Some Technology Trends in the DNS

Geoff Huston
October 2020

Three broad topics:

1. DNSSEC
2. DNS Privacy
3. Other Stuff

1. DNSSEC - Why?

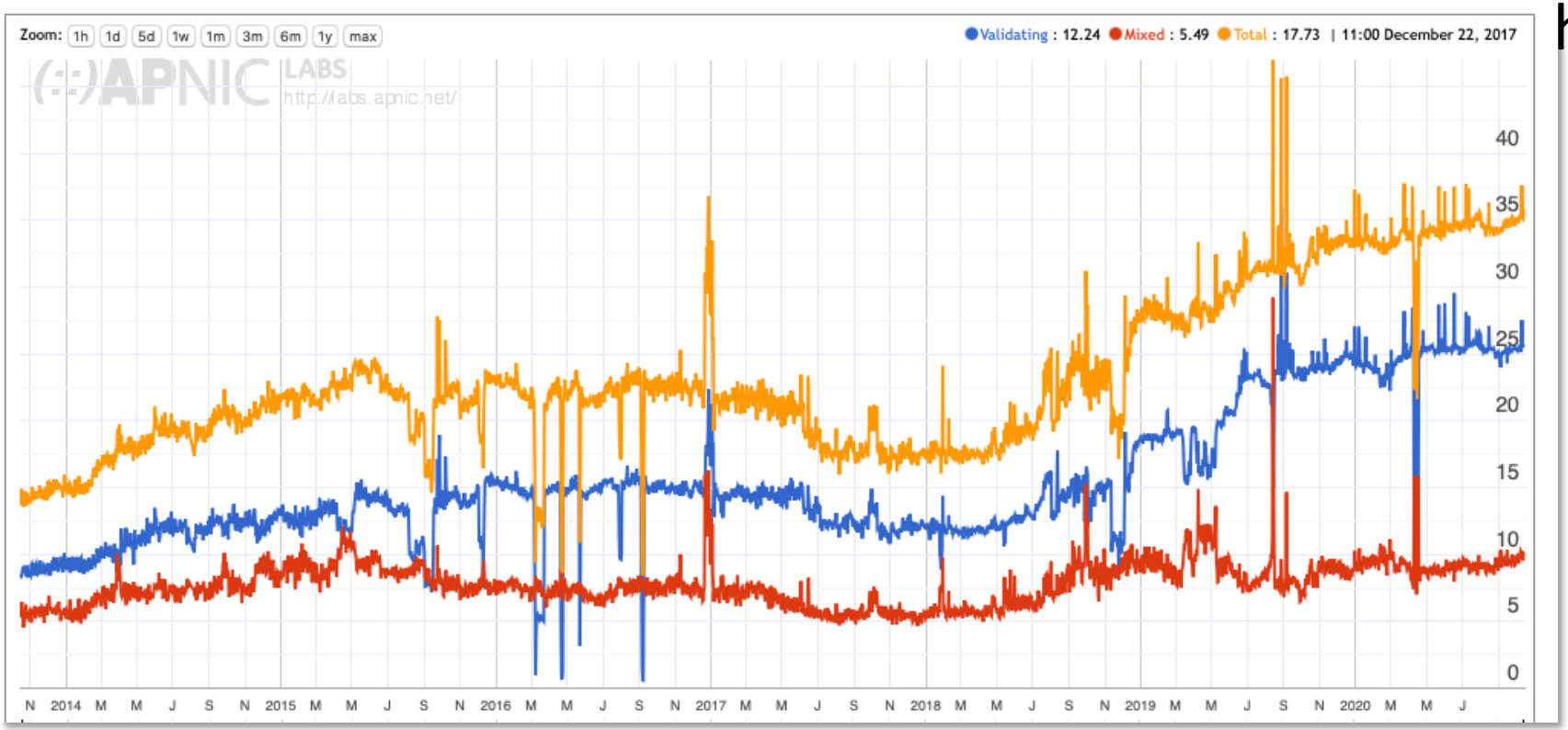
- How can you believe what the DNS tells you?
  - You can't!
- DNS interception and rewriting is common these days
  - "Clean Feed" DNS resolvers
  - NXDOMAIN rewriters
  - DNS 6to4 rewriters
- And then there is hostility
  - Glue attacks (Kaminsky attack)
  - Fragmentation attacks

