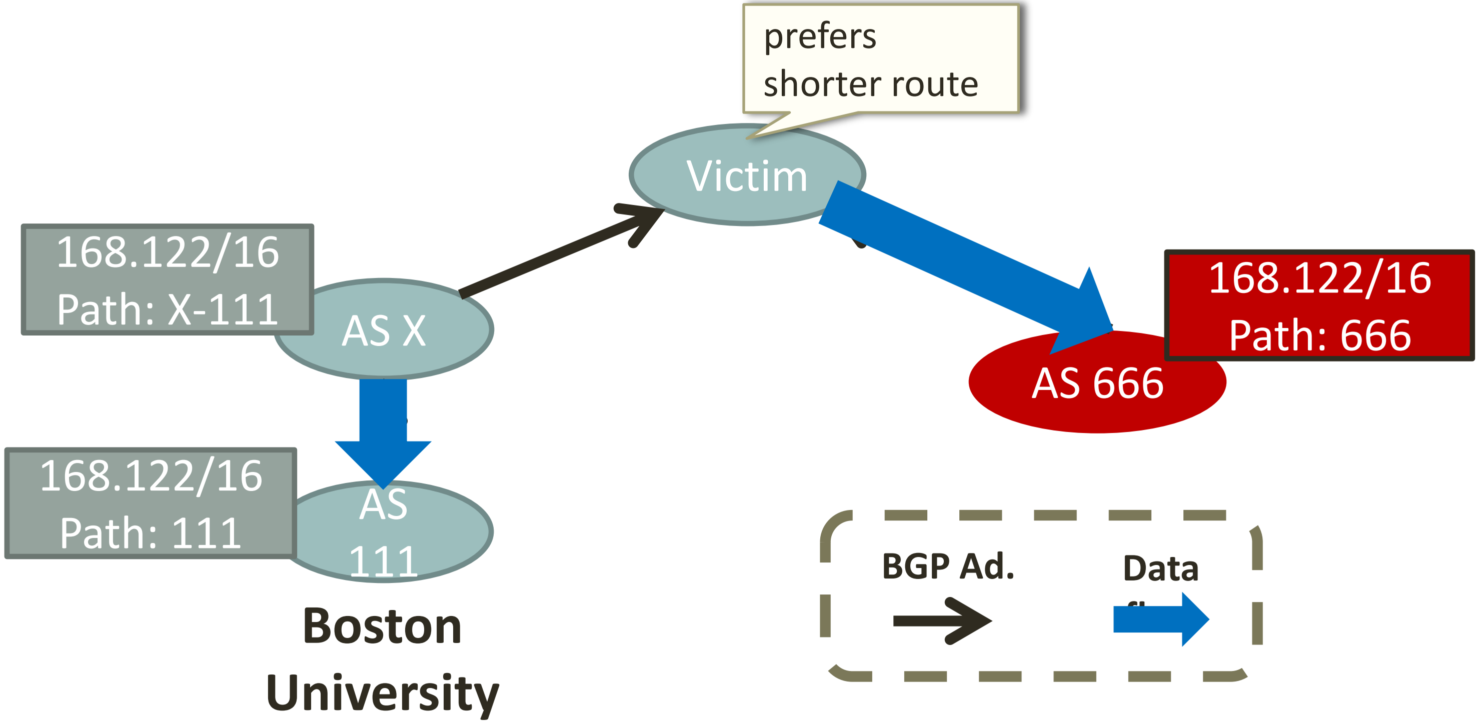
Jumpstarting BGP Security

Yossi Gilad

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

Prefix hijacking



prefers shorter route

Victim

168.122/16
Path: X-111

AS X

168.122/16
Path: 666

AS 666

168.122/16
Path: 111

AS 111

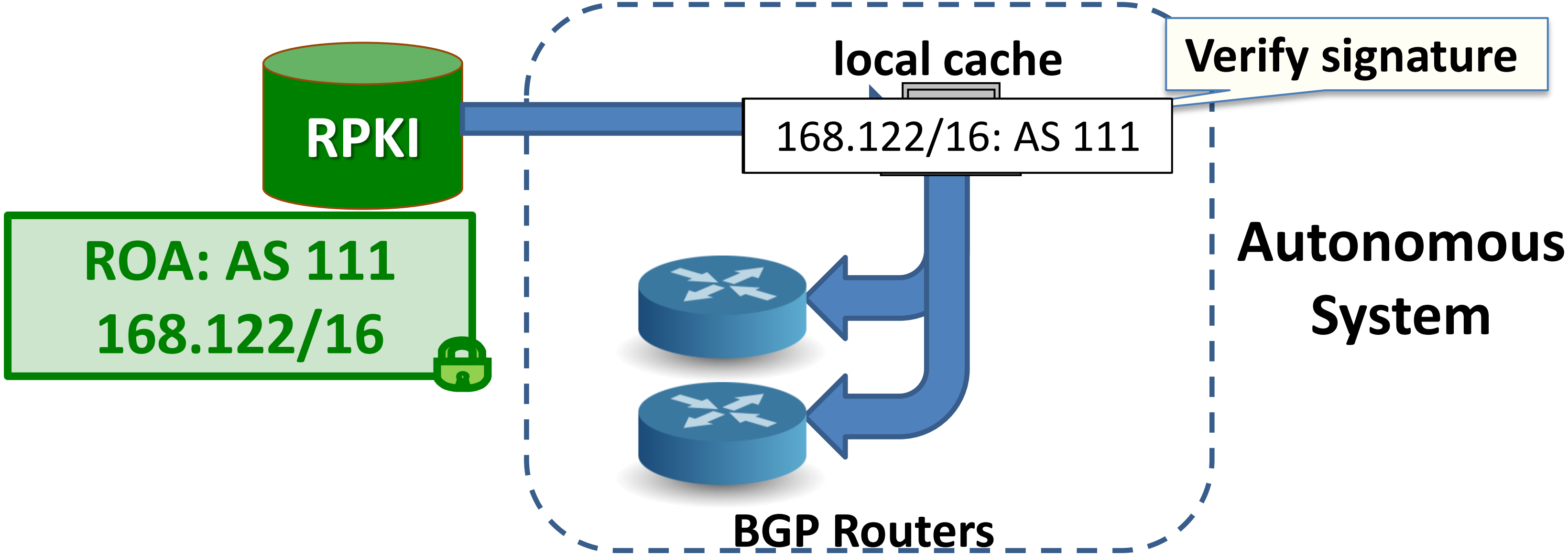
Boston University

BGP Ad.

