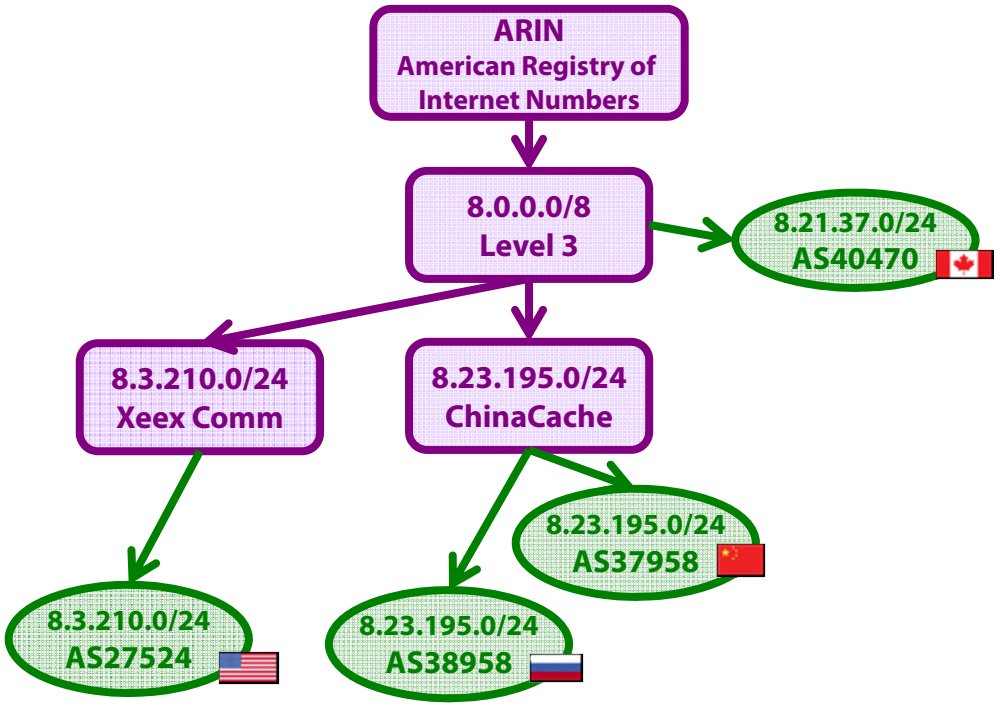
Impacting IP Address Reachability via RPKI Manipulations



Danny Cooper

Kyle Brogle Ethan Heilman Sharon Goldberg Leonid Reyzin

Boston University

The RPKI

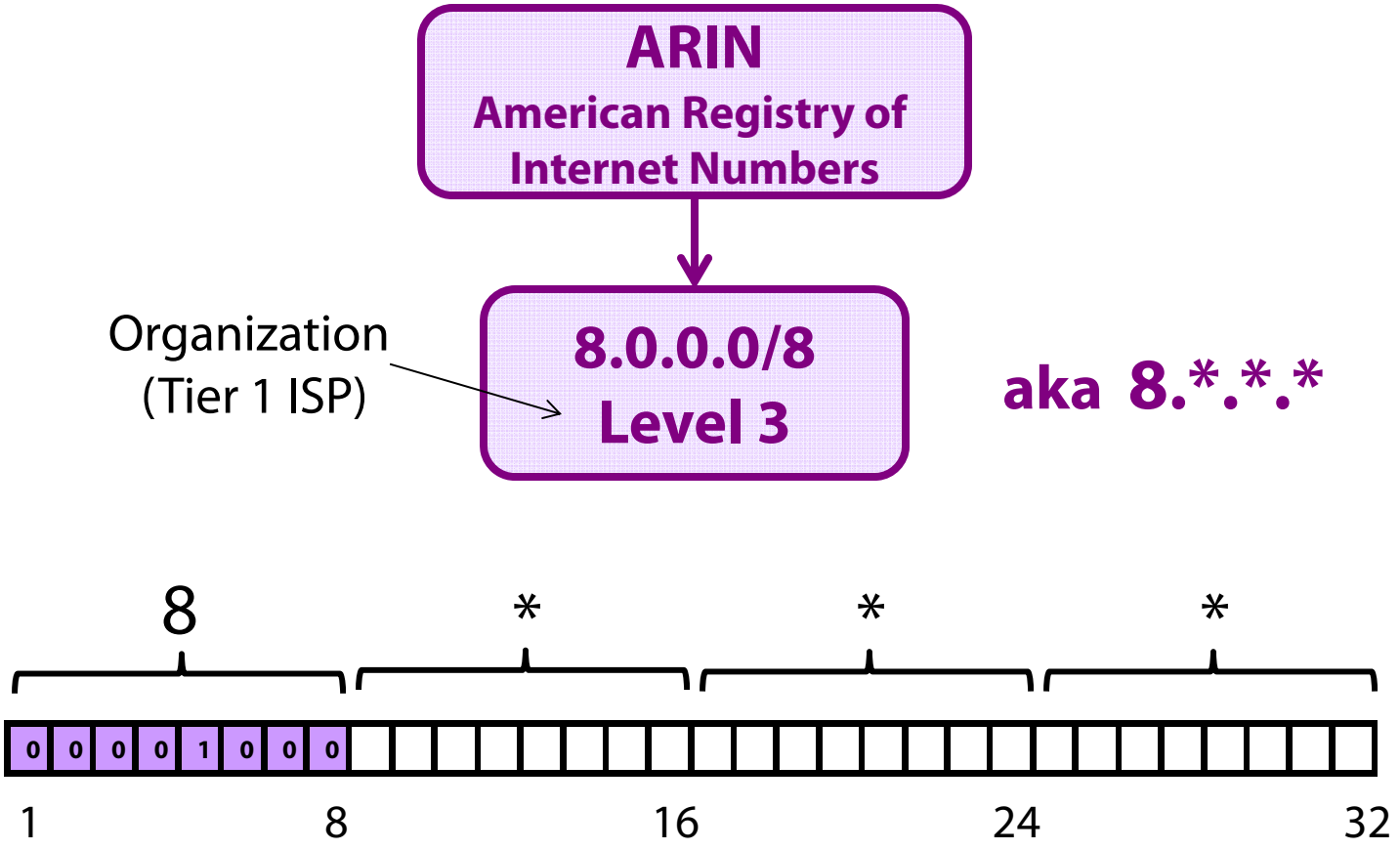
(Resource Public Key Infrastructure)

