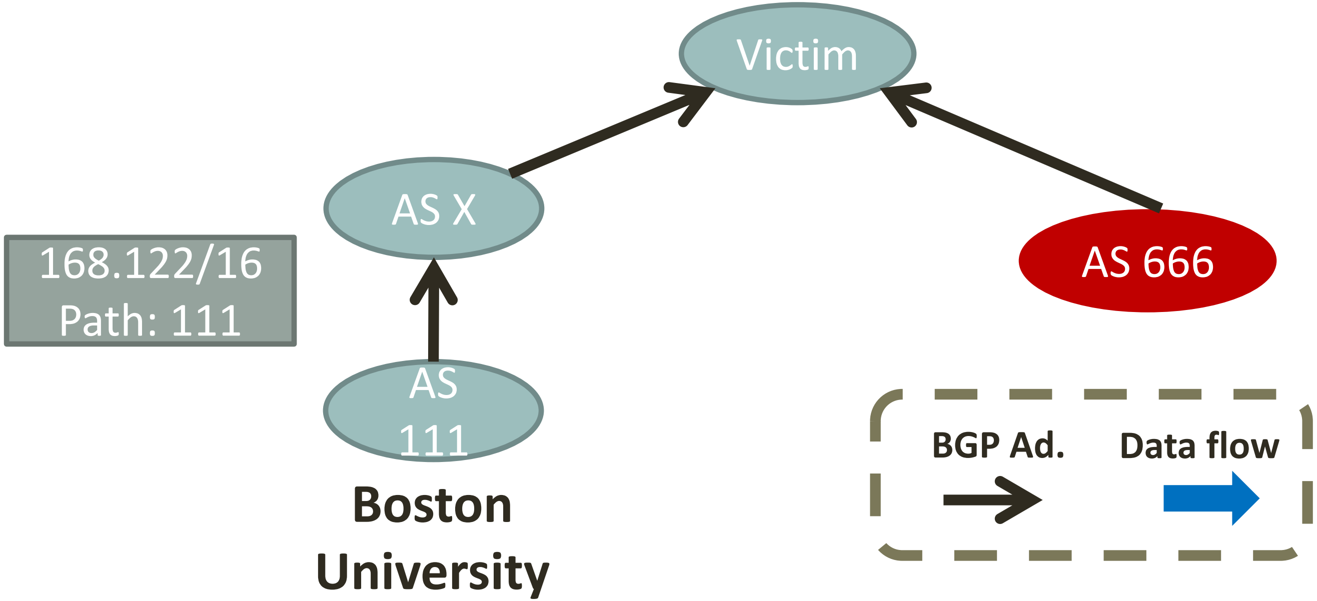
Jumpstarting BGP Security

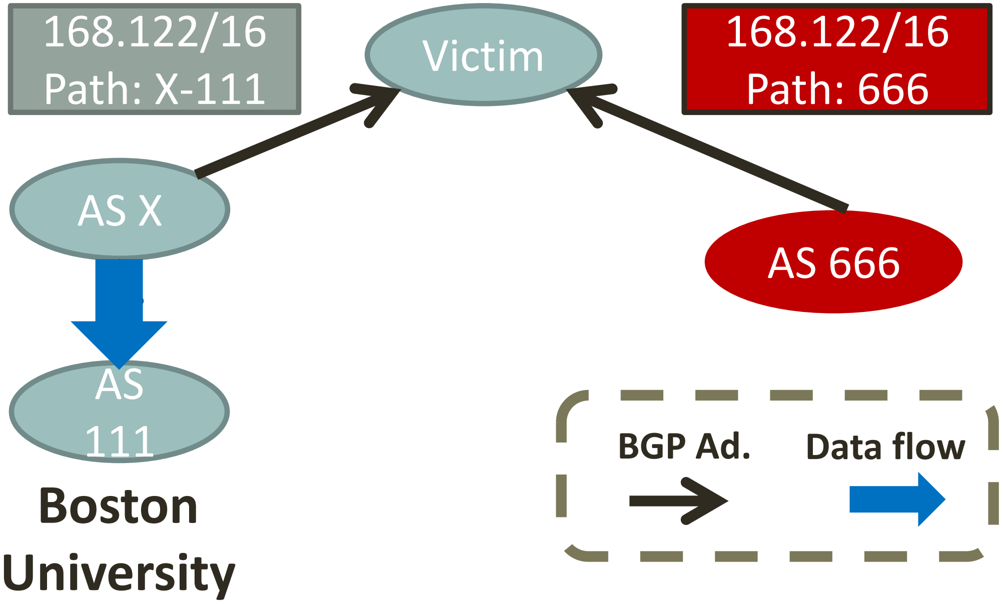
Yossi Gilad

Joint work with: Avichai Cohen, Amir Herzberg, and Michael Schapira

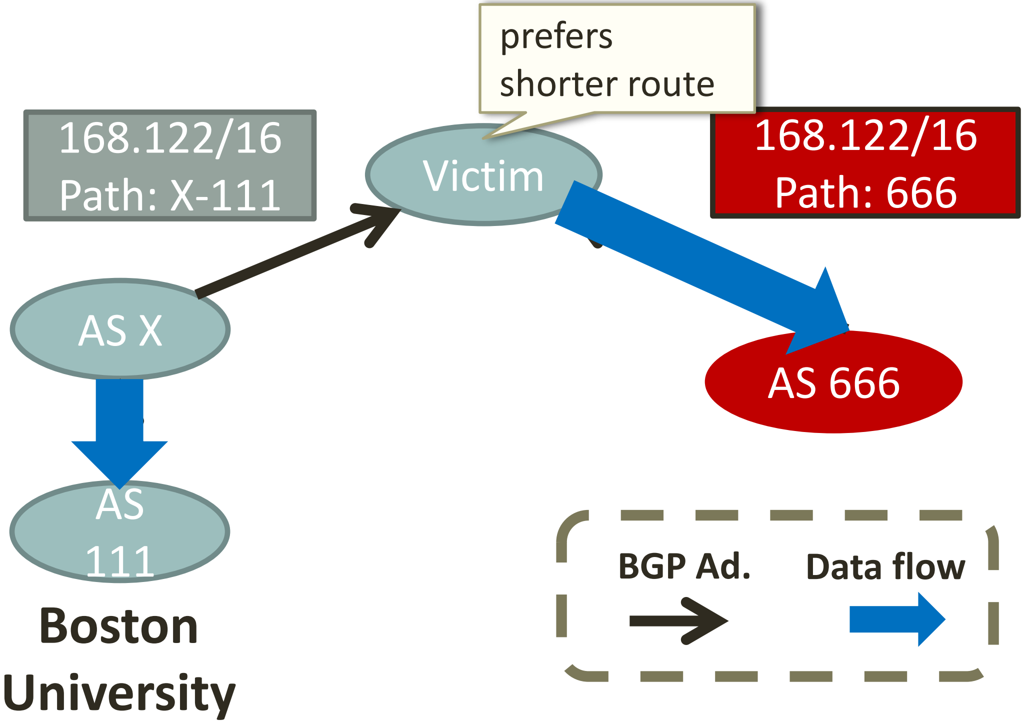
Prefix hijacking



Prefix hijacking



Prefix hijacking



Resource Public Key Infrastructure (RPKI)

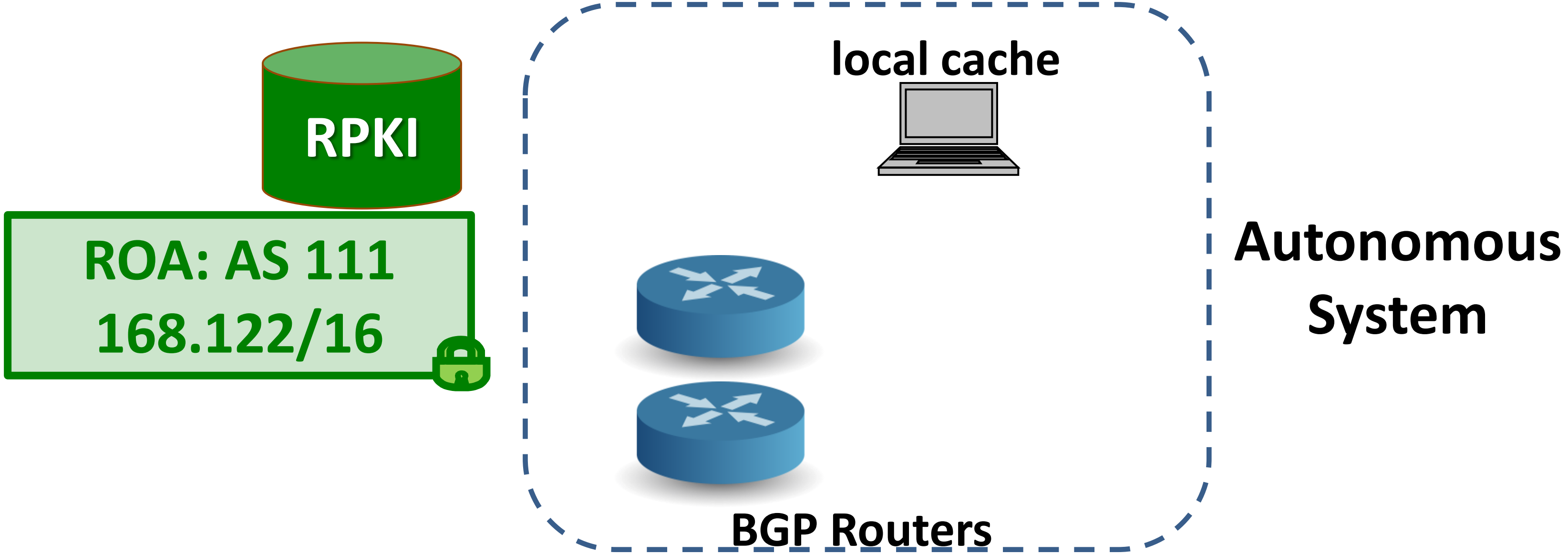
The Resource Public Key Infrastructure (RPKI) maps IP prefixes to organizations that own them [RFC 6480]

- Provides origin authentication to prevent hijacks

- Lays the foundation for protection against more sophisticated attacks on interdomain routing
  - e.g., required for BGPsec

Resource Public Key Infrastructure (RPKI)

- Origin Authentication
  - Protects against hijacks
  - Slowly gaining traction (6% of prefixes covered)



