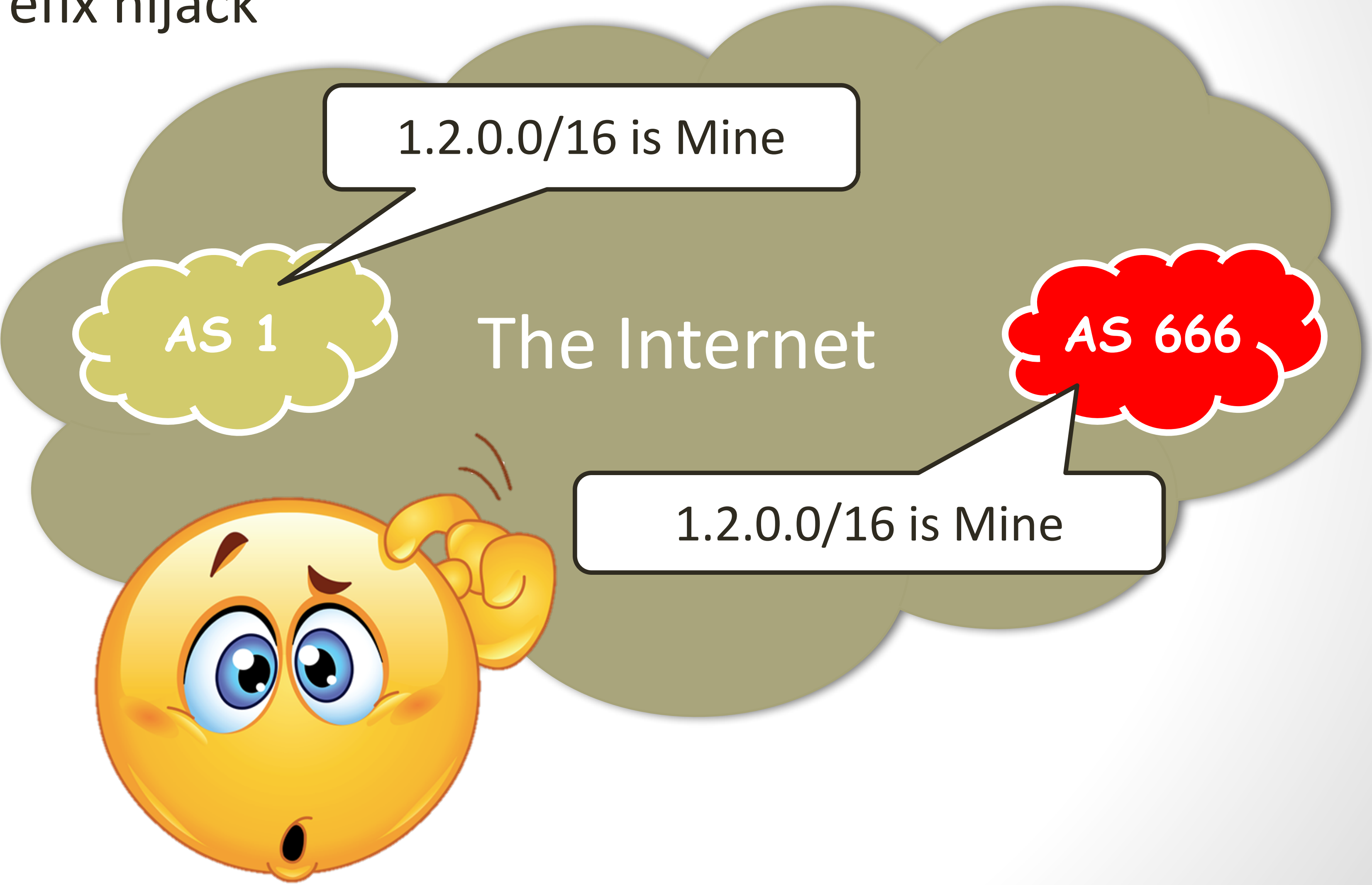
Jumpstarting BGP Security

Yossi Gilad

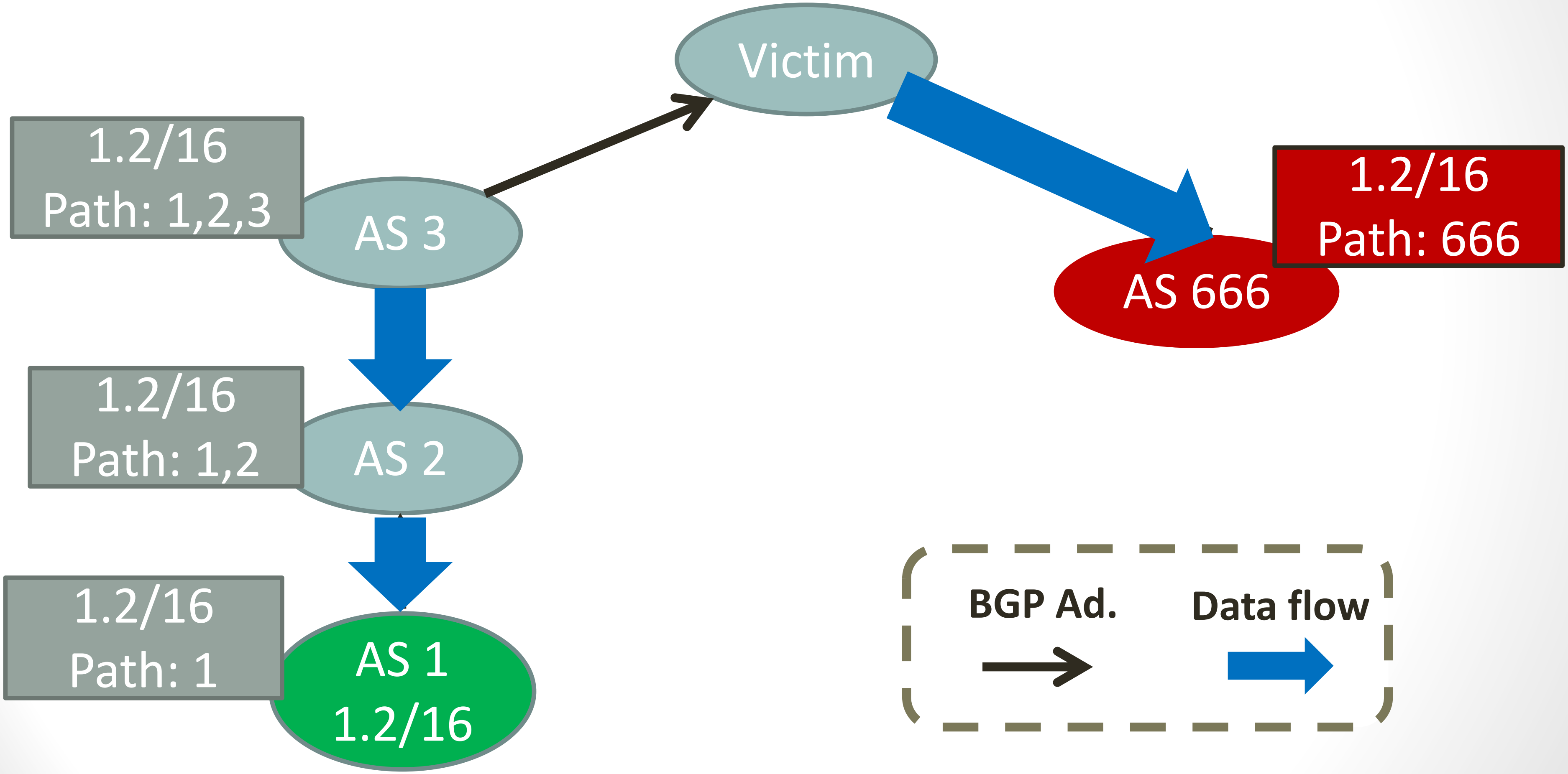
Joint work with: Avichai Cohen, Amir Herzberg, and Michael Schapira

BGP is insecure!