is a new infrastructure to secure Internet routing

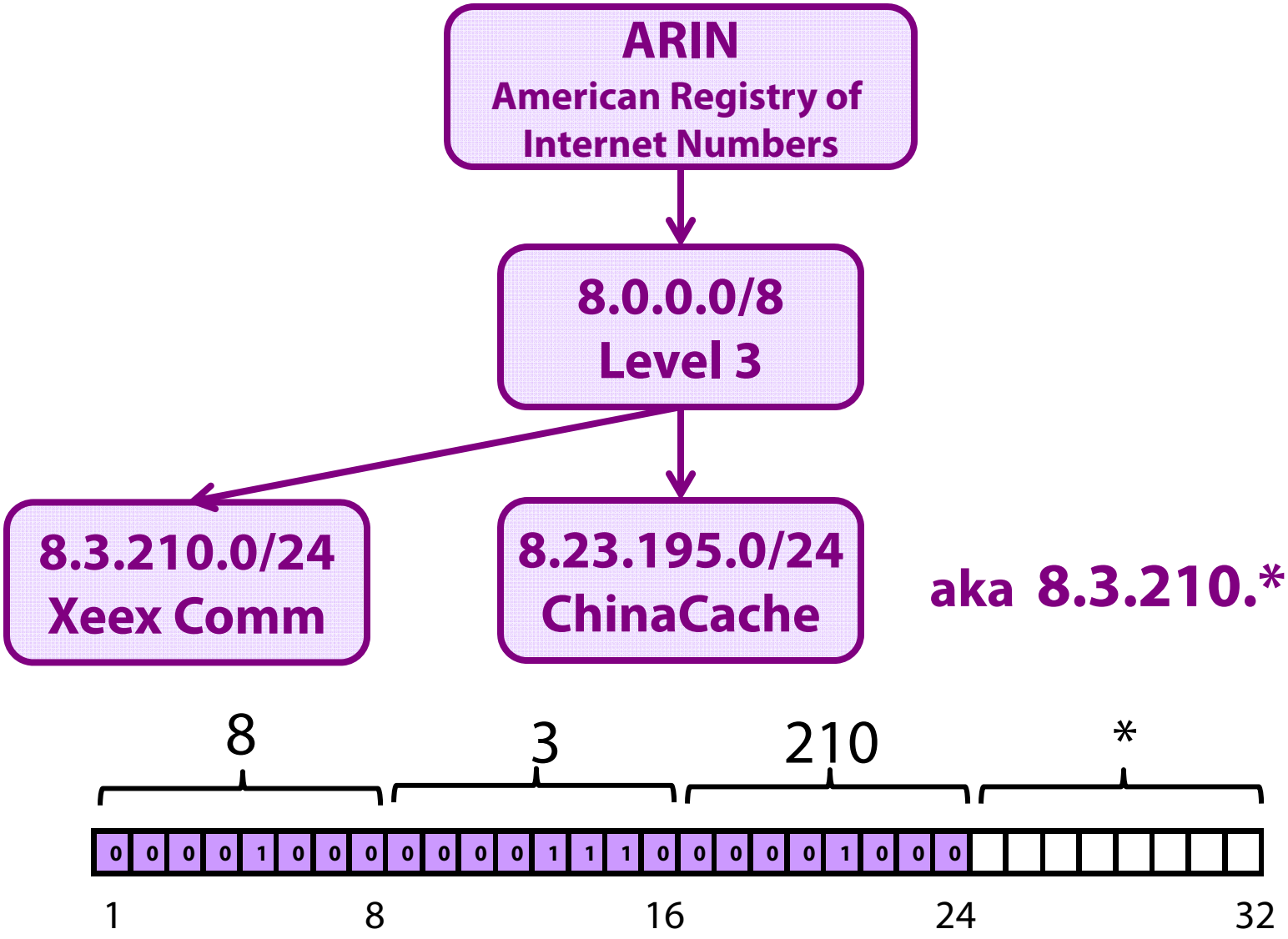
It's been in deployment since ~2011

But, it also creates new risks
(misconfigurations and takedowns)
that could make IP prefixes unreachable

the IP address allocation hierarchy (1)

