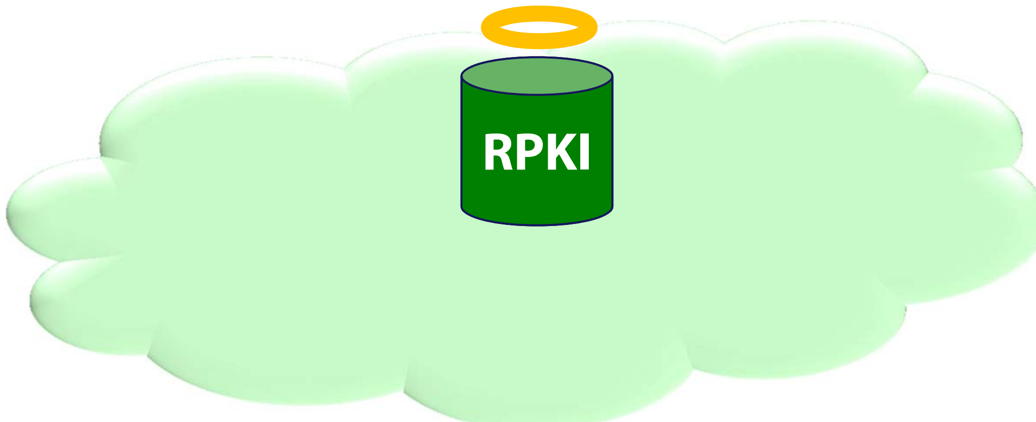
The Transition to BGP Security

Is the Juice Worth the Squeeze?



Sharon Goldberg

Boston University

November 2013

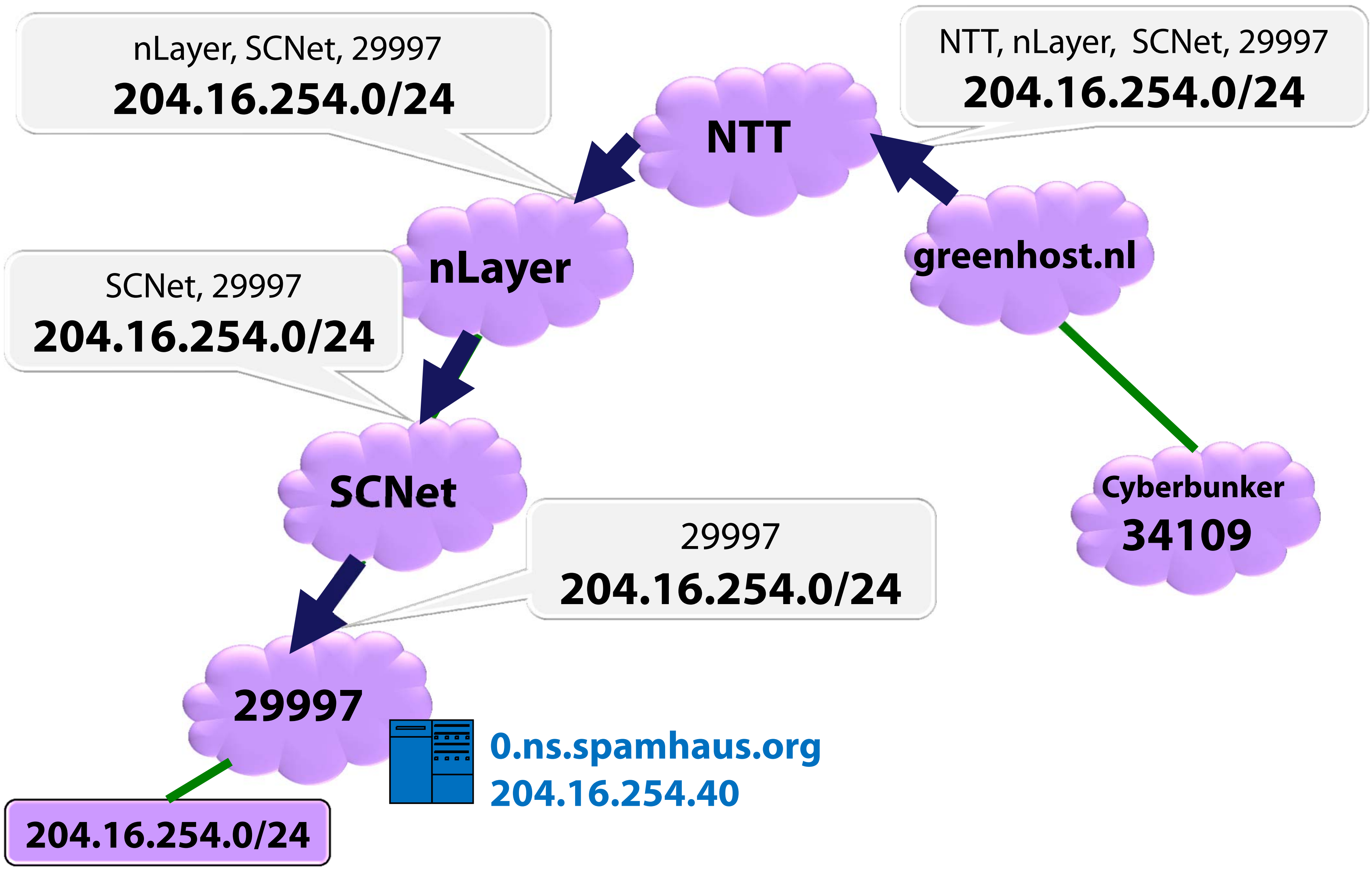
BOSTON UNIVERSITY

Work with Kyle Brogle (Stanford), Danny Cooper (BU), Ethan Heilman (BU), Robert Lychev (GATech/BU), Leonid Reyzin (BU), Michael Schapira (Hebrew U)

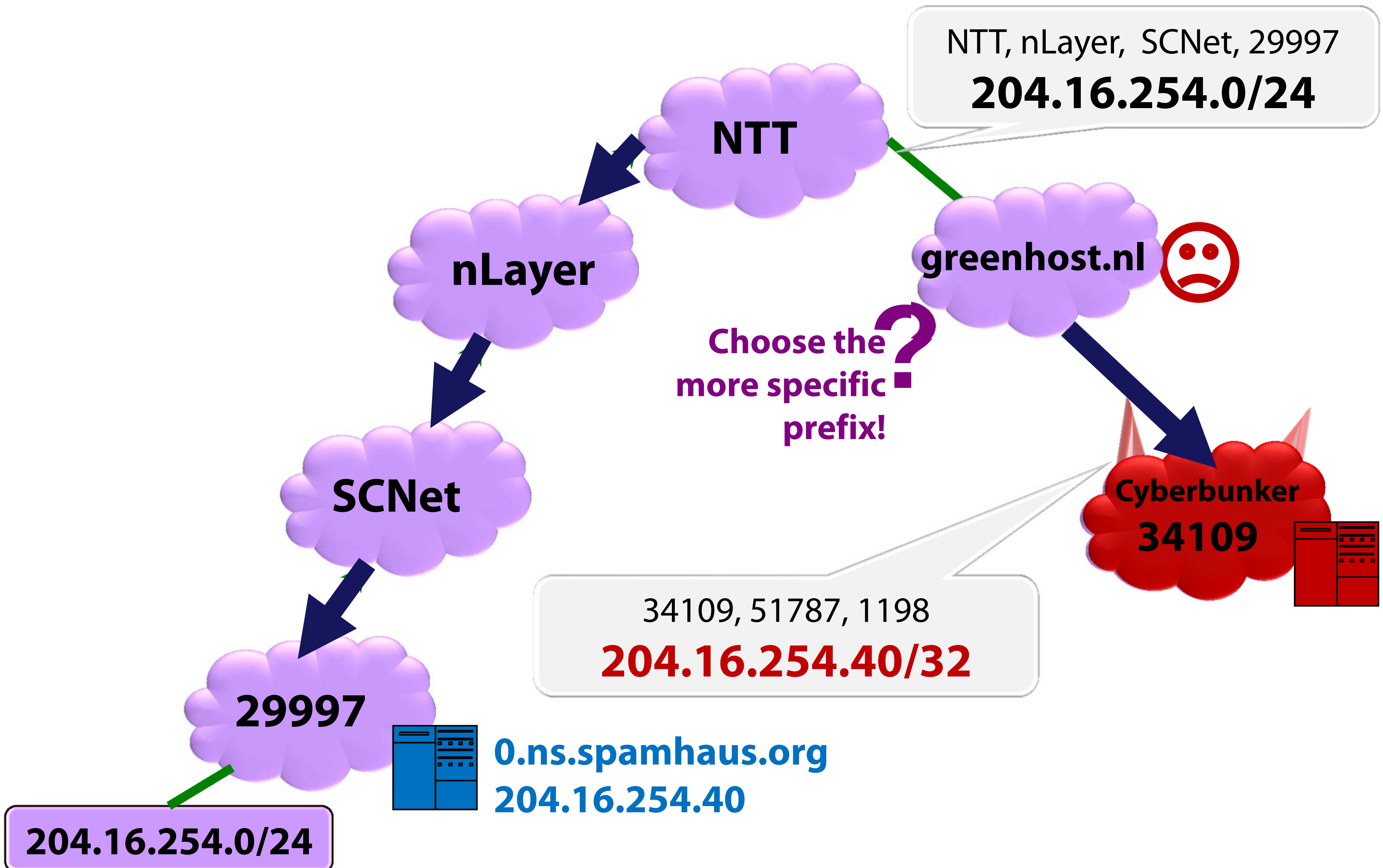
from SIGCOMM'13 and HotNets'13

interdomain routing

BGP is used to learn routes between Autonomous Systems (ASes)



the subprefix hijack of spamhaus from 03/2013



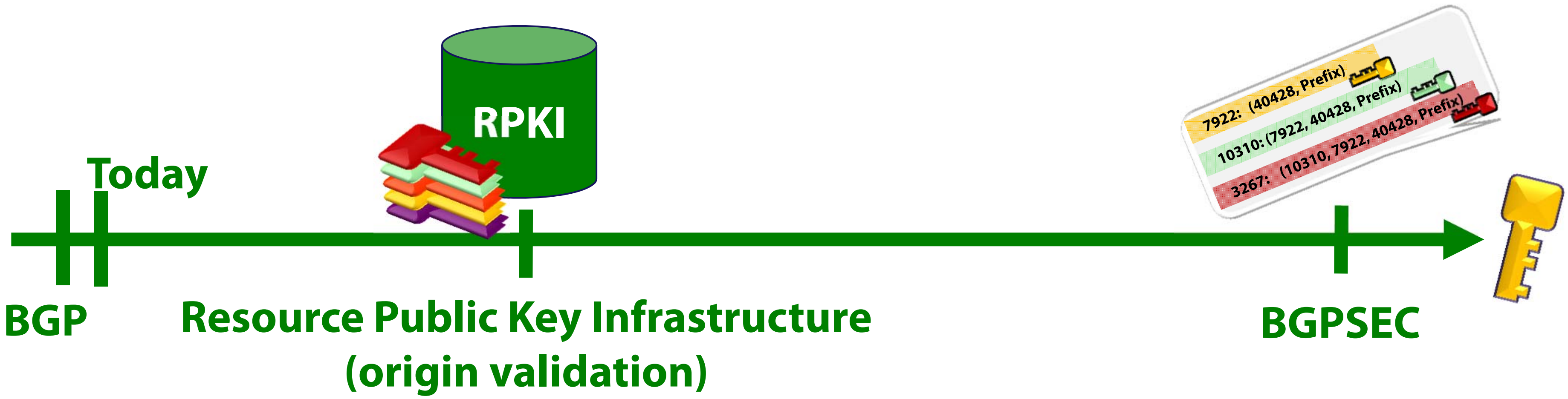
Source: https://greenhost.nl/2013/03/21/spam-not-spam-tracking-hijacked-spamhaus-ip/

the subprefix hijack of spamhaus from 03/2013

Source: https://greenhost.nl/2013/03/21/spam-not-spam-tracking-hijacked-spamhaus-ip/

& other routing incidents

crypto to the rescue!



- IETF Standard published 2012.
- Deployment started in 2011.
- Certifies IP prefix allocations.
- Crypto done out-of-band
- No change to BGP messages

- Builds on the RPKI
- Now being standardized
- Certifies announced routes
- Crypto done online
- Major change to BGP msgs

Main challenge?

