Are We There Yet?
On RPKI Deployment and Security

Yossi Gilad

joint work with: Avichai Cohen,

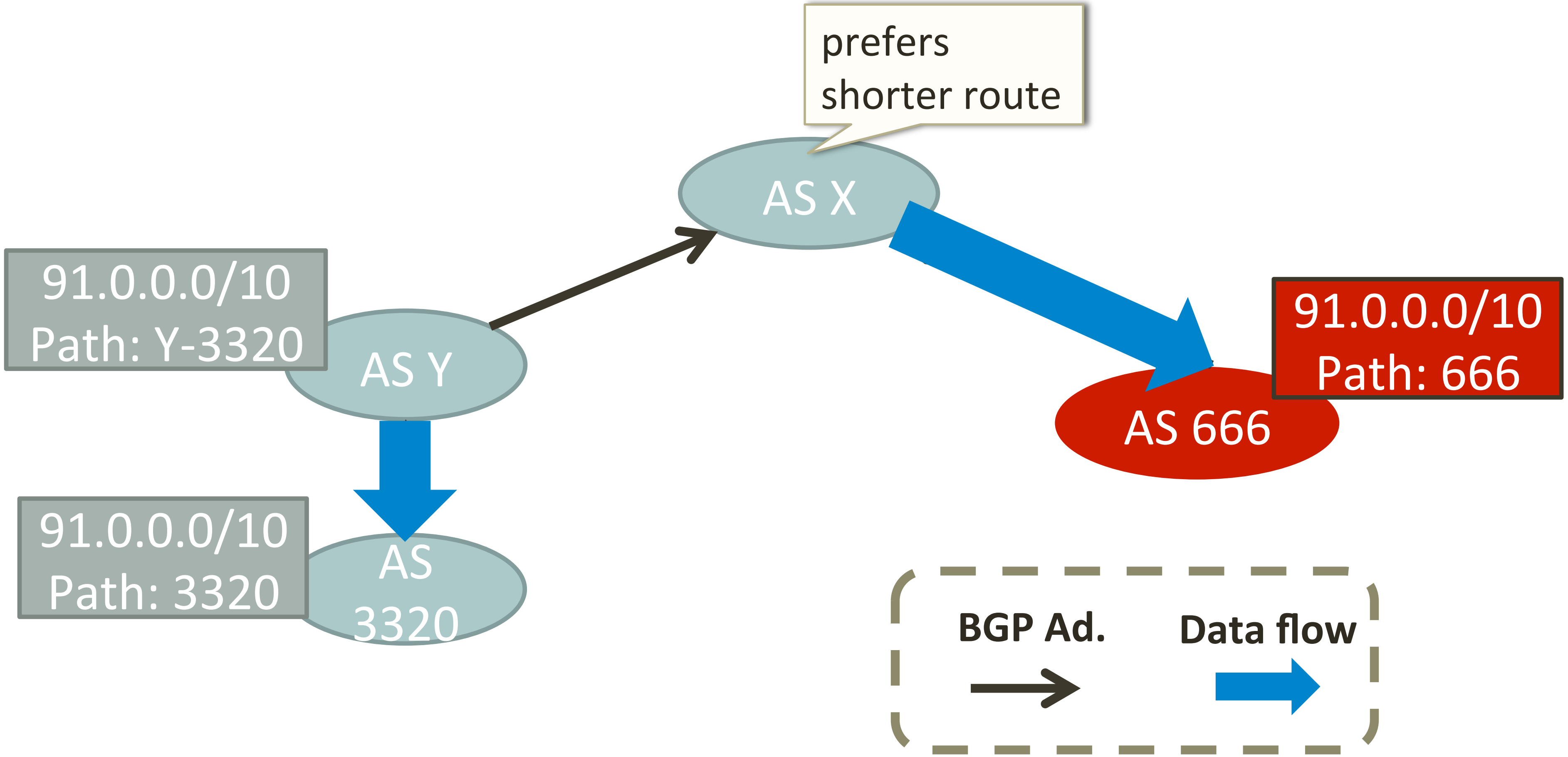
Amir Herzberg, Michael Schapira, Haya Shulman

The Resource Public Key Infrastructure

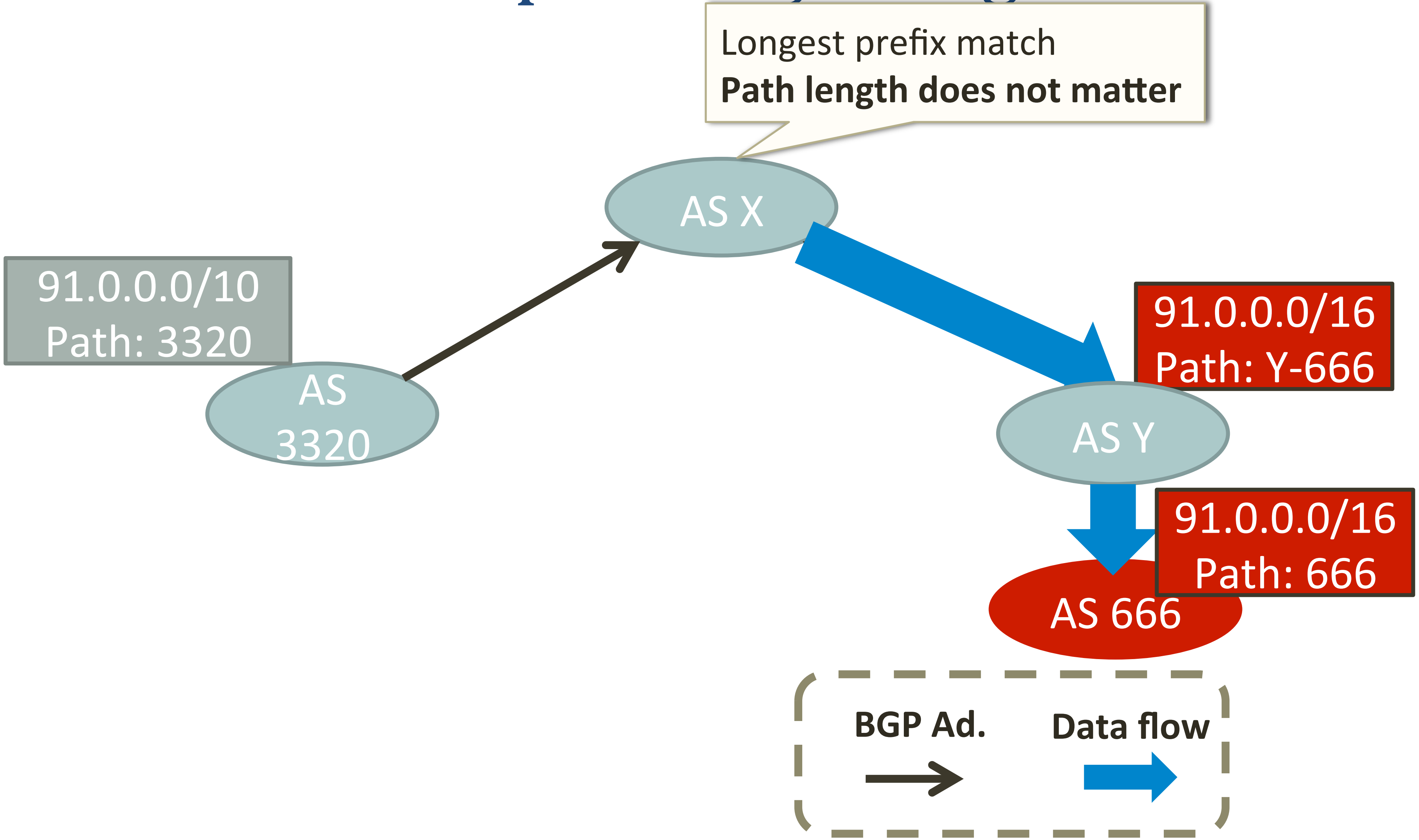
- Intended to **prevent** prefix/subprefix hijacks

