Fourteen Years in the Life:

A Root Server's Perspective on DNS Resolver Security

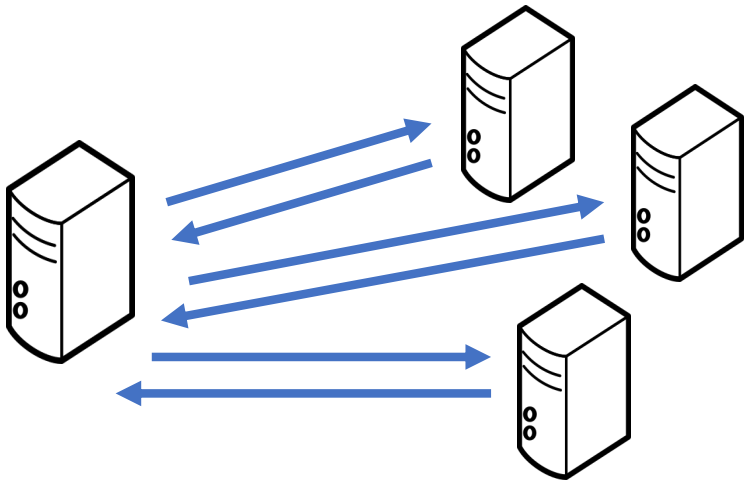
Alden Hilton*, **Casey Deccio****, Jacob Davis*

Sandia National Laboratories*, Brigham Young University**

OARC 39

Prior Research – Source Port Randomization

- **Problem:** In 2019 we analyzed source port randomization of DNS resolvers.
- **Method:** Analysis was based on comparing source ports from 10 unique resolver-to-authoritative queries induced by direct queries.
- **Result:** In 6% of ASes, we found at least one resolver lacking source port randomization.



Question – How to Expand Our Analysis?

Research Questions

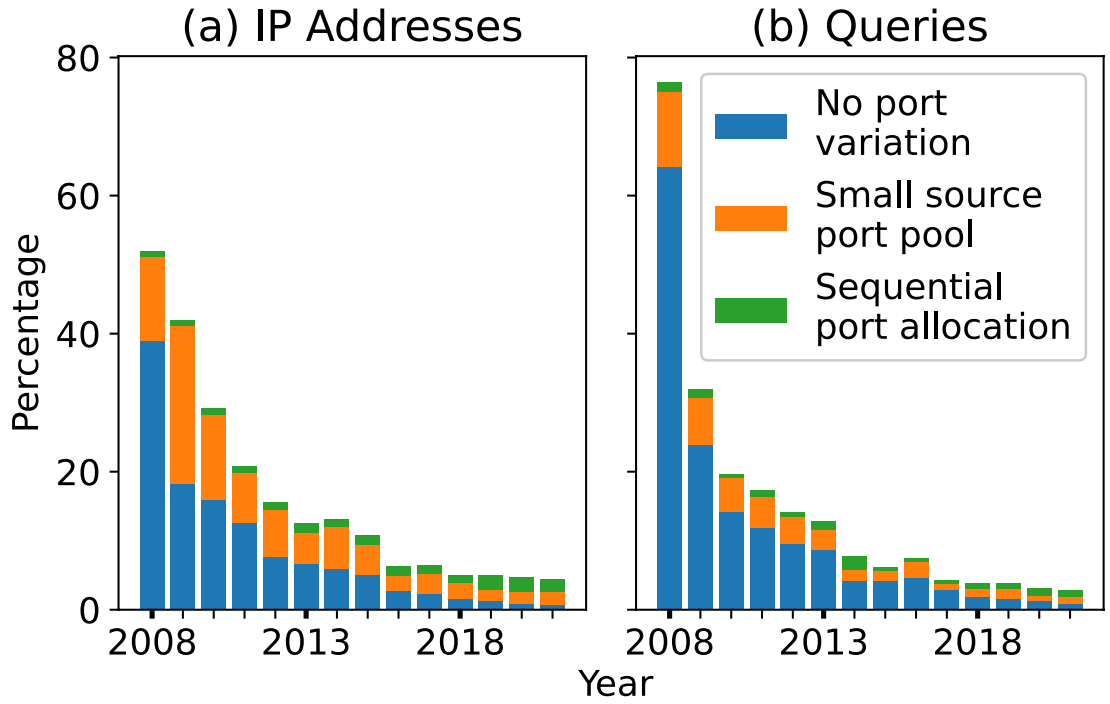
- What does source port randomization look like with a larger data set?
- What other resolver security and privacy and mechanisms can be observed?
- What does deployment look like over a 14-year period?