Incremental deployment & backward compatibility

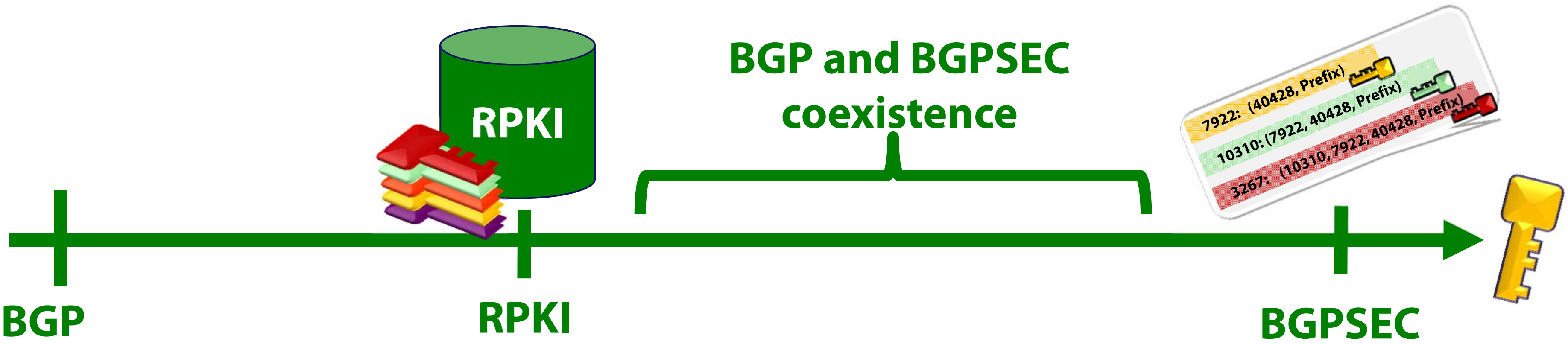
our main goal: recommendations for protocol adoption

What are the security benefits of adopting these protocols? [SIGCOMM'13] [SIGCOMM'10]

What are the incentives for adopting them? [SIGCOMM'11] [SODA'13]

How do they alter trust relationships? [HotNets'13]

talk overview



What are the security benefits of adopting these protocols?

[SIGCOMM'13]

- What does BGPSEC offer over the RPKI?
- Focus on the transition, when BGP and BGPSEC coexist.
- Experiments with deployment scenarios on empirical Internet topologies
- **Result:** We find that the RPKI is much more crucial than BGPSEC

How do they alter trust relationships?

[HotNets'13]

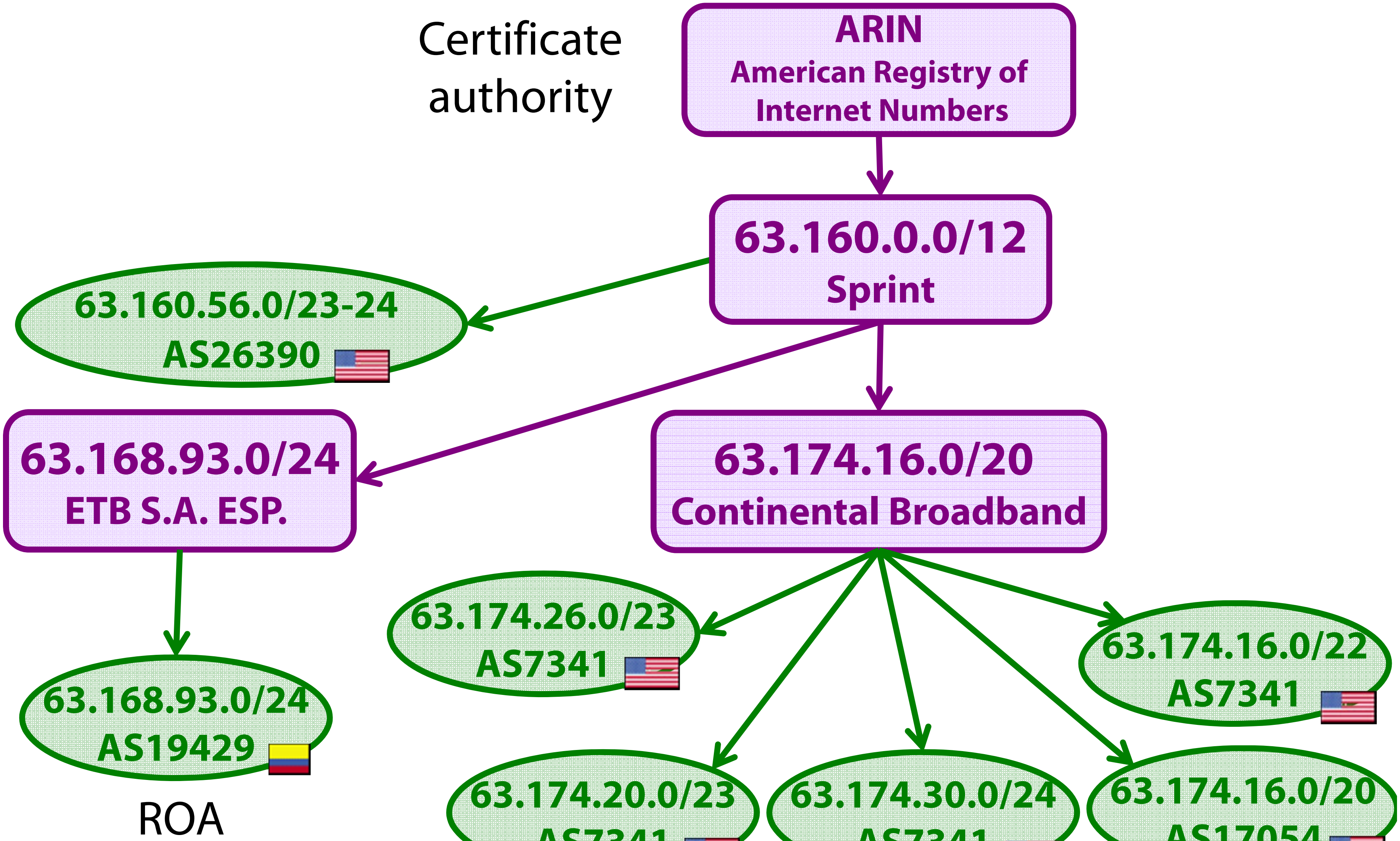
- Analyze the RPKI in a threat model where certificate authorities are compromised.

part 1: security benefits of RPKI and BGPSEC

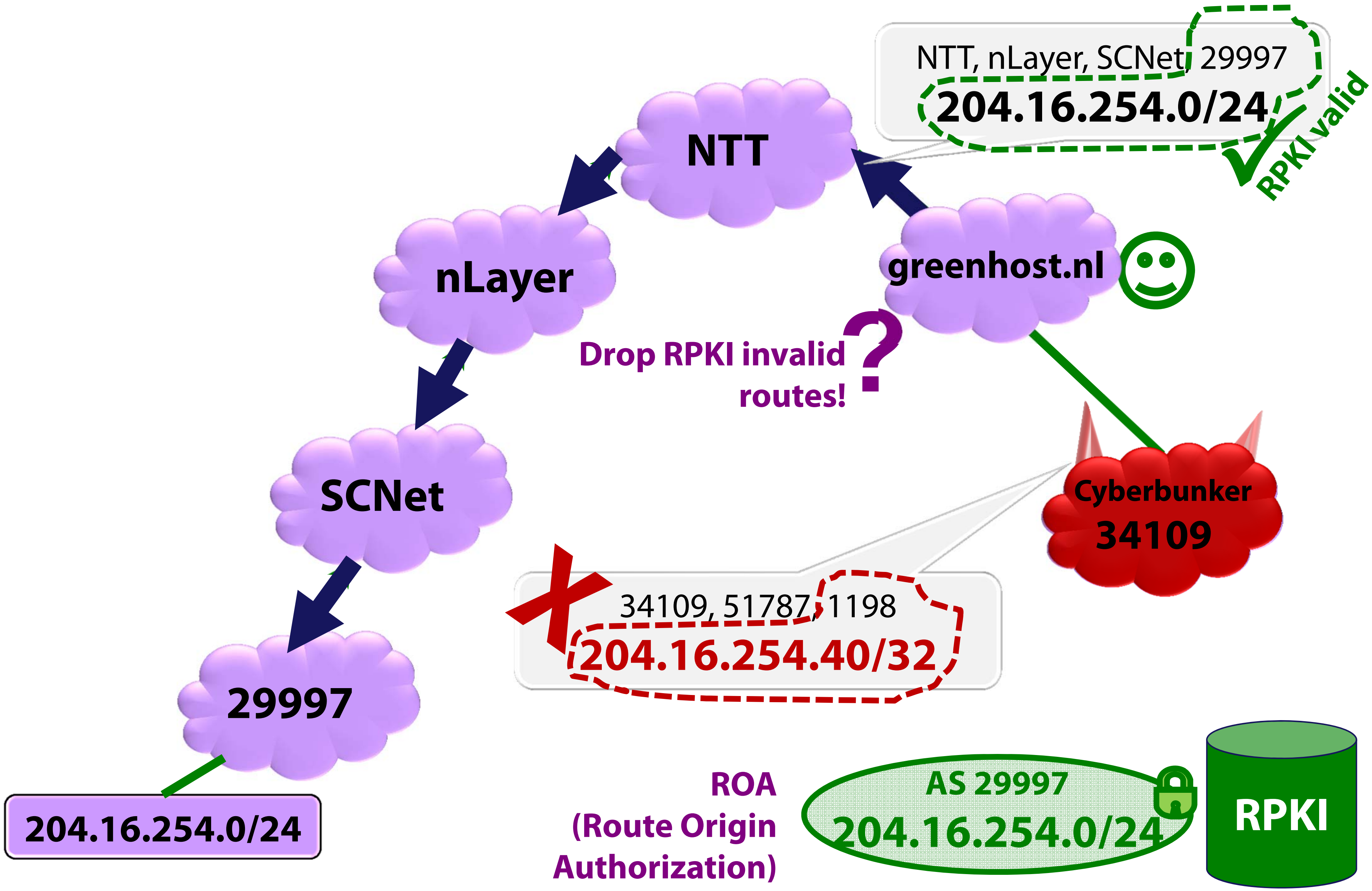
1. background: RPKI, BGPSEC
2. why BGP / BGPSEC coexistence is tricky
3. experimental evaluation of security for RPKI and BGPSEC

