Fourteen Years in the Life:

A Root Server’s Perspective on DNS Resolver Security

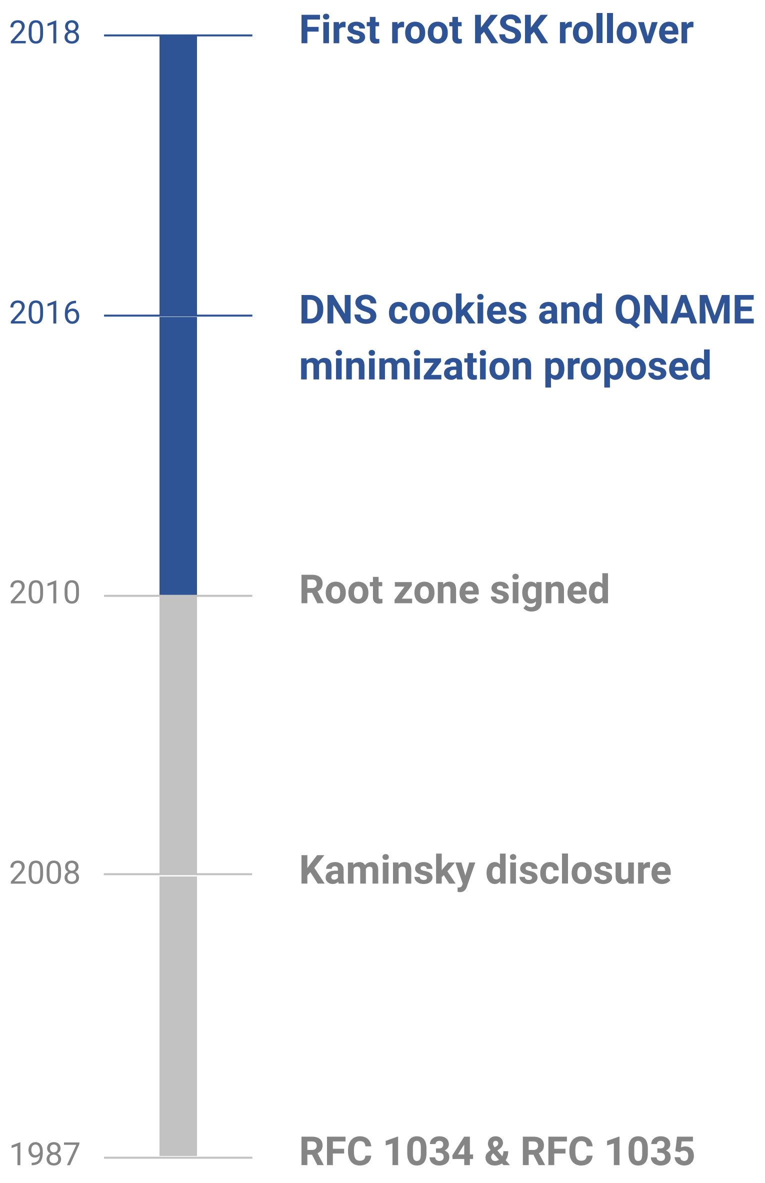
Alden Hilton
Alden.Hilton@sandia.gov

Casey Deccio
casey@byu.edu

Jacob Davis
javdavi@sandia.gov

Research Questions

- How has DNS security and privacy evolved over time?
- What is the current state today?
- What security and privacy practices can be observed from the root?



2018 First root KSK rollover

2016 DNS cookies and QNAME minimization proposed

2010 Root zone signed

2008 Kaminsky disclosure

1987 RFC 1034 & RFC 1035

Security and Privacy Techniques Considered

TXID/Source Port Randomization

- Randomize source port + TXID
- Up to 32 bits of entropy

0x20 Encoding

aAa
AaA
AA

- Randomize QNAME capitalization
- 1 bit of entropy per letter
- Not standardized

DNSSEC

- Cryptographic signatures
- Deployed by authoritative servers and verified by resolvers

Cookies

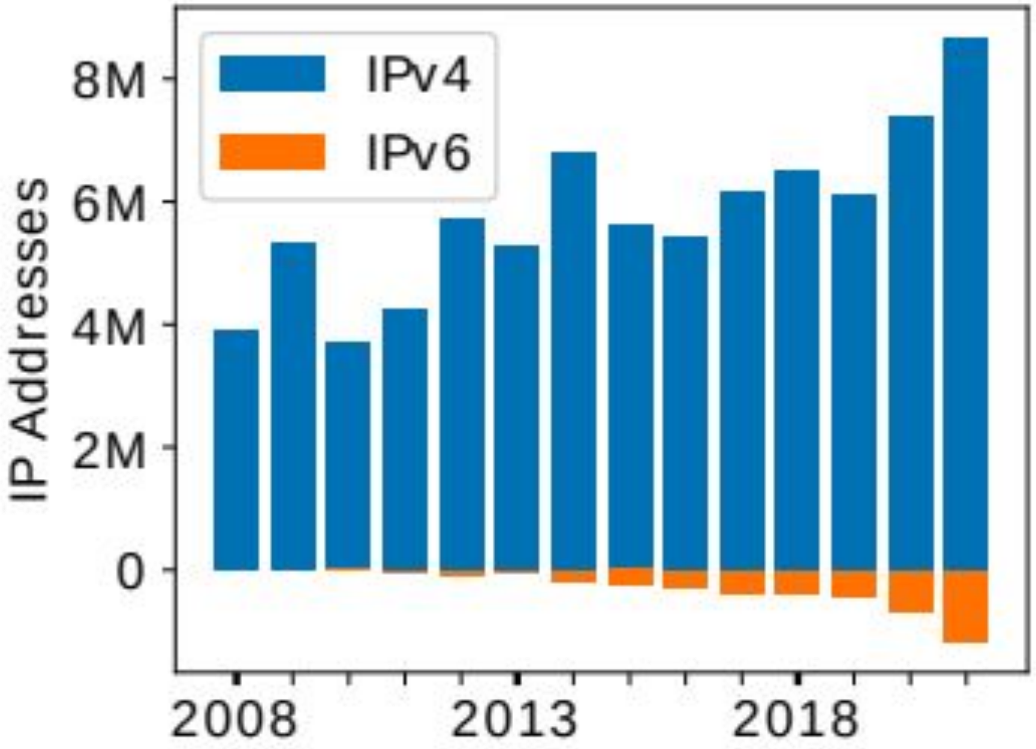
- 64 bits of transaction security
- Client + server mutual authentication

QNAME Minimization

- Privacy mechanism
- Only include labels needed for the next step in the resolution process

