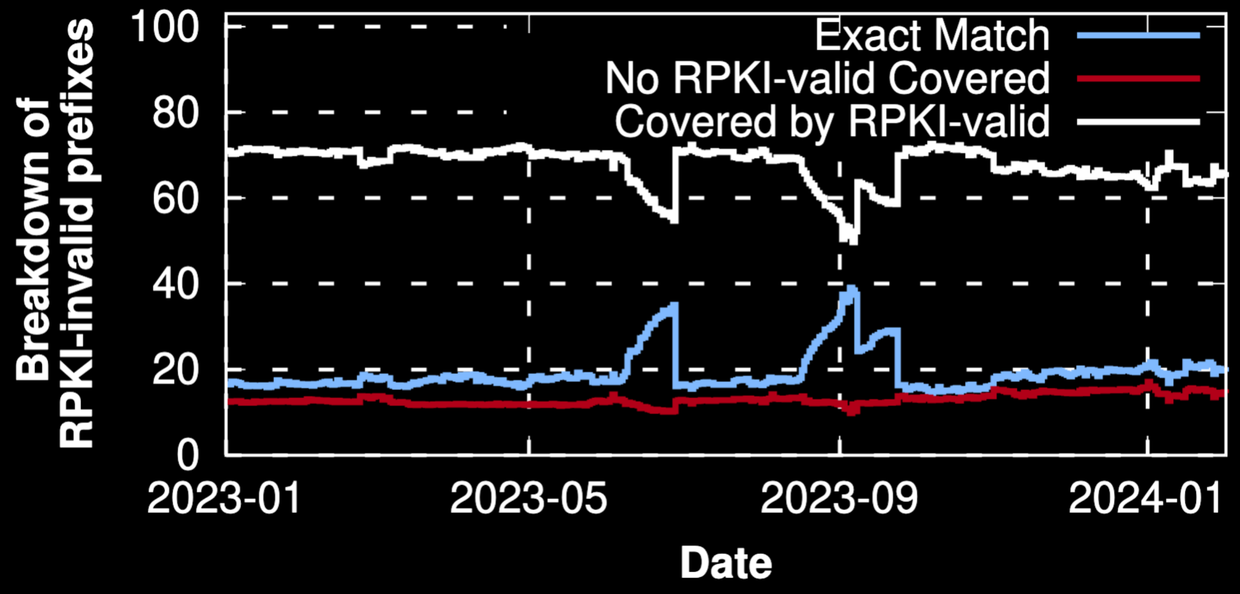
Measuring Collateral Damage

RPKI-invalid Prefixes

- To make collateral damage happens, there need to be both RPKI-valid and invalid prefixes

RPKI-invalid Prefixes

- To make collateral damage happens, there need to be both RPKI-valid and invalid prefixes
- But: 85.6% of RPKI-invalid prefixes have accompanied RPKI-valid prefixes