BOSTON UNIVERSITY

the RPKI and its cryptographic objects

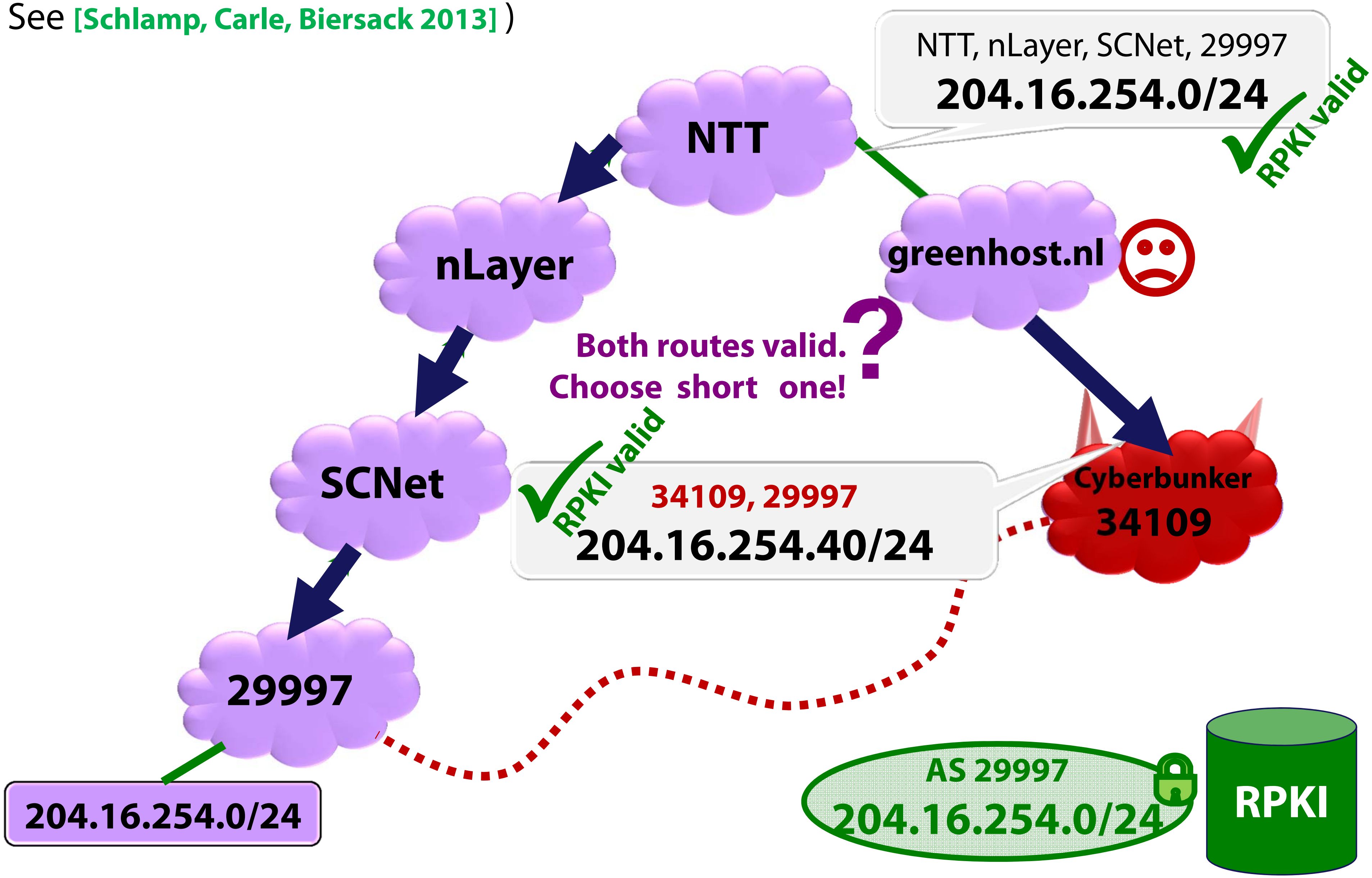


the RPKI defeats all subprefix & prefix hijacks

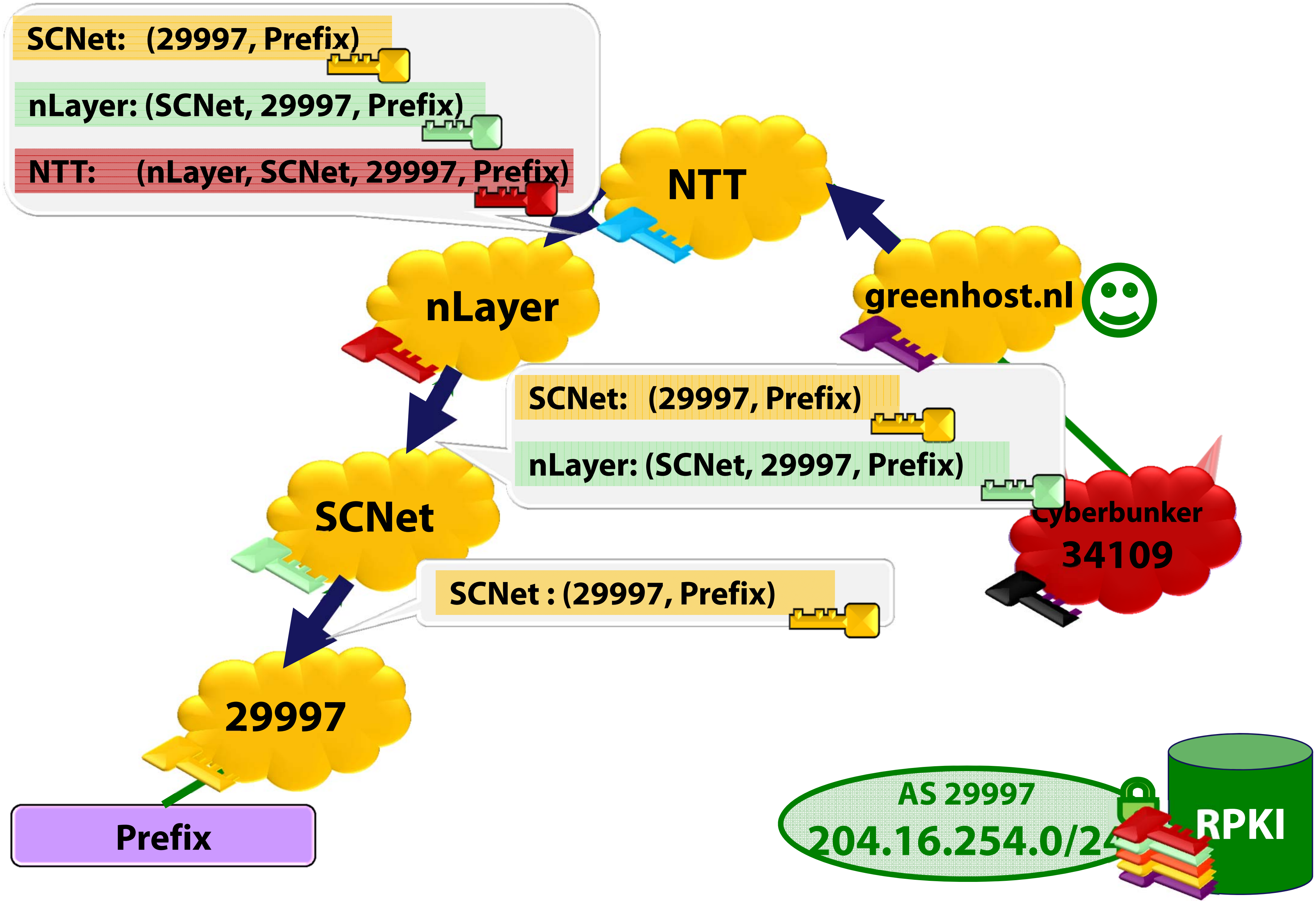


the "1-hop hijack" defeats the RPKI

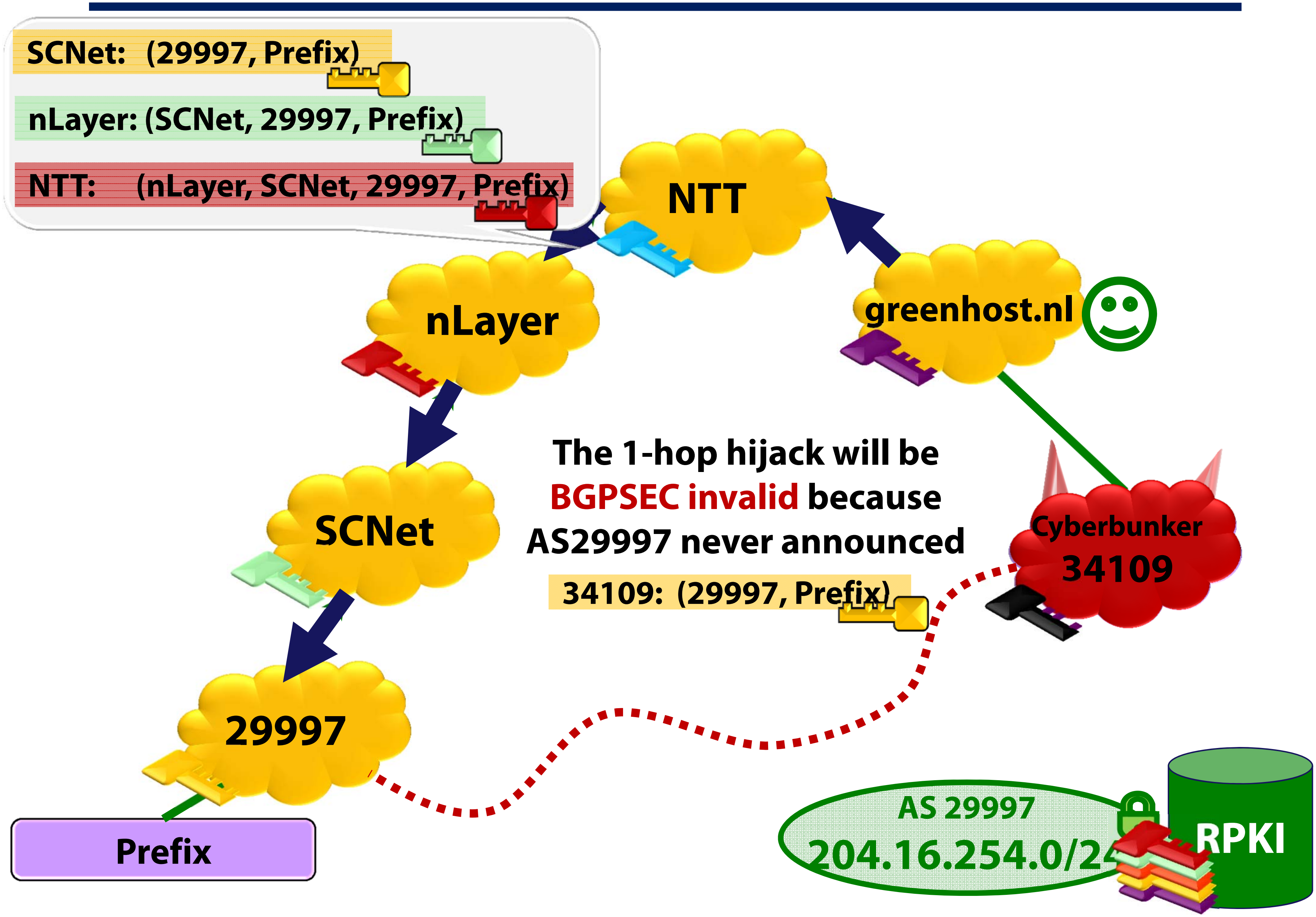
(This exact situation is hypothetical, but this type of attack has been seen in the wild, See **[Schlamp, Carle, Biersack 2013]**)



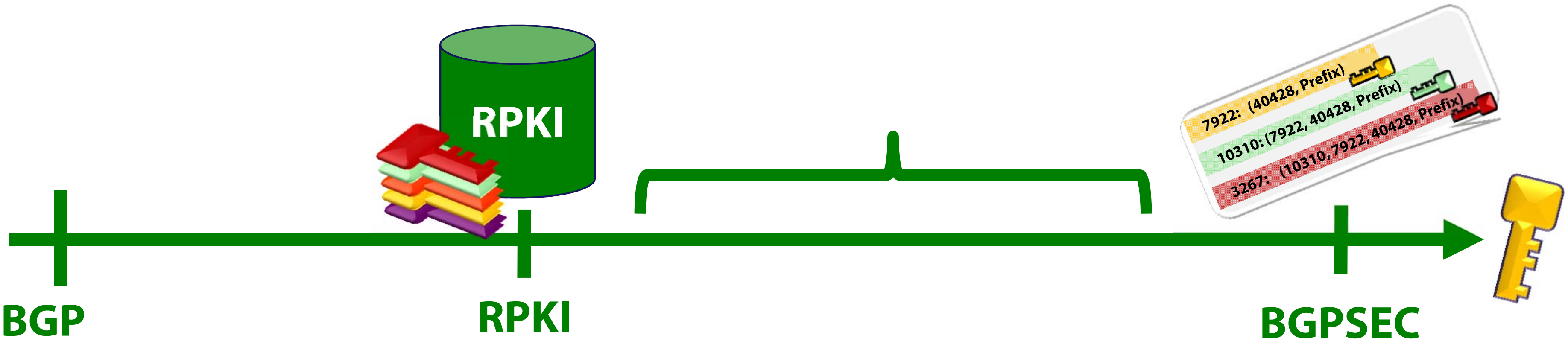
BGPSEC defeats the "1-hop hijack" (& all path-shortening attacks)



BGPSEC defeats the “1-hop hijack” (& all path-shortening attacks)



setup for our analysis in [SIGCOMM'13]



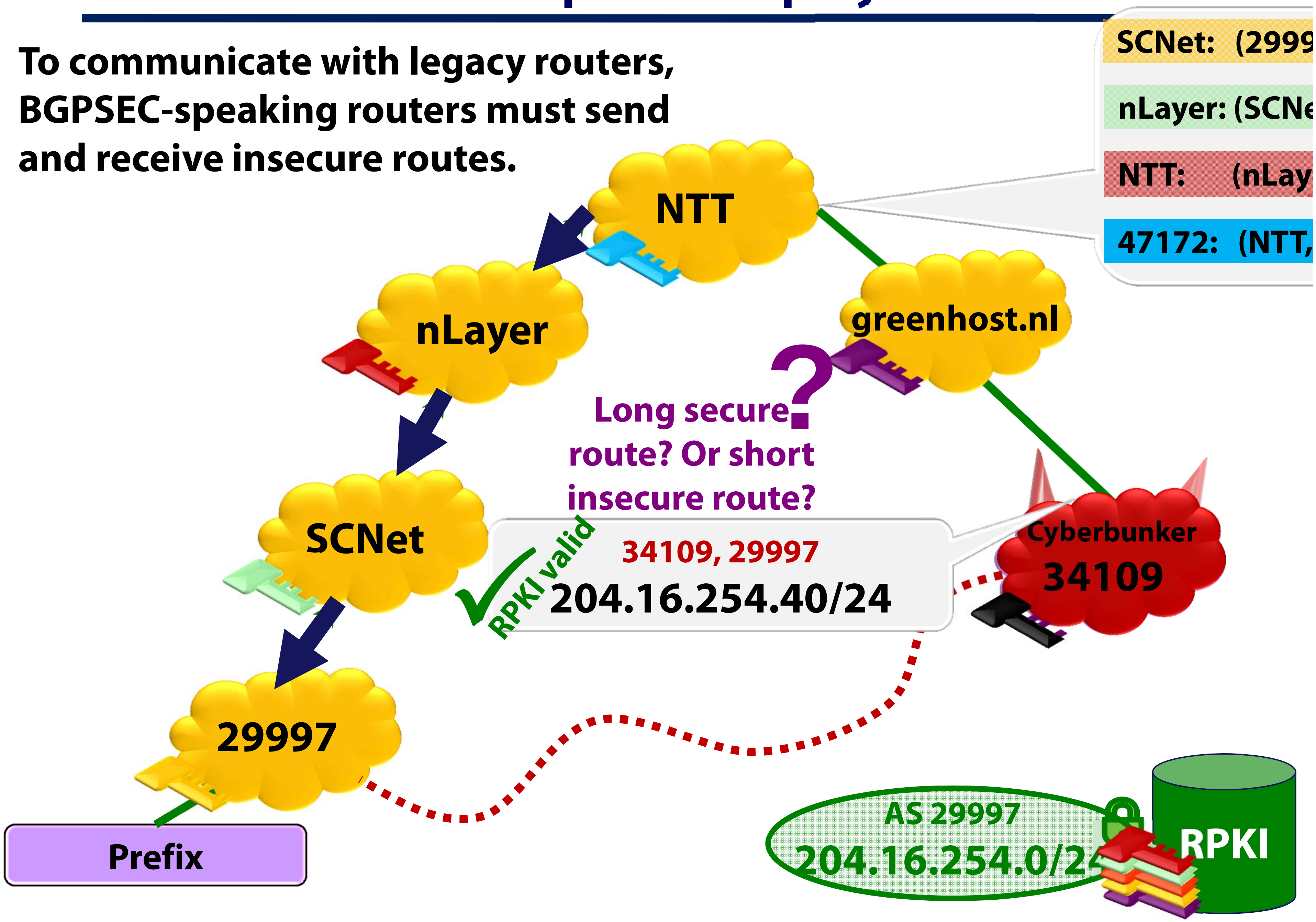
We suppose RPKI is fully deployed.