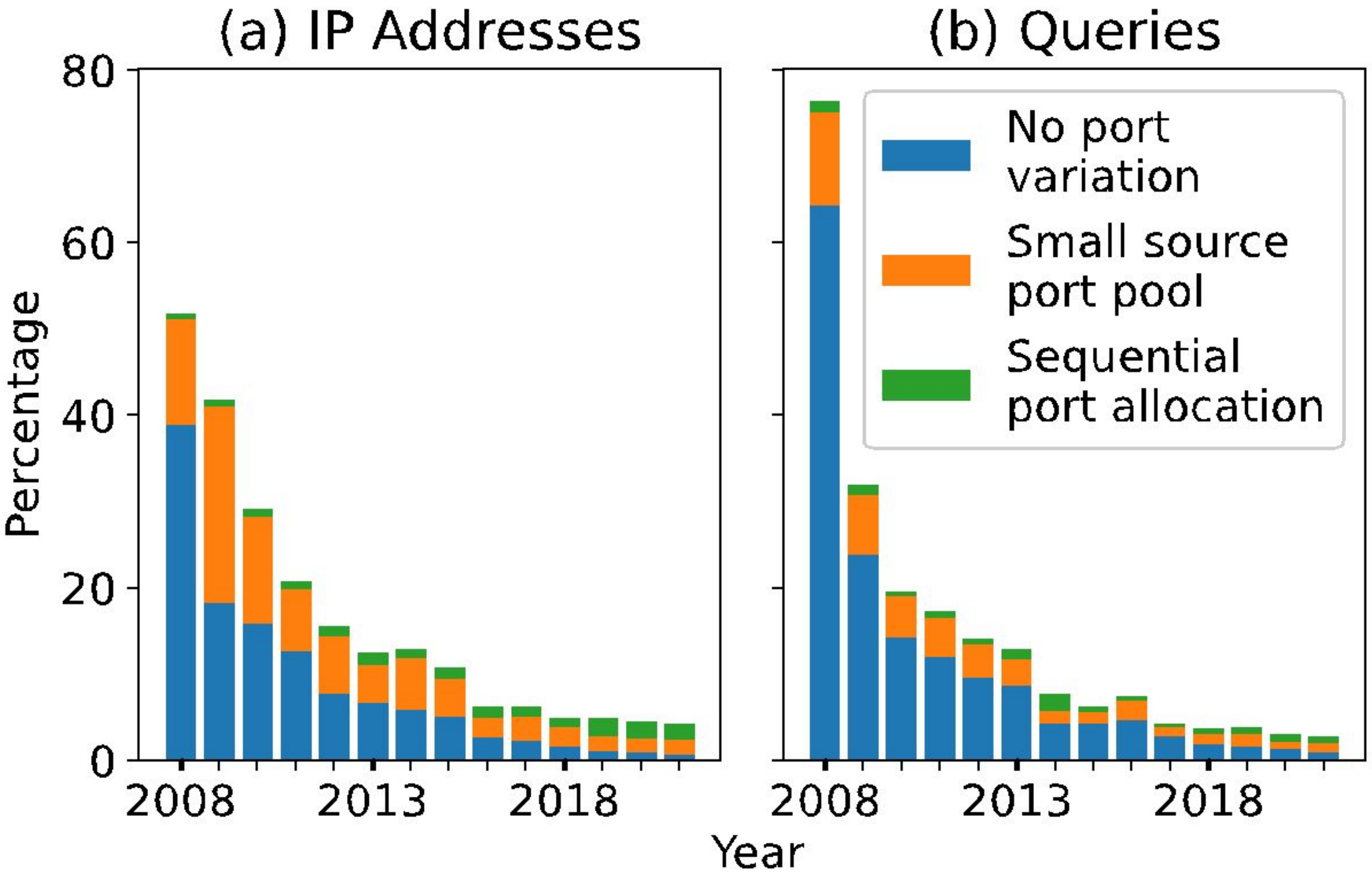
Data Set

- "Day in the Life" (DITL), annual ~48 hour collection of traffic received at the root servers, sponsored by OARC
- A-root from 2008-2021



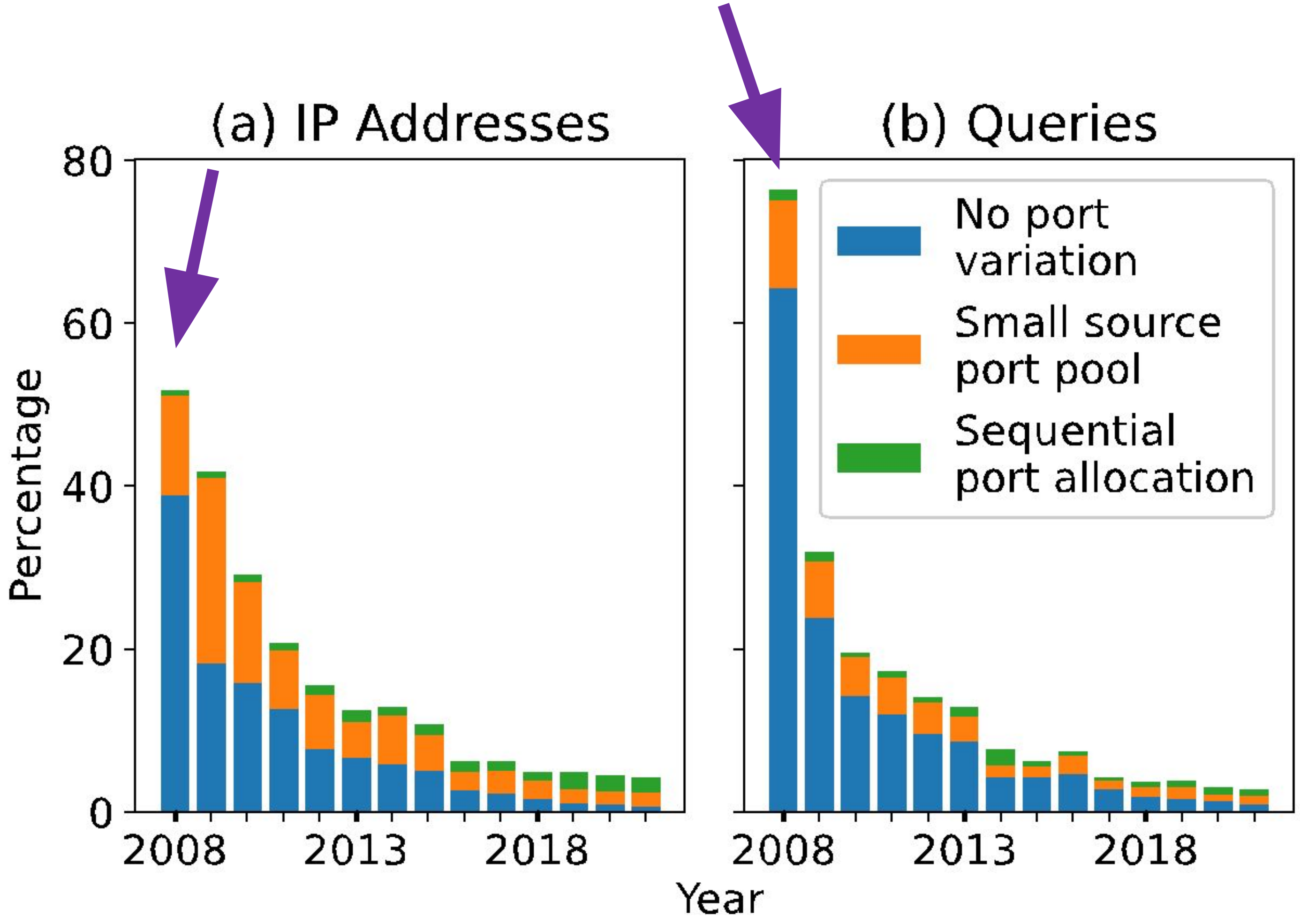
Source Port Randomization - Results

- **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.