VIRGINIA TECH

Controlled experiment

Controlled experiment

Peering Testbed

184.164.240.0/24 AS6574

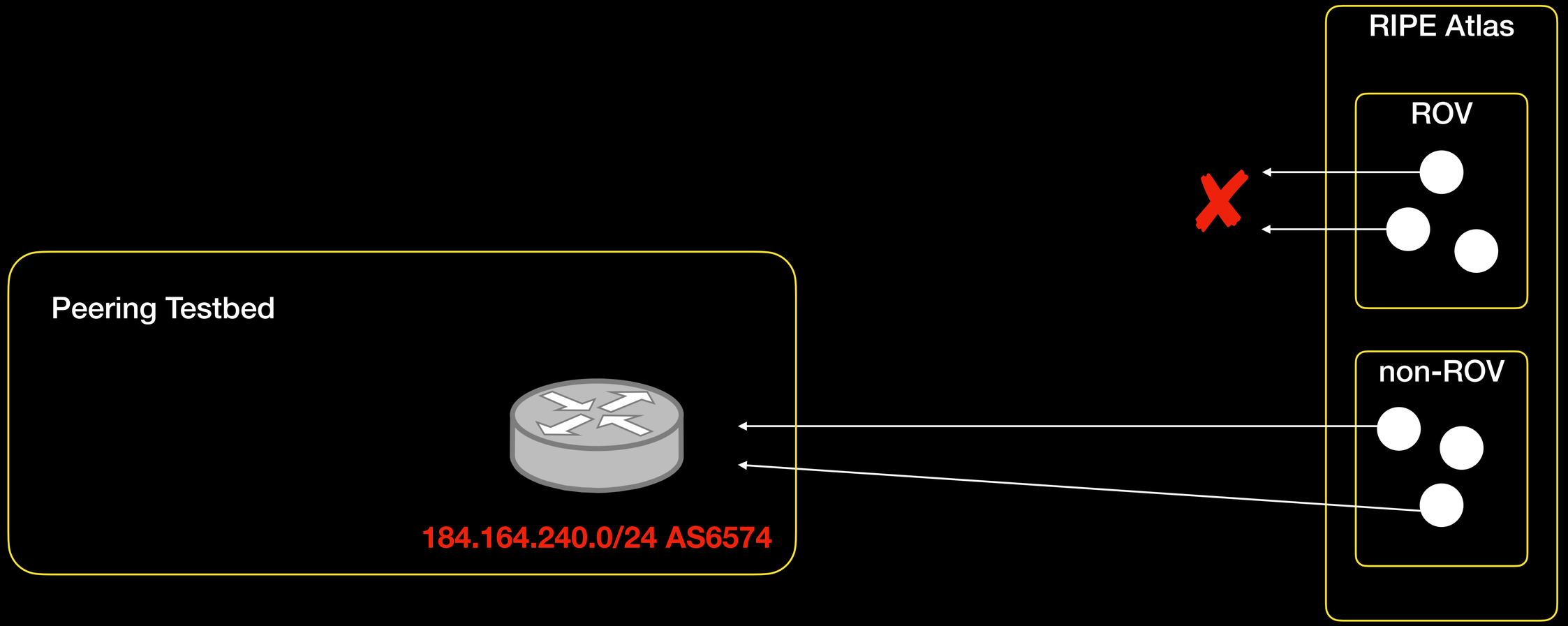
RIPE Atlas

ROV

non-ROV

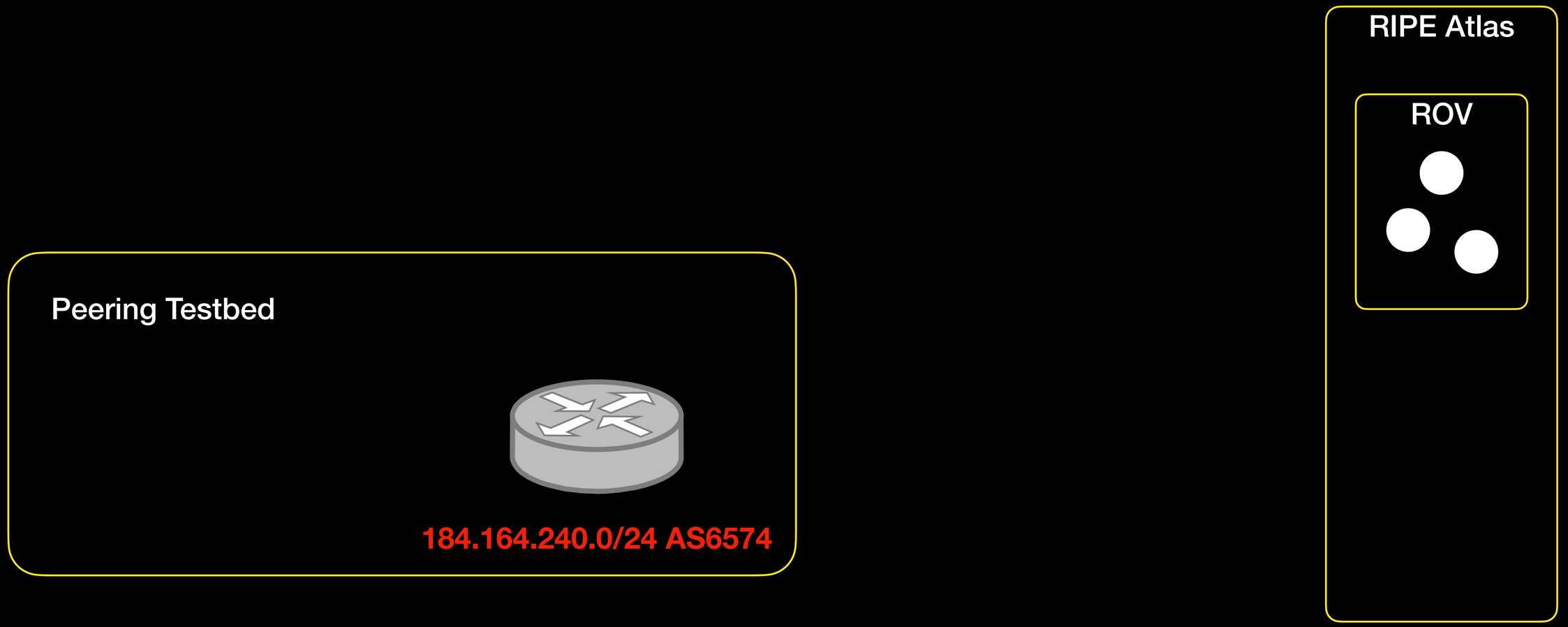
VIRGINIA TECH

Controlled experiment



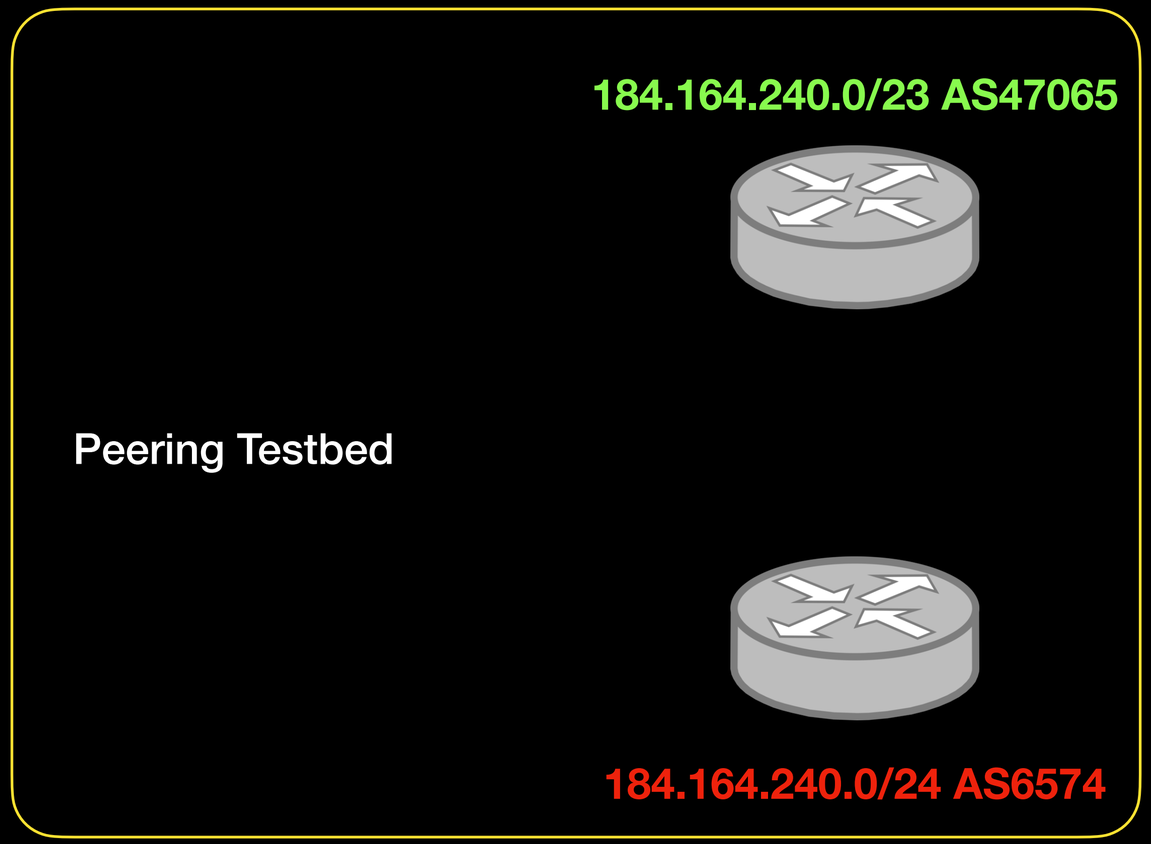
VIRGINIA TECH

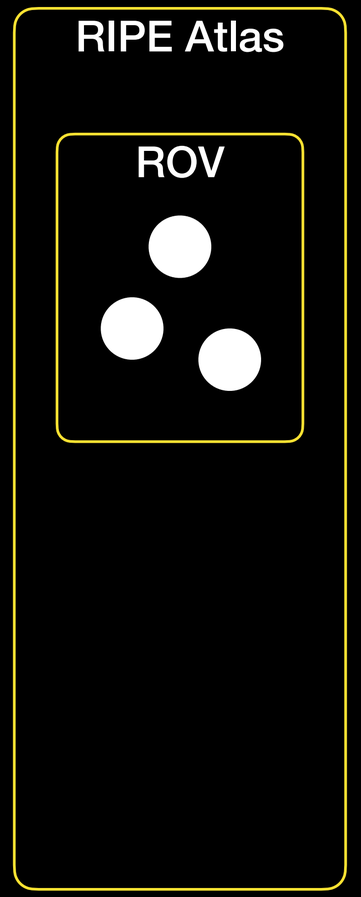
Controlled experiment



VIRGINIA TECH

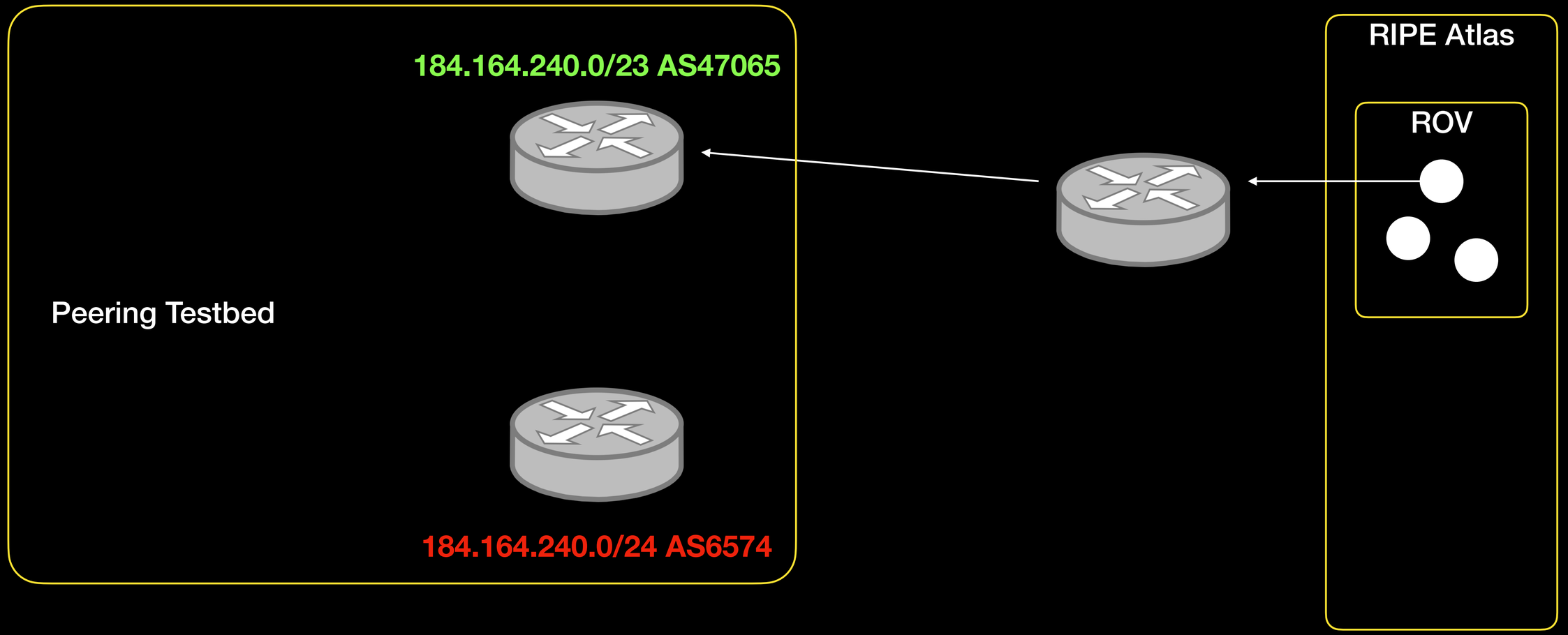
Controlled experiment





