BOSTON UNIVERSITY

THE HEBREW UNIVERSITY OF JERUSALEM

Are We There Yet?
On RPKI Deployment and Security

Yossi Gilad

joint work with: Avichai Cohen,

Amir Herzberg, Michael Schapira, Haya Shulman

Massachusetts Institute of Technology

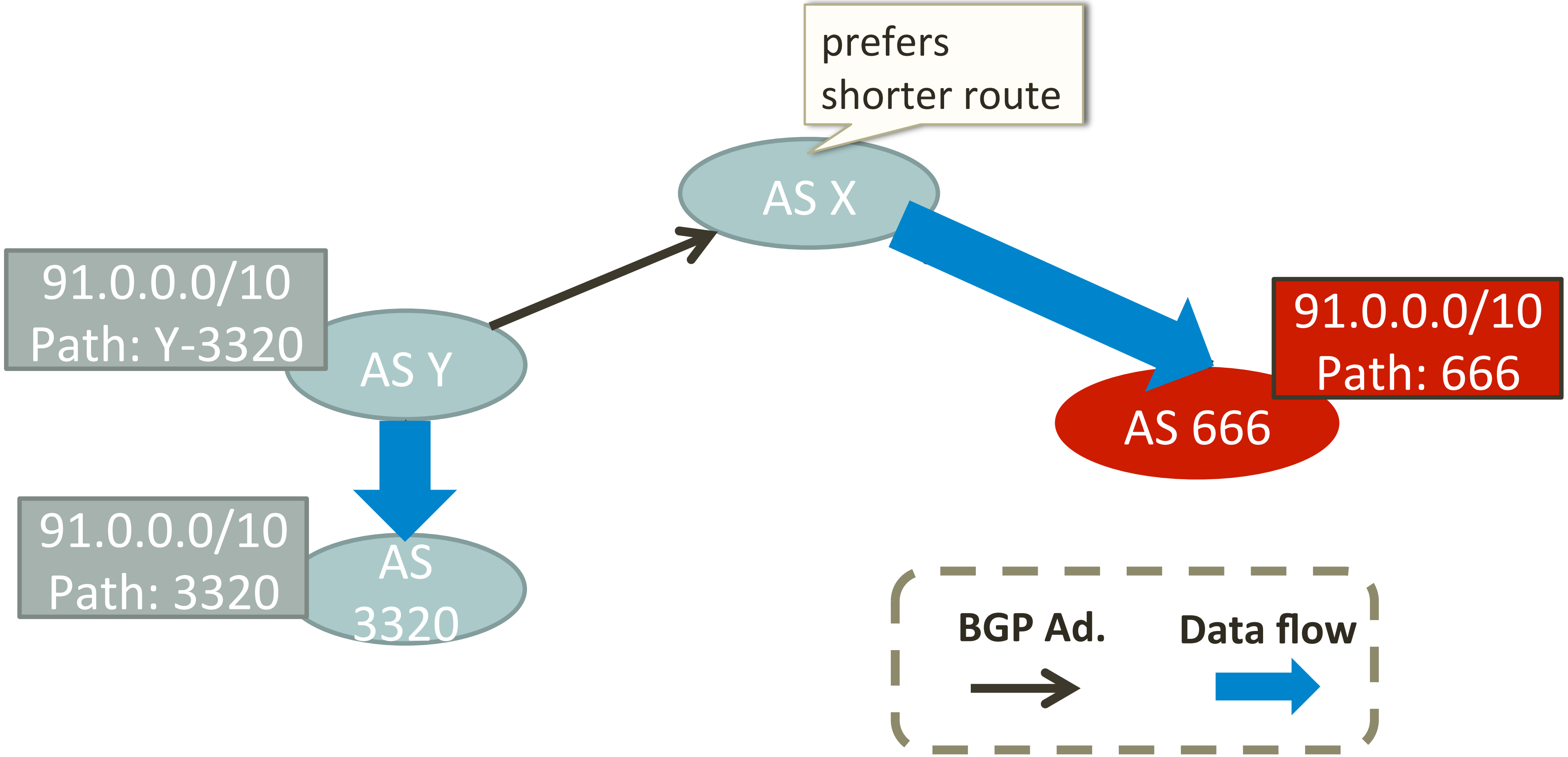
Fraunhofer SIT

The Resource Public Key Infrastructure

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

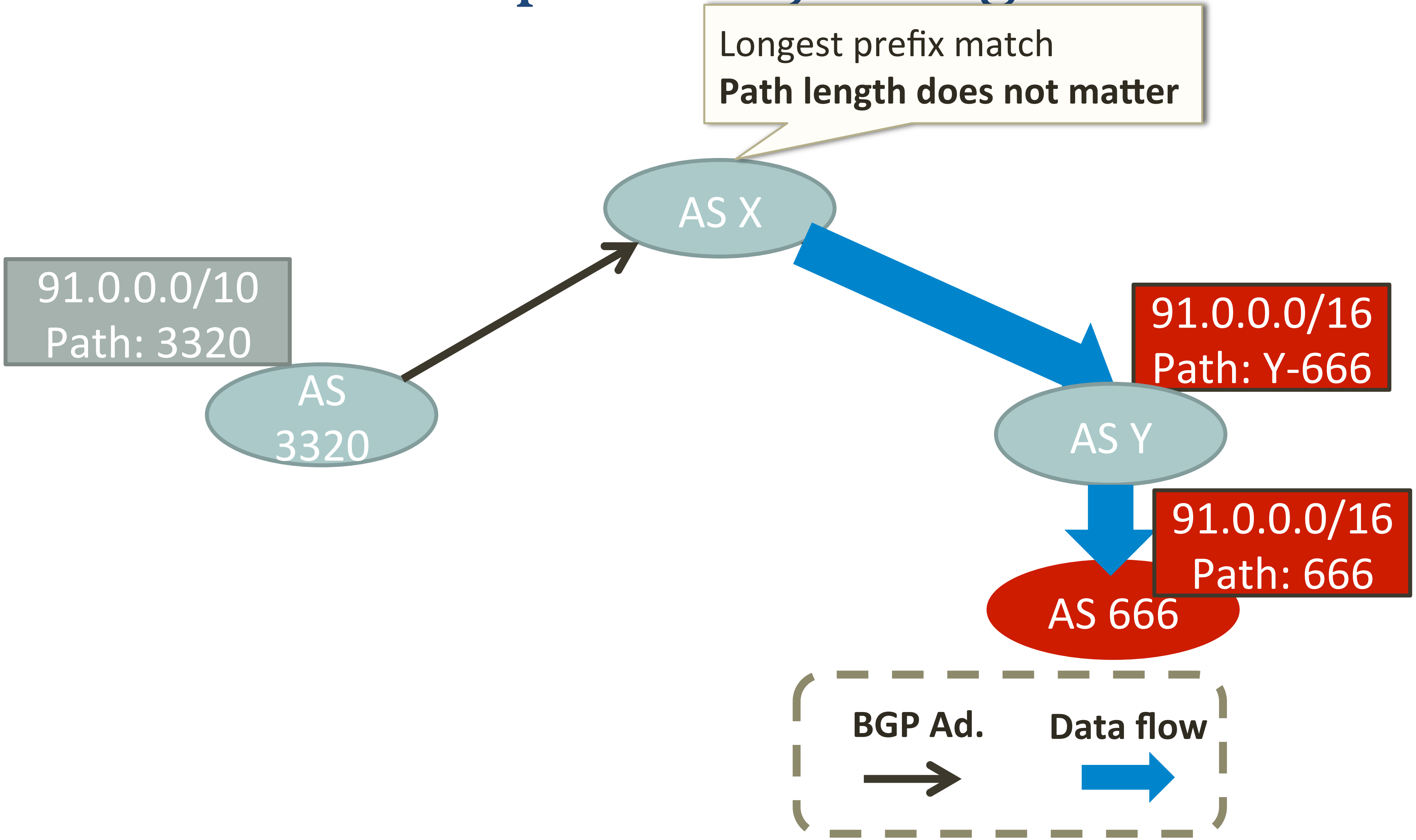
- Intended to **prevent** prefix/subprefix hijacks
- Lays the **foundation** for protection against more sophisticated attacks on interdomain routing
  - BGPsec, SoBGP,…

Prefix Hijacking



prefers shorter route

Subprefix Hijacking



Certifying Ownership with RPKI

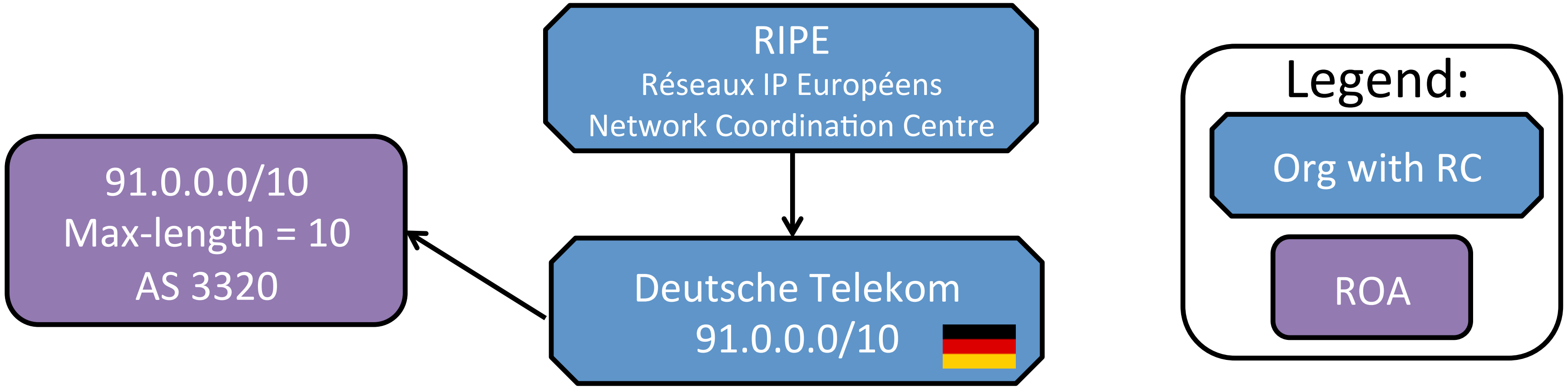
- RPKI assigns an IP prefix to a public key via a Resource Certificate (RC)