RPKI

ROA: AS 111
168.122/16

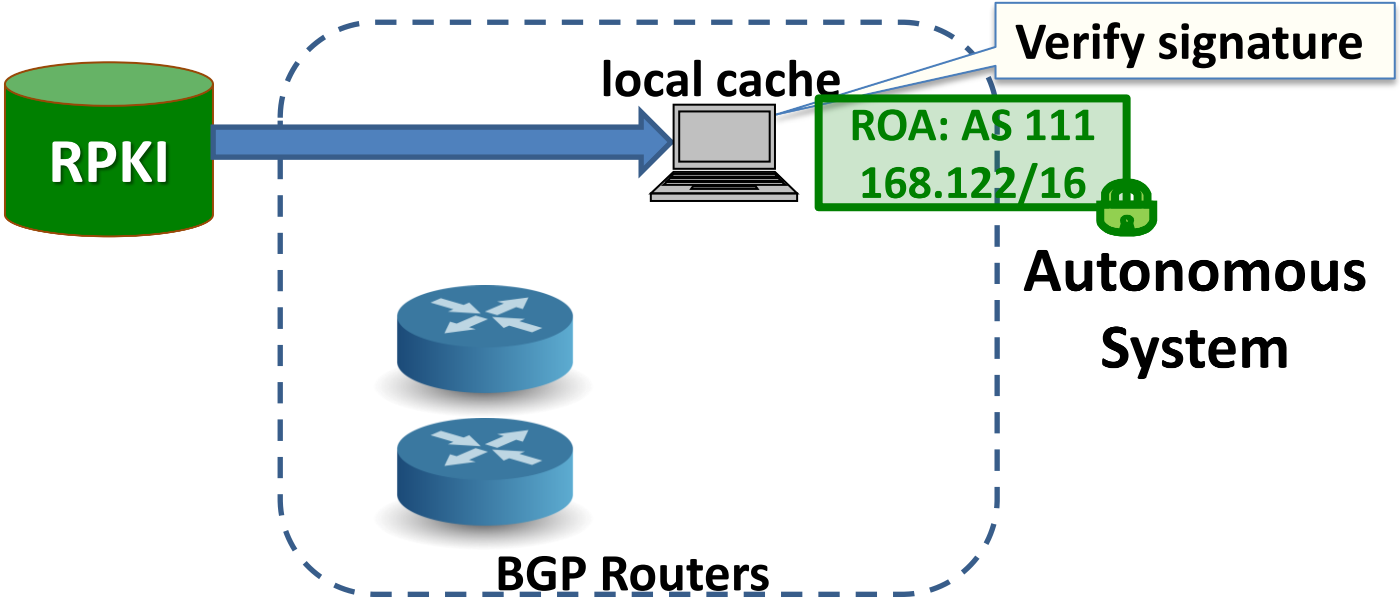
local cache

Autonomous System

BGP Routers

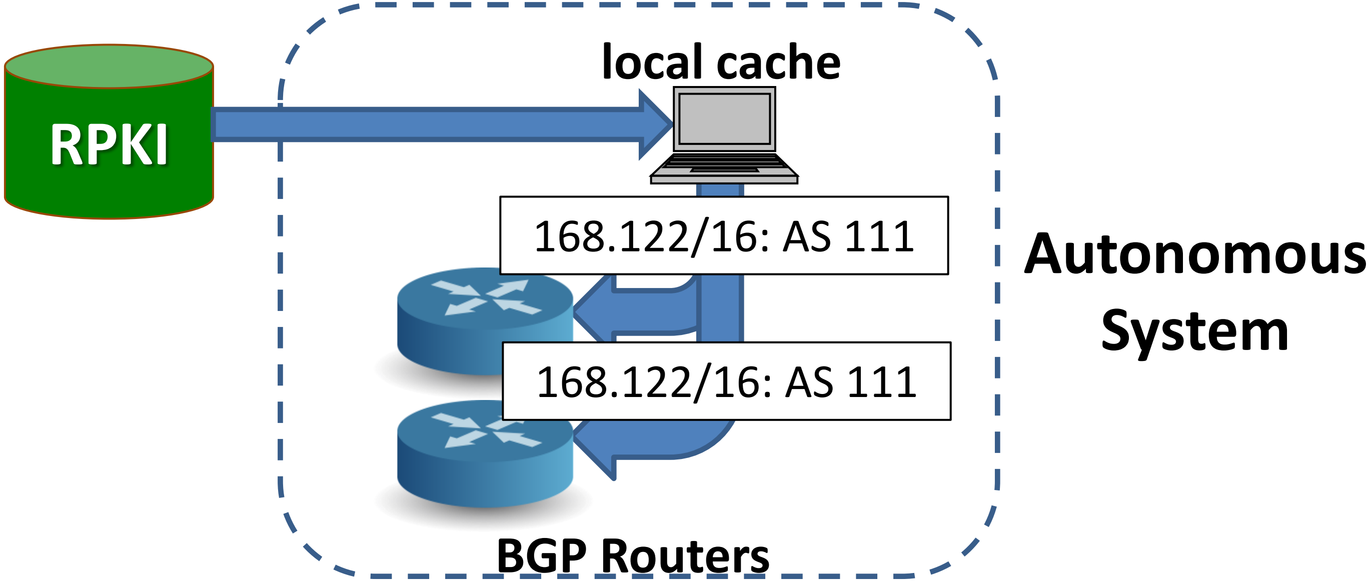
Resource Public Key Infrastructure (RPKI)

- Origin Authentication
  - Protects against hijacks
  - Slowly gaining traction (6% of prefixes covered)

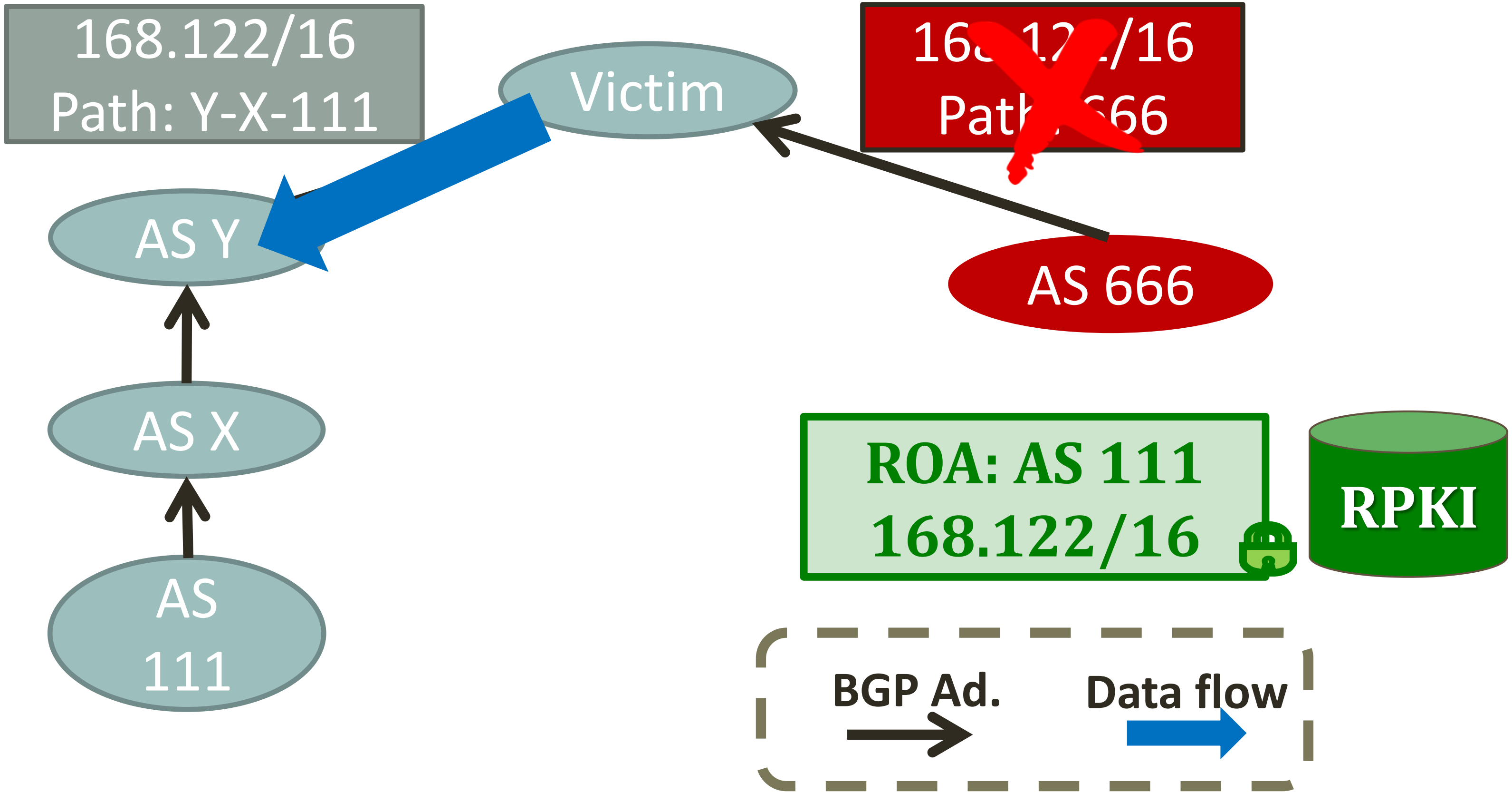


Resource Public Key Infrastructure (RPKI)

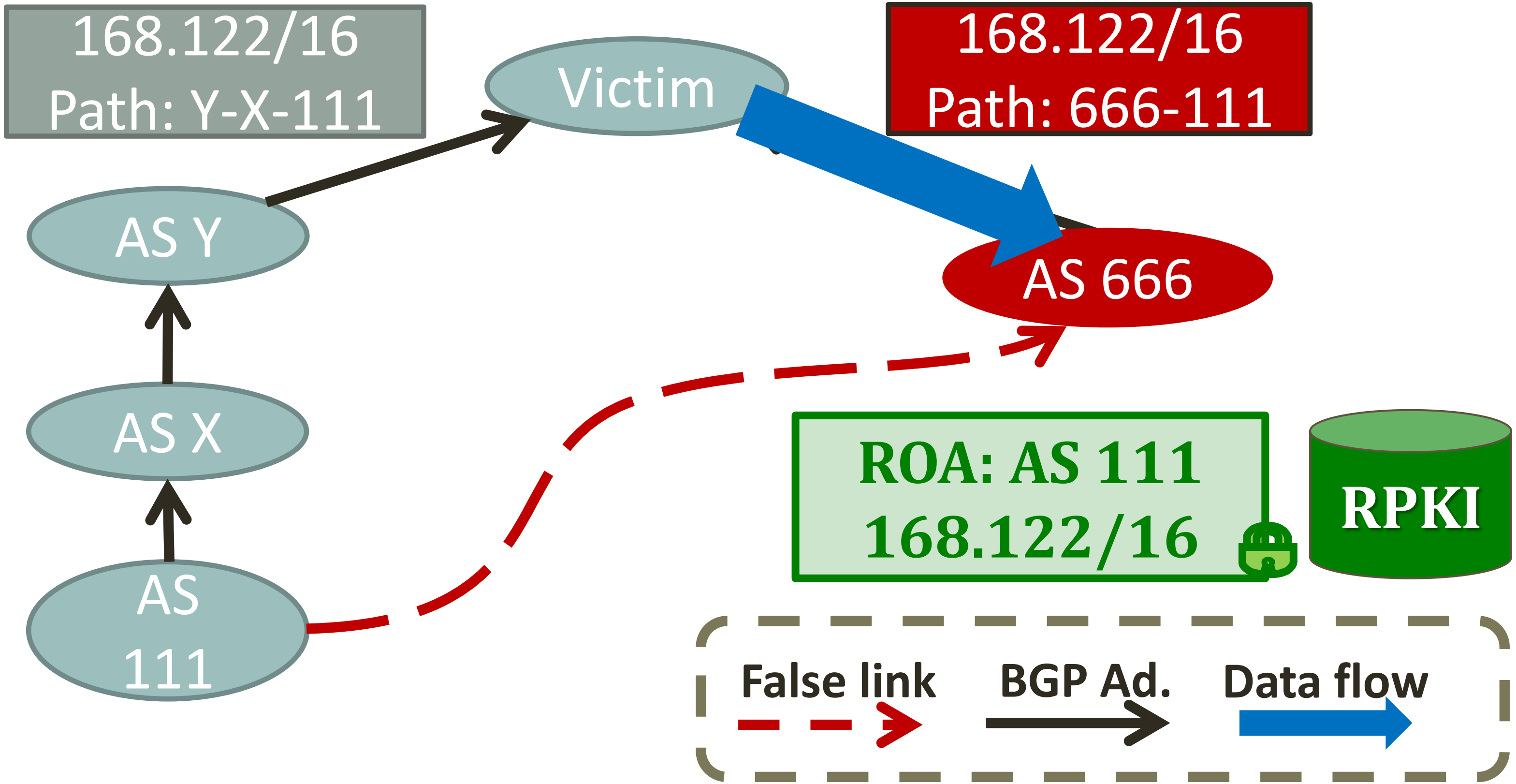
- Origin Authentication
  - Protects against hijacks
  - Slowly gaining traction (6% of prefixes covered)