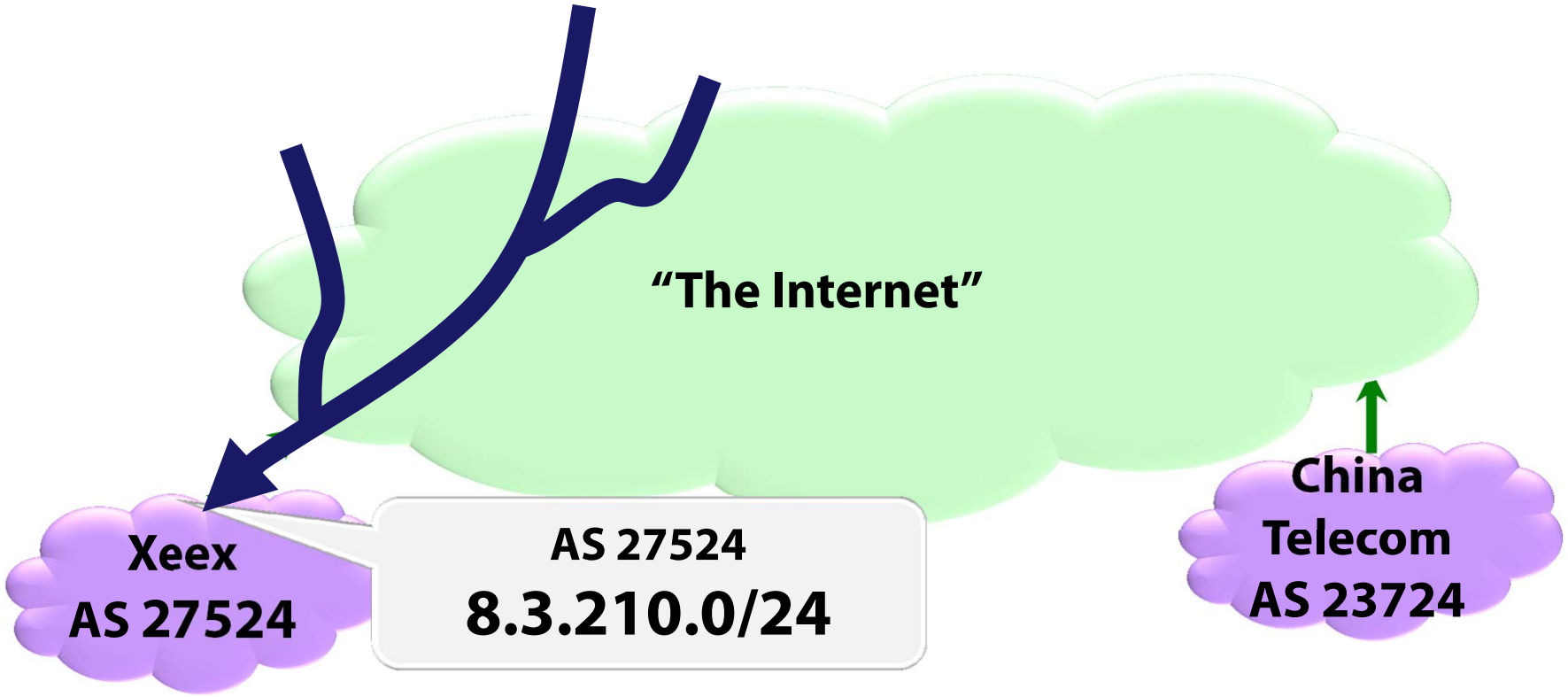


the IP address allocation hierarchy (2)



Internet routing security

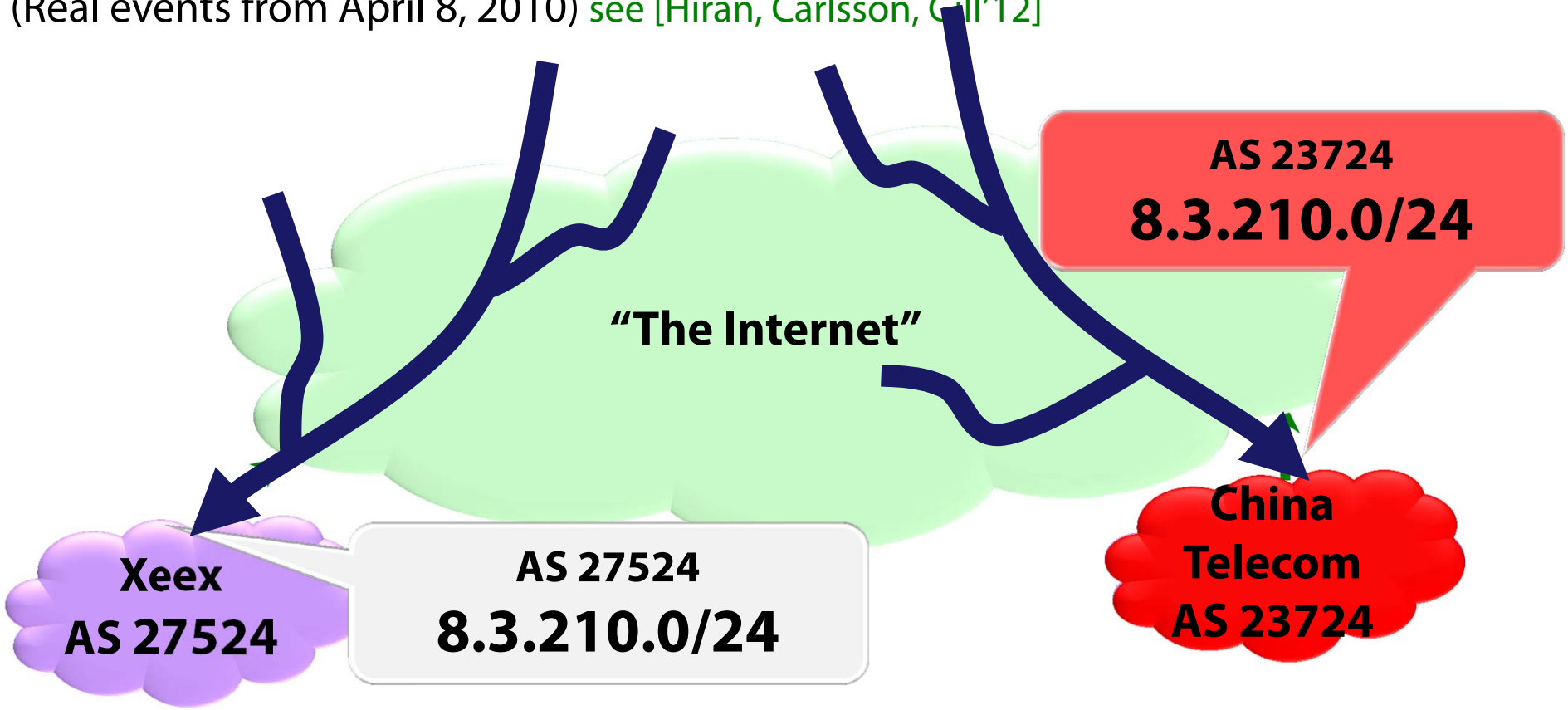
(Real events from April 8, 2010) see [Hiran, Carlsson, Gill'12]



The internet is a graph. Each node is an AS (autonomous system), with an identifying AS Number.
Organizations can have more than one AS Number.

Internet routing security

(Real events from April 8, 2010) see [Hiran, Carlsson, Gill'12]