- Prefix hijack

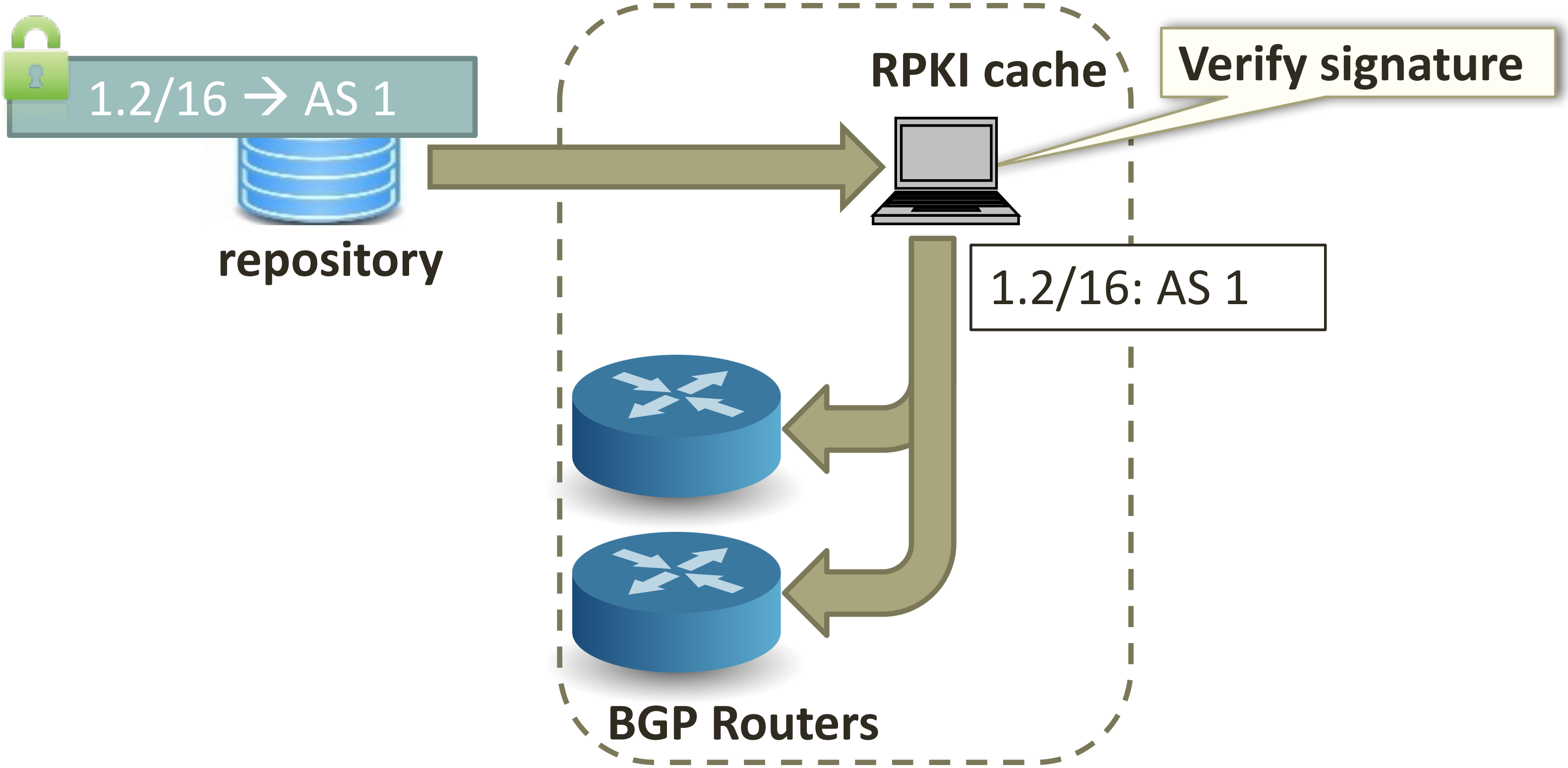


BGP is insecure! Prefix hijacks



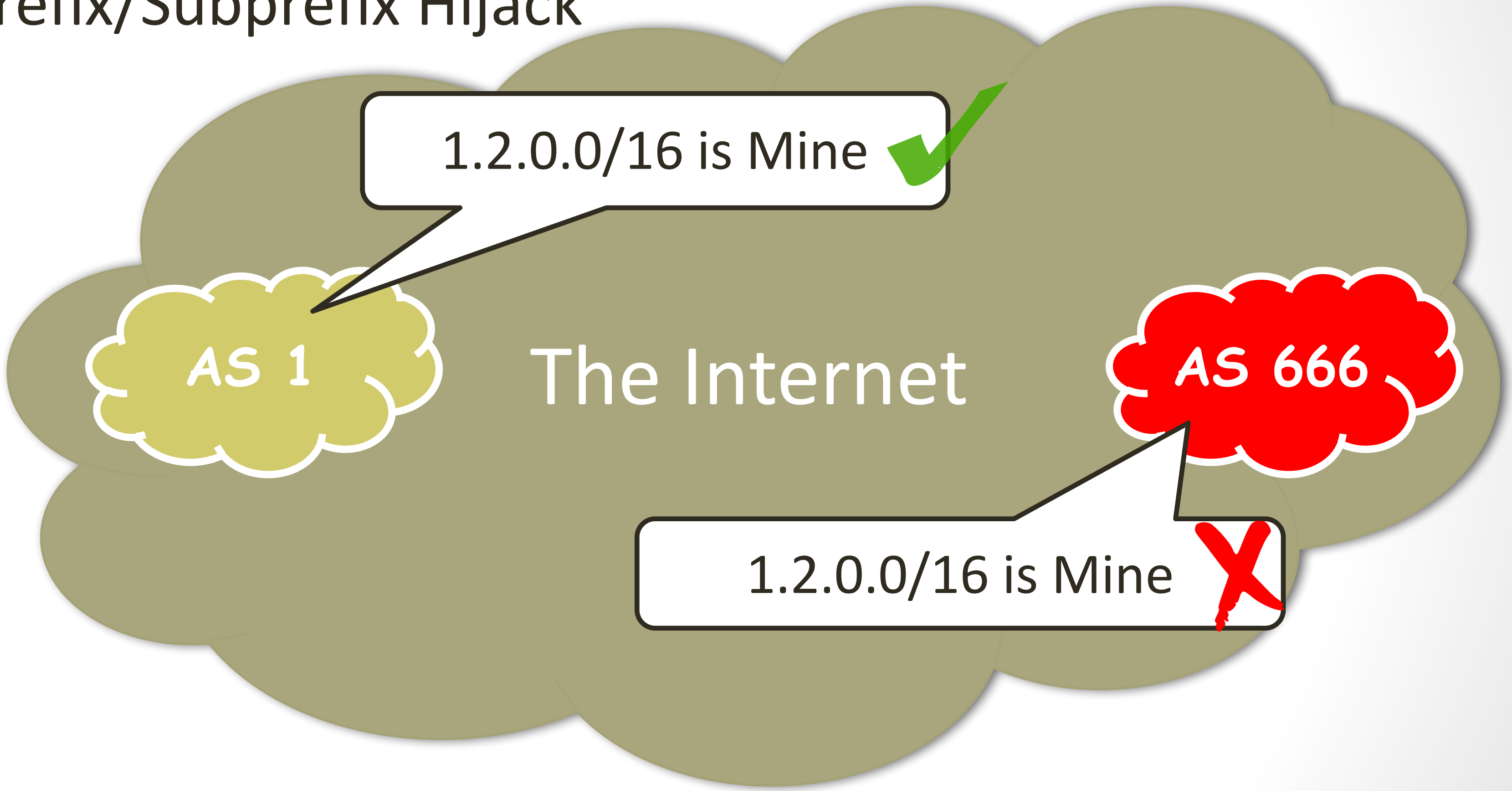
Resource PKI (RPKI)

- Origin Authentication
  - Protects against prefix/subprefix hijacks
  - Slowly gaining traction (protects 6% of prefixes)

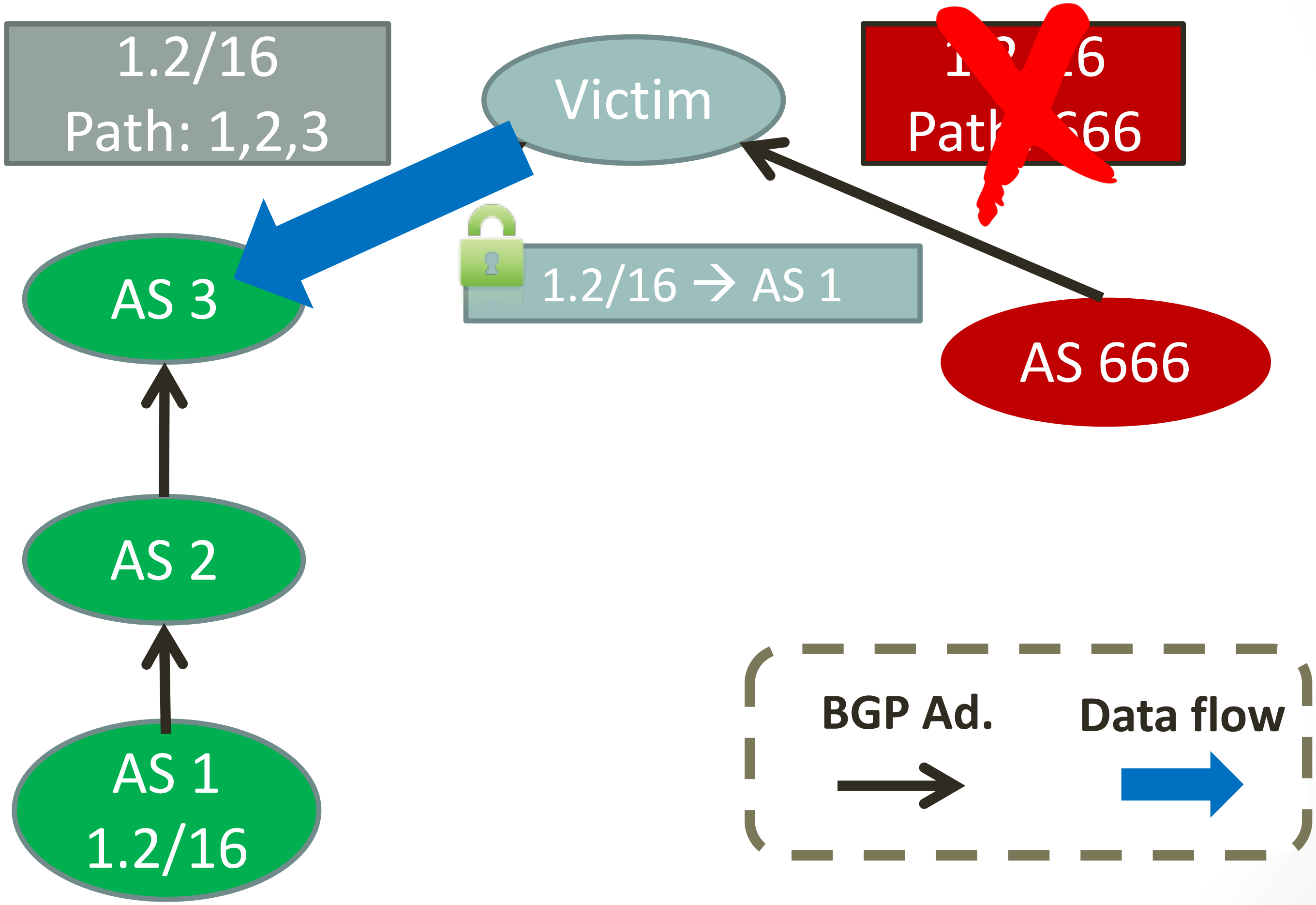


BGP is insecure!