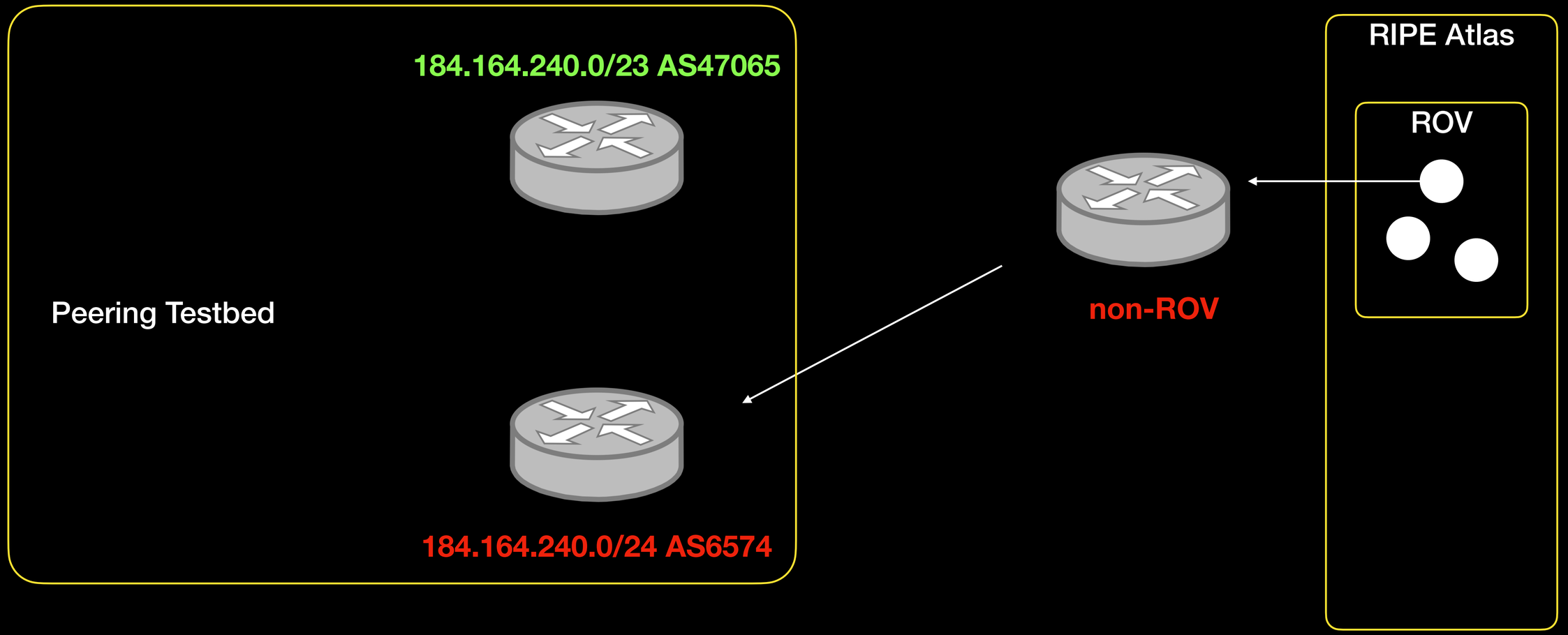
VIRGINIA TECH

No Collateral Damage



VIRGINIA TECH

Collateral Damage



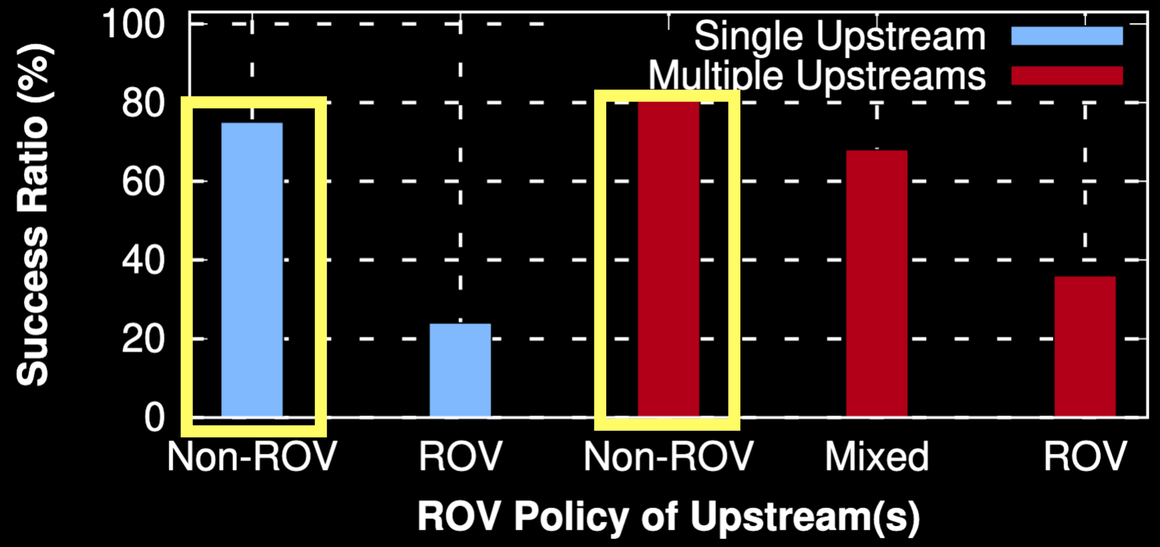
VIRGINIA TECH

Result

- From 3036 ASes that RIPE Atlas covers, 902 ASes are ROV (not able to reach the /24 RPKI-invalid prefix)
- Among 902 ROV ASes, 34%(307) of them are able to reach the invalid prefix after we announce the /23 RPKI-valid prefix.

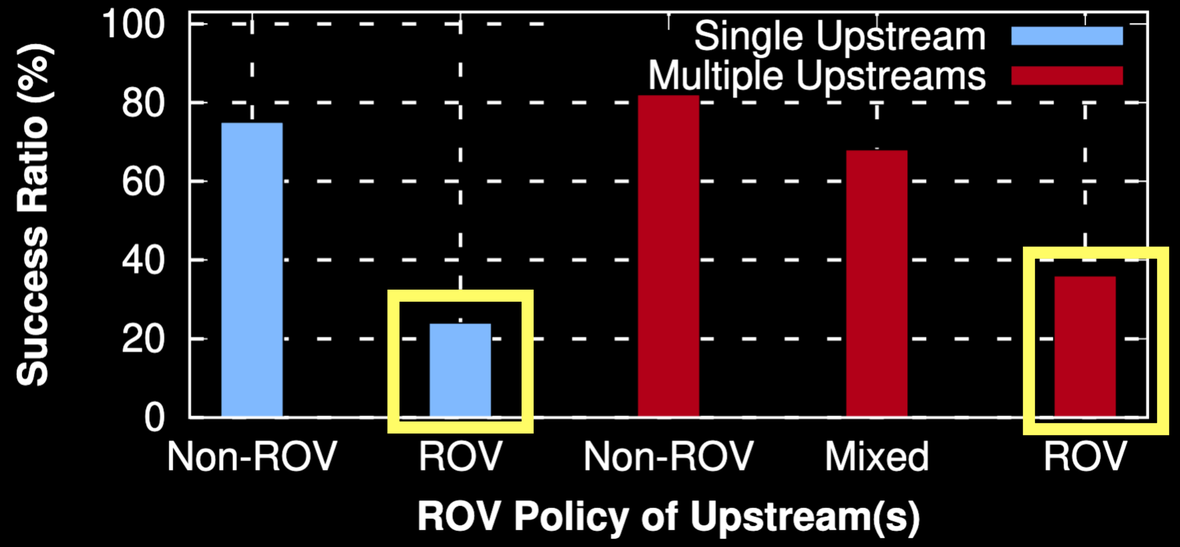