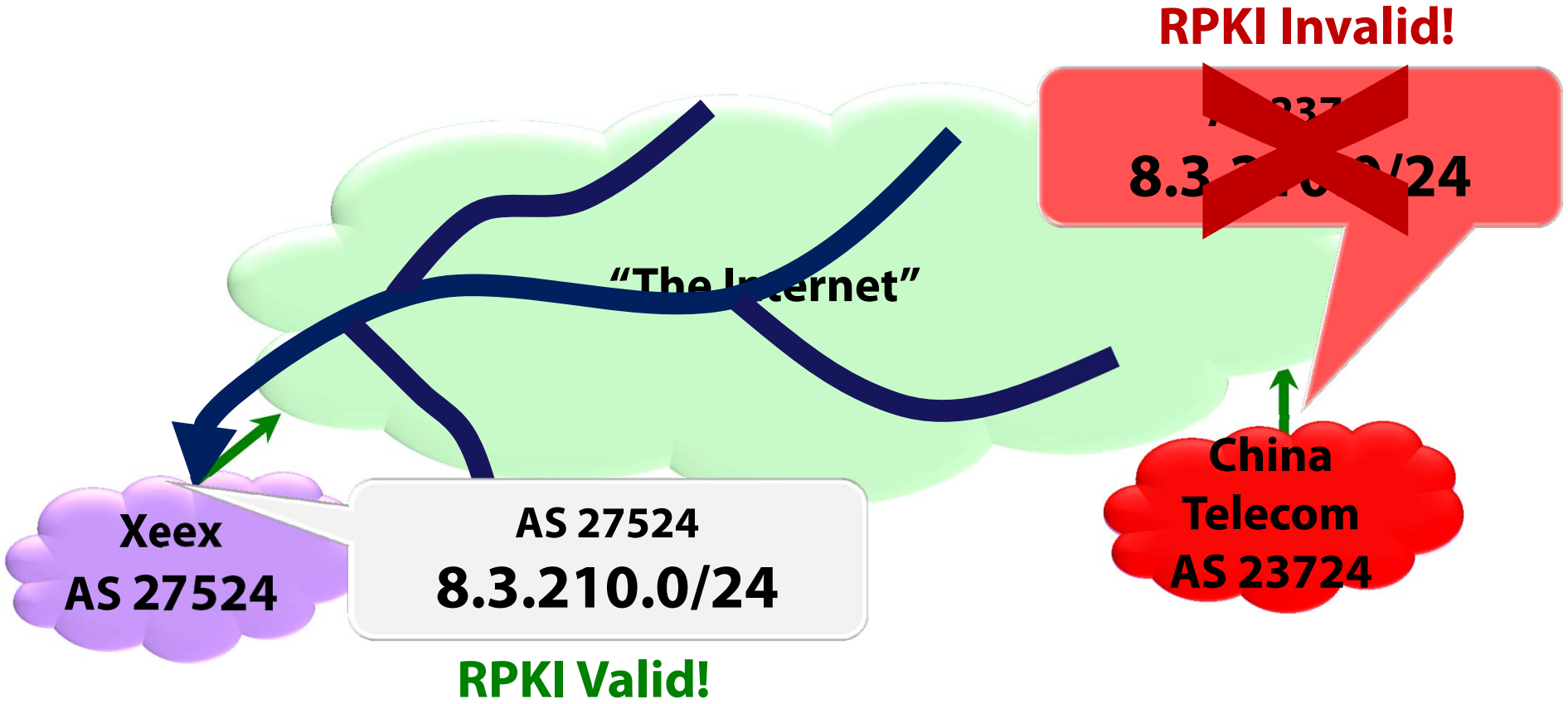


A prefix hijack:

Traffic for 8.3.210.0/24 splits between Xeex and China Telecom

the fix: use RPKI as part of routing policies

RPKI has been in deployment since ~ 2011

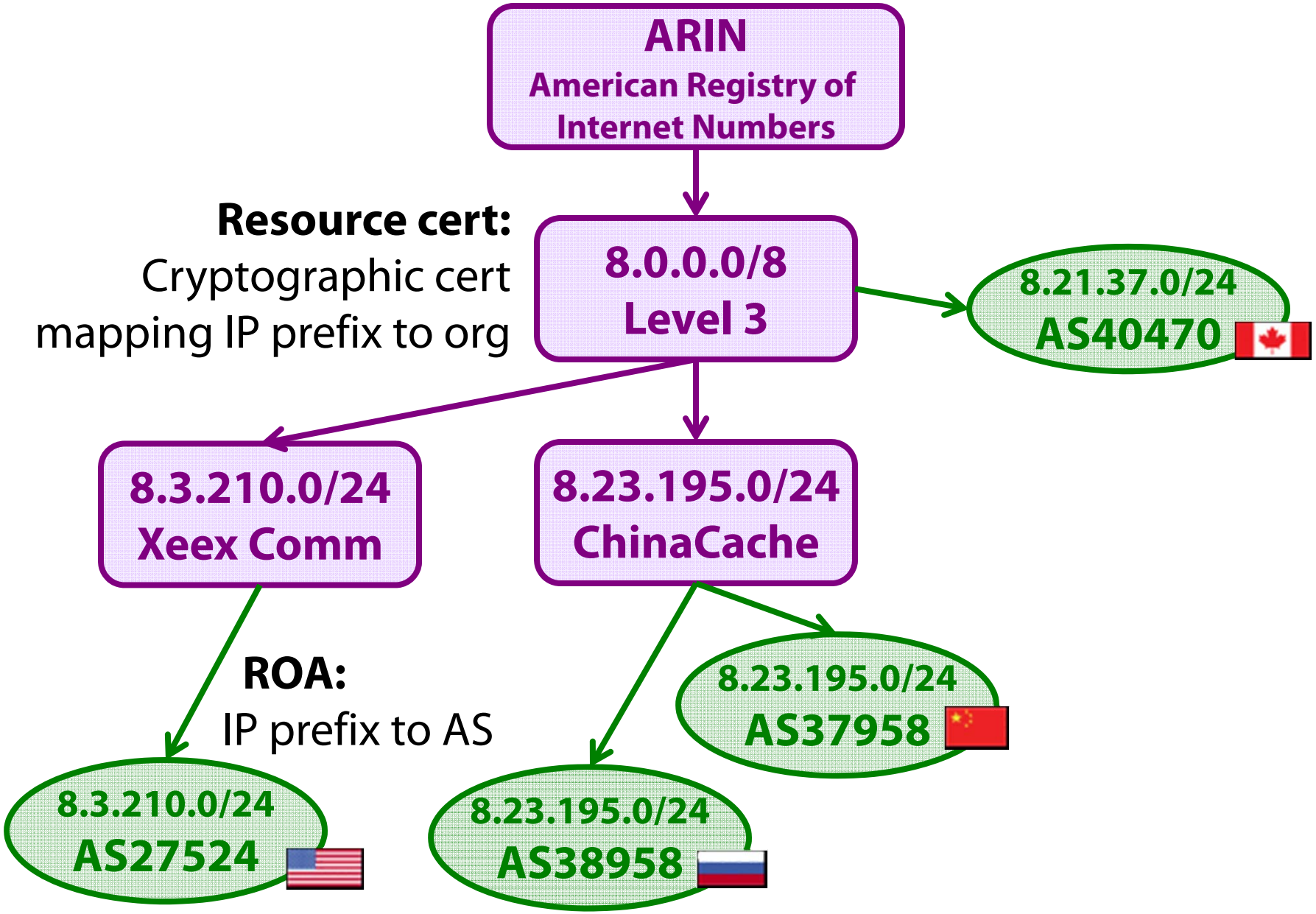


RPKI

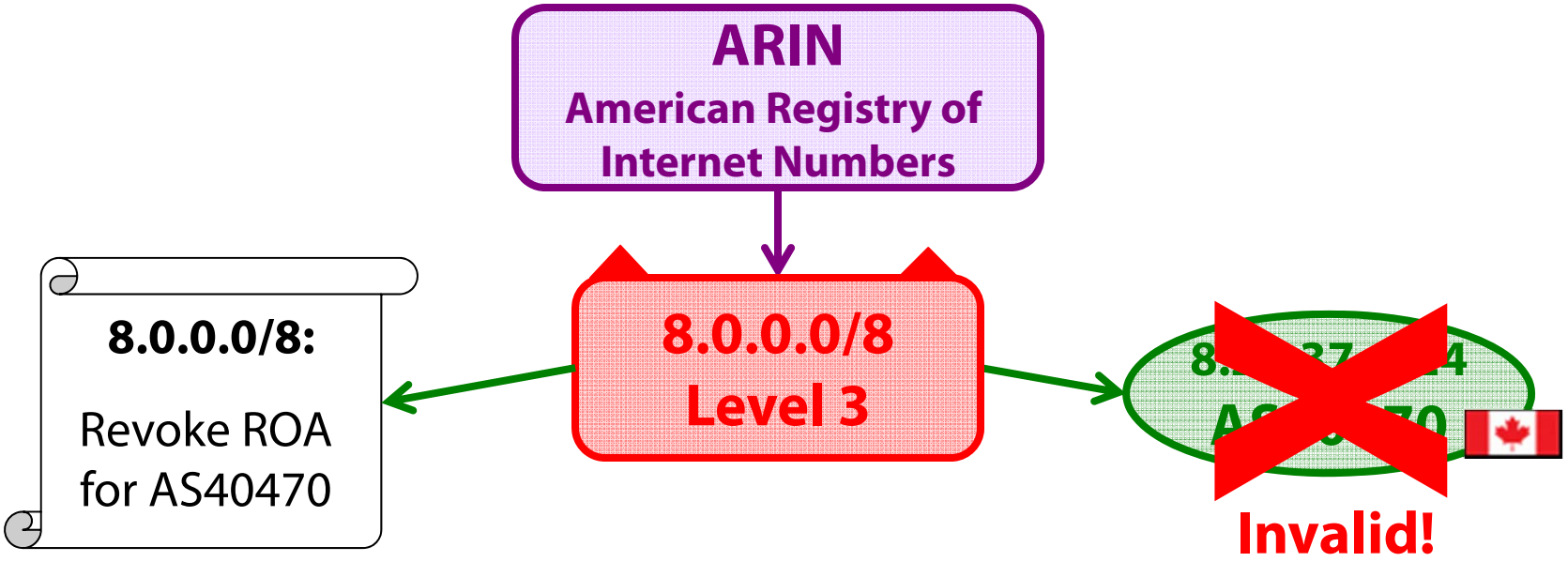
ROA: "AS 27524 is authorized to announce 8.3.210.0/24"

Importantly, RPKI validity must impact routing decisions.

the RPKI: a cryptographic certificate hierarchy



new infrastructure = new attack vector



Anyone with a ROA is vulnerable to revocation…

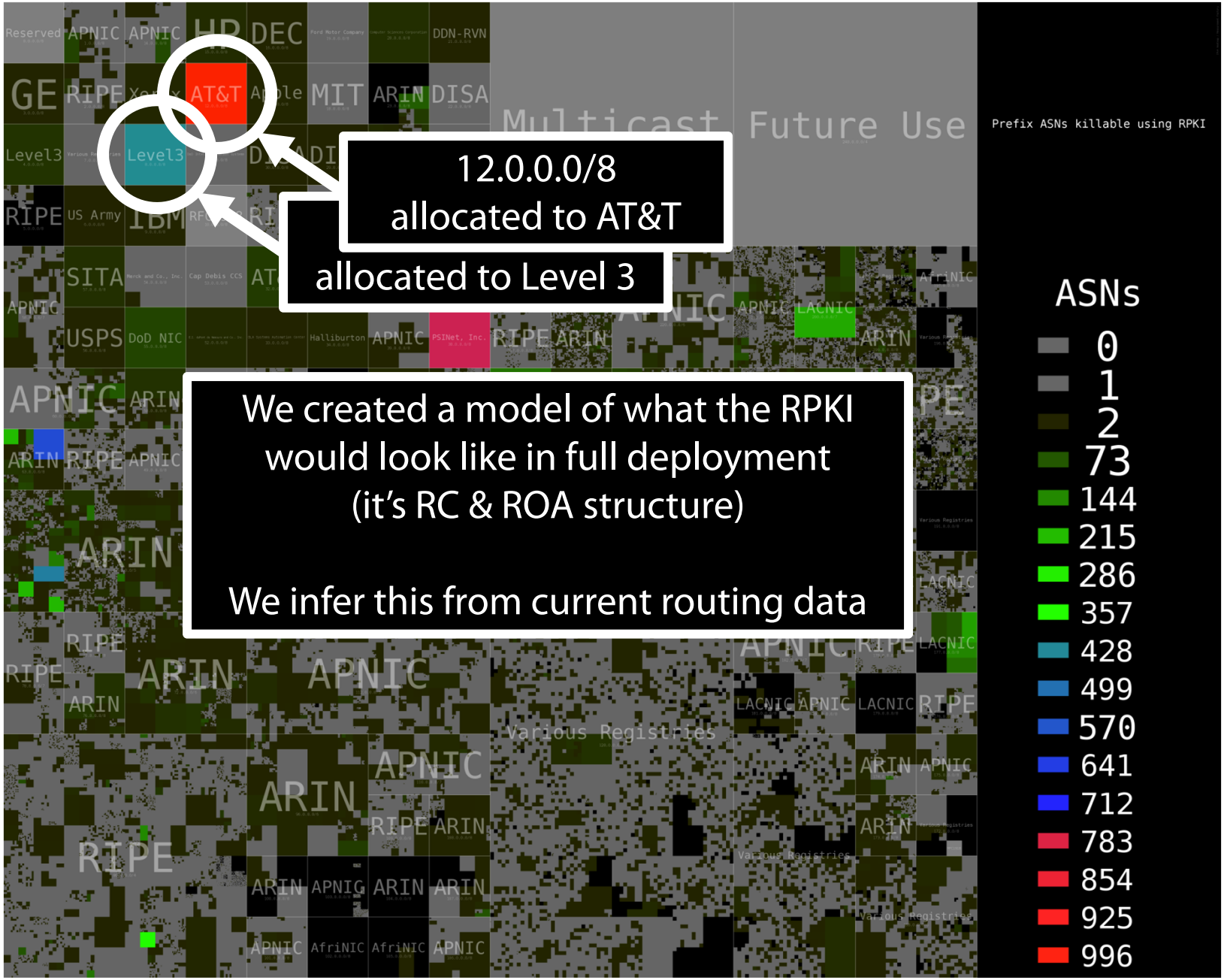
(and we show that revocation is possible
by any entity higher up in the RPKI hierarchy)