RPKI prevents prefix hijacks

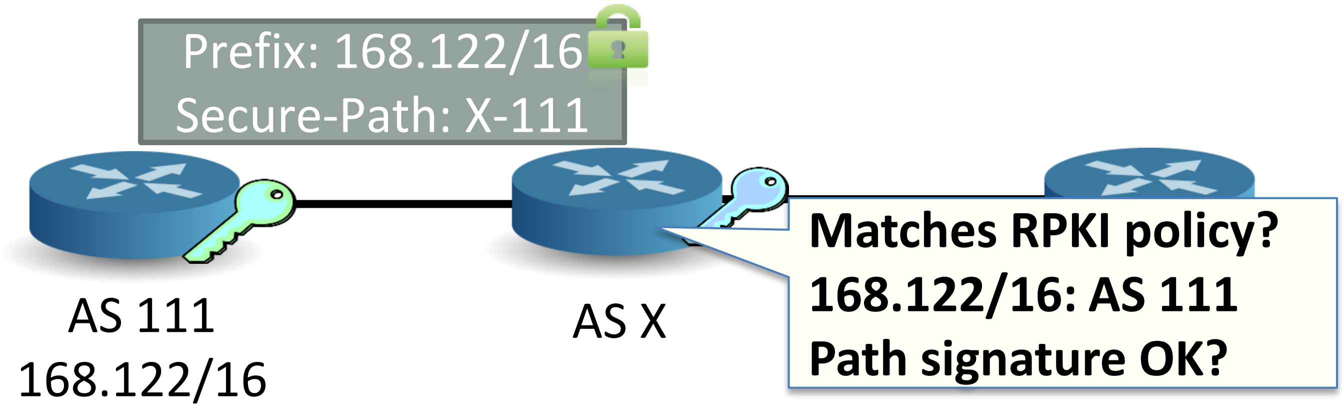


Forged origin circumvents RPKI



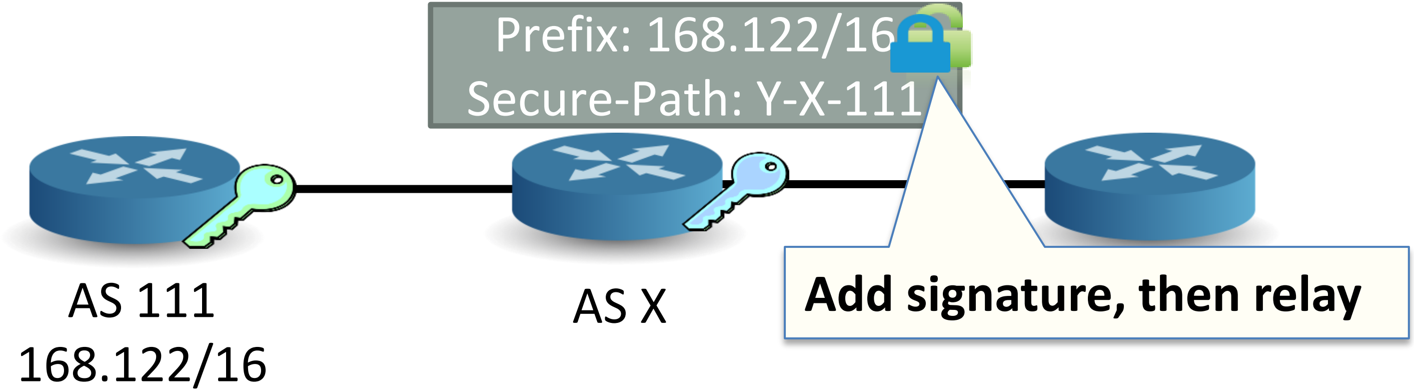
Current paradigm: a two step solution

- First, RPKI against hijacking
- Then, add BGPsec
  - – Protects against ``false links” in the route



Current paradigm: a two step solution

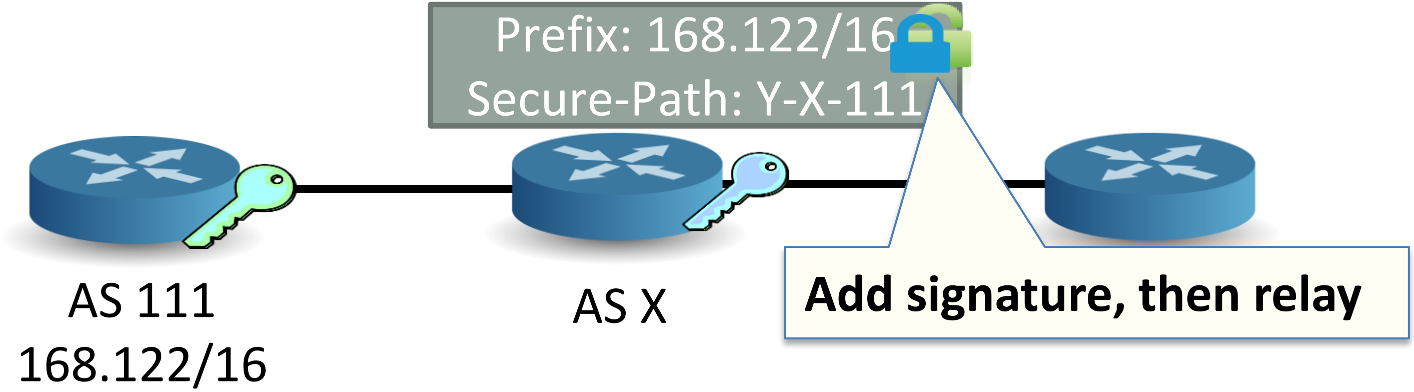
- First, RPKI against hijacking
- Then, add BGPsec
  - – Protects against ``false links” in the route



Add signature, then relay

Current paradigm: a two step solution

- First, RPKI against hijacking
- Then, add BGPsec
  - Protects against ``false links" in the route
  - Deployment challenge:
    - Real-time signature and validation
    - Different message format