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

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

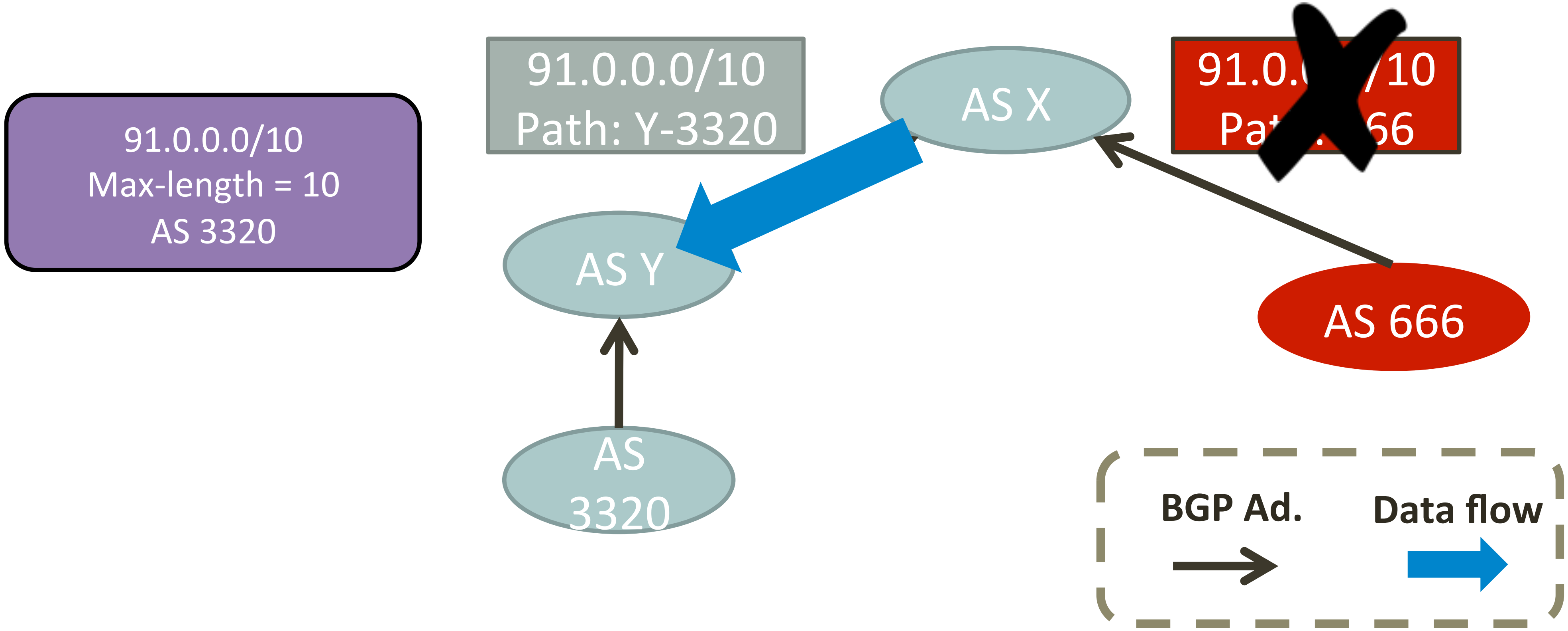
Example: Certifying Ownership

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



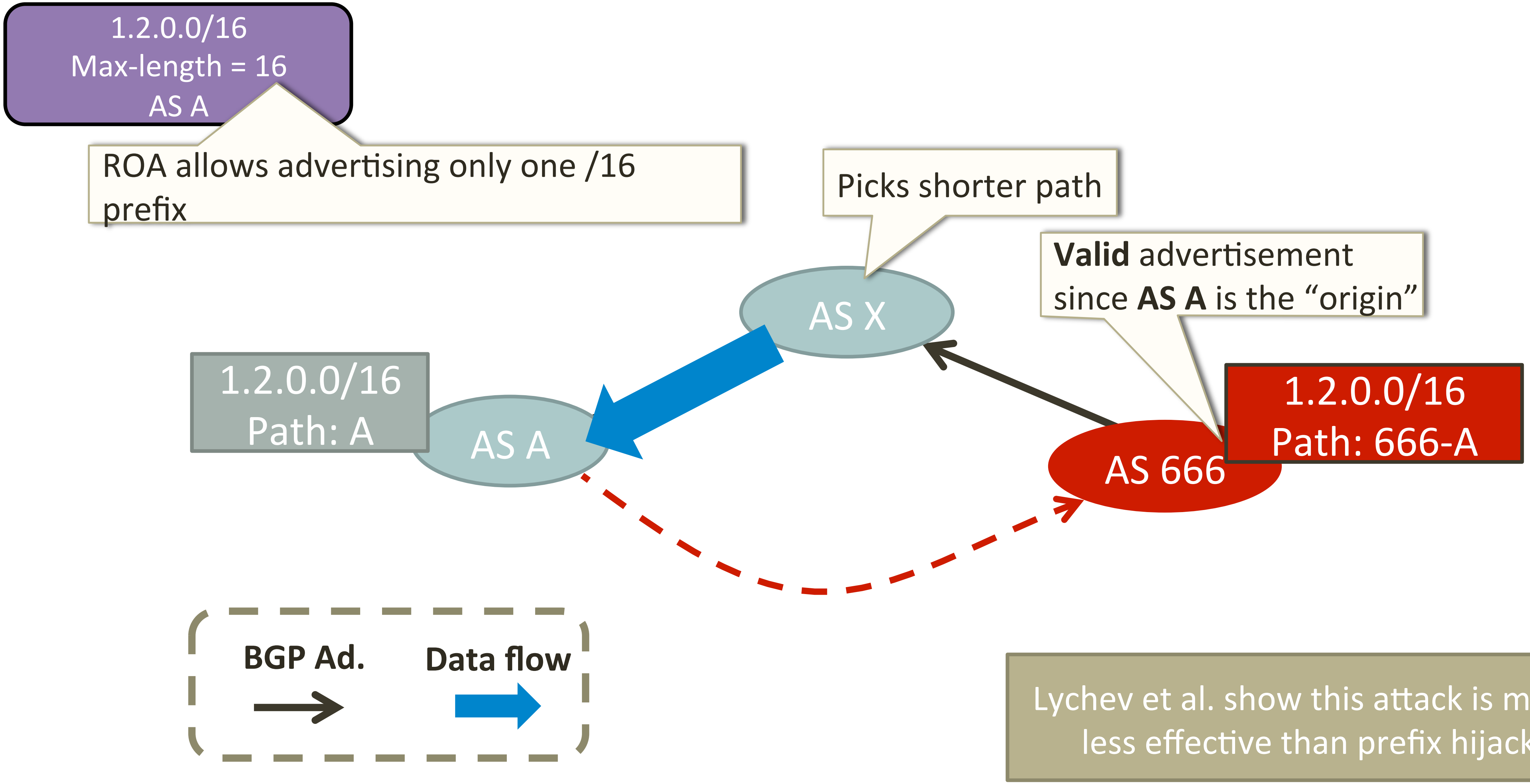
Talk Outline

- **Obstacles facing deployment**
  - **Insecure deployment**
  - Human error
  - Inter-organization dependencies

- Improving information accuracy with ROAlert

- Route origin validation in partial deployment
  - First measurements
  - How “good” is ROV in partial deployment?

Insecure Deployment: Loose ROAs



1.2.0.0/16
Max-length = 16
AS A

ROA allows advertising only one /16 prefix

Picks shorter path

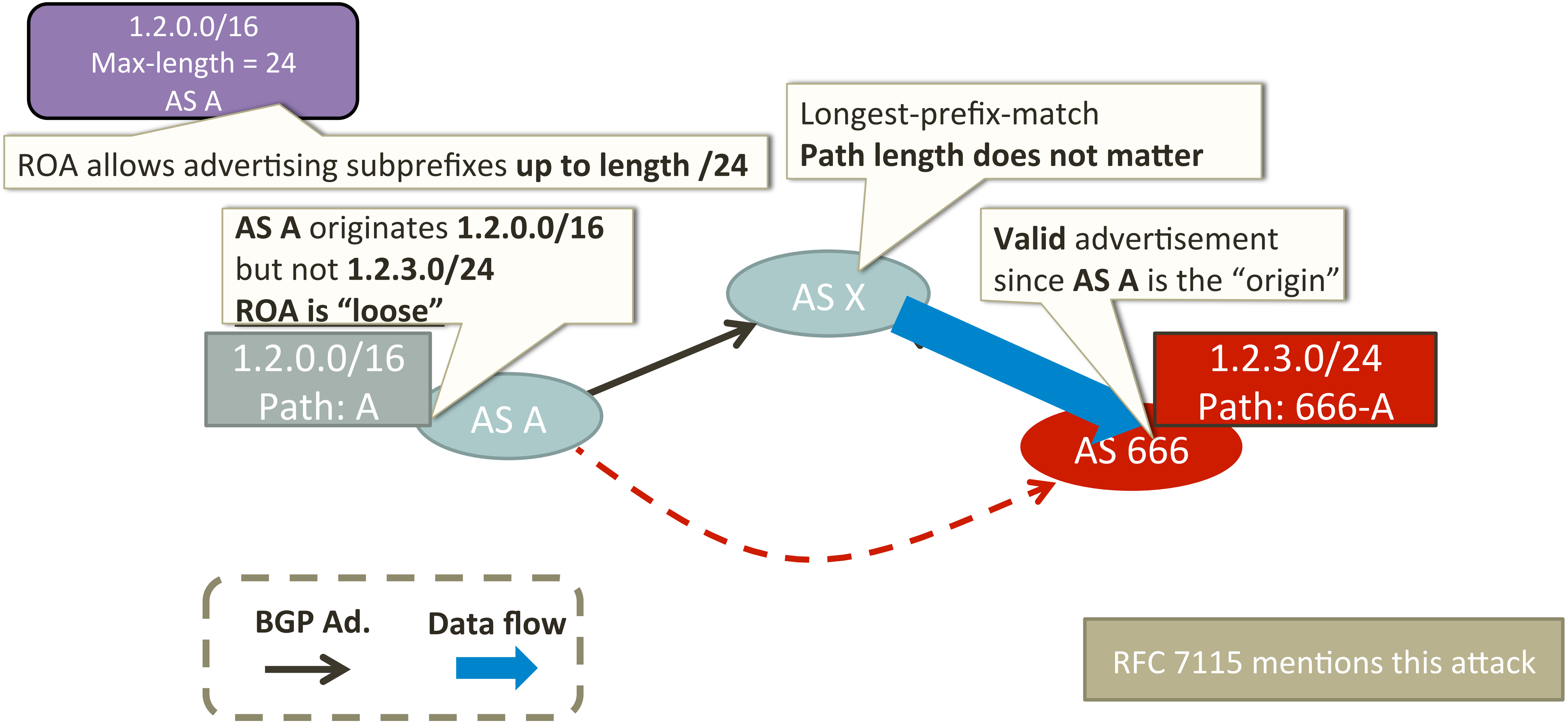
Valid advertisement since **AS A** is the “origin”

1.2.0.0/16
Path: A

1.2.0.0/16
Path: 666-A

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

Insecure Deployments: Loose ROAs



1.2.0.0/16
Max-length = 24
AS A

ROA allows advertising subprefixes **up to length /24**

Longest-prefix-match
Path length does not matter

AS A originates **1.2.0.0/16**
but not **1.2.3.0/24**
ROA is "loose"

Valid advertisement
since **AS A** is the "origin"

RFC 7115 mentions this attack

Loose ROAs in RFC 7115

``one advantage of minimal ROA length is that the forged origin attack does not work for sub-prefixes that are not covered by overly long max length. For example, if, instead of 10.0.0.0/16-24, one issues 10.0.0.0/16 and 10.0.42.0/24, a forged origin attack cannot succeed against 10.0.666.0/24. They must attack the whole /16, which is more likely to be noticed because of its size.''

- **We point out: hijacking the /16 is actually also <u>less effective</u>!**

Why Does This Attack Work?