Power concentrates in entities at the top of the RPKI hierarchy

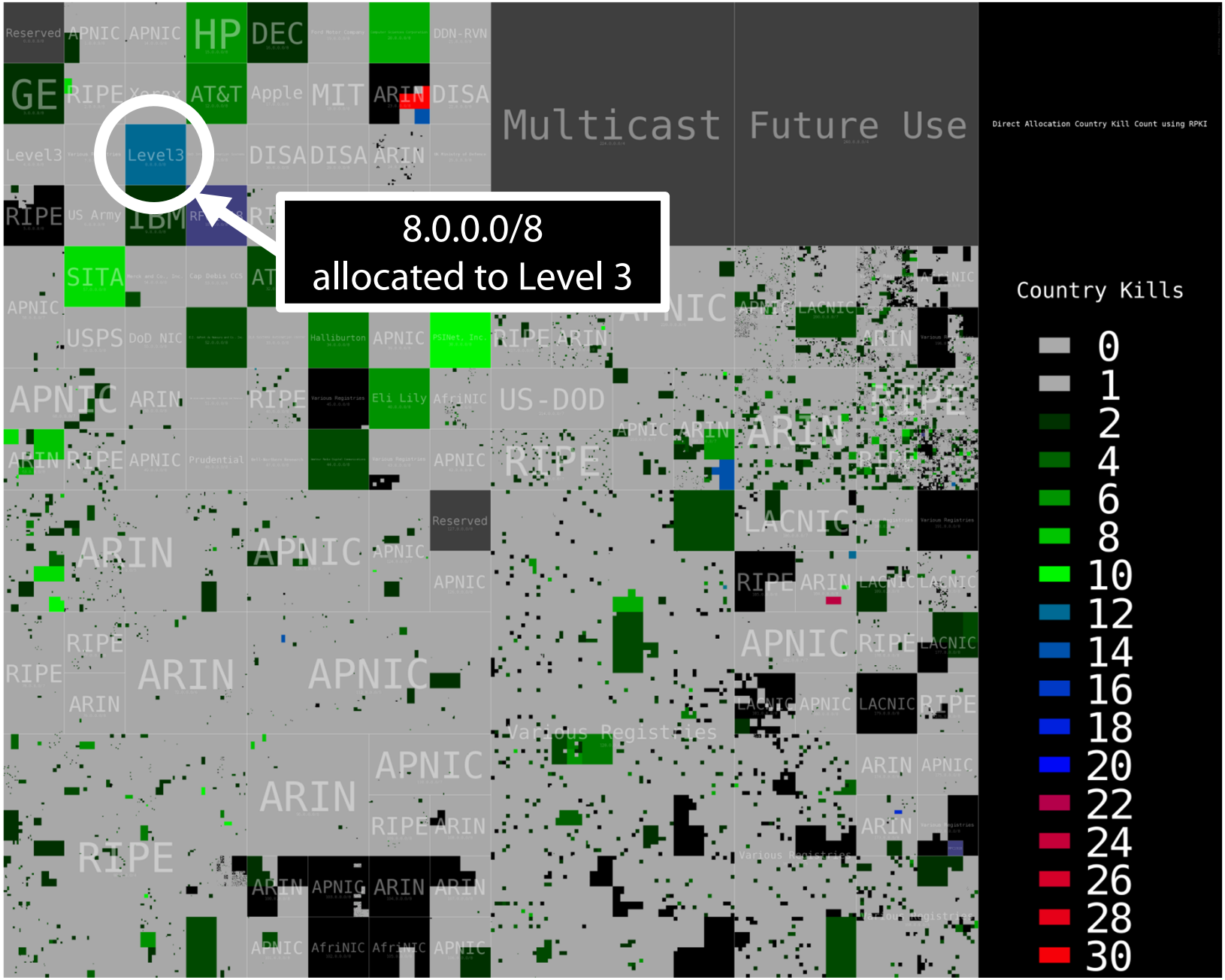
(potential for misconfigs, malice or takedowns?)

(This Level 3 cert can invalidate ROAs for 400 ASes in 16 countries)