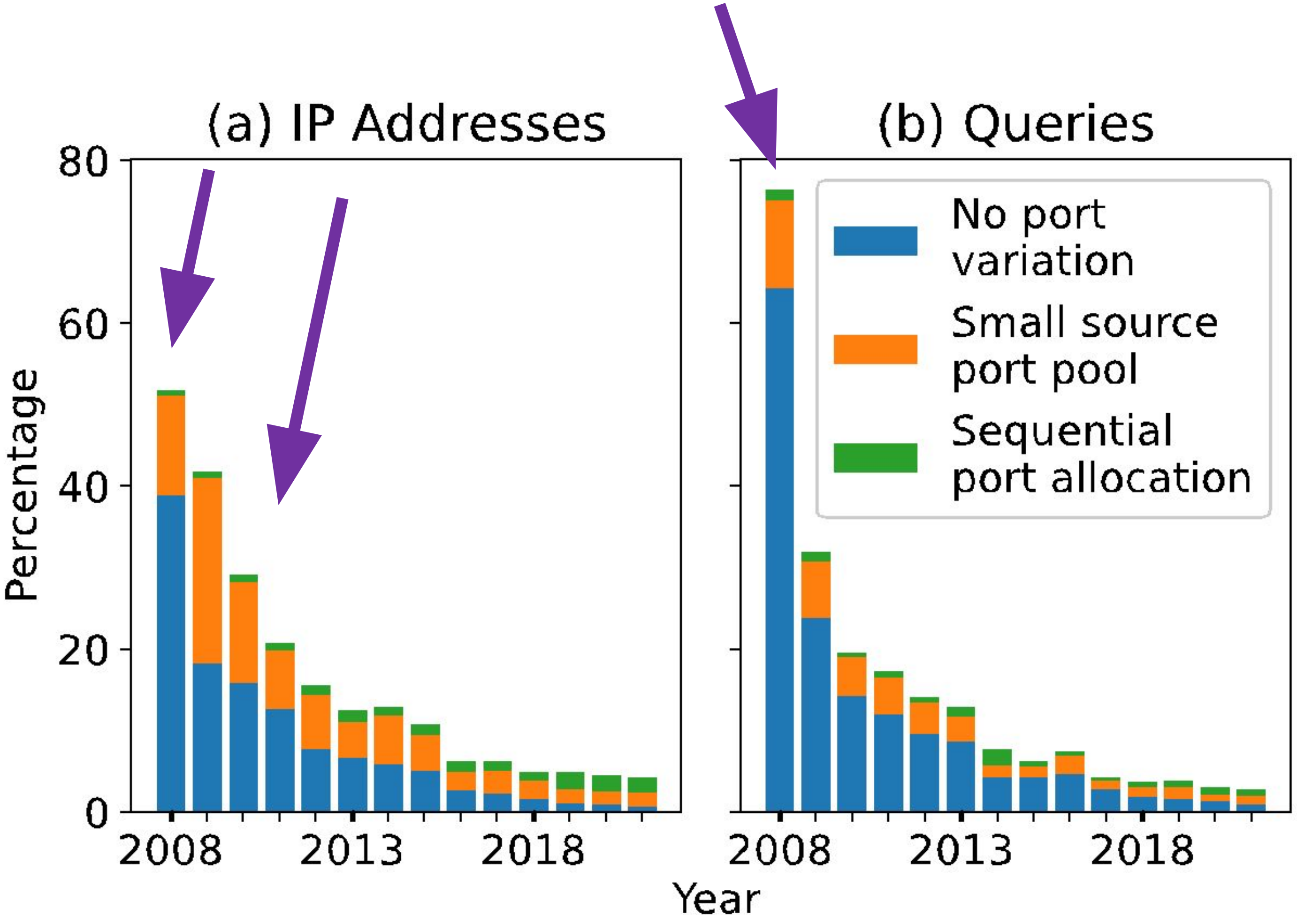
Source Port Randomization - Results

- 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, making 3% of queries.
- From 10K ASes and over 200 countries.



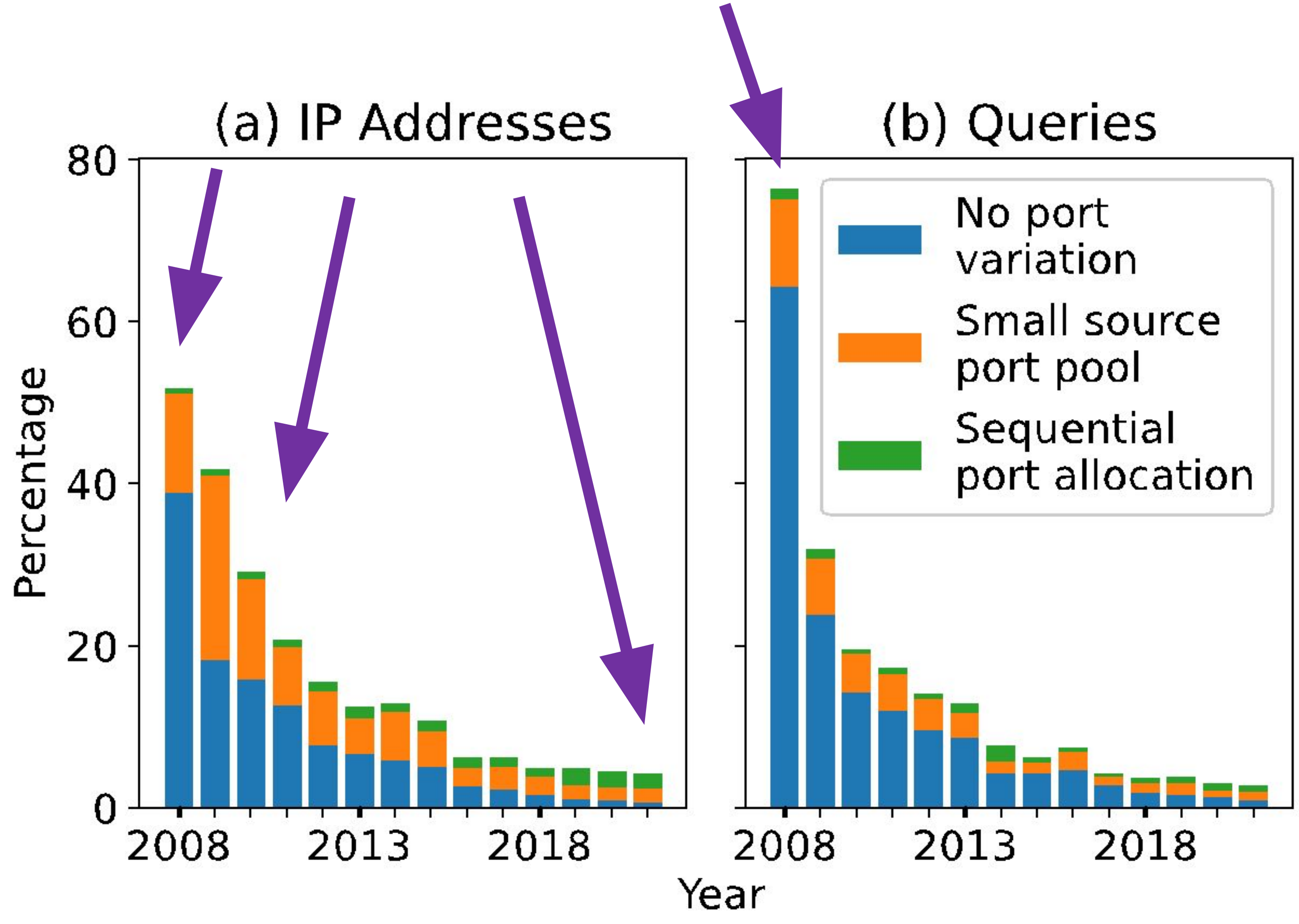
Source Port Randomization - Results

- 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, making 3% of queries.
- From 10K ASes and over 200 countries.



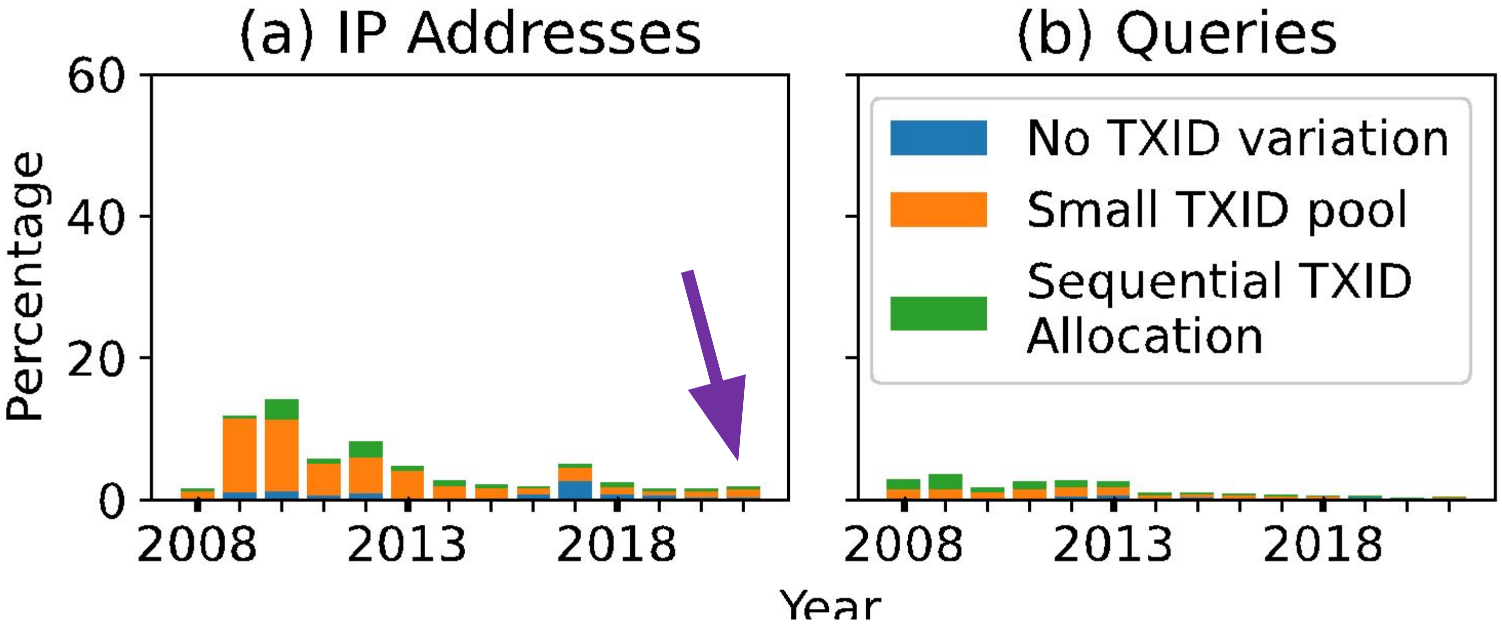
Source Port Randomization - Results

- 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, making 3% of queries.
- From 10K ASes and over 200 countries