- Lays the **foundation** for protection against more sophisticated attacks on interdomain routing
  - BGPsec, SoBGP,…

Prefix Hijacking



Subprefix Hijacking



Longest prefix match

Path length does not matter

Certifying Ownership with RPKI

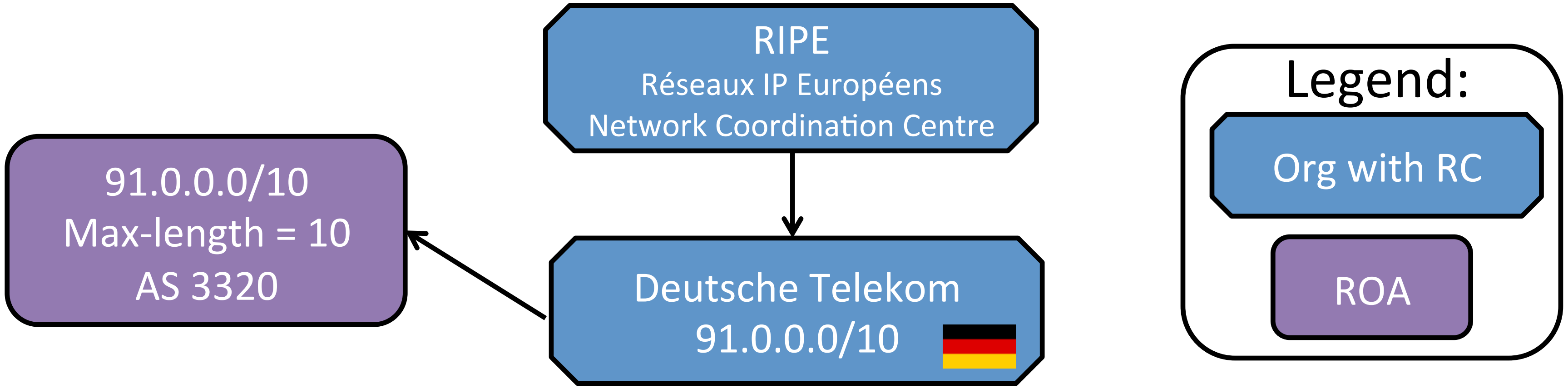
- RPKI assigns an IP prefix to a public key via a Resource Certificate (RC)

- Owners can use their private key to issue a Route Origin Authorization (ROA)