Dataset

- A-root data from DITL collection from 2008 through 2021
- Saved at most 13 queries from each client IP address over 48-hour period:
  - Query name, Query type, Transaction ID, source port
- Total per-type query counts

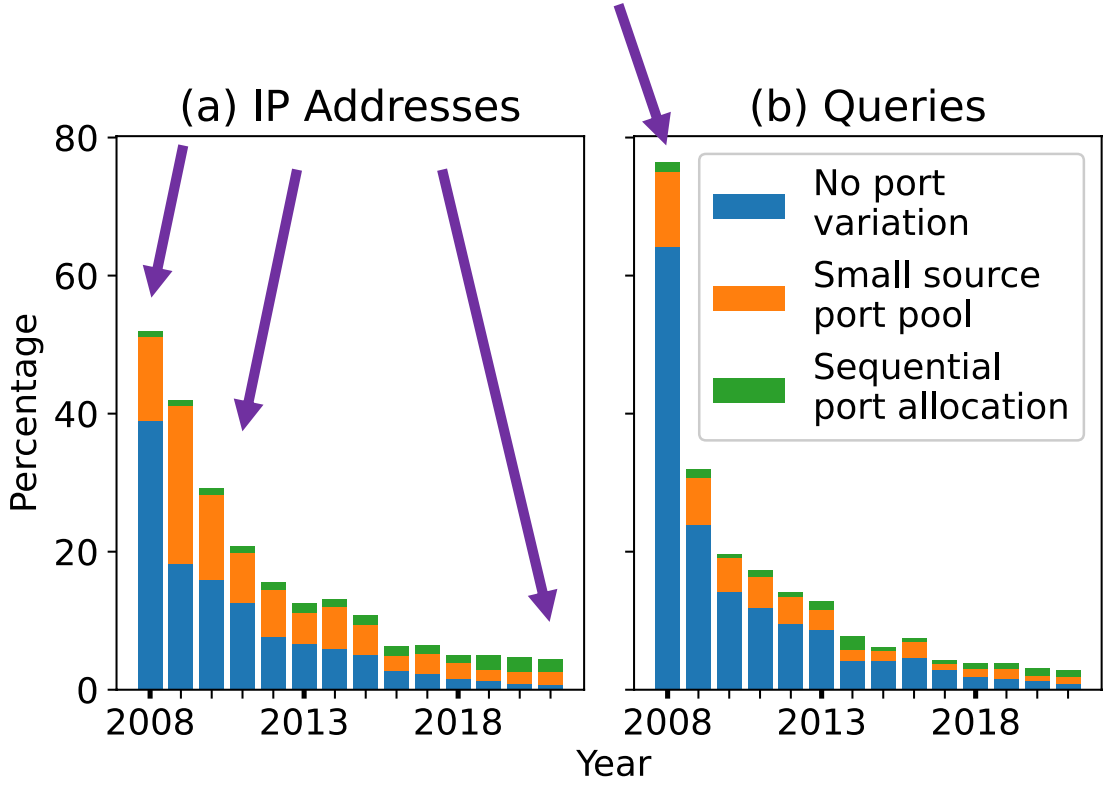
Source Port Randomization – Results

- **No port variation.** Same port used across all queries.
- **Small source port pool.** Only a handful of ports used Detected probabilistically by counting duplicate ports in sample.
- **Sequential port allocation.** Source ports have a range of 100.