- Hijacker claims that **AS 666** is a neighbor of **AS A**
  - but the RPKI does not allow to check that the announcement is valid, since the origin is **AS A**

- **AS A** doesn't actually originate a route for **1.2.3.0/24**
  - but the ROA allows it → ROA is ``**loose**"
  - hijacker's route is the only route to this subprefix

- Longest-prefix-match: hijacker's route is always taken

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>

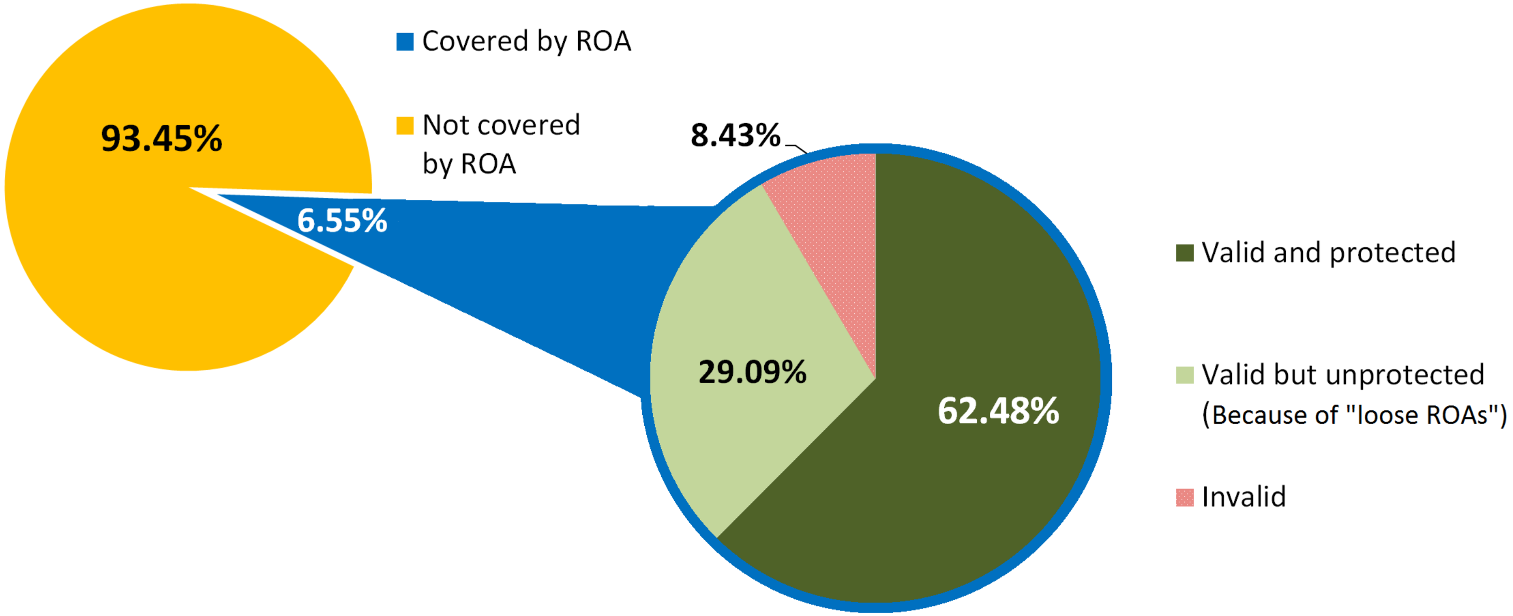
Talk Outline

- **Obstacles facing deployment**
  - Insecure deployment
  - **Human error**
  - Inter-organization dependencies
- Improving information accuracy with ROAlert
- Route origin validation in partial deployment
  - First measurements
  - How “good” is ROV in partial deployment?

Obstacles 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]

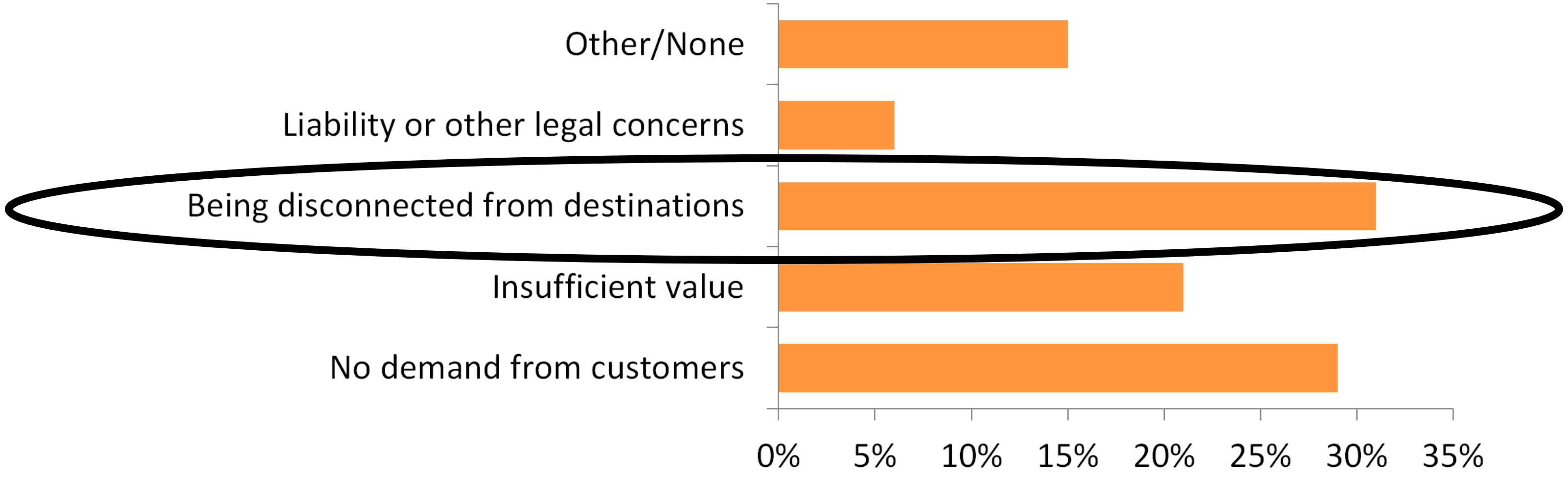


Obstacles to Deployment: Human Error

Concern for disconnection was pointed out in our survey

- anonymous survey of over 100 network operators (details in paper)

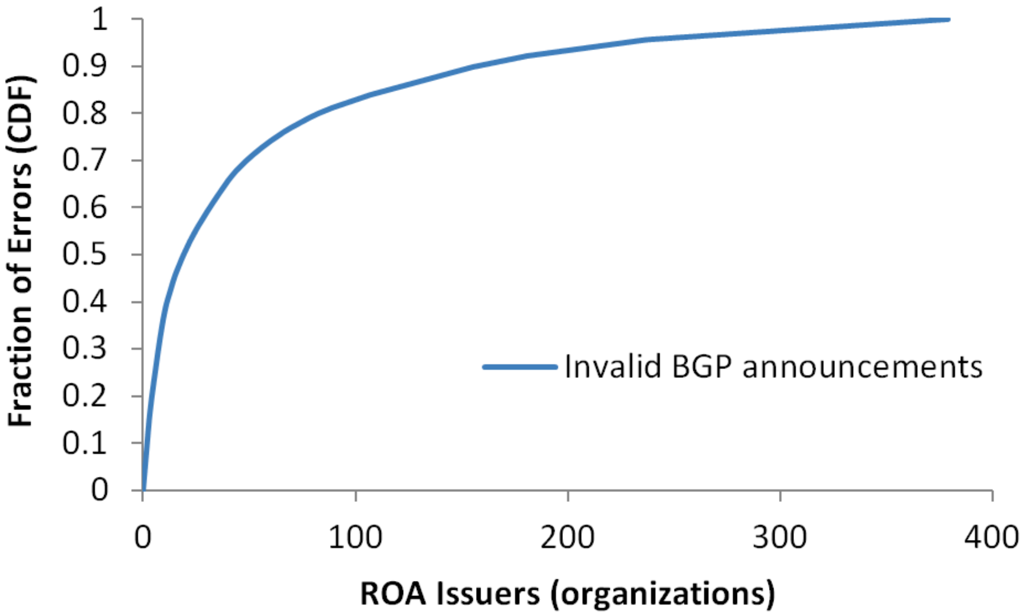
What are your main concerns regarding executing RPKI-based origin authentication in your network?



Obstacles to Deployment: Human Error

Who is responsible for “bad ROAs”?

- Hundreds of organizations are responsible for invalid IP prefixes, but…
- Good news: most errors due to small number of organizations



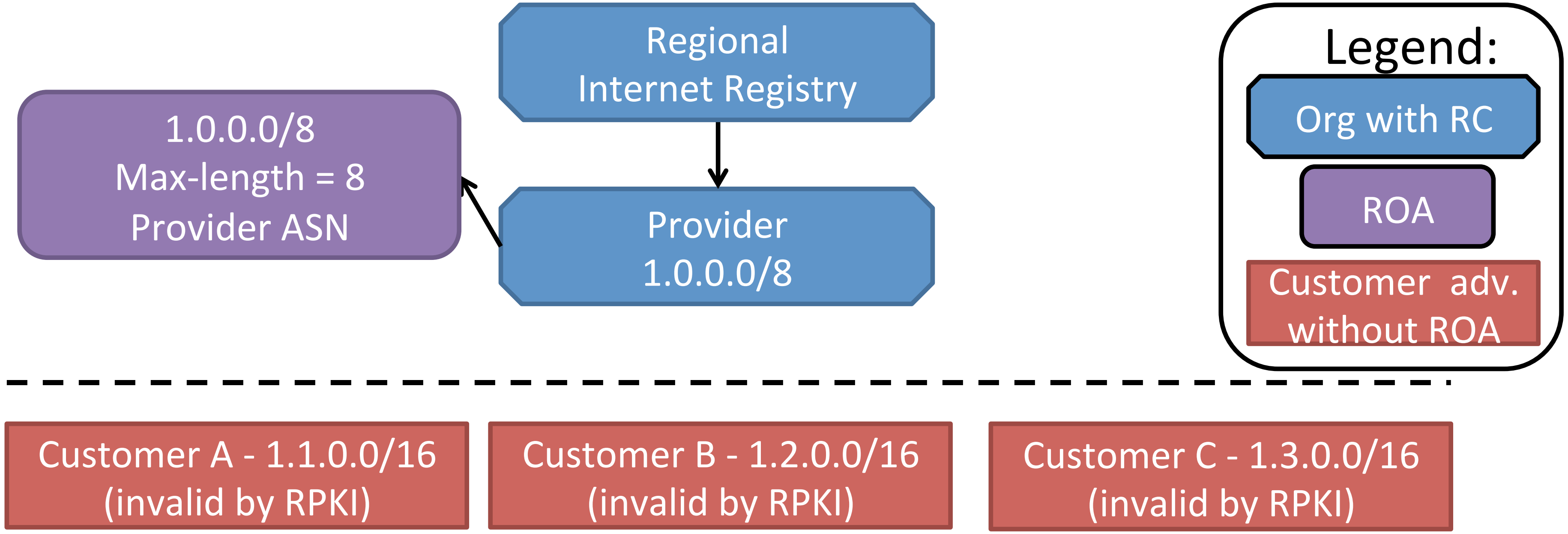
Talk Outline

- **Obstacles facing deployment**
  - Insecure deployment
  - Human error
  - **Inter-organization dependencies**
- Improving information accuracy with ROAlert
- Route origin validation in partial deployment
  - Initial measurements
  - How “good” is ROV in partial deployment?