Result

- Collateral damage is highly related to the first hop.



Result

- Collateral damage is highly related to the first hop.



Measuring “in-the-wild” RPKI-invalid

- Collateral damage is highly related to the routing path

Measuring “in-the-wild” RPKI-invalid

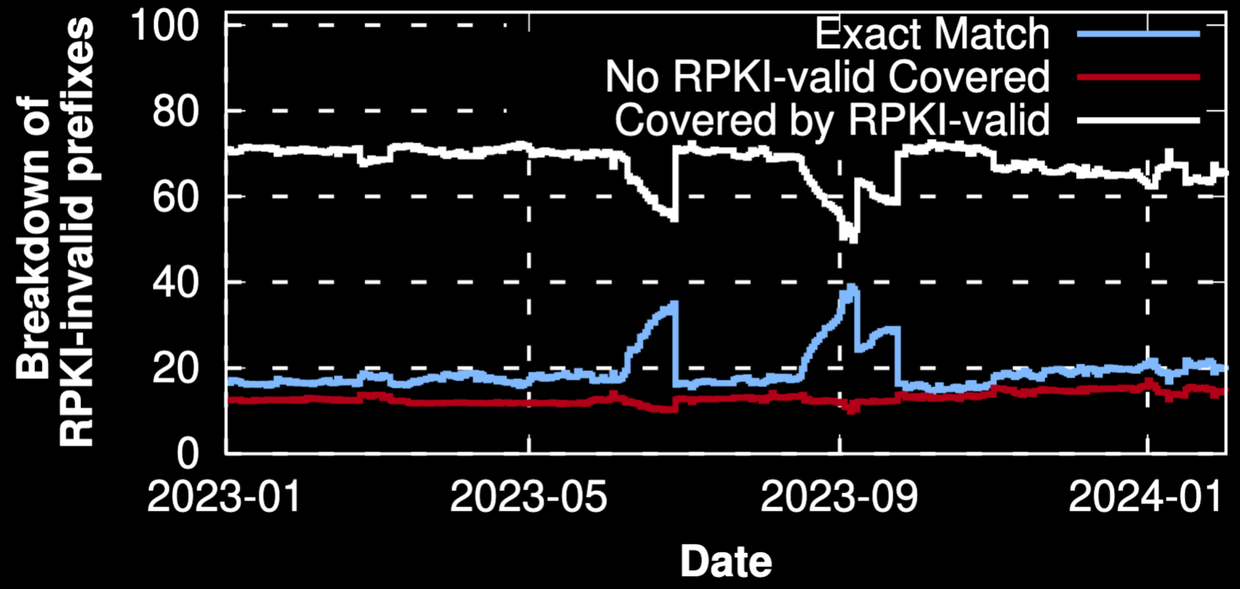
- Collateral damage is highly related to the routing path
- Can we have more RPKI-invalid prefixes to cover more path?