- ROAs identify ASes authorized to advertise an IP prefix in BGP

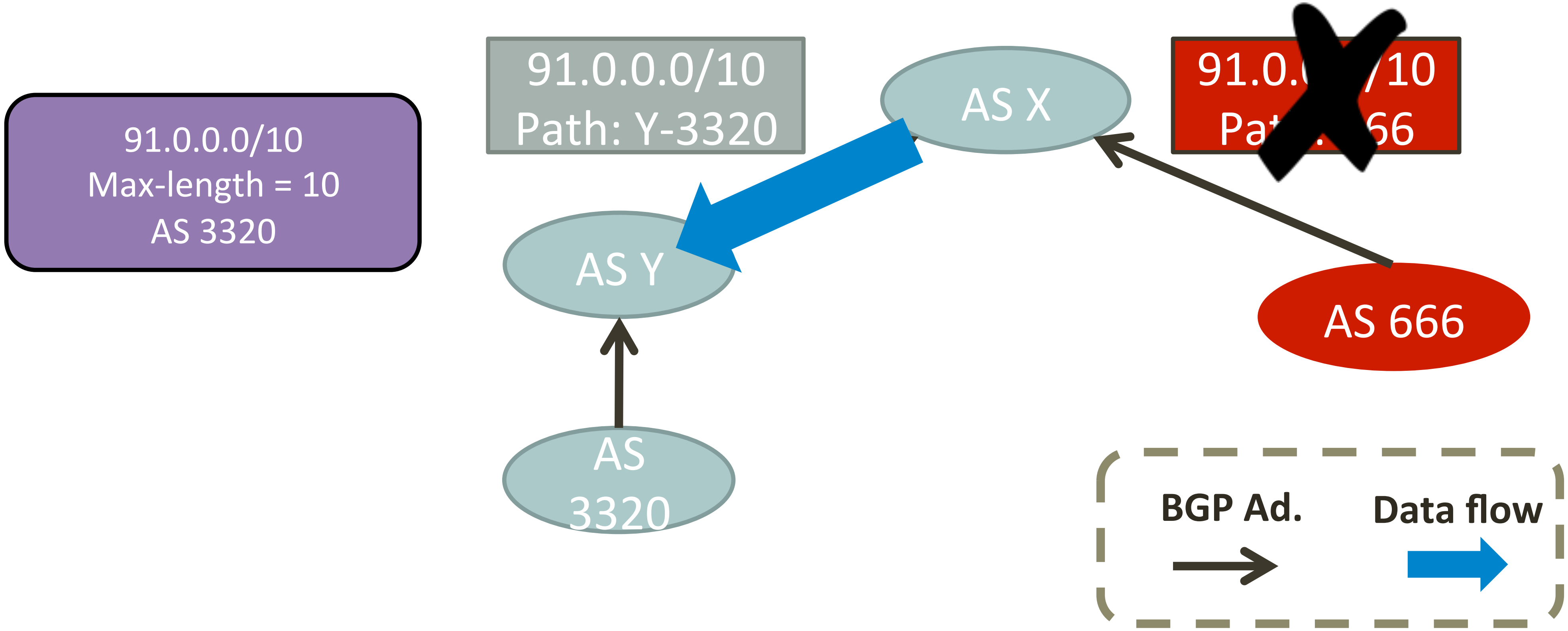
Example: Certifying Ownership

Deutsche Telekom certified by RIPE
for address space 91.0.0.0/10



RPKI Can Prevent Prefix Hijacks

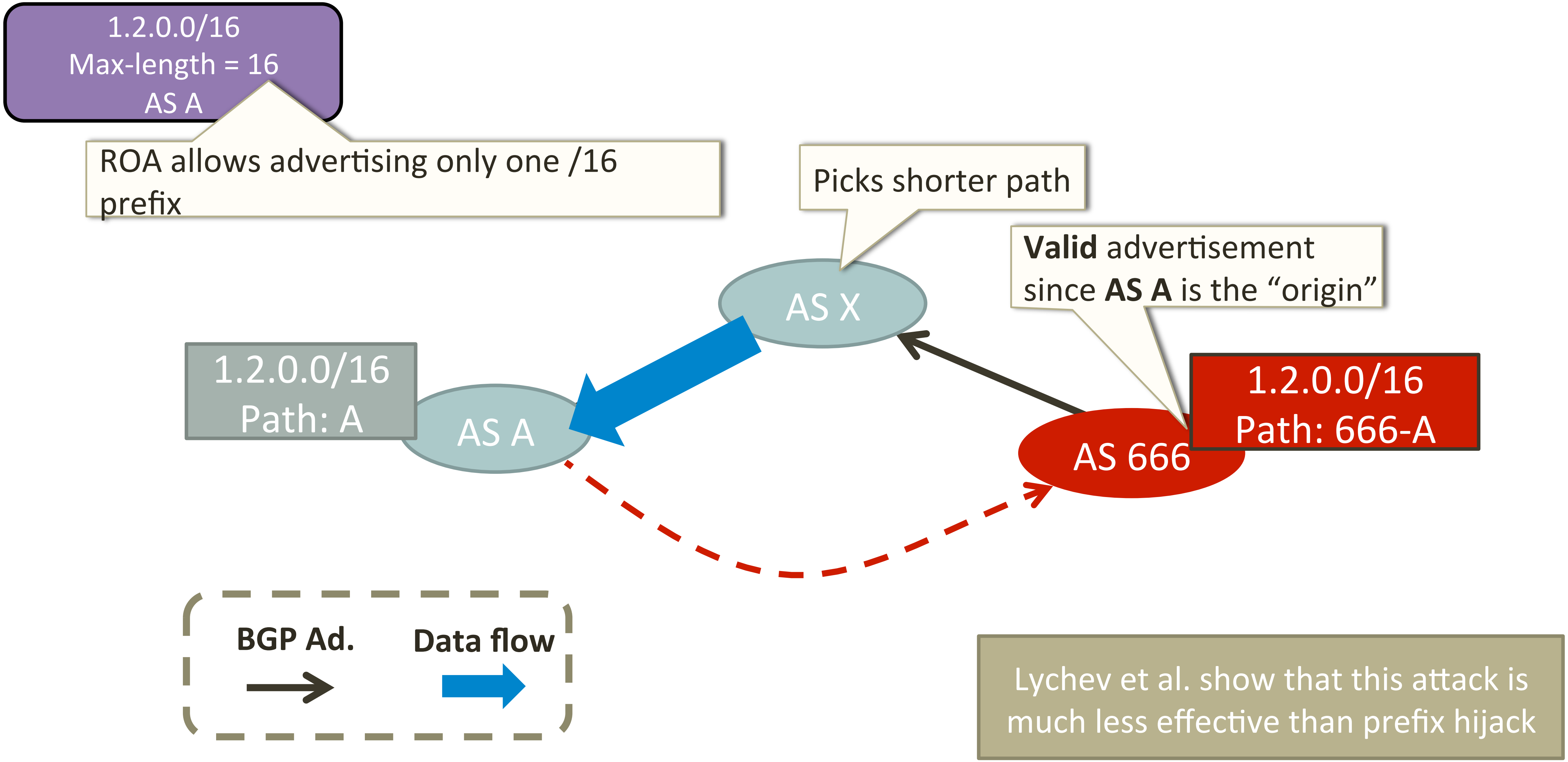
AS X uses the authenticated mapping (ROA) from 91.0/10 to AS 3320 to discard the attacker’s route-advertisement



Talk Outline

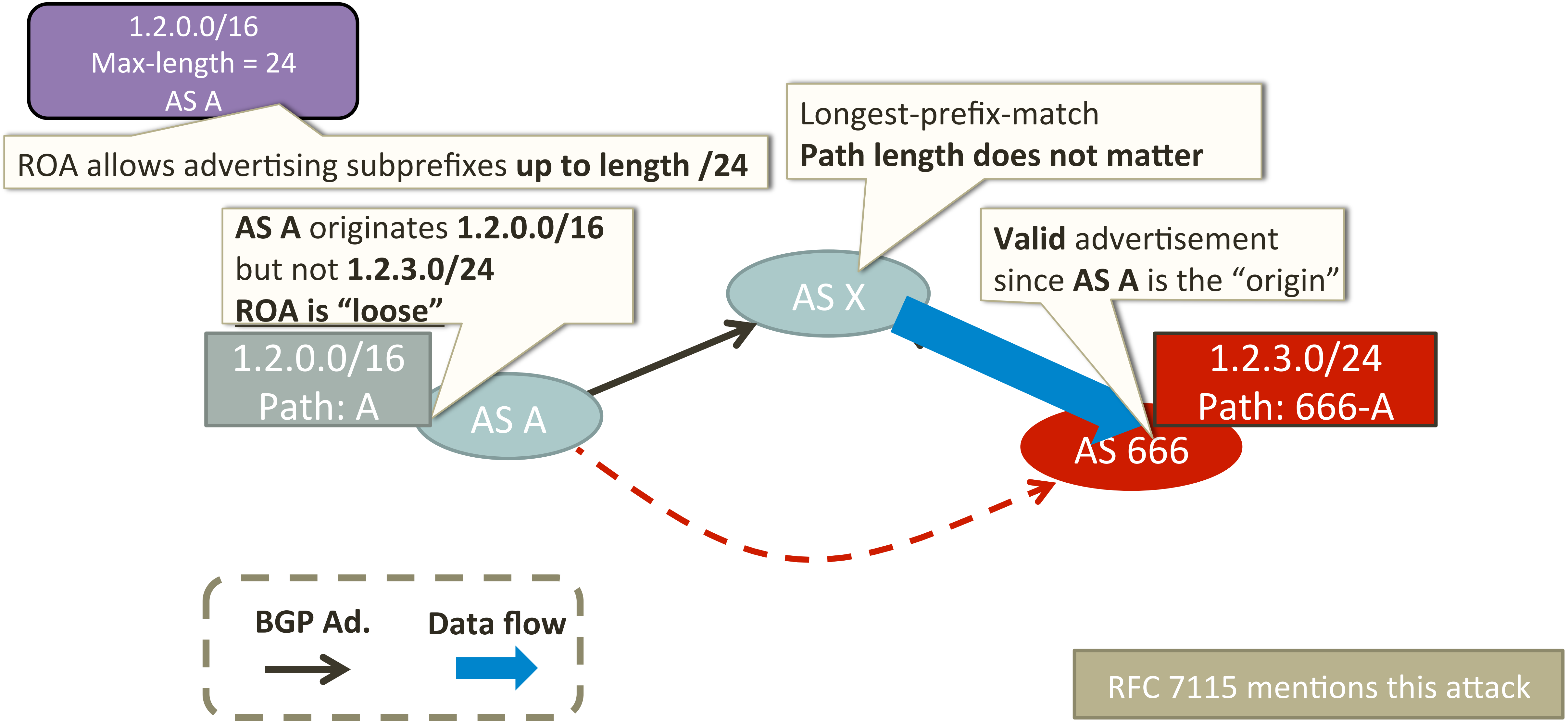
- **Challenges facing deployment**
- Route origin validation in partial deployment

