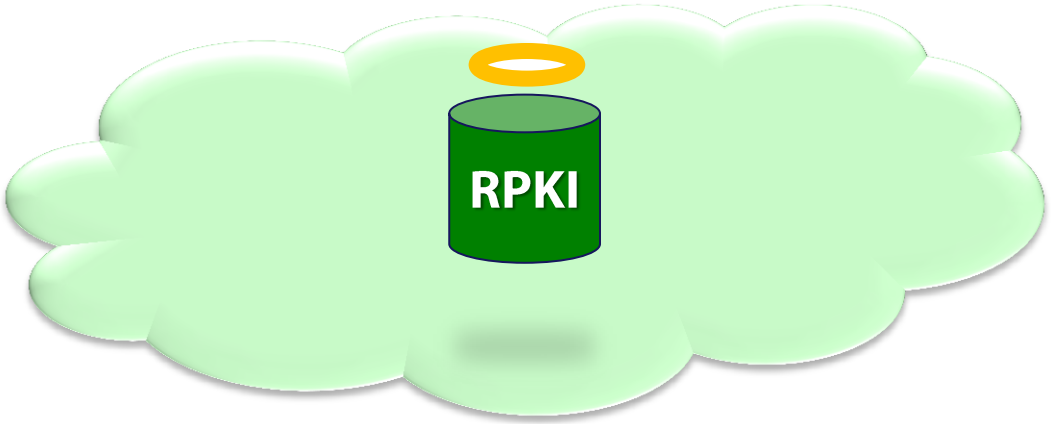
Why is it taking so long to secure BGP?



Sharon Goldberg

Boston University

Technion Summer School in Computer Security (3 hour tutorial)
September 2016

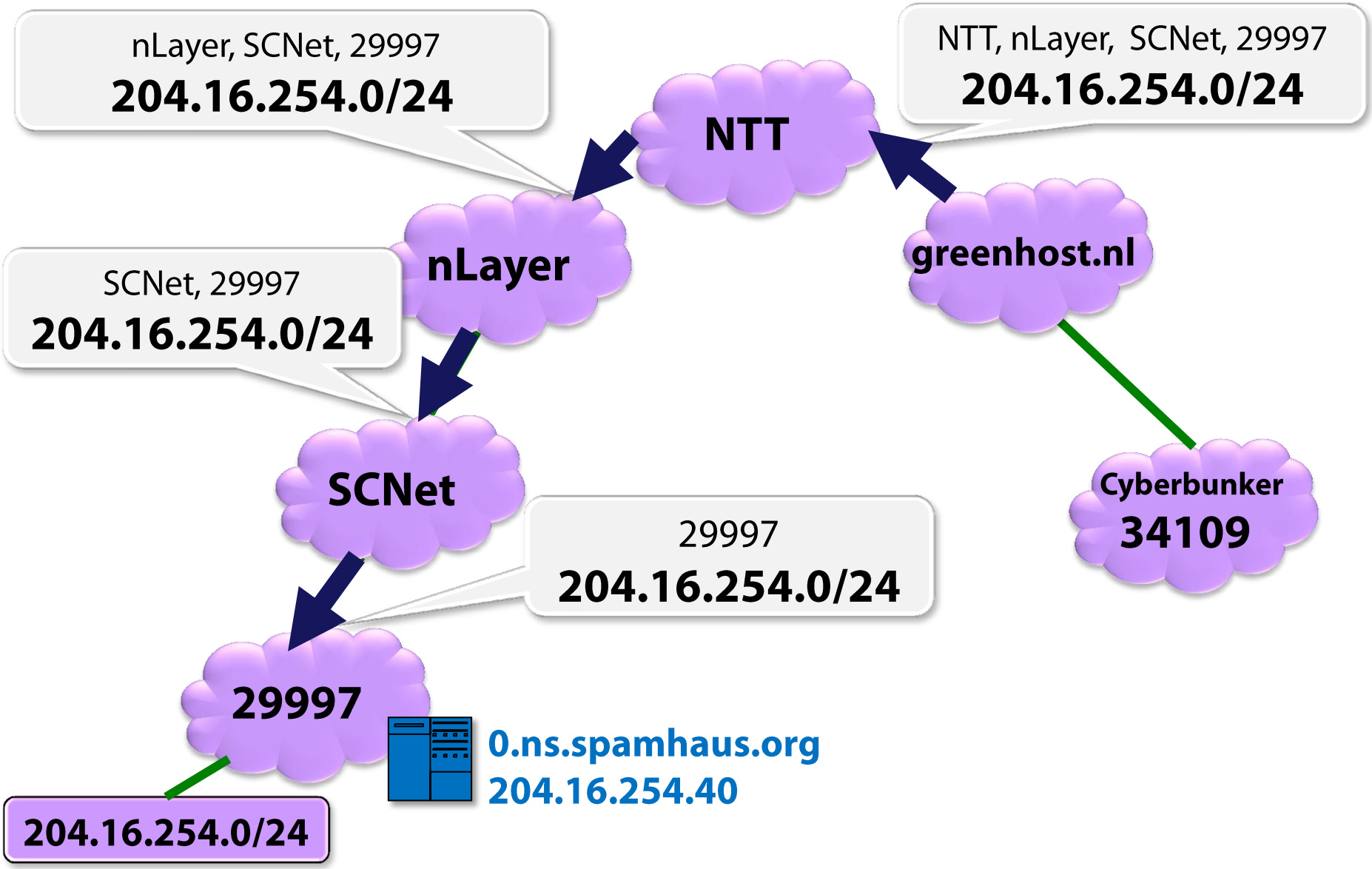
BOSTON UNIVERSITY

Based on joint work with Kyle Brogle, Danny Cooper, Ethan Heilman, Pete Hummon, Robert Lychev, Leonid Reyzin, Jennifer Rexford, Michael Schapira

SIGCOMM'11, SIGCOMM'13, HotNets'13 and SIGCOMM'14

interdomain routing

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



the subprefix hijack of spamhaus from 03/2013

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | U.S. Edition

The New York Times

Business Day
Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Attacks Used the Internet Against Itself to Clog Traffic

By JOHN MARKOFF and NICOLE PERLROTH
Published: March 27, 2013

An escalating cyberattack involving an antispam group and a shadowy group of attackers has now affected millions of people across the Internet, raising the question: How can such attacks be stopped?

Enlarge This Image

Gerry Shih/Reuters

Matthew Prince, chief executive of CloudFlare. The attacks first centered on his company's client Spamhaus and spiraled outward.

The short answer is: Not easily. The digital "fire hose" being wielded by the attackers to jam traffic on the Internet in recent weeks was made possible by both the best and worst aspects of the sprawling global computer network. The Internet is, by default, an open, loosely regulated platform for communication, but many of the servers that make its communication possible have been configured in such a way that they can be easily fooled.

The latest attacks, which appeared to have subsided by

FACEBOOK
TWITTER
GOOGLE+
SAVE
E-MAIL
SHARE
PRINT
SINGLE PAGE
REPRINTS

Enough Said
Now Playing

More Tech Coverage
News from the Bits

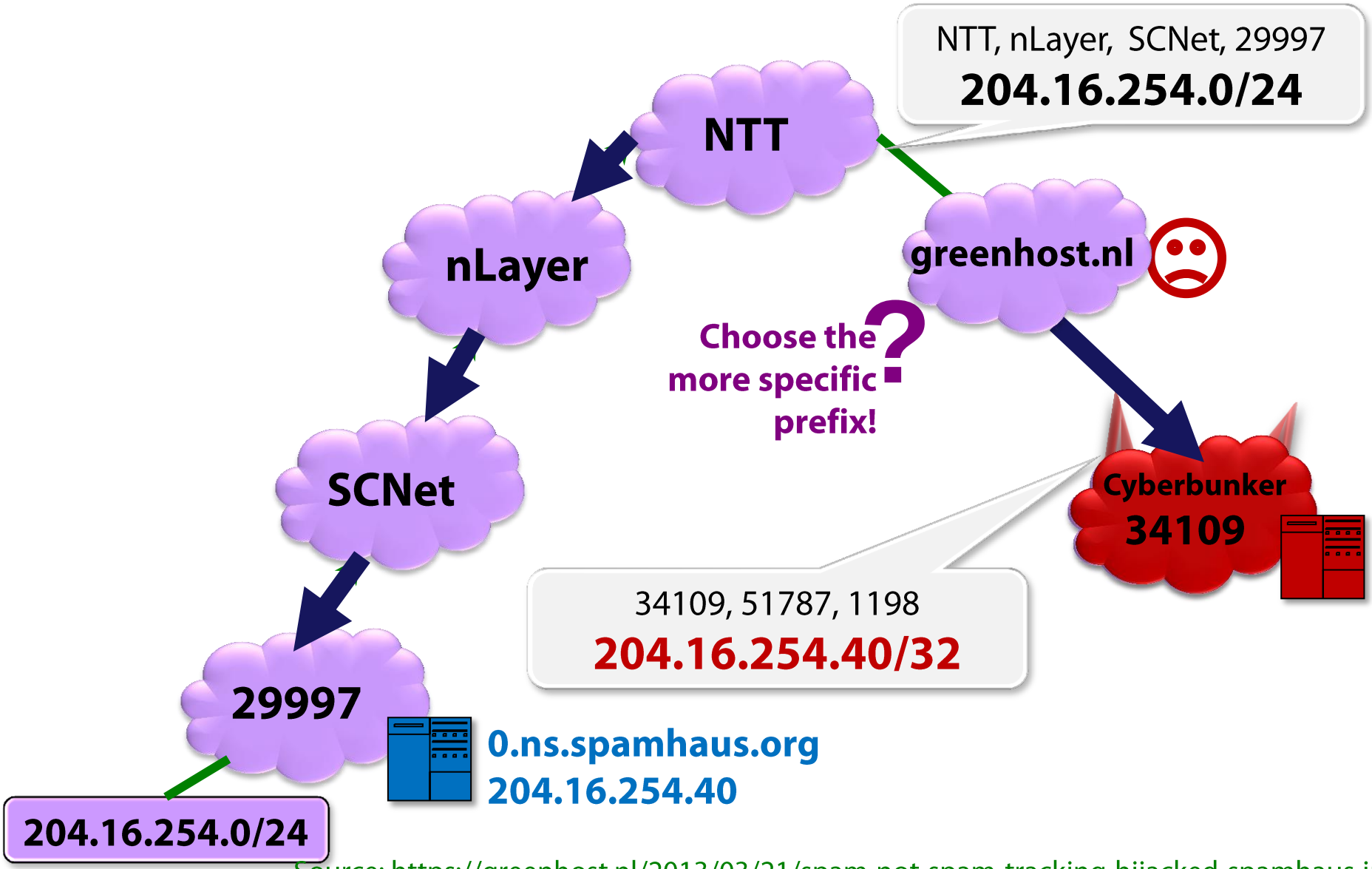
t, 29997
0/24

unker
09

204.16.254

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/

the subprefix hijack of spamhaus from 03/2013

@eqe (Andy Isaacson) @eqe 29 Mar
Much worse than the 300Gbps DoS, CyberBunker BGP hijacked Spamhaus IPs. greenhost.nl/2013/03/21/spa…
Details

explanoit @explanoit 29 Mar
Whoa. RT "@eqe: Much worse than the 300Gbps DoS, CyberBunker BGP hijacked Spamhaus IPs. greenhost.nl/2013/03/21/spa…"
Details

TheSTOPhaus Movement Follow
@stophaus

@explanoit @eqe No one here cares about #spamhaus or that are affected by using them. We hope you ZEN query bites you and it might lulz

Reply Retweet Favorite More

6:45 PM - 30 Mar 13

t, 29997
0/24

unker
09

204.16.254.0/24

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

and many other incidents…

2010

REPORT TO CONGRESS

of the

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Interception of Internet Traffic

For a brief period in April 2010, a state-owned Chinese telecommunications firm "hijacked" massive volumes of Internet traffic.* [114] Evidence related to this incident does not clearly indicate whether it was perpetrated intentionally and, if so, to what ends. However, computer security researchers have noted that the capability could enable severe malicious activities.[115]

and many other incidents…

The New York Times

The Lede

The New York Times News Blog

Pakistan Blamed for Worldwide YouTube Break

By MIKE NIZZA FEBRUARY 25, 2008 9:34 AM

If all had gone according to plan, Pakistan would have been th
latest government taking part in an unsettling trend from Bra
Thailand: YouTube blocking. Unlike its predecessors, though,
Pakistan also affected thousands of people beyond its borders.

In case you were wondering on Sunday why you couldn't watc

and many other incidents…

2010

REPORT TO CONGRESS

of the

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Interception of Internet Traffic

For a brief period in April 2010, a state-owned Chinese telecommunications firm "hijacked" massive volumes of Internet traffic.* [114] Evidence related to this incident does not clearly indicate whether it was perpetrated intentionally and, if so, to what ends. However, computer security researchers have noted that the capability could enable severe malicious activities.[115]

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESI

THREAT LEVEL

Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins

BY ANDY GREENBERG 08.07.14 | 1:00 PM | PERMALINK

Share 1.0K Tweet 1,465 g+1 214 Share 524 Pin it

and many other incidents…

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION M

Someone's Been Siphoning Data Through a Huge Security Hole in the Internet

BY KIM ZETTER 12.05.13 | 6:30 AM | PERMALINK

Traceroute Path 2: from Denver, CO to Denver, CO via *Iceland*

Hijacked traffic went all the way to Iceland, where it may have been copied before being released to its intended destination. The green arrows show the path the traffic should have traveled; the red arrows show the path it took. *Map courtesy of Renesys*

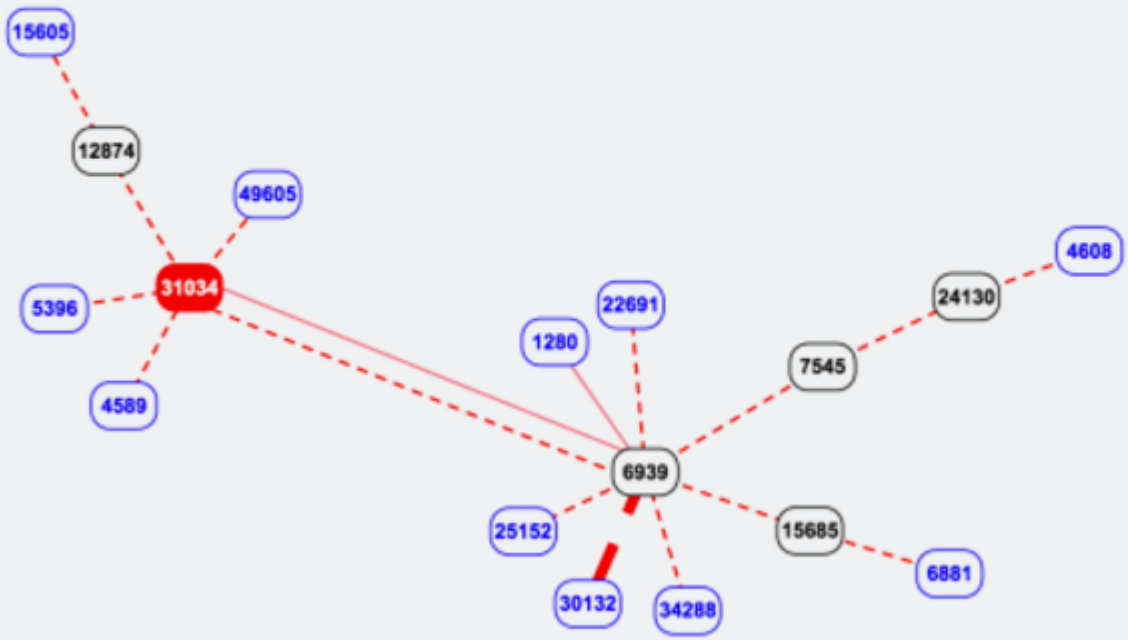
and many other incidents…

RISK ASSESSMENT —

Hacking Team orchestrated brazen BGP hack to hijack IPs it didn't own

Hijacking was initiated after Italian Police lost control of infected machines.