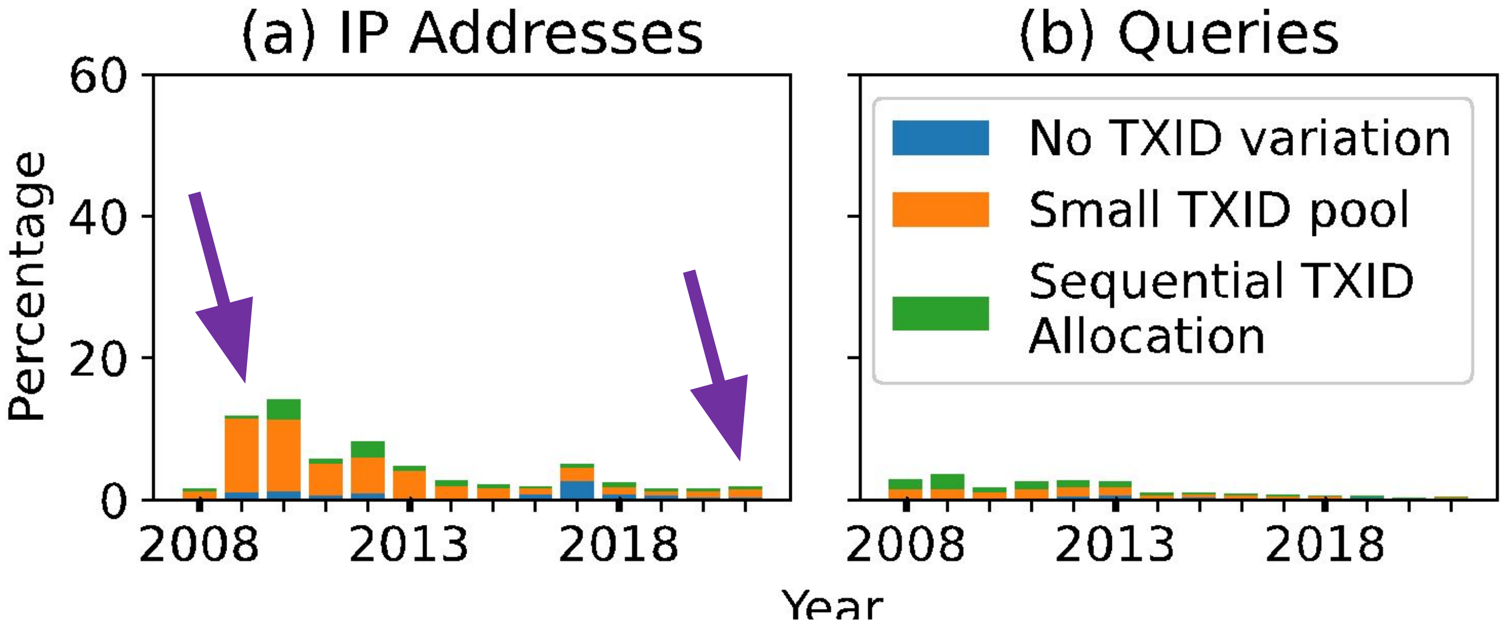
Transaction ID Randomization – Results

- Smaller rates of vulnerable resolvers.
- In 2021, 2% of resolvers lacked TXID randomization, with 0.44% of queries.
- 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?



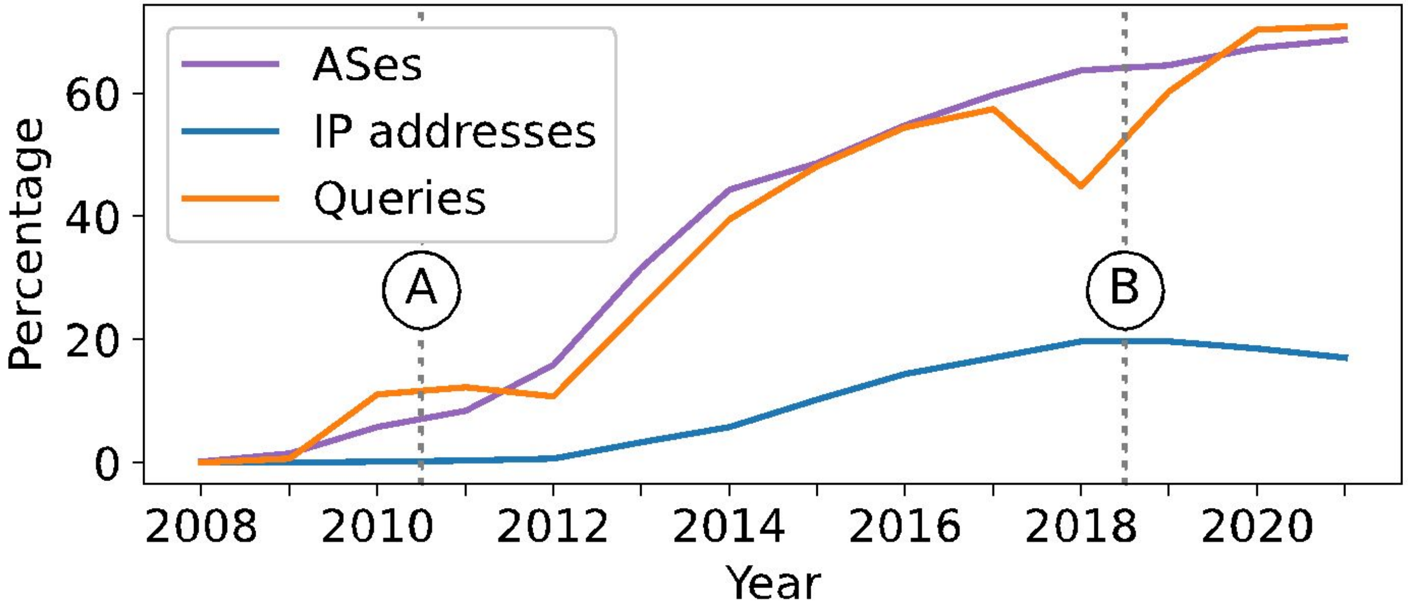
Transaction ID Randomization – Results

- Smaller rates of vulnerable resolvers.
- In 2021, 2% of resolvers lacked TXID randomization, with 0.44% of queries
- 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.