Prefix: 168.122/16

Secure-Path: Y-X-111

AS 111

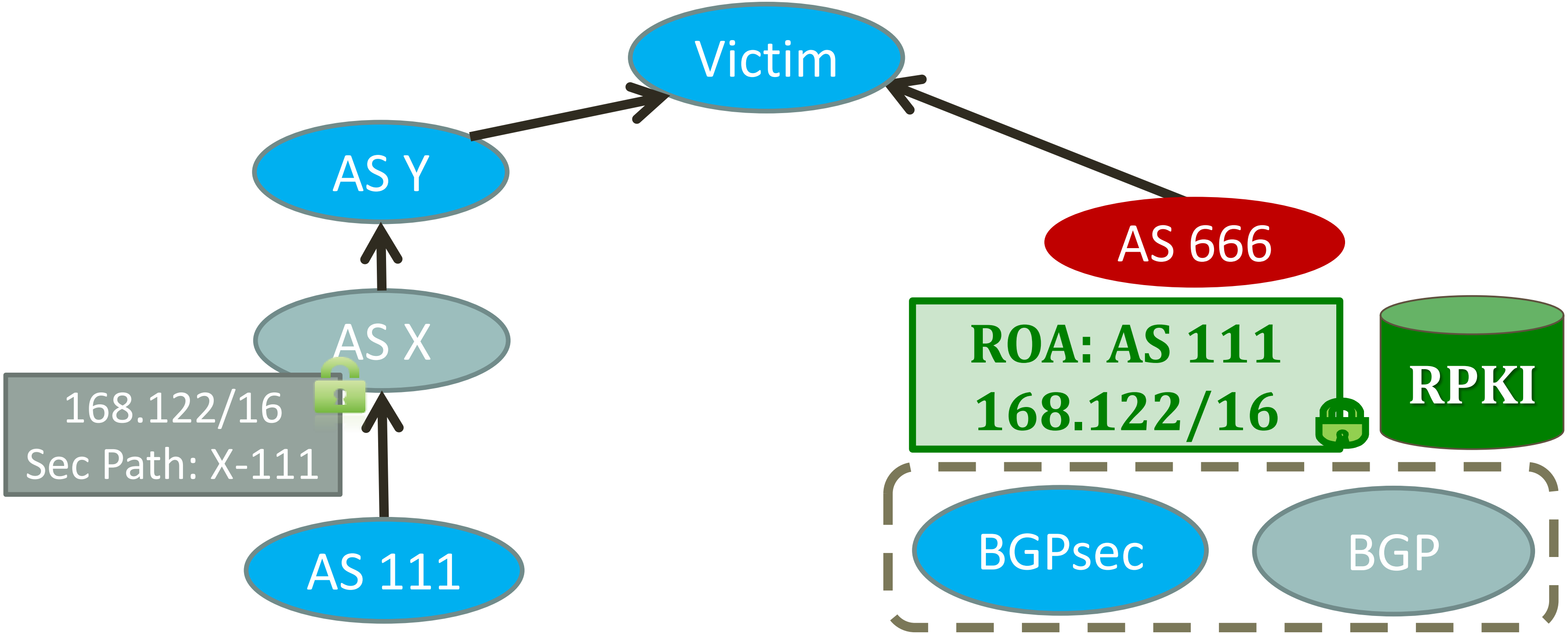
168.122/16

AS X

Add signature, then relay

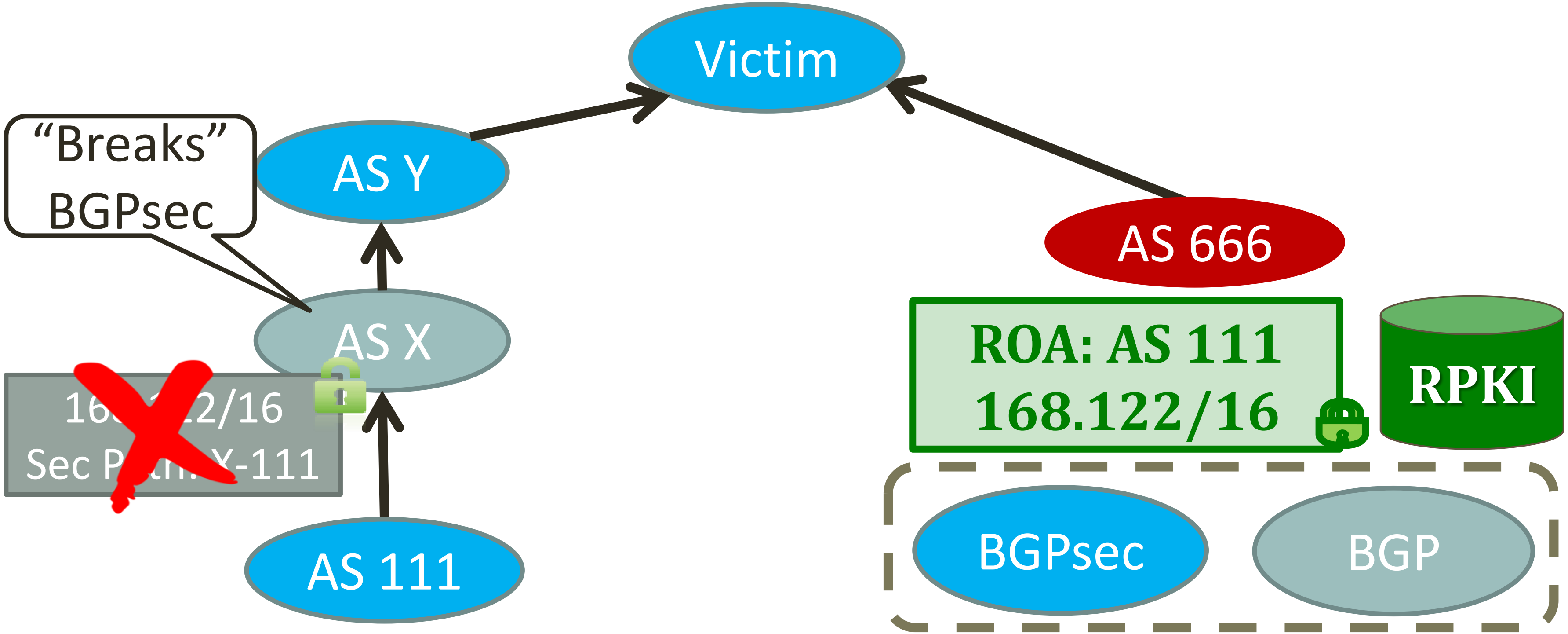
BGPsec in partial adoption?

Meager benefits [Lychev et al., SIGCOMM'13]



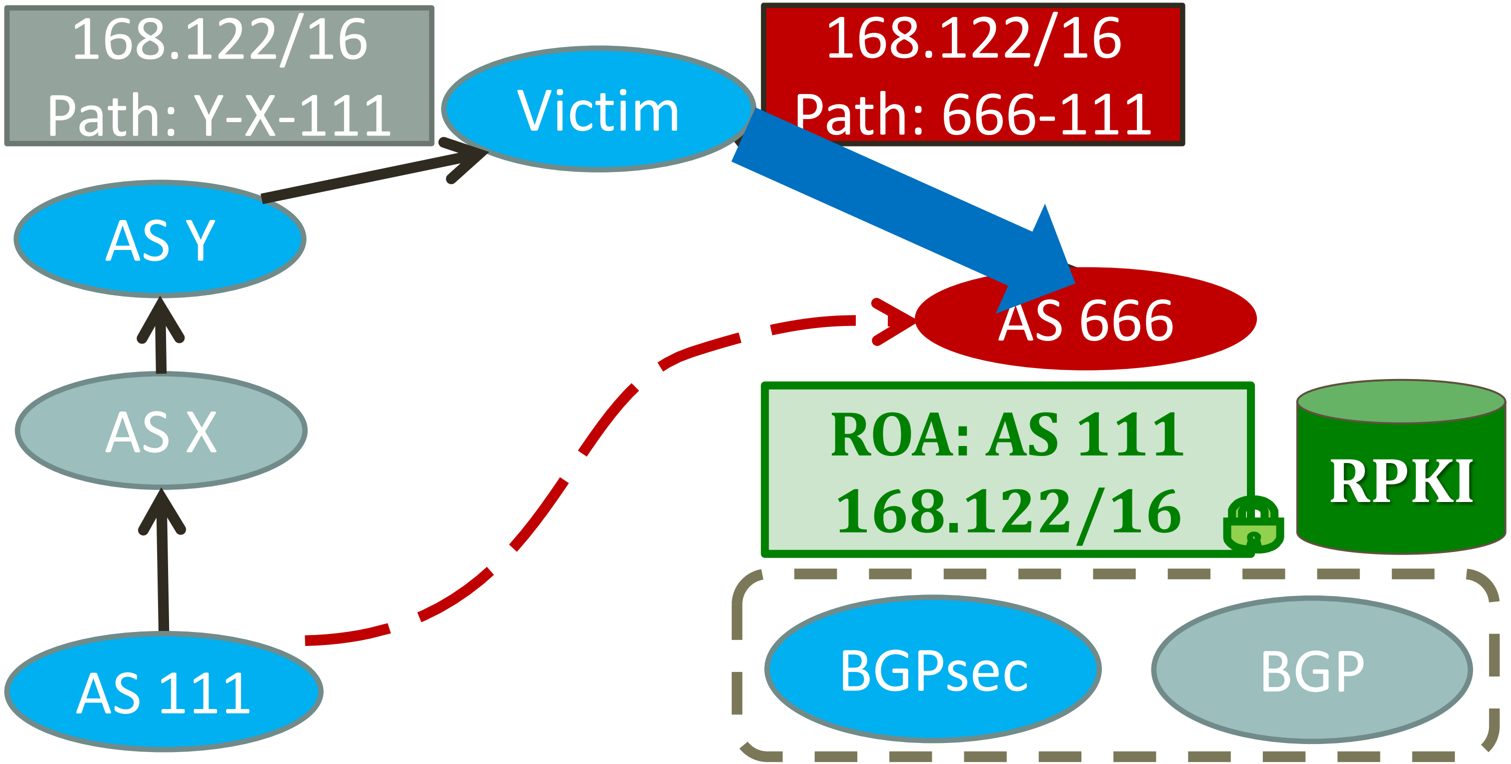
BGPsec in partial adoption?

Meager benefits [Lychev et al., SIGCOMM'13]



BGPsec in partial adoption?

Meager benefits [Lychev et al., SIGCOMM'13]



Our Goals

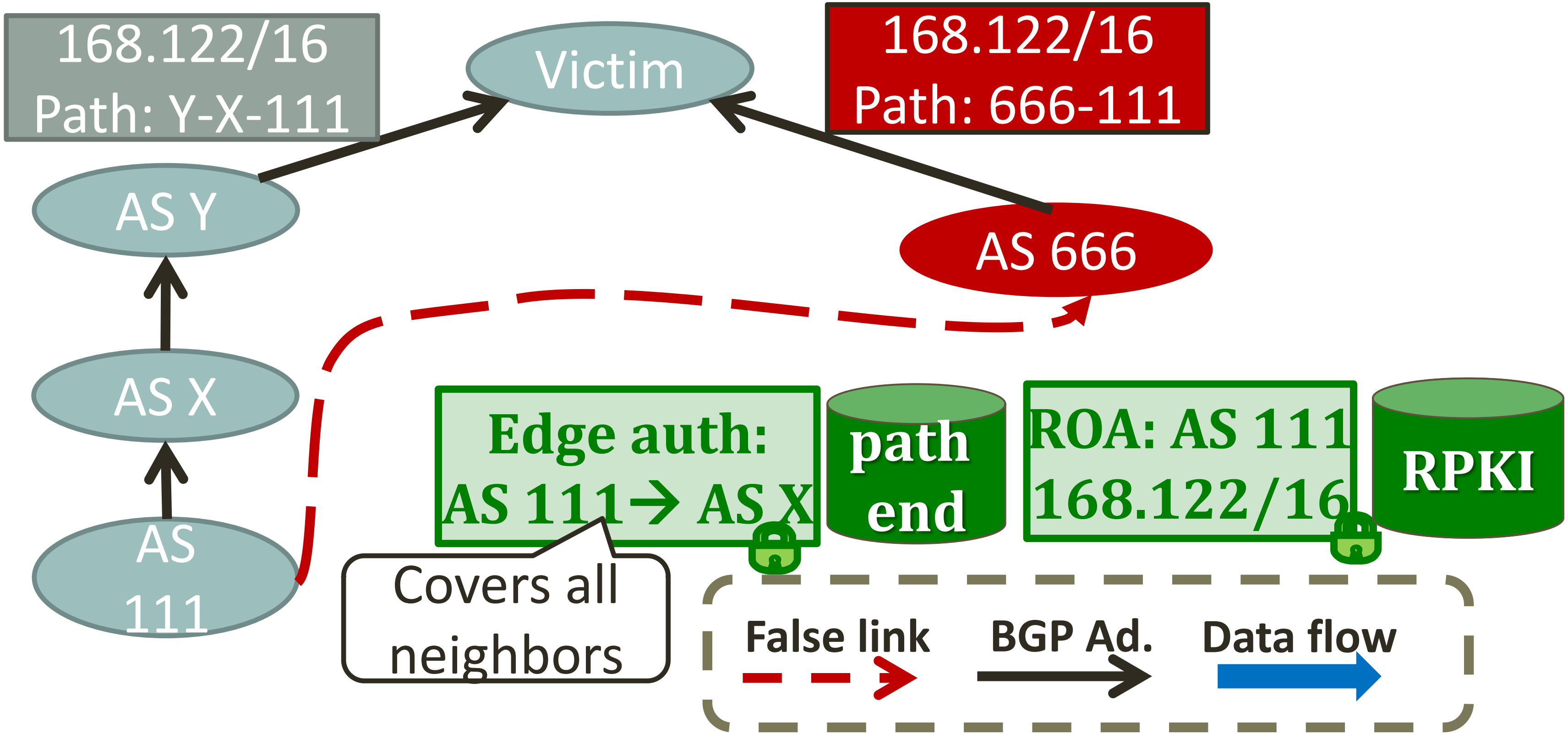
Security:

- Protect against “forged origin” in BGP advertisements
- Significant benefits in partial deployment
  - In contrast to BGPsec

