Are We There Yet?
On RPKI Deployment and Security

Yossi Gilad

joint work with: Avichai Cohen,

Amir Herzberg, Michael Schapira, Haya Shulman

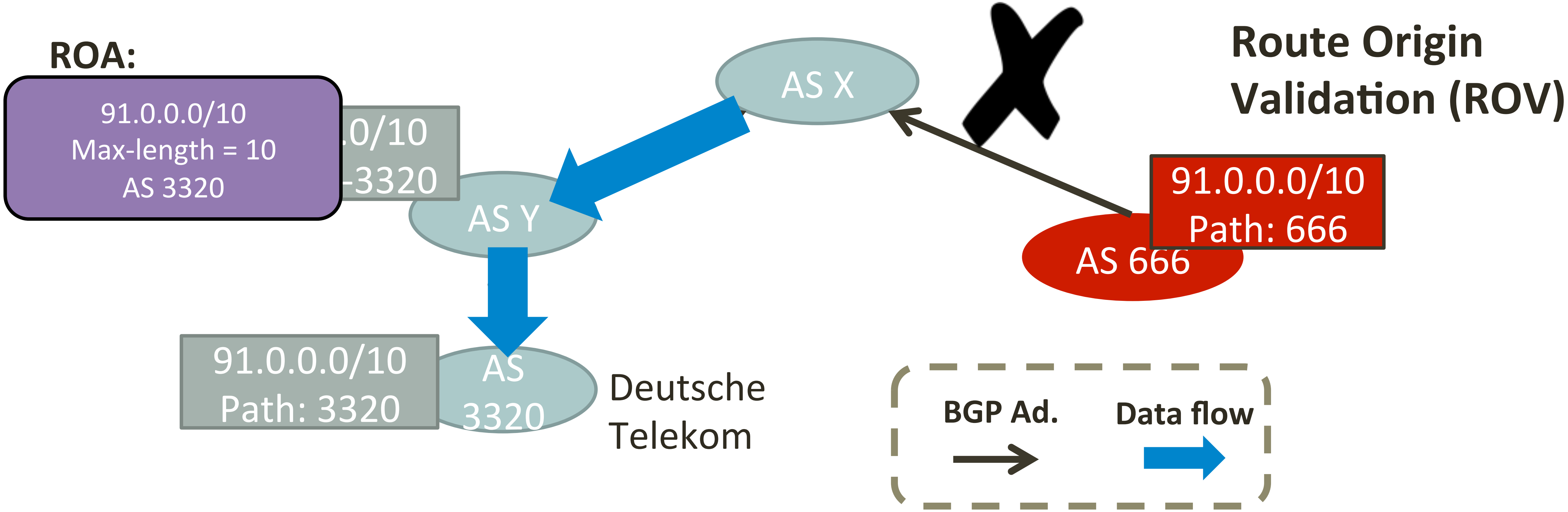
The Resource Public Key Infrastructure

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 advanced defenses against path-manipulation attacks on interdomain routing
  - BGPsec, SoBGP,…

RPKI Allows Route Origin Validation

Autonomous System (AS) X uses the RPKI to issue a **Route Origin Authorization (ROA)** mapping from 91.0/10 to AS 3320