- Prefix/Subprefix Hijack



RPKI prevents prefix hijacks



1.2/16
Path: 1,2,3

Victim

~~1.2/16~~
~~Path: 666~~

AS 3

1.2/16 → AS 1

AS 666

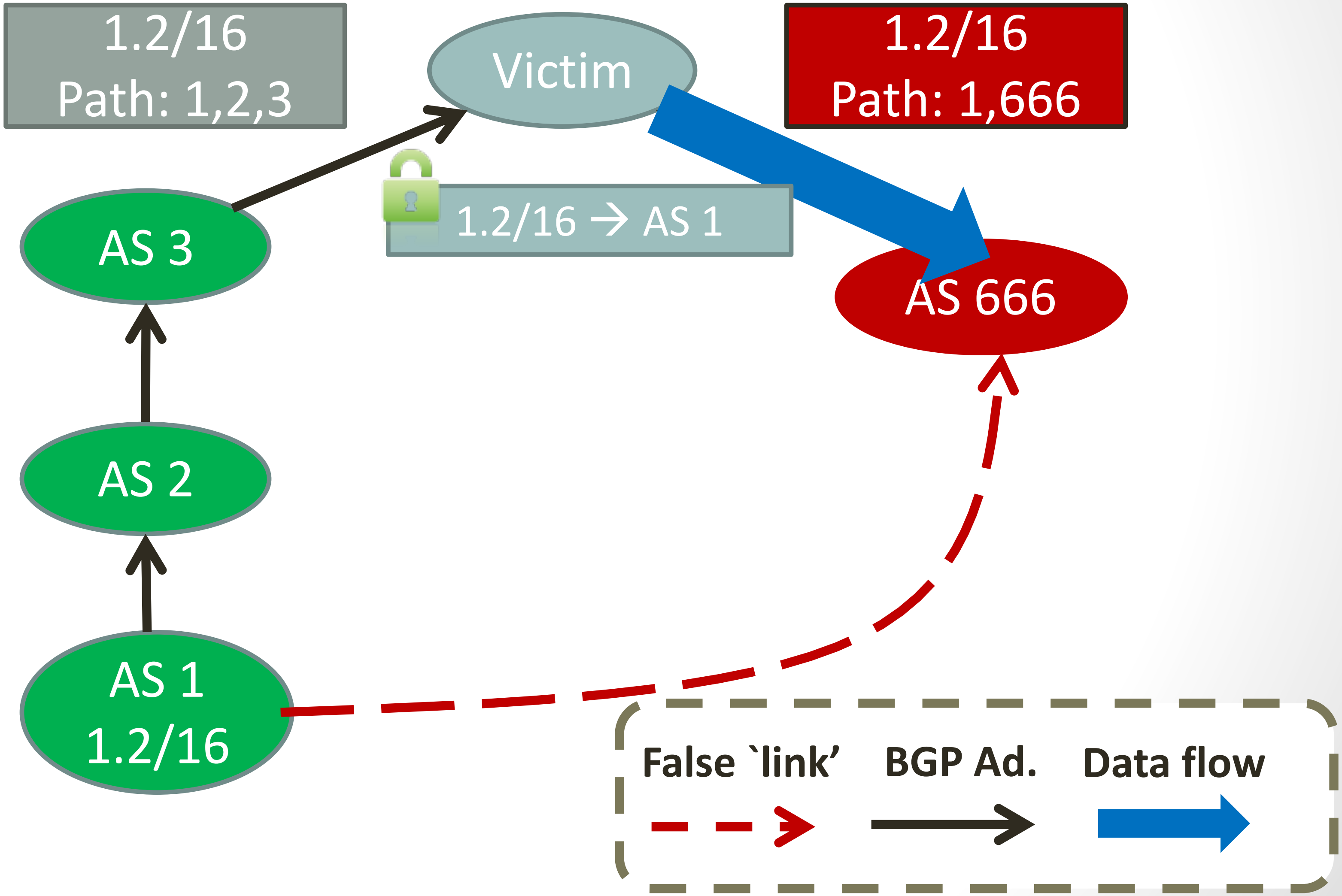
AS 2

AS 1
1.2/16

BGP Ad.

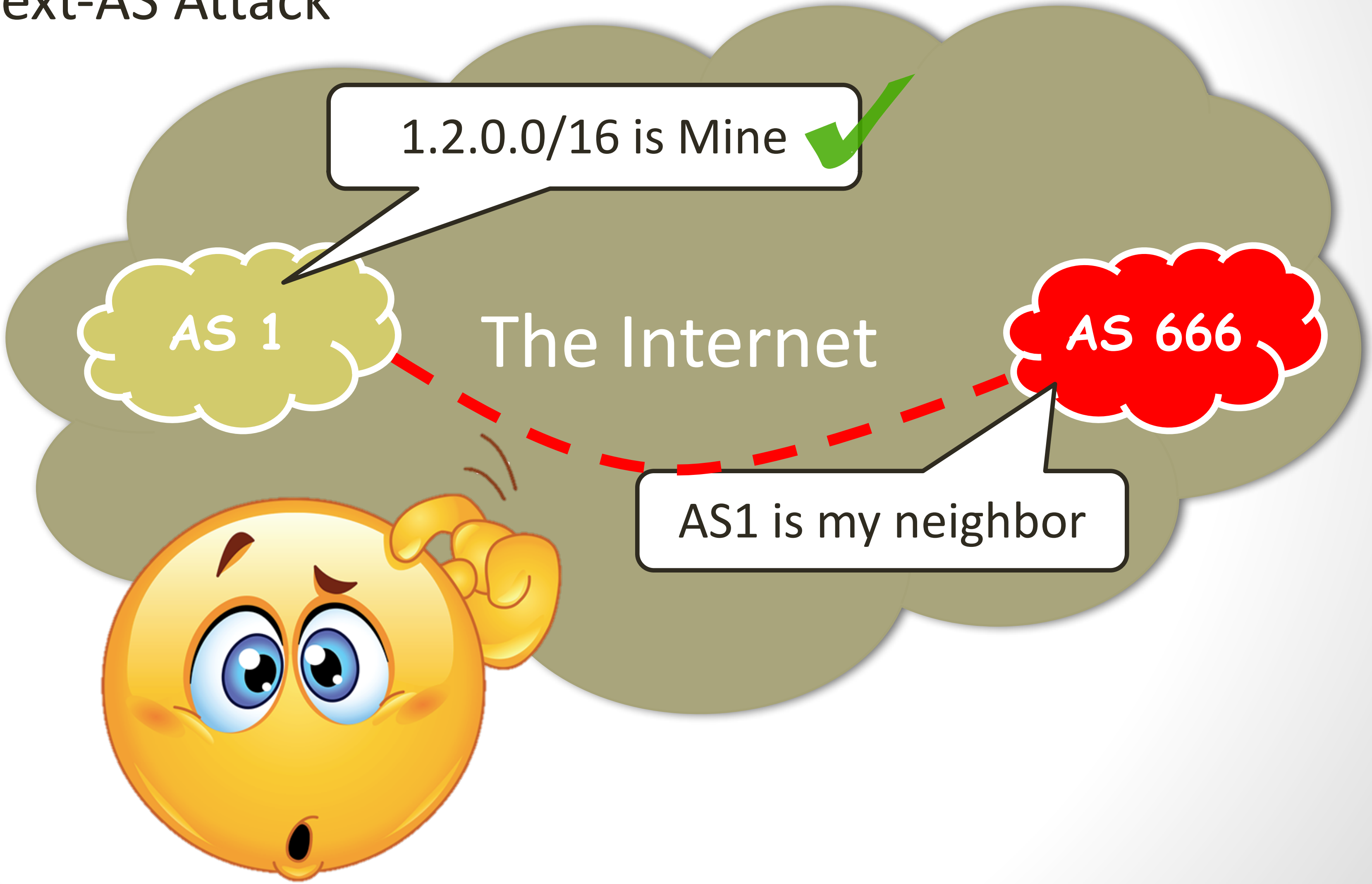
Data flow

Next-AS attack circumvents RPKI



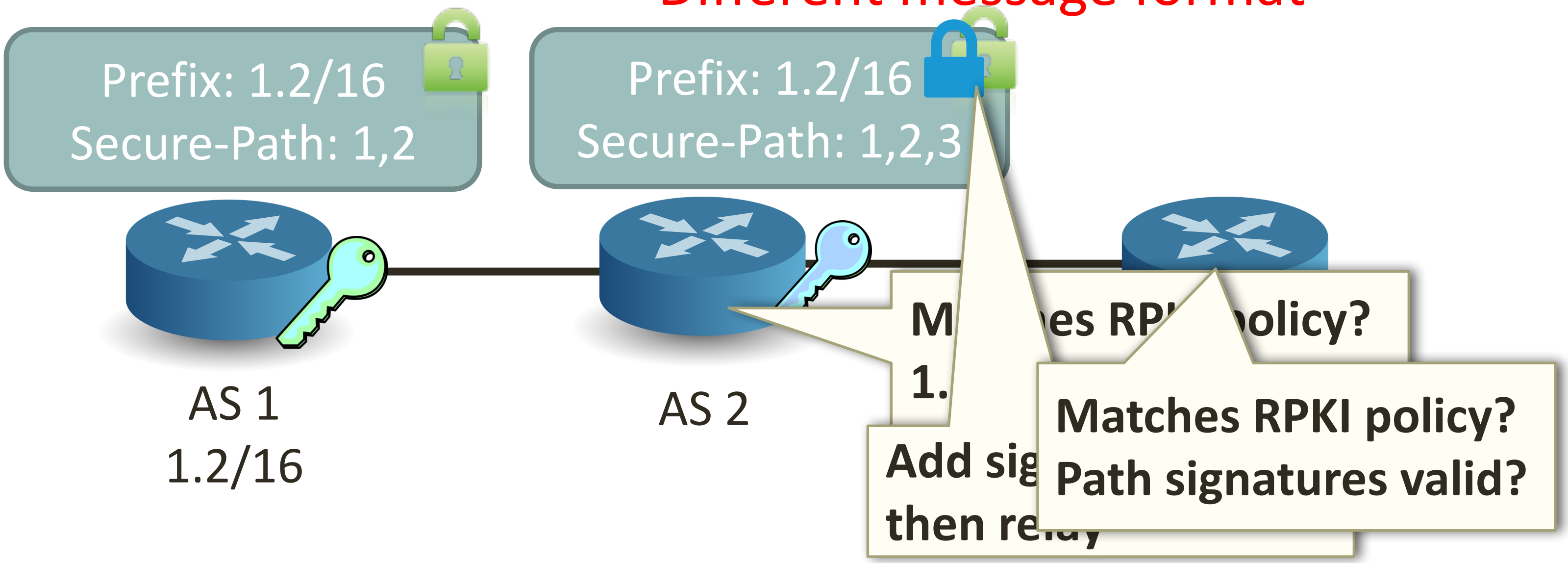
BGP is insecure!