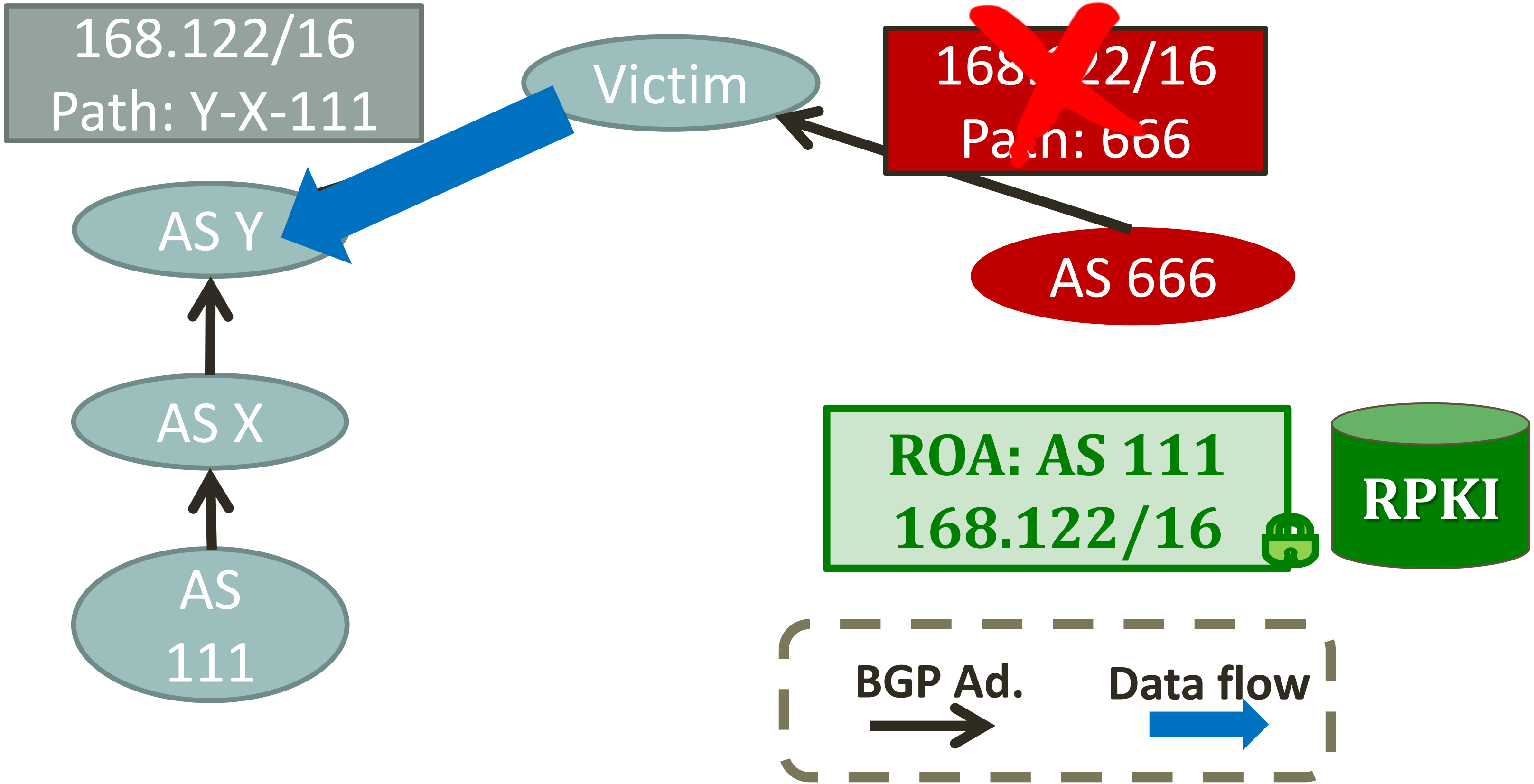
Data

Resource Public Key Infrastructure (RPKI)