Insecure Deployment: Loose ROAs



Lychev et al. show that this attack is much less effective than prefix hijack

Insecure Deployment: Loose ROAs



Insecure Deployment: Loose ROAs

- Loose ROAs are <u>common</u>!
  - almost 30% of IP prefixes in ROAs
  - 89% of prefixes with maxLen > prefixLen
  - manifests even in large providers!

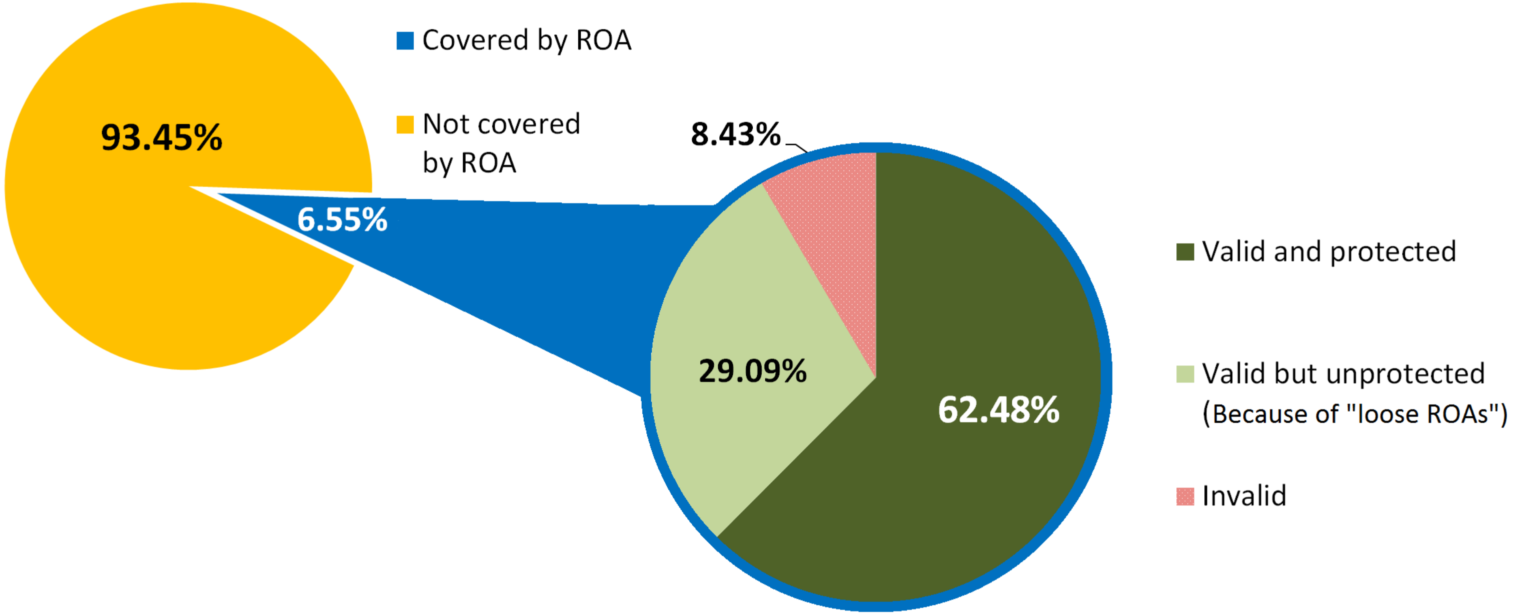
- Attacker can hijack **<u>all</u>** traffic to non-advertised subprefixes covered by a loose ROA

- Vulnerability will be solved only when BGPsec is fully deployed, but a long way to go until then…
  - <u>better not to issue loose ROAs!</u>

Challenges to Deployment: Human Error

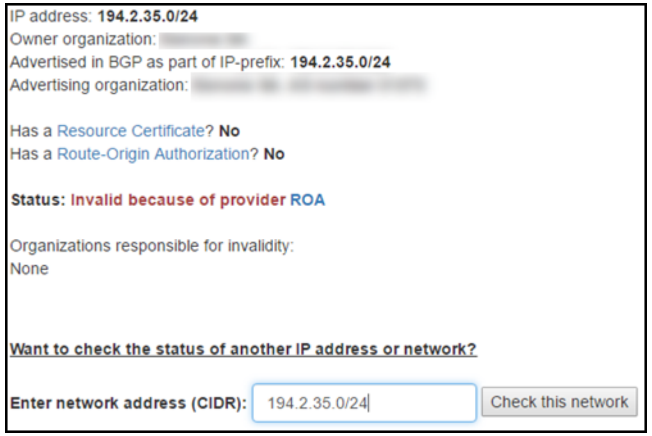
Many other mistakes in ROAs (see RPKI monitor)

- ``bad ROAs'' cause legitimate prefixes to appear invalid
- filtering by ROAs may cause disconnection from legitimate destinations
- extensive measurements in [Iamartino et al., PAM'15]