- Next-AS Attack



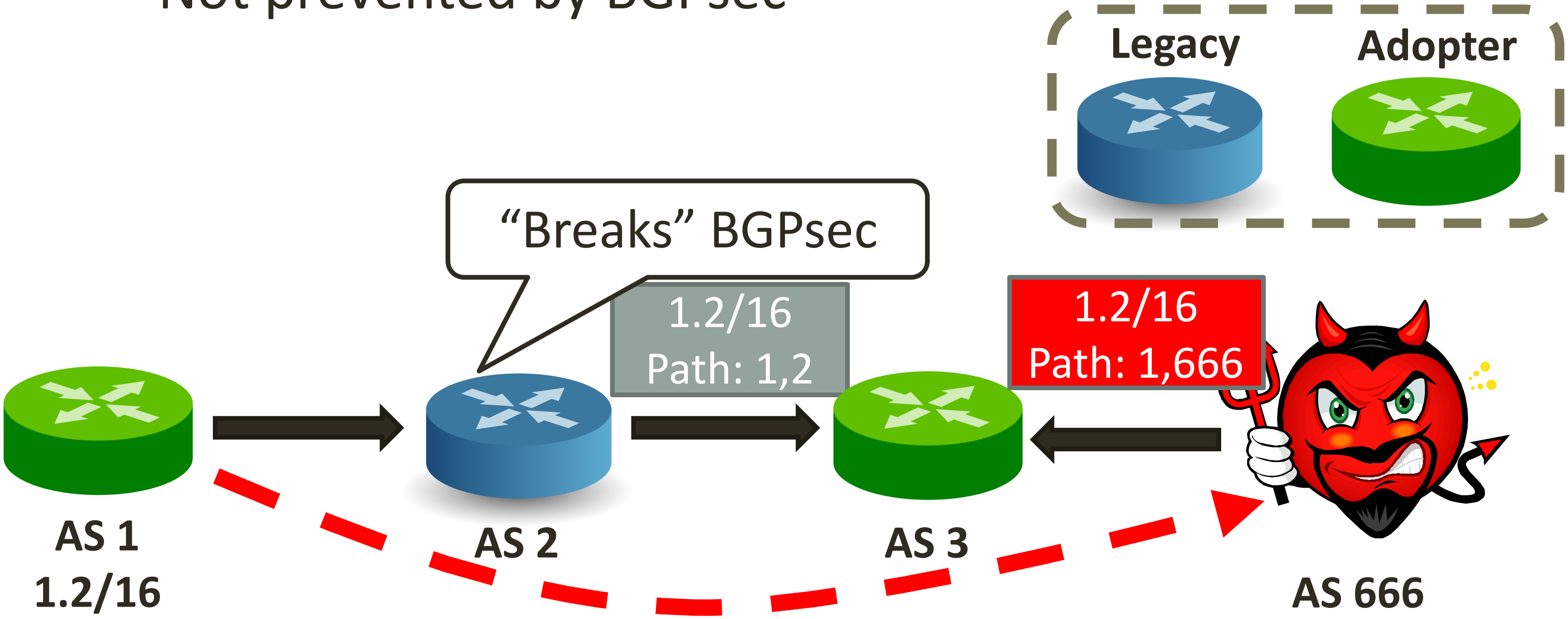
Current paradigm: a two step solution

- 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

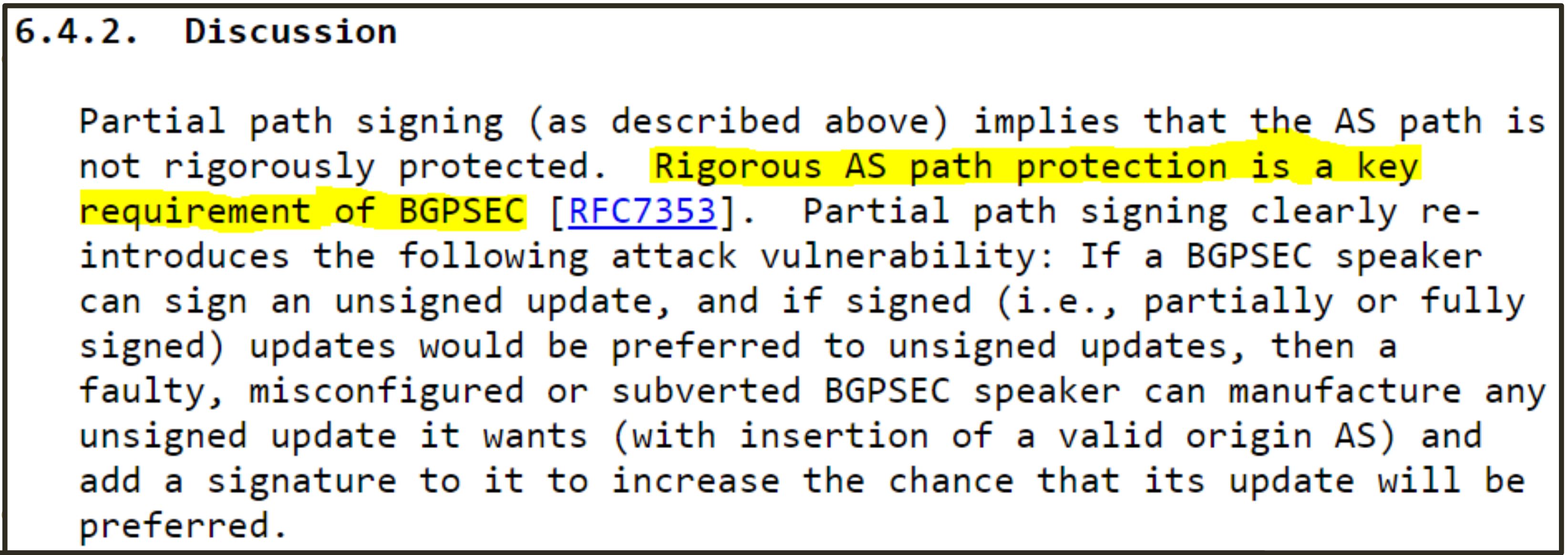


BGPsec in partial adoption? Meager benefits [Lychev et al., SIGCOMM'13]

- AS 666 launches a next-AS attack against AS 1
  - Not prevented by BGPsec



BGPsec: deployment challenges



6.4.2. **Discussion**

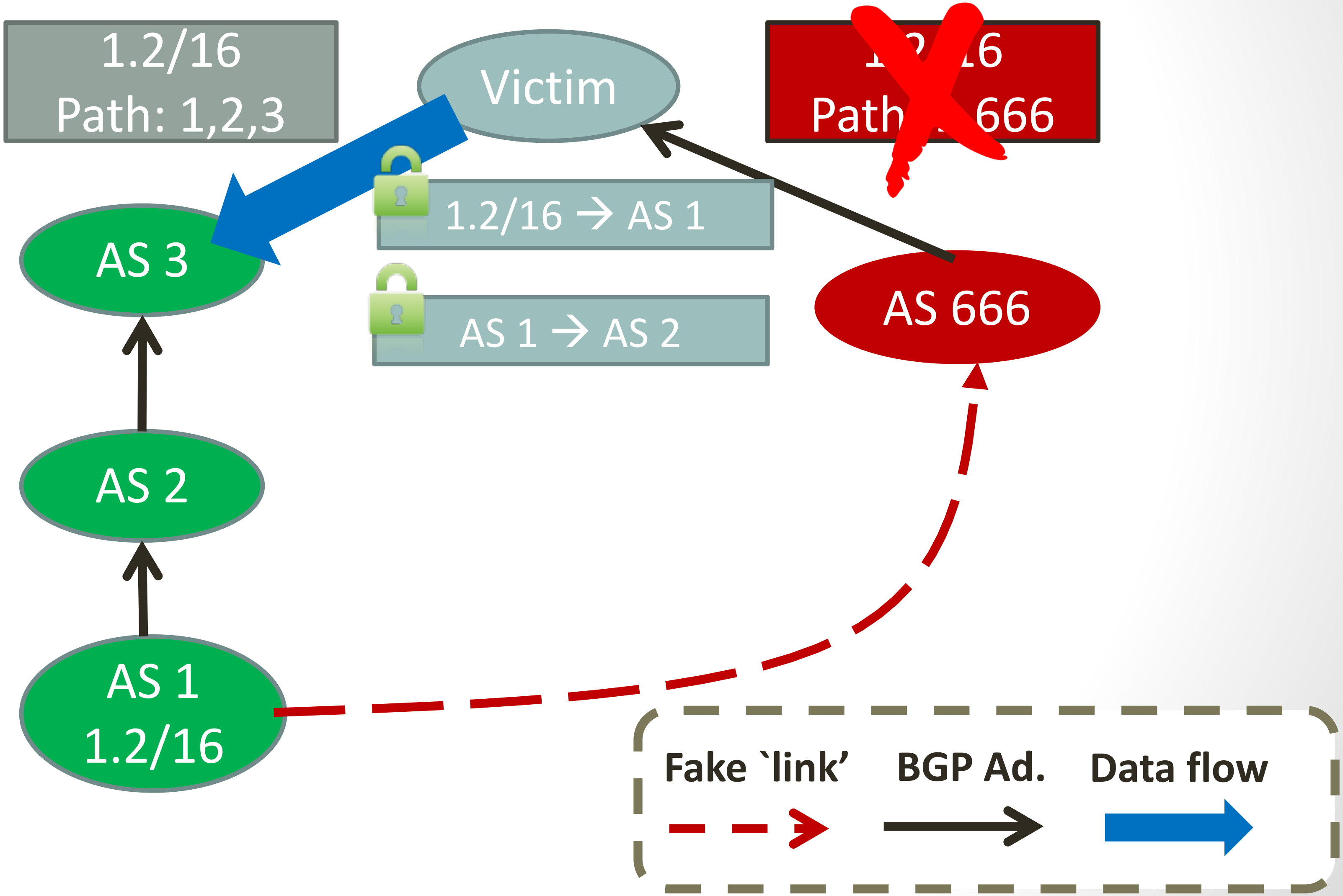
Partial path signing (as described above) implies that the AS path is not rigorously protected. Rigorous AS path protection is a key requirement of BGPSEC [RFC7353]. Partial path signing clearly re-introduces the following attack vulnerability: If a BGPSEC speaker can sign an unsigned update, and if signed (i.e., partially or fully signed) updates would be preferred to unsigned updates, then a faulty, misconfigured or subverted BGPSEC speaker can manufacture any unsigned update it wants (with insertion of a valid origin AS) and add a signature to it to increase the chance that its update will be preferred.