Measuring “in-the-wild” RPKI-invalid

- Collateral damage is highly related to the routing path
- Can we have more RPKI-invalid prefixes to cover more path?
- But we don’t have many prefixes….

Measuring "in-the-wild" RPKI-invalid

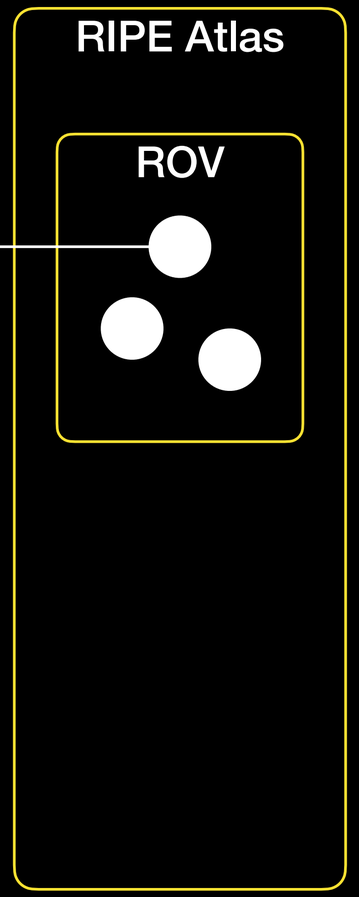
- Wait, there are more than 5,000 RPKI-invalid prefixes we can use!



Measuring “in-the-wild” RPKI-invalid

x.x.x.0/23 RPKI-valid

x.x.x.0/24 RPKI-invalid



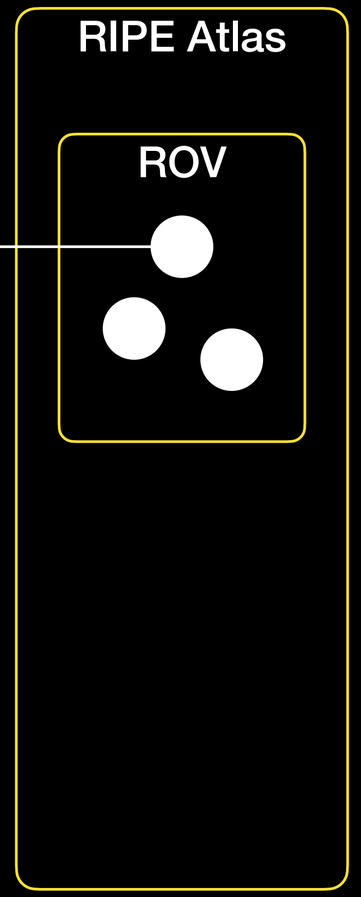
VIRGINIA TECH

Measuring “in-the-wild” RPKI-invalid

x.x.x.0/23 RPKI-valid

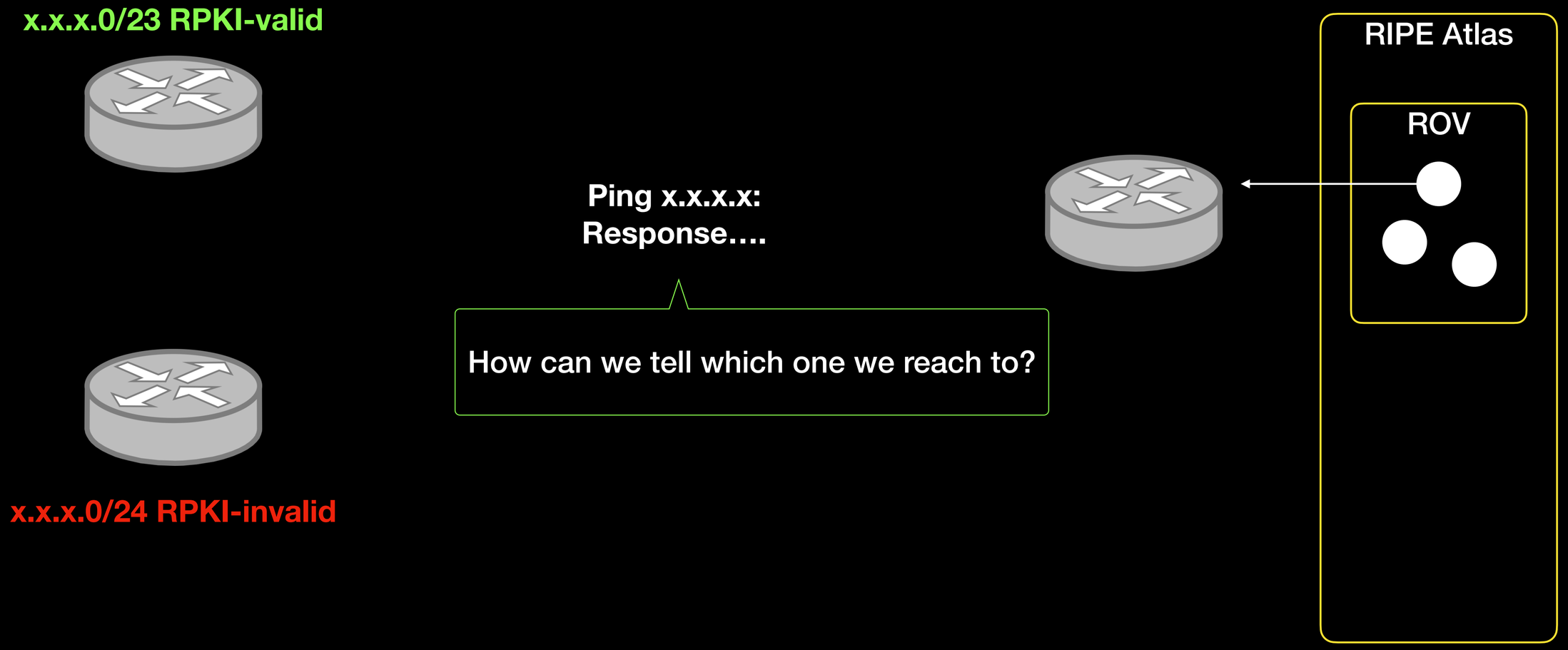
x.x.x.0/24 RPKI-invalid

Ping x.x.x.x:
Response….