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



RPKI prevents prefix hijacks



168.122/16
Path: Y-X-111

Victim

168.122/16
Path: 666

AS Y

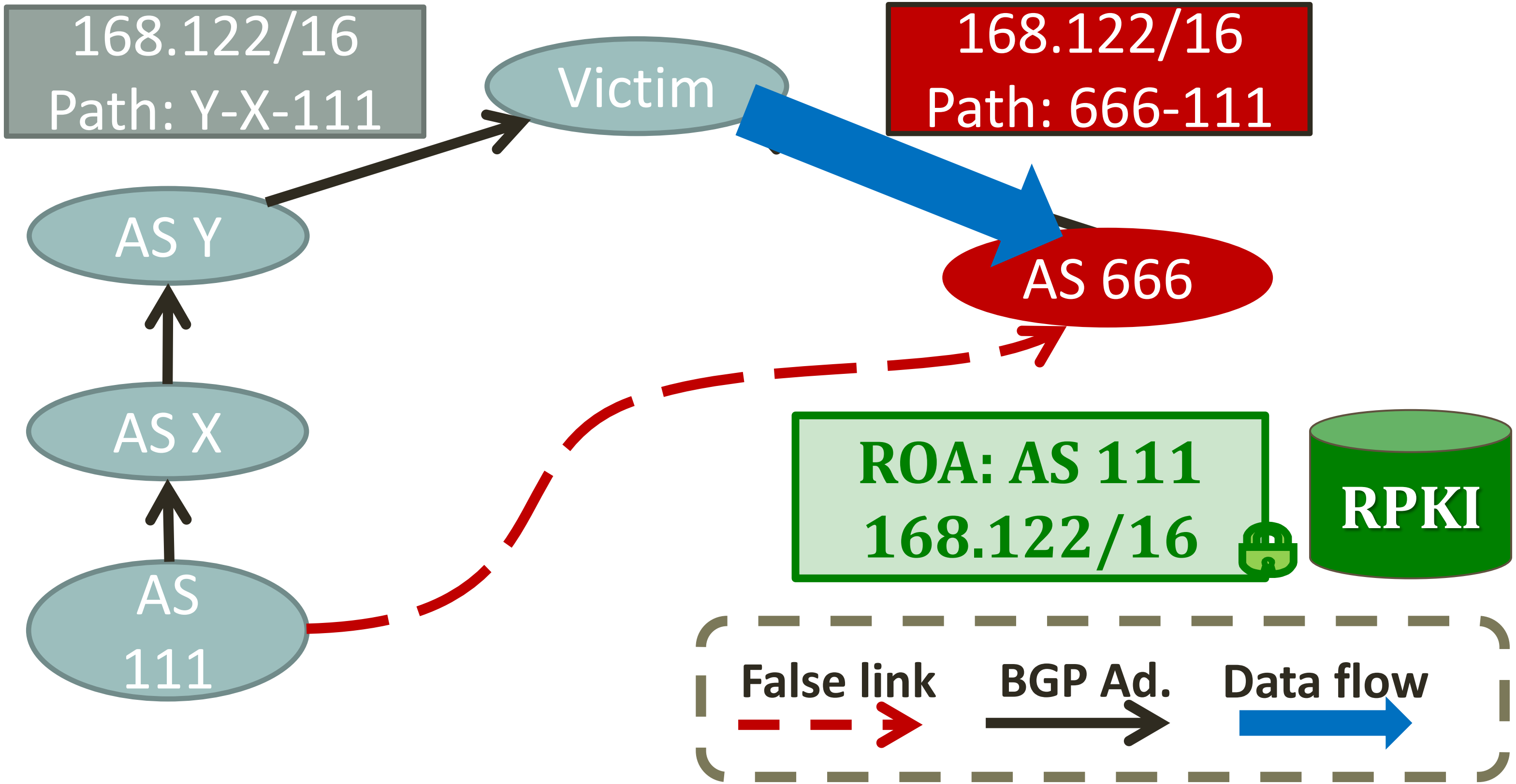
AS 666

AS X

AS 111

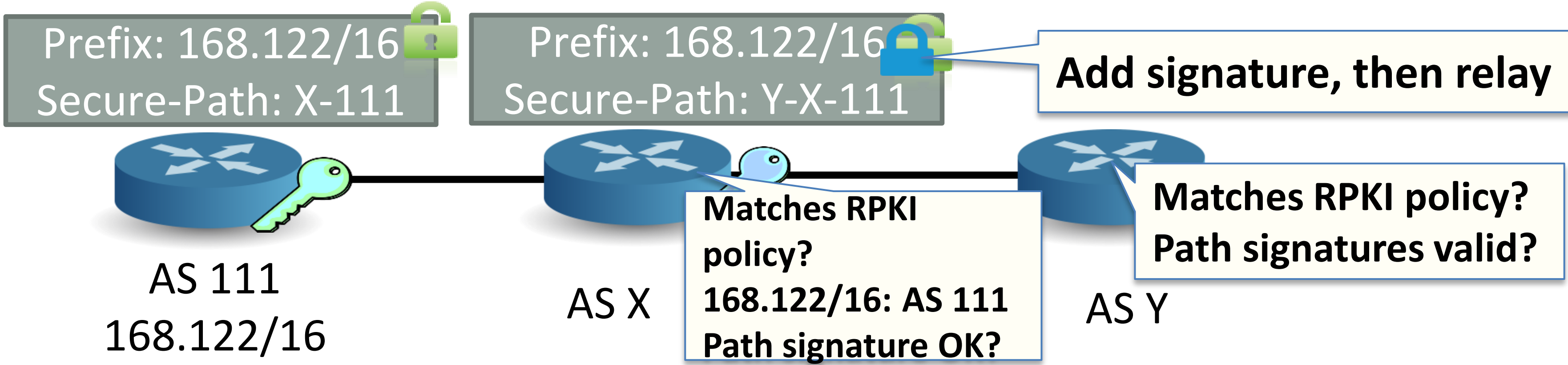
ROA: AS 111
168.122/16

Forged origin circumvents RPKI



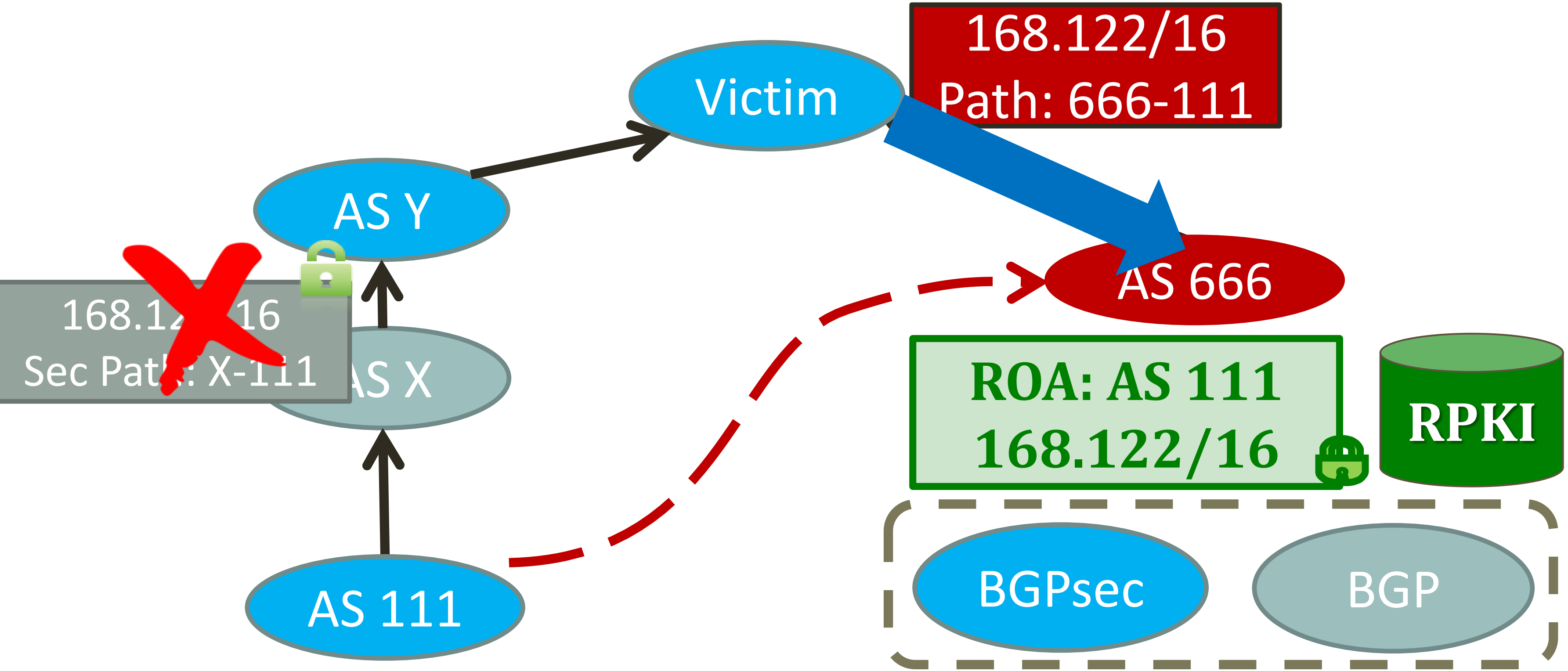
Current paradigm: a two step solution

- First, RPKI against prefix-hijacking
- Then, add BGPsec
  - Protects against false paths (e.g., next-AS attacks)
  - Deployment challenge:
    - Real-time signature and validation
    - Different message format