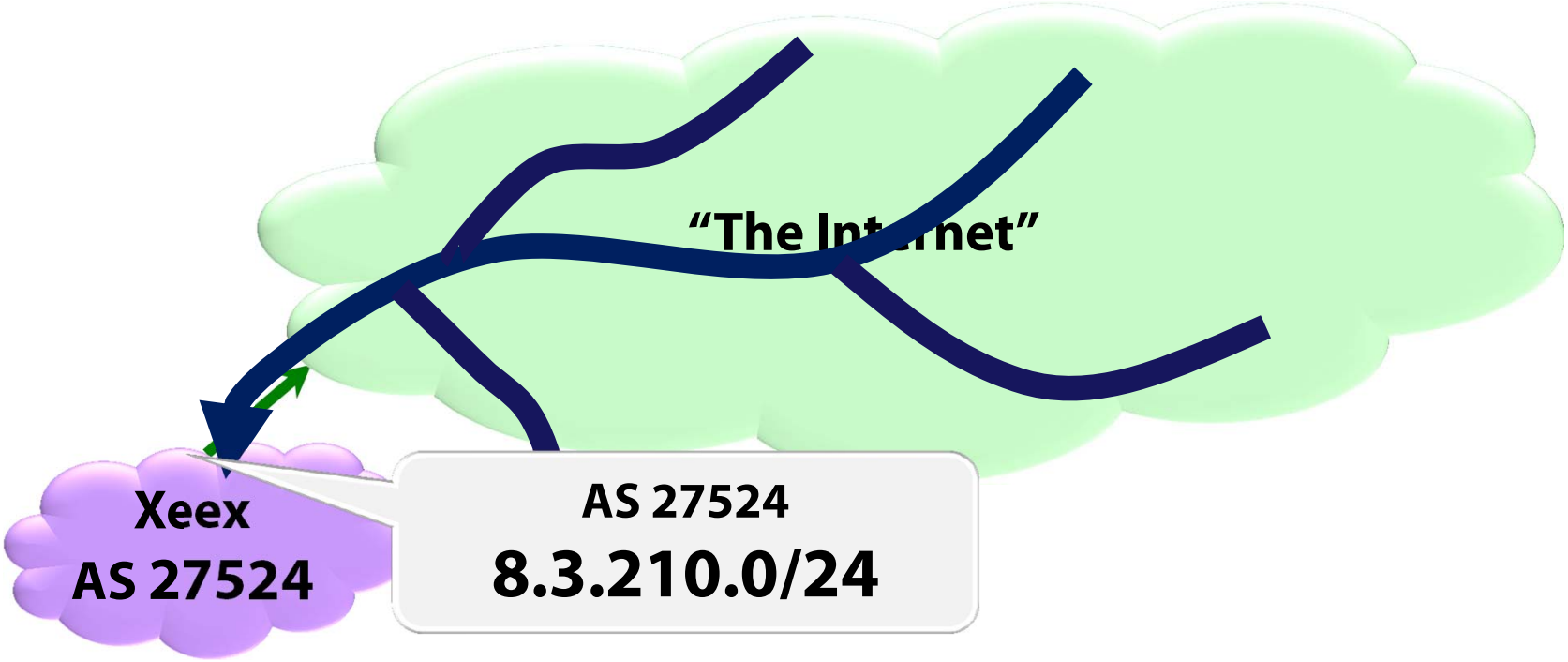
One organization can invalidate ROAs for many ASes…



… in many countries!