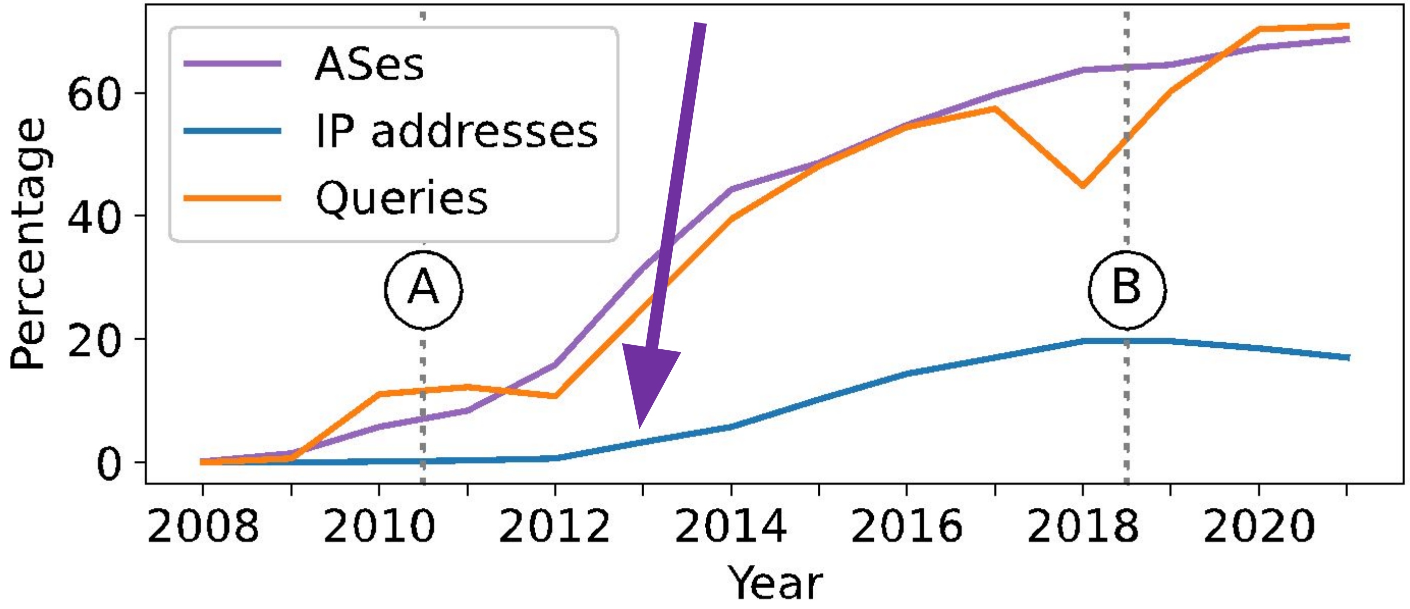


A: Root zone signed

B: Root zone KSK rollover

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.

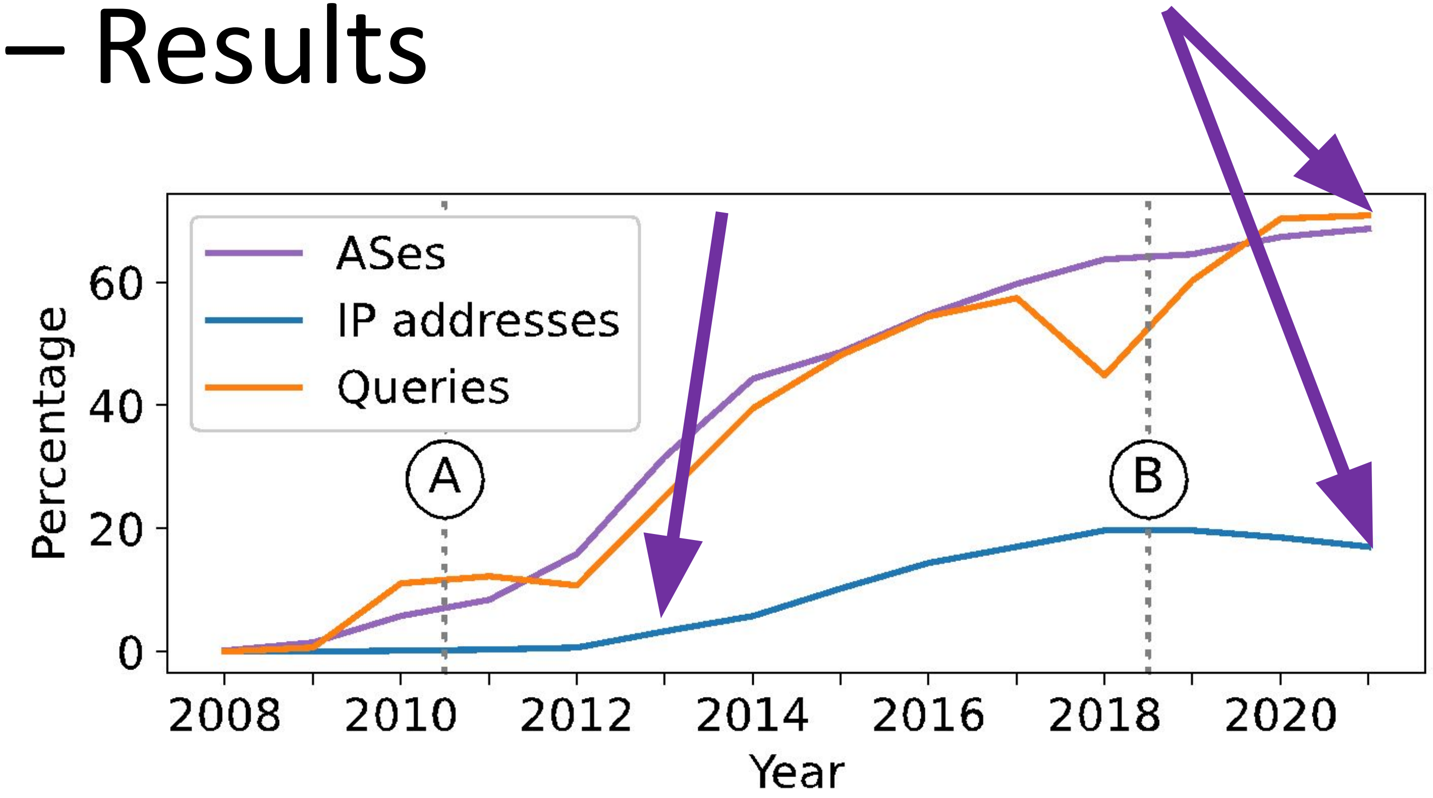


A: Root zone signed

B: Root zone KSK rollover

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.

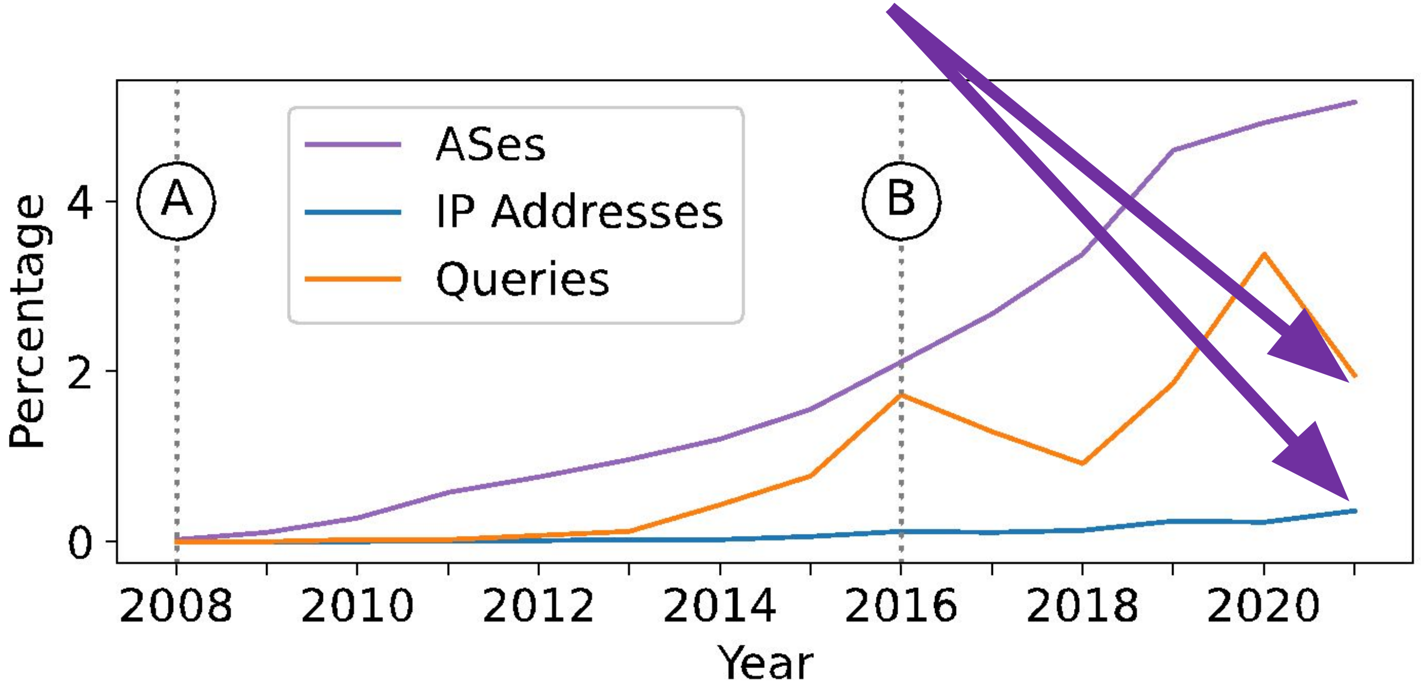


A: Root zone signed

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.