VIRGINIA TECH

Measuring “in-the-wild” RPKI-invalid



VIRGINIA TECH

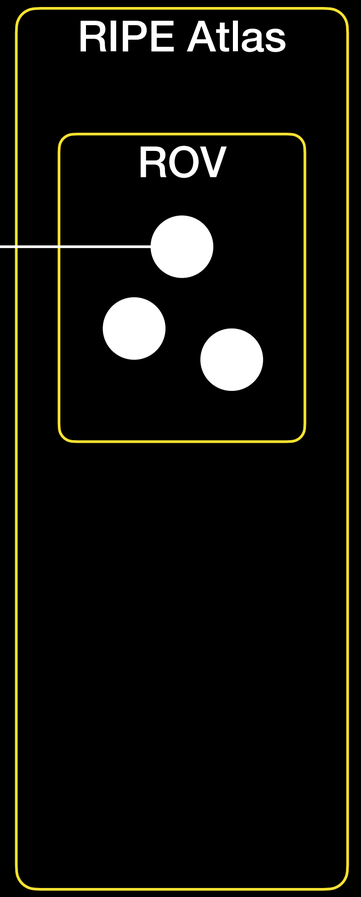
Measuring “in-the-wild” RPKI-invalid

x.x.x.0/23 RPKI-valid

x.x.x.0/23 AS_Path: …., X, Valid Origin

x.x.x.0/24 AS_Path: …., Y, Invalid Origin

x.x.x.0/24 RPKI-invalid



VIRGINIA TECH

Measuring “in-the-wild” RPKI-invalid

Penultimate hop

x.x.x.0/23 RPKI-valid

AS X

x.x.x.0/23 AS_Path: …., X, Valid Origin

AS Y

x.x.x.0/24 RPKI-invalid

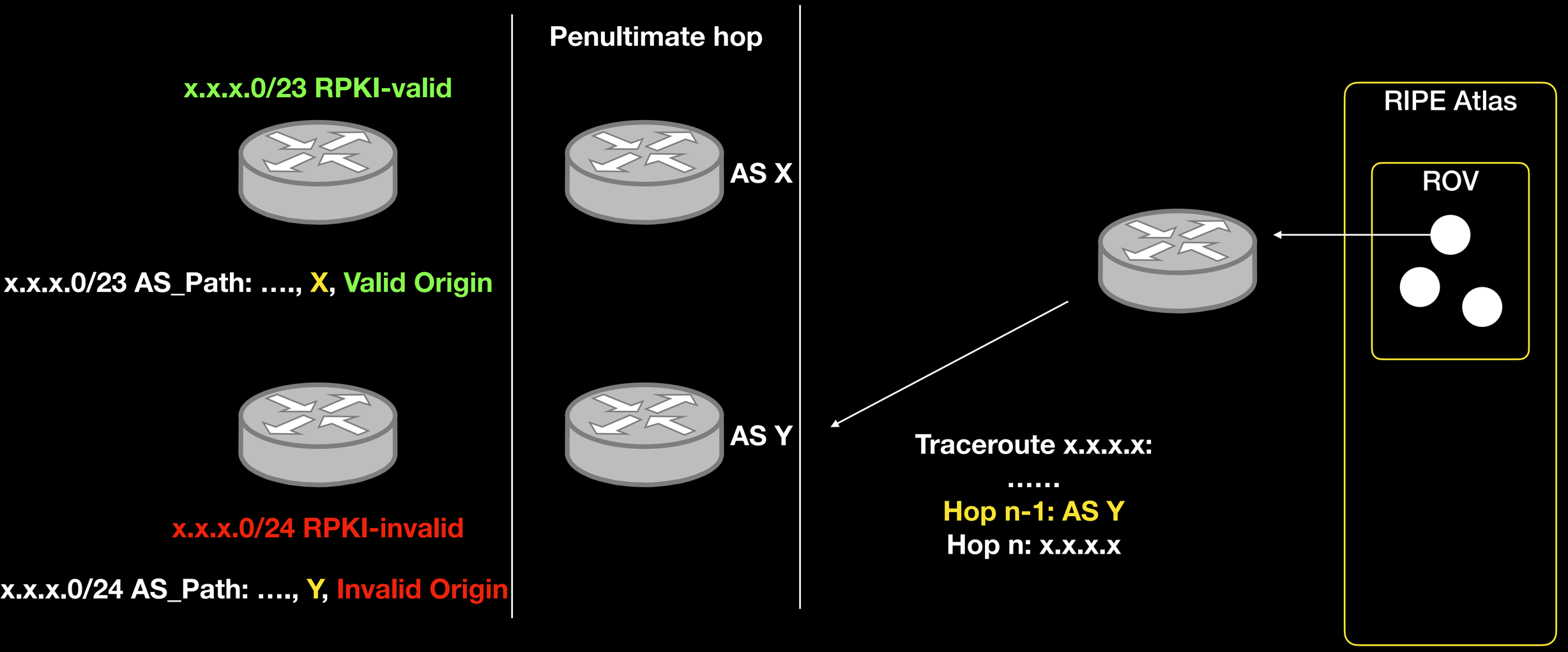
x.x.x.0/24 AS_Path: …., Y, Invalid Origin

RIPE Atlas

ROV

VIRGINIA TECH

Measuring “in-the-wild” RPKI-invalid



VIRGINIA TECH

Results

- Select RPKI-valid / invalid prefixes that have different next-hop in BGP
- Use the same RIPE Atlas nodes from 902 ROV ASes
- We see 63% (568) of them are reaching to at least one RPKI-invalid origin

Results

- Select RPKI-valid / invalid prefixes that have different next-hop in BGP
- Use the same RIPE Atlas nodes from 902 ROV ASes
- We see 63% (568) of them are reaching to at least one RPKI-invalid origin

Conclusion

- Most RPKI-invalid prefixes have accompanied RPKI-valid prefixes
- Collateral damage is weakening the protection of ROV for more than 63% ASes