Obstacles to Deployment: Inter-Organization Dependencies

Downward dependencies:

When provider has a ROA,
customer-announcements without ROAs are invalid

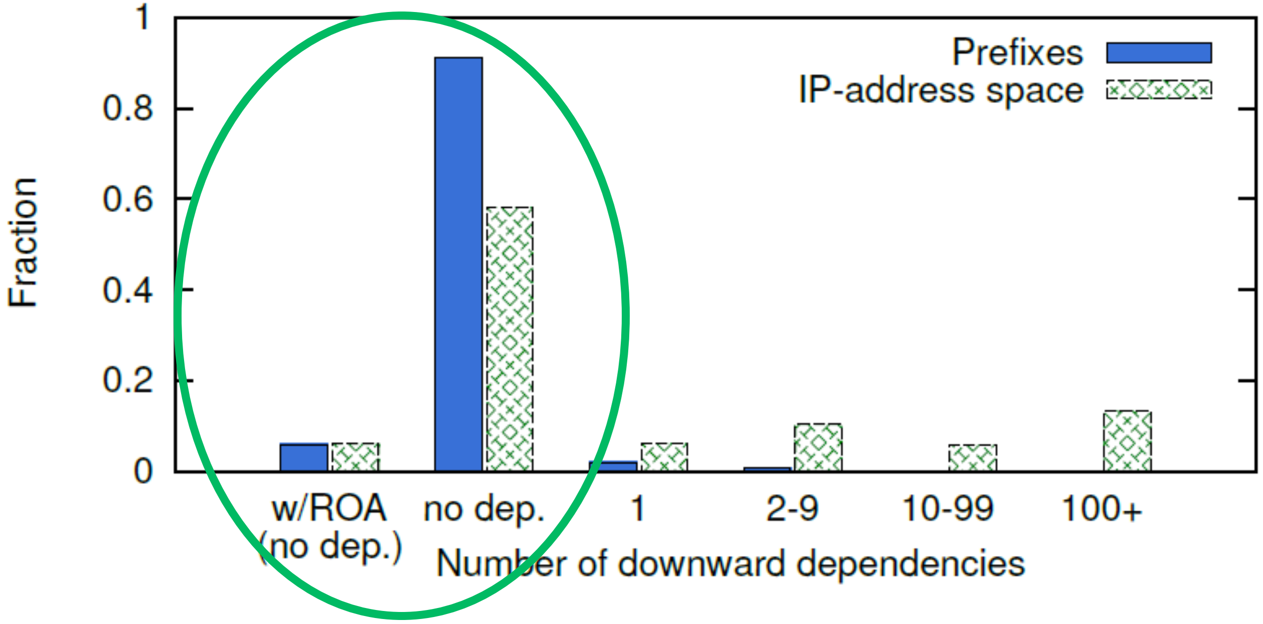


Regional Internet Registry
1.0.0.0/8
Max-length = 8
Provider ASN
Provider
1.0.0.0/8
Legend:
Org with RC
ROA
Customer adv. without ROA
Customer A - 1.1.0.0/16 (invalid by RPKI)
Customer B - 1.2.0.0/16 (invalid by RPKI)
Customer C - 1.3.0.0/16 (invalid by RPKI)

Obstacles to Deployment: Inter-Organization Dependencies

Good news:

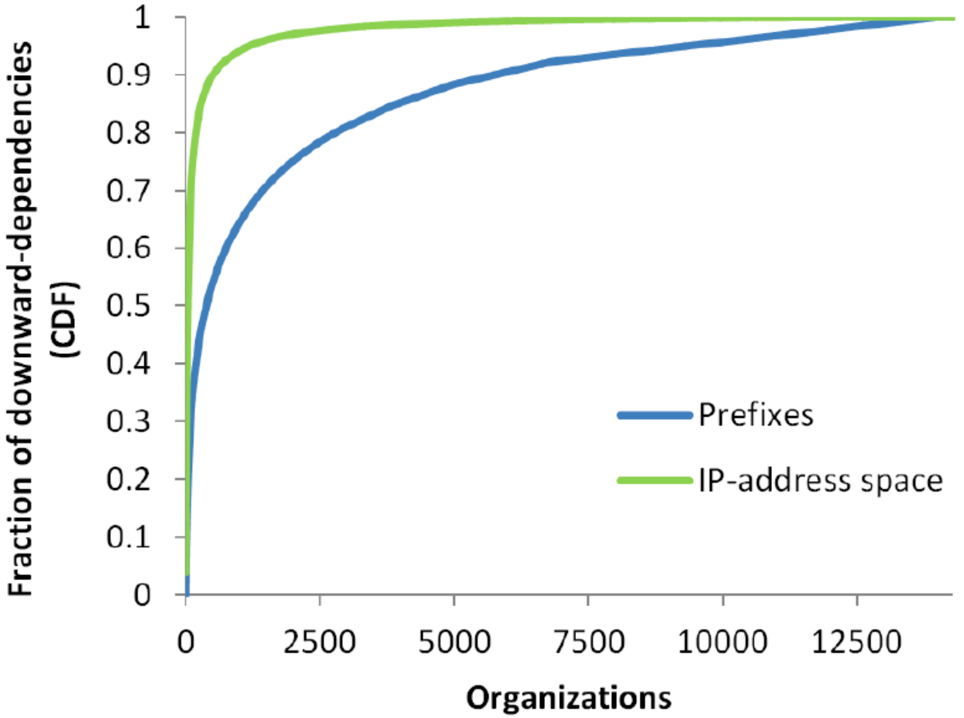
Only a handful of prefixes are downward dependent



Obstacles to Deployment: Inter-Organization Dependencies

Bad news:

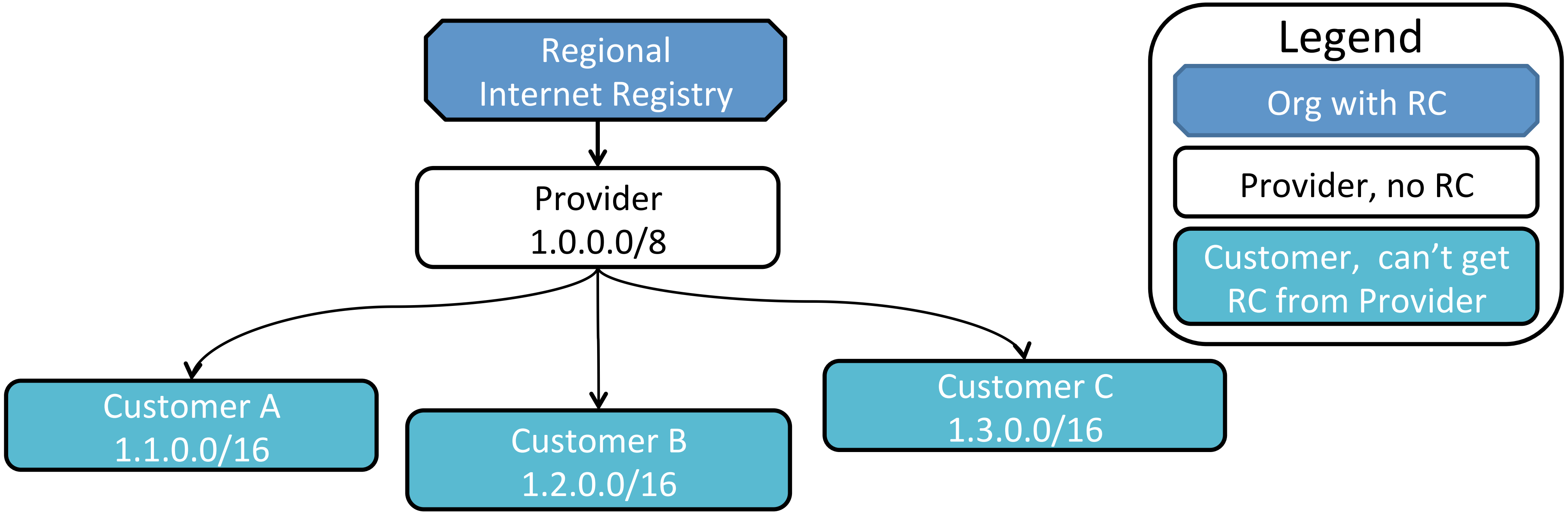
these are large prefixes that belong to large providers



Obstacles to Deployment: Inter-Organization Dependencies

Upward dependencies:

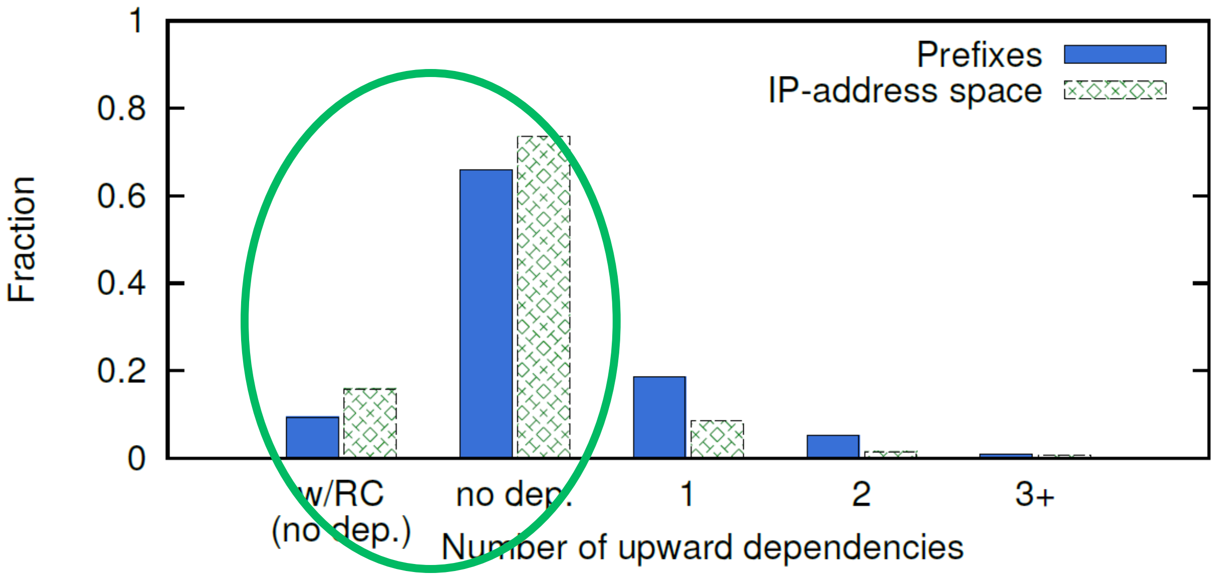
When provider doesn't have an RC, customers might be unable to get an RC



Obstacles to Deployment: Inter-Organization Dependencies

Good news:

Not many organizations are upward-dependent



Talk Outline

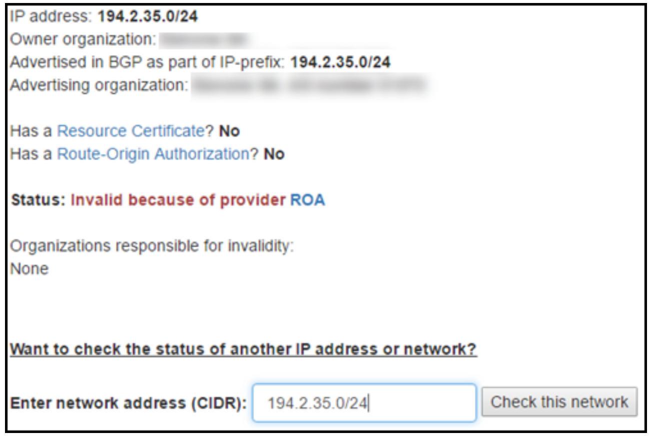
- Obstacles facing deployment
  - Insecure deployment
  - Human error
  - Inter-organization dependencies

- **Improving information accuracy with ROAlert**

- Route origin validation in partial deployment
  - First measurements
  - How "good" is RPKI in partial deployment?