BGPSEC Design Choices and Summary of Supporting Discussions
draft-sriram-bgpsec-design-choices-08

Goals

- Easy deployment, minimal overhead
  - Signatures and verifications: only **offline, off-router**
- Significant security benefits in partial deployment
- No changes to routing protocol

Path-end validation



1.2/16
Path: 1,2,3

Victim

~~1.2/16~~
~~Path: 1,666~~

1.2/16 → AS 1

AS 1 → AS 2

AS 3

AS 2

AS 1
1.2/16

AS 666

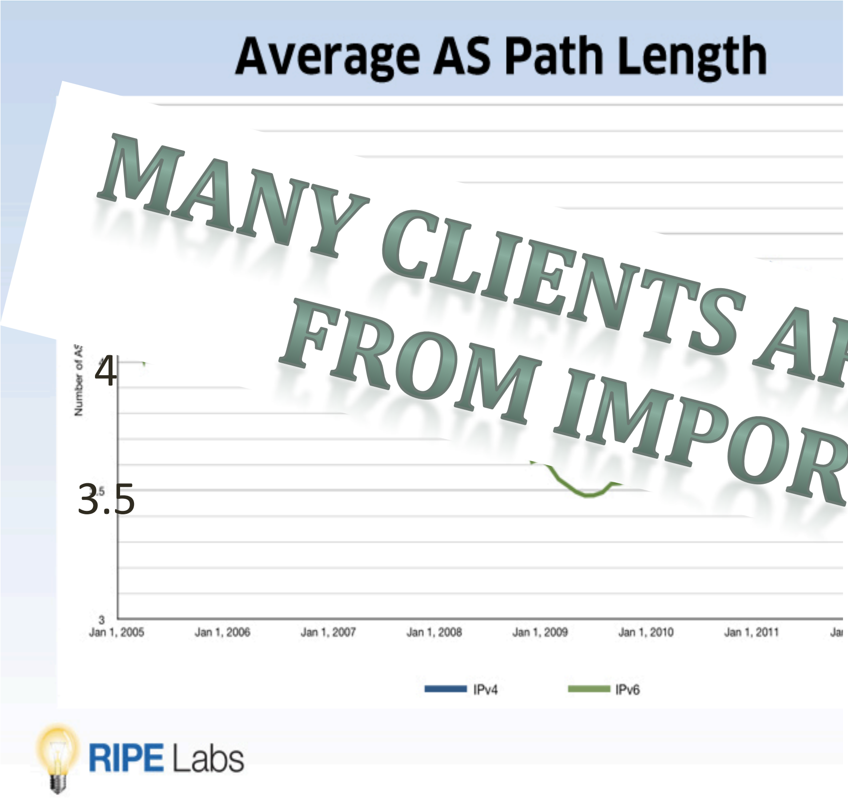
Fake `link' – – ➤

BGP Ad. ⟶

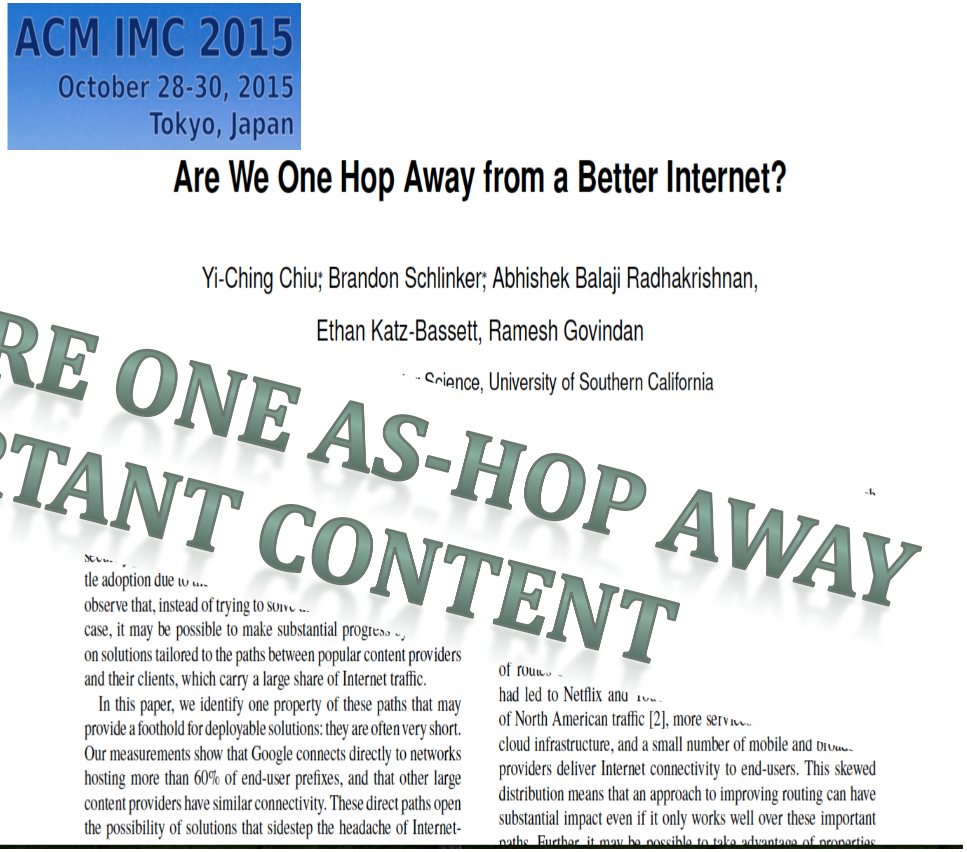
Data flow ➡

Path-end validation

- Key insight: **“last hop” is critical**
- Extend RPKI to authenticate the “last hop”



MANY CLIENTS ARE ONE AS-HOP AWAY FROM IMPORTANT CONTENT


ACM IMC 2015
October 28-30, 2015
Tokyo, Japan

Are We One Hop Away from a Better Internet?

Yi-Ching Chiu*, Brandon Schlinker*, Abhishek Balaji Radhakrishnan,
Ethan Katz-Bassett, Ramesh Govindan
Science, University of Southern California

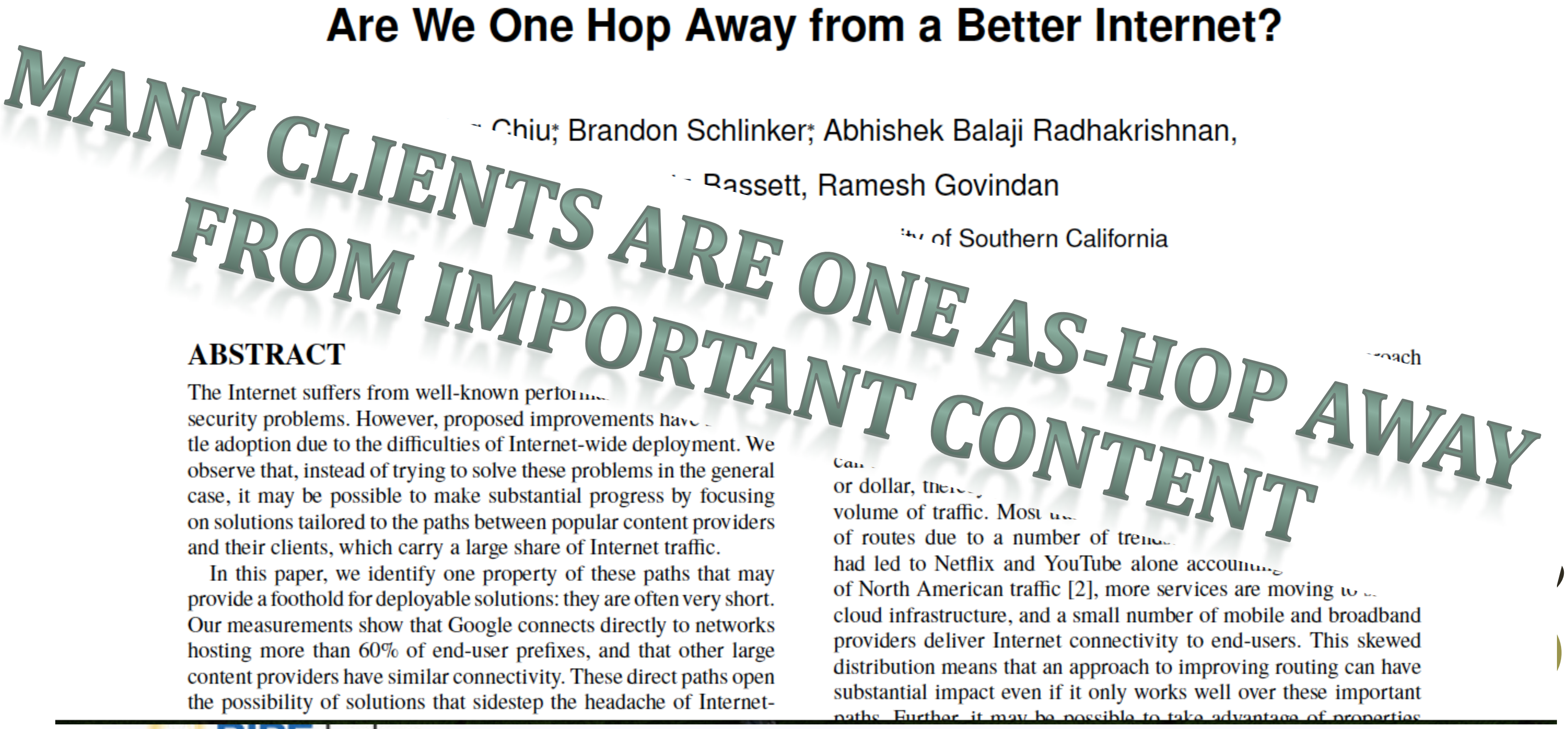
tle adoption due to th
observe that, instead of trying to solve
case, it may be possible to make substantial progress
on solutions tailored to the paths between popular content providers and their clients, which carry a large share of Internet traffic.