- prefix- and subprefix hijacks are eliminated.
- our threat model is therefore the 1-hop hijack

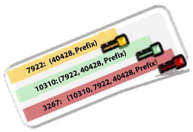
What happens when BGP and BGPSEC coexist?

BGPSEC in partial deployment

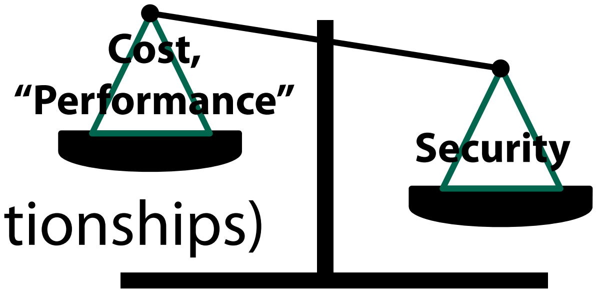
To communicate with legacy routers, BGPSEC-speaking routers must send and receive insecure routes.



how to prioritize security in partial deployment?

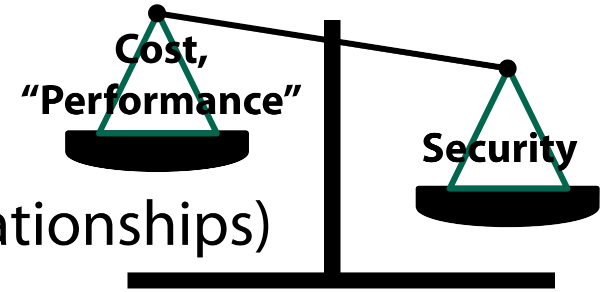


BGPSEC Security 1st

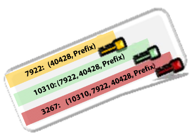


1. local preference (cost, business relationships)
2. prefer short routes ("performance")
3. tiebreak on interdomain criteria

how to prioritize security in partial deployment?



1. local preference (cost, business relationships)

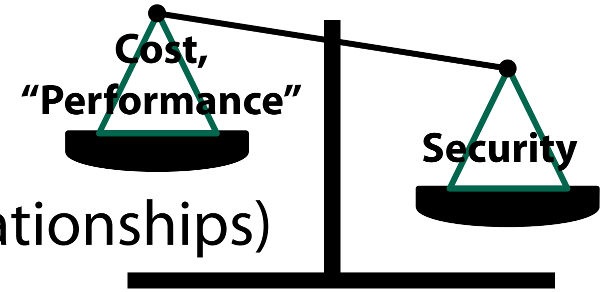


BGPSEC Security 2nd

2. prefer short routes (“performance”)

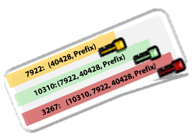
3. tiebreak on interdomain criteria

how to prioritize security in partial deployment?



1. local preference (cost, business relationships)

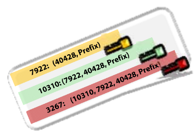
2. prefer short routes (“performance”)



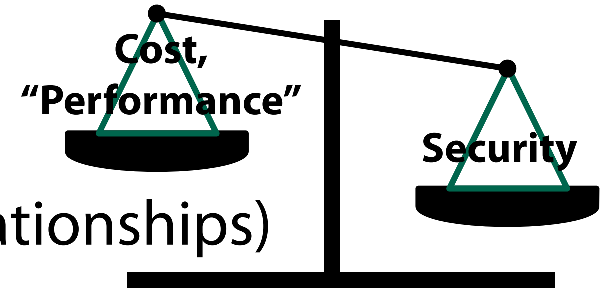
BGPSEC Security 3rd

3. tiebreak on interdomain criteria

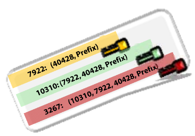
how to prioritize security in partial deployment?



BGPSEC Security 1st

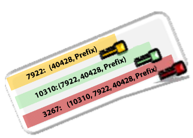


1. local preference (cost, business relationships)



BGPSEC Security 2nd

2. prefer short routes ("performance")



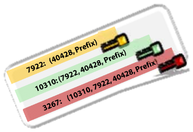
BGPSEC Security 3rd

3. tiebreak on interdomain criteria

✧ Survey of 100 network operators shows that 10%, 20% and 41% would place security 1st, 2nd, and 3rd. **[NANOG'12]**

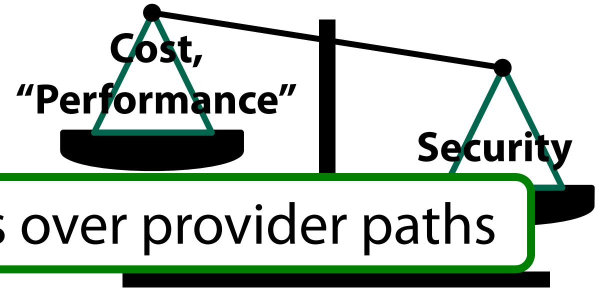
Main question: If everyone uses the **same security model**, what are the "security benefits" of deploying BGPSEC at a set of **S** ASes?

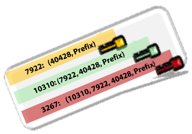
how to prioritize security in partial deployment?



BGPSEC Security 1st

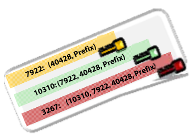
1. Prefer customer paths over peer paths over provider paths





BGPSEC Security 2nd

2. prefer short routes (“performance”)



BGPSEC Security 3rd

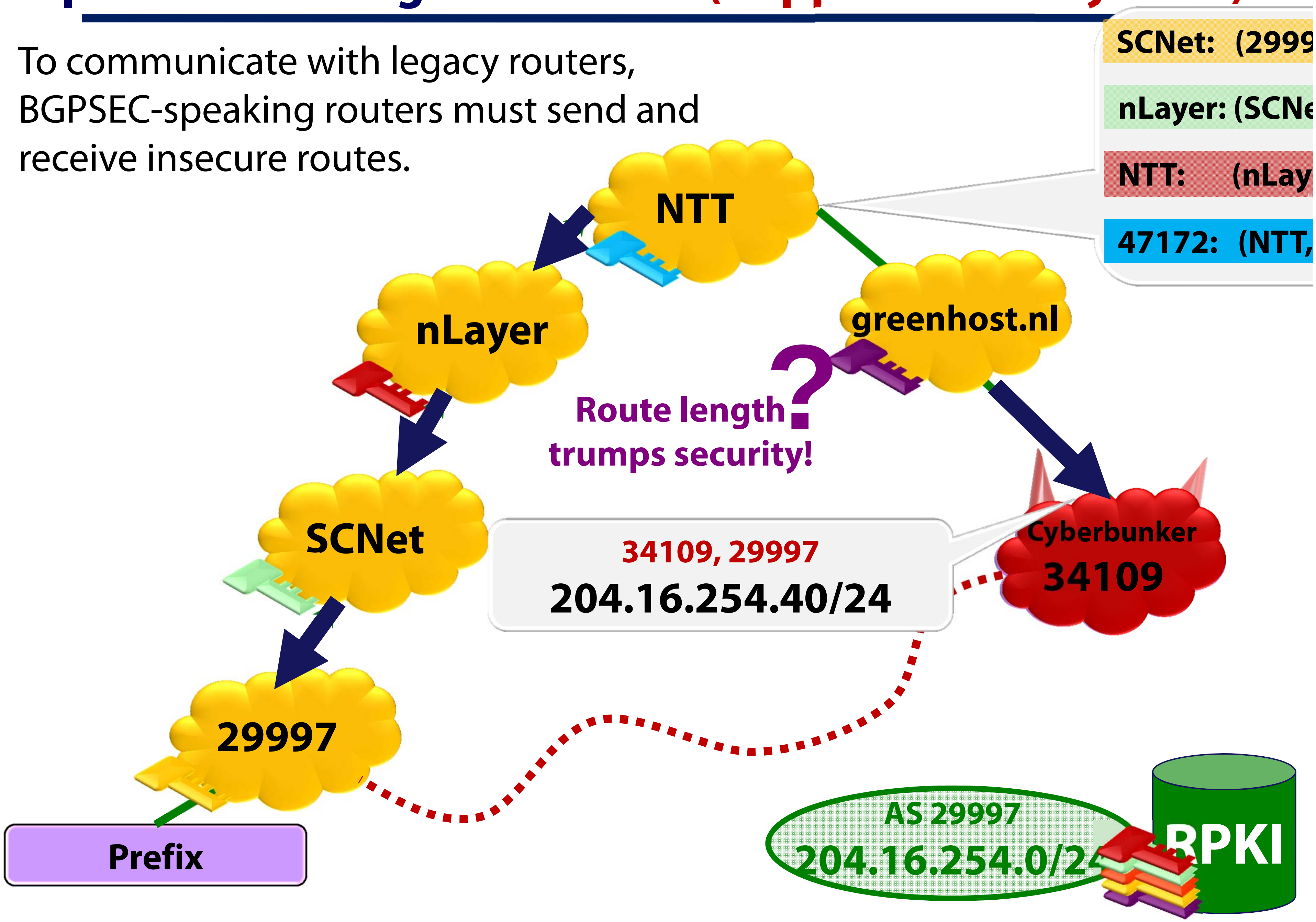
3. tiebreak on interdomain criteria

✧ Survey of 100 network operators shows that 10%, 20% and 41% would place security 1st, 2nd, and 3rd. **[NANOG’12]**

Main question: If everyone uses the **same security model**, what are the “security benefits” of deploying BGPSEC at a set of **S** ASes?

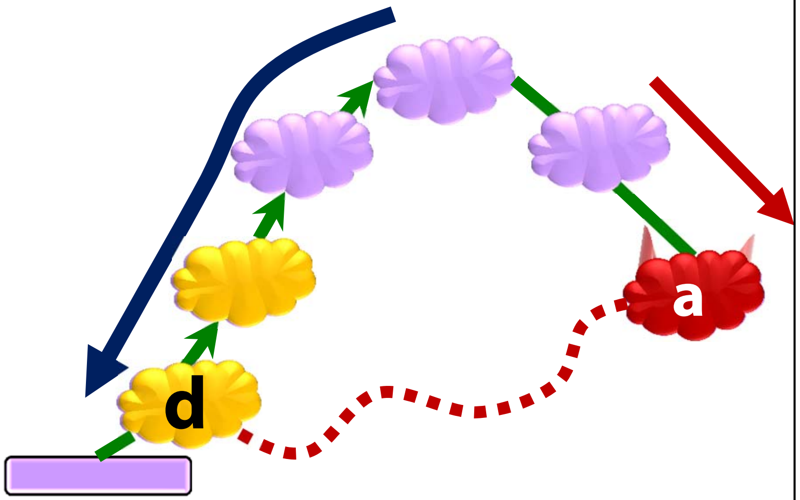
protocol downgrade attack. (Suppose security is 3rd)

To communicate with legacy routers, BGPSEC-speaking routers must send and receive insecure routes.



quantifying security

Let **S** be the set of ASes deploying BGPSEC



The number of ASes choosing a legitimate route is

Happy[S, a, d] = 3

Our security metric averages this over all a and d.