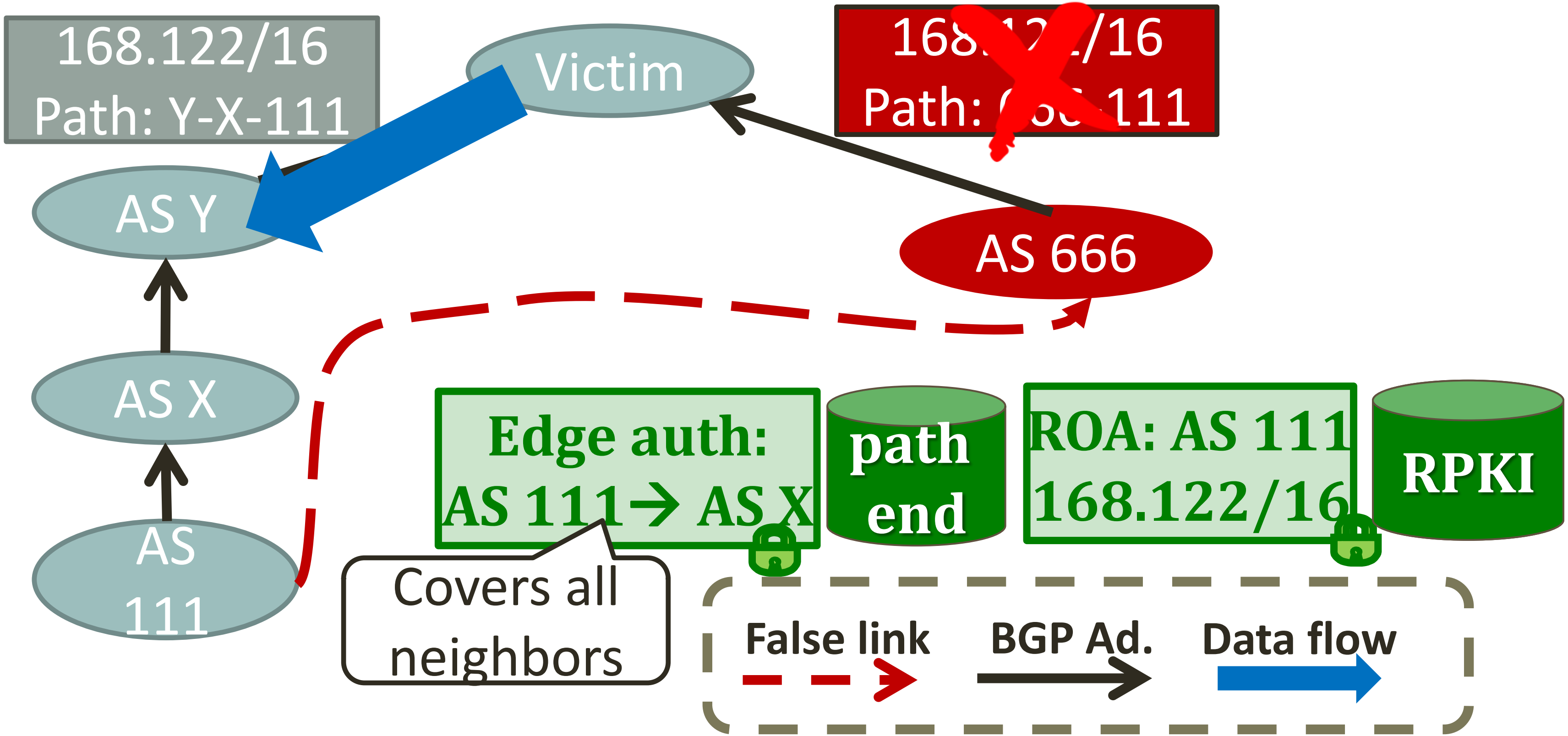
Deployment:

- Minimal computation overhead
  - Signatures and verifications: only **offline, off-router**
- No changes to BGP messages
- Similar to RPKI