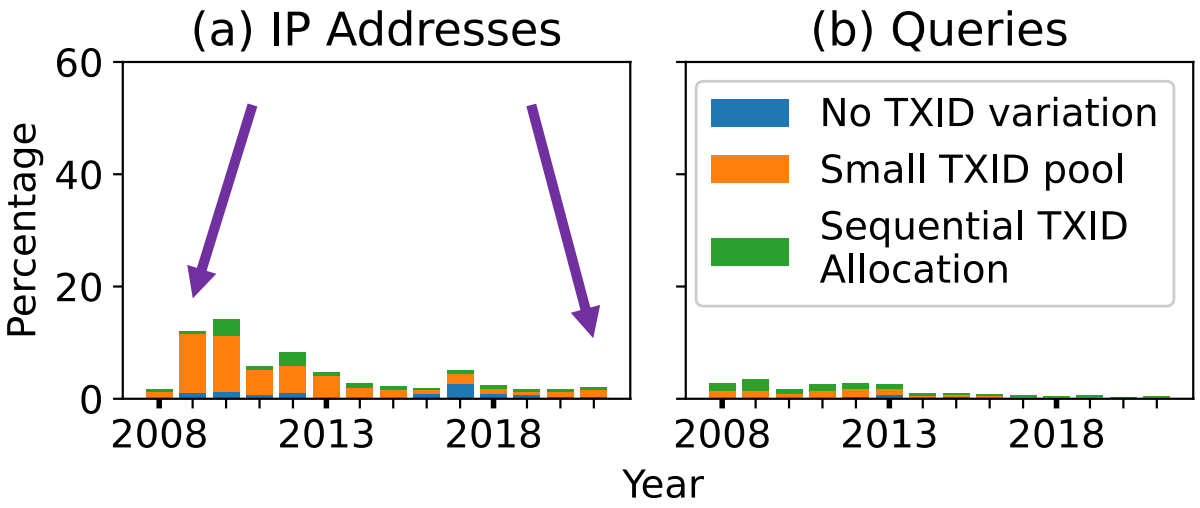
Source Port Randomization – Results

- In 2008, half of resolvers lacked source port randomization – accounting for 75% of queries.
- Only after 3 years (2011) did the fraction of vulnerable resolvers halve in size.
- In 2021, 4% of resolvers lacked source port randomization.
- Countries with highest fractions of vulnerable resolvers: China (8%), India (8%), Russia (5%).