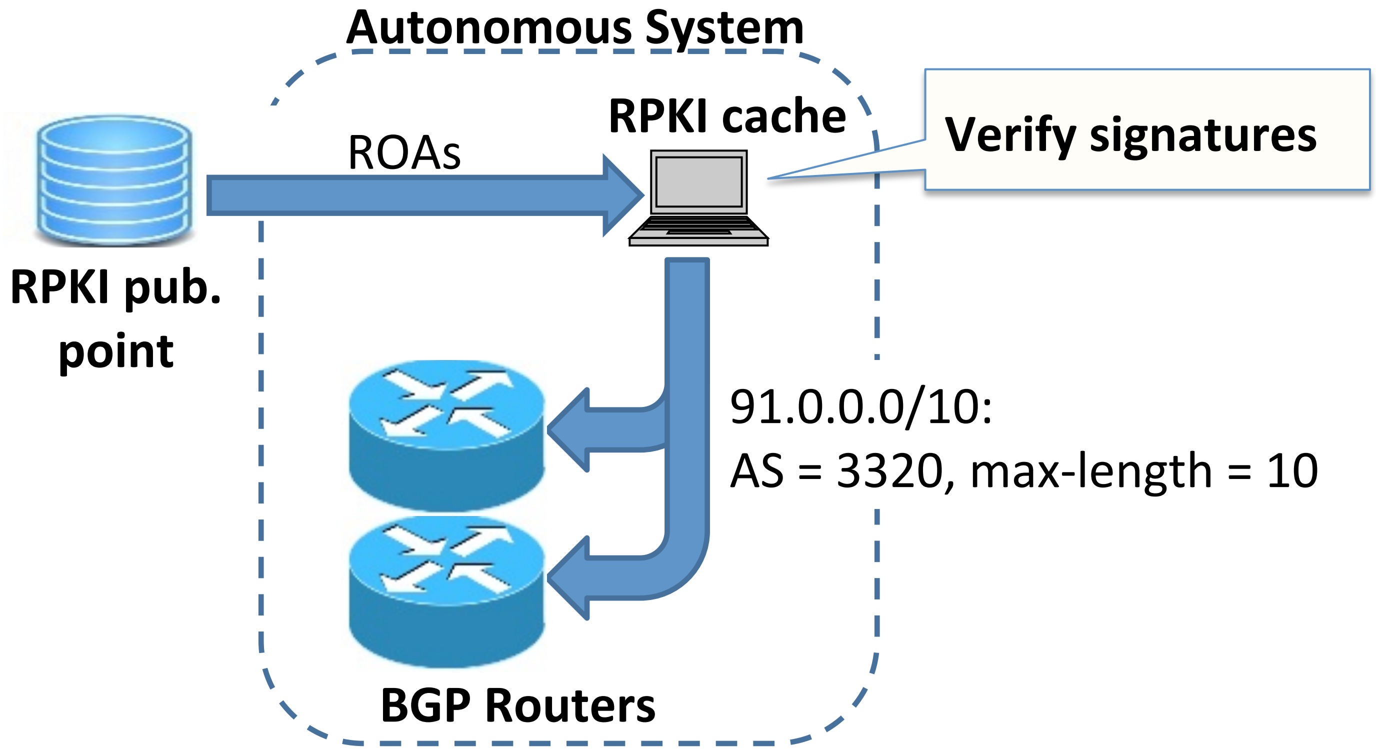


Talk Outline

- **ROV**
  - First measurements of ROV
  - How “good” is ROV in partial deployment?
- **ROAs**
  - Mistakes
  - Improving accuracy with ROAlert