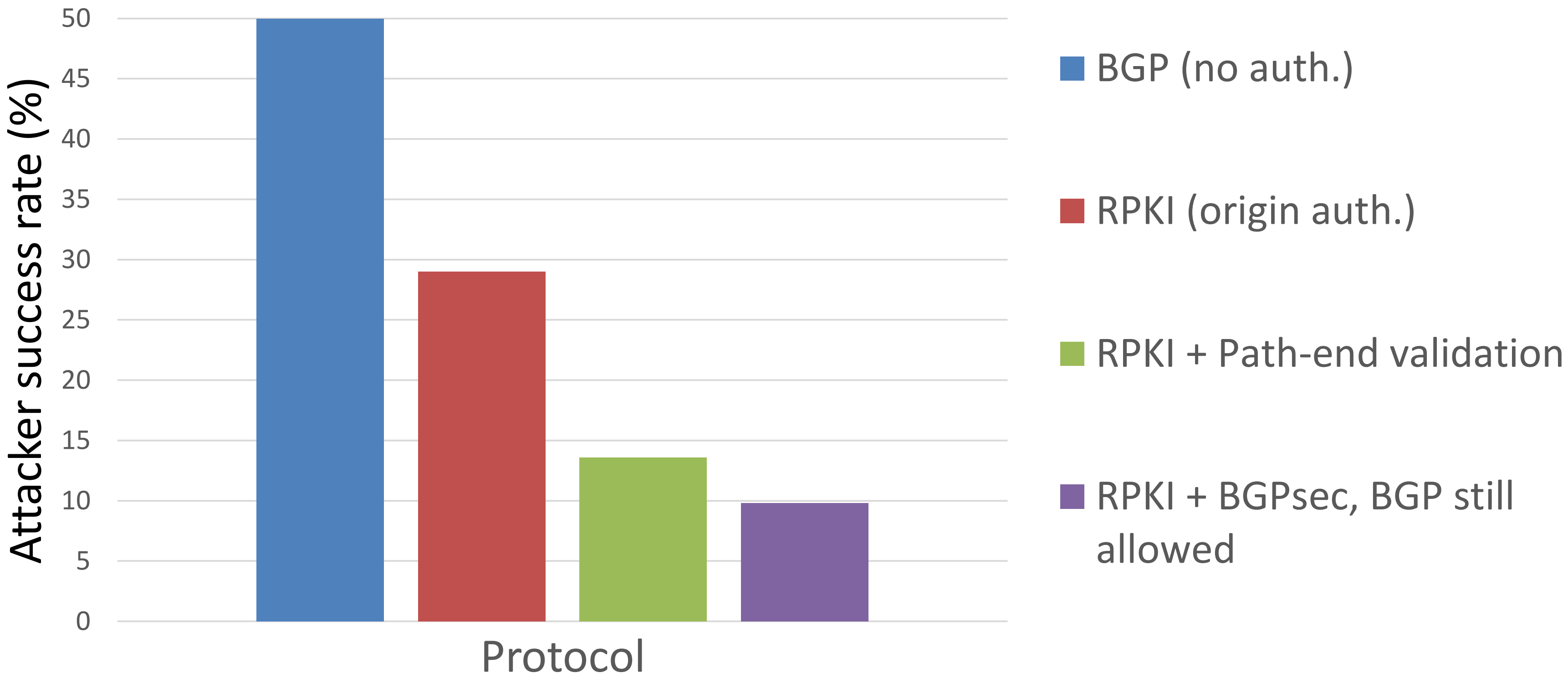
Path-end validation



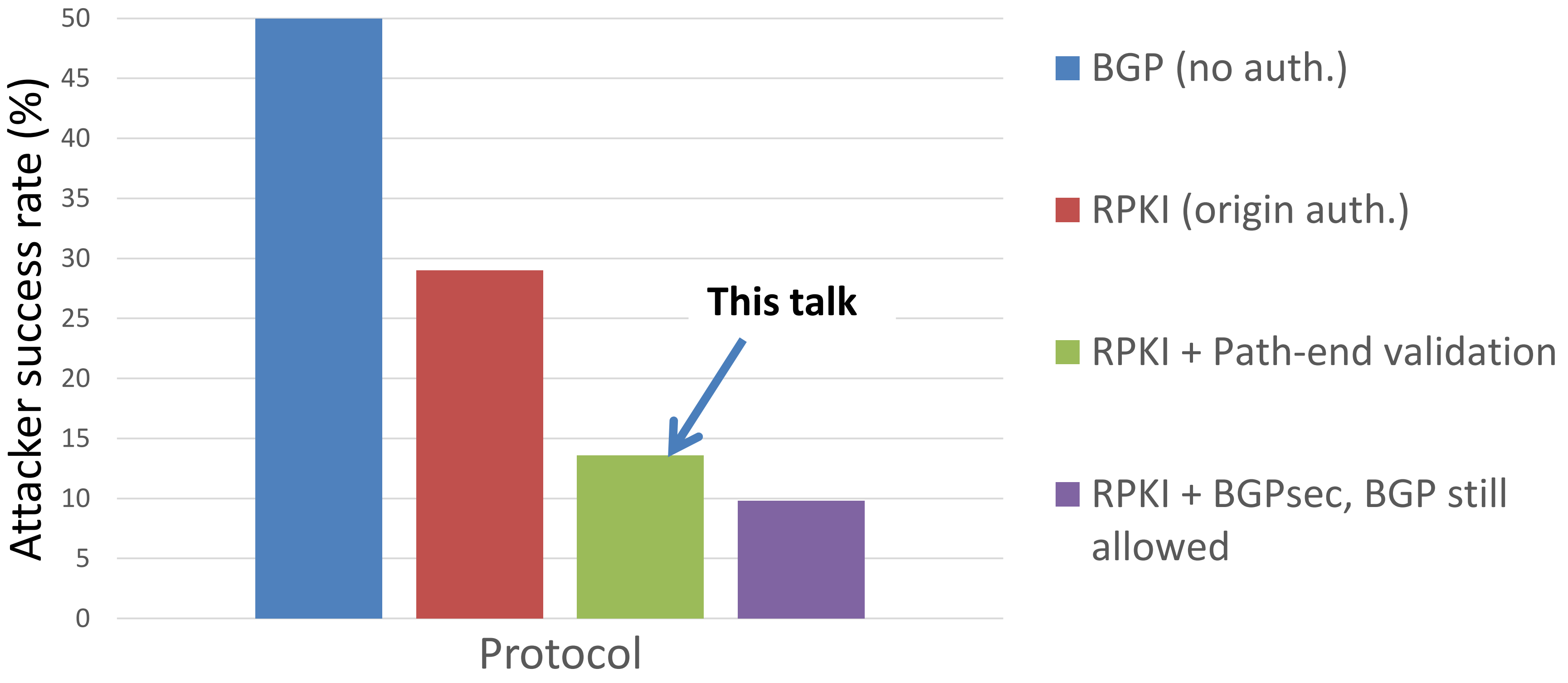
Path-end validation



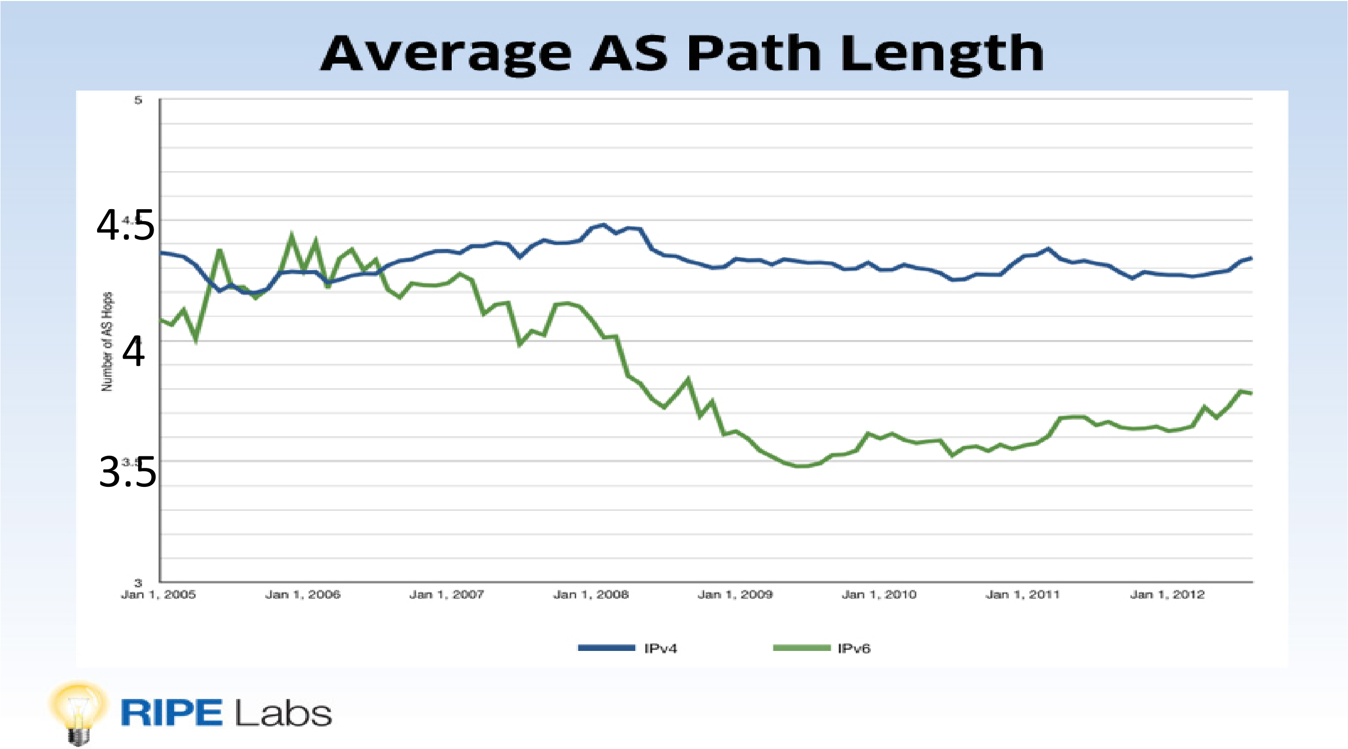
Inter domain routing security: Mechanism comparison



Inter domain routing security: Mechanism comparison

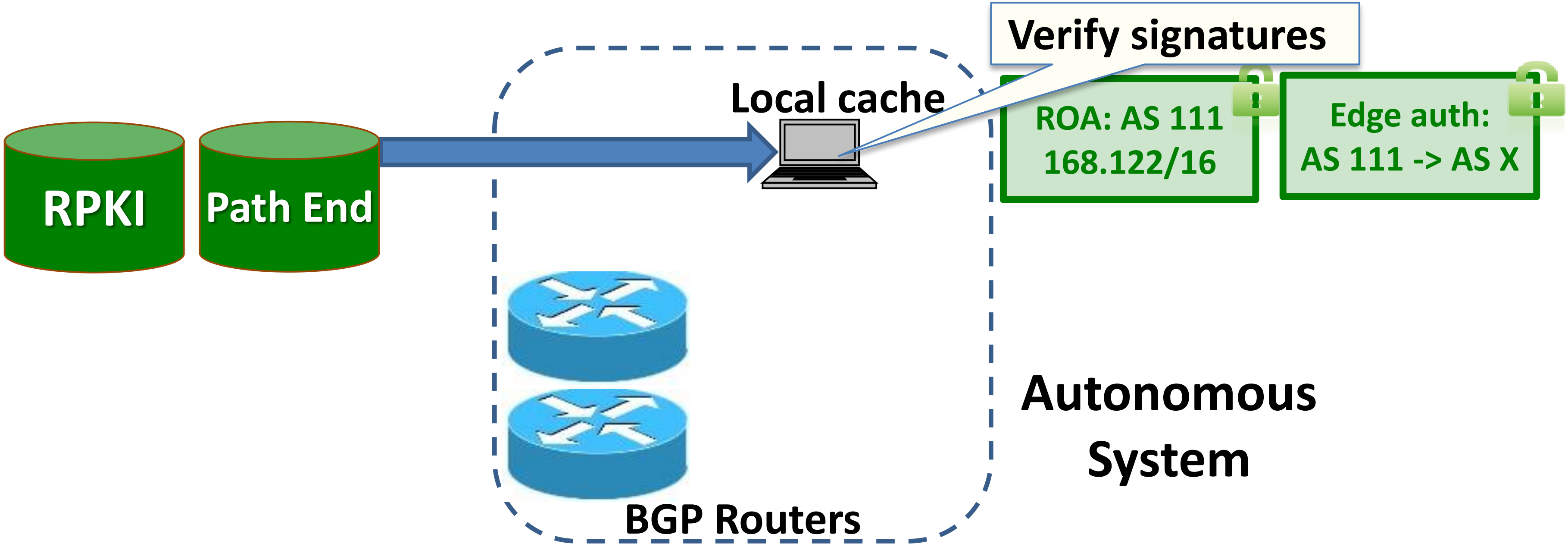


Path-end validation: Intuition



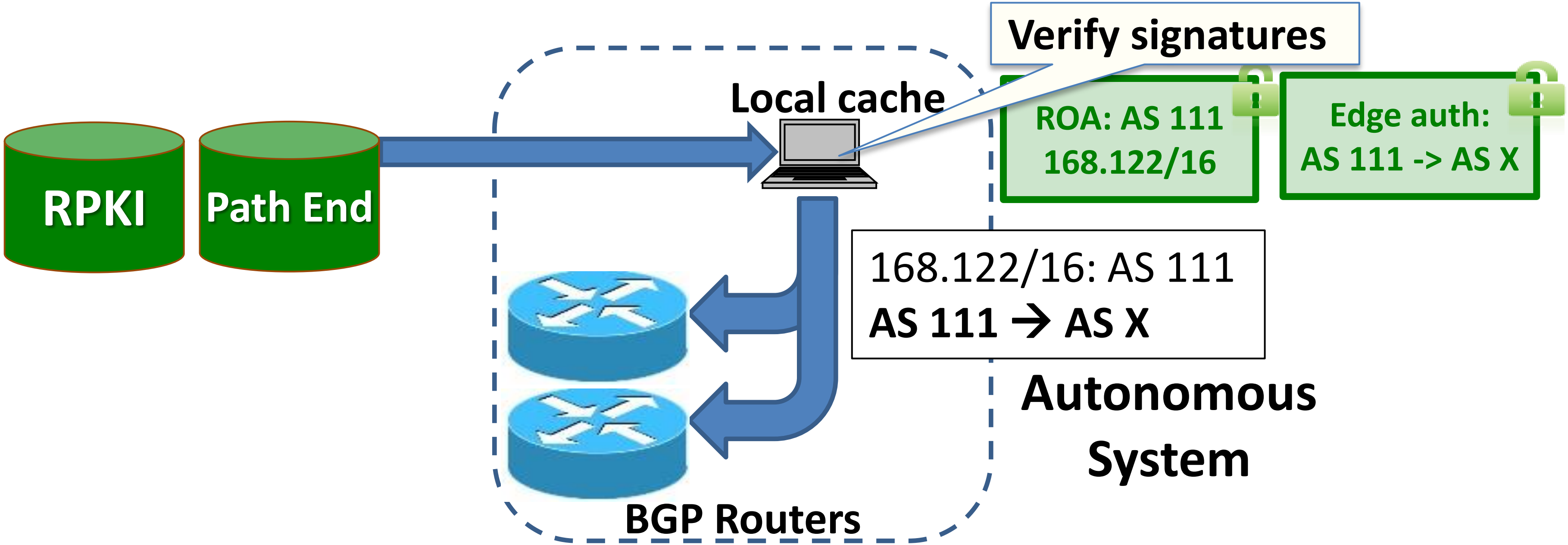
Deployment

- Similar to RPKI



Deployment

- Similar to RPKI



Deployment

```
ip as-path access-list as1 deny _[^X]_111_
```

- Use existing Access List interface
- Validated suffix extends automatically with adoption

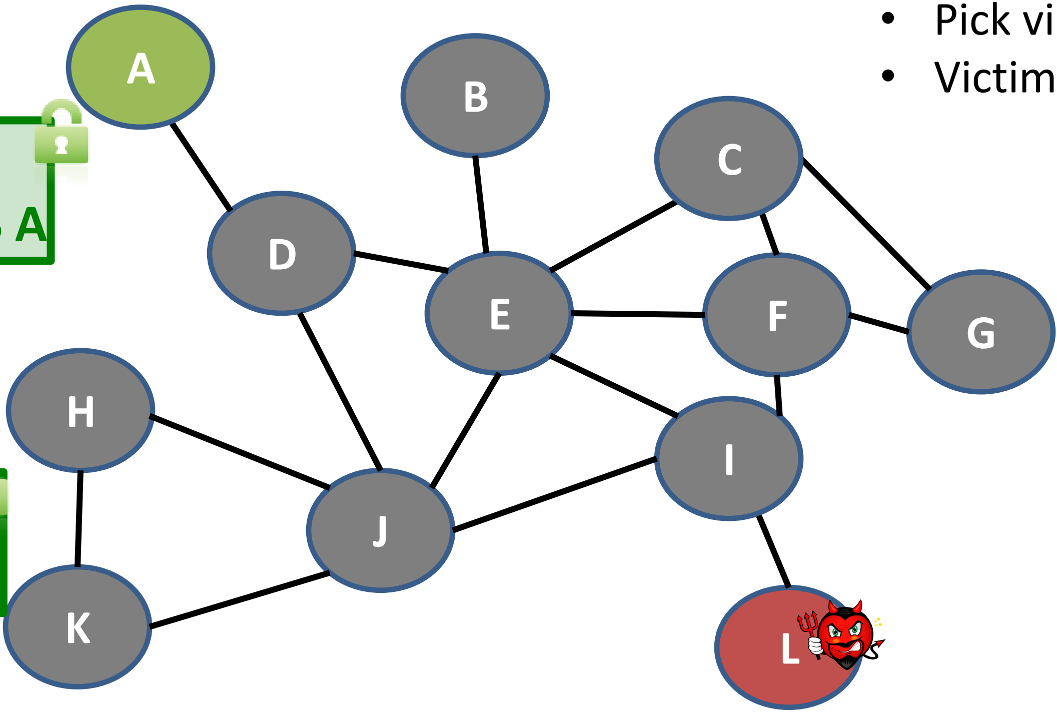
Security in partial adoption: Simulation framework