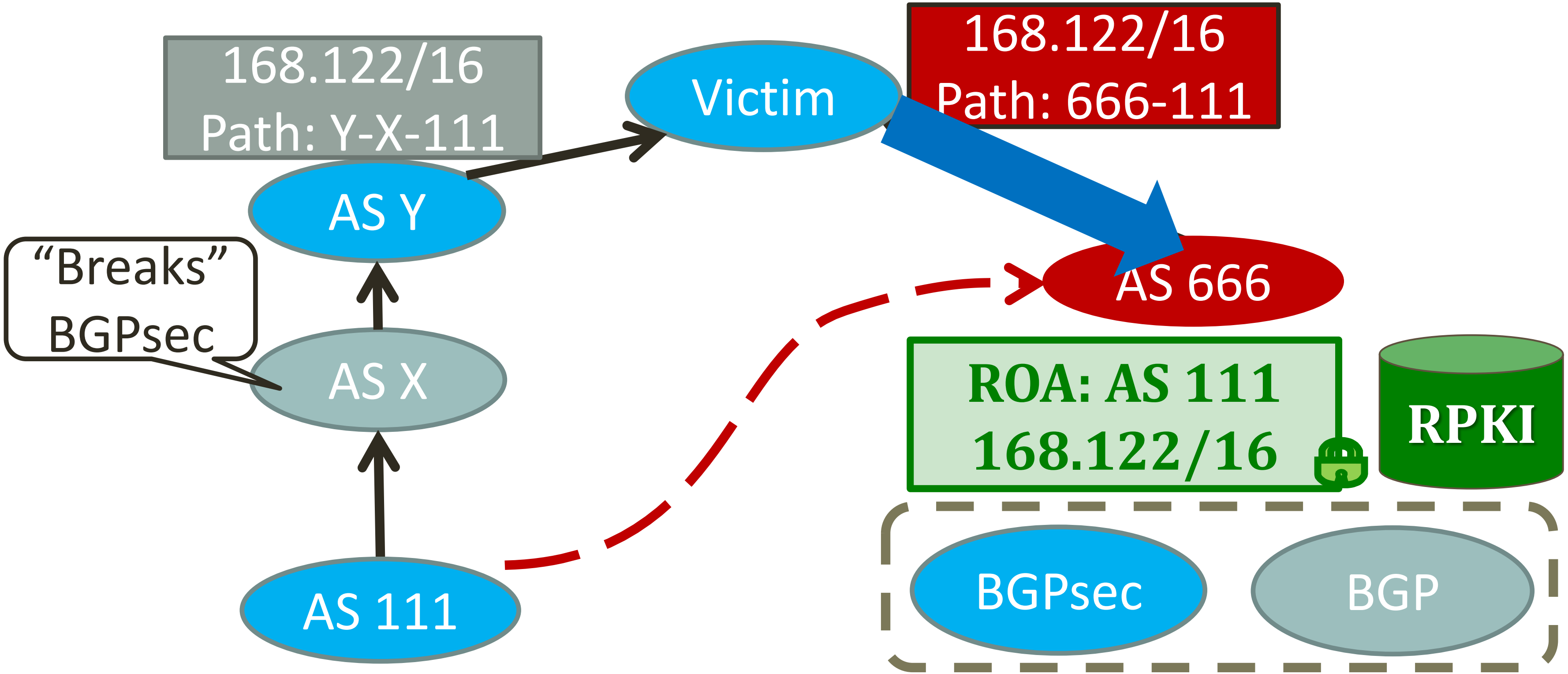
BGPsec in partial adoption?

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



BGPsec in partial adoption?

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



Our Goals

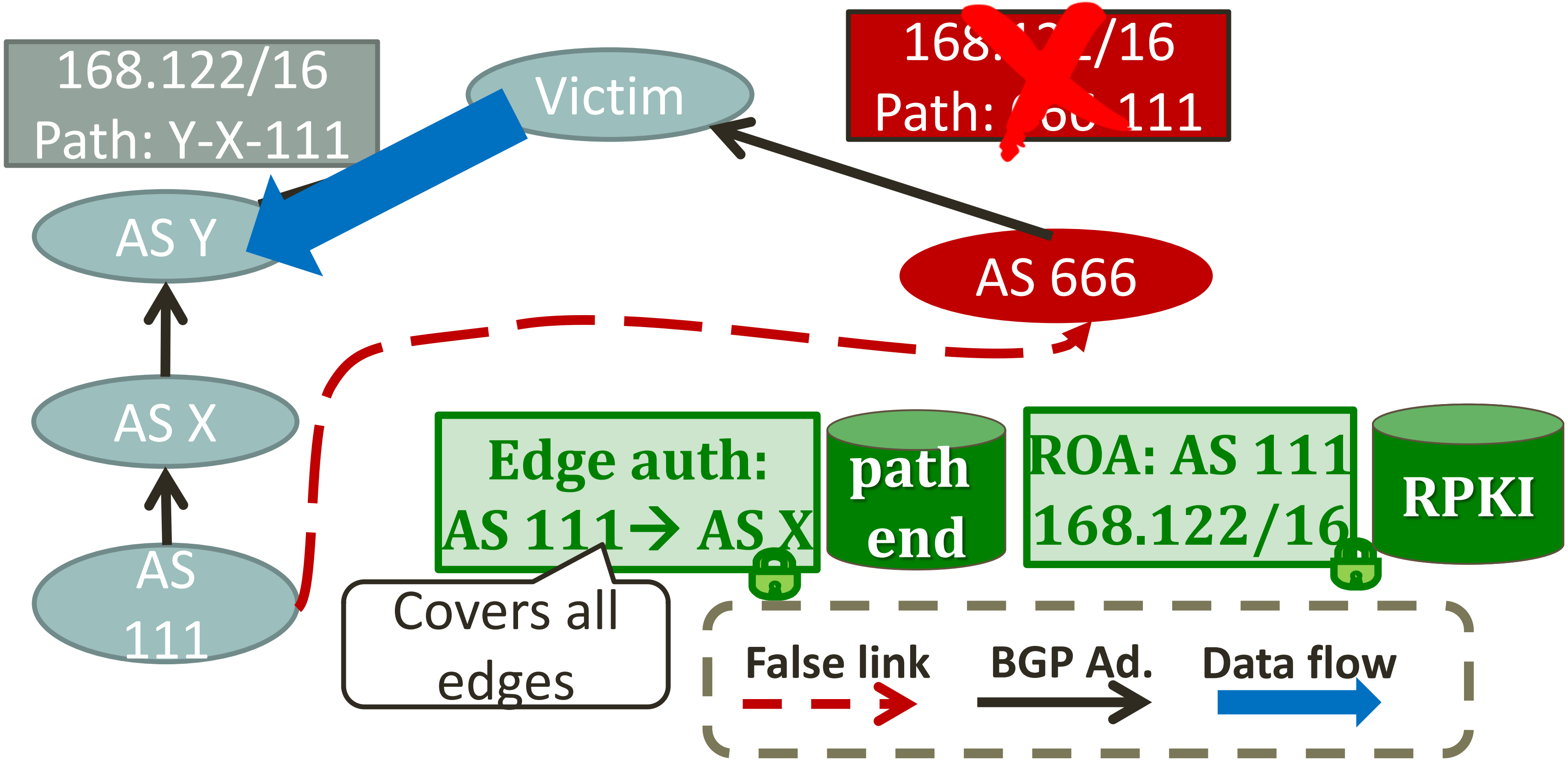
Security:

- Protect against ``false links" 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