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]

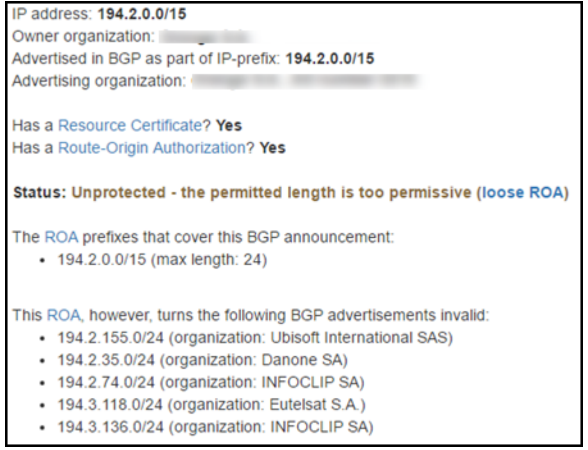
Has a Resource Certificate? **No**
Has a Route-Origin Authorization? **No**

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



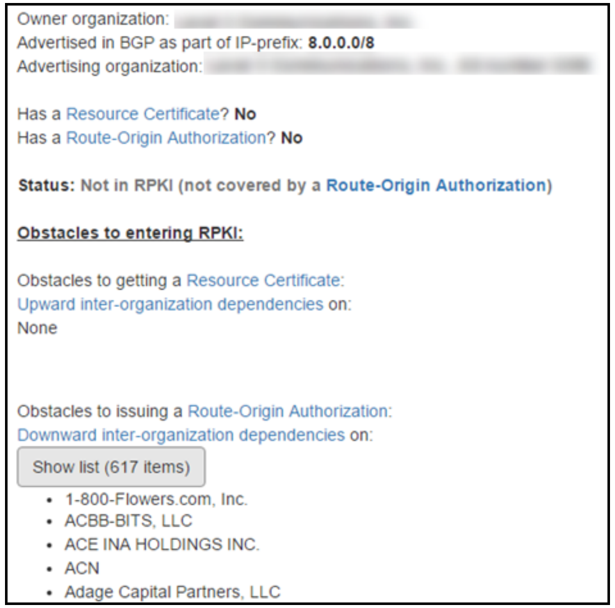
IP address: **194.2.0.0/15**
Owner organization: [redacted]
Advertised in BGP as part of IP-prefix: **194.2.0.0/15**
Advertising organization: [redacted]

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]

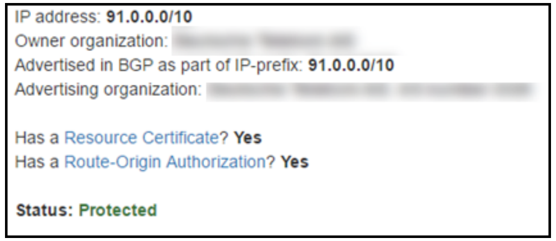
Has a Resource Certificate? **No**
Has a Route-Origin Authorization? **No**

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

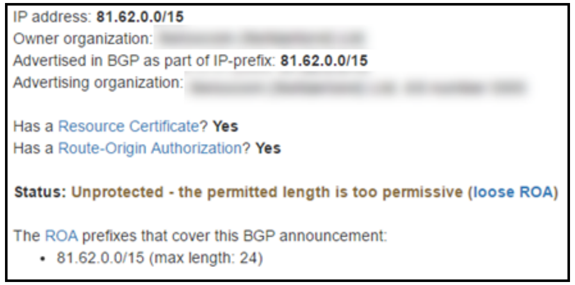
Obstacles to issuing a Route-Origin Authorization:
Downward inter-organization dependencies on:
Show list (617 items)
- 1-800-Flowers.com, Inc.
- ACBB-BITS, LLC
- ACE INA HOLDINGS INC.
- ACN
- Adage Capital Partners, LLC



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**

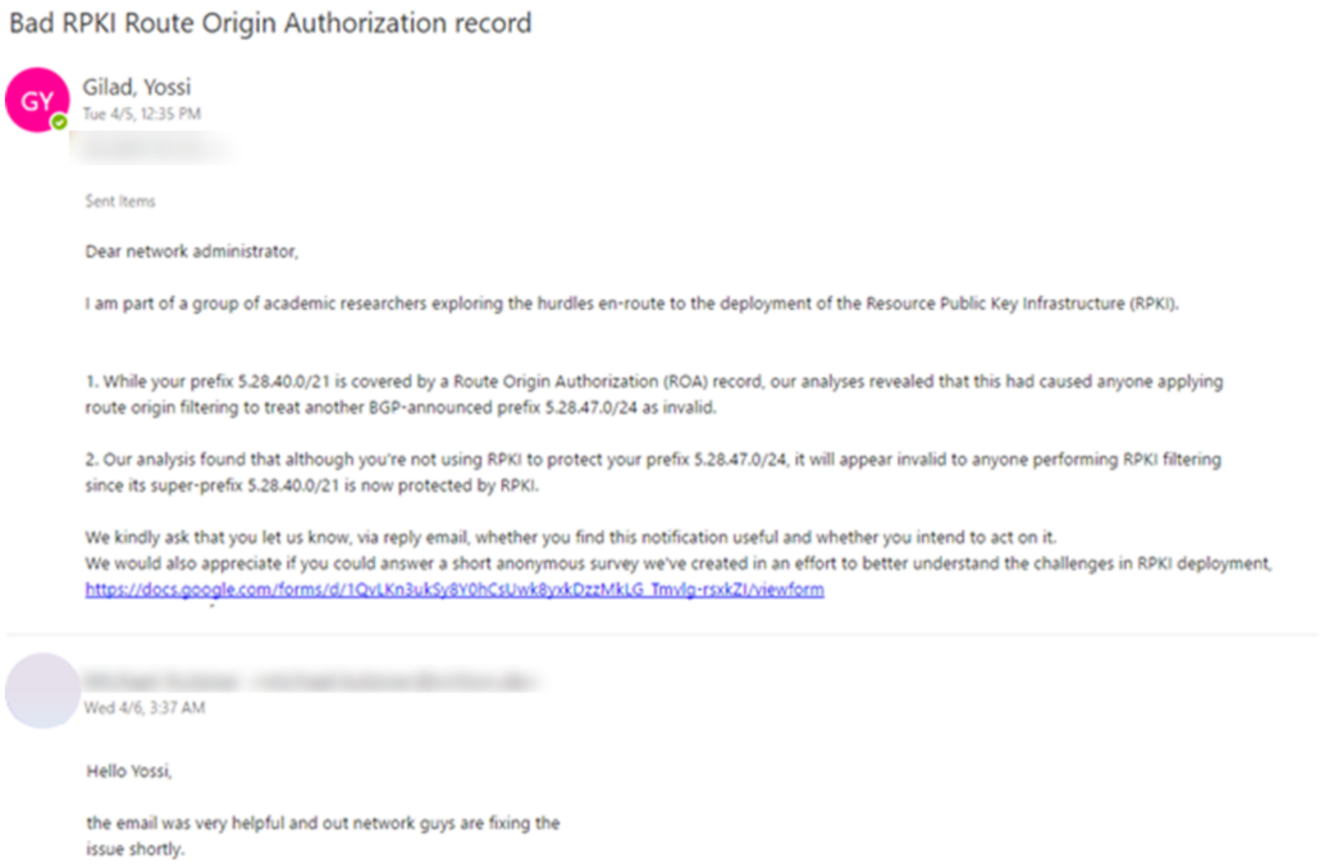
Status: Unprotected - the permitted length is too permissive (loose ROA)

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” (offenders and victims alike!)

Improving Accuracy with ROAlert



Bad RPKI Route Origin Authorization record

GY

Gilad, Yossi

Tue 4/5, 12:35 PM

[redacted]

Sent Items

Dear network administrator,

I am part of a group of academic researchers exploring the hurdles en-route to the deployment of the Resource Public Key Infrastructure (RPKI).

1. While your prefix 5.28.40.0/21 is covered by a Route Origin Authorization (ROA) record, our analyses revealed that this had caused anyone applying route origin filtering to treat another BGP-announced prefix 5.28.47.0/24 as invalid.

2. Our analysis found that although you're not using RPKI to protect your prefix 5.28.47.0/24, it will appear invalid to anyone performing RPKI filtering since its super-prefix 5.28.40.0/21 is now protected by RPKI.

We kindly ask that you let us know, via reply email, whether you find this notification useful and whether you intend to act on it.
We would also appreciate if you could answer a short anonymous survey we've created in an effort to better understand the challenges in RPKI deployment,
https://docs.google.com/forms/d/1QvLKn3ukSy8Y0hCsUwk8yxkDzzMkLG_Tmvlg-rsxkZI/viewform

[redacted]

Wed 4/6, 3:37 AM

Hello Yossi,

the email was very helpful and out network guys are fixing the
issue shortly.

Improving Accuracy with ROAlert

- Initial results are promising!
  - notifications reached 168 victims and offenders
  - 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

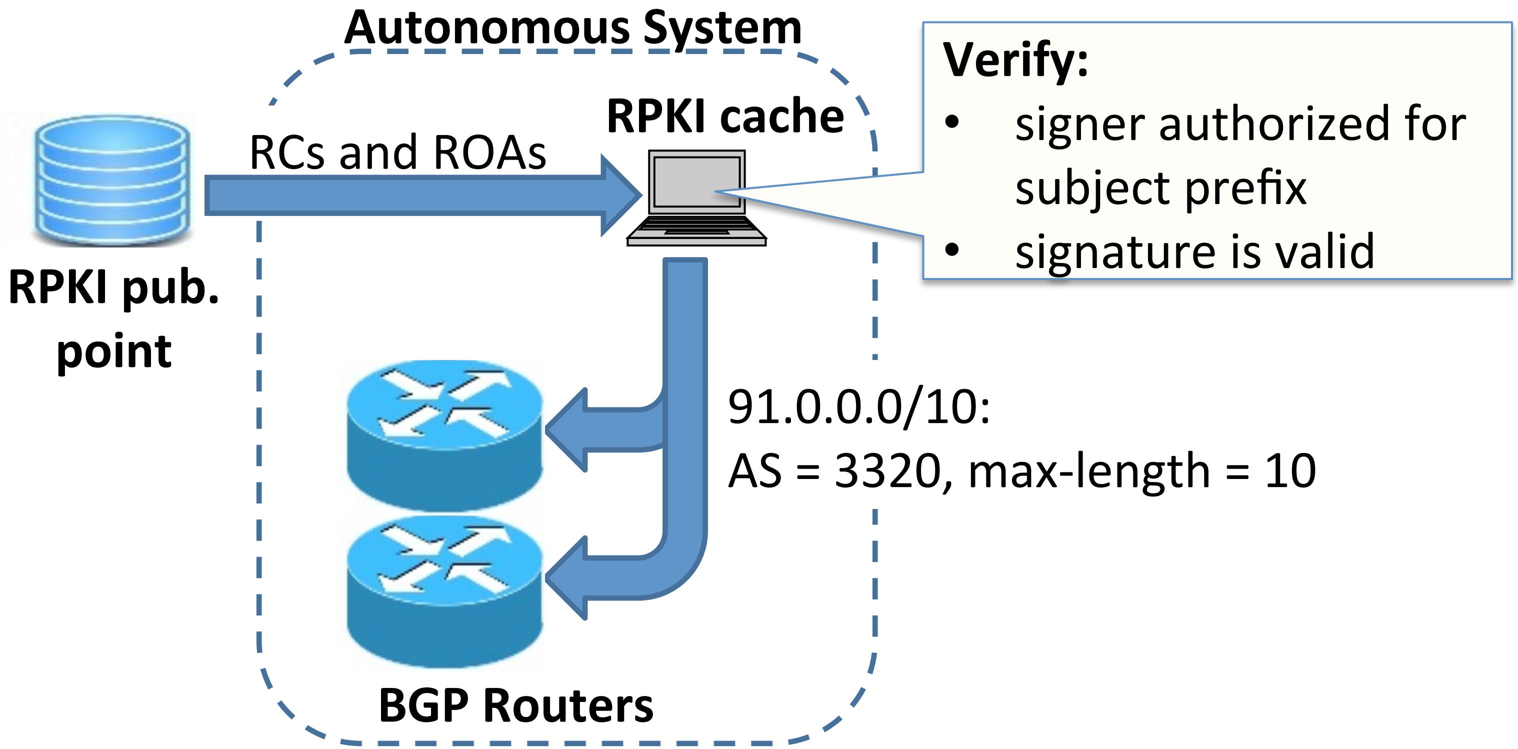
- Obstacles facing deployment
  - Insecure deployment
  - Human error
  - Inter-organization dependencies

- Improving information accuracy with ROAlert

- **Route origin validation in partial deployment**
  - **First measurements**
  - How “good” is ROV in partial deployment?