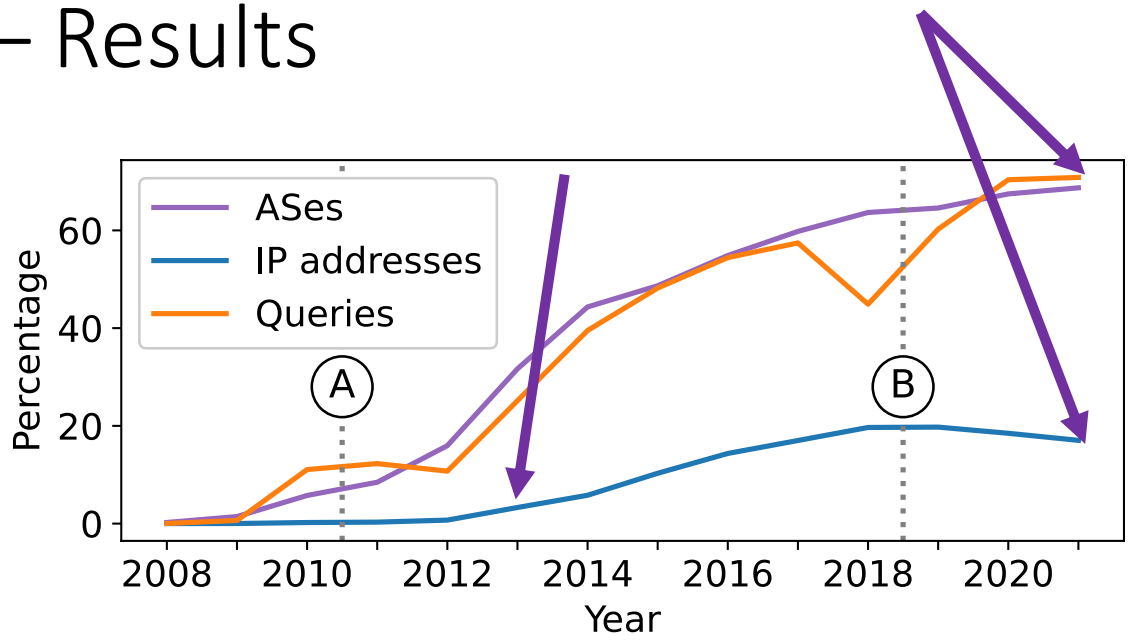
Transaction ID Randomization – Results

- Smaller rates of vulnerable resolvers.
- In 2021, 2% of resolvers lacked TXID randomization.
- High fraction of “small TXID” pool in 2009/2010.
  - 91% of resolvers in this category made at least two queries for type MX with TXID 10.
  - Fraction reduced in 2011.
  - Resolver software error?



DNSSEC Validation – Results

- Measure of resolvers with at least one DS or DNSKEY query.
- First significant presence of validating resolvers in 2013.
- In 2021, 17% of resolvers, making 70% of queries, exhibited validating behavior.
- Countries with highest fractions of validating resolvers: France (36%), Russia (29%), Brazil (26%).