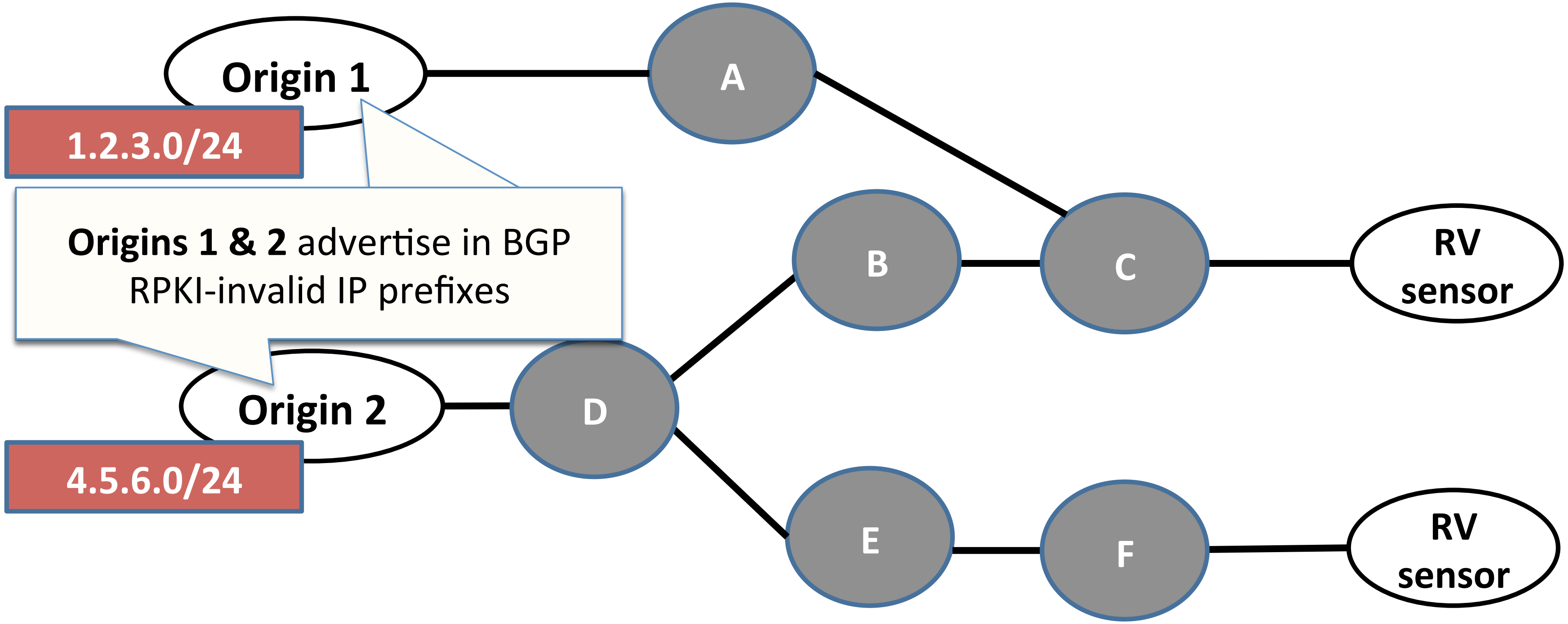
Filtering Bogus Advertisements

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



Measuring Non-ROV-Filtering ASes

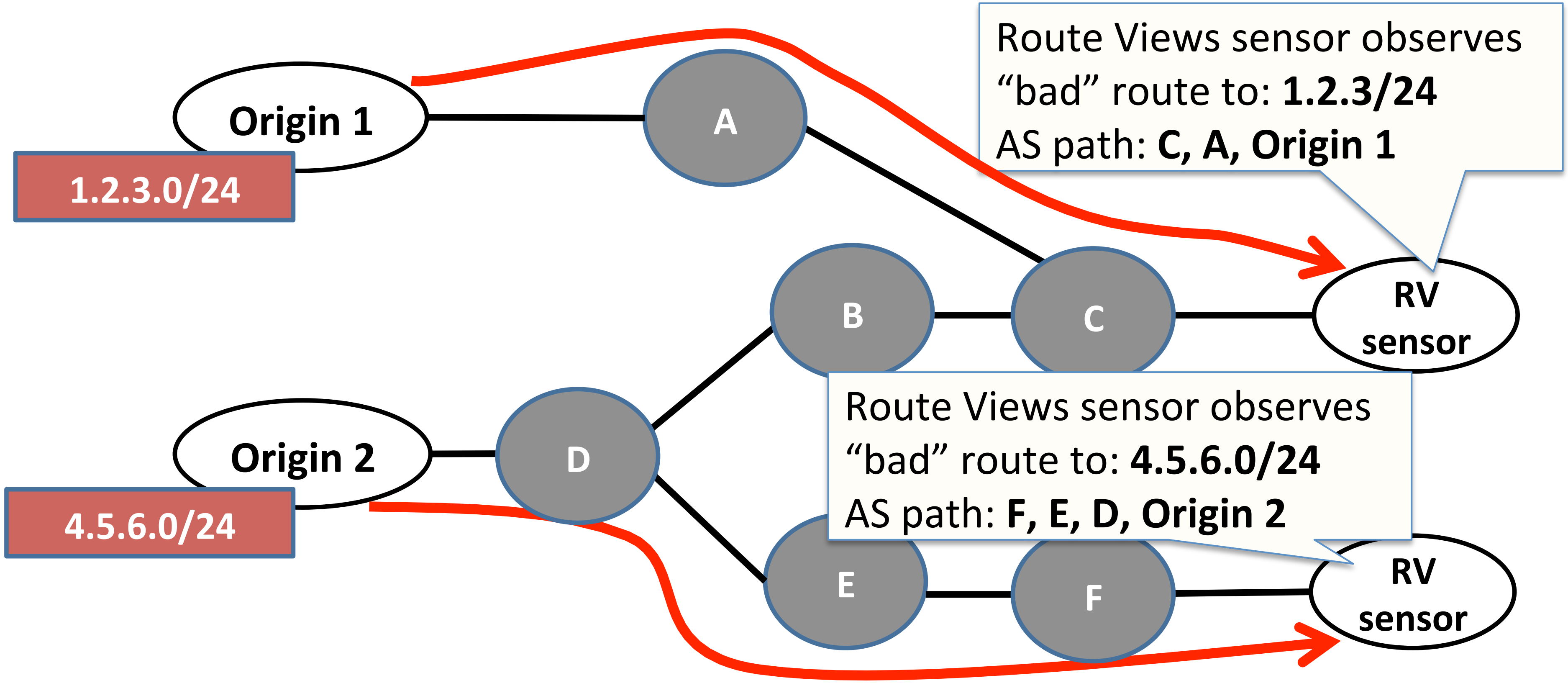
ASes that propagate invalid BGP advertisements do not perform filtering



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

Measuring Non-ROV-Filtering ASes

ASes that propagate invalid BGP advertisements do not perform filtering

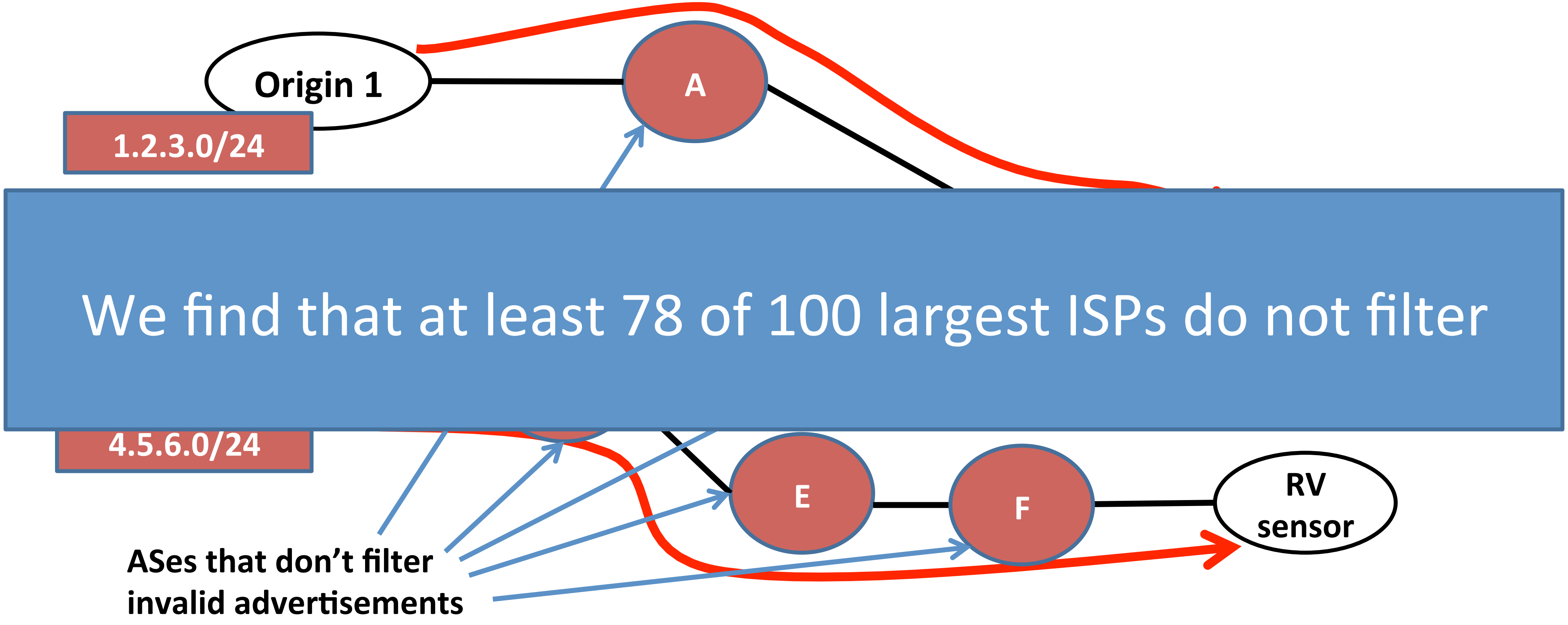


Route Views sensor observes "bad" route to: **1.2.3/24**
AS path: **C, A, Origin 1**