Improving Accuracy with ROAlert

- roalert.org allows you to check whether your network is properly protected by ROAs
- … and if not, why not


IP address: **194.2.35.0/24**
Owner organization: [redacted]
Advertised in BGP as part of IP-prefix: **194.2.35.0/24**
Advertising organization: [redacted]

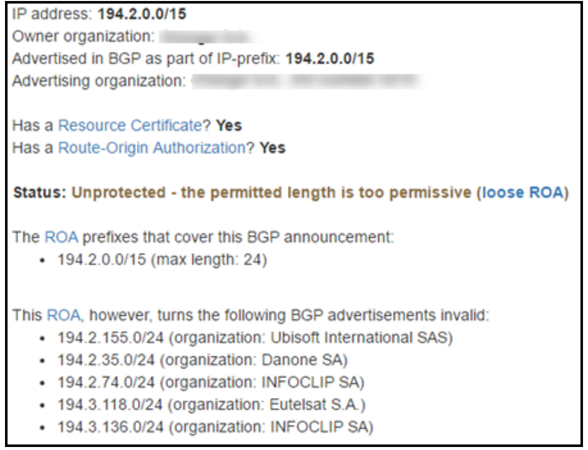
Has a Resource Certificate? **No**
Has a Route-Origin Authorization? **No**

Status: Invalid because of provider ROA

Organizations responsible for invalidity:
None

Want to check the status of another IP address or network?

Enter network address (CIDR): 194.2.35.0/24 Check this network

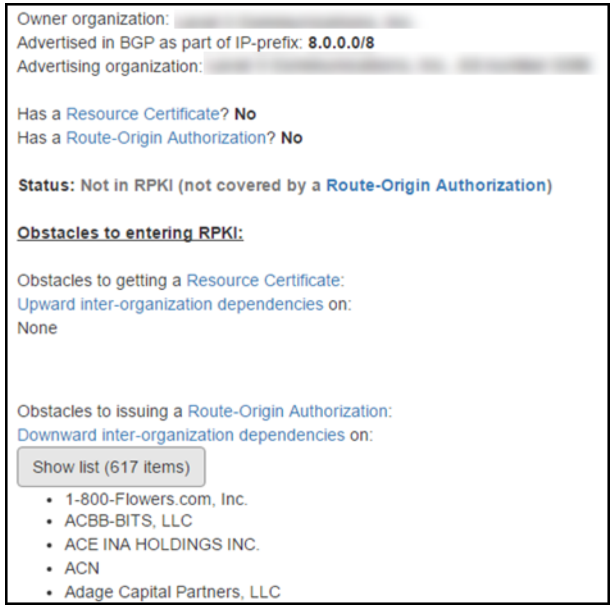

IP address: **194.2.0.0/15**
Owner organization: [redacted]
Advertised in BGP as part of IP-prefix: **194.2.0.0/15**
Advertising organization: [redacted]

Has a Resource Certificate? **Yes**
Has a Route-Origin Authorization? **Yes**

Status: Unprotected - the permitted length is too permissive (loose ROA)

The ROA prefixes that cover this BGP announcement:
- 194.2.0.0/15 (max length: 24)

This ROA, however, turns the following BGP advertisements invalid:
- 194.2.155.0/24 (organization: Ubisoft International SAS)
- 194.2.35.0/24 (organization: Danone SA)
- 194.2.74.0/24 (organization: INFOCLIP SA)
- 194.3.118.0/24 (organization: Eutelsat S.A.)
- 194.3.136.0/24 (organization: INFOCLIP SA)


Owner organization: [redacted]
Advertised in BGP as part of IP-prefix: **8.0.0.0/8**
Advertising organization: [redacted]

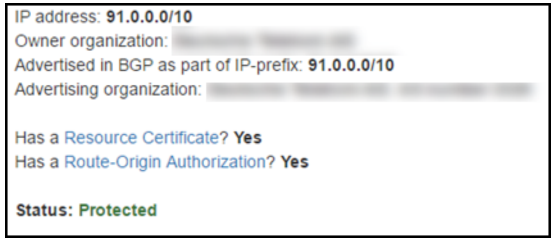
Has a Resource Certificate? **No**
Has a Route-Origin Authorization? **No**

Status: Not in RPKI (not covered by a Route-Origin Authorization)

Obstacles to entering RPKI:

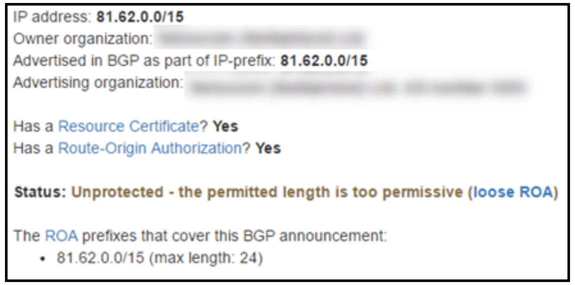
Obstacles to getting a Resource Certificate:
Upward inter-organization dependencies on:
None

Obstacles to issuing a Route-Origin Authorization:
Downward inter-organization dependencies on:
Show list (617 items)
- 1-800-Flowers.com, Inc.
- ACBB-BITS, LLC
- ACE INA HOLDINGS INC.
- ACN
- Adage Capital Partners, LLC


IP address: **91.0.0.0/10**
Owner organization: [redacted]
Advertised in BGP as part of IP-prefix: **91.0.0.0/10**
Advertising organization: [redacted]

Has a Resource Certificate? **Yes**
Has a Route-Origin Authorization? **Yes**

Status: Protected


IP address: **81.62.0.0/15**
Owner organization: [redacted]
Advertised in BGP as part of IP-prefix: **81.62.0.0/15**
Advertising organization: [redacted]

Has a Resource Certificate? **Yes**
Has a Route-Origin Authorization? **Yes**

Status: Unprotected - the permitted length is too permissive (loose ROA)

The ROA prefixes that cover this BGP announcement:
- 81.62.0.0/15 (max length: 24)

Improving Accuracy with ROAlert

- Online, proactive notification system
- Retrieves ROAs from the RPKI and compares them against BGP advertisements
- Alerts network operators about “loose ROAs” & “bad ROAs”