1. DNSSEC - How?

- Add a digital signature to the entries in the DNS zone
- Provide the signature along with the resource records in the answer
- Validate the signature before using the response data

1. DNSSEC - Who uses it?

- Add a digital signature to the entries in the DNS zone
- Pr… …he answer
- Va…

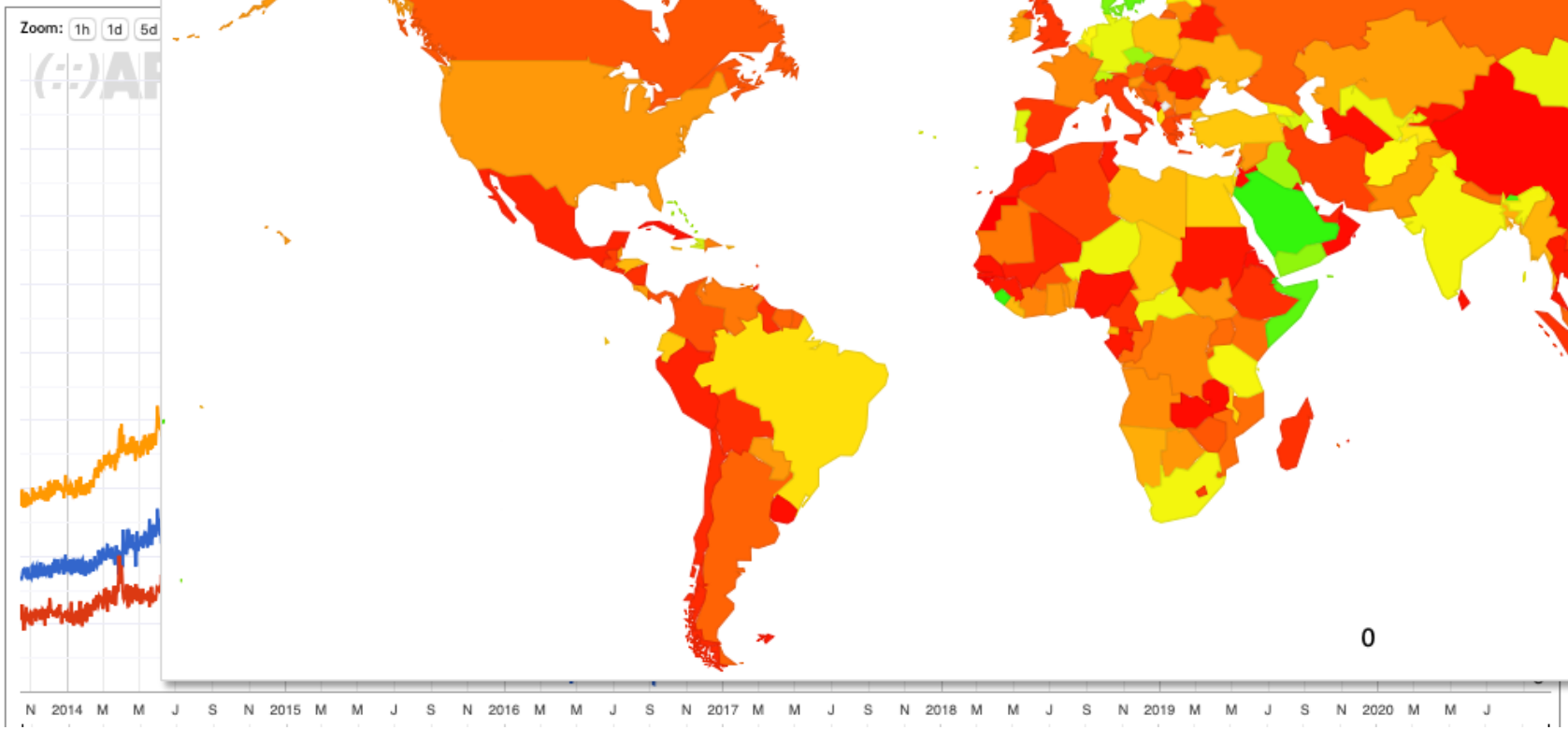


Those who do it

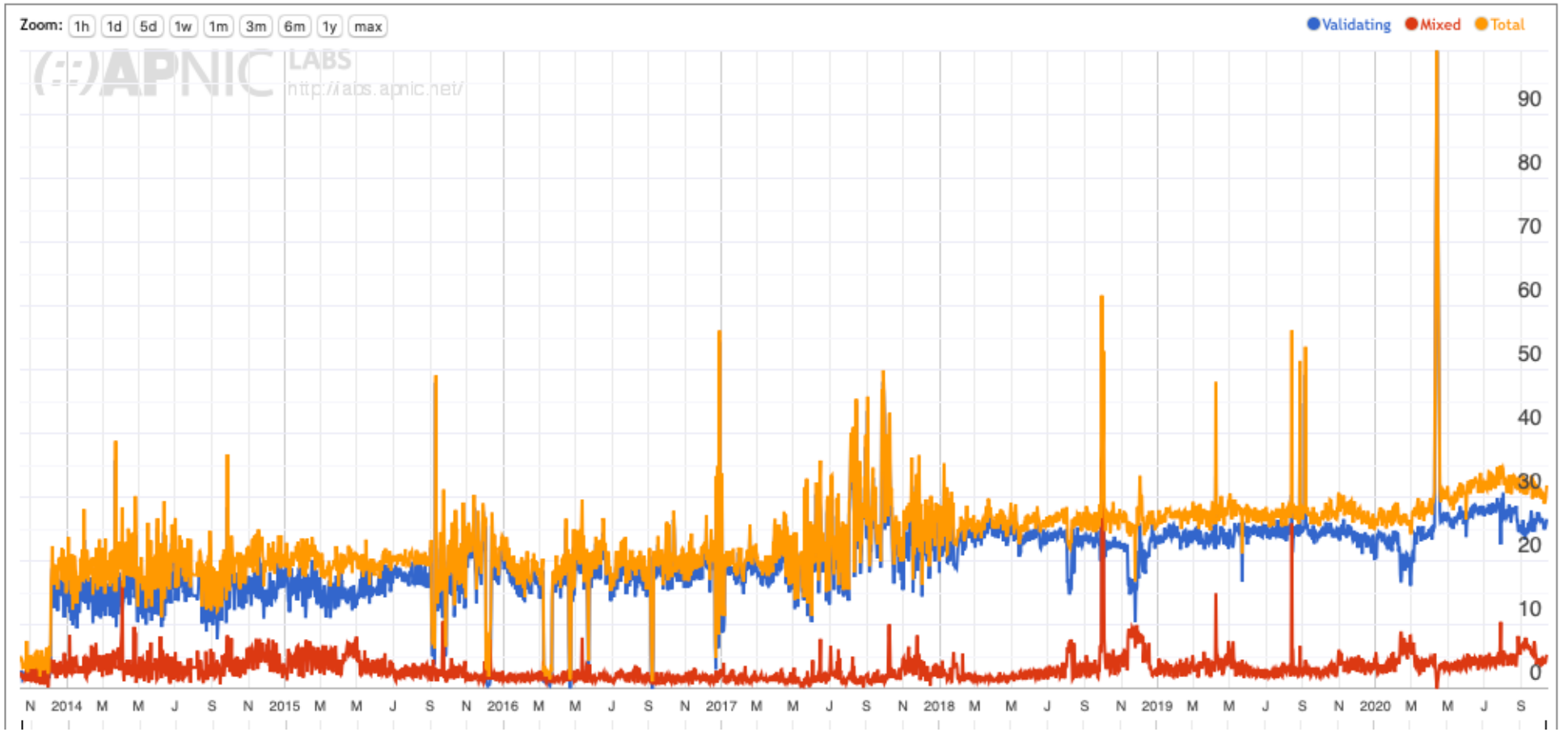
Those who do it a little

1. DNSSEC - Who uses it?

- Add a d
- Pr
- Va



1. DNSSEC validation in Australia



1. DNSSEC validation in Australia

ASN	AS Name	DNSSEC Validates	Partial Validation	Samples
AS1221	ASN-TELSTRA Telstra Corporation Ltd	1.77%	1.15%	11,155
AS4804	~~MPX-AS Microplex PTY LTD~~ Optus	91.64%	8.34%	4,763
AS7545	TPG-INTERNET-AP TPG Telecom Limited	20.09%	4.24%	4,076
AS9443	INTERNETPRIMUS-AS-AP Primus Telecommunications	2.96%	1.12%	1,251
AS133612	VODAFONE-AS-AP Vodafone Australia Pty Ltd	3.14%	1.53%	1,242
AS4764	WIDEBAND-AS-AP Aussie Broadband	42.63%	20.34%	821
AS135887	TELSTRA-BELONG-AP Telstra Corporation	1.04%	1.19%	670
AS10143	EXETEL-AS-AP Exetel Pty Ltd	92.72%	7.01%	371