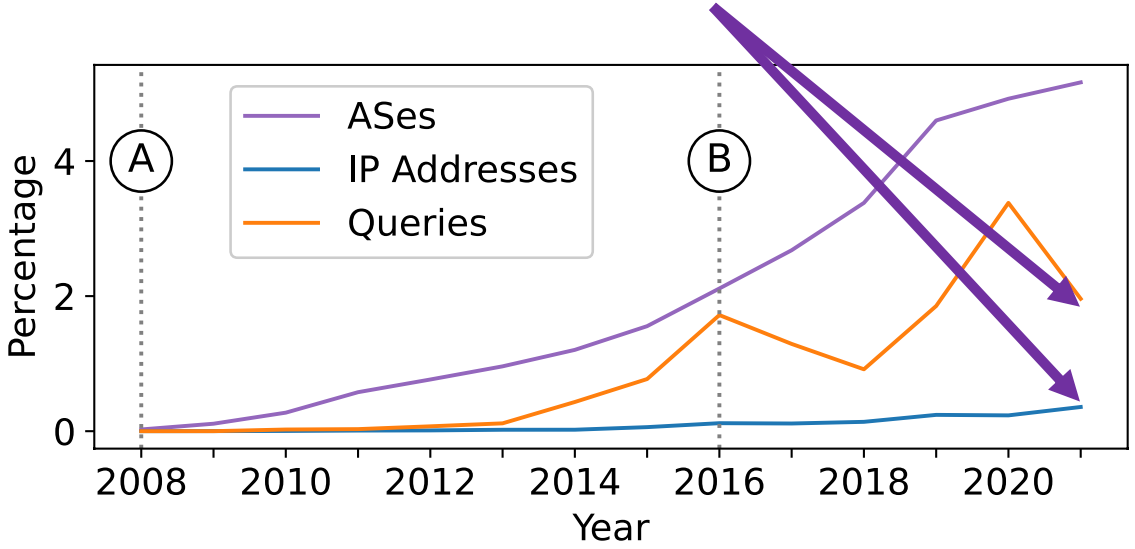


A: Root zone signed

B: Root zone KSK rollover

0x20 Encoding – Results

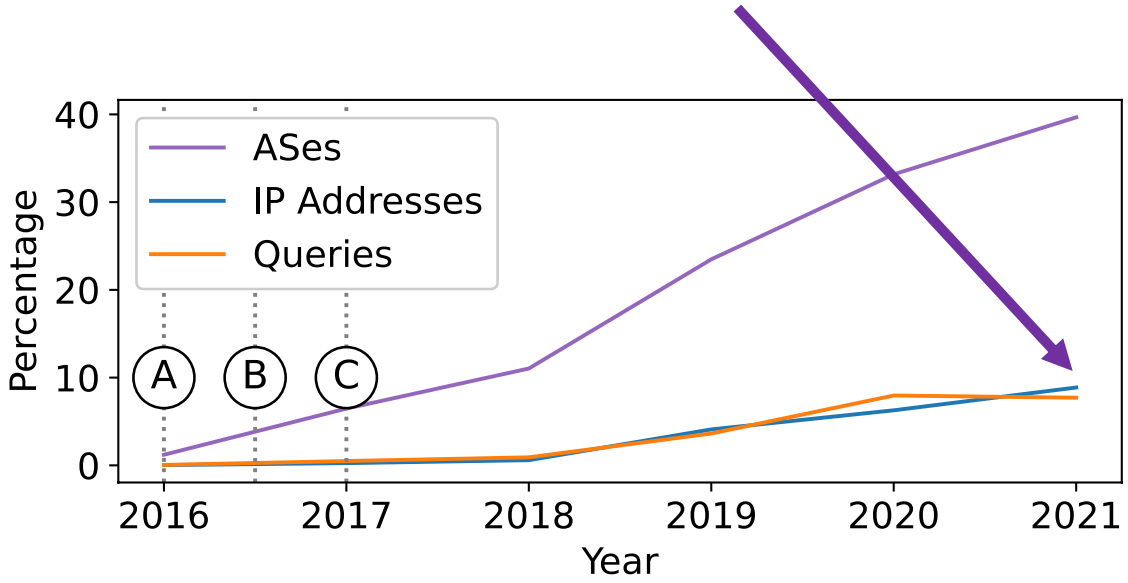
- Measure of resolvers with 50% chance of being upper-case.
- In 2021, 0.4% of resolvers, making 2% of queries, exhibited 0x20 behavior.



A: 0x20 Internet Draft; unbound introduces 0x20 encoding
B: Knot resolver with 0x20 encoding

DNS Cookie Usage – Results

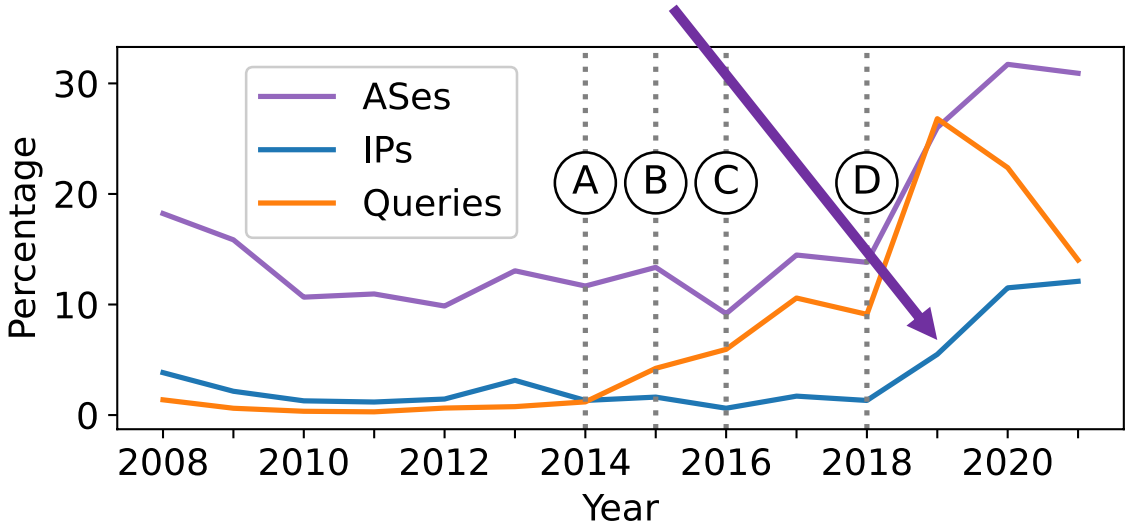
- Measure of resolvers with at least one query with DNS cookie.
- In 2021, 8% of resolvers, making 8% of queries, supported DNS cookies; up to 40% of ASes.



A: DNS cookie RFC published
B: Knot resolver introduces DNS cookies
C: BIND resolver introduces DNS cookies

QNAME Minimization – Results

- Measure of resolvers for which entire query sample (5 – 13 non-root queries) consisted of one label or one label with underscore.
- Less than 5% of resolvers exhibited QNAME minimization behaviors prior to 2019.
- There has been a steady increase since 2019, with the addition of QNAME min to BIND.