Improving Accuracy with ROAlert

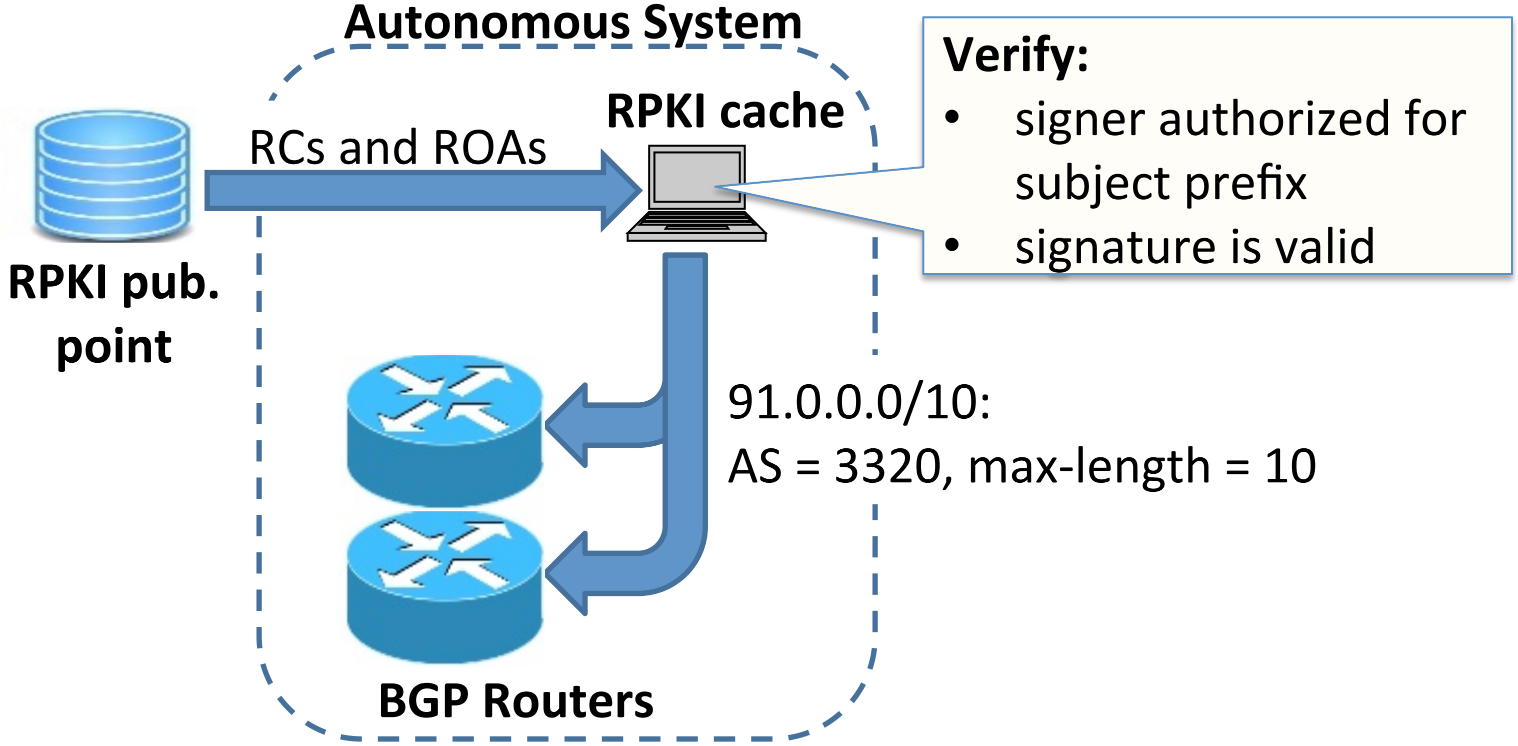
- Initial results are promising!
  - notifications reached 168 operators
  - 42% of errors were fixed within a month
- ROAlert is:
  - constantly monitoring (not only at registration)
  - not opt-in
- We advocate that ROAlert be adopted and adapted by RIRs!

Talk Outline

- Challenges facing deployment
- **Route origin validation in partial deployment**

Filtering Bogus Advertisements

Route-Origin Validation (ROV):
use ROAs to discard/deprioritize route-advertisements from unauthorized origins [RFC 6811]



Verify:

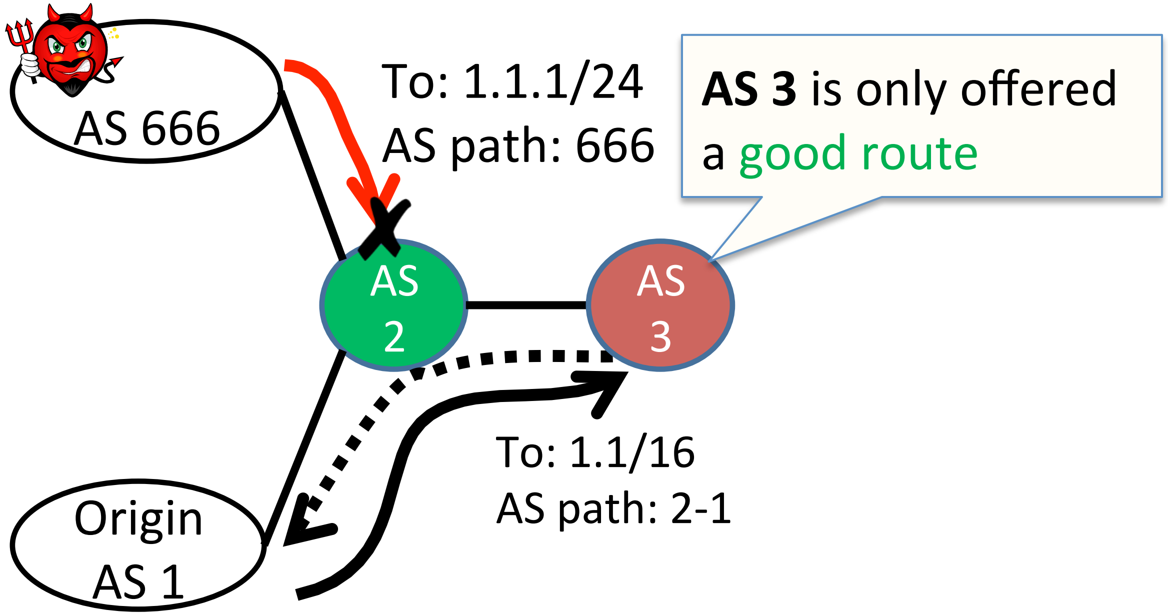
- signer authorized for subject prefix
- signature is valid

91.0.0.0/10:
AS = 3320, max-length = 10

What is the Impact of Partial ROV Adoption?