But, it's hard to find the "right" S :

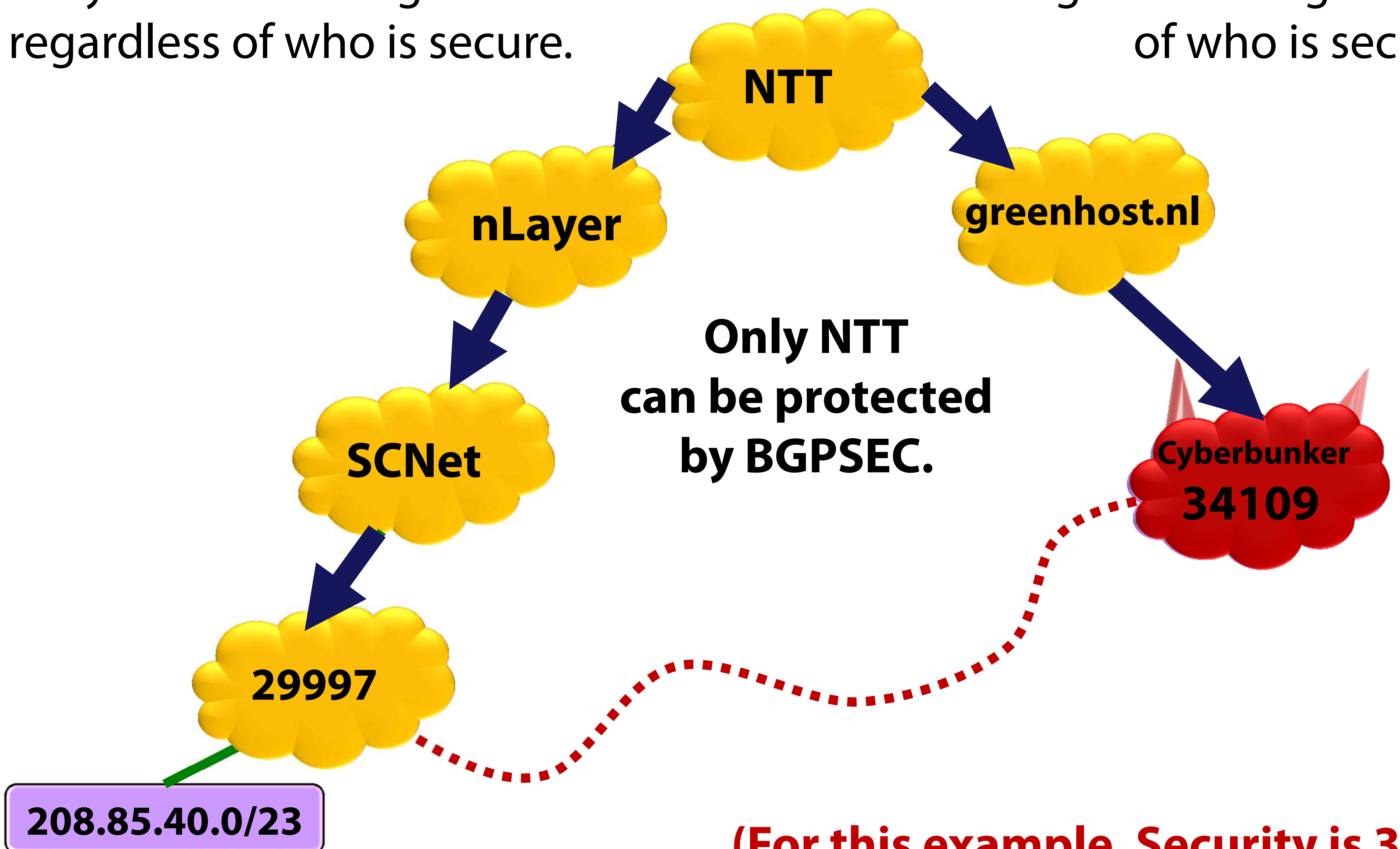
- Future deployment patterns are hard to predict
- Finding **S** (of size **k**) maximizing security metric is NP-hard

Instead, we quantify security *irrespective of the scenario* S*!*

quantify security using only topology & routing model!

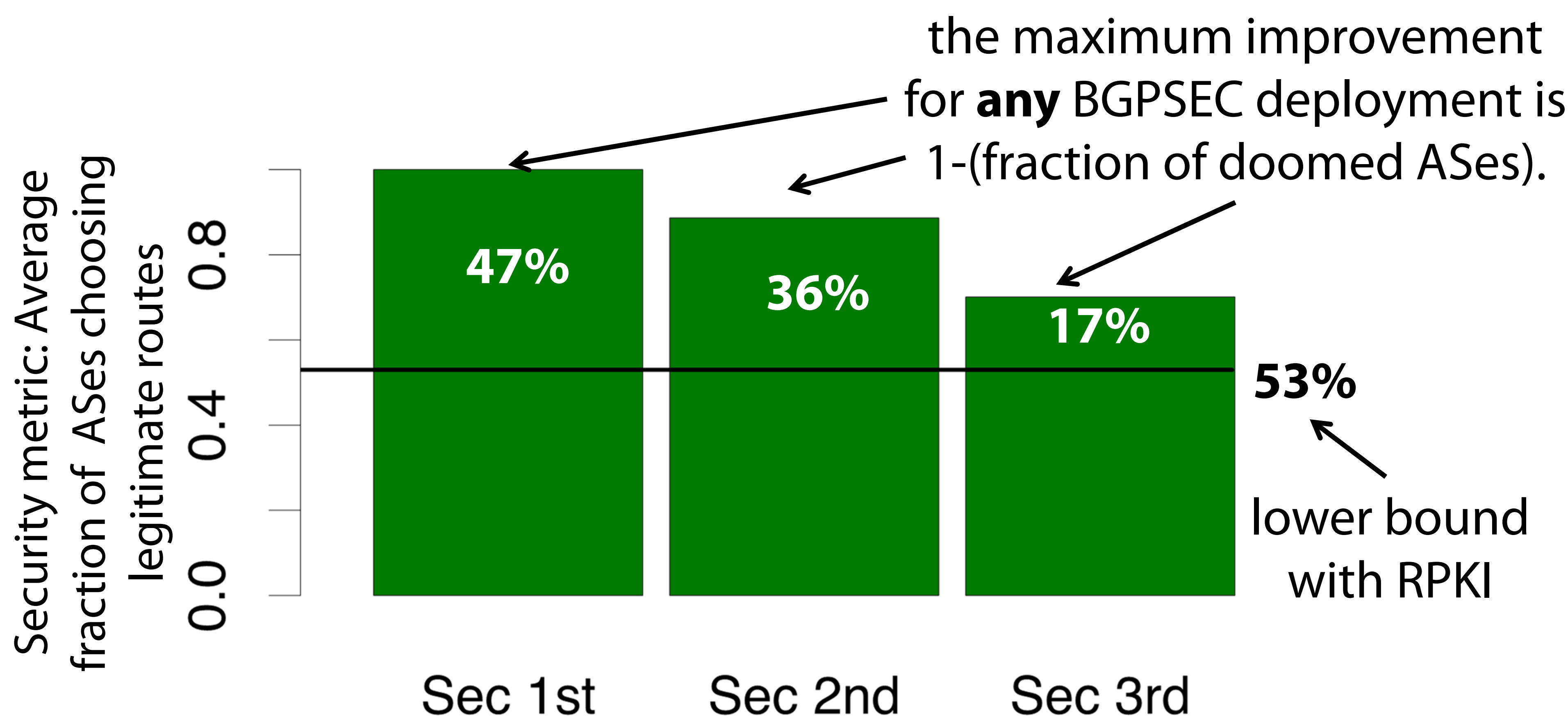
SCNet and nLayer are immune! They choose the legitimate route regardless of who is secure.

greenhost is doomed! It chooses the bogus route regardless of who is secure.

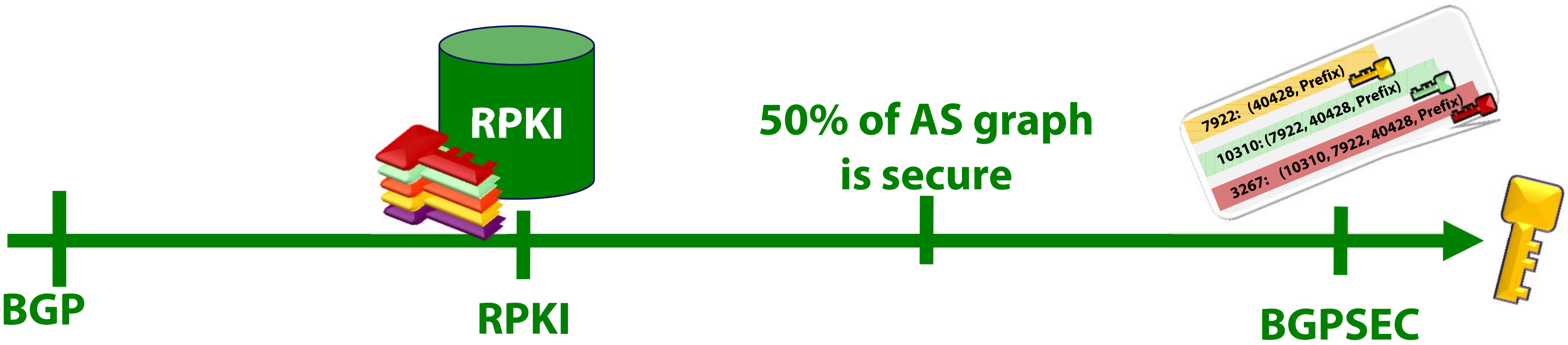


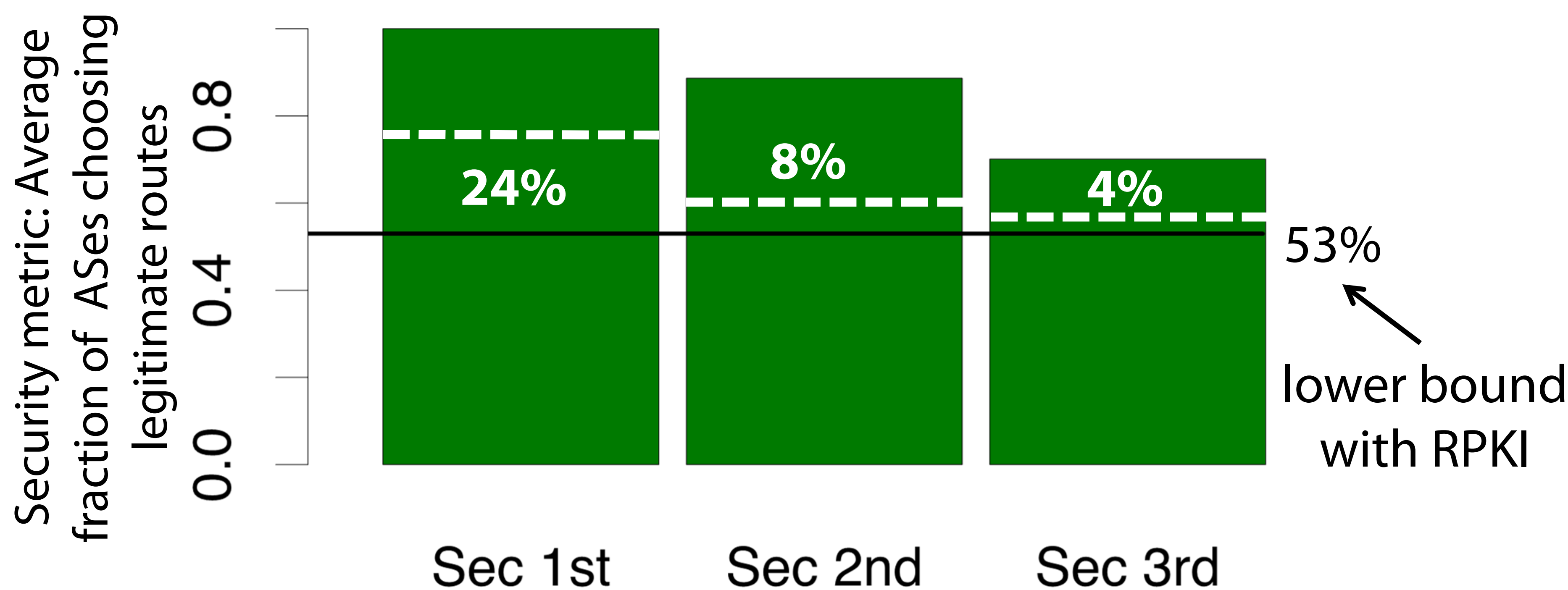
(For this example, Security is 3rd)

bounding security provided by **any** BGPSEC deployment



securing 113 high degree ASes & their stubs





methodology (& more results in [SIGCOMM'13])

- **Graph:** A UCLA AS-level topology from 09-24-2012
  - 39K ASes, 73.5K and 62K customer-provider and peer links
- **LocalPref model**: The Gao-Rexford (& Huston) model:
  - Prefer customer path over peer path over provider paths.
- **Traffic patterns:** All ASes equal; non-stub attackers.