A: Internet Draft on Qname Min.
B: unbound resolver introduces Qname Min.
C: Qname Min. RFC published;
Knot resolver introduces Qname Min.
D: BIND resolver introduces Qname Min.

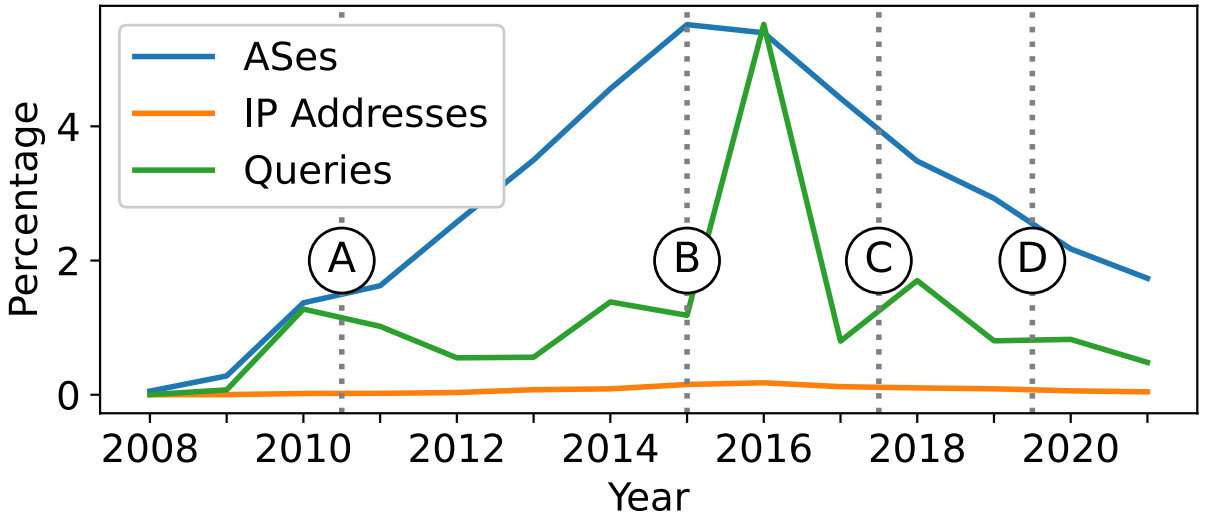
Holistic Analysis - 2021

	SPR	DNSSEC	0x20	Cookies	QMIN
BIND	9.5.0-P1 (2008 [13]) ●	9.4.0 (2007 [12]) ◐ 9.5.0-P1 (2008 [14]) ●		9.11.0 (2016 [15]) ●	9.13.2 (2018 [16]) ●
Knot	1.0.0 (2016 [18]) ●	1.1.0 (2016 [19]) ◐ 4.0.0 (2019 [21]) ●	1.1.0 (2016 [19]) ●	1.1.0 (2016 [19]) ◐ 3.0.0 (2018 [20]) ○	1.1.0 (2016 [19]) ●
Unbound	1.0.0 (2008 [41]) ●	1.0.0 (2008 [41]) ◐	1.0.0 (2008 [41]) ◐		1.5.7 (2015 [42]) ◐ 1.7.2 (2018 [43]) ●

TXID	SPR	DNSSEC	0x20	Cookies	QMIN	IP Addresses		ASes		Queries	
						#	%	#	%	#	%
✓	✓	×	×	×	×	2,189,133	59.0%	40,173	79.8%	1,268	19.9%
✓	✓	✓	×	×	×	503,799	13.6%	26,486	52.6%	15,449	55.8%
✓	✓	×	×	✓	×	315,015	8.5%	13,168	26.2%	857	1.9%
✓	✓	×	×	×	✓	189,895	5.1%	7,956	15.8%	2,242	3.1%
✓	✓	✓	×	×	✓	157,278	4.2%	9,782	19.4%	7,895	8.9%
✓	✓	✓	×	✓	×	133,099	3.6%	12,398	24.6%	5,296	5.1%
✓	×	×	×	×	×	114,592	3.1%	6,931	13.8%	2,527	2.1%
×	×	×	×	×	×	47,069	1.3%	3,202	6.4%	383	0.1%
×	✓	×	×	×	×	24,192	0.7%	2,191	4.4%	849	0.1%
other						38,716	1.0%	5,471	10.9%	11,042	3.1%