168.122/16
Path: Y-X-111

Victim

168.122/16
Path: 666-111

AS Y

AS 666

AS X

AS 111

Edge auth:
AS 111→ AS X

path end

ROA: AS 111
168.122/16

RPKI

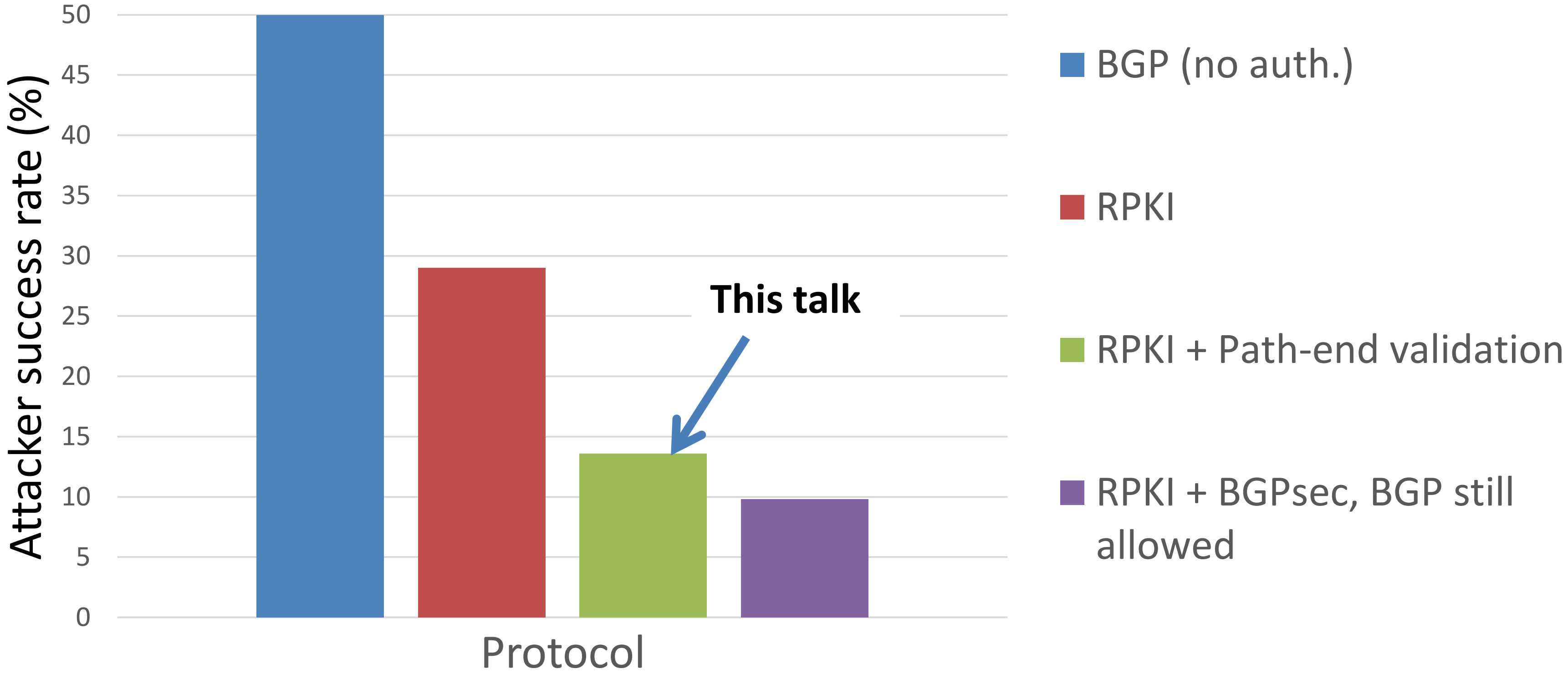
Covers all edges

False link

BGP Ad.

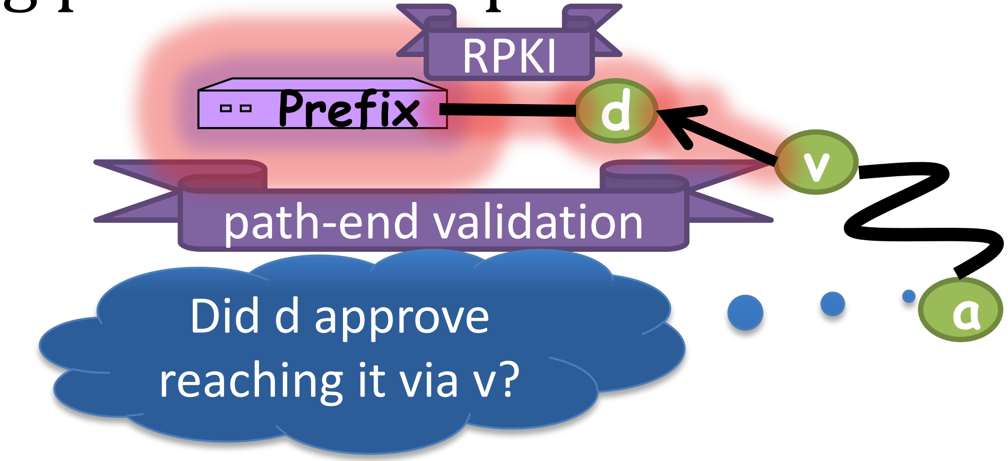
Data flow

Inter domain routing security: Mechanism comparison



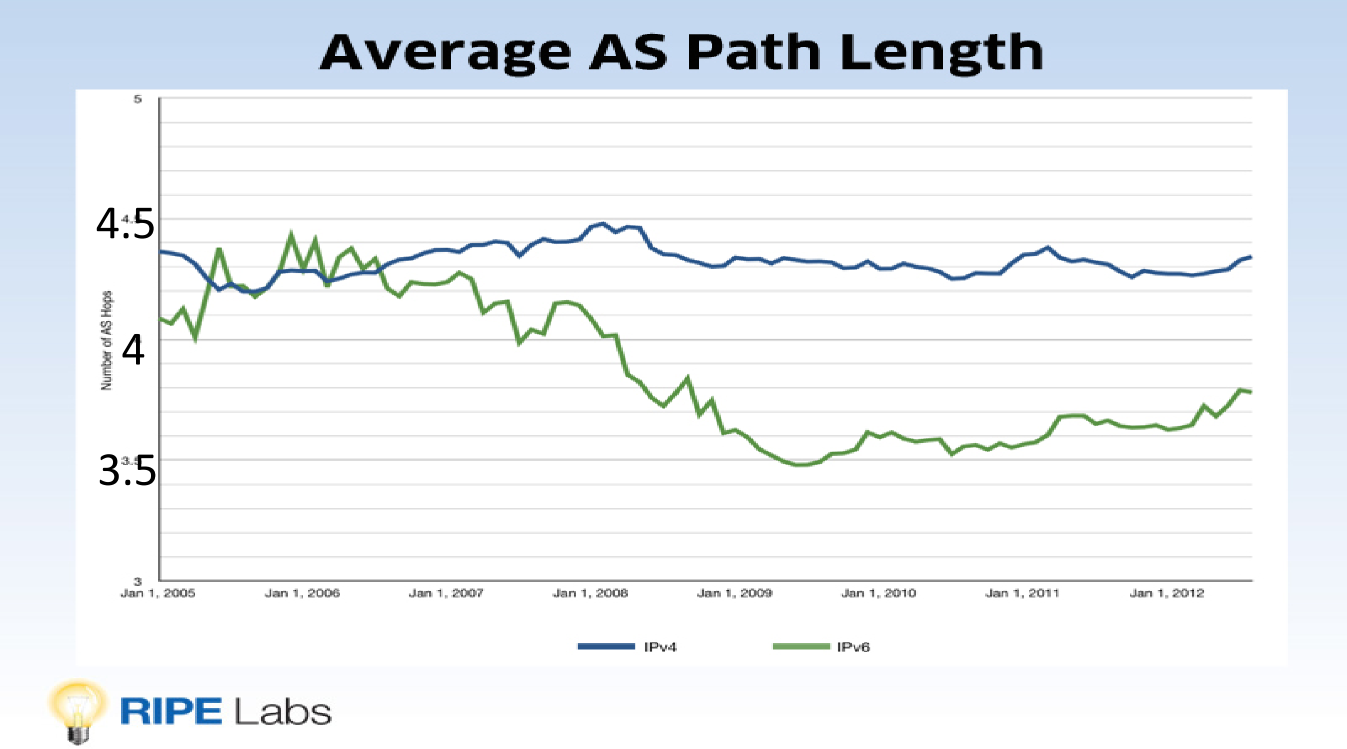
Path-end validation

- Path-end validation extends RPKI to authenticate the “last hop”
- Key insight: Securing path-suffixes provides significant benefits