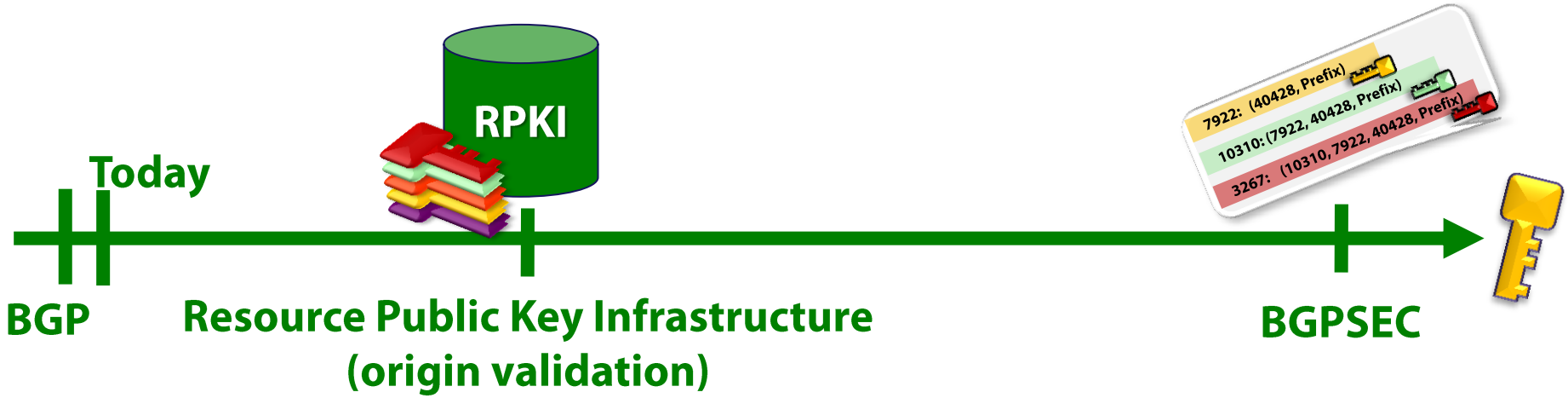
DAN GOODIN - 7/12/2015, 6:53 PM



OpenDNS

Enlarge / A border gateway network graph for 46.166.163.0/24

crypto to the rescue!



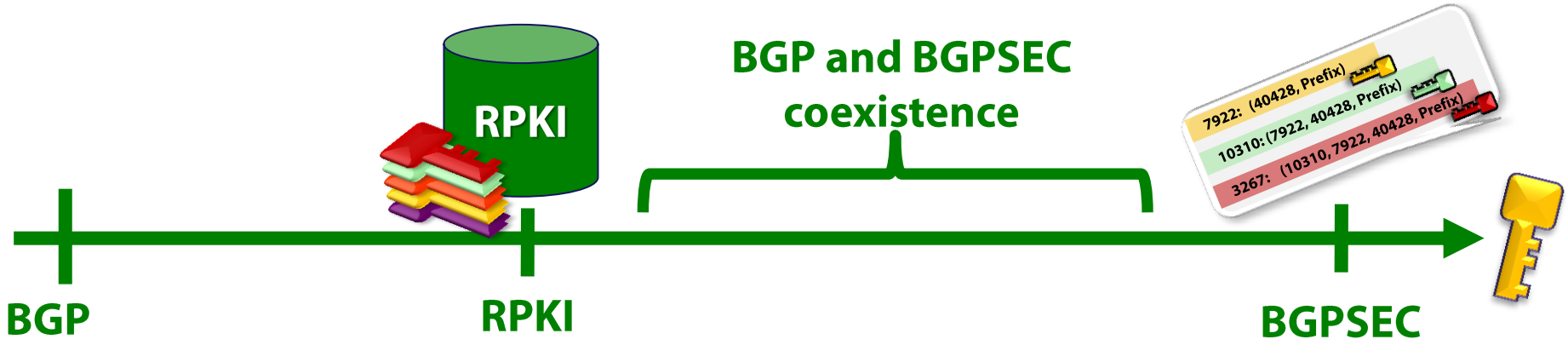
- IETF Standard published 2012.
- Deployment started in 2011.
- Certifies IP prefix allocations.
- Crypto done out-of-band
- No change to BGP messages

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

Main challenge?

Incremental deployment & backward compatibility

talk overview



What are the security benefits of adopting these protocols?

- What does BGPSEC offer over the RPKI? **[SIGCOMM'11]**
- Focus on the transition, when BGP and BGPSEC coexist. **[SIGCOMM'13]**
- 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]**

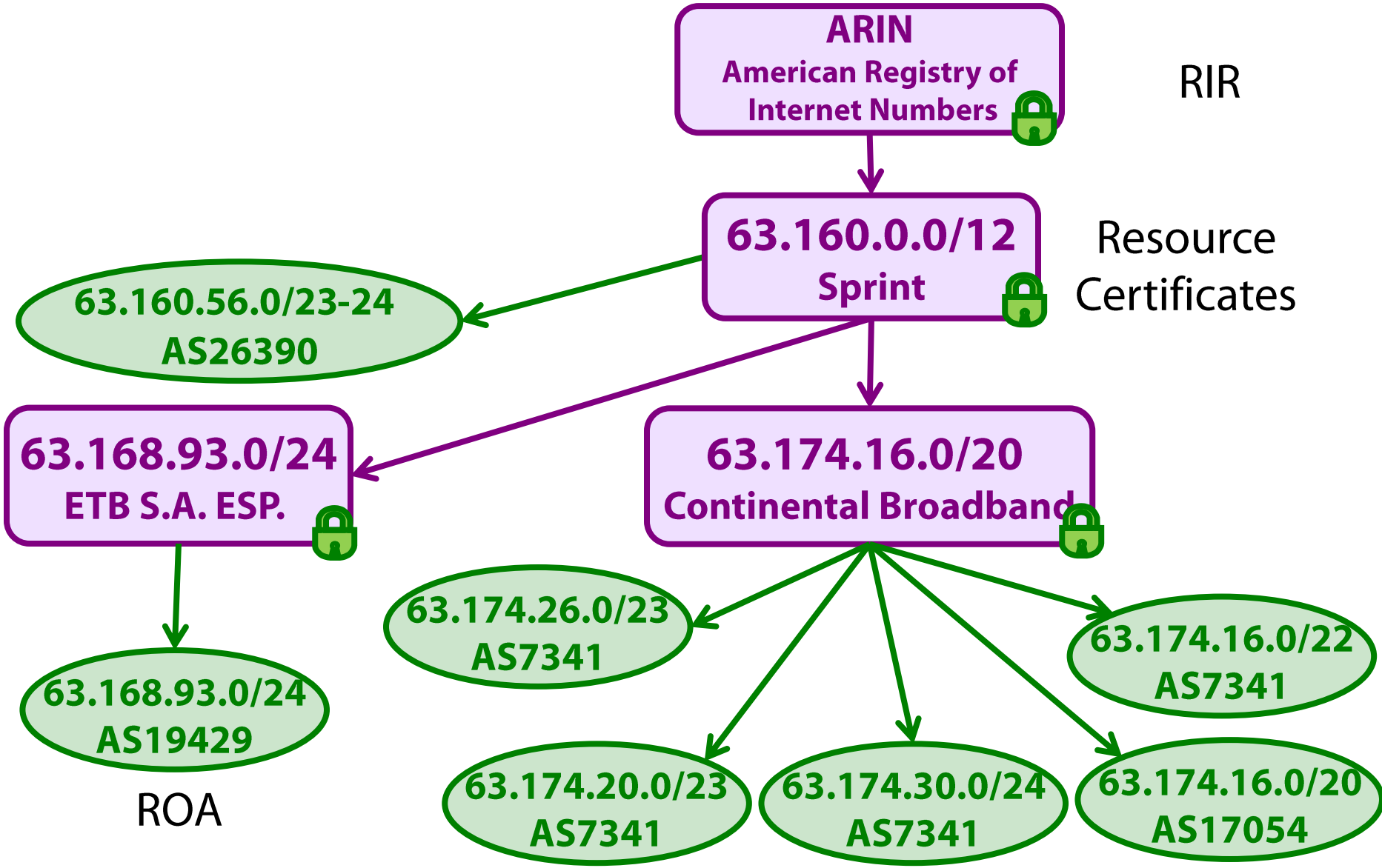
- Analyze the RPKI in a threat model where certificate authorities are compromised.

part 1: security benefits of RPKI and BGPSEC

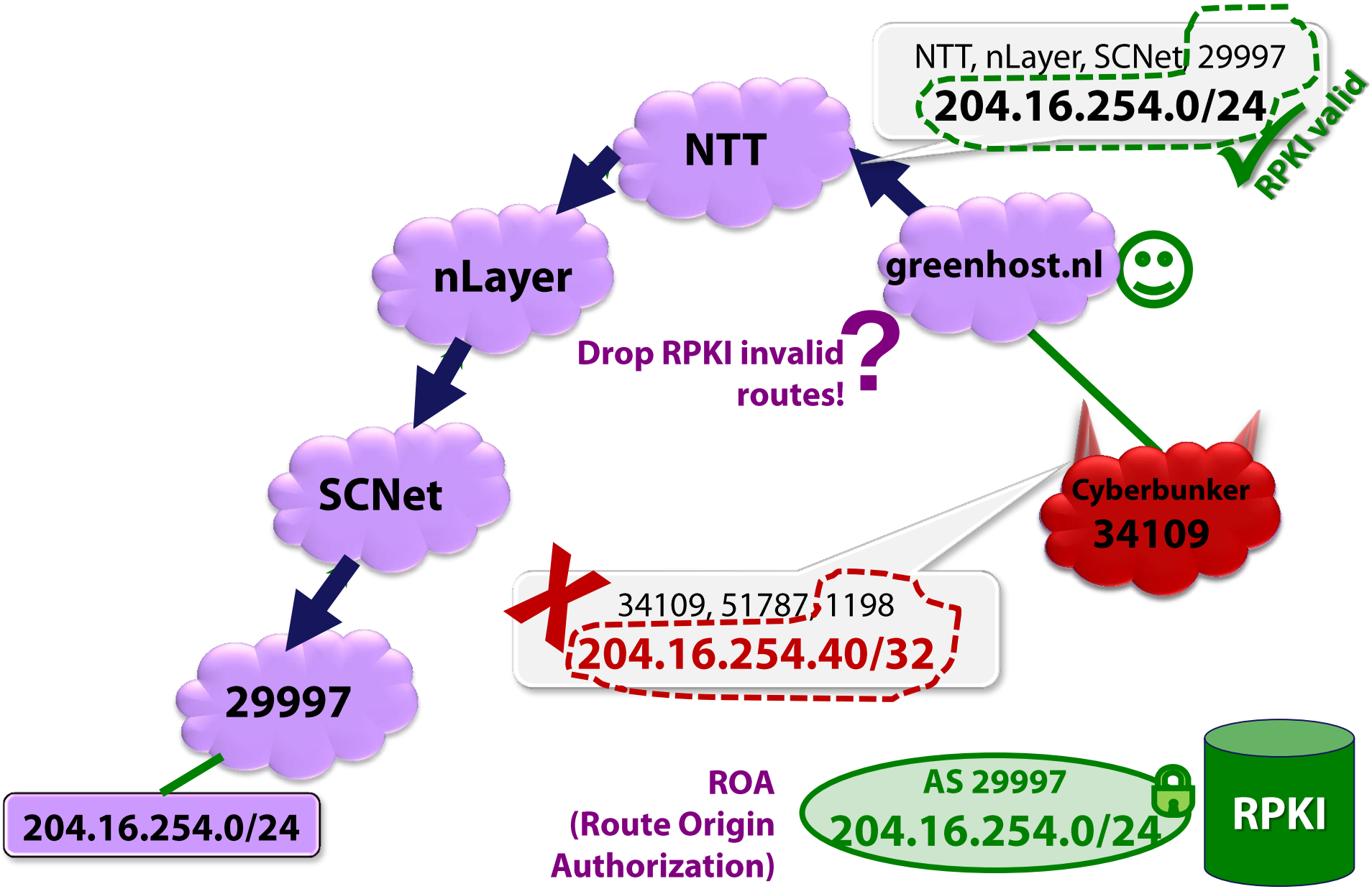
1. background: RPKI, BGPSEC
2. why BGP / BGPSEC coexistence is tricky
3. experimental evaluation of security for RPKI and BGPSEC