In this paper, we identify one property of these paths that may provide a foothold for deployable solutions: they are often very short. Our measurements show that Google connects directly to networks hosting more than 60% of end-user prefixes, and that other large content providers have similar connectivity. These direct paths open the possibility of solutions that sidestep the headache of Internet-

of route
had led to Netflix and You
of North American traffic [2], more servic
cloud infrastructure, and a small number of mobile and broad
providers deliver Internet connectivity to end-users. This skewed distribution means that an approach to improving routing can have substantial impact even if it only works well over these important paths. Further, it may be possible to take advantage of properties

Path-end validation

- ACM IMC 2015
  October 28-30, 2015
  Tokyo, Japan



Are We One Hop Away from a Better Internet?

Chiu; Brandon Schlinker; Abhishek Balaji Radhakrishnan,

Bassett, Ramesh Govindan

of Southern California

ABSTRACT

The Internet suffers from well-known perform security problems. However, proposed improvements have tle adoption due to the difficulties of Internet-wide deployment. We observe that, instead of trying to solve these problems in the general case, it may be possible to make substantial progress by focusing on solutions tailored to the paths between popular content providers and their clients, which carry a large share of Internet traffic.

In this paper, we identify one property of these paths that may provide a foothold for deployable solutions: they are often very short. Our measurements show that Google connects directly to networks hosting more than 60% of end-user prefixes, and that other large content providers have similar connectivity. These direct paths open the possibility of solutions that sidestep the headache of Internet-

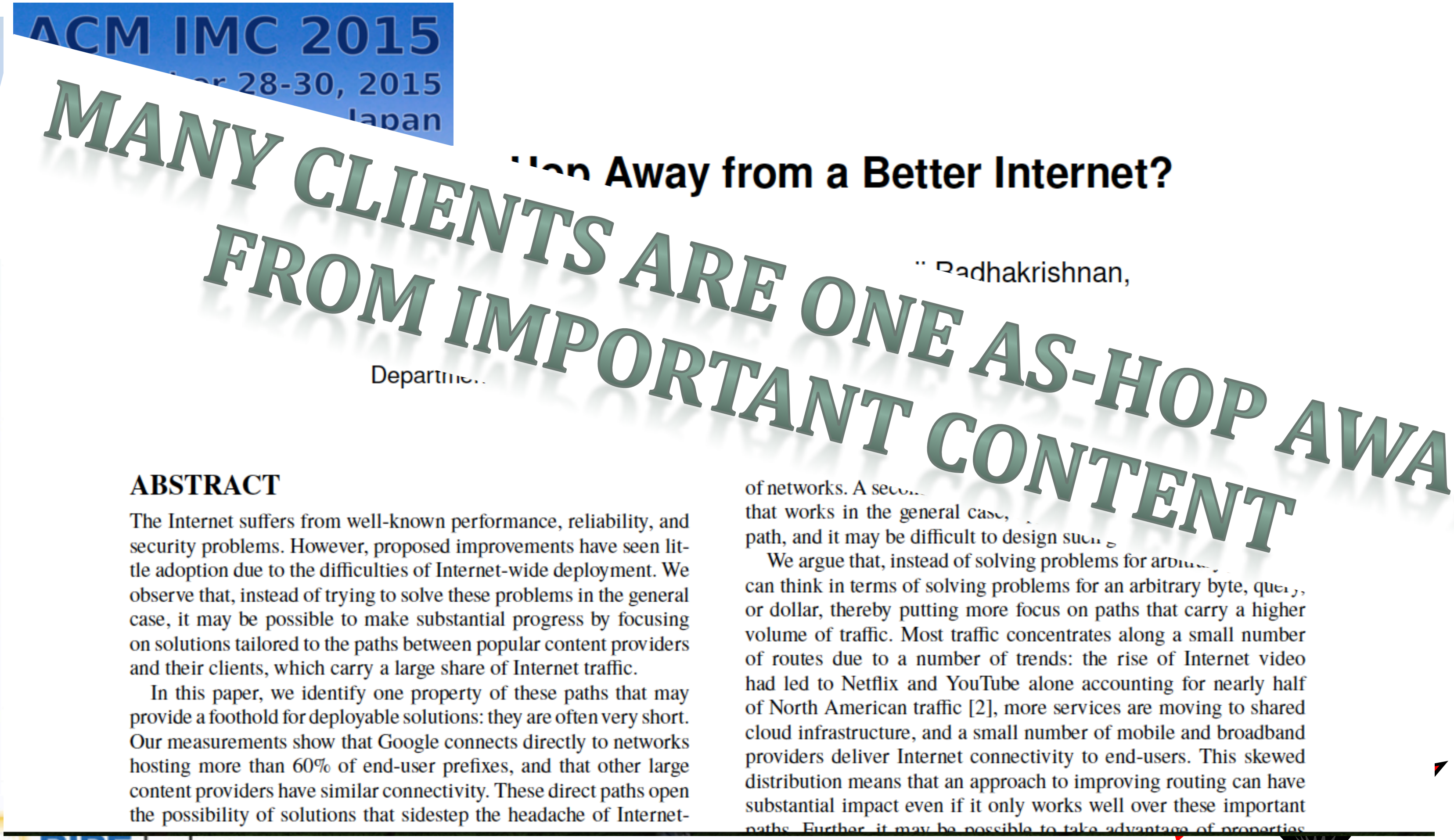
roach

or dollar, there volume of traffic. Most of routes due to a number of trends had led to Netflix and YouTube alone accounting of North American traffic [2], more services are moving to cloud infrastructure, and a small number of mobile and broadband providers deliver Internet connectivity to end-users. This skewed distribution means that an approach to improving routing can have substantial impact even if it only works well over these important paths. Further, it may be possible to take advantage of properties

MANY CLIENTS ARE ONE AS-HOP AWAY FROM IMPORTANT CONTENT

RIPE Labs

Intuition



ACM IMC 2015

er 28-30, 2015

Japan

Hop Away from a Better Internet?

Radhakrishnan,

Departm

ABSTRACT

The Internet suffers from well-known performance, reliability, and security problems. However, proposed improvements have seen little adoption due to the difficulties of Internet-wide deployment. We observe that, instead of trying to solve these problems in the general case, it may be possible to make substantial progress by focusing on solutions tailored to the paths between popular content providers and their clients, which carry a large share of Internet traffic.

In this paper, we identify one property of these paths that may provide a foothold for deployable solutions: they are often very short. Our measurements show that Google connects directly to networks hosting more than 60% of end-user prefixes, and that other large content providers have similar connectivity. These direct paths open the possibility of solutions that sidestep the headache of Internet-

of networks. A seco that works in the general case, path, and it may be difficult to design such

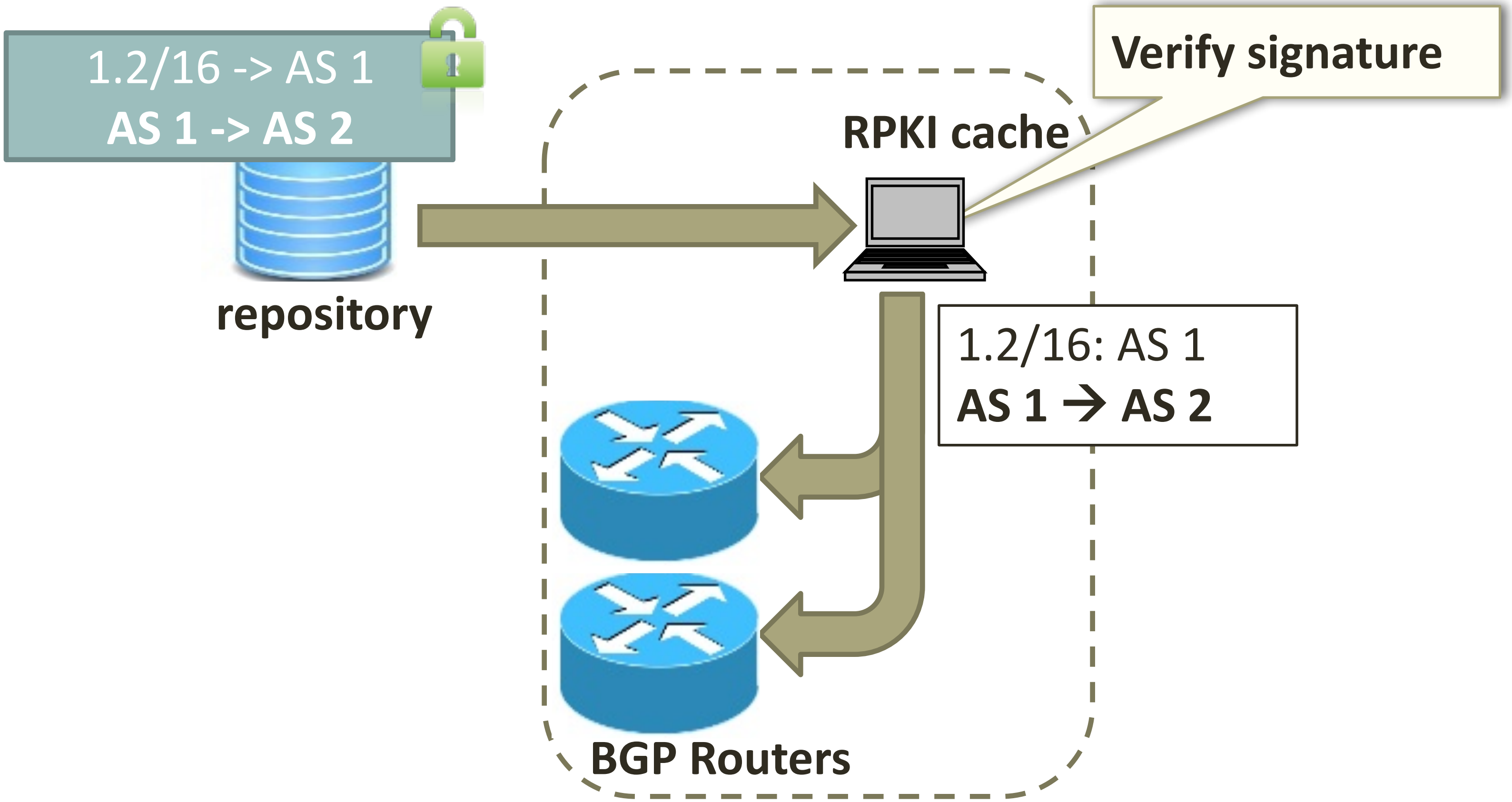
We argue that, instead of solving problems for arbitr can think in terms of solving problems for an arbitrary byte, query, or dollar, thereby putting more focus on paths that carry a higher volume of traffic. Most traffic concentrates along a small number of routes due to a number of trends: the rise of Internet video had led to Netflix and YouTube alone accounting for nearly half of North American traffic [2], more services are moving to shared cloud infrastructure, and a small number of mobile and broadband providers deliver Internet connectivity to end-users. This skewed distribution means that an approach to improving routing can have substantial impact even if it only works well over these important paths. Further, it may be possible to take advantage of properties