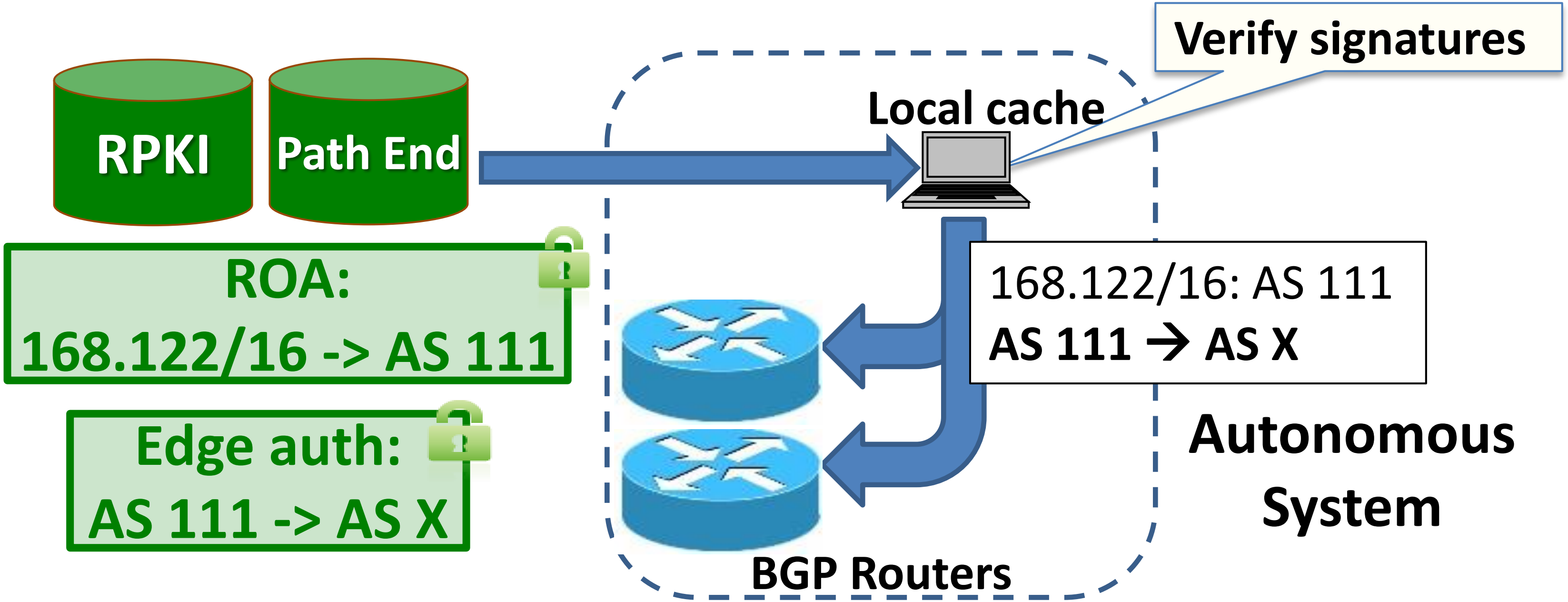
Did d approve reaching it via v?

Path-end validation



Deployment

- Similar to RPKI



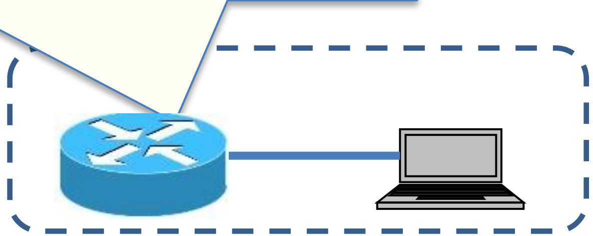
ROA:
168.122/16 -> AS 111

Edge auth:
AS 111 -> AS X

168.122/16: AS 111
AS 111 → AS X

Deployment

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



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

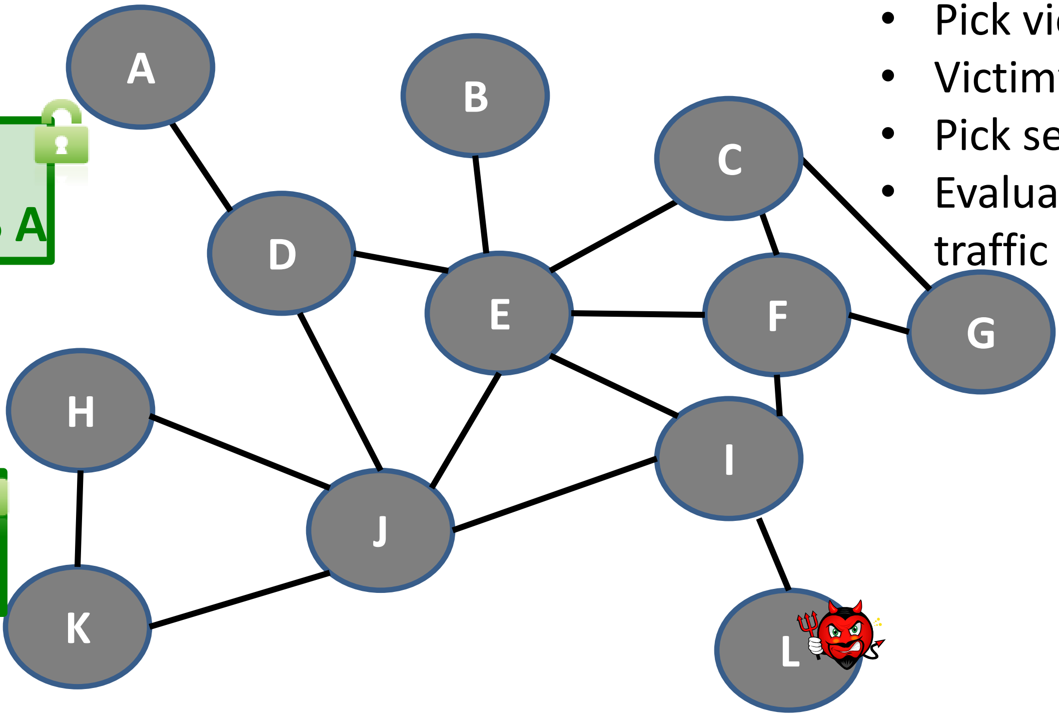
Security in partial adoption: Simulation framework