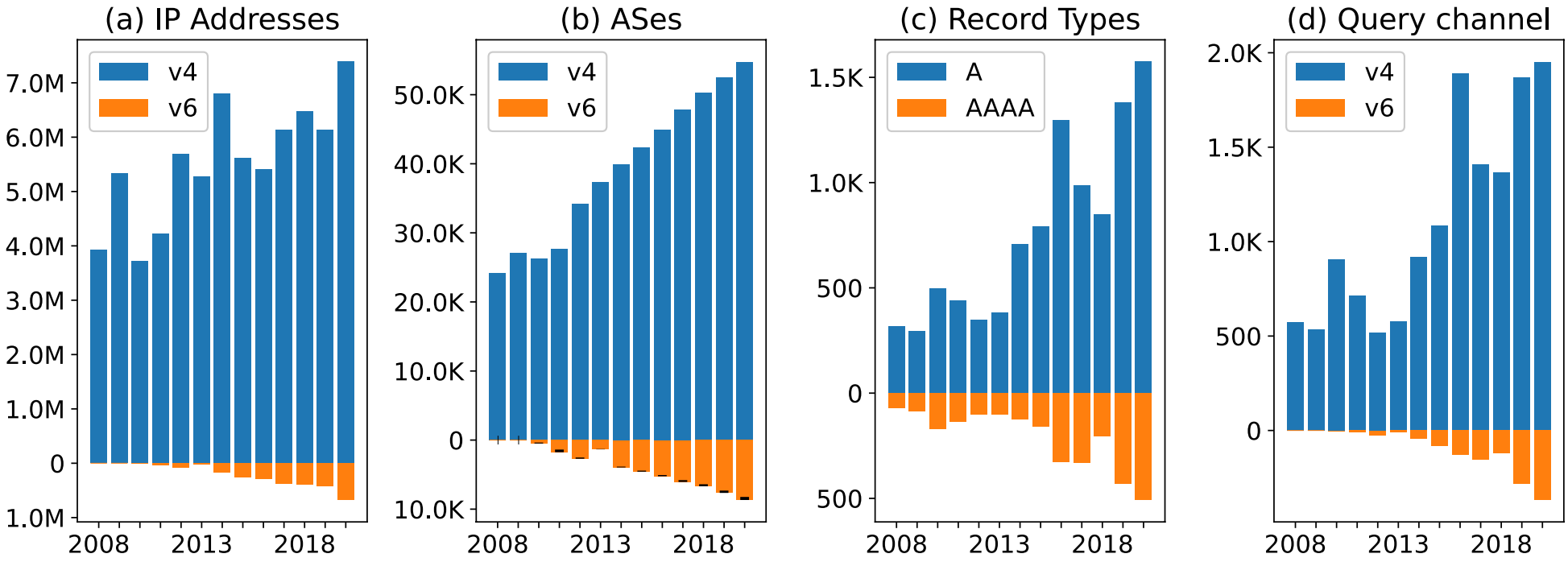
Bonus: DLV Queries at the root

- DLV usage never reached even 1% of resolvers.
- ASes with at least one resolver using DLV peaked at over 5%.
- Numbers have declined since 2015.
- In 2021, over 4K resolvers (0.04%) in over 1K Ases (2%) queried for DLV.



A: the root zone signing
B: the sunsetting of ISC's DLV service and the remove of DLV from Fedora
C: the decommissioning of ISC's DLV service
D: the official marking of DLV as “historic”

Bonus: IPv6 at A-Root



Summary

- Fixing bad security is slow!
- In 2021, DNSSEC-validating resolvers are relatively few but produced the majority of traffic to A-root.
- Removing old things takes time.

Questions?

All images are public domain, obtained from openclipart.org