Robustness Tests:

- **Graph:** added 550K peering links from IXP data on 09-24-2012;
- **Traffic patterns**: focused on certain destinations (e.g. content providers) and attackers
- **Local pref:** Repeating all analysis for different LocalPref models

security benefits: summary

The RPKI is the most crucial step from a security perspective

✧ Limiting the attacker to 1-hop hijacks already weakens him significantly

There is no free lunch with BGPSEC

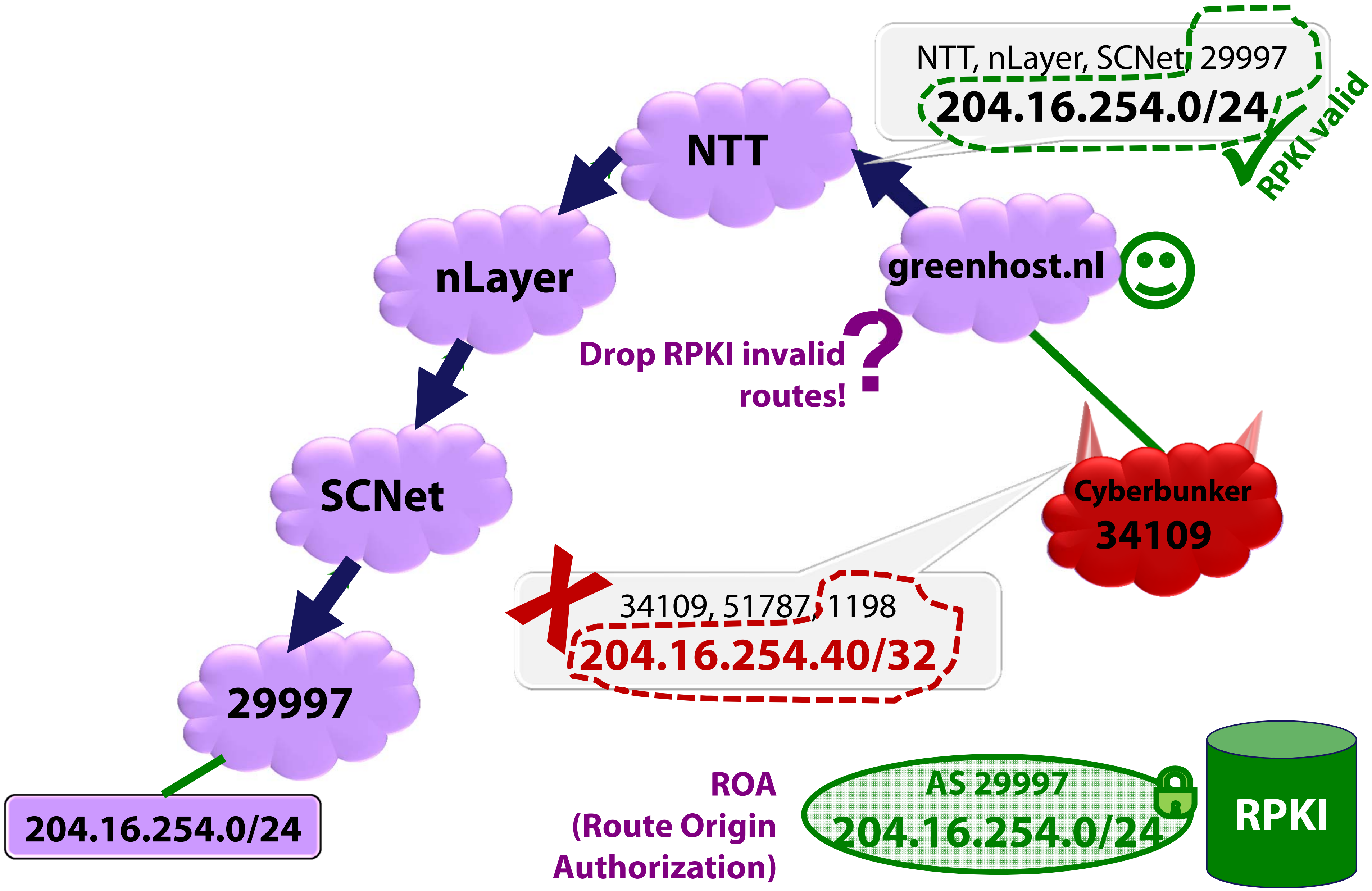
✧ If security is not 1st, protocol downgrade attacks are a serious problem

Part 2: How does the RPKI alter trust relationships?

flip the threat model: what if the RPKI is compromised?

BOSTON UNIVERSITY

the RPKI defeats all subprefix & prefix hijacks

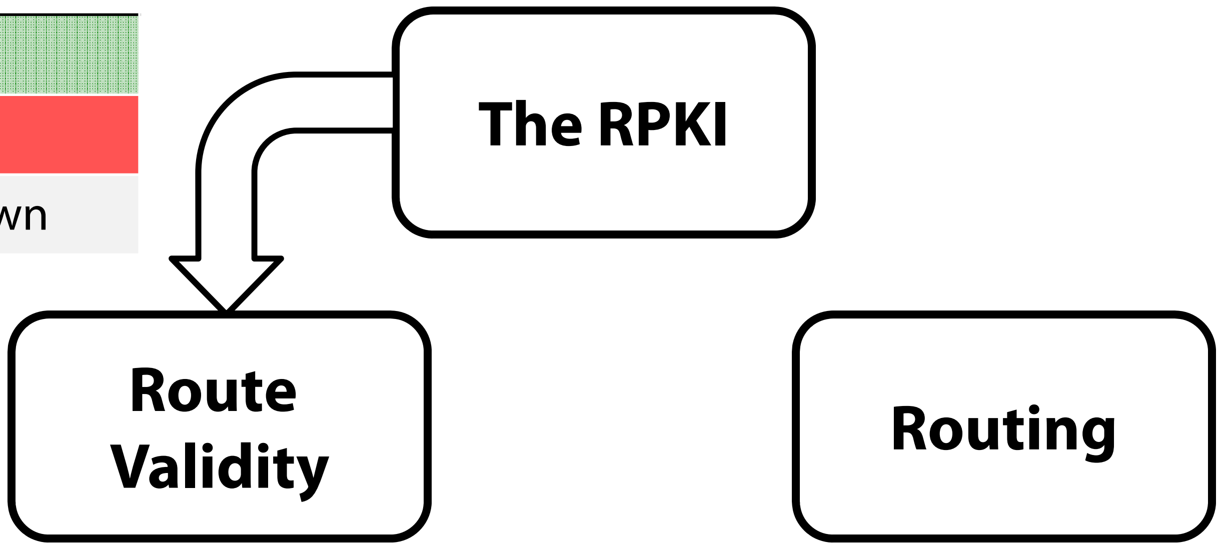


RPKI challenges (discussed in [HotNets'13])

what you'd expect:

ROA	➔	**BGP msg**
valid	➔	RPKI valid
invalid	➔	RPKI invalid
Missing	➔	RPKI unknown

creates issues for partial deployment, misconfigurations

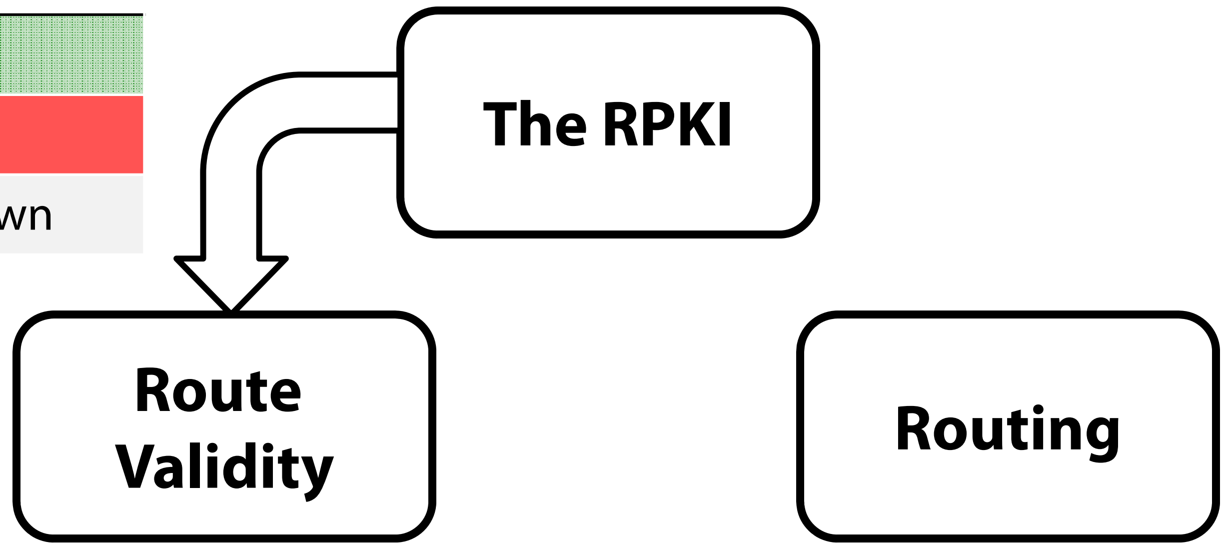


RPKI challenges (discussed in [HotNets'13])

what really happens

ROA	➔	**BGP msg**
valid	➔	RPKI valid
invalid		RPKI invalid
Missing		RPKI unknown

creates issues for partial deployment, misconfigurations

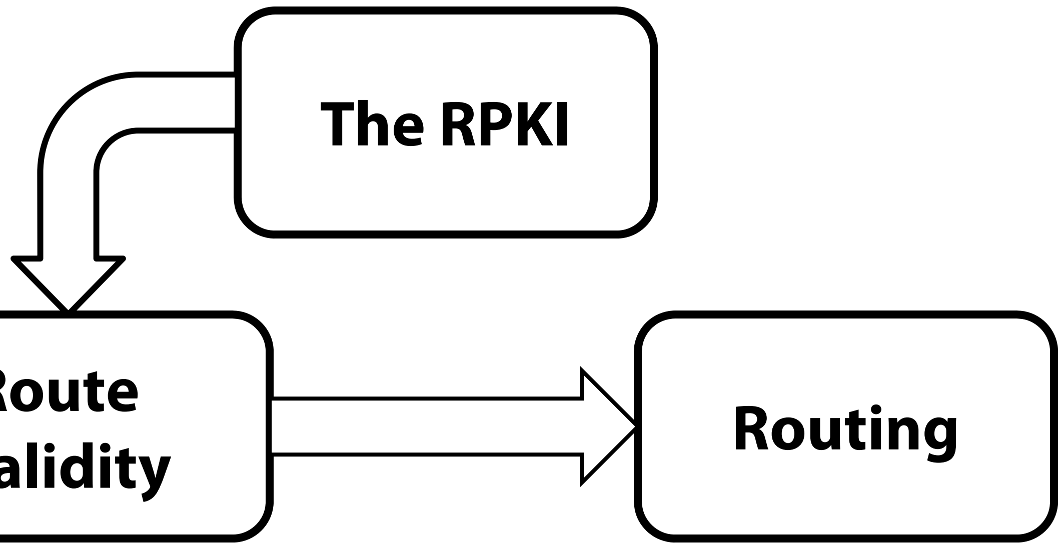


RPKI challenges (discussed in [HotNets'13])

what really happens

ROA	➔	BGP msg
valid	➔	RPKI valid
invalid		RPKI invalid
Missing		RPKI unknown

creates issues for partial deployment, misconfigurations



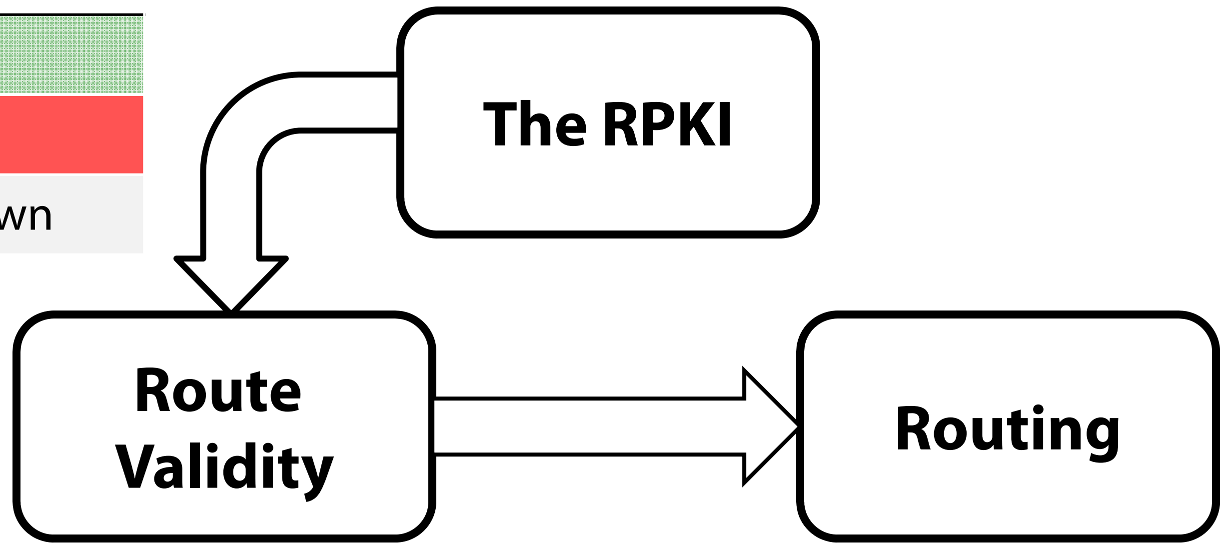
Routing policy:	Prefix remains reachable during …	
	routing hijack	RPKI problem
Drop Invalid	✓	X