- Collateral benefit:
  - Adopters protect ASes behind them by discarding invalid routes

1.1.0.0/16
Max-length = 16
AS 1



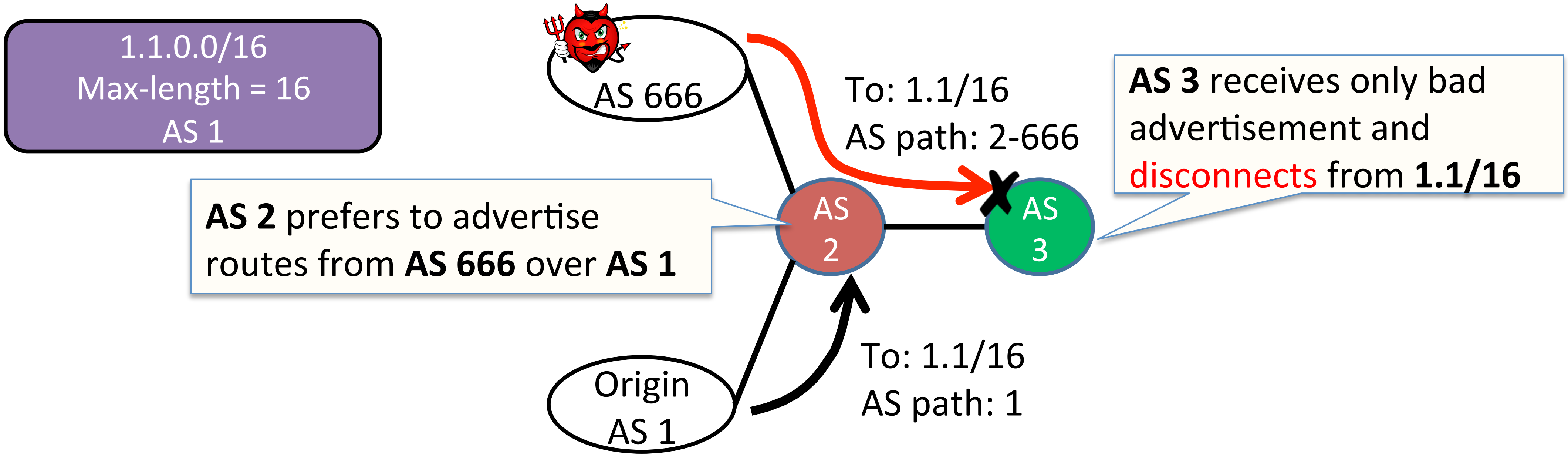
To: 1.1.1/24
AS path: 666

AS 3 is only offered a good route

To: 1.1/16
AS path: 2-1

What is the Impact of Partial ROV Adoption?

- Collateral damage: ASes not doing ROV might cause ASes that do ROV to fall victim to attacks!
  - Disconnection: Adopters might be offered only bad routes



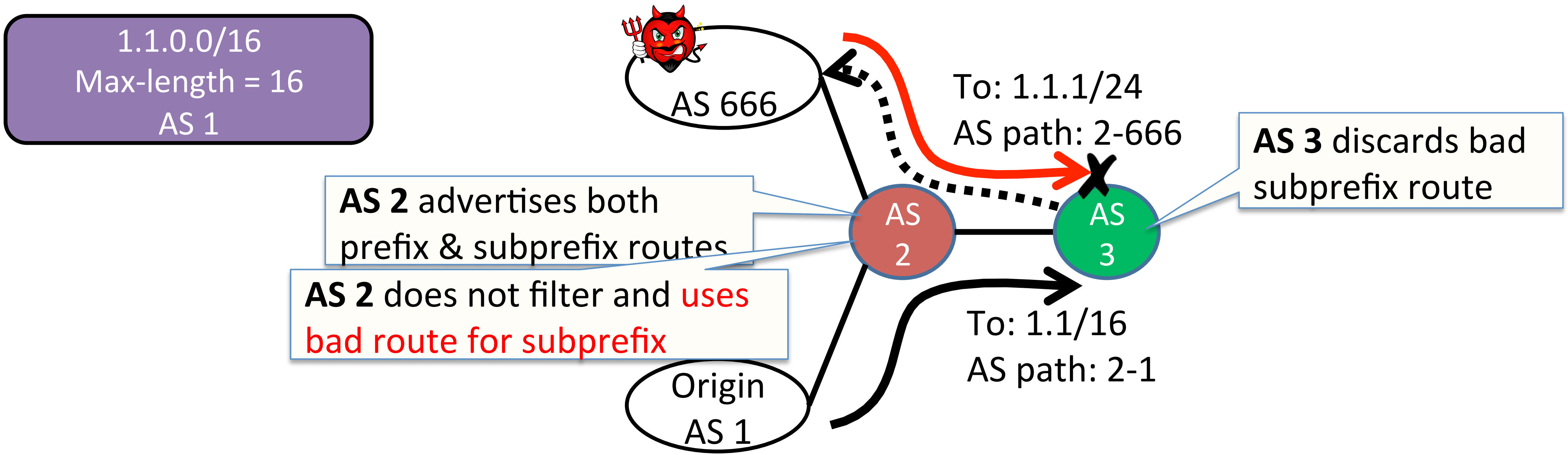
1.1.0.0/16
Max-length = 16
AS 1

AS 2 prefers to advertise routes from **AS 666** over **AS 1**

AS 3 receives only bad advertisement and disconnects from **1.1/16**

What is the Impact of Partial ROV Adoption?

- Collateral damage: ASes not doing ROV might cause ASes that do ROV to fall victim to attacks!
  - Control-Plane-Data-Plane Mismatch! data flows to attacker, although AS 3 discarded it