Filtering Bogus Advertisements

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



Verify:

- signer authorized for subject prefix
- signature is valid

ROV in Partial Deployment

Major router vendors support ROV with negligible overhead

Any AS, anywhere, can do ROV ✓

But is it actually enforced?

ROV in Partial Deployment

We gain empirical insights regarding ROV enforcement via invalid BGP advertisements

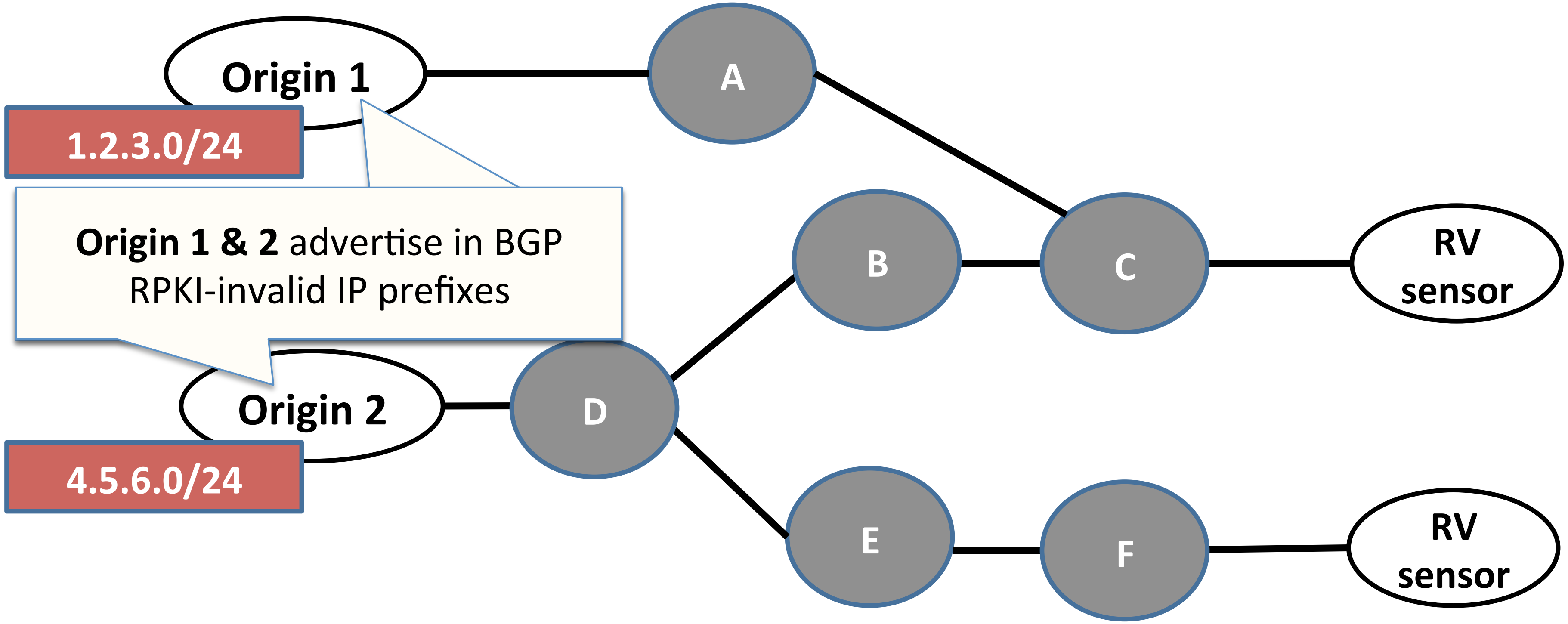
We monitored BGP paths from multiple vantage points afforded by 44 Route Views sensors[1]

- An ongoing follow-up study by Katz-Bassett et. al uses more advanced active techniques

[1] http://www.routeviews.org/

Measurements: Non-Filtering ASes

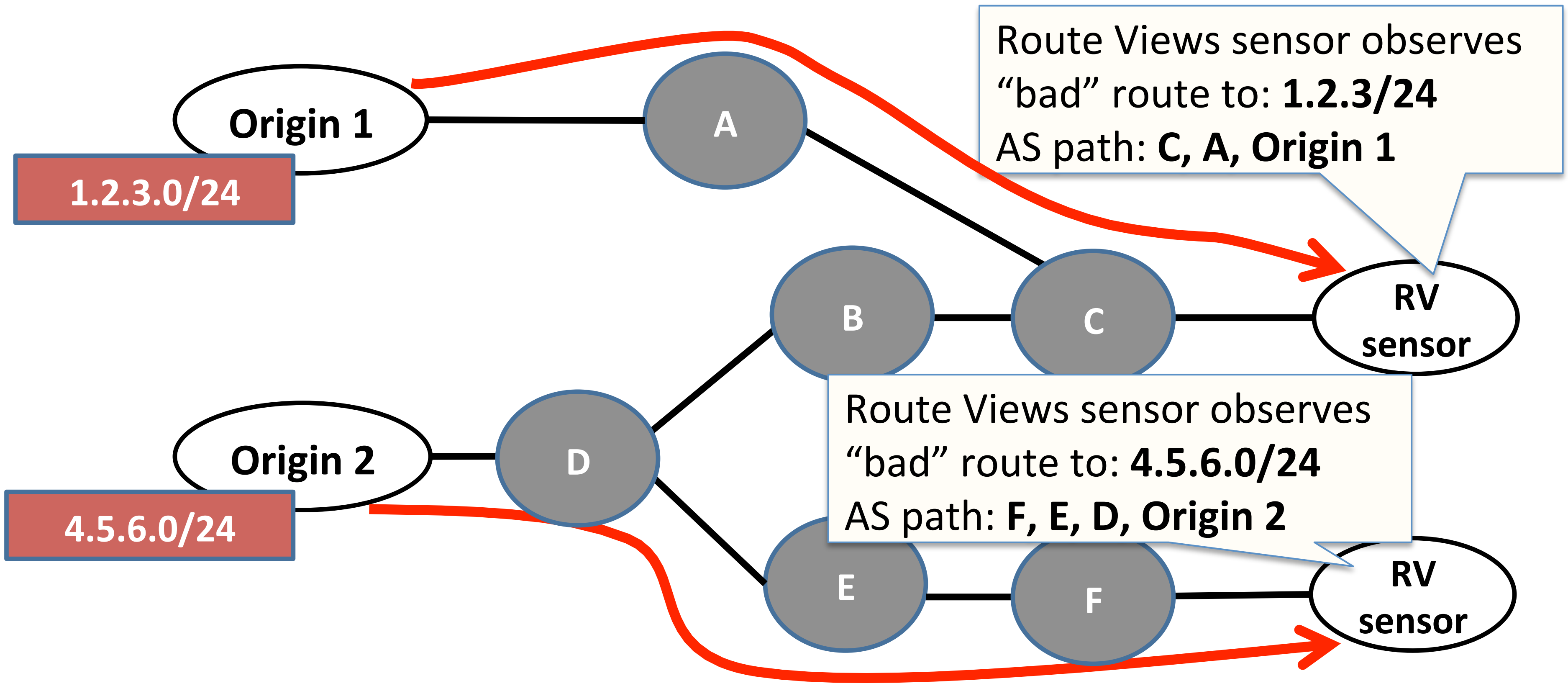
ASes that propagate invalid BGP advertisements do not perform filtering



Origin 1 & 2 advertise in BGP RPKI-invalid IP prefixes

Measurements: Non-Filtering ASes

ASes that propagate invalid BGP advertisements do not perform filtering

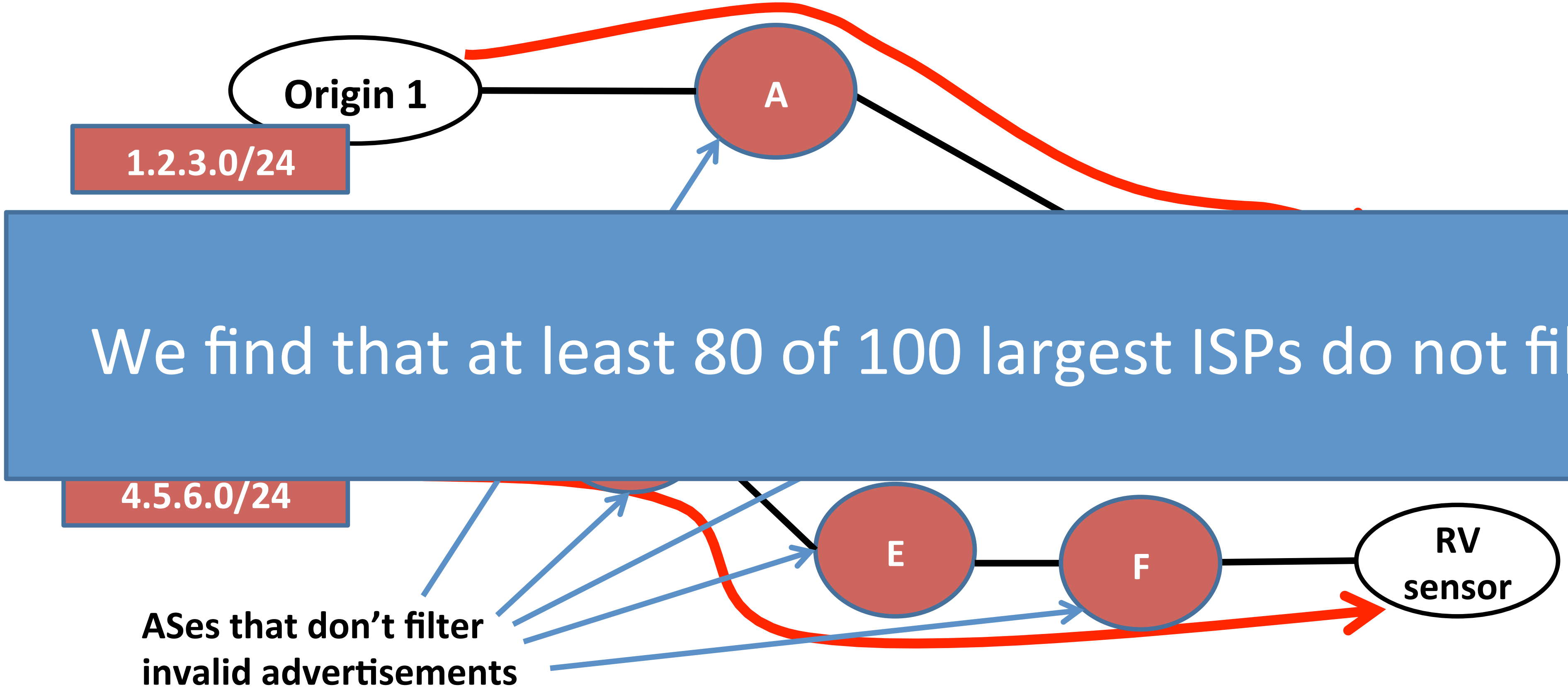


Route Views sensor observes “bad” route to: **1.2.3/24**
AS path: **C, A, Origin 1**