RPKI challenges (discussed in [HotNets'13])

what really happens

ROA	➔	**BGP msg**
valid	➔	RPKI valid
invalid	↘	RPKI invalid
Missing	↗	RPKI unknown

creates issues for partial deployment, misconfigurations



Routing policy:	Prefix remains reachable during …	
	routing hijack	RPKI problem
Drop Invalid	✓	X
"Depref invalid"	**subprefix hijacks possible**	✓

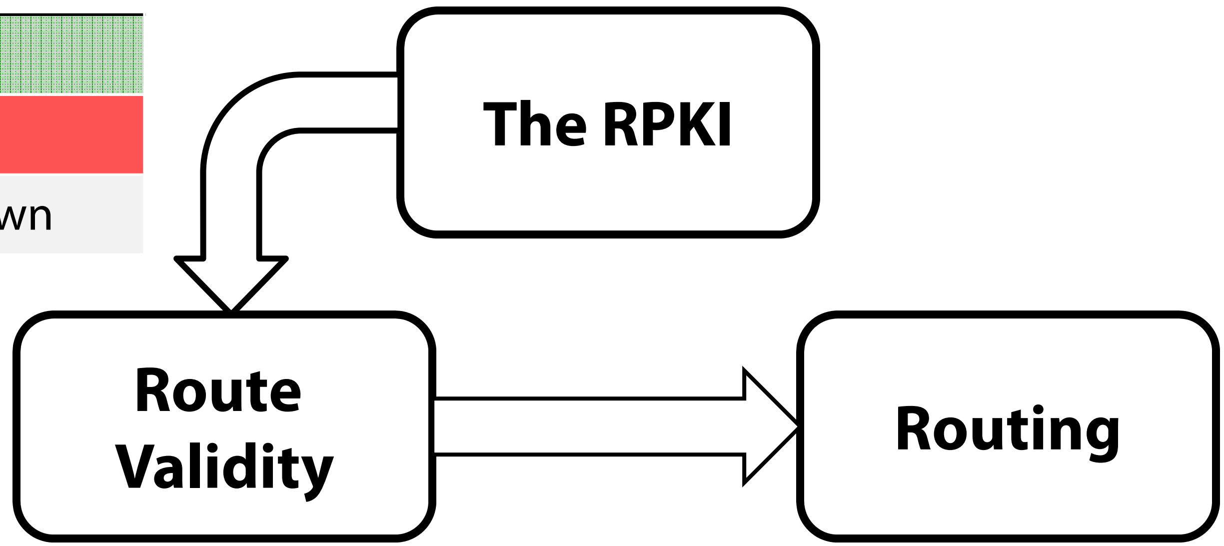
RPKI challenges (discussed in [HotNets'13])

what really happens

ROA	➔	**BGP msg**
valid	➔	RPKI valid
invalid	↘ / ↗	RPKI invalid
Missing	↘ / ↗	RPKI unknown

creates issues for partial deployment, misconfigurations

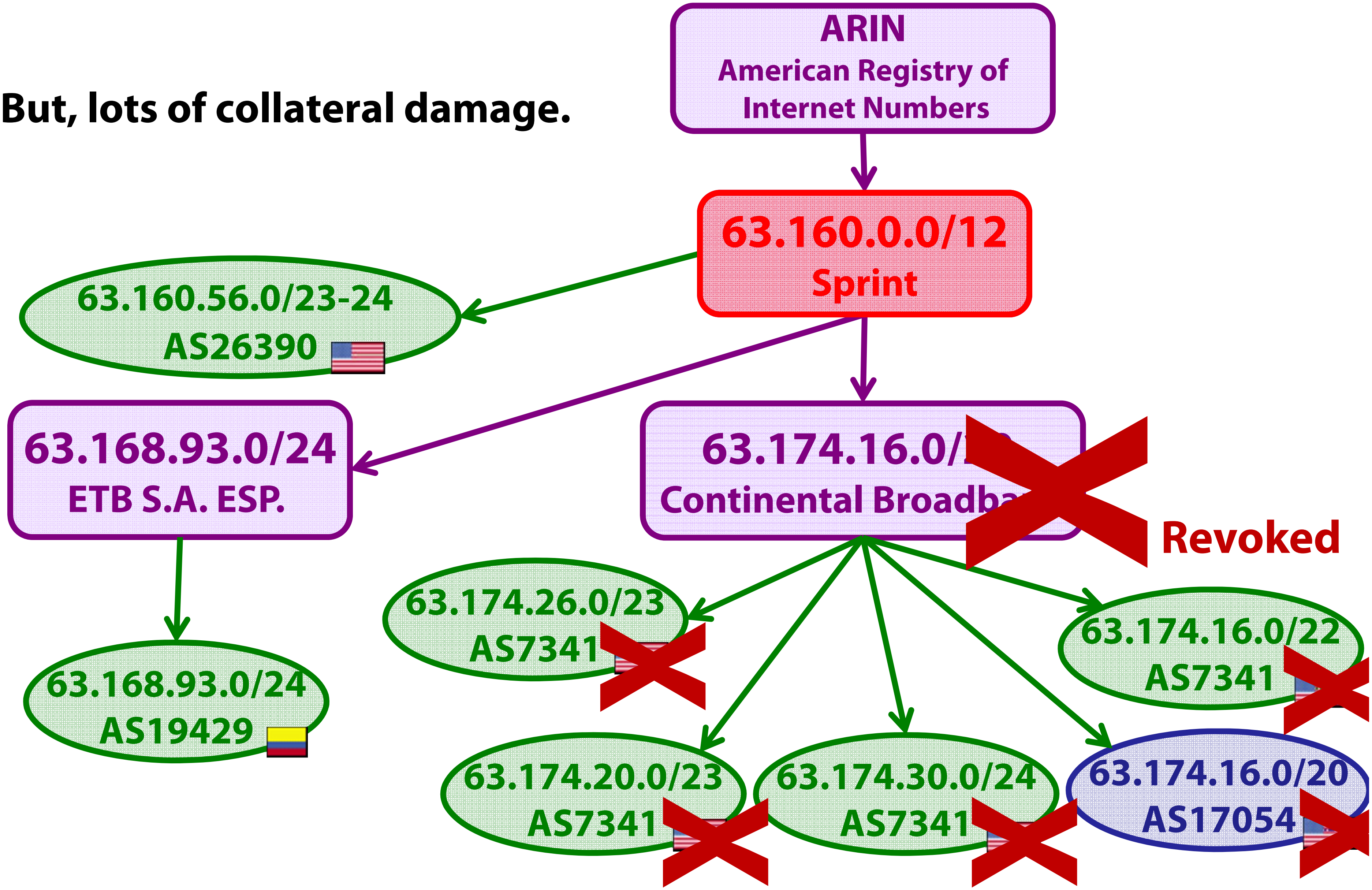
creates a new technical means to seize an IP prefix



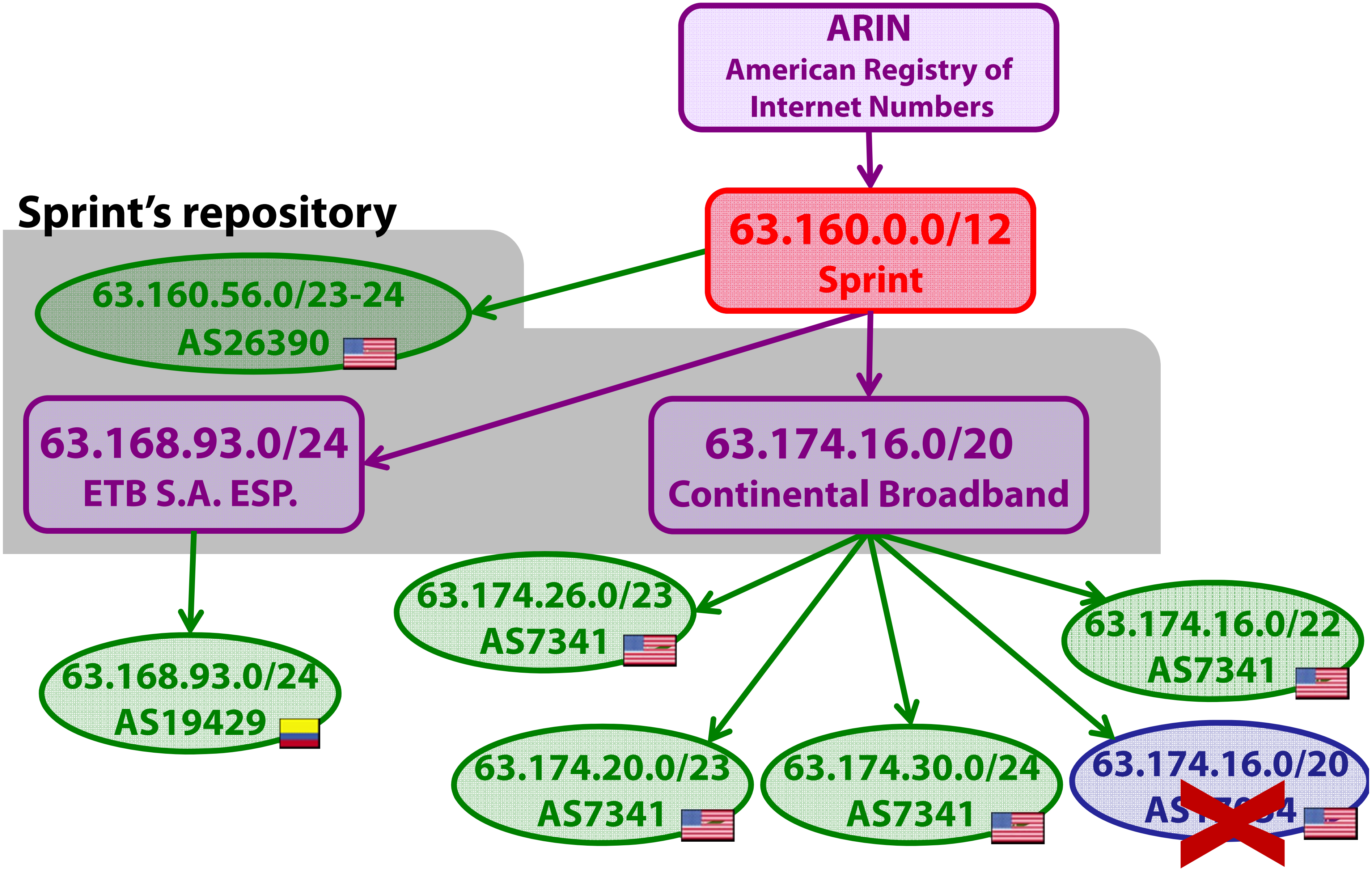
Routing policy:	Prefix remains reachable during …	
	routing hijack	RPKI problem
Drop Invalid	✓	X
"Depref invalid"	**subprefix hijacks possible**	✓