BOSTON UNIVERSITY

the RPKI and its cryptographic objects

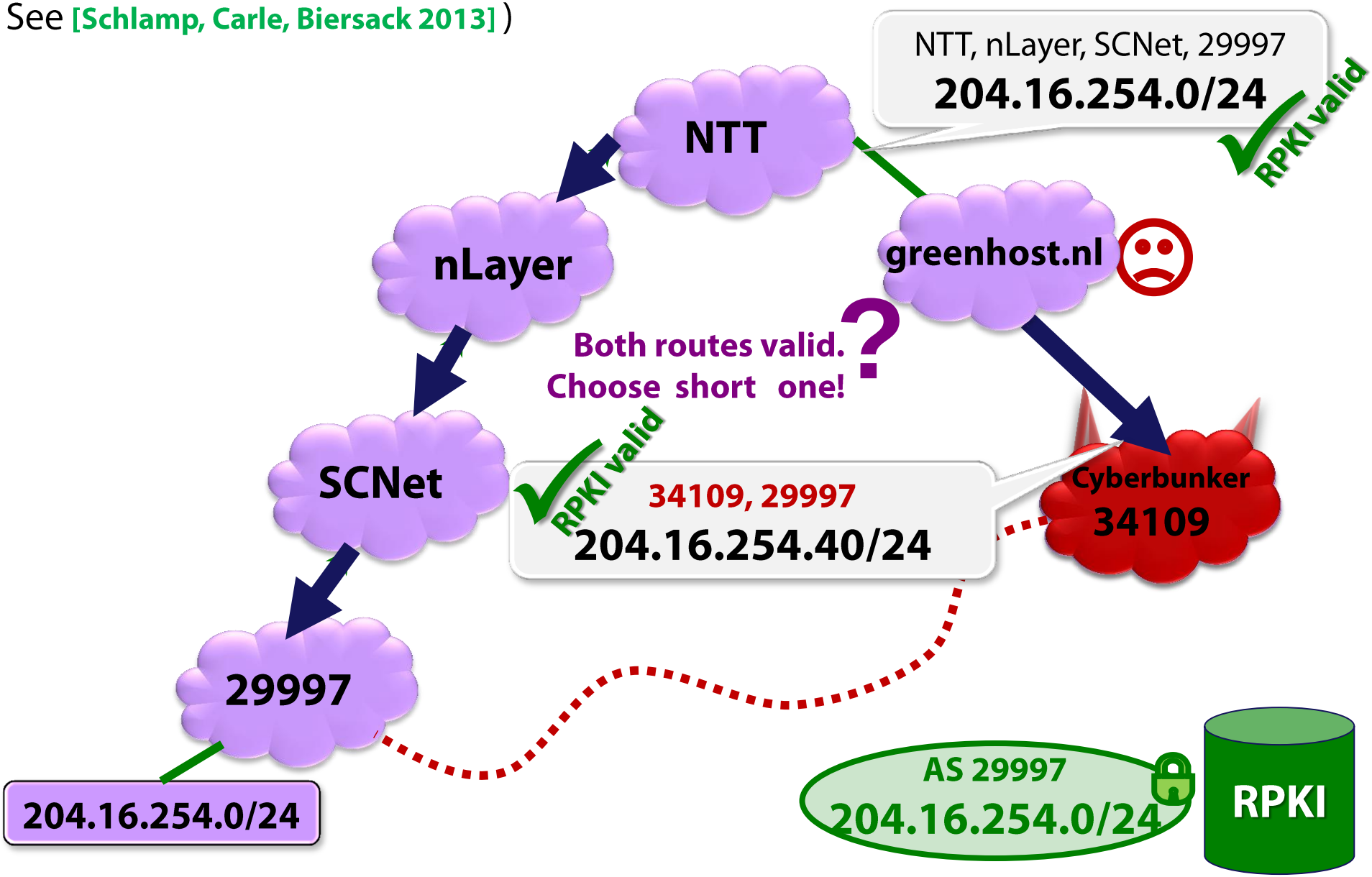


the RPKI defeats all subprefix & prefix hijacks

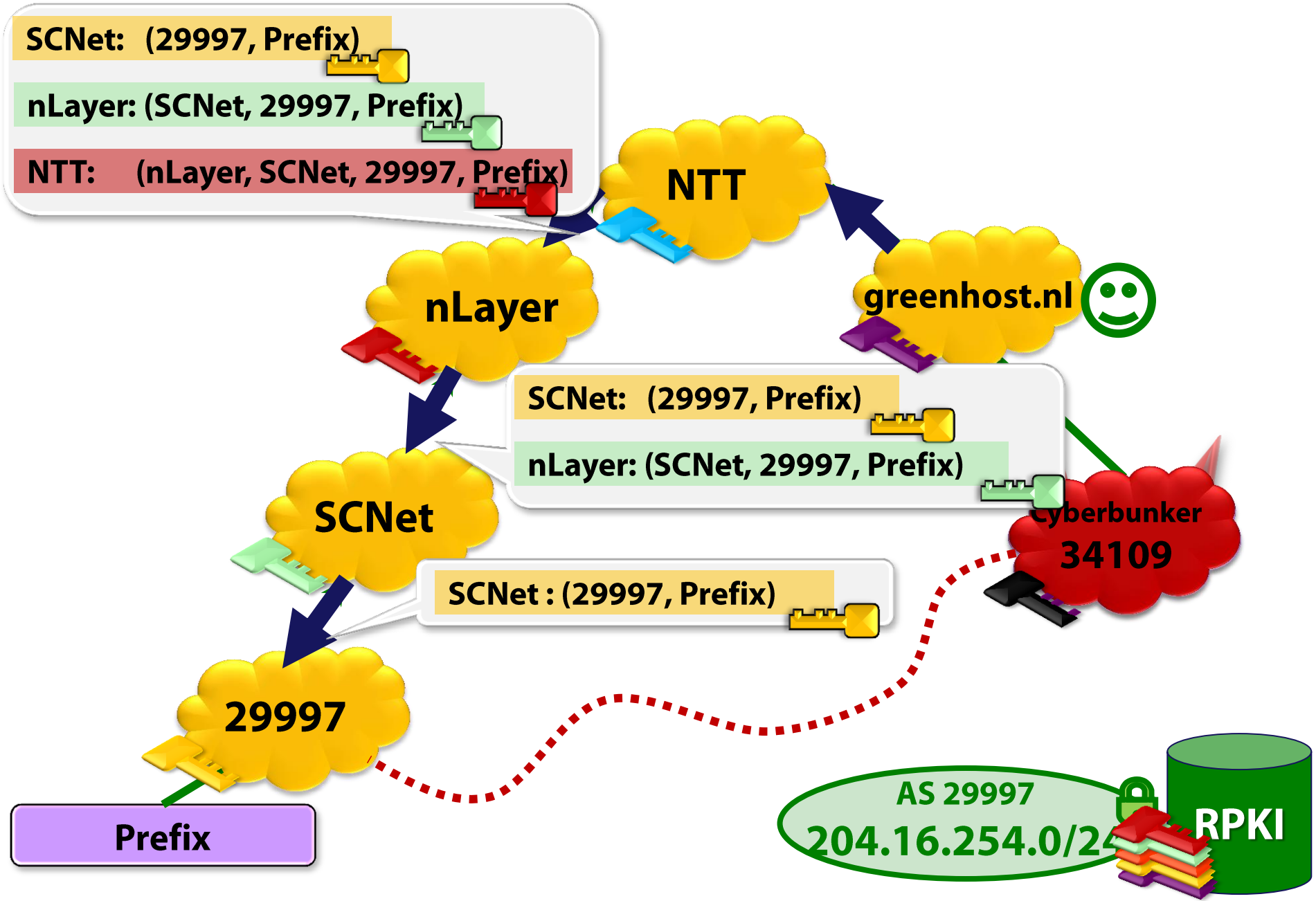


the "1-hop hijack" defeats the RPKI

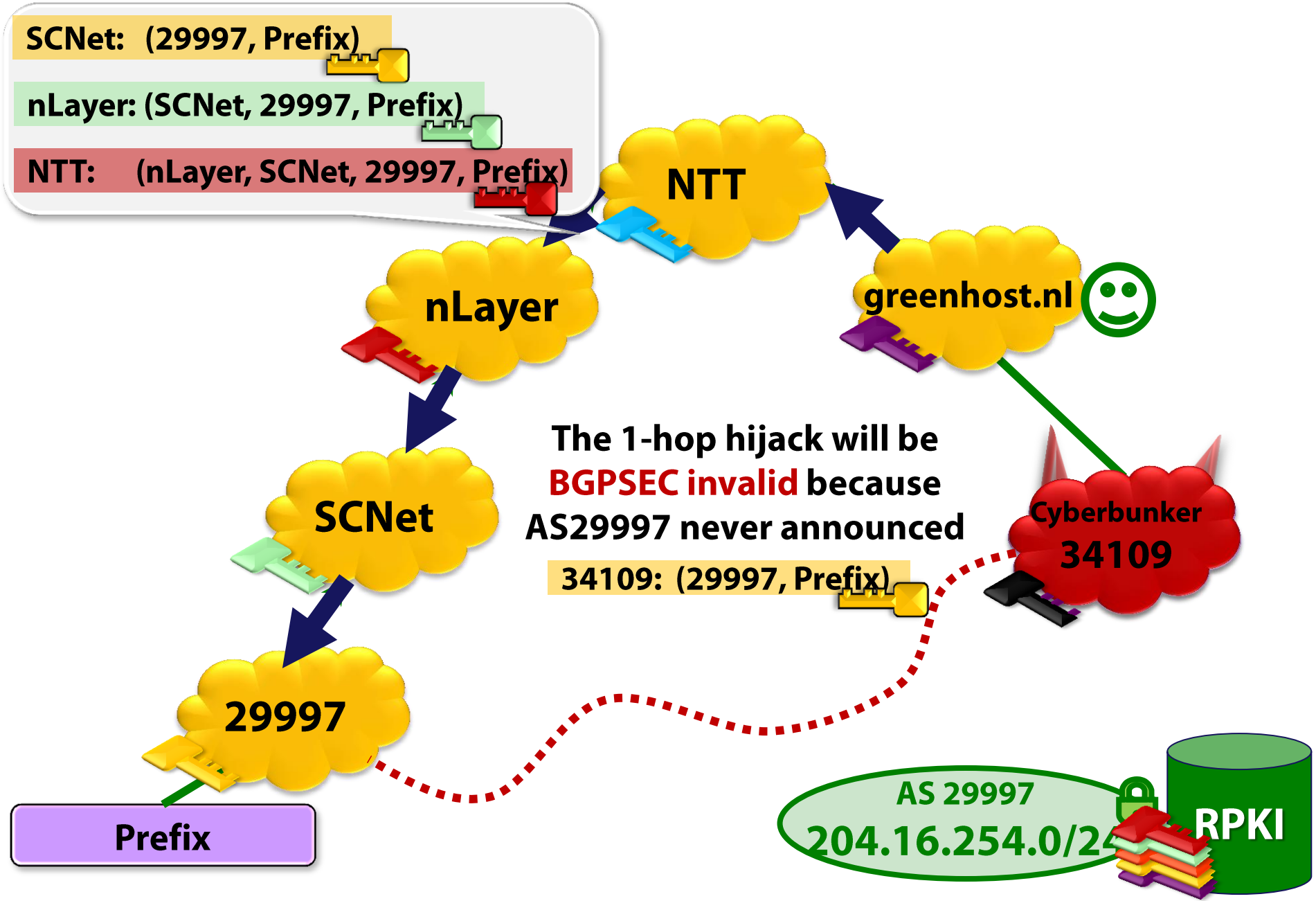
(This exact situation is hypothetical, but this type of attack has been seen in the wild, See [Schlamp, Carle, Biersack 2013])



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



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

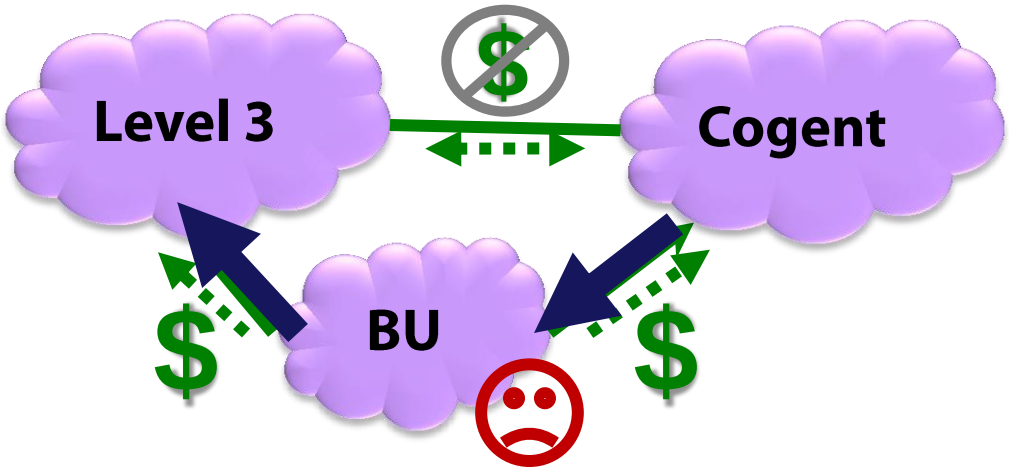


how do ASes choose routes?

Routing Policy

The Gao-Rexford Model

1. Prefer customer paths over peer paths over provider paths
2. prefer short routes ("performance")
3. tiebreak on interdomain criteria



Export policy:

Announce BGP route to neighbor only if:

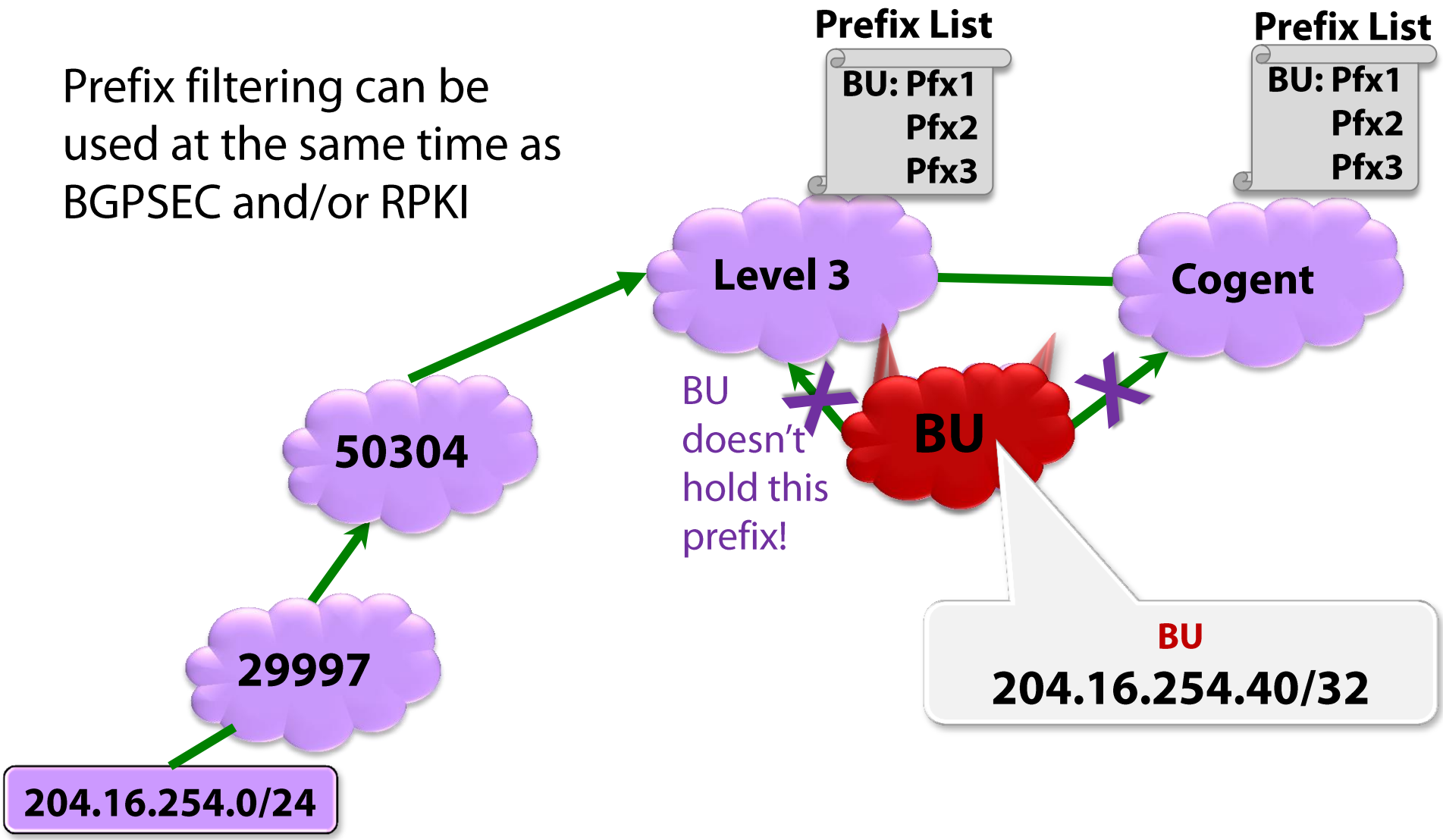
- The neighbor is a customer, OR
- The path is a customer path.