Mitigation

Mitigation

Upstreams

ROV Router

non-ROV Router

ROV Router

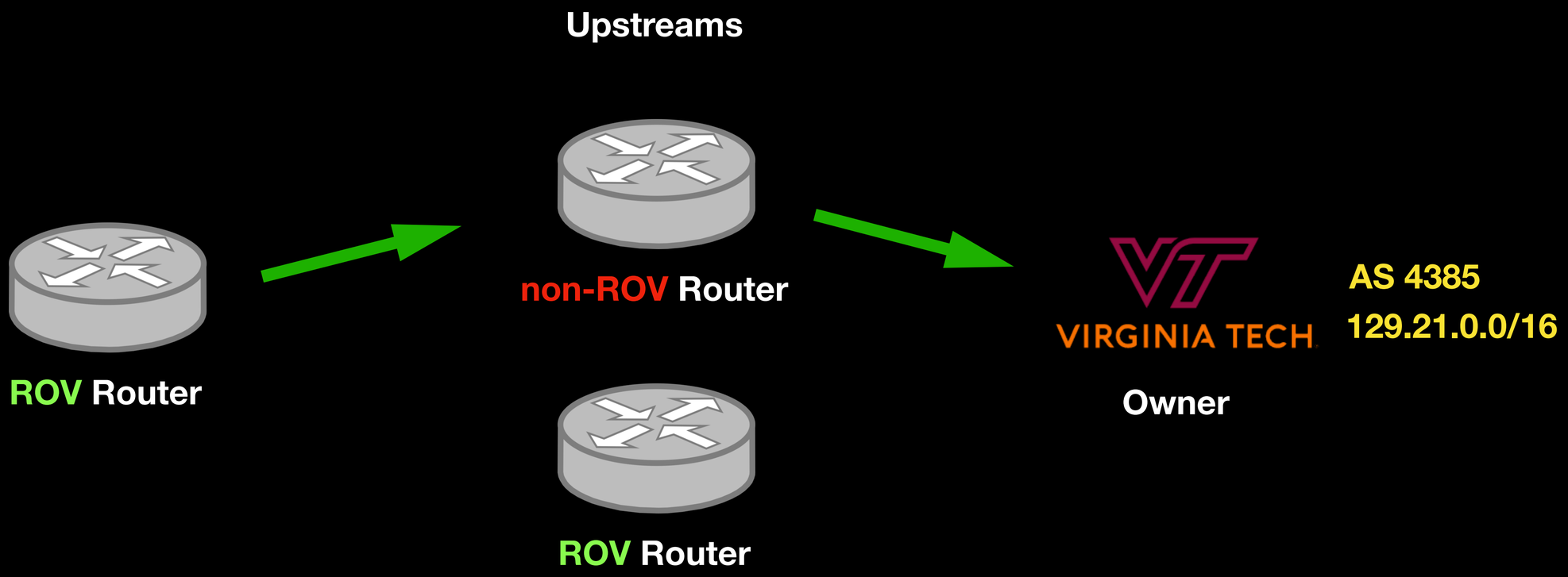
VIRGINIA TECH

Owner

AS 4385

129.21.0.0/16

Mitigation


Upstreams
non-ROV Router
ROV Router
ROV Router
VIRGINIA TECH
Owner
AS 4385
129.21.0.0/16