MANY CLIENTS ARE ONE AS-HOP AWAY FROM IMPORTANT CONTENT

RIPE Labs

AS 666

Deployment



1.2/16 -> AS 1

AS 1 -> AS 2

Verify signature

RPKI cache

repository

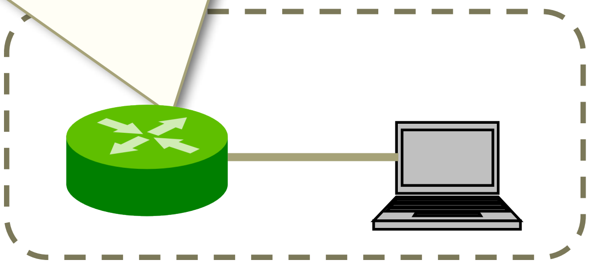
1.2/16: AS 1

AS 1 → AS 2

BGP Routers

Deployment: today!

```
ip as-path access-list as1 deny _[^2]_1_
```

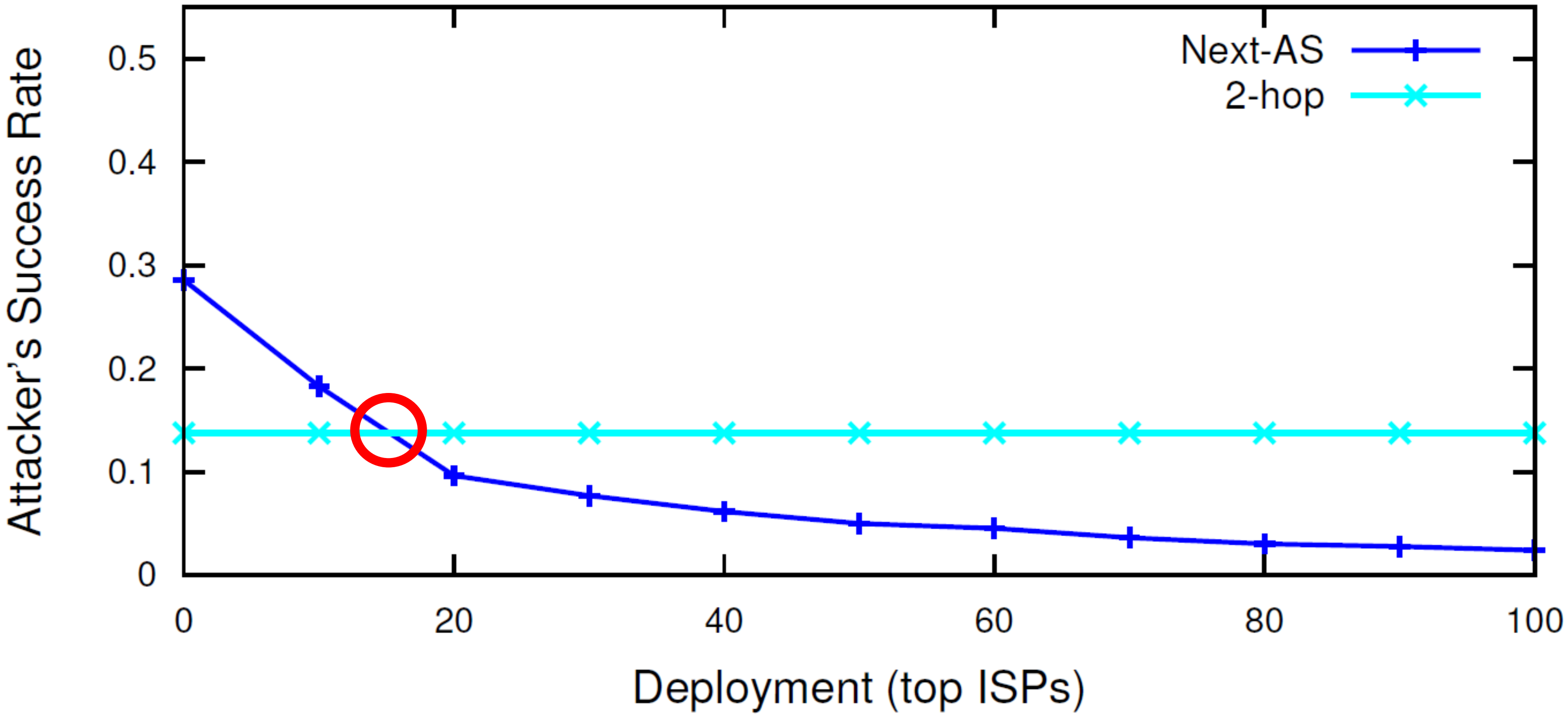


- Use existing Access List interface
- Validated suffix extends automatically with adoption

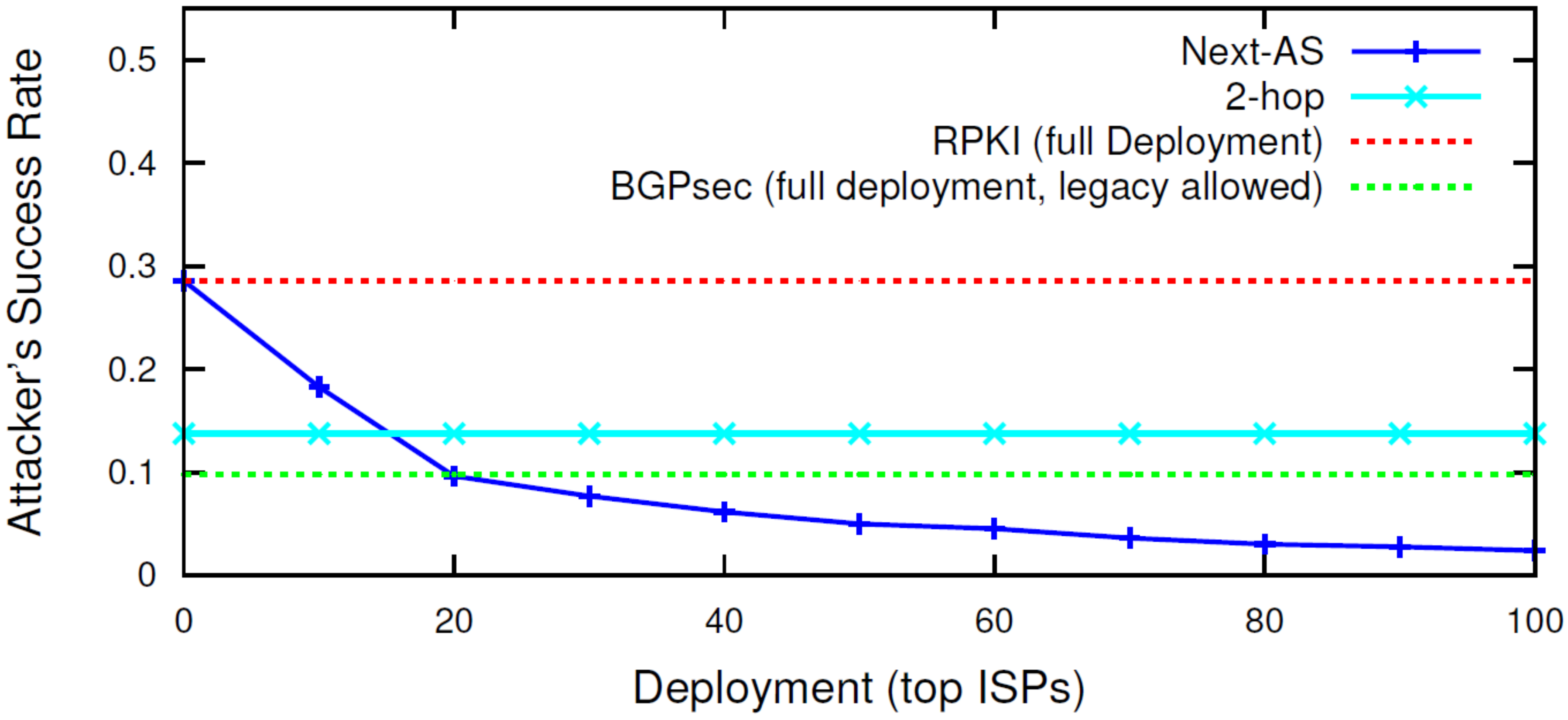
Evaluating impact

- **How significant is path-end validation?**
- Empirically-derived AS-level network from CAIDA
  - Including inferred peering links
    [Giotsas et al., SIGCOMM’13]
- Evaluate fraction of ASes an attacker can attract
  - For different adoption scenarios
  - For different types of attack
- Using the simulation framework in [Gill et al., CCR’12]