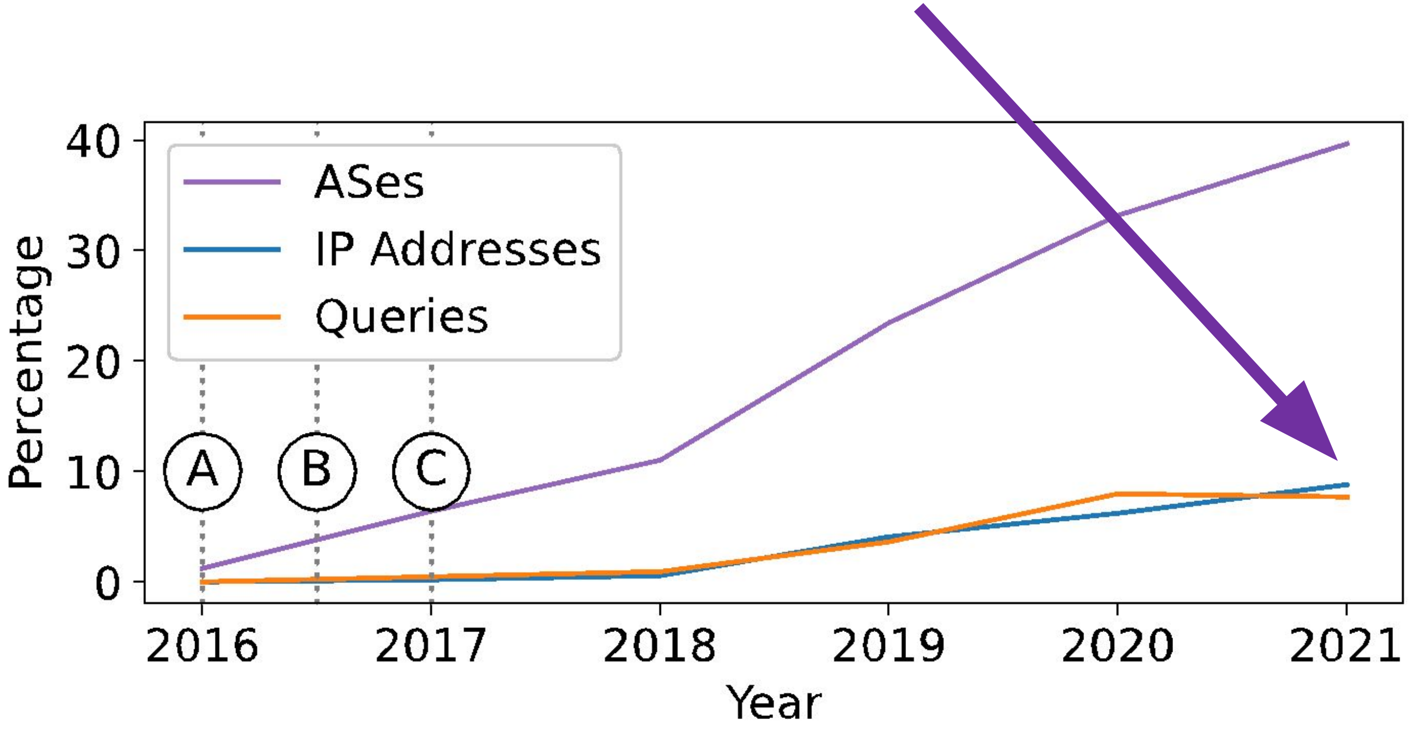


A: 0x20 Internet Draft; unbound introduces 0x20 encoding

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



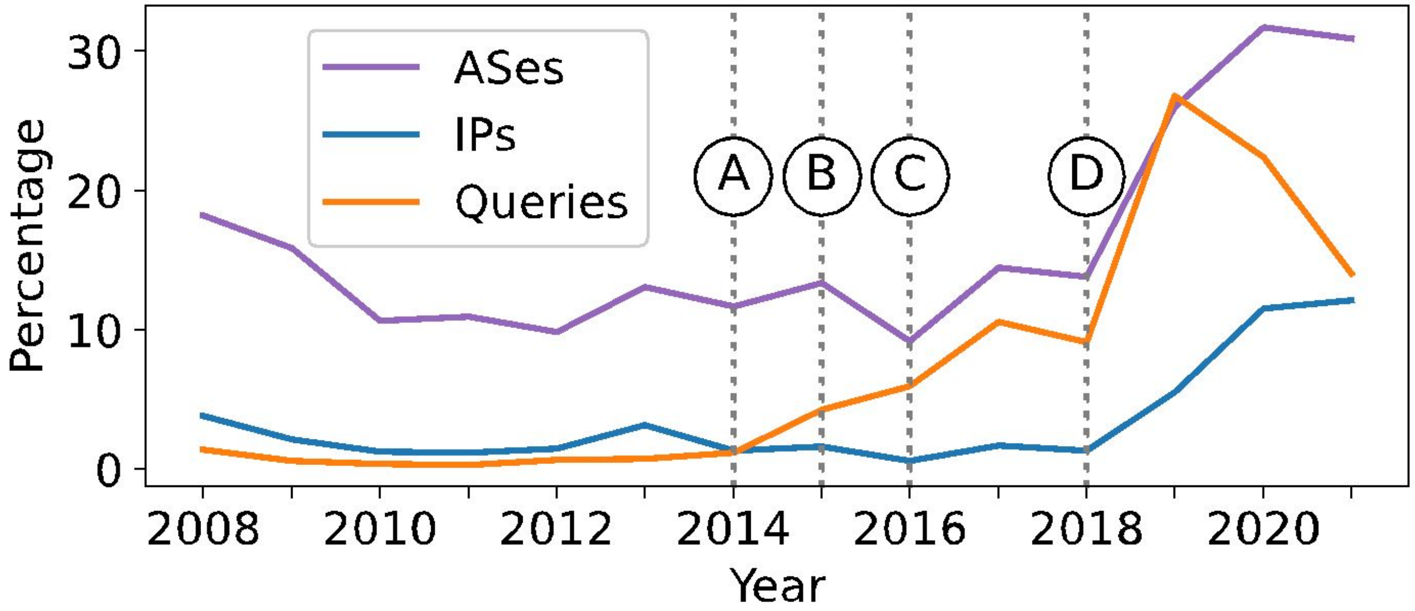
A: DNS cookie RFC published

B: Knot resolver introduces DNS cookies

C: BIND resolver introduces DNS cookies

QNAME Minimization – Results

- Measure of resolvers for which entire query sample 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.