AS4739	INTERNODE-AS Internode Pty Ltd	18.00%	24.40%	250
AS133414	FOXTEL-AS-AP Foxtel Management Pty Ltd	0.00%	1.69%	237
AS9310	MYREPUBLICNETS-AS-AP MYREPUBLIC PTY LTD	0.00%	1.50%	200
AS20473	AS-CHOOPA	84.72%	4.17%	144
AS24033	ACTIV8ME-AS-AP Australian Private Networks Pty Ltd	1.77%	0.00%	113
AS136994	SOUTHERNPHONE-AS-AP Southern Phone Company Ltd	92.94%	7.06%	85
AS38195	SUPERLOOP-AS-AP Superloop	27.06%	3.53%	85
AS18371	NCABLE-AP Neighbourhood Cable	3.90%	0.00%	77
AS58731	TELINTLSA-AS Telekomunikasi Indonesia International (T.L.) S.A.	42.47%	43.84%	73
AS7477	TEREDONN-AS-AP SkyMesh Pty Ltd	90.00%	10.00%	70
AS18390	SPIN-INTERNET-AP Spin Internet Service	14.29%	37.14%	70

1. DNSSEC - Registry Tasks

- DS record alongside delegation NS records
  - Potential use of CDS automated DS tracking from child zone
- Zone management
  - All-of-Zone signing or dynamic signing?
  - Sync of secondary servers
  - Using multiple secondary service providers and dynamic signing
- Key Management
  - Algorithm choice
  - Key rollovers
- Server Management
  - DNS Response Sizes will grow:
    - UDP configuration
    - TCP capacity
    - Large Packet Handling

1. Why Not DNSSEC?

- Validation is time-expensive
  - Unravel the delegation chain to reproduce the DS/DNSKEY linkages and validate them
  - Resolution is slower
  - Large responses can be a LOT slower if the DNS needs to kick into TCP to retrieve key records
- Its another point of vulnerability
  - Poor key management
  - Poor management of big DNS responses
- End users don’t validate!
  - All that effort and no actual protection for end users!

1. DNSSEC has no Use Case!

- DANE is a failure!
- As long as 75% of user site behind non–validating DNS resolver systems and 99.9% of users don’t directly validate DNS responses then we cannot place critical information in the DNS in a secure fashion and expect everyone to be protected by DNSSEC
- No natural market-based incentive for deployment
- Which means that Internet security is a failure as well!

2. DNS Privacy

- EVERYBODY peeks at the DNS
  - Because everything you do online is exposed to the DNS
  - And the DNS is promiscuously chatty – it over-exposes information
  - DNS query logs are collected, packaged and sold as user profile intel
- How can we make the DNS less chatty?