A Smart Attack Strategy:
Announce the **shortest** path can get away with to **all** my neighbors!

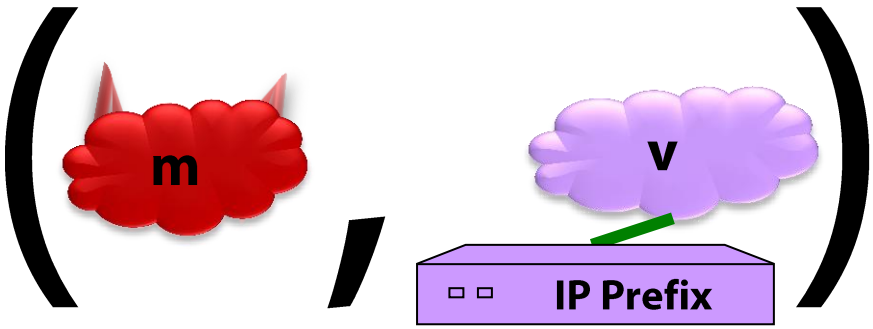
prefix filtering stops all attacks by stubs

A stub is an AS that has no customers of its own (eg. BU)

Prefix filtering can be used at the same time as BGPSEC and/or RPKI



obtaining our simulation results



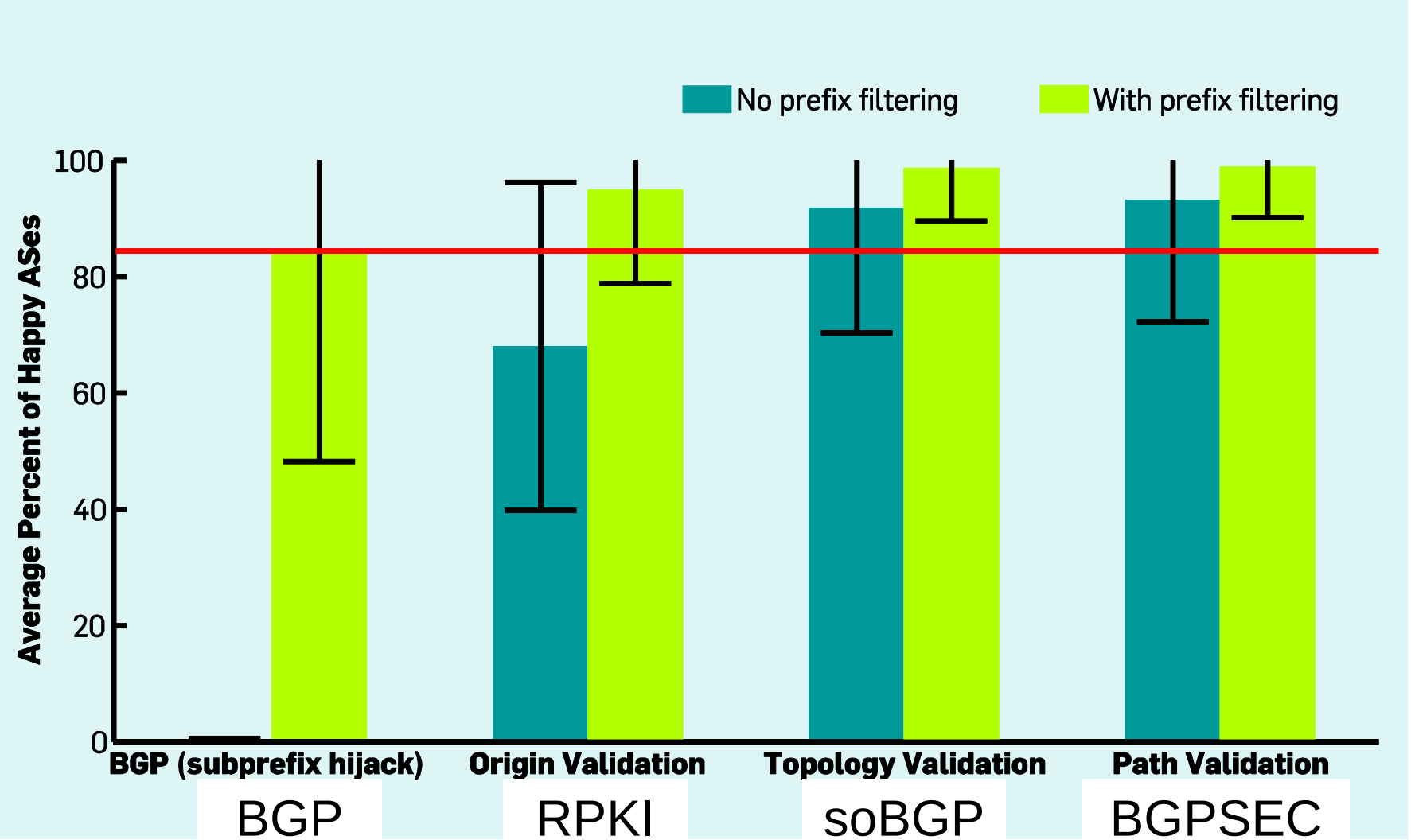
A Smart Attack Strategy:
Announce the **shortest** path can get away with to **all** my neighbors!

We ran multiple experiments

- For each, randomly chose (attacker, victim) pair, and
- … simulate Smart Attack on each security protocol.
- … with Gao-Rexford model on an empirical AS graph (from 2012)

comparing defenses: % safe ASes during smart attack

Figure 2. Comparing defenses. The average percentage of safe ASes during naive attack with a randomly chosen (attacker, victim) pair; error bars represent one standard deviation; and the horizontal line represents the effect of prefix filtering.

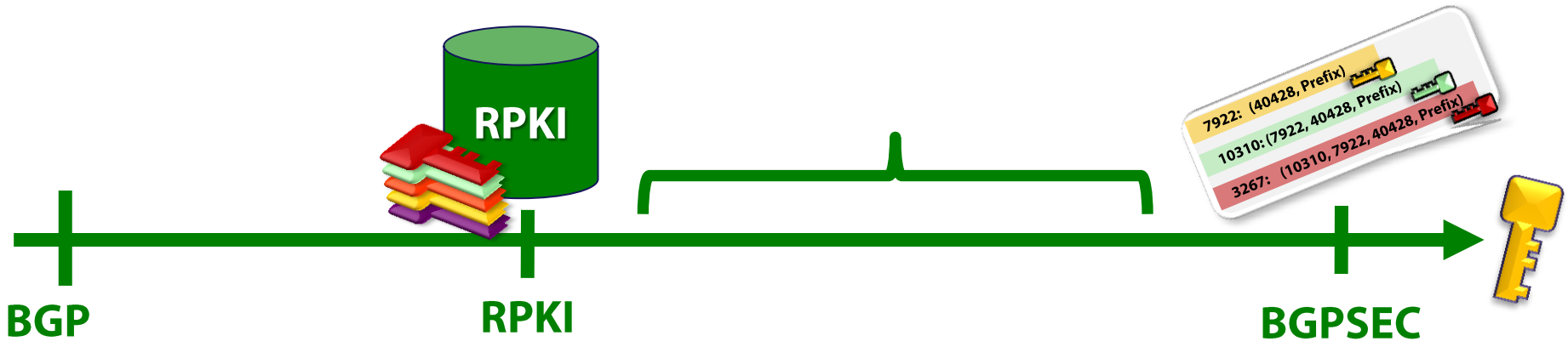


part 2: security in partial deployment

1. when some ASes deploy BGPSEC, but others don't
2. why BGP / BGPSEC coexistence is tricky
3. evaluation of security for RPKI and BGPSEC

BOSTON UNIVERSITY

setup for our analysis in [SIGCOMM'13]



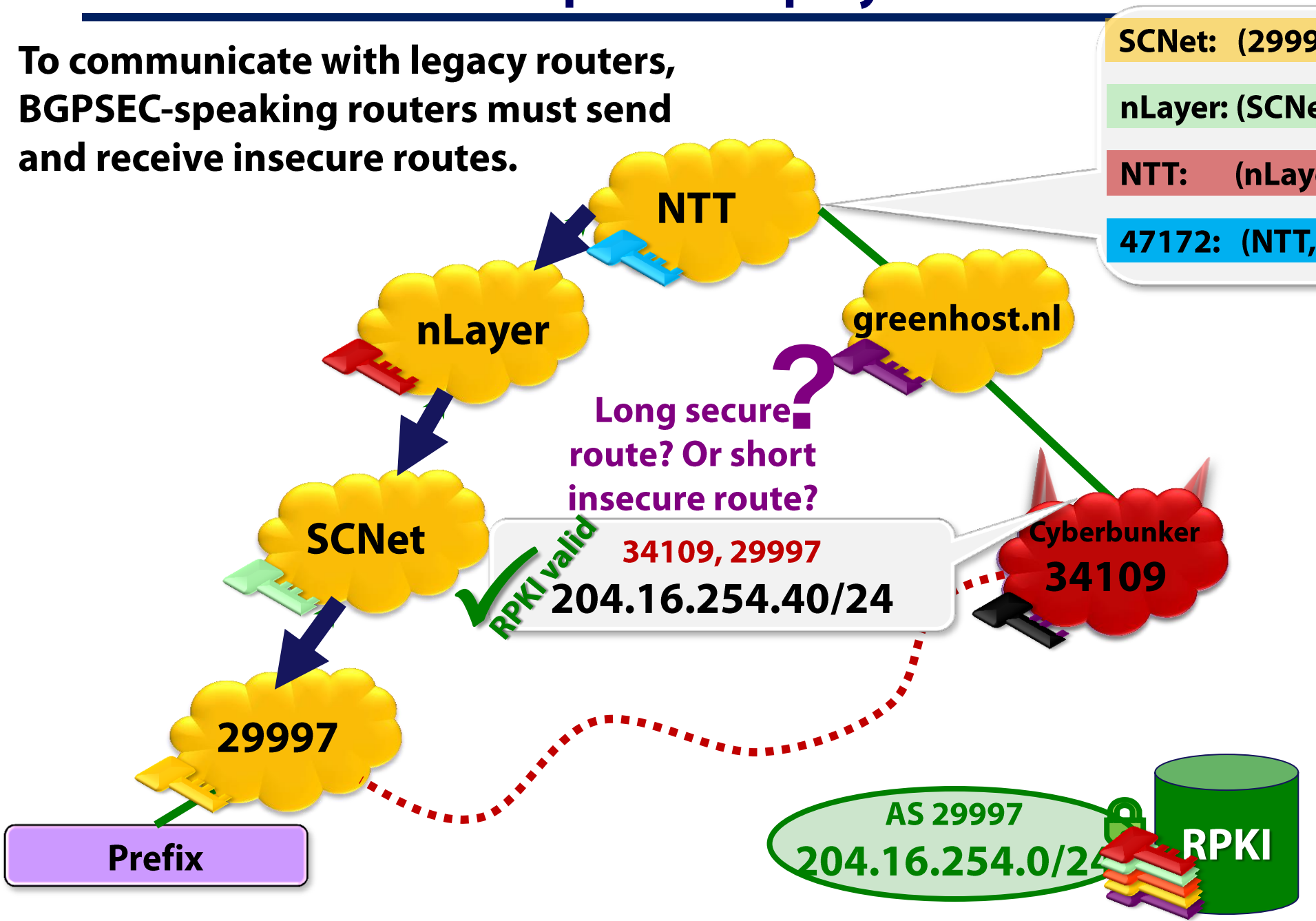
We suppose RPKI is fully deployed.

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

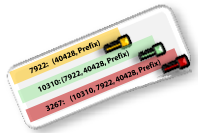
What happens when BGP and BGPSEC coexist?

BGPSEC in partial deployment

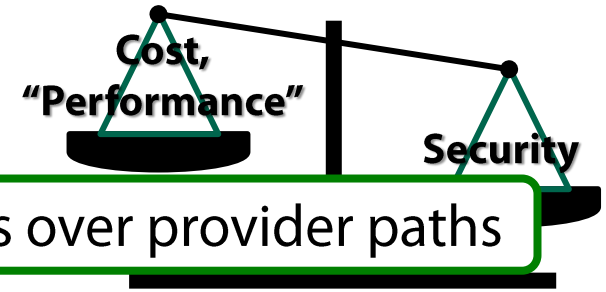
To communicate with legacy routers, BGPSEC-speaking routers must send and receive insecure routes.



how to prioritize security in partial deployment?