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

Measuring Non-ROV-Filtering ASes

ASes that propagate invalid BGP advertisements do not perform filtering

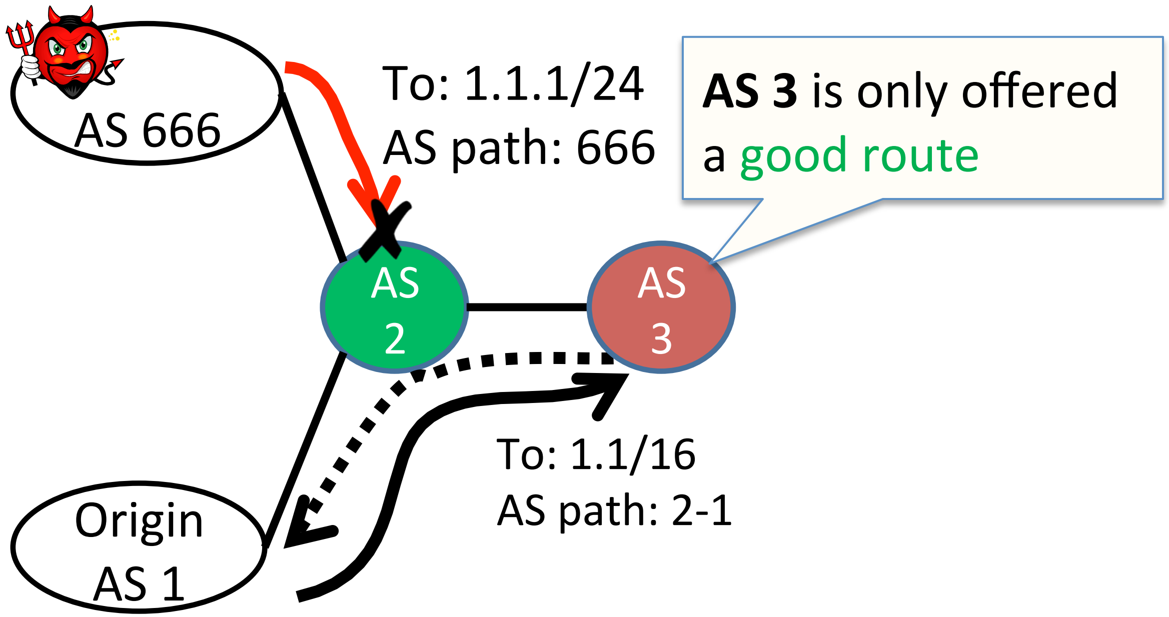


We find that at least 78 of 100 largest ISPs do not filter

What is the Impact of Partial ROV Adoption?

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

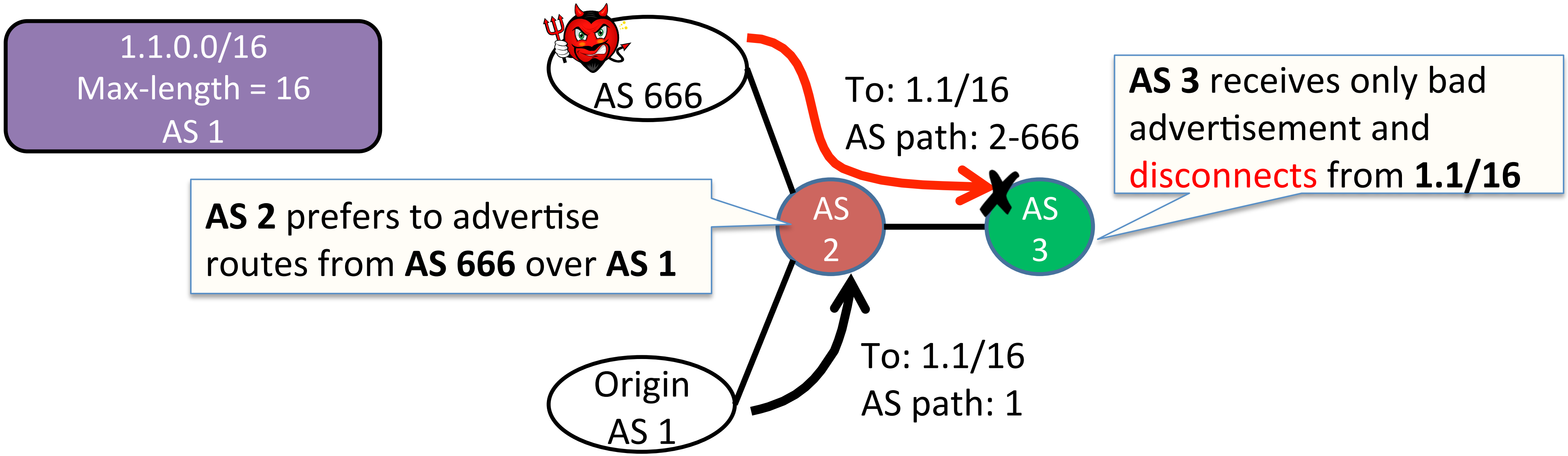
1.1.0.0/16
Max-length = 16
AS 1



AS 3 is only offered a good route

What is the Impact of Partial ROV Adoption?