2. Privacy - Resolver Behaviour and Qname Minimisation

- Stop over-asking
  - Trim the query name to match the scope in the zone you are querying for
  - Terminal label query data is only exposed to the zone server that contains the terminal label
- Implementations are “approximate”
  - Qname minimisation typically is used for the first three labels and then full name is used thereafter

2. Not Privacy - EDNS(0)Client Subnet

- DNS does not expose the end user beyond the first recursive resolver
- But the DNS is used by a number of CDNs for content steering
- The rise of open recursive resolvers increased the distance between the user and the resolver which impacted the accuracy of the DNS-based content steering mechanisms
- Add a client subnet to the DNS query which is passed across recursive resolvers
  - Massive privacy leak
  - Negative impact on caching performance

2. Privacy - DNS Channel Encryption

- Stub to Recursive solutions
  - DNS over TLS (DoT)
    - Replaces UDP and TCP between stub to recursive with TLS/TCP
    - Supported on current Android platforms
    - Readily blocked (TCP port 853)
    - TLS 1.3 with ECH still some time away, so the SNI is still in the clear
    - Adds TCP overhead to recursive resolvers (reduces query capacity by around 2/3 at least)
    - Used as a platform tool
  - DNS over HTTPS (DoH)
    - Uses DNS with HTTP framing over TLS/TCP
    - Supported on Firefox browsers
    - Uses TCP port 443
    - Similar TCP overhewad
    - Used as an application tool

2. Privacy - DoT implications

- Not that many
  - Queries and responses are now in a cloaked TLS wrapper, but its little different to DNS as we knew it
- It probably won’t take off
  - It requires users fiddling with the knobs and users don’t fiddle on the whole

2. Privacy - DoH implications

- Allows an application to create its own DNS name resolution context
  - No visibility on the part of the user, the platform, other applications
  - Which implies that applications can operate in their own application-specific name space
- Server push
  - “resolverless DNS” where the application is ‘primed’ by a server with DNS response
- DoH is NOT secured content – its just secured transit
  - People can still lie in the DNS, but now the lie is all but invisible

2. Privacy - Recursive to Server Privacy

- Unclear why this is necessary or even useful
- Once you've shared all your DNS with Google, there is nothing left to see in the path from 8.8.8.8 to the auth servers!
- And if you are running your own recursive resolver then getting servers to deal with encrypted sessions seems like a out-of-all-proportion solution to the privacy problem

3 - others: IDNs

- Unicode has just one purpose, and that purpose is NOT to encode DNS labels!
  - The DNS is largely a “what you see is where you are going” model
  - It relies on the property that this is only one way to encode a visible sequence of displayed character glyphs
  - This is true in ascii
  - Its not true in Unicode – by design
- IDNs may be good for a laugh but it’s almost impossible to use in a secure and reliable manner

3 - others:"DNS Abuse"

- Moves to replicate the measures for self-regulation in the DNS industry that parallels self-regulation in the banking industry
  - But without oversight, without reporting, without legal framework of enforcement
  - And it doesn't work for the banking industry in any case!
- DNS registrars and registries are expected to use service contracts that define "acceptable use" and enforce these contracts in their (paying) customers
- Unlikely to be successful in reducing the levels of criminal activity in the Internet
- "Never mistake motion for progress" some Roman dude a couple of thousand years ago

3 - others: DNS Fragmentation

- A perennial topic in name circles
- DoH has added a new breath of life to this discussion by lifting the name space out from common infrastructure to application attribute

3 - others: DNS Flattening

- Noone really wants to be buried.down.deep.in.the.dns.underneath.some.one.elses.names
- They all want to be .myname
- The role of the hierarchies in the name space is under constant erosive pressure, and as the top level name space continues to be opened up the price premium of being in the top level drops
- It produces an increasing tension between the operators of the tlds and the root zone itself.

3 - others: It's not about us any more

- We have constructed a DNS name infrastructure because we humans communicate using ‘natural languages’
- But silicon is multiplying at far higher rates than human populations
- And the DNS is a universal signalling and tunnelling protocol
- So its pretty logical that the DNS becomes a command and control mechanism of devices, and the residual human use sector becomes an increasingly esoteric luxury good business
- The high level of manual handling of DNS names (and cost) during the DNS name lifecycle is unsustainable in the shift from human to automated use
- Which implies that the current “high touch” business models of the DNS are close to end-of-life and the new model of crypto-generated bulk names and fully automated instantiation and use are coming
- Think of the the DNS as the new HTML – it’s a command and control micro-code language and no longer a distributed database of words intended for human-use

3 - others: Not the DNS any more?

- Search terms as the new name space?
- Handles?
- Name Based Networking – the DNS as a name space but not a resolution protocol