Mitigation

ROV Router

non-ROV Router

Attacker

AS 6666
129.21.0.0/16

ROV Router

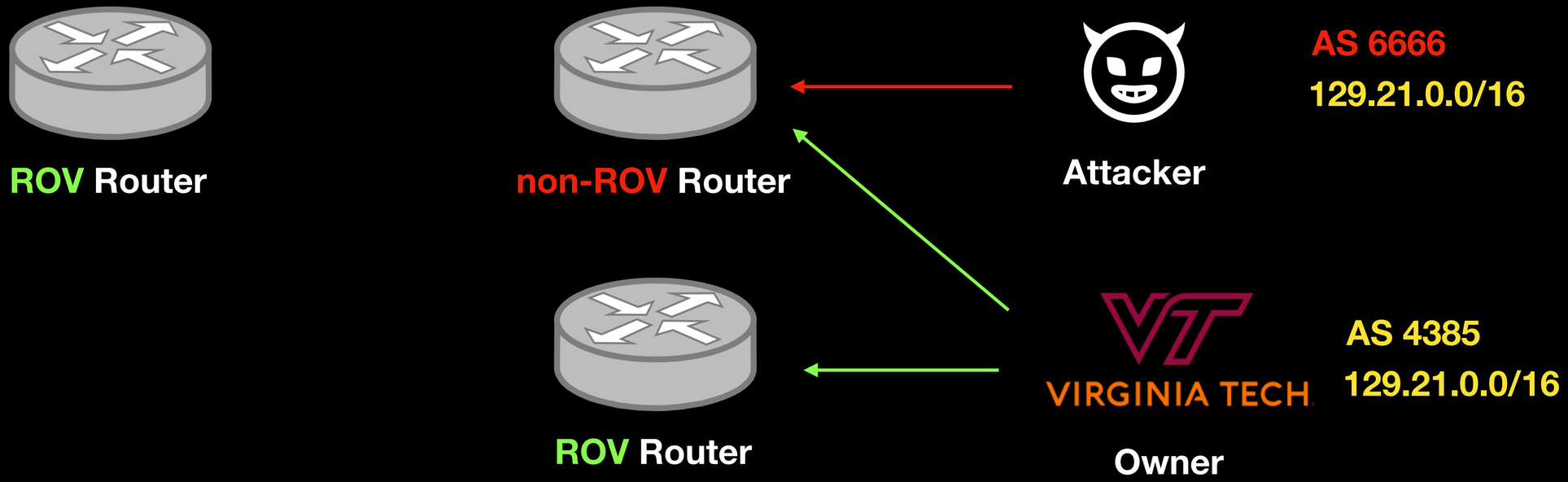
VIRGINIA TECH

Owner

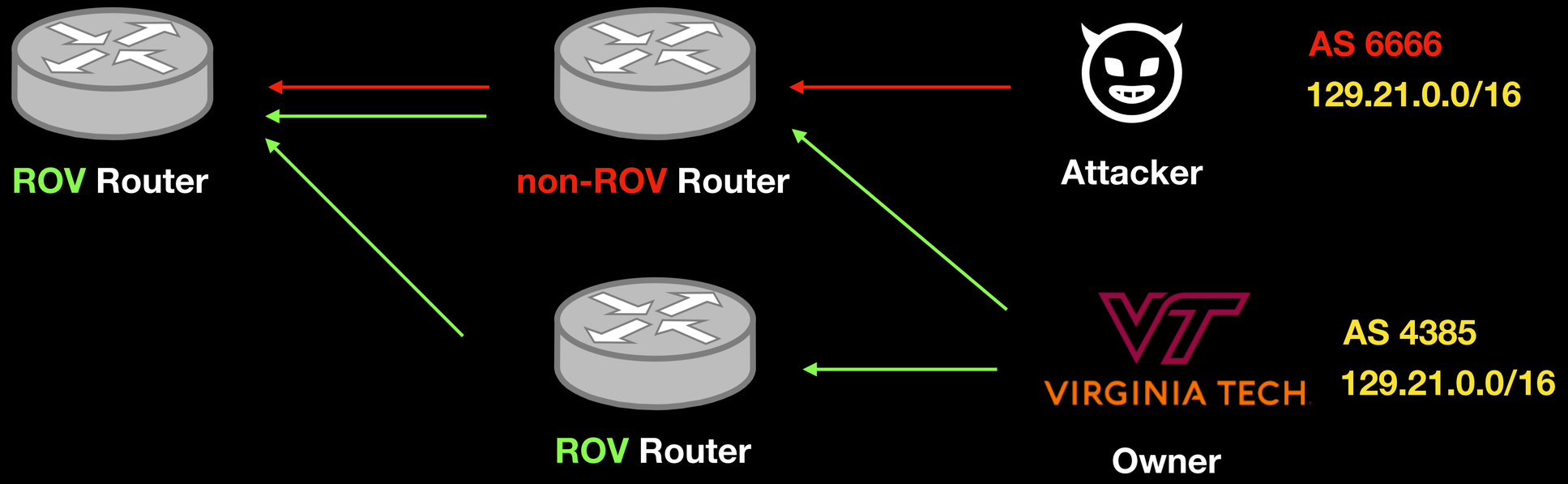
AS 4385
129.21.0.0/16

VIRGINIA TECH

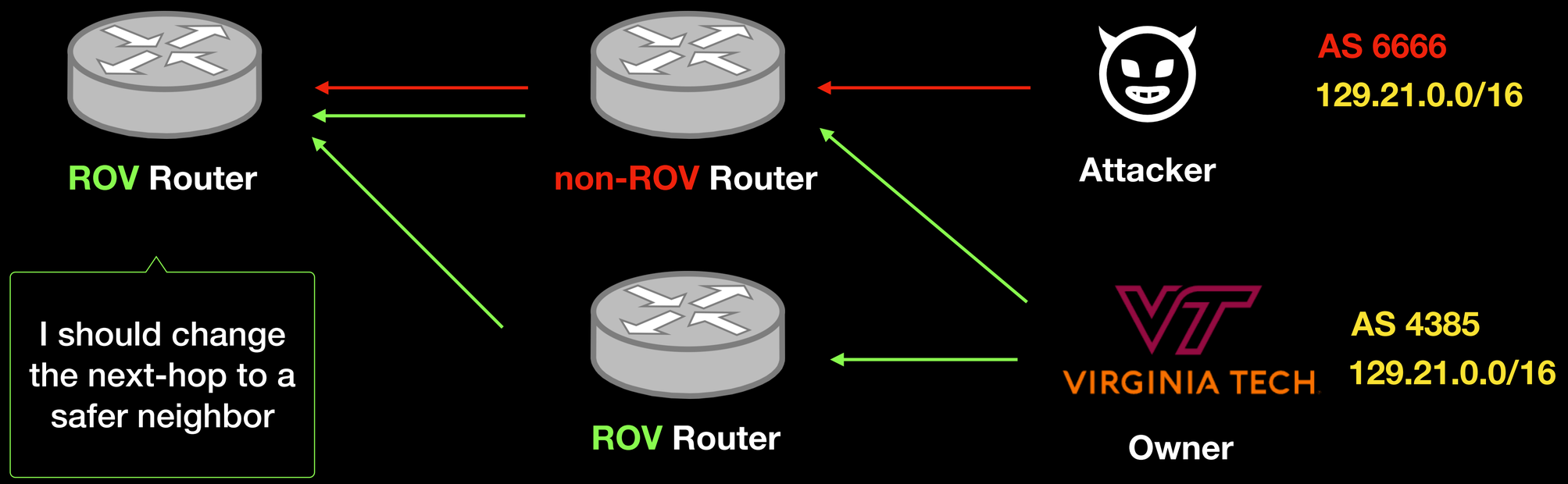
Mitigation


ROV Router
non-ROV Router
Attacker
AS 6666
129.21.0.0/16
ROV Router
VIRGINIA TECH
Owner
AS 4385
129.21.0.0/16

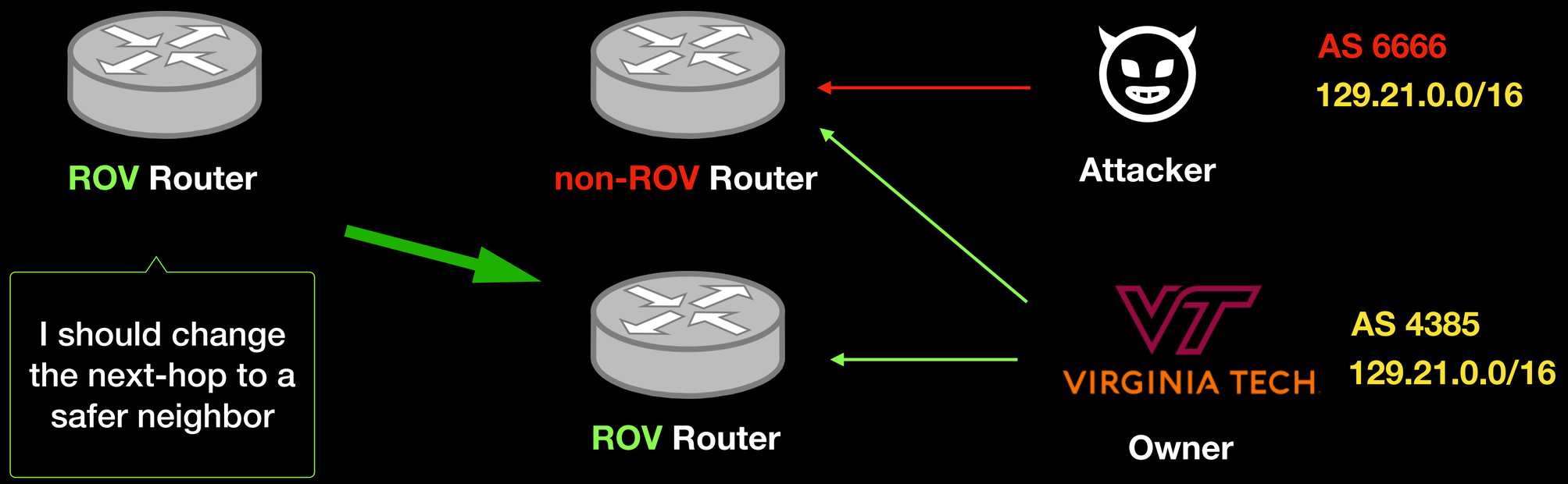
Mitigation


ROV Router
non-ROV Router
Attacker
AS 6666
129.21.0.0/16
ROV Router
VIRGINIA TECH
Owner
AS 4385
129.21.0.0/16

Mitigation



Mitigation



Thanks!