RPKI

ROA:
1.2.0.0/16 → AS A

Path End

Edge auth:
AS A → AS D

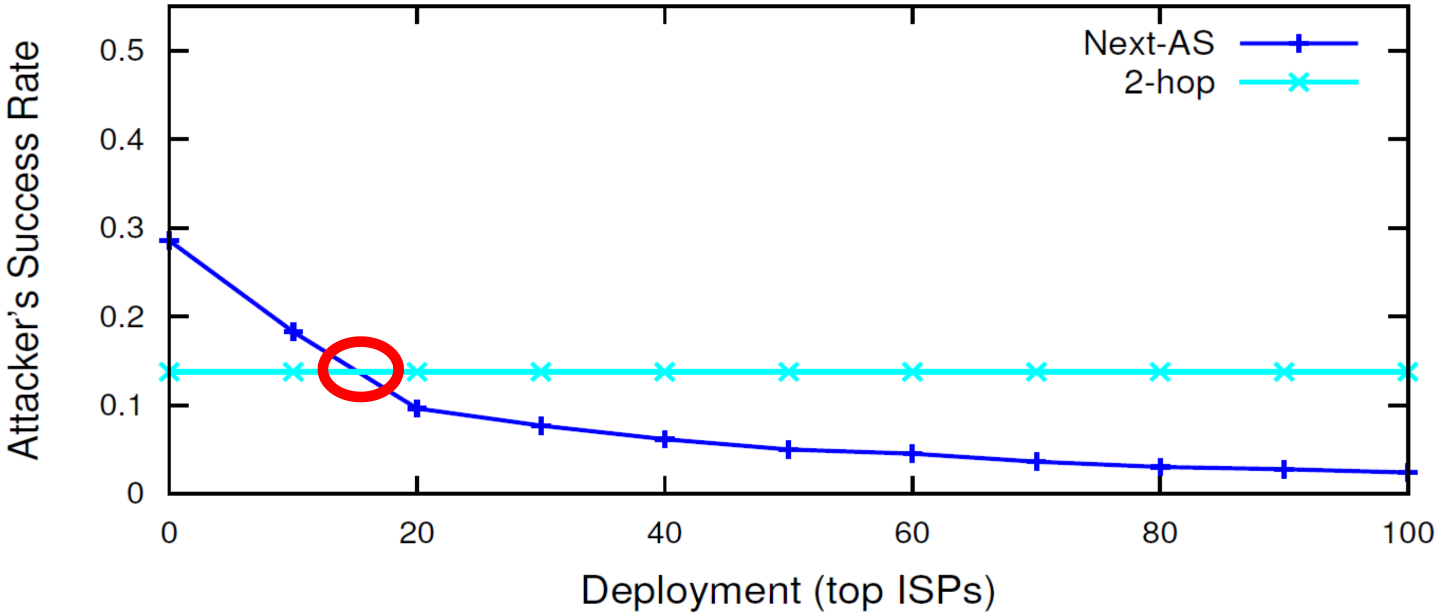


- Pick victim & attacker
- Victim’s prefix has a ROA+EA
- Pick set of filtering ASes
- Evaluate which ASes send traffic to the attacker

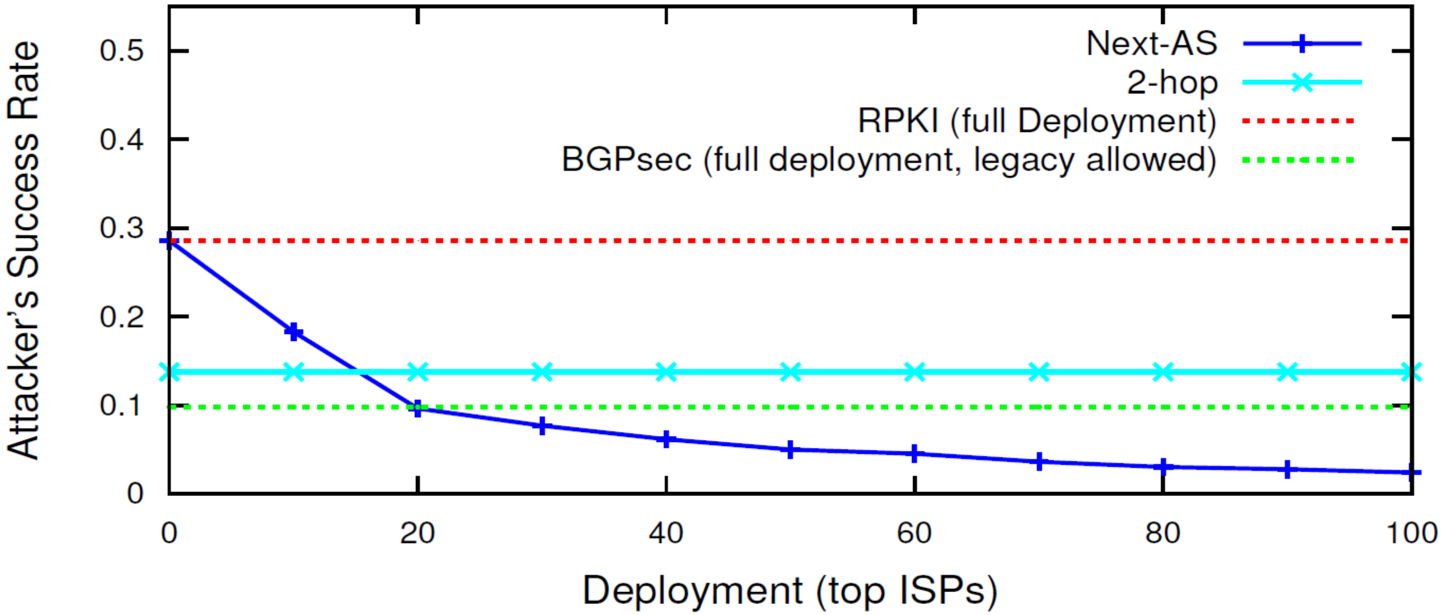
Empirically-derived AS-level network from CAIDA