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



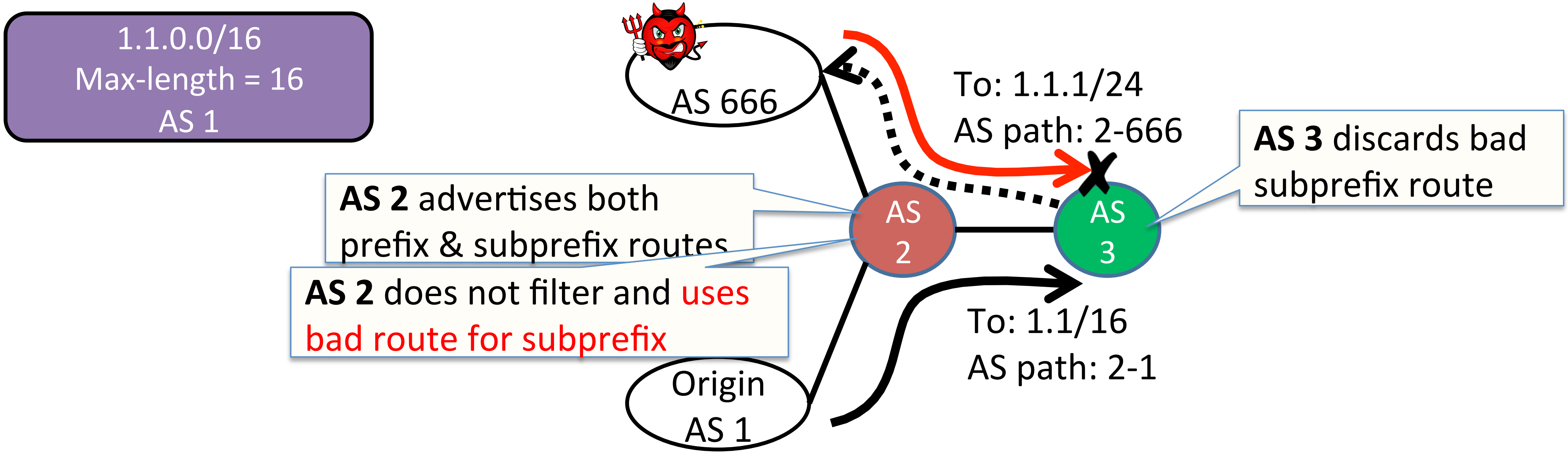
1.1.0.0/16
Max-length = 16
AS 1

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

To: 1.1.1/24
AS path: 2-666

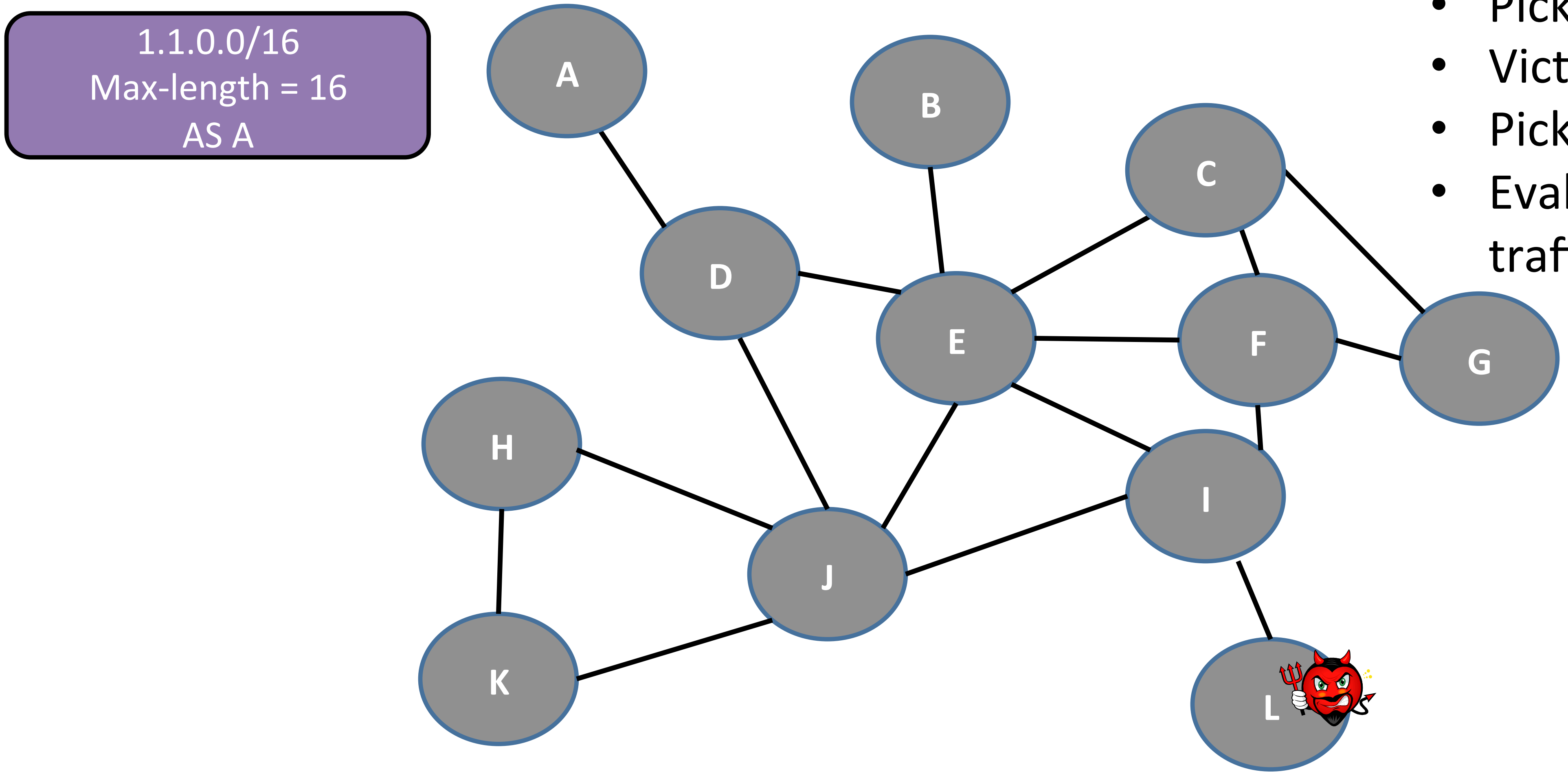
AS 3 discards bad subprefix route

AS 2 advertises both prefix & subprefix routes

AS 2 does not filter and uses bad route for subprefix

To: 1.1/16
AS path: 2-1

Quantify Security in Partial Adoption: Simulation Framework