RPKI

ROA:
1.2.0.0/16 → AS A

Path End

Edge auth:
AS A → AS D

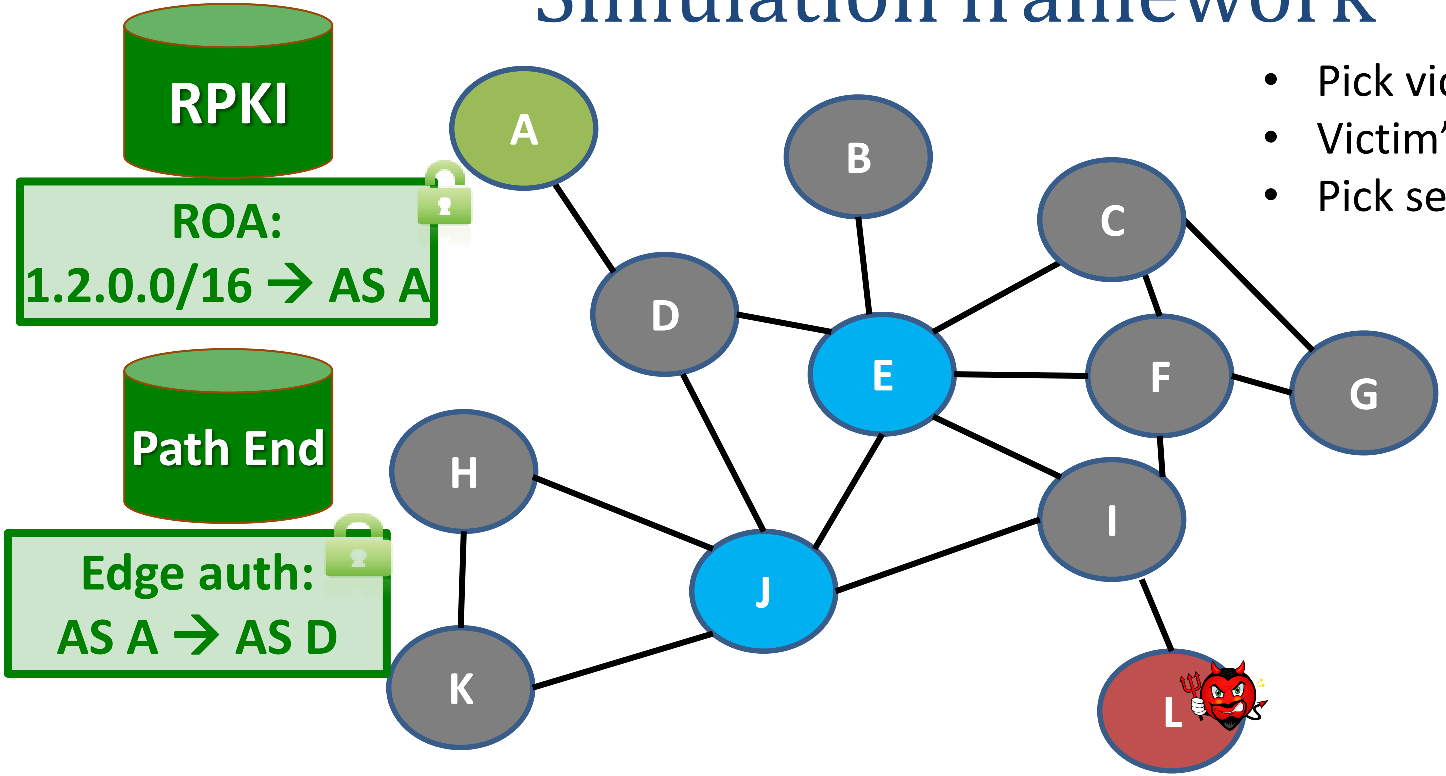


- Pick victim & attacker
- Victim's prefix has a ROA+EA

Empirically-derived AS-level network from CAIDA

Including inferred peering links [Giotsas et al., SIGCOMM'13]

Security in partial adoption: Simulation framework

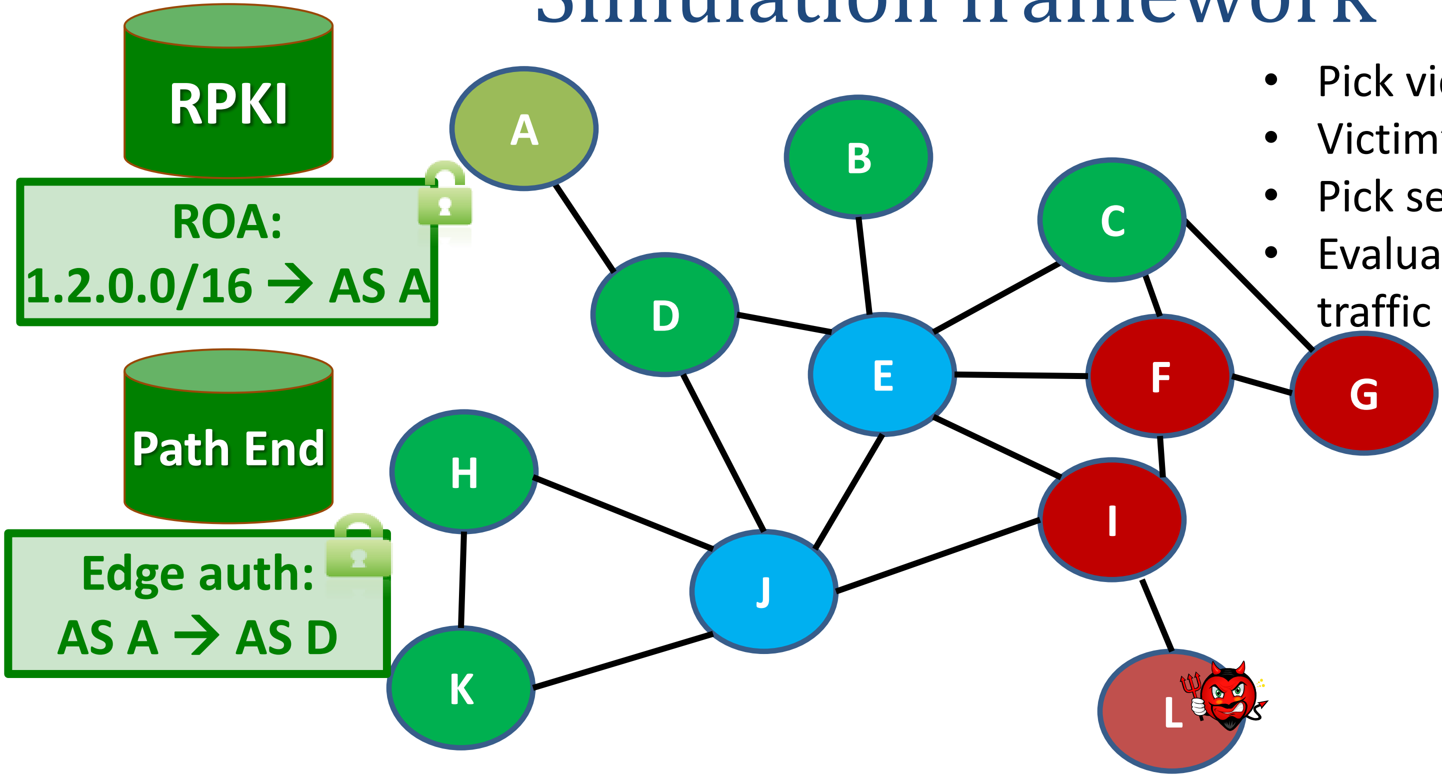


- Pick victim & attacker
- Victim's prefix has a ROA+EA
- Pick set of filtering ASes

Empirically-derived AS-level network from CAIDA

Including inferred peering links [Giotsas et al., SIGCOMM'13]