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

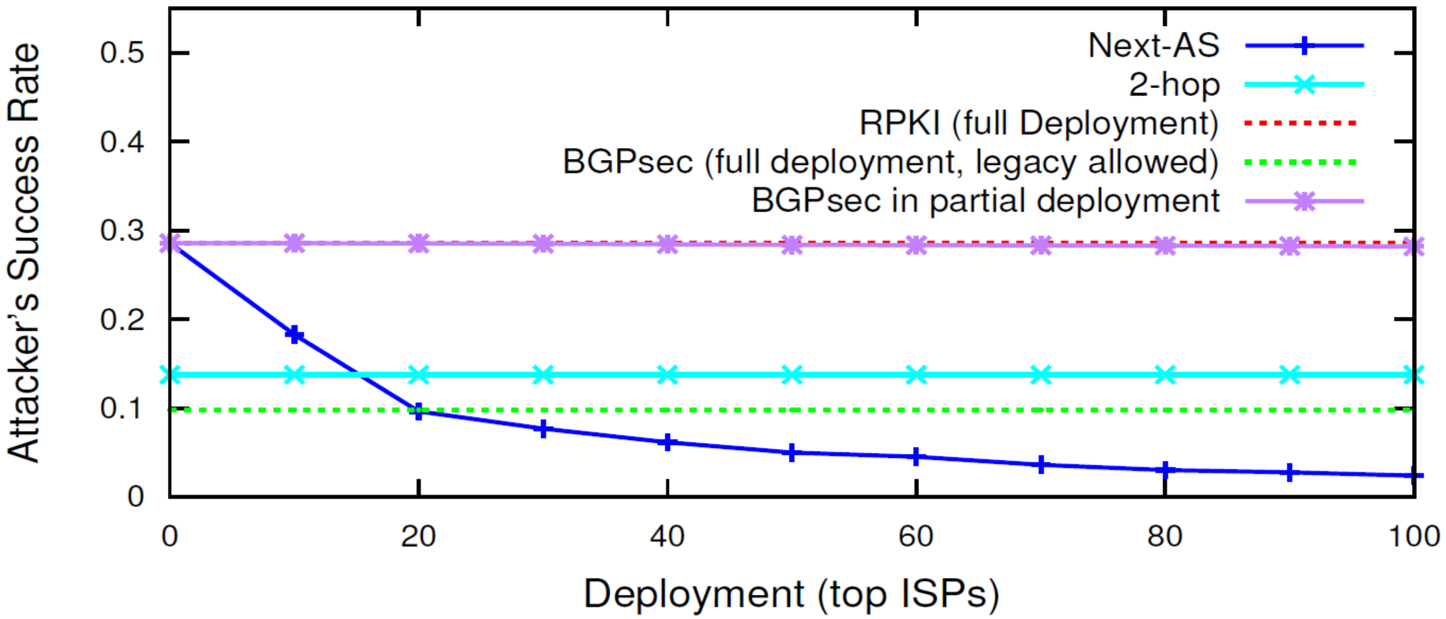
Simulation results



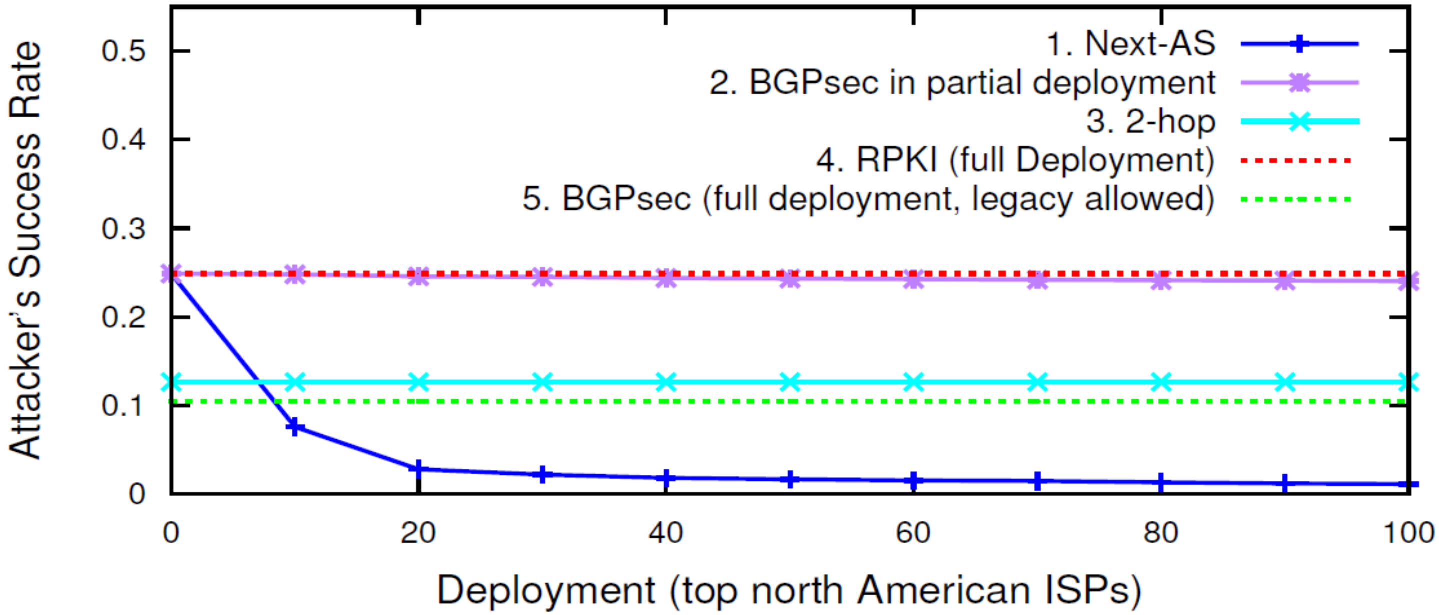
Simulation results



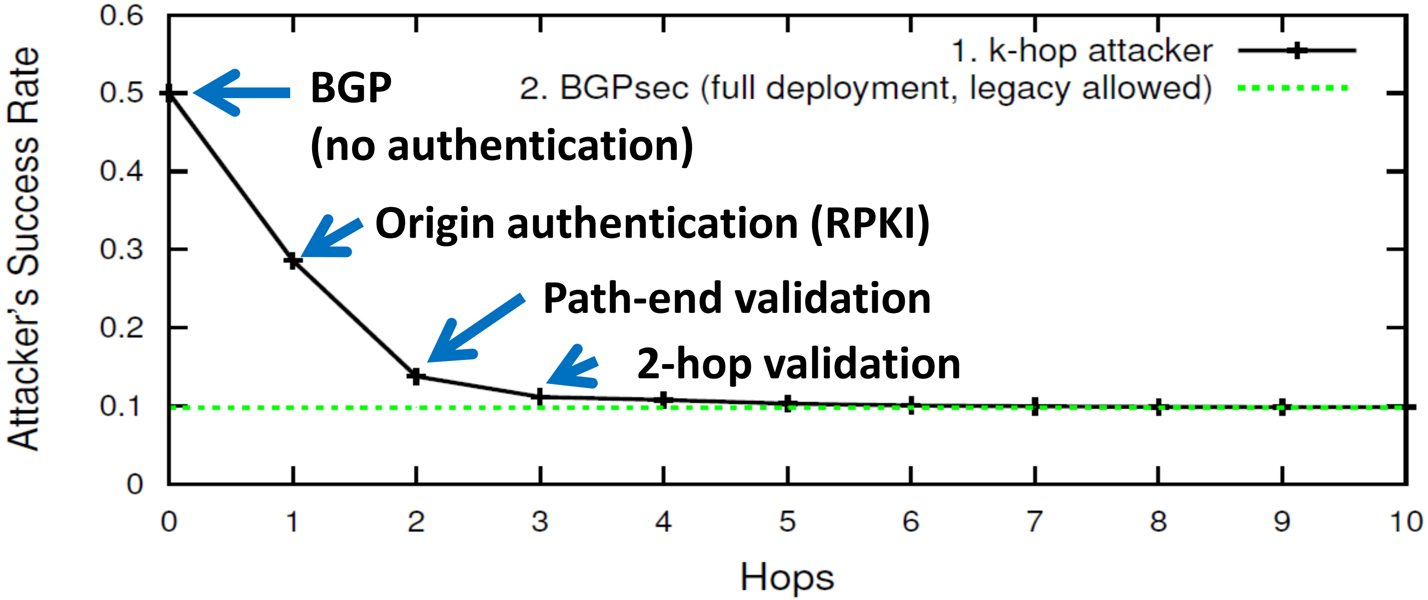
Simulation results



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