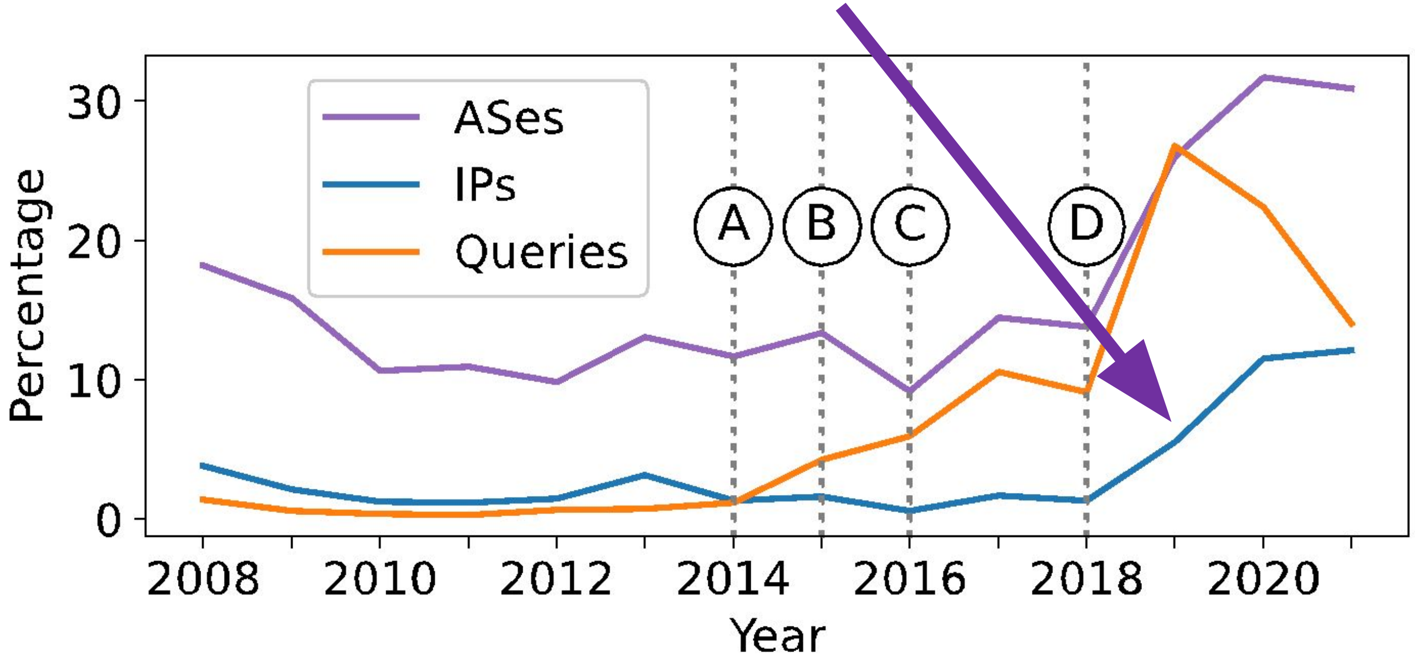
B: unbound resolver introduces Qname Min.

C: Qname Min. RFC published;
Knot resolver introduces Qname Min.

D: BIND resolver introduces Qname Min.

QNAME Minimization – Results

- Measure of resolvers for which entire query sample 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.



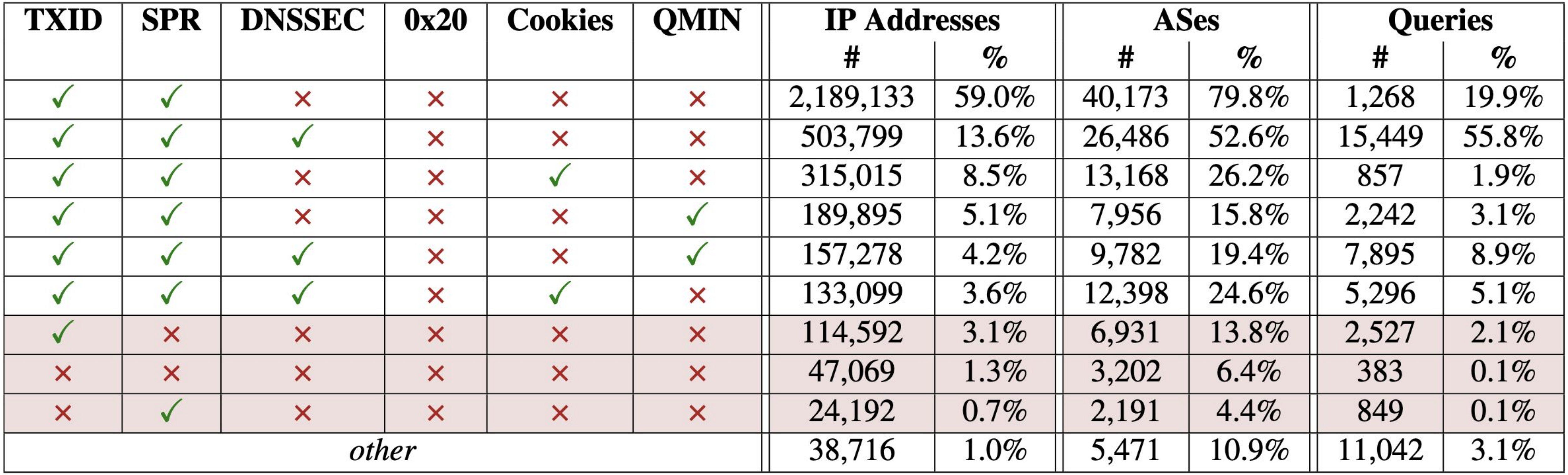
A: Internet Draft on Qname Min.

B: unbound resolver introduces Qname Min.

C: Qname Min. RFC published;
Knot resolver introduces Qname Min.

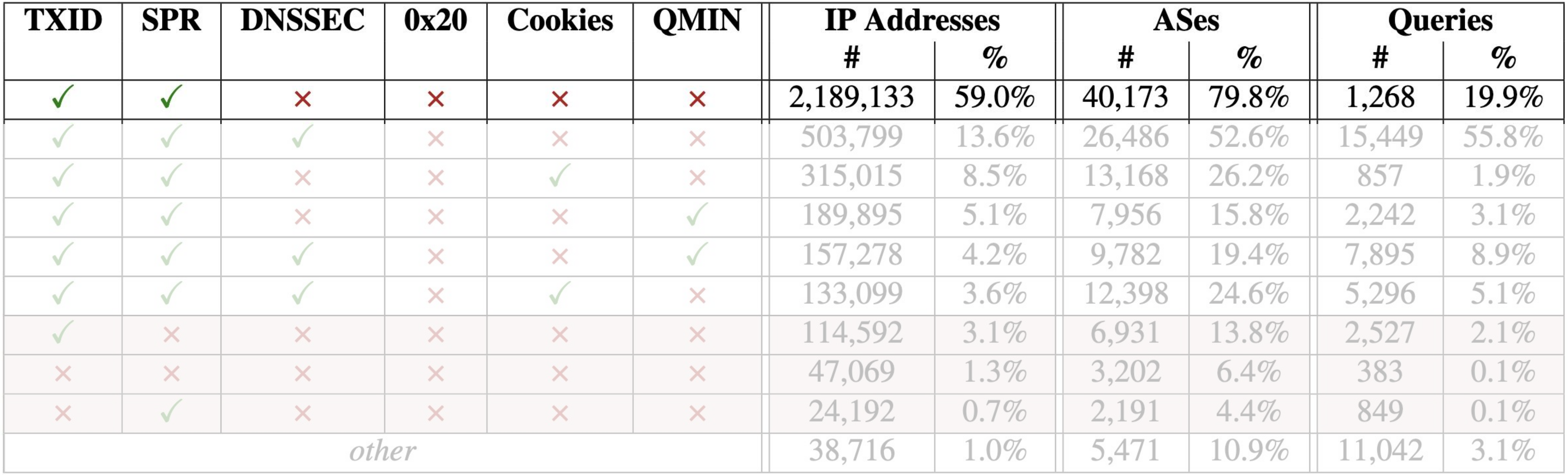
D: BIND resolver introduces Qname Min.