Security in partial adoption: Simulation framework



RPKI

ROA:
1.2.0.0/16 → AS A

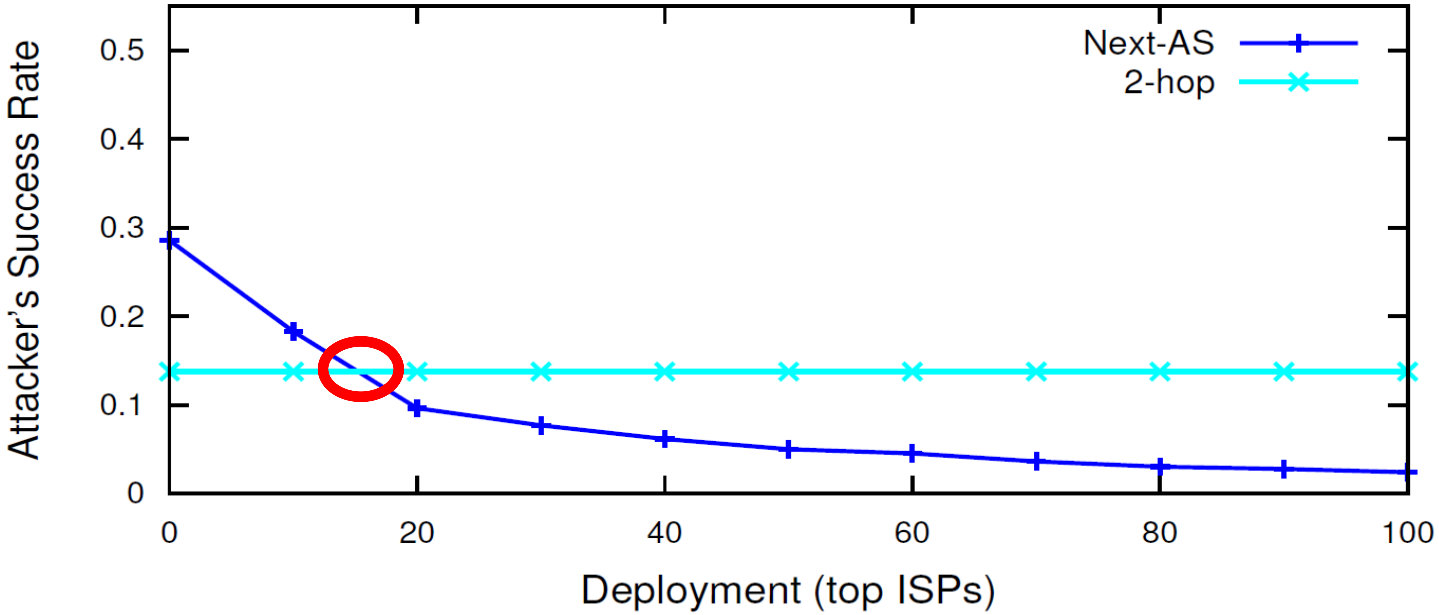
Path End

Edge auth:
AS A → AS D

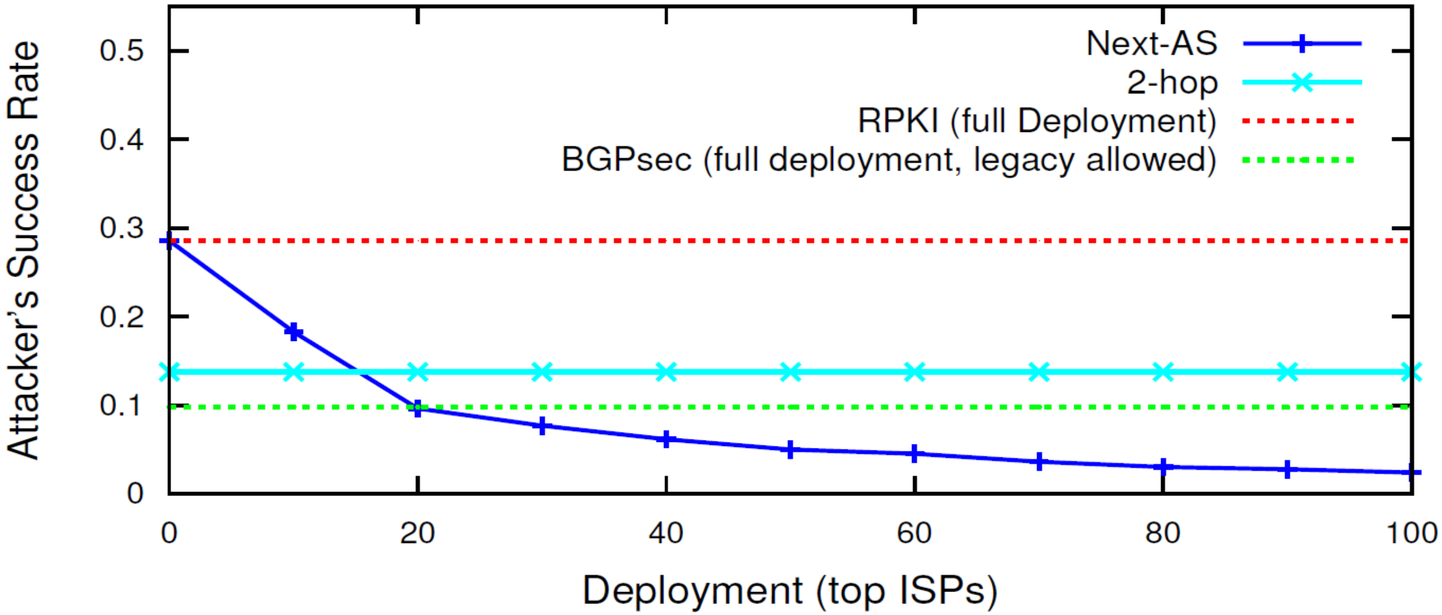
- Pick victim & attacker
- Victim’s prefix has a ROA+EA
- Pick set of filtering ASes
- Evaluate which ASes send traffic to the attacker

Empirically-derived AS-level network from CAIDA
Including inferred peering links [Giotsas et al., SIGCOMM’13]

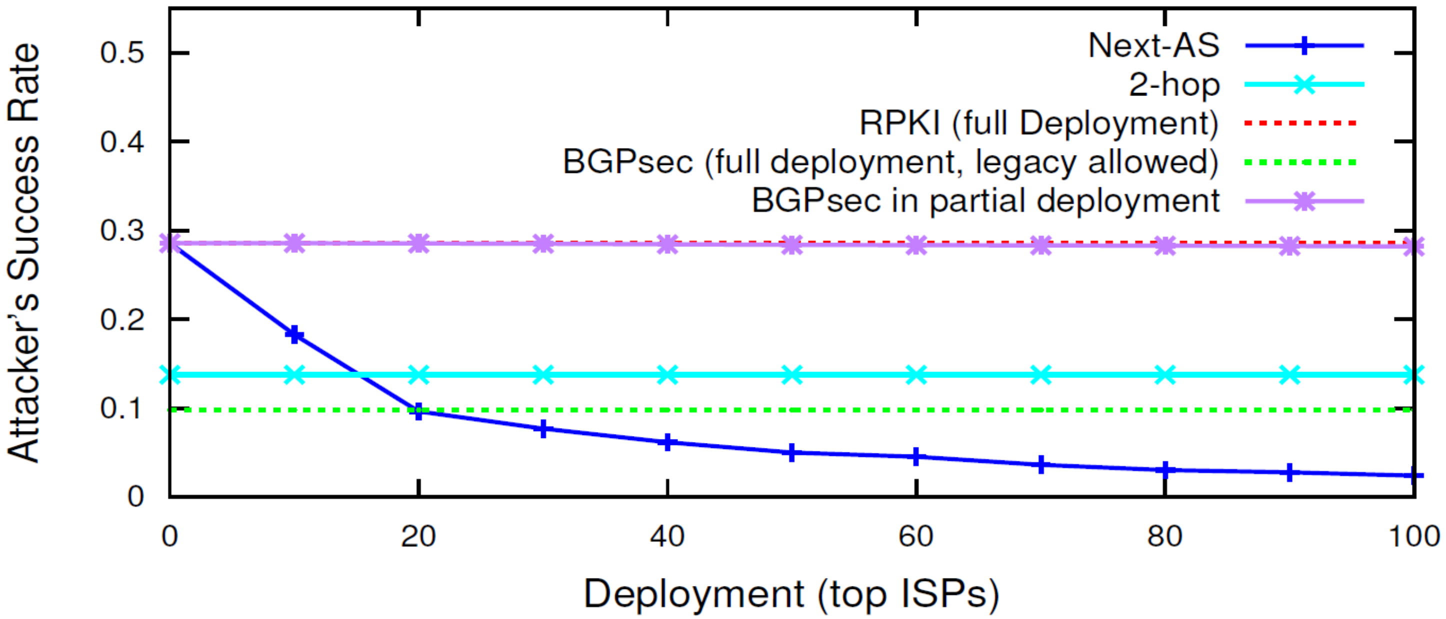
Simulation results



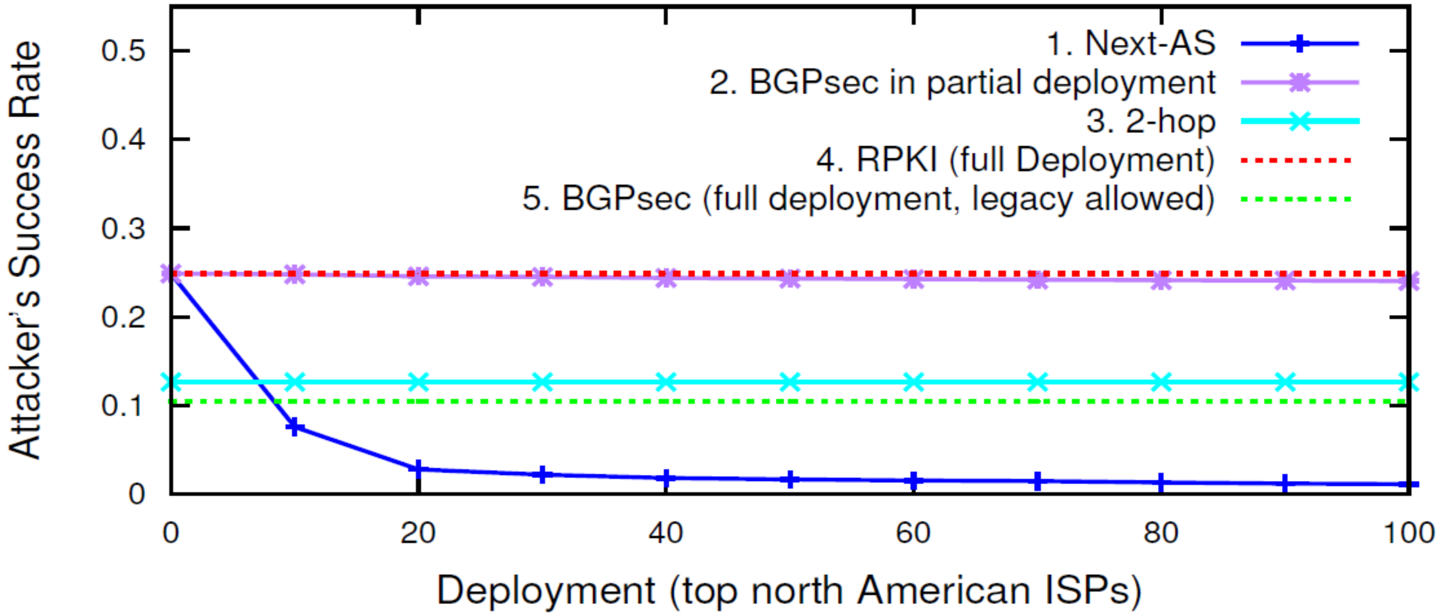
Simulation results



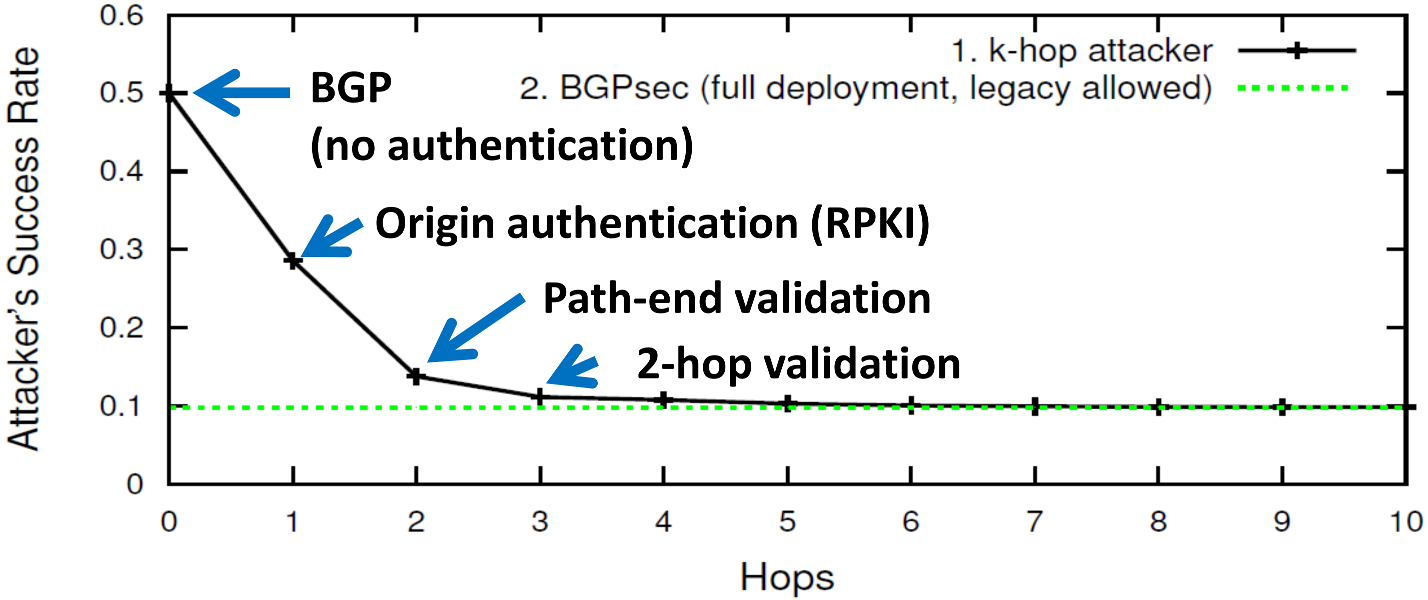
Simulation results



Local deployment & local benefits



Impact of authenticating hops



BGP (no authentication)

Origin authentication (RPKI)

Path-end validation

2-hop validation

More results

- Large content providers are better protected
- Path-end validation mitigates high profile incidents
- Security monotone
  - BGPsec is not [Lychev et al., SIGCOMM’13]

Conclusion

- Path-end validation
  - Can significantly improve inter-domain routing security while avoiding BGPsec’s deployment hurdles

- We advocate
  - Extending RPKI to support path-end validation
  - Regulatory/financial efforts on gathering critical mass of adopters

Thank You