Route Views sensor observes “bad” route to: **4.5.6.0/24**
AS path: **F, E, D, Origin 2**

Measurements: Non-Filtering ASes

ASes that propagate invalid BGP advertisements do not perform filtering



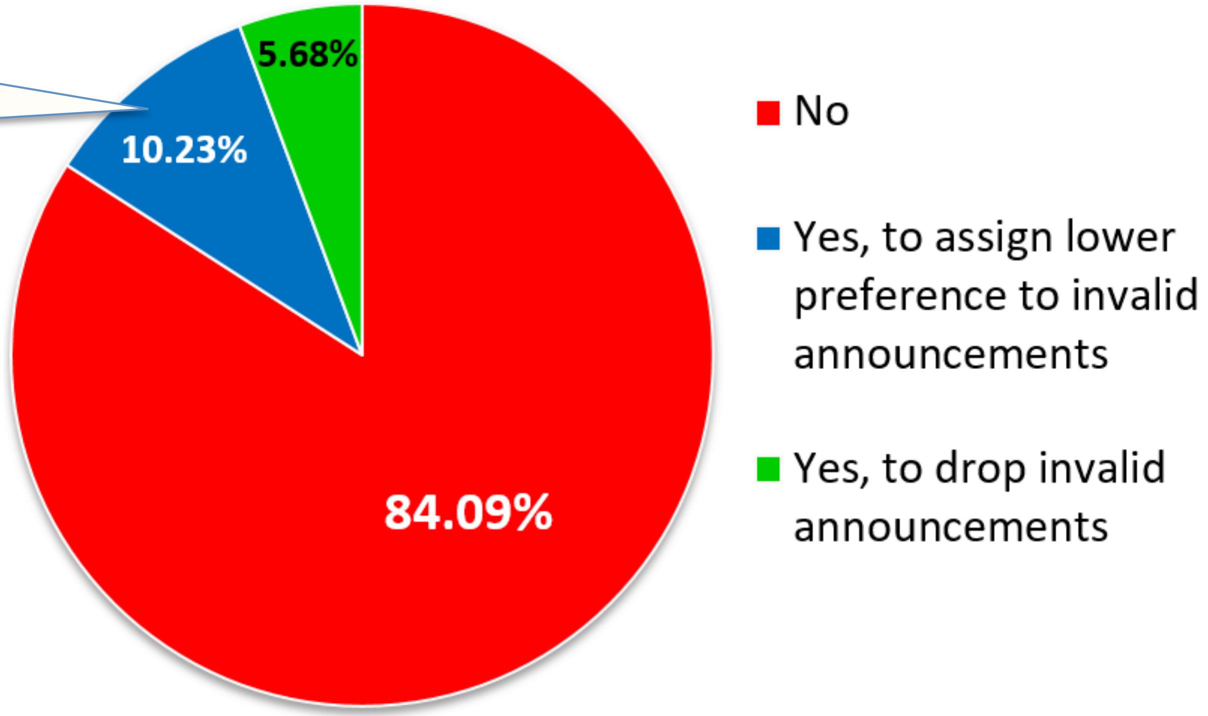
We find that at least 80 of 100 largest ISPs do not filter

Survey on ROV Adoption

Our survey confirms the measurements -
ROV deployment is very partial

Does not protect against subprefix hijacks [Heilman et al. 2014]

Do you apply RPKI-based route-origin validation?



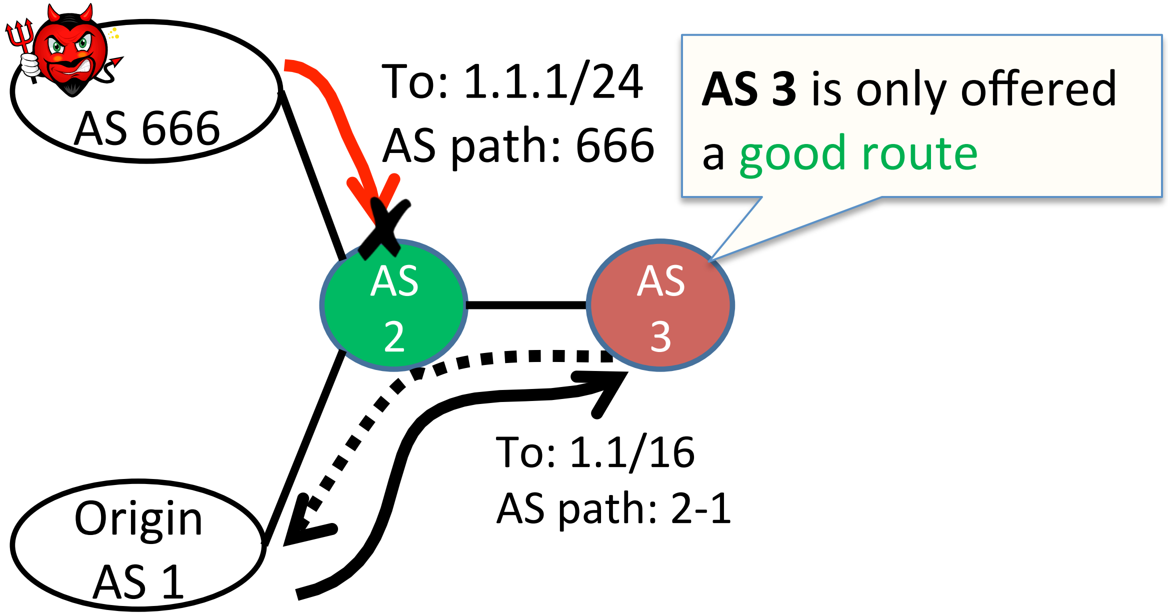
Talk Outline

- Obstacles facing deployment
  - insecure deployment
  - human error
  - inter-organization dependencies
- Improving information accuracy with ROAlert
- **Route origin validation in partial deployment**
  - First measurements
  - **How “good” is ROV in partial deployment?**