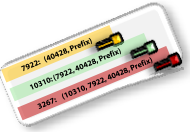
BGPSEC Security 1st



1. Prefer customer paths over peer paths over provider paths

BGPSEC Security 2nd

2. prefer short routes ("performance")



BGPSEC Security 3rd

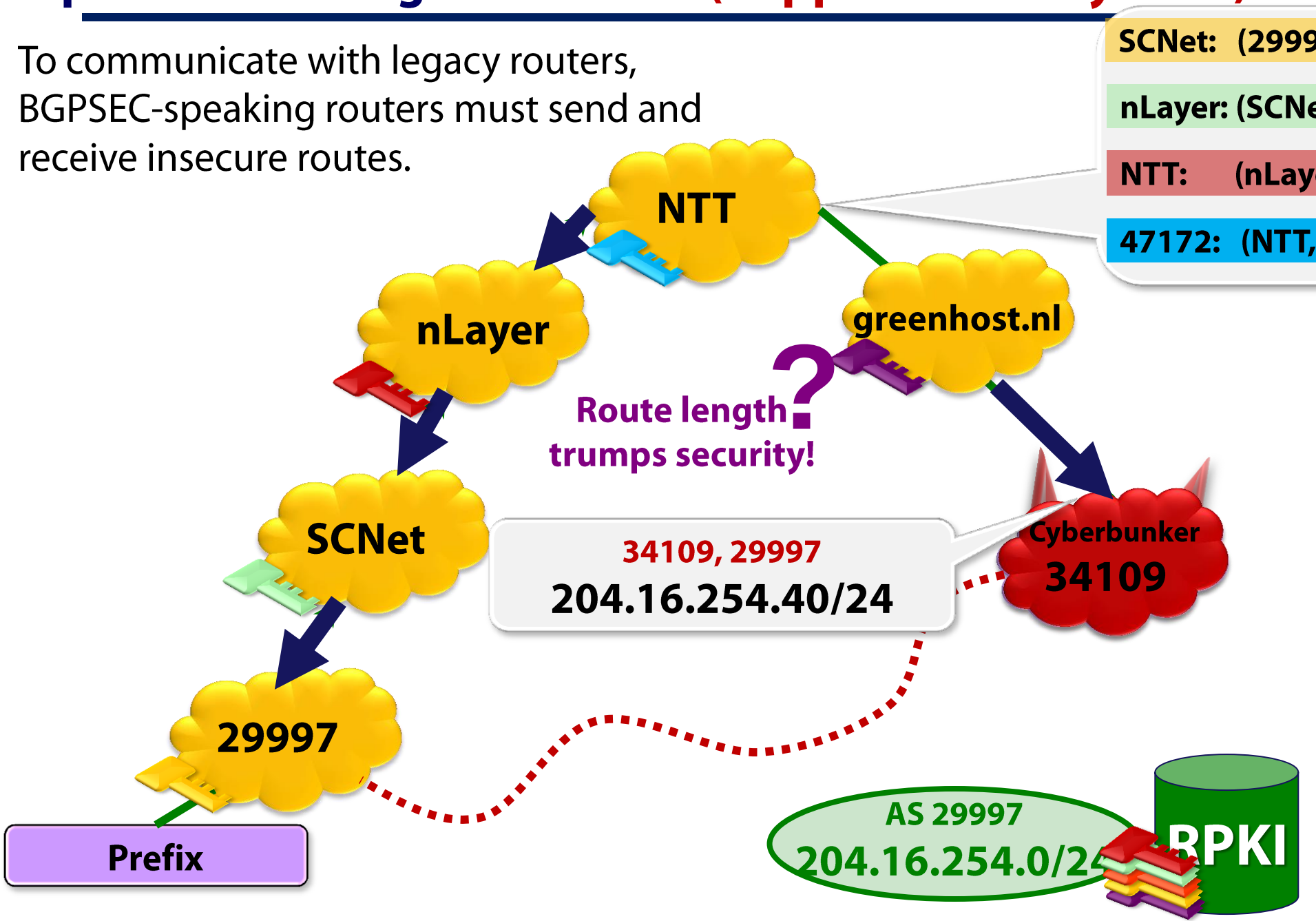
3. tiebreak on interdomain criteria

✧ 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)

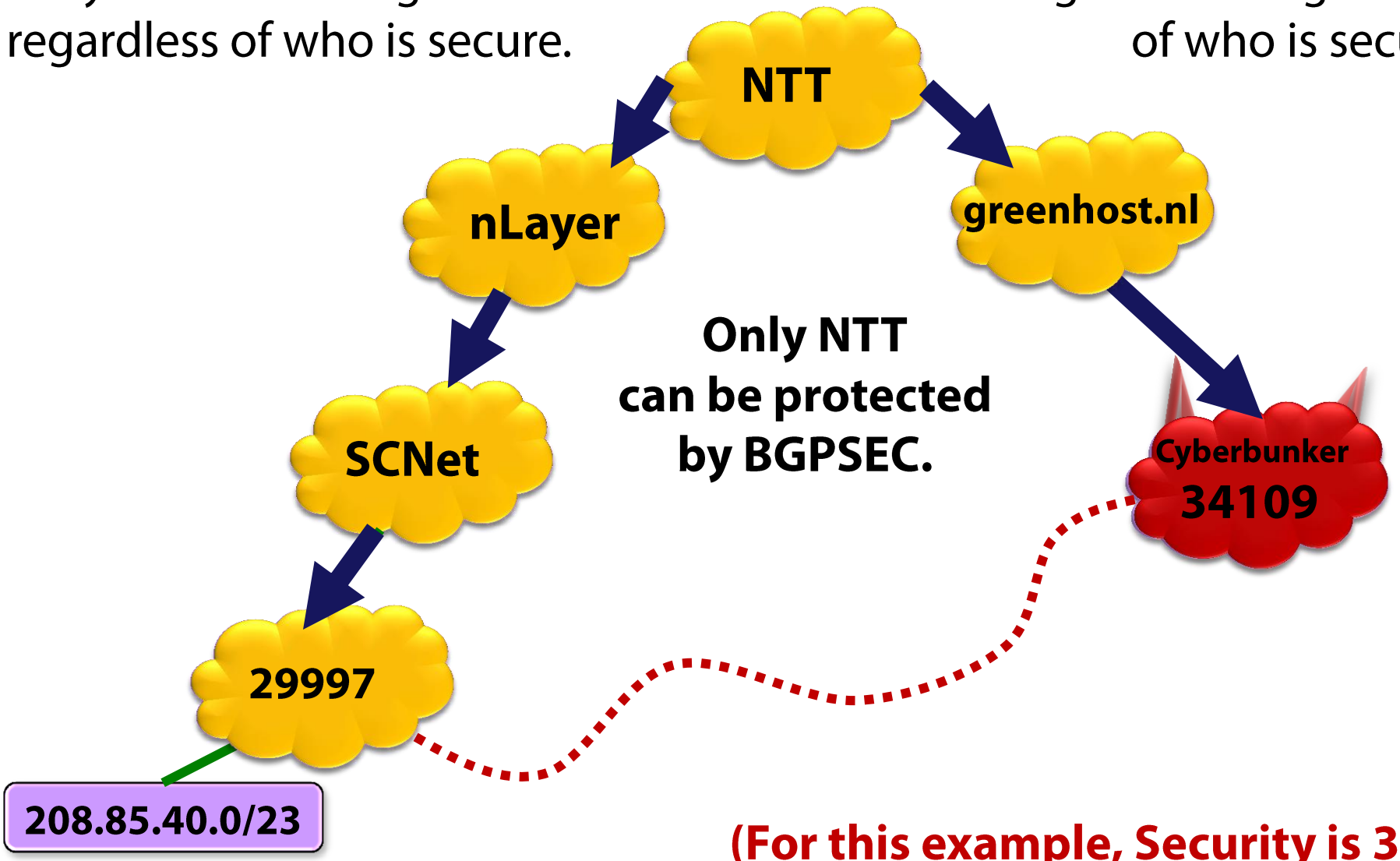
To communicate with legacy routers, BGPSEC-speaking routers must send and receive insecure routes.



quantify security using only topology & routing model!

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

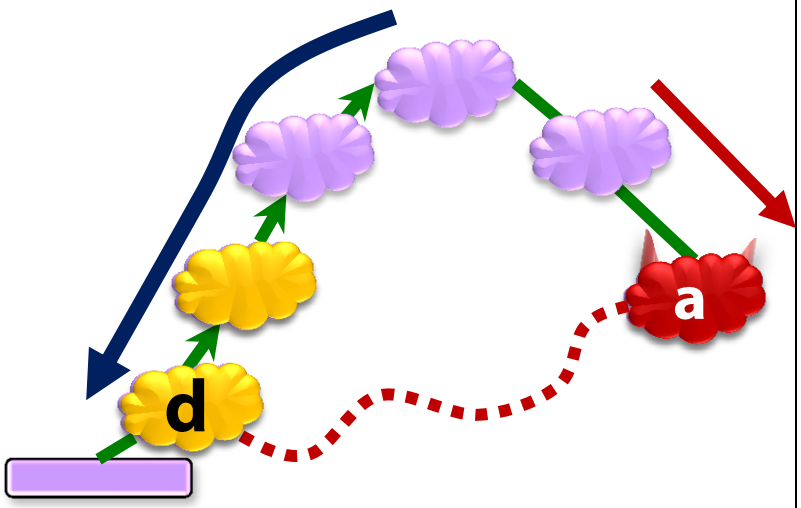
greenhost is doomed! It chooses the bogus route regardless of who is secure.



(For this example, Security is 3rd)

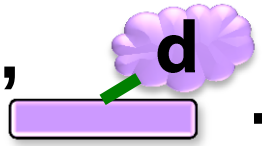
quantifying security

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



The number of ASes choosing a legitimate route is

Happy[**S**, 

, 

] = 3

Our security metric averages this over all non-stub a and all d.

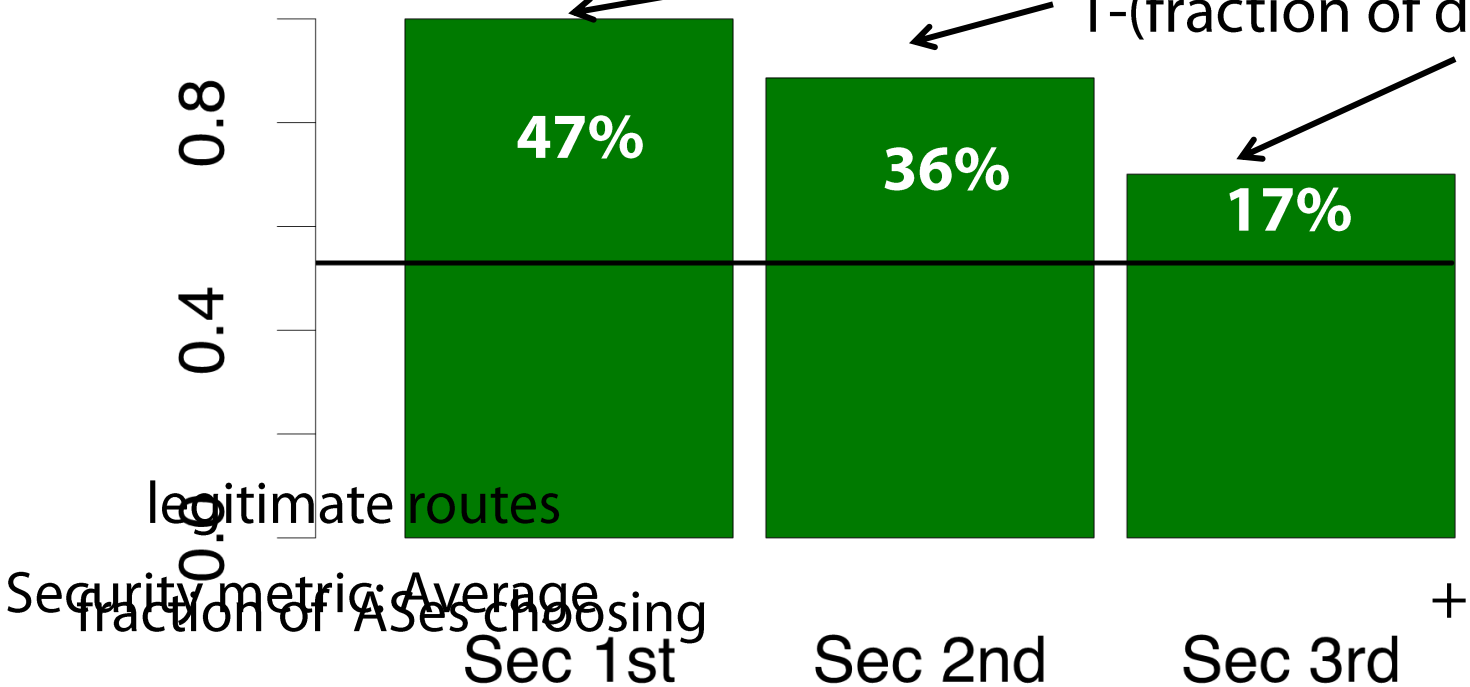
But, it's hard to find the "right" S :

- 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

bounding security provided by any BGPSEC deployment

the maximum improvement for **any** BGPSEC deployment is 1-(fraction of doomed ASes).

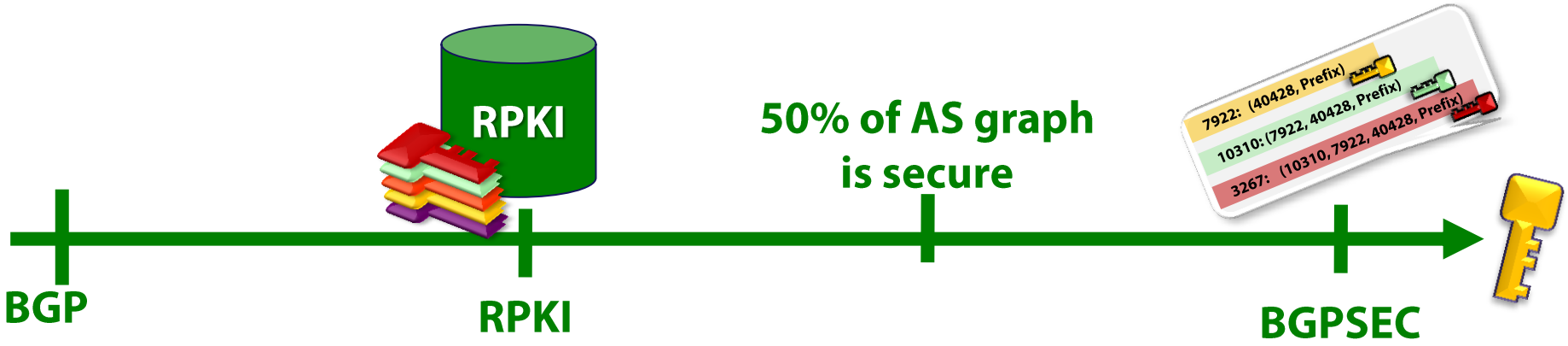


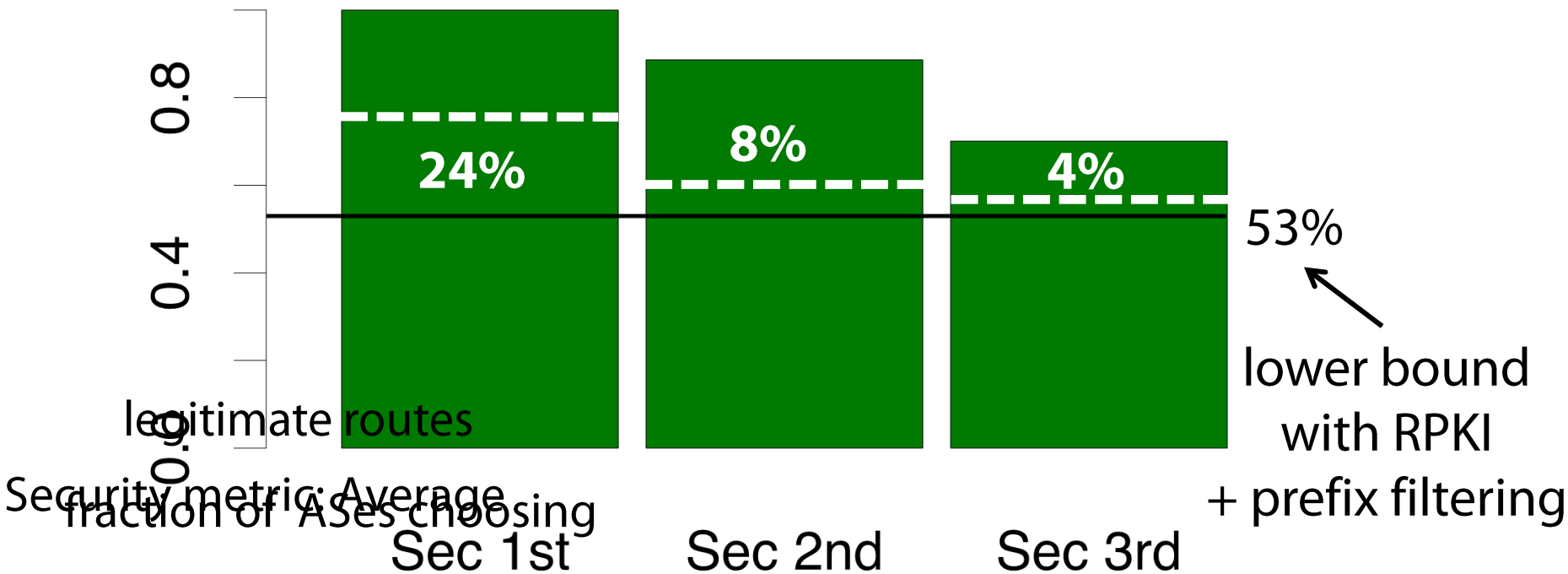
lower bound with RPKI + prefix filtering