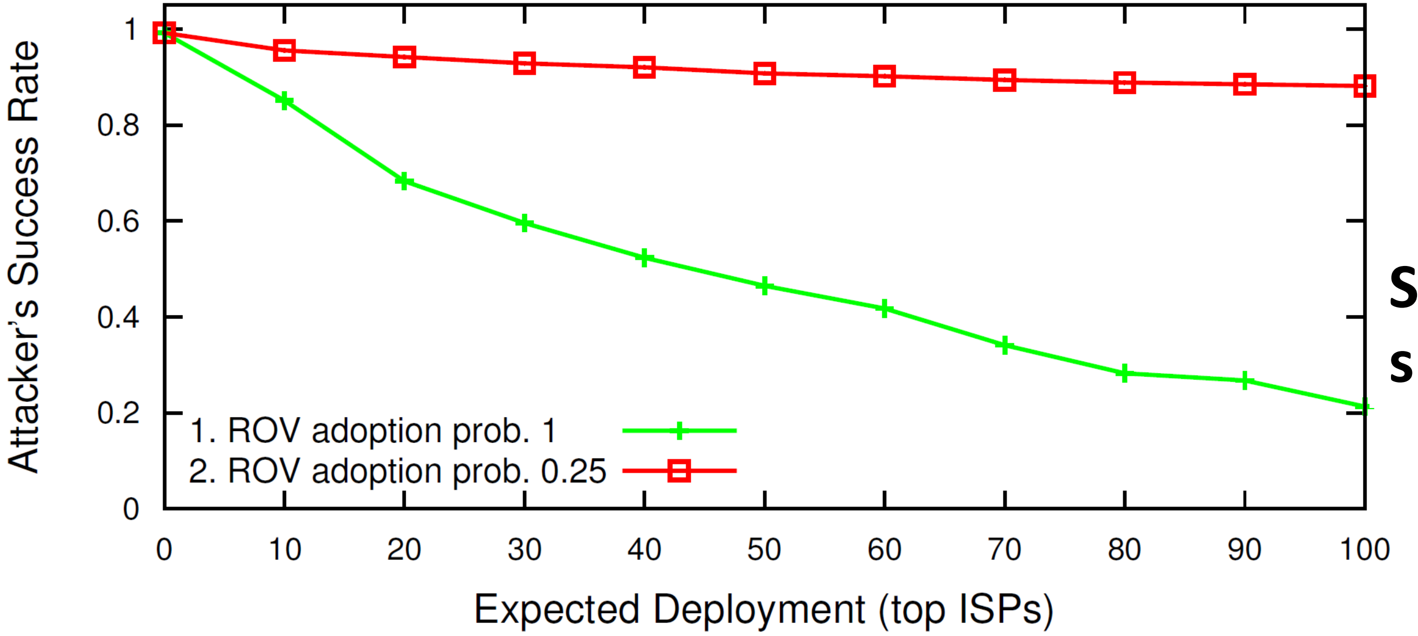
- Pick victim & attacker
- Victim's prefix has a ROA
- Pick set of ASes doing ROV
- Evaluate which ASes send traffic to the attacker

Empirically-derived AS-level network from CAIDA

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

Quantify Security in Partial Adoption

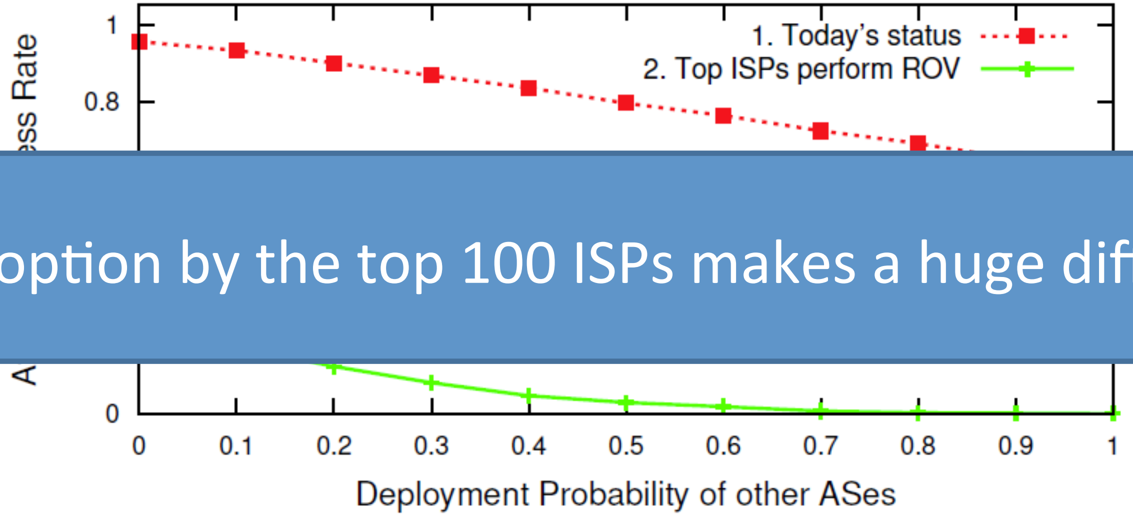
- Top ISP adopts with probability *p*
- Significant benefit only when *p* is high