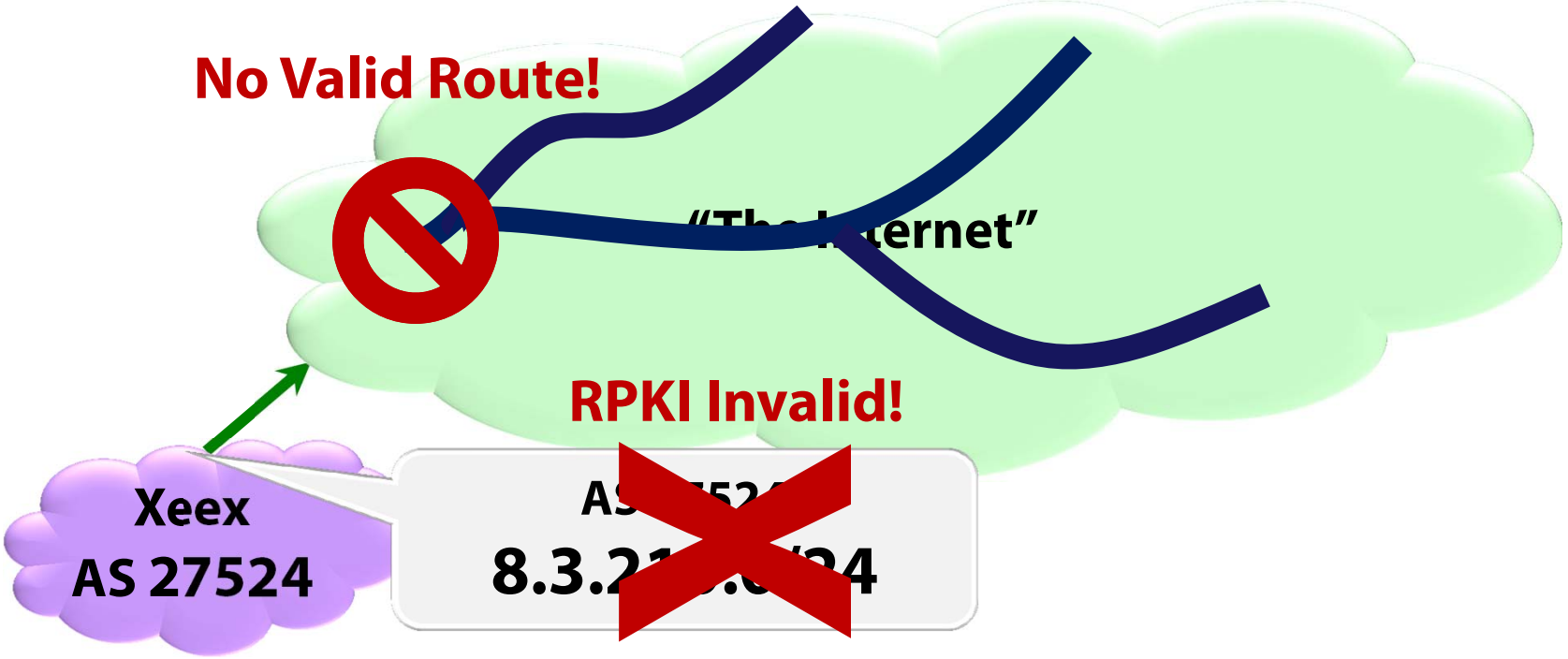


impact of different routing policies



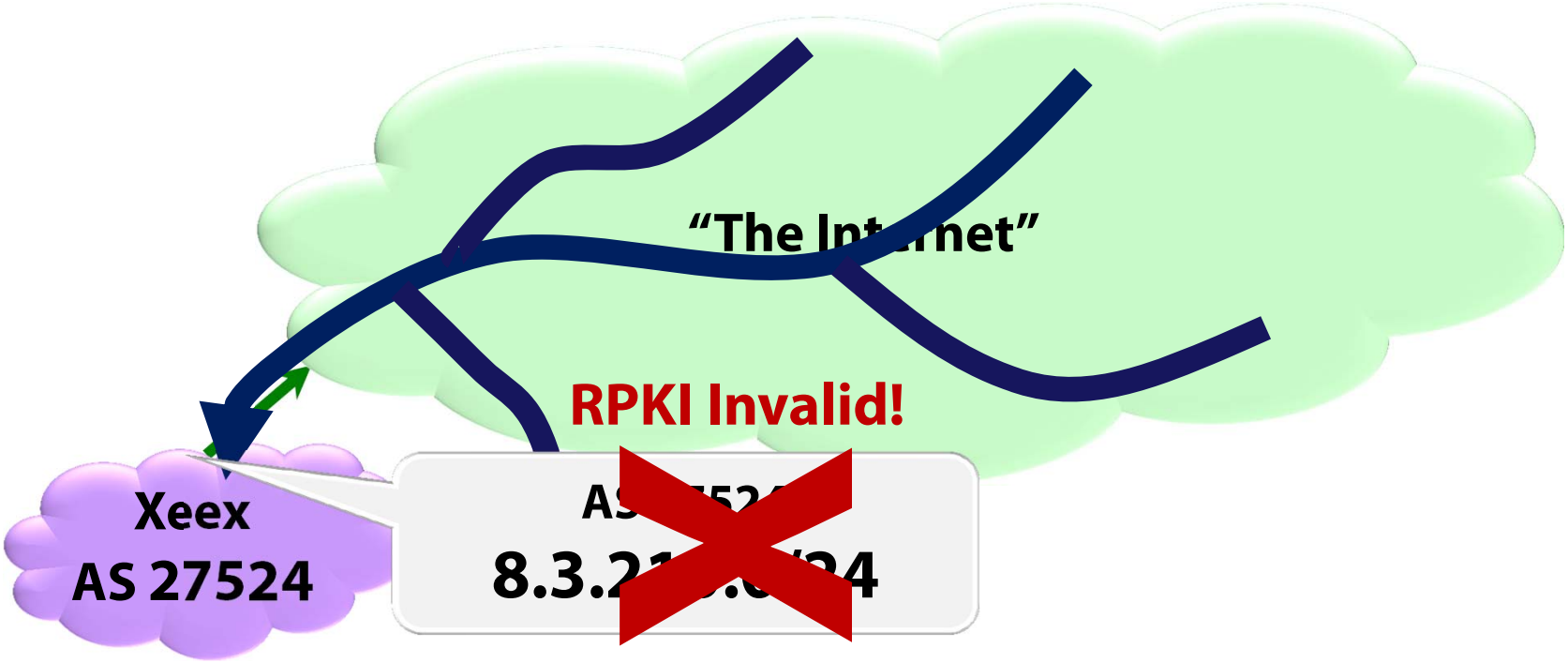
Routing policy:	Prefix remains reachable …	
	during routing hijack	during RPKI manipulation
Drop Invalid	✓	

impact of different routing policies



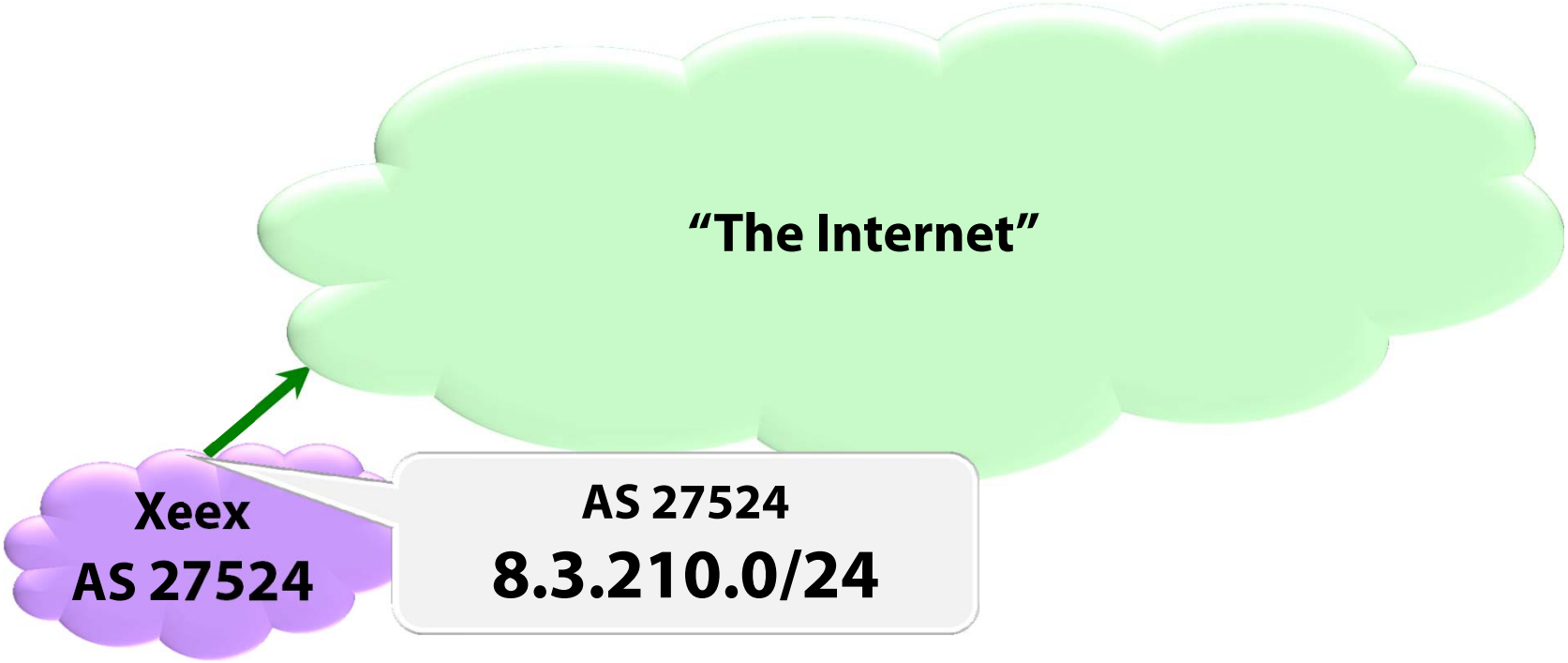
Routing policy:	Prefix remains reachable …	
	during routing hijack	during RPKI manipulation
Drop Invalid	✓	X

impact of different routing policies



Routing policy:	Prefix remains reachable …	
	during routing hijack	during RPKI manipulation
Drop Invalid	✓	X
Depreference invalid		✓

impact of different routing policies



Routing policy:	Prefix remains reachable …	
	during routing hijack	during RPKI manipulation
Drop Invalid	✓	X
Depreference invalid	Subprefix hijacks possible	✓

Our current focus:

Can we prevent routing attacks
without
introducing a new attack vector through the RPKI?

Anomaly detection for RPKI
To detect "suspicious" refactoring of the RPKI
and prevent it from impacting routing.

Full Report: **http://www.cs.bu.edu/~goldbe/papers/RPKImanip.html**