Holistic Analysis - 2021



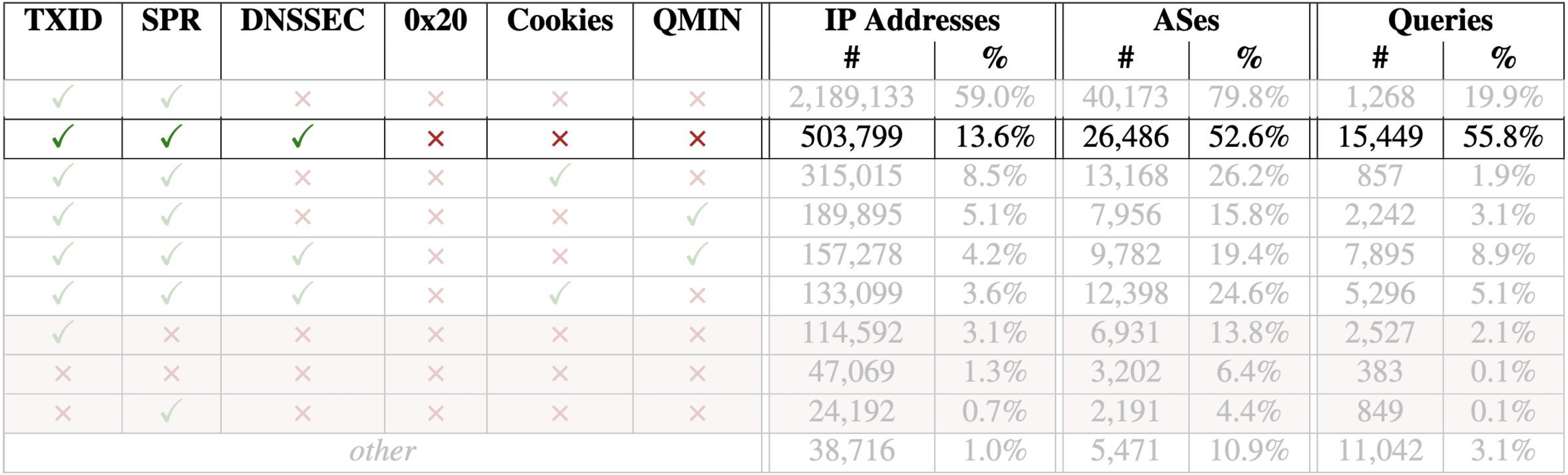
TXID	**SPR**	**DNSSEC**	**0x20**	**Cookies**	**QMIN**	**IP Addresses**		**ASes**		**Queries**	
						#	**%**	**#**	**%**	**#**	**%**
✓	✓	×	×	×	×	2,189,133	59.0%	40,173	79.8%	1,268	19.9%
✓	✓	✓	×	×	×	503,799	13.6%	26,486	52.6%	15,449	55.8%
✓	✓	×	×	✓	×	315,015	8.5%	13,168	26.2%	857	1.9%
✓	✓	×	×	×	✓	189,895	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%

Holistic Analysis - 2021



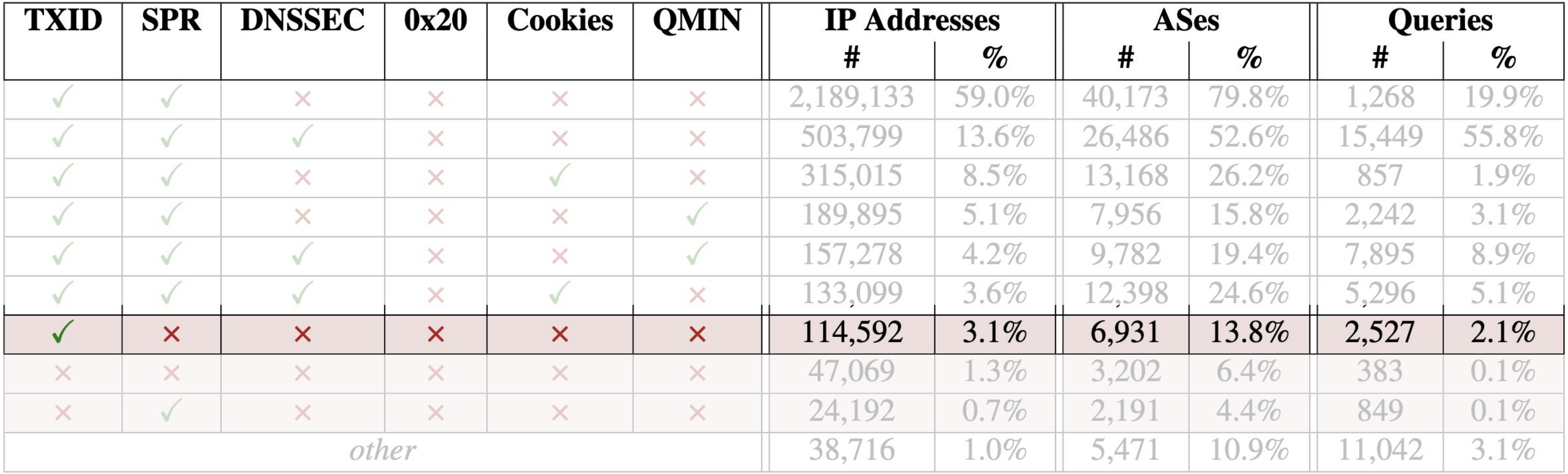
TXID	SPR	DNSSEC	0x20	Cookies	QMIN	IP Addresses		ASes		Queries	
						#	%	#	%	#	%
✓	✓	×	×	×	×	2,189,133	59.0%	40,173	79.8%	1,268	19.9%
✓	✓	✓	×	×	×	503,799	13.6%	26,486	52.6%	15,449	55.8%
✓	✓	×	×	✓	×	315,015	8.5%	13,168	26.2%	857	1.9%
✓	✓	×	×	×	✓	189,895	5.1%	7,956	15.8%	2,242	3.1%
✓	✓	✓	×	×	✓	157,278	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%

Holistic Analysis - 2021



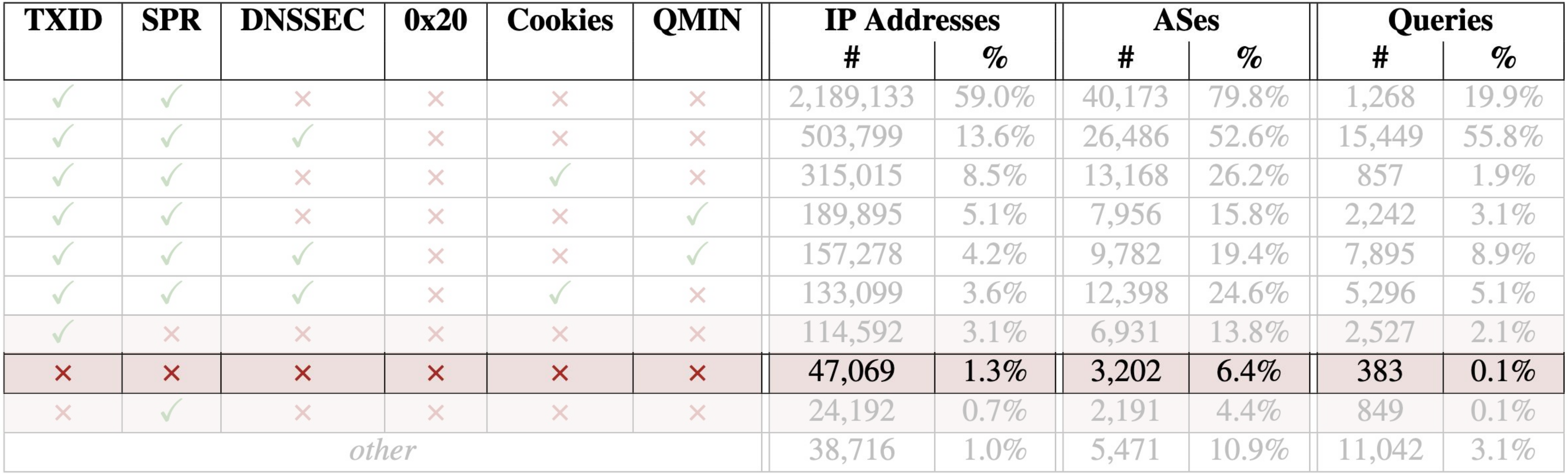
TXID	SPR	DNSSEC	0x20	Cookies	QMIN	IP Addresses		ASes		Queries	
						#	%	#	%	#	%
✓	✓	×	×	×	×	2,189,133	59.0%	40,173	79.8%	1,268	19.9%
✓	✓	✓	×	×	×	503,799	13.6%	26,486	52.6%	15,449	55.8%
✓	✓	×	×	✓	×	315,015	8.5%	13,168	26.2%	857	1.9%
✓	✓	×	×	×	✓	189,895	5.1%	7,956	15.8%	2,242	3.1%
✓	✓	✓	×	×	✓	157,278	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%

Holistic Analysis - 2021



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%

Holistic Analysis - 2021



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%

Conclusion

- Basic DNS resolver security mechanisms are not ubiquitously deployed
- In 2021, DNSSEC-validating resolvers are relatively few but produced the majority of traffic to A-root.
- Security fixes take time

Questions?

Alden Hilton
Alden.Hilton@sandia.gov

Casey Deccio
casey@byu.edu

Jacob Davis
javdavi@sandia.gov