1.1.0.0/16
Max-length = 16
AS 1

AS 2 advertises both prefix & subprefix routes

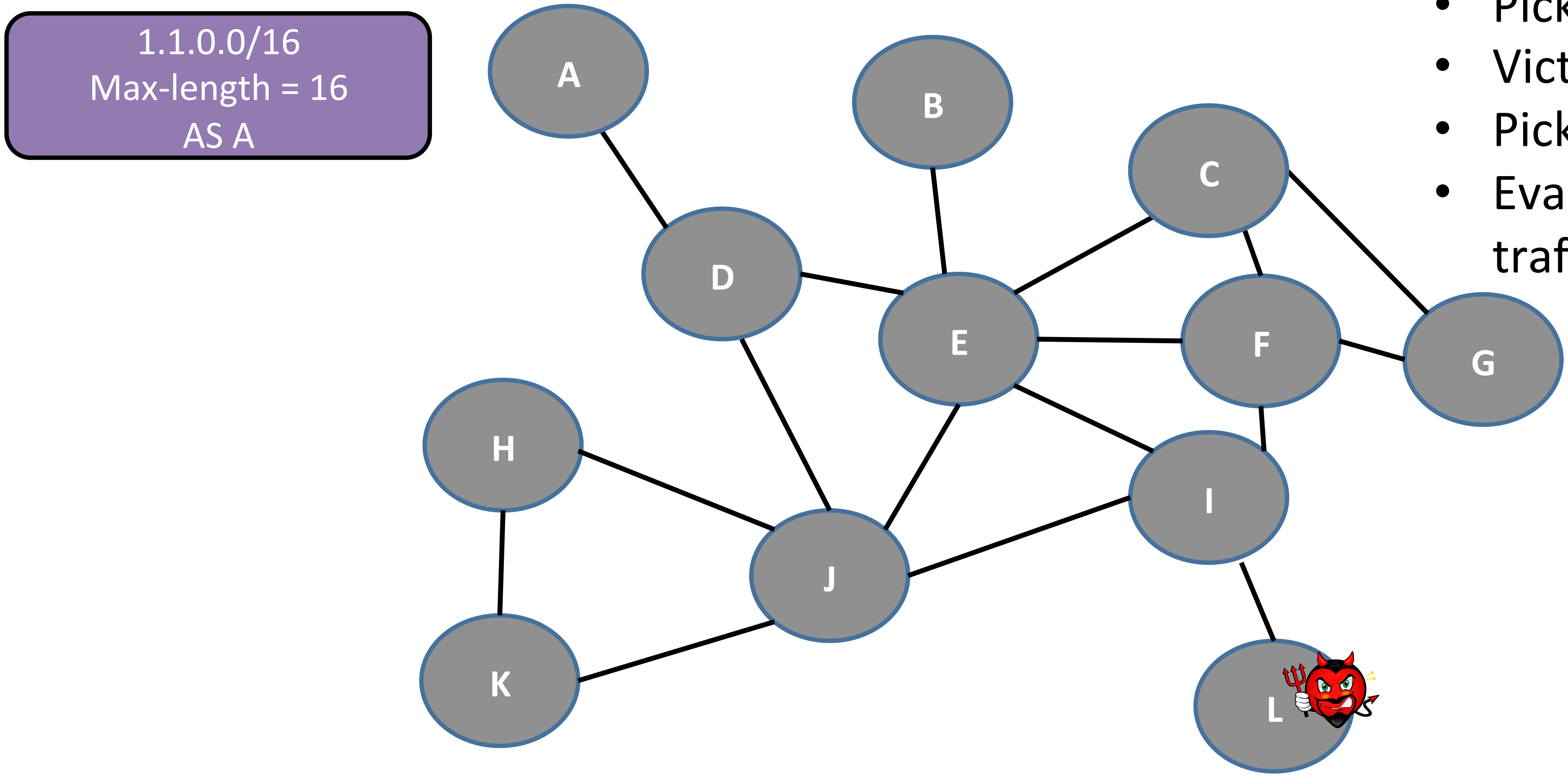
AS 2 does not filter and uses bad route for subprefix

AS 3 discards bad subprefix route

To: 1.1.1/24
AS path: 2-666

To: 1.1/16
AS path: 2-1

Quantify Security in Partial Adoption: Simulation Framework



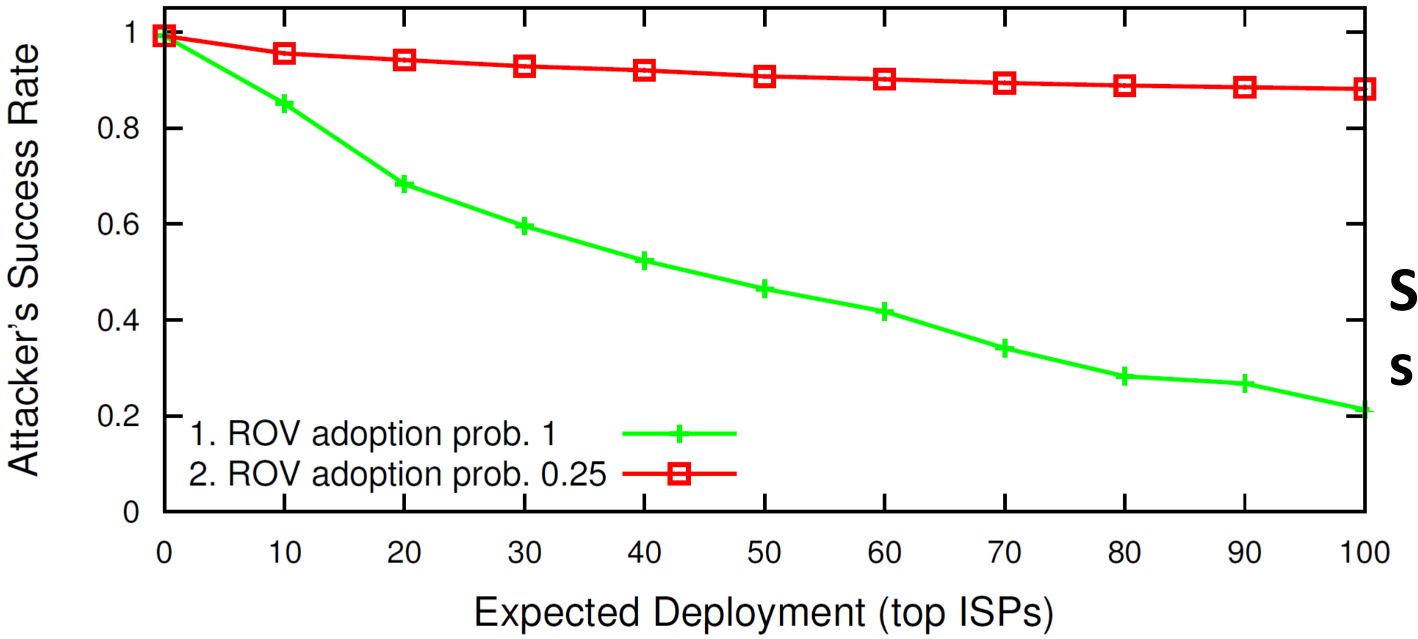
- Pick victim & attacker
- Victim's prefix has a ROA
- Pick set of ASes doing ROV
- Evaluate which ASes send traffic to the attacker

Empirically-derived AS-level network from CAIDA

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

Quantify Security in Partial Adoption

- Top ISP adopts with probability *p*
- Significant benefit only when *p* is high



Subprefix hijack success rate

Conclusion: What Can We Improve?

- Information accuracy
  - – ROAlert informs & alerts operators about:
    - Bad ROAs
    - Loose ROAs
- Preventing hijacks
  - – Incentivize ROV adoption by the top ISPs!

Thank You!

This work appeared at NDSS'17

Tech report at https://eprint.iacr.org/2016/1010.pdf

Questions? ☺