legitimate routes

Security metric: Average fraction of ASes choosing

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

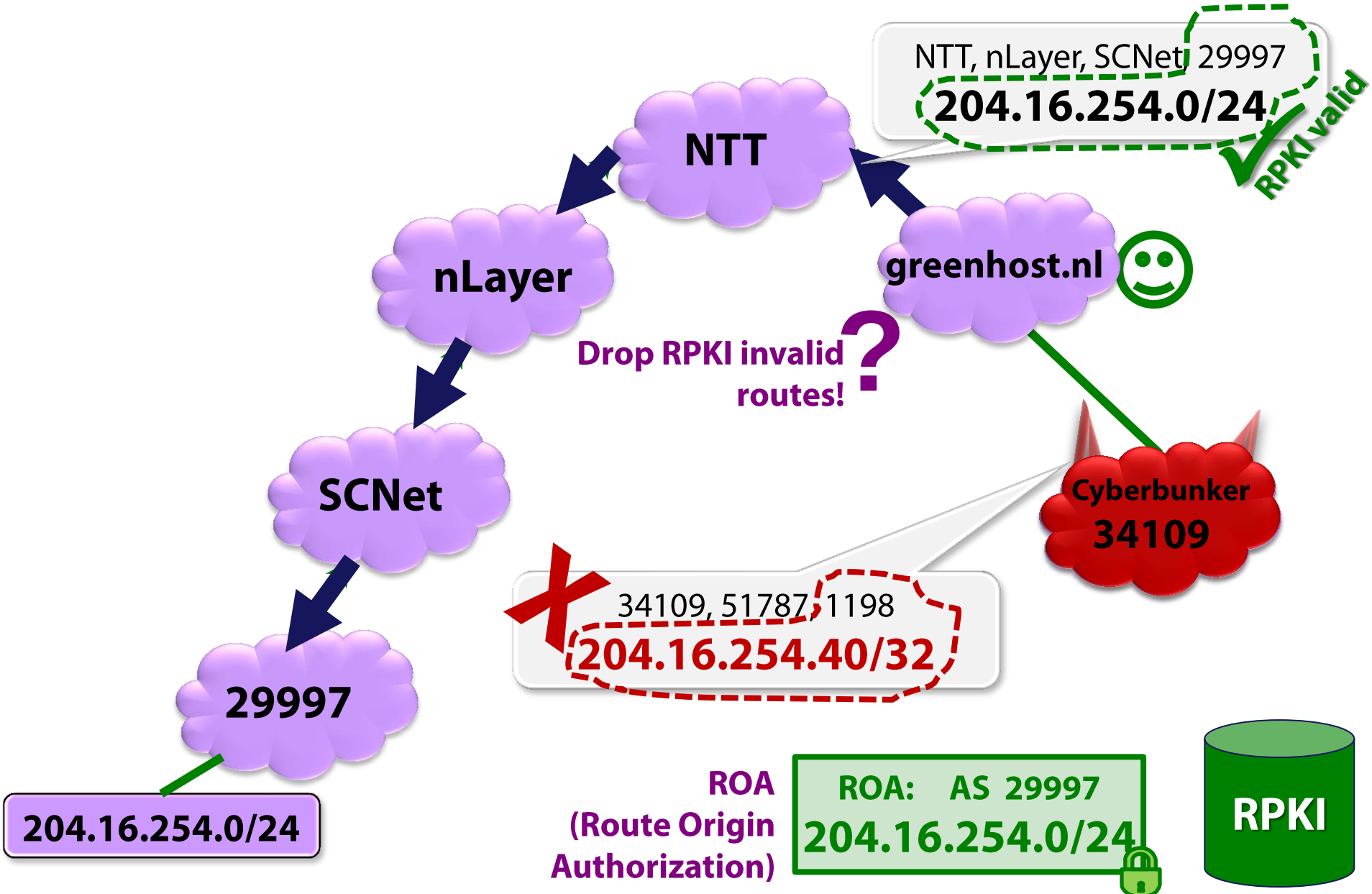
✧ If security is not 1st, protocol downgrade attacks are a serious problem

Part 3: 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

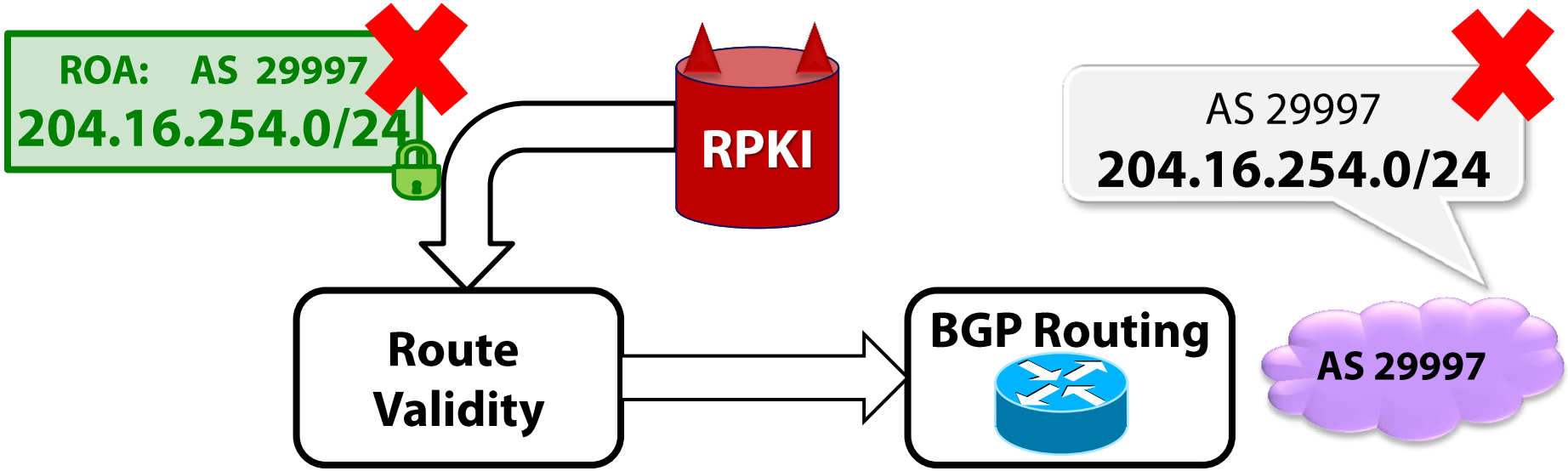


Flipped threat model: What about problems with RPKI?

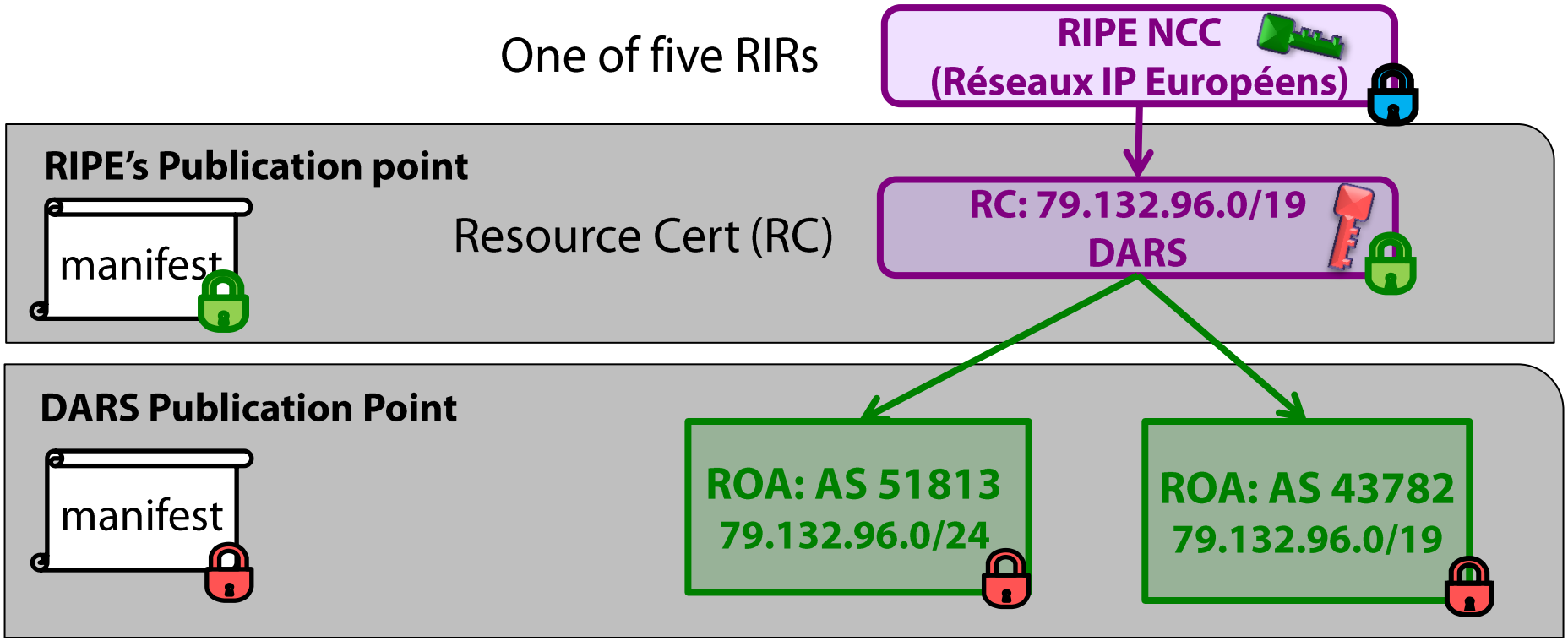
Security audit of the RPKI [HotNets'13]

Misbehaving RPKI authorities can blackhole routes in BGP. Why?

1. RPKI authorities can whack ROAs
2. Whacked ROAs can cause BGP routes to become **invalid**
3. Should drop **invalid** BGP routes to stop **sub**prefix hijacks.



structure of the RPKI [RFC 6480]

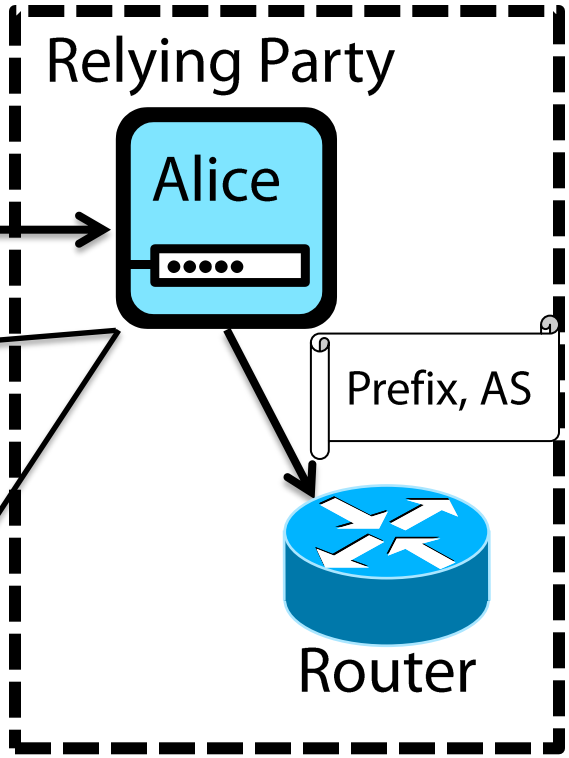


(ROA) Route Origin Authorization

Deployment Status of the RPKI:

- Today: ROAs cover about 6% of interdomain routes.
- Goal: Cover all routes!

how relying parties sync to the RPKI [RFC 6480]

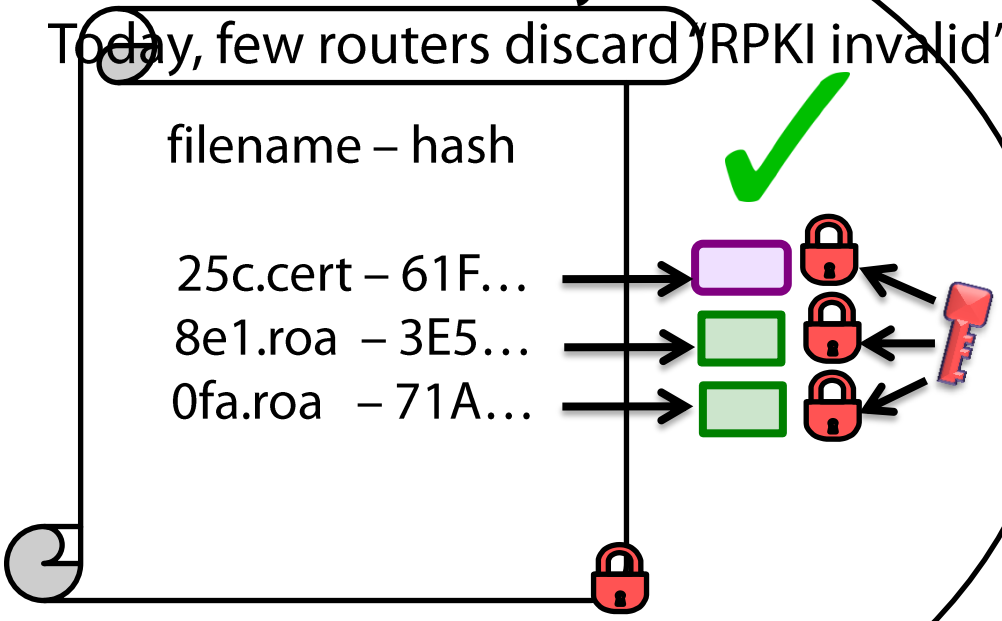


Status of the RPKI today:

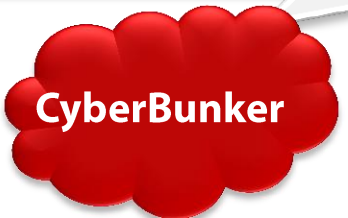
- Today, few routers discard "RPKI invalid" routes

filename – hash

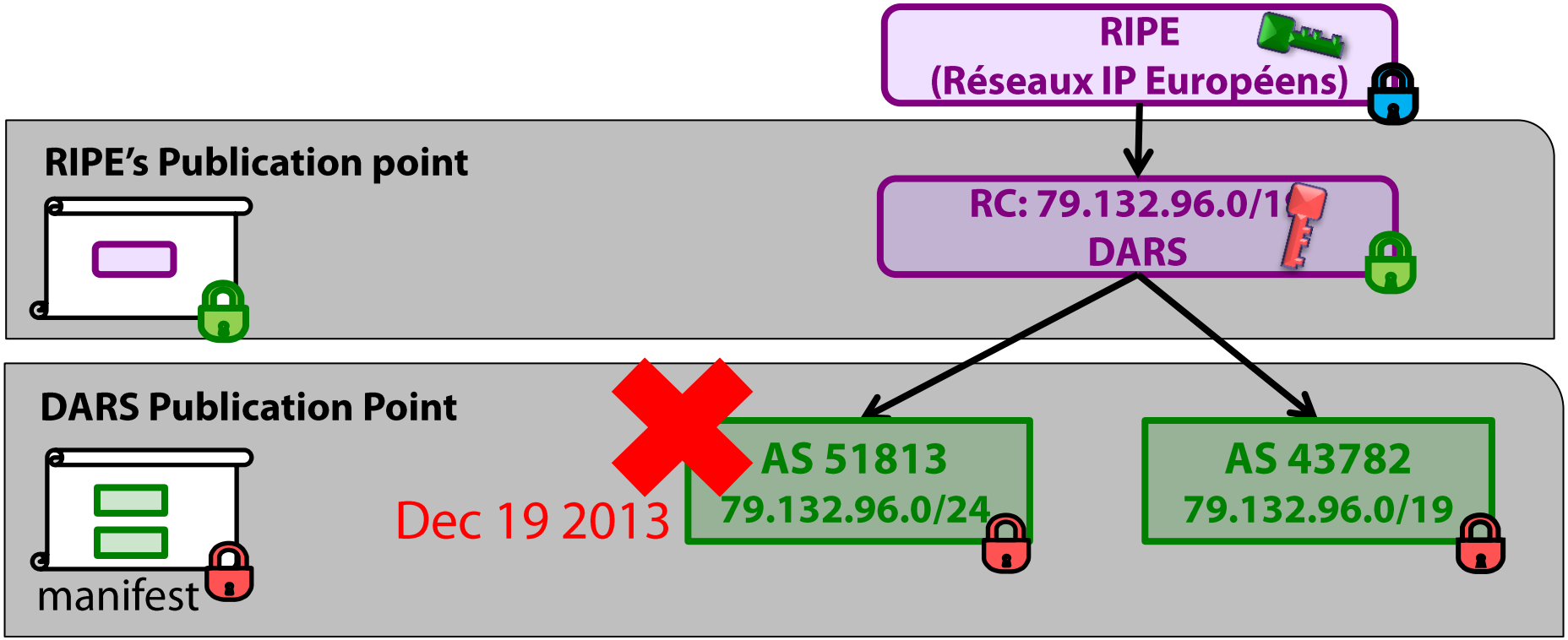
25c.cert – 61F…
8e1.roa – 3E5…
0fa.roa – 71A…



AS 34109
204.16.254.0/32



issue 1: RPKI authorities can unilaterally whack ROAs

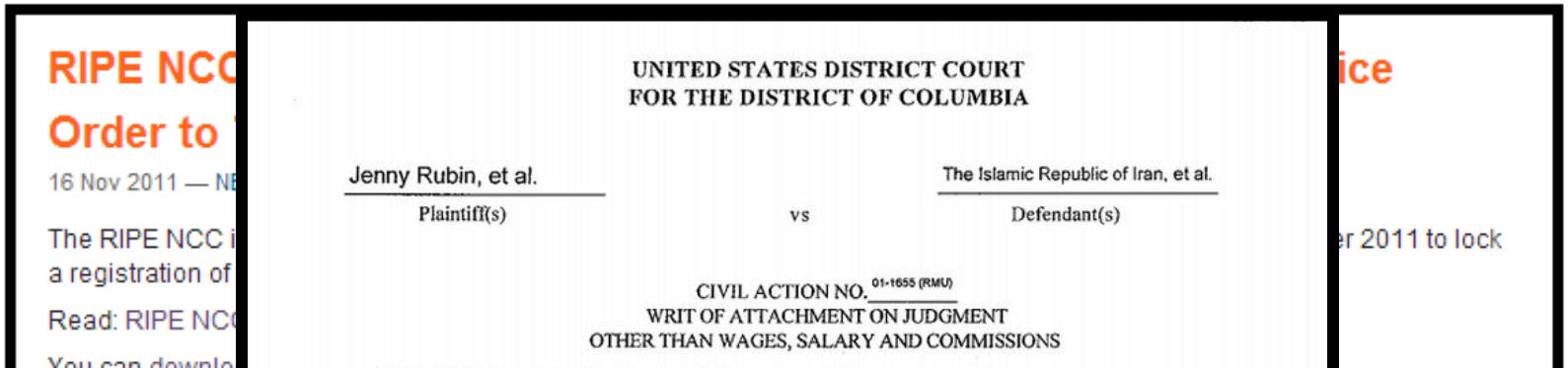


(BTW: Manifest are important!
They detect on-path attackers that delete ROAs!)

IP prefix takedowns by deleting ROAs?

- Prior to the RPKI, authorities could allocate IPs but not revoke them.
- But RPKI authorities **can** revoke IP allocations!
- Creates a risk that the RPKI can be used for unilateral takedowns.
  - Law enforcement? Business disputes? Extortion?
  - The RPKI designed to secure routing, not enable takedowns.
  - **[Mueller-Kuerbis'11, Mueller-Schmidt-Kuerbis'13, Amante'12, FCC'13,…]**

- States seem to want the ability to takedown IP prefixes…
  - Dutch court ordered RIPE to lockdown prefixes registration (Nov'11)
  - US court issued a writ of attachment on Iran's IP prefixes (June'14)
  - IP allocation does not reflect jurisdiction.


RIPE NCC
Order to
16 Nov 2011 — NE
The RIPE NCC i
a registration of
Read: RIPE NC

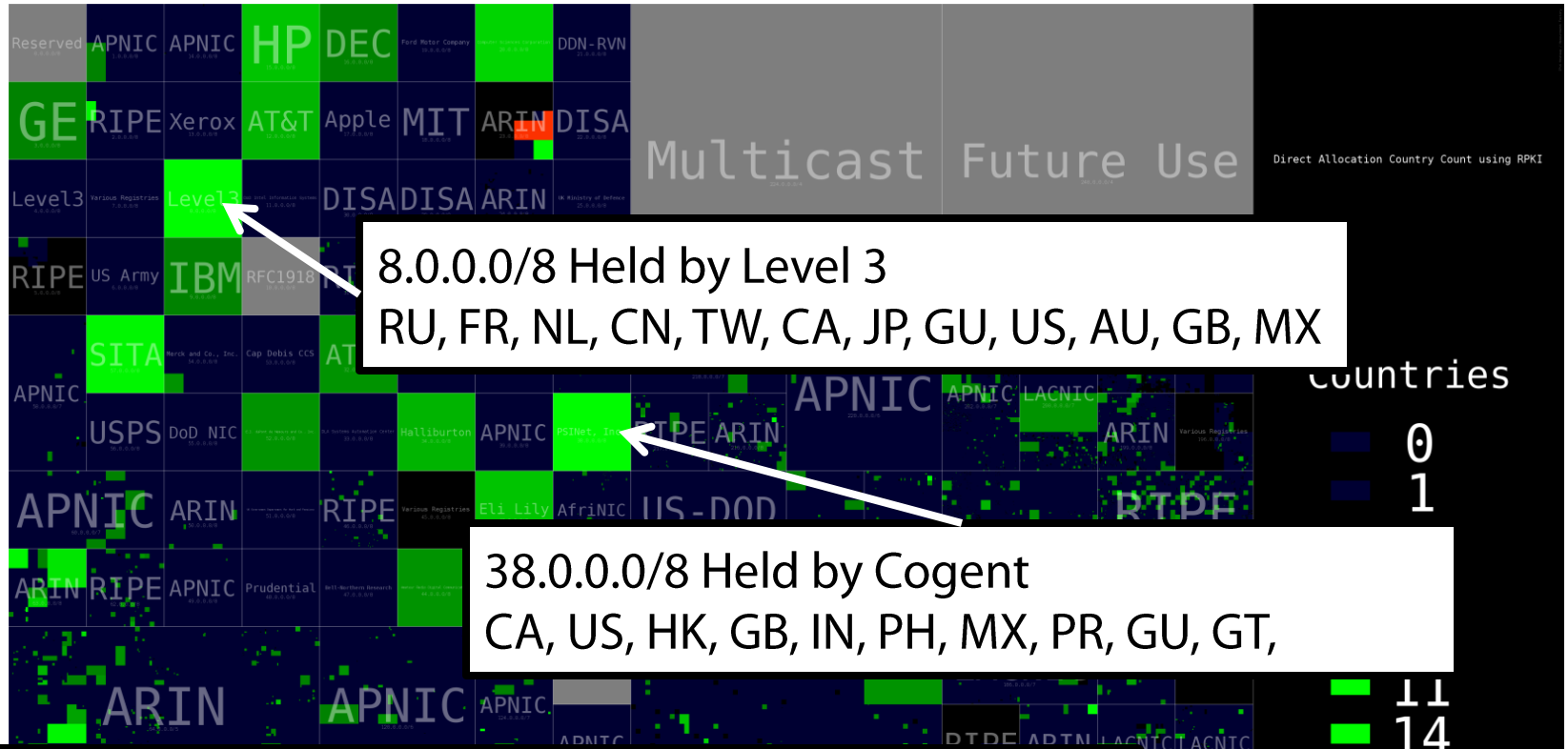
UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Jenny Rubin, et al. — Plaintiff(s)
vs
The Islamic Republic of Iran, et al. — Defendant(s)

CIVIL ACTION NO. 01-1655 (RMU)
WRIT OF ATTACHMENT ON JUDGMENT
OTHER THAN WAGES, SALARY AND COMMISSIONS

ice
er 2011 to lock

IP address allocation does not always reflect jurisdiction



8.0.0.0/8 Held by Level 3
RU, FR, NL, CN, TW, CA, JP, GU, US, AU, GB, MX

38.0.0.0/8 Held by Cogent
CA, US, HK, GB, IN, PH, MX, PR, GU, GT,

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

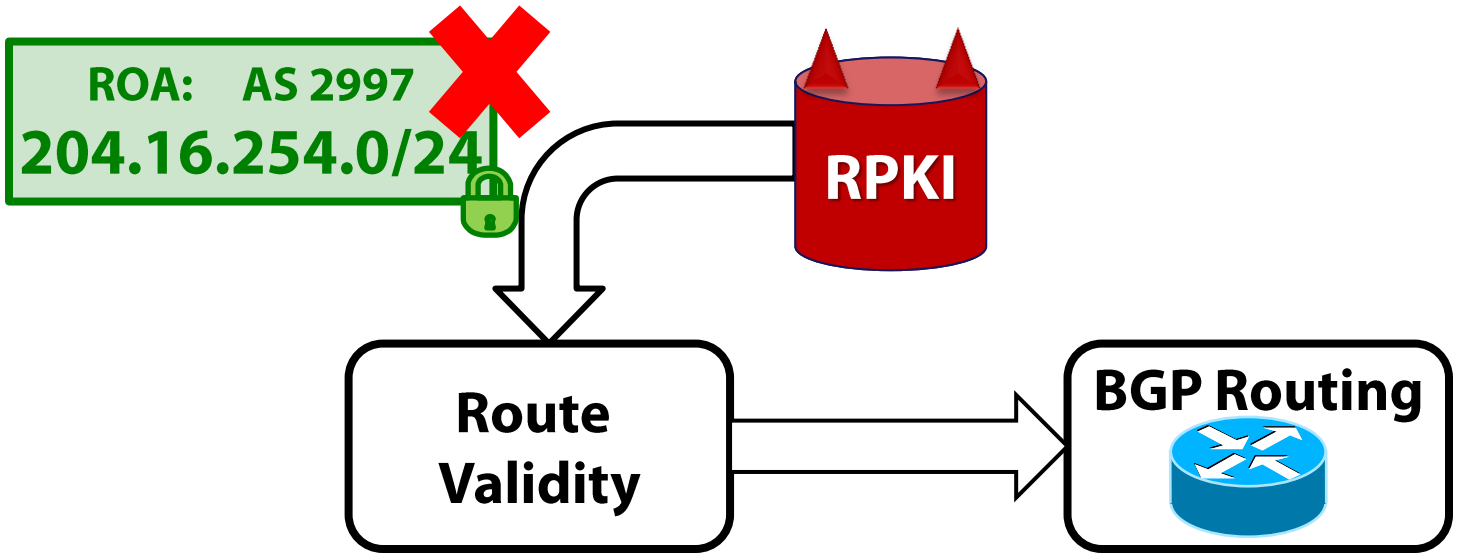
- ✧ Using RIR direct allocations, routeviews, BGP table dumps
- ✧ RIRs and their direct allocations get RCs, other (prefix,origin AS) pairs in the table dumps get a ROA
- ✧ ASes mapped to countries using RIR data

RPKI issues

Security audit of the RPKI [HotNets'13]

Misbehaving RPKI authorities can blackhole routes in BGP. Why?