IP prefixes can be seized…

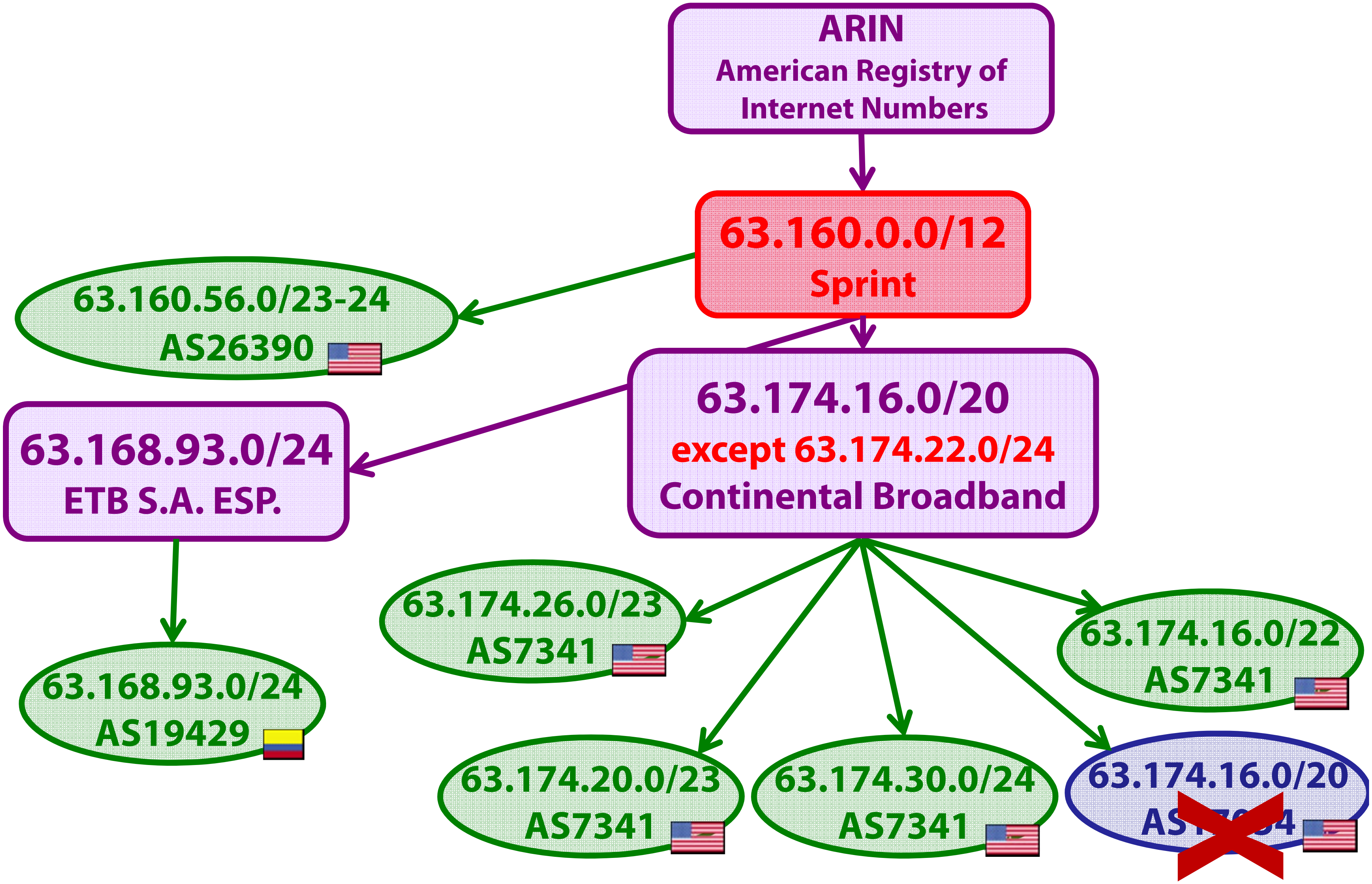
But, lots of collateral damage.



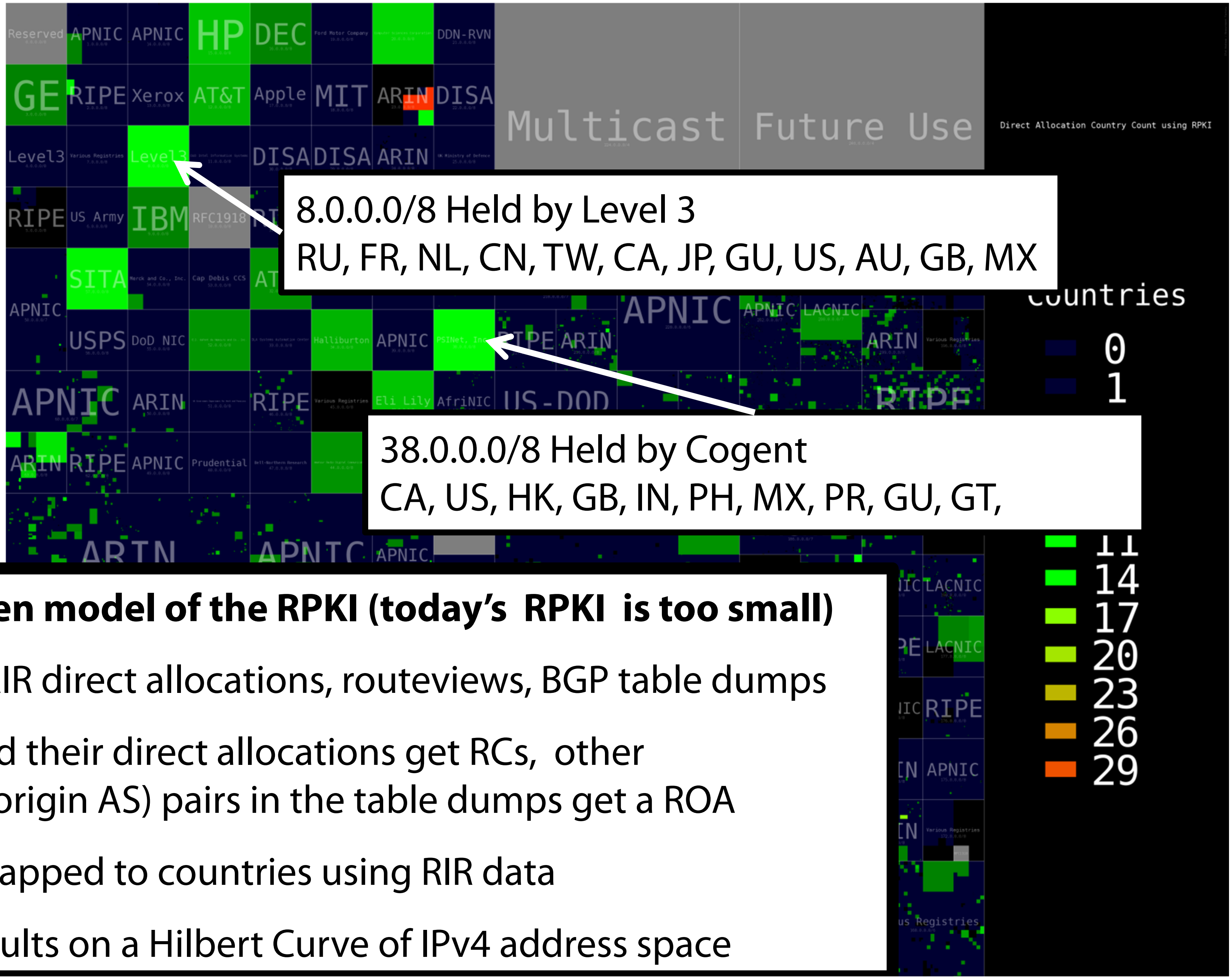
IP prefixes can be seized in a targeted manner…



IP prefixes can be seized in a **targeted** manner…



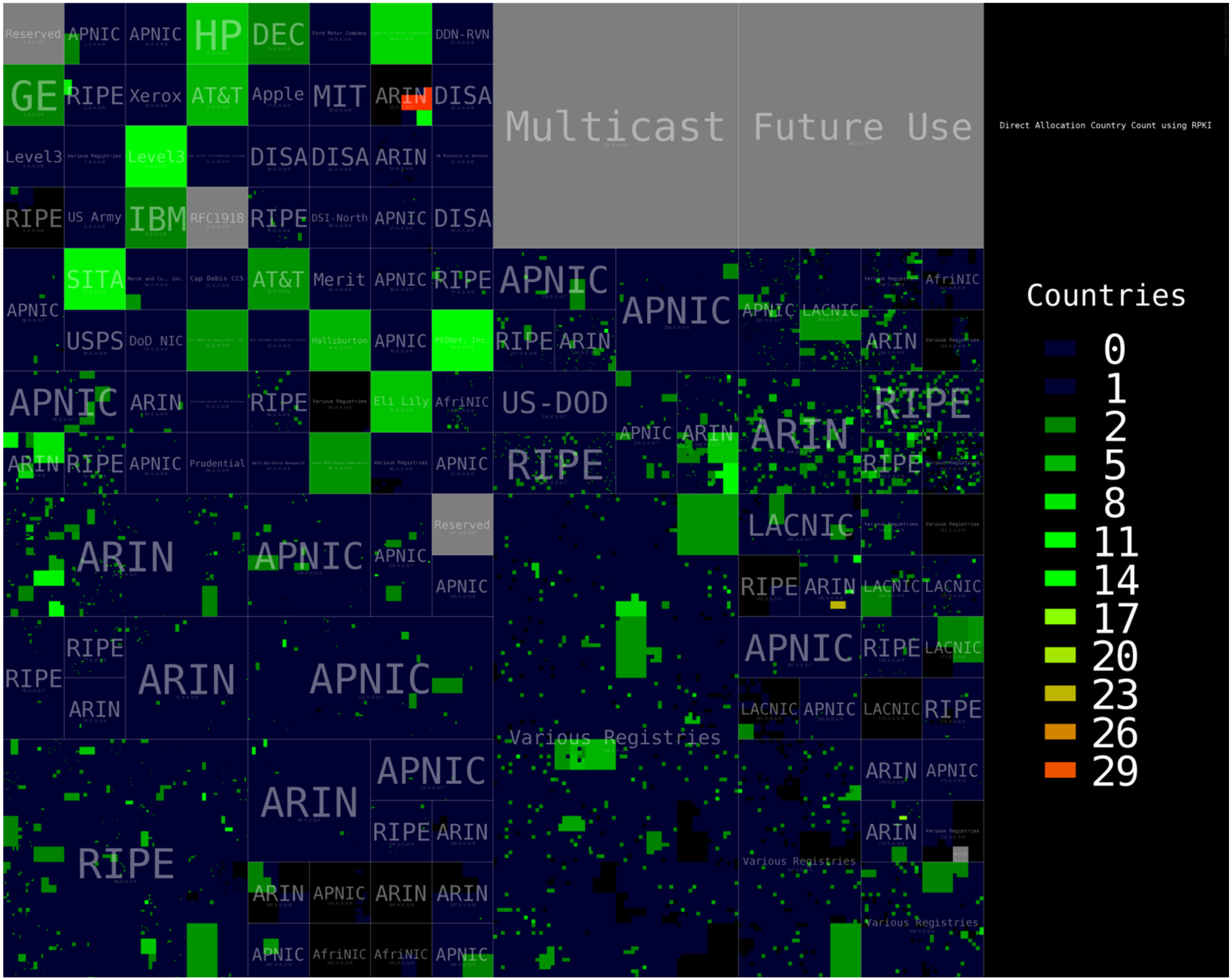
… that can cross international borders.



Data-driven model of the RPKI (today's RPKI is too small)

- ✧ Using RIR direct allocations, routeviews, BGP table dumps
- ✧ RIRs and their direct allocations get RCs, other (prefix,origin AS) pairs in the table dumps get a ROA
- ✧ ASes mapped to countries using RIR data
- ✧ Plot results on a Hilbert Curve of IPv4 address space

… that can cross international borders.



summary & future work

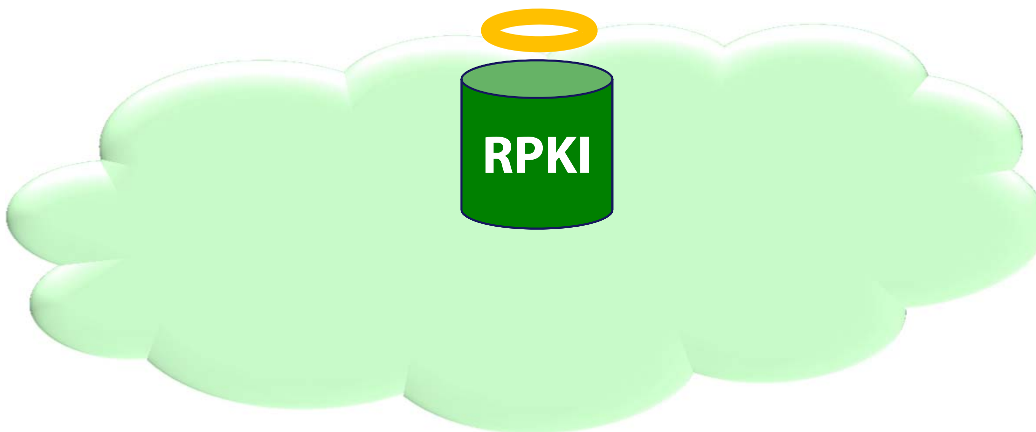
RPKI is the most crucial step in terms of security

- BGPSEC provides marginal gains;
- hard to realize these gains due to conflicting priorities in routing policies

RPKI alters trust relationships

- creates a small number of powerful authorities; crosses international borders
- Important work needs to be done to make RPKI more robust, including:
  - Recommendations for routing policies
  - Increasing certificate transparency (monitoring, logging, pinning, notaries)
  - And various other things (circular dependencies, partial deployment, etc)

Thanks!



Is the Juice Worth the Squeeze? BGP Security in Partial Deployment
Robert Lychev, Sharon Goldberg, Michael Schapira.
SIGCOMM'13, Hong Kong, China. August 2013

On the Risk of Misbehaving RPKI Authorities
Danny Cooper, Ethan Heilman, Kyle Brogle, Leonid Reyzin, Sharon Goldberg
HotNets'13, Maryland. November 2013.