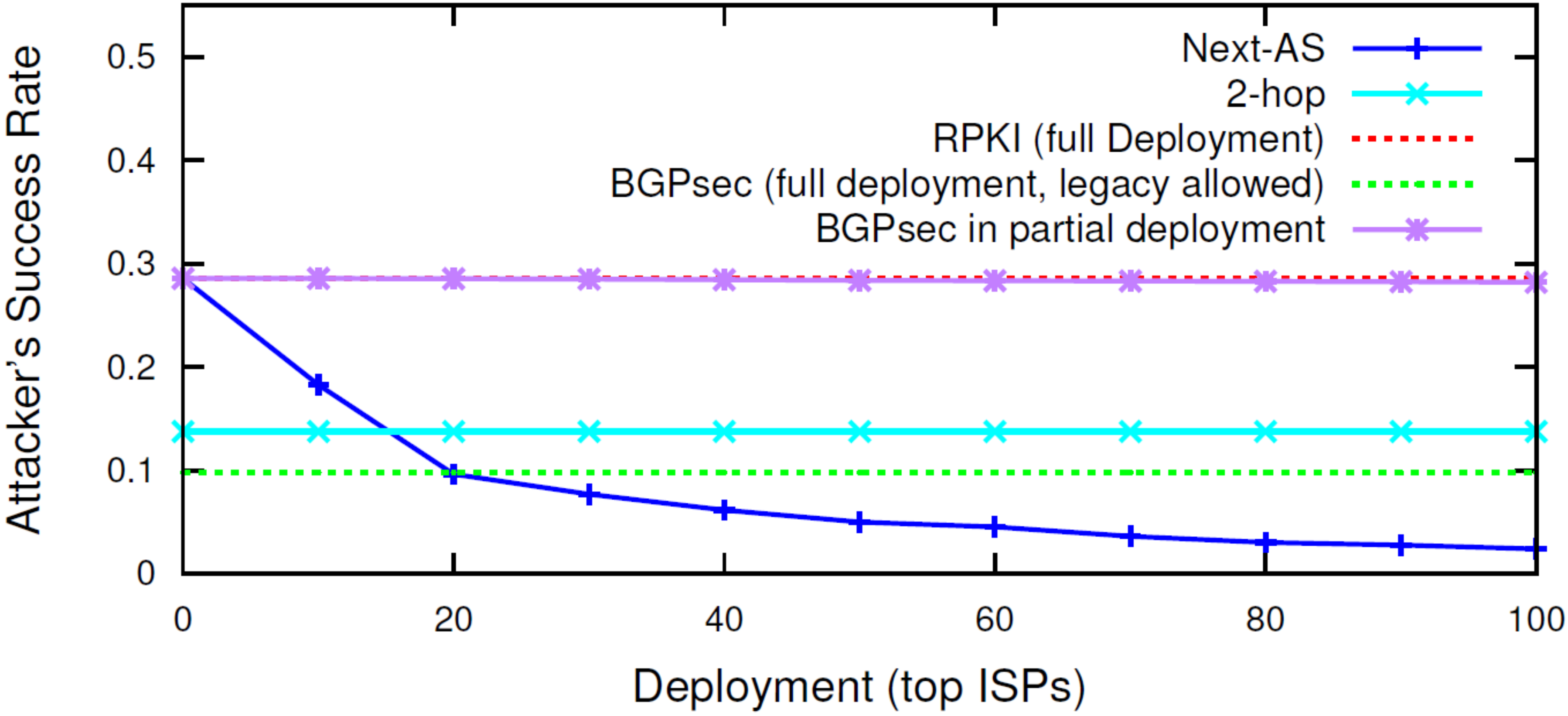
Simulation results



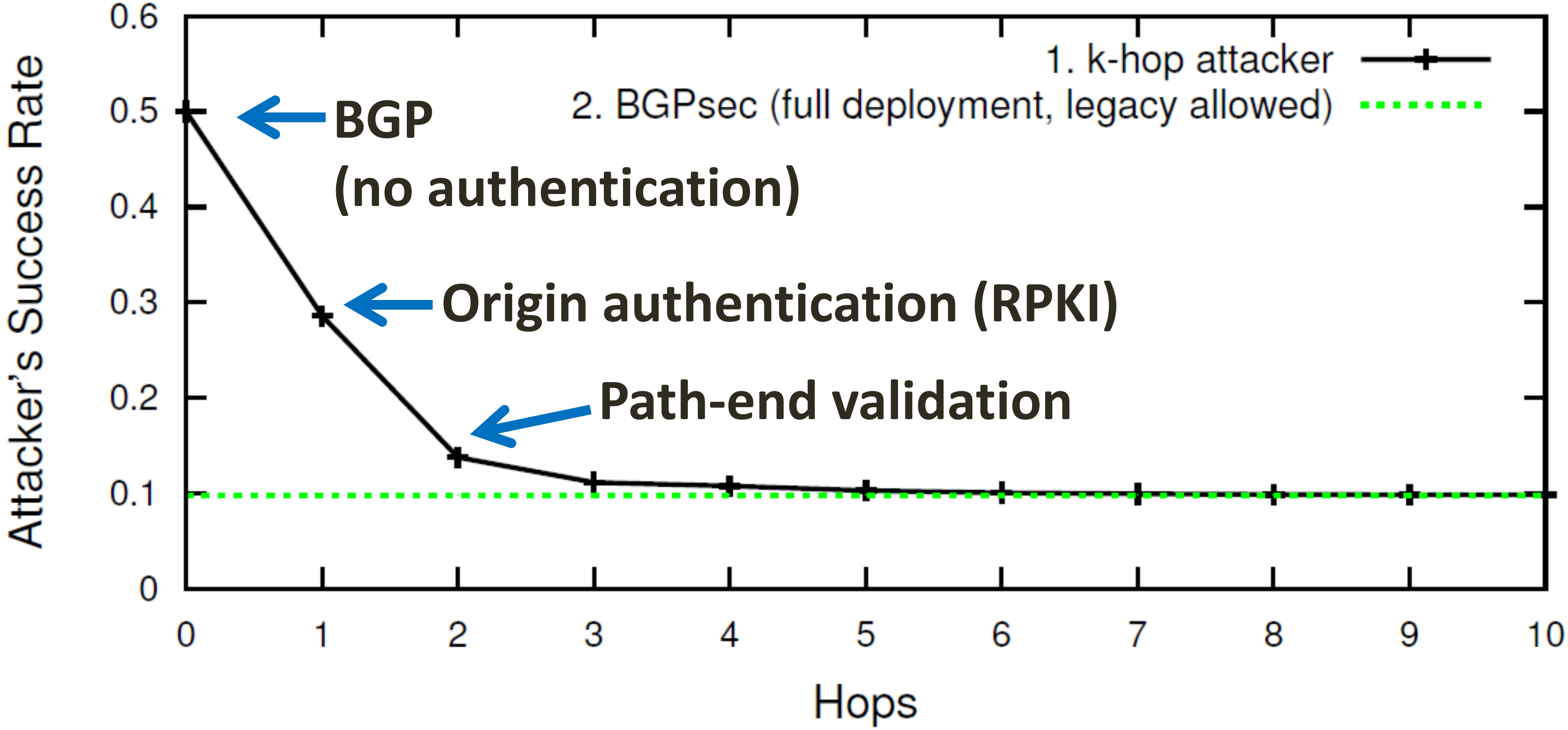
Simulation results



Simulation results



Impact of authenticating hops

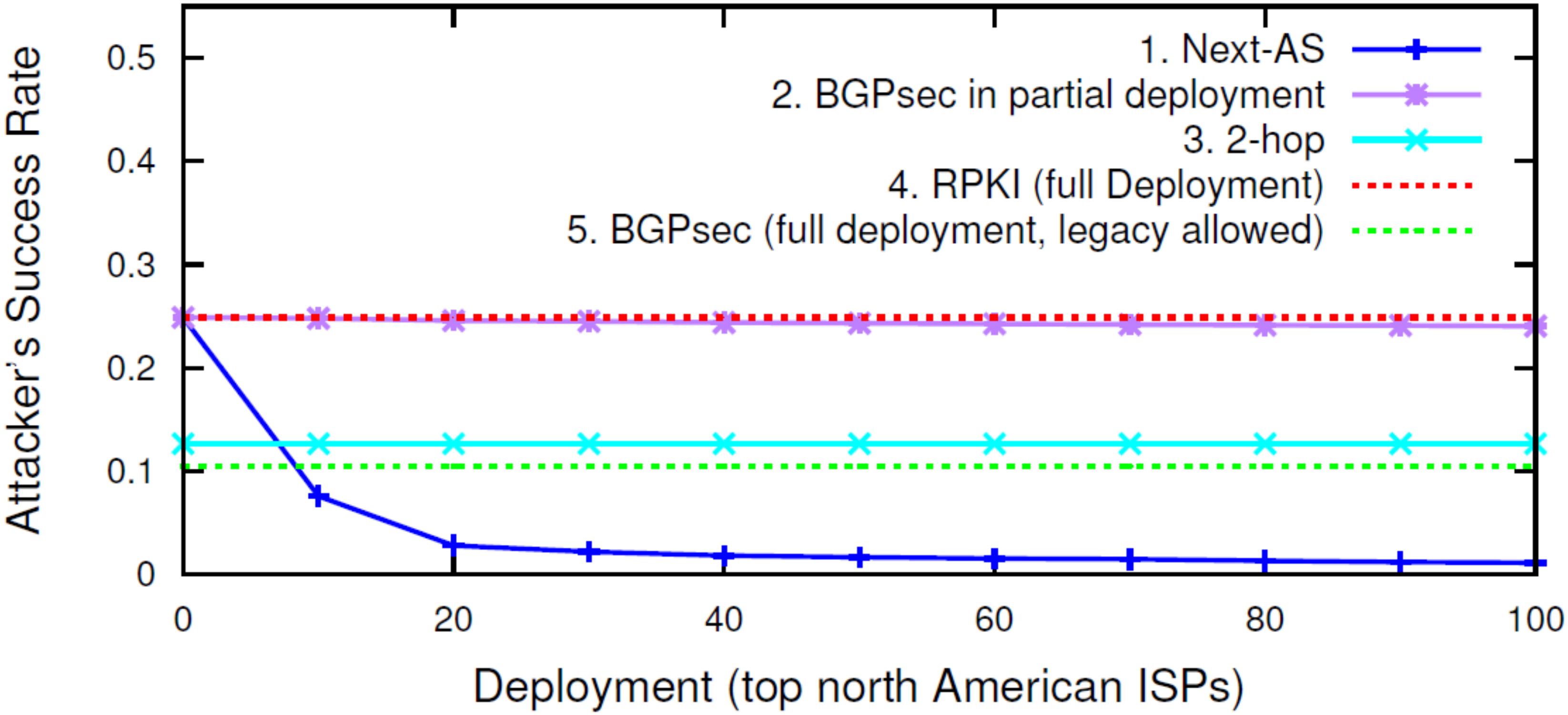


BGP
(no authentication)

Origin authentication (RPKI)

Path-end validation

Local deployment



Additional results

- *Local* deployment protects *local* traffic
- Large content providers are better protected
- Path-end validation mitigates high profile incidents
- Security monotone

Conclusion

- Path-end validation
  - Is a modest extension to RPKI
  - Can significantly impact BGP security while avoiding BGPsec's deployment hurdles
- We advocate
  - Incorporating path-end validation into the RPKI
  - Regulatory/financial efforts on gathering critical mass of adopters

Thank You