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



AS 666

To: 1.1.1/24
AS path: 666

AS 3 is only offered a good route

AS 2

AS 3

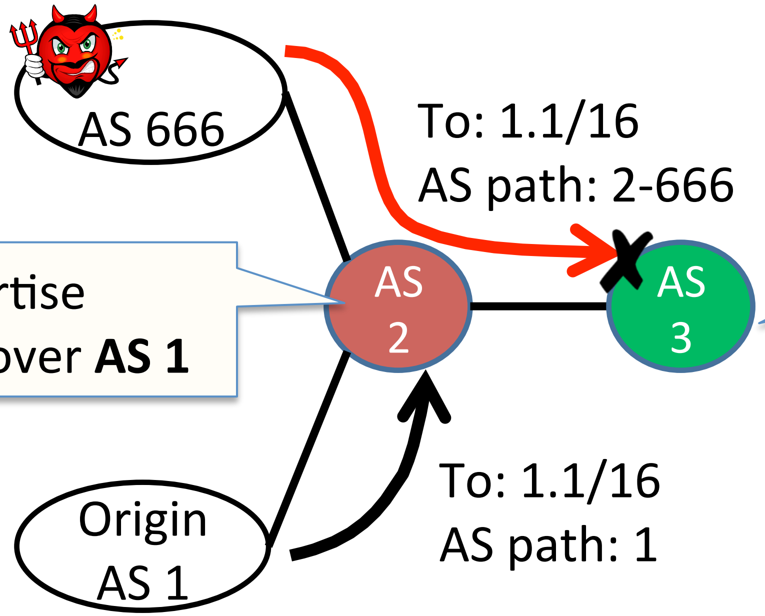
To: 1.1/16
AS path: 2-1

Origin AS 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

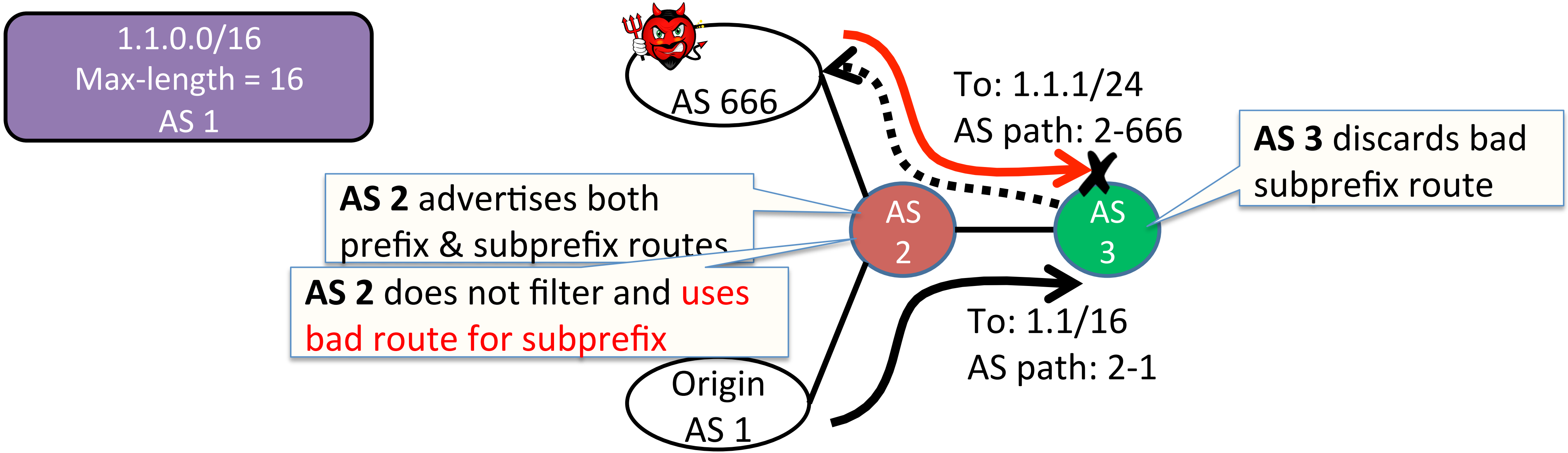


AS 2 prefers to advertise routes from **AS 666** over **AS 1**

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

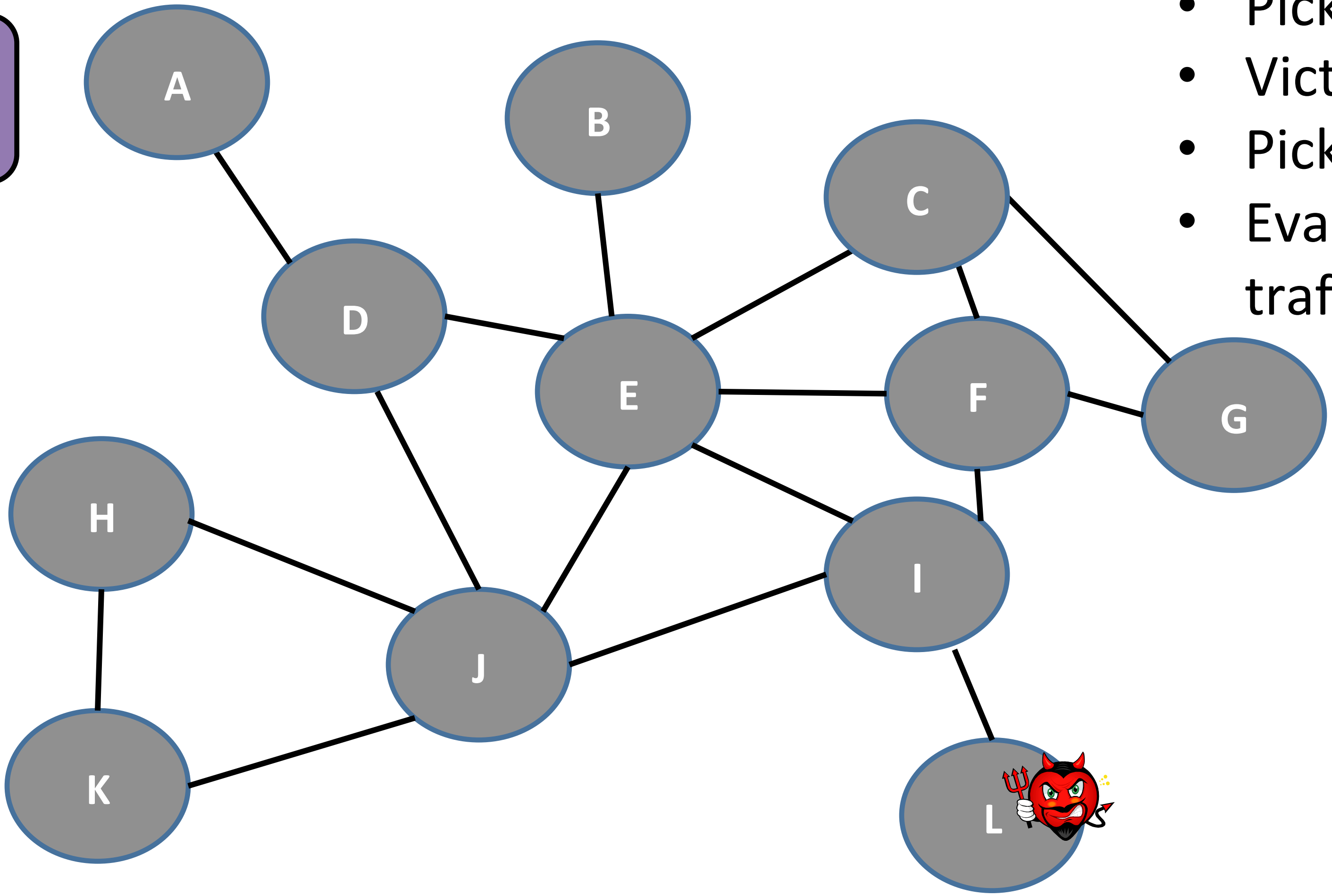
Simulation Framework

- We ran simulations to quantify security:
  - empirically-derived AS-level network from CAIDA
    - Including inferred peering links [Giotsas et al., SIGCOMM'13]
  - using the simulation framework in [Gill et al., CCR'12]

- We measured the attacker success rate
  - in terms of #ASes attracted
  - for different attack scenarios
  - for different ROV deployment scenarios
  - averaged over 1M attacker/victim pairs

Quantify Security in Partial Adoption: Simulation Framework

1.1.0.0/16
Max-length = 16
AS A



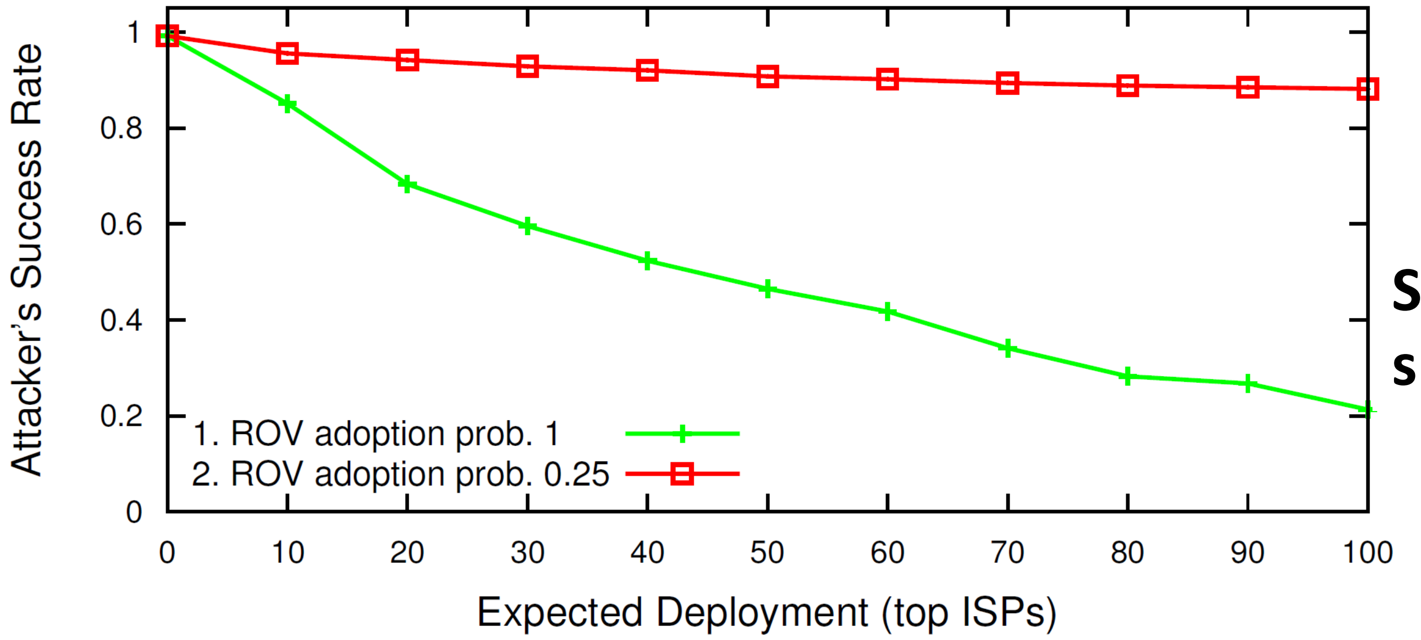
- Pick victim & attacker
- Victim's prefix has a ROA
- Pick set of ASes doing ROV
- Evaluate which ASes send traffic to the attacker

Empirically-derived AS-level network from CAIDA

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

Quantify Security in Partial Adoption

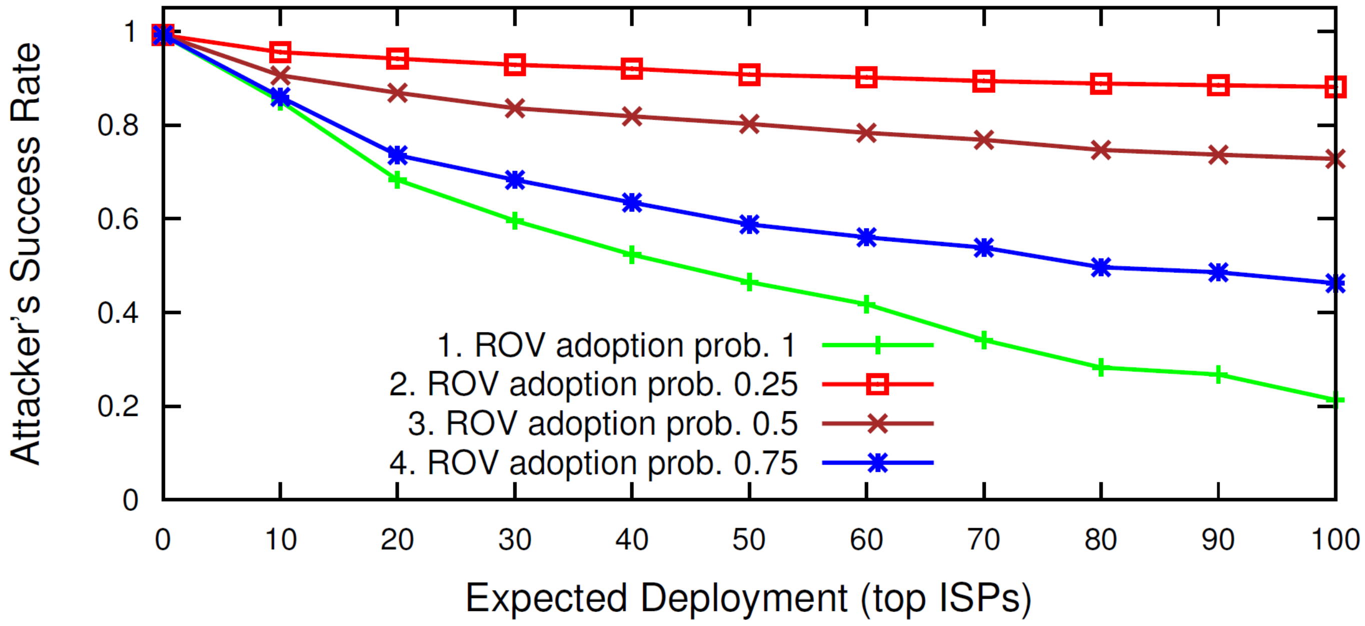
- Top ISP adopts with probability *p*
- Significant benefit only when *p* is high



Subprefix hijack success rate

Quantify Security in Partial Adoption

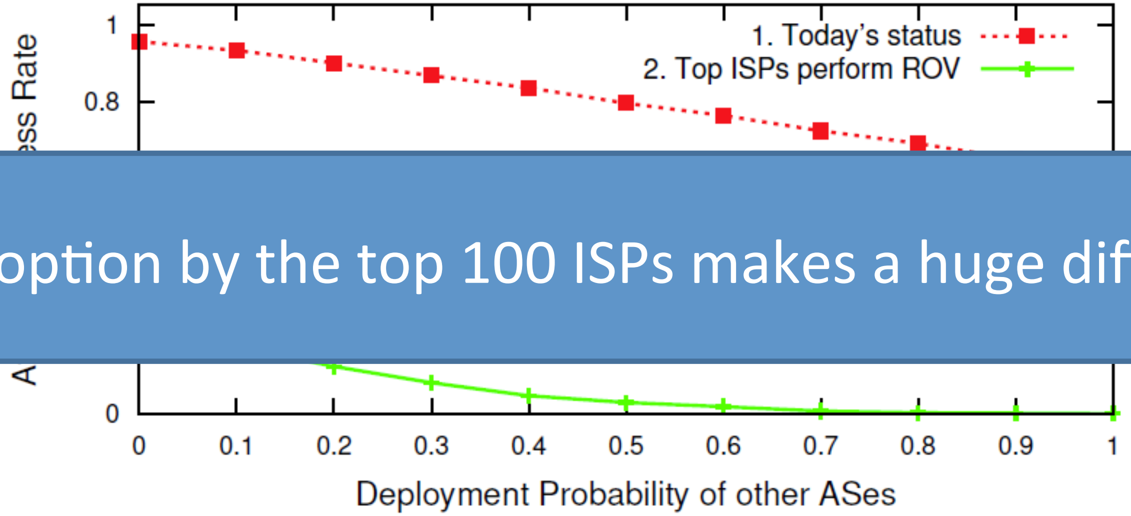
- Top ISP adopts with probability p (p=¼, ½, ¾, 1)
- Significant benefit only when p is high (p= ¾, 1)



Subprefix hijack success rate

Quantify Security in Partial Adoption

- Comparison between two scenarios:
  - today's status, as reflected by our measurements
  - all top 100 ISPs perform ROV
- Each other AS does ROV with fixed probability



Adoption by the top 100 ISPs makes a huge difference!

hijack
te

Security in Partial Adoption

Bottom line:

ROV enforcement by the top ISPs is both **necessary** and **sufficient** for substantial security benefits from RPKI

Getting RPKI Adopted: What Can We Improve?

- Information accuracy
  - ROAlert informs & alerts operators about:
    - Bad ROAs
    - Loose ROAs
    - Inter-org dependencies
- Preventing hijacks
  - Incentivize ROV adoption by the top ISPs!
  - Both sufficient and necessary for significant security benefits

Thank You!

This work will also appear at NDSS’17

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

Questions? ☺