Subprefix hijack success rate

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

Talk Outline

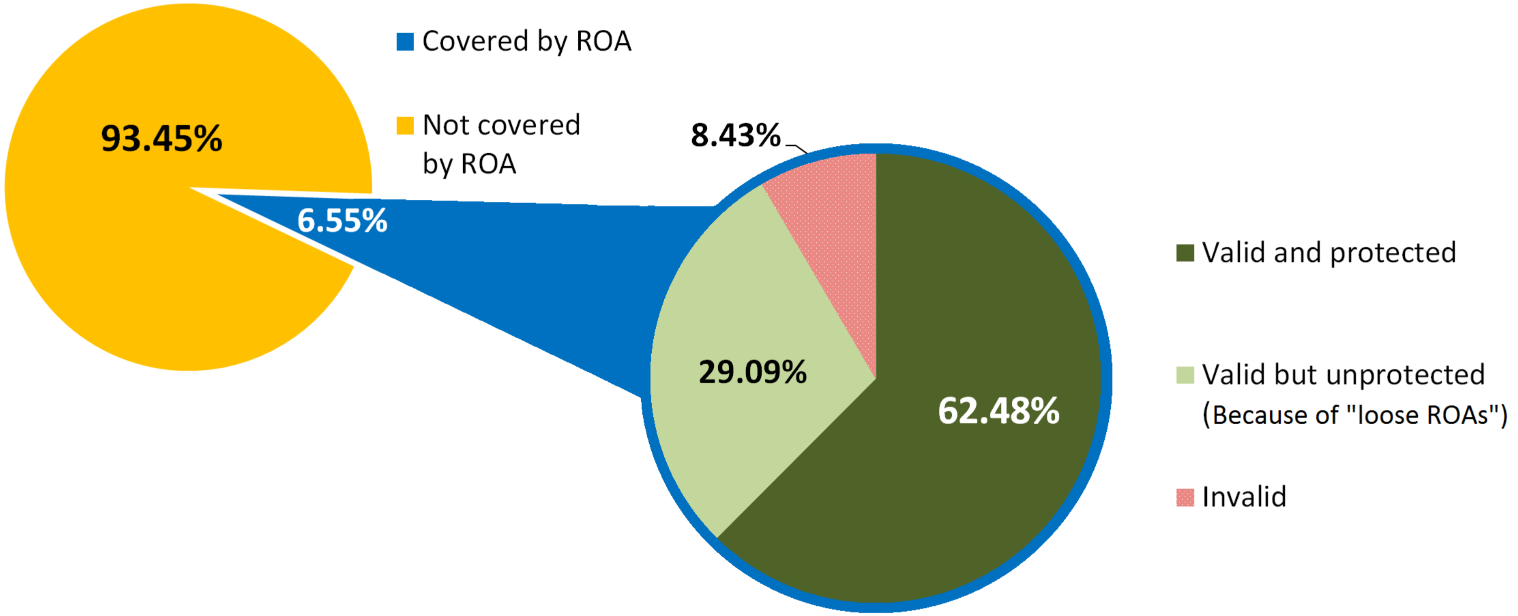
- **Security in partial ROV deployment**
  - First measurements of ROV
  - How “good” is ROV in partial deployment?

- **ROAs**
  - Mistakes
  - Improving accuracy with ROAlert

Mistakes in ROAs

Many 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]