1. RPKI authorities can whack ROAs
2. Whacked ROAs can cause BGP routes to become **invalid**



issue 2: whacked ROAs can cause BGP routes to be invalid

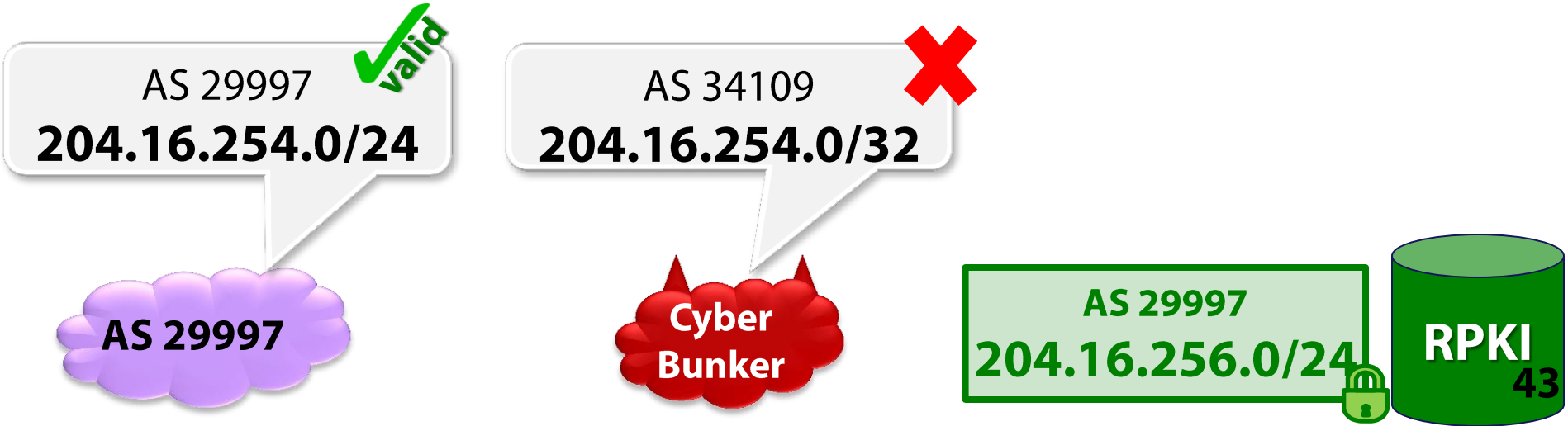
valid BGP route

invalid BGP route

unknown BGP route ← "World before RPKI"

Reality: interdependent validity outcomes

valid ROA → valid BGP route | invalid subroutes!



issue 2: whacked ROAs can cause BGP routes to be invalid

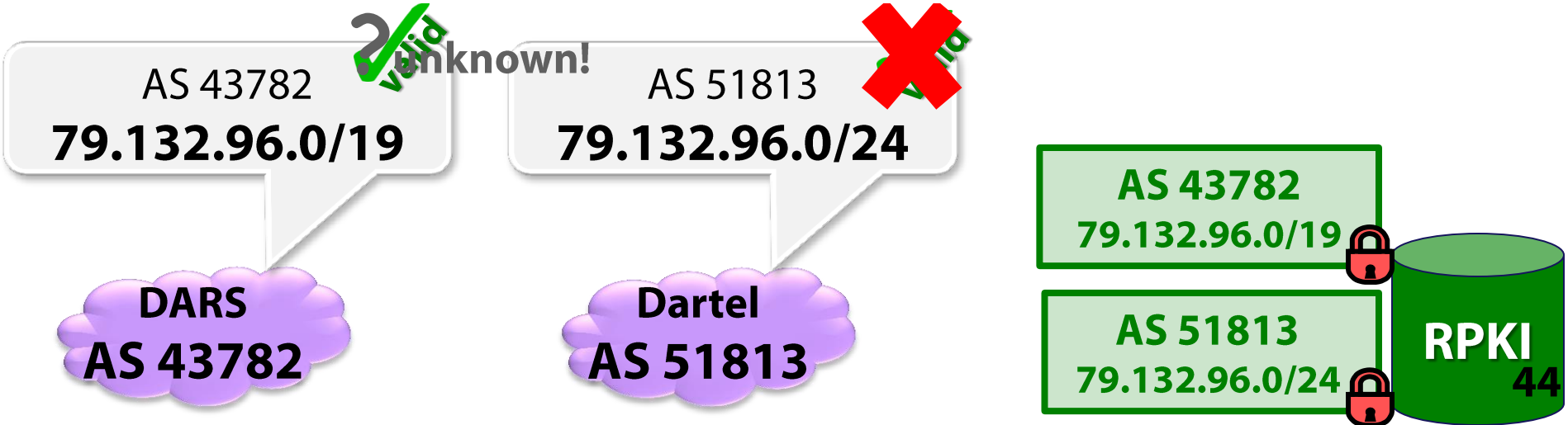
valid BGP route

invalid BGP route

unknown BGP route ← "World before RPKI"

Reality: interdependent validity outcomes

valid ROA → valid BGP route | invalid subroutes!

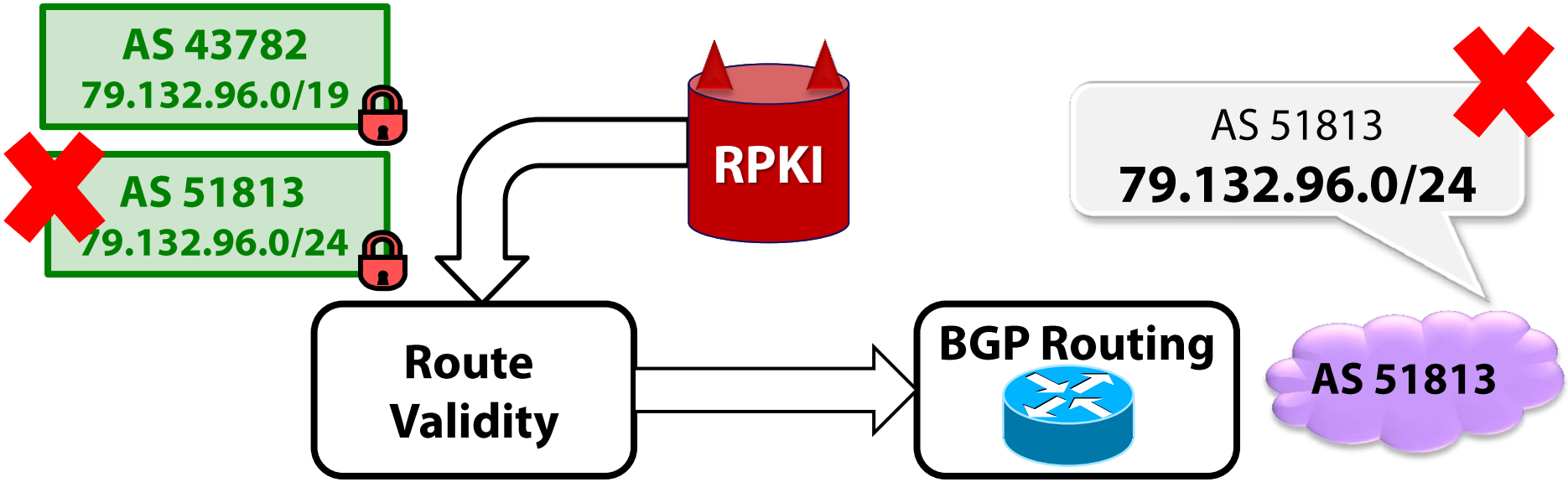


RPKI issues

- **Security audit of the RPKI [HotNets'13]**

  Misbehaving RPKI authorities can blackhole routes in BGP. Why?

  1. RPKI authorities can whack ROAs
  2. Whacked ROAs can cause BGP routes to become **invalid**
  3. Should drop **invalid** BGP routes to stop **sub**prefix hijacks.



- **Proposal to require consent for whacked objects [SIGCOMM'14]**
  - There is a draft for similar proposal: **[draft-kent-sidr-suspenders-02]**

summary & future work

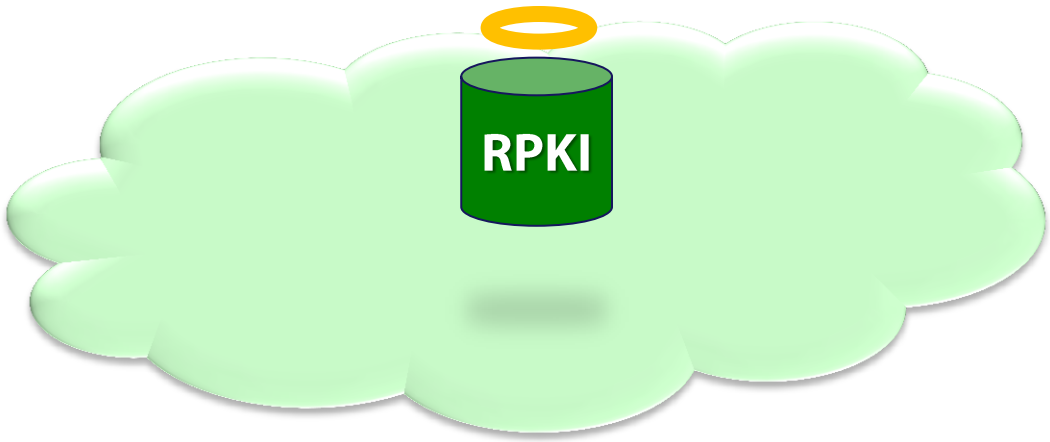
RPKI is the most crucial step in terms of security

- 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!



http://www.cs.bu.edu/~goldbe

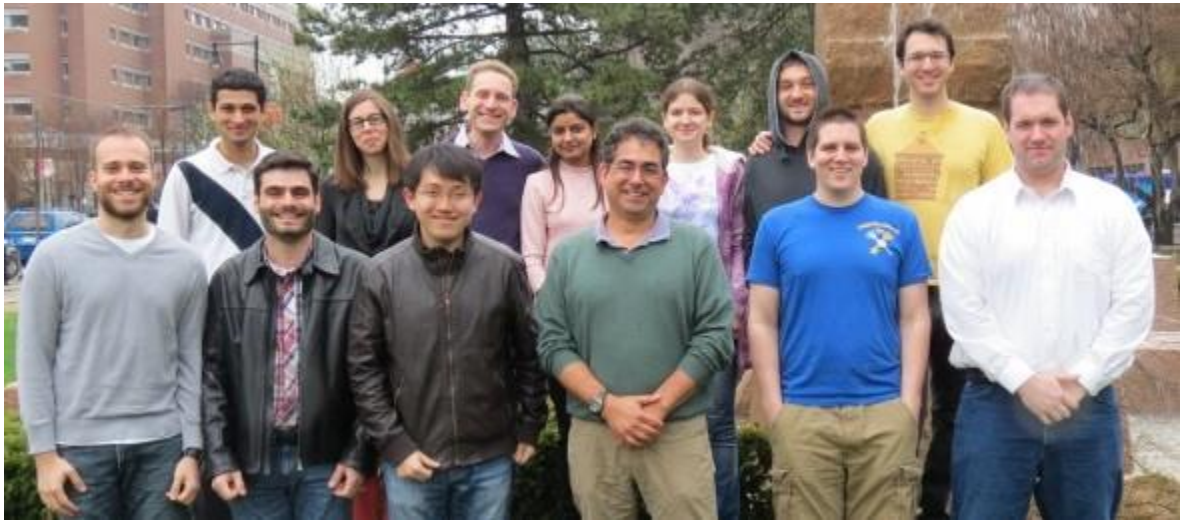
phds, postdocs with BUSEC at Boston University

Faculty

Canetti Goldberg Reyzin

We have funding for PhDs and postdocs in network security, cryptocurrencies and cryptography

Group (circa 2014)



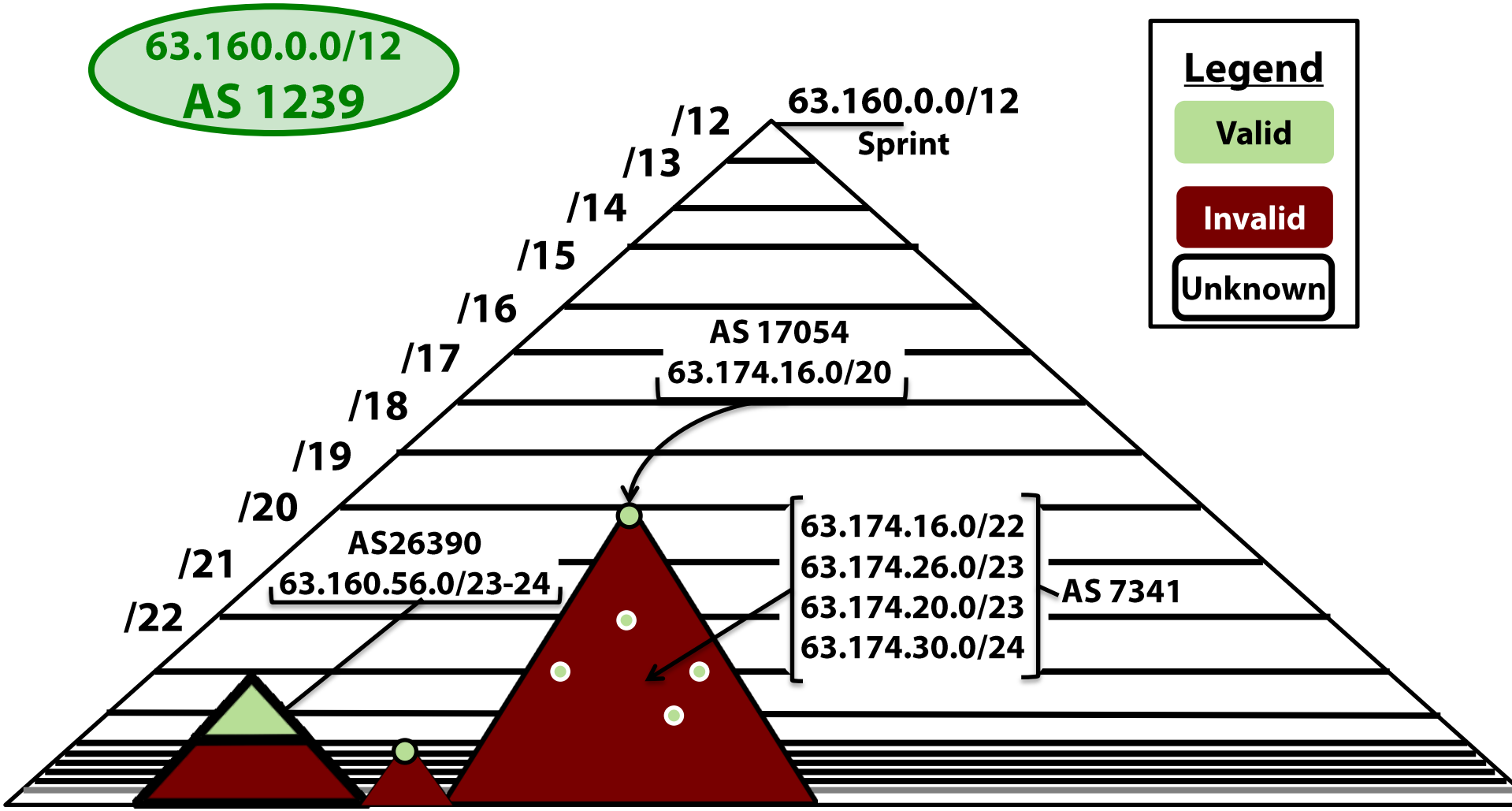
BOSTON UNIVERSITY

http://www.bu.edu/cs/busec/

goldbe@cs.bu.edu

Validity of routes for subprefixes of 63.160.0.0/12

What if Sprints adds a ROA?



Validity of routes for subprefixes of 63.160.0.0/12

What if Sprints adds a ROA?