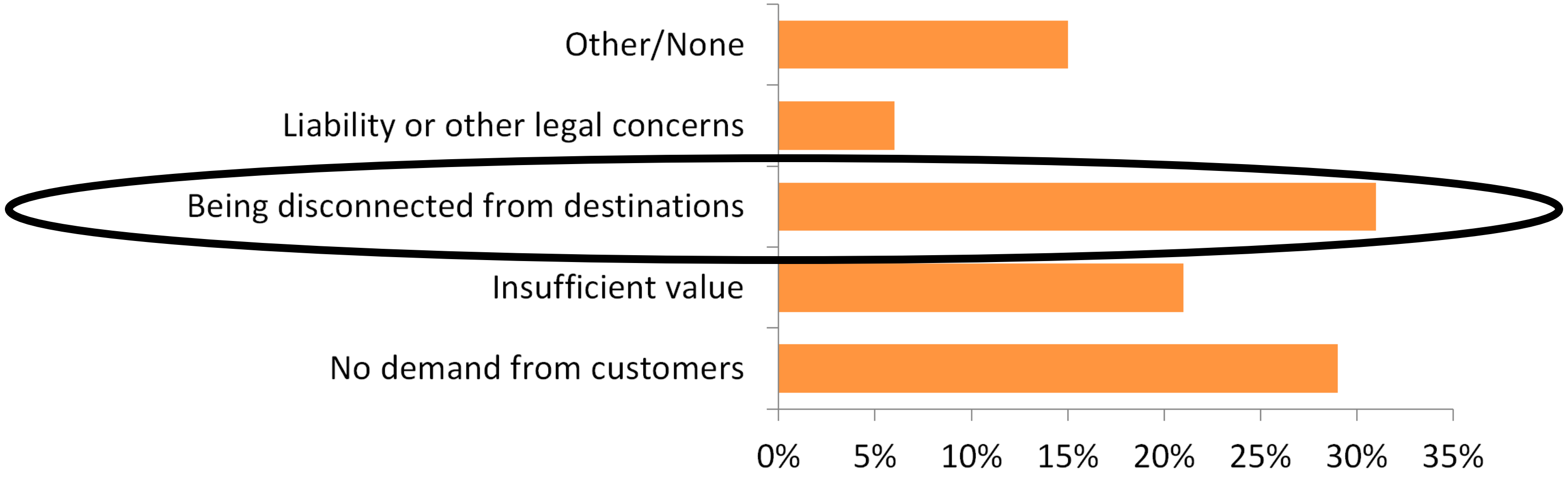


Bad ROAs

Concern for disconnection was pointed out in our survey

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

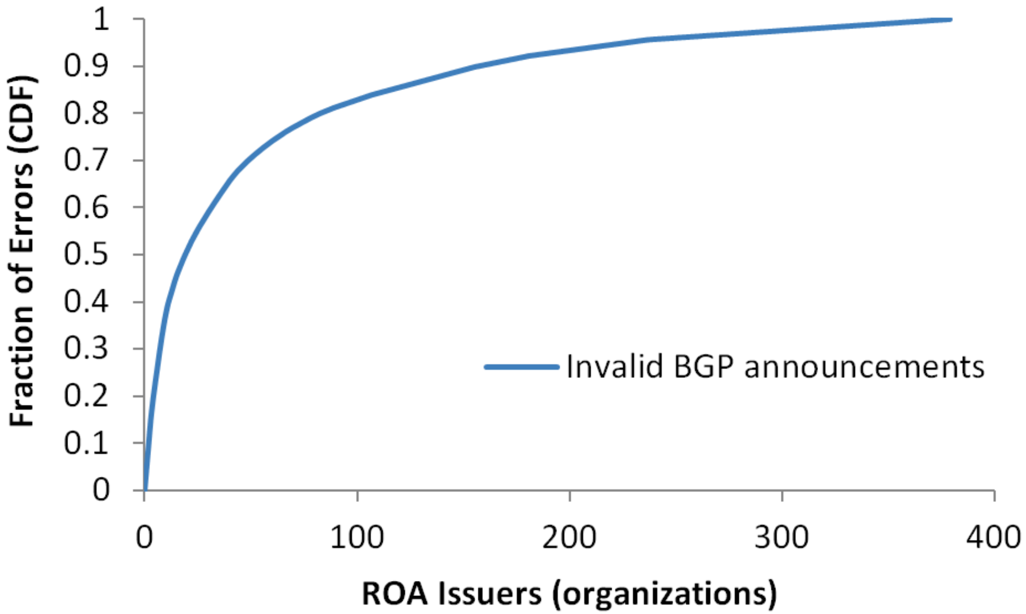
What are your main concerns regarding executing RPKI-based origin authentication in your network?



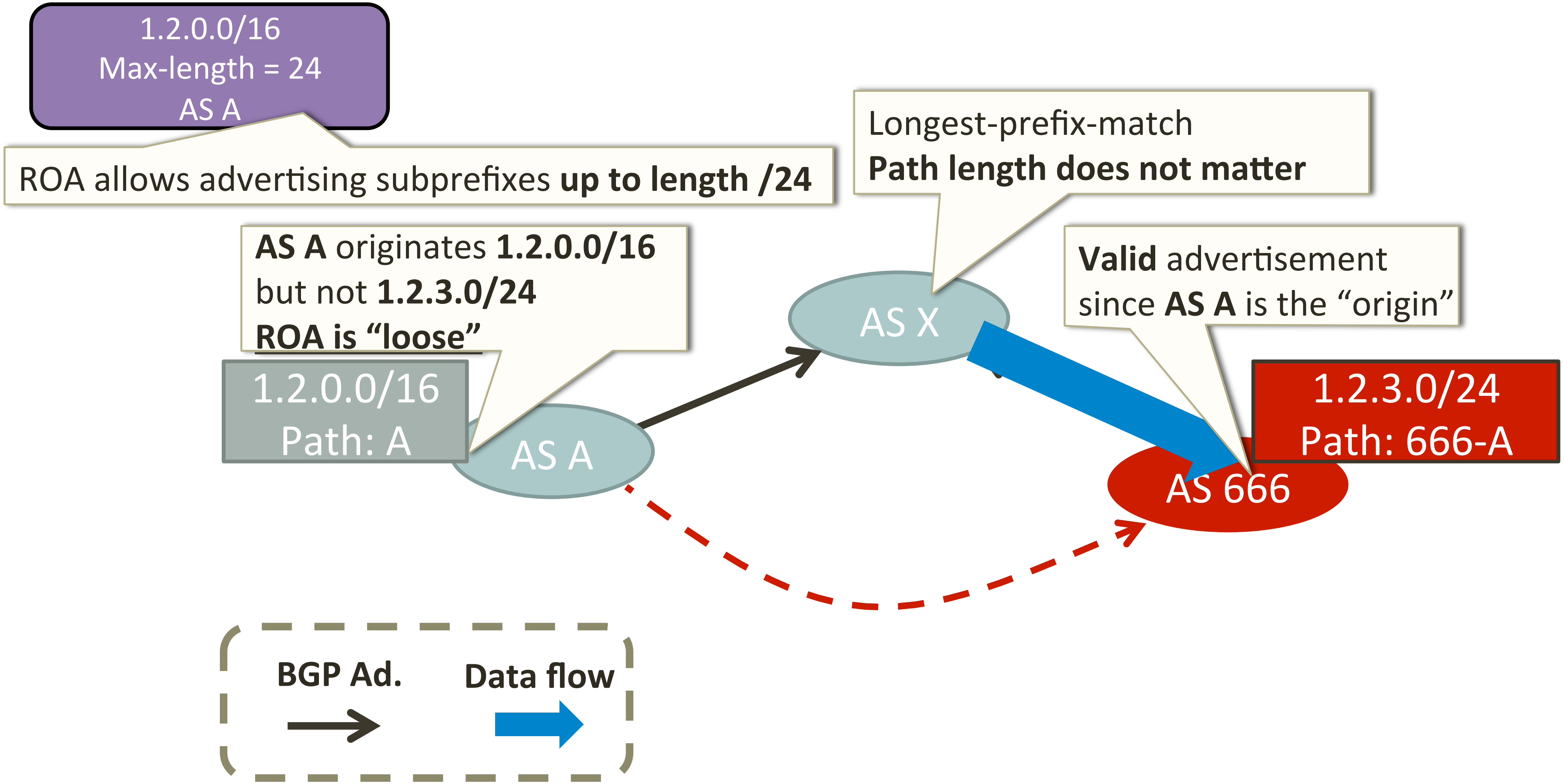
Bad ROAs

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



Insecure Deployment: 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"

Insecure Deployment: Loose ROAs

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

Improving Accuracy with ROAlert

- roalert.org allows to check whether networks are protected by ROAs
  - … and if not, why not
- Online, proactive notification system
  - constantly monitoring
  - not opt-in
- Retrieves ROAs from the RPKI and compares them against BGP advs.
- 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

Conclusion

- The RPKI can be very effective in preventing hijacks
  - Incentivize ROV adoption by the top ISPs!
  - Both sufficient and necessary for significant security benefits

- Information accuracy is a major challenge
  - ROAlert informs & alerts operators about:
    - Bad ROAs
    - Loose ROAs

Thank You!

Questions? ☺