(Further) Dispatches from the DNS Frontier

Keith Mitchell

DNS-OARC

NANOG71

San Jose, Oct 2017

OARC's Mission Statement

The Domain Name System Operations Analysis and Research Center (DNS-OARC) is a non-profit, membership organization that seeks to improve the security, stability, and understanding of the Internet's DNS infrastructure.

DNS-OARC's mission is to:

- *promote and conduct research with operational relevance through data collection and analysis*
- *offer useful services and tools*
- *build relationships among its community of members*
- *facilitate an environment where information can be shared responsibly*
- *enable knowledge transfer by organizing open workshops*
- *increase public awareness of the DNS's significance*

OARC Governance

- Independent legal entity
- Diverse member base (87)
- Financially self-supporting
  - ~$700k annual revenue ~= expenses
- Self-governing, neutral
- Elected Board reflecting member interests
- Contracted ~4FTE Executive Staff
- Volunteer workshop Programme Committee
- *501(c)3* non-profit public benefit corporation

2017-18 OARC Board

- David Lawrence, *Akamai*
- George Michaelson, *APNIC*
- Jacques Latour, *CIRA*
- Jaromir Talir, *CZ.NIC*
- Ondrej Sury, *ISC*
- Duane Wessels, *Verisign*

Bylaw amendment passed at AGM means future Board positions will be individuals, not Member organizations

OARC Workshops

- Sharing of latest operational and research knowledge, experiences, data analysis, best practices & insights
  - like NANOG, but with global scope and tight DNS focus
- 2 open workshops per year, 1½-2 days long
- Rotating co-location with RIPE / NANOG / ICANN / IETF
- OARC27 held here September 29/30th
  - **https://indico.dns-oarc.net/event/27/**
  - biggest yet, 176 registered attendees
- Seeking nominations for 2018 Programme Committee

OARC27 Hot Topics

- ICANN is postponing Root DNSSEC KSK rollover
- Interaction between DNS, Anycast, CDNs and BGP for traffic engineering
- Measuring and fixing IPv6 and DNSSEC deployment
- Abuse Prevention, Detection, Mitigation
- New Protocol Feature Deployment
- New & improved OARC DNS software tools
- **D**eath of **L**ookaside **V**alidation ☠

2017 Root KSK Rollover

- Although the DNSSEC zone-signing key (ZSK) for the root has been regularly rolled over many times, the key-signing key (KSK) has never been rolled since the root was signed in 2010
- ICANN & Verisign had planned carefully to do this on October 11th
- Late-breaking data suggests this might be a bad idea, so the rollover has been postponed for at least 3 months

2017 Root KSK Rollover

- RFC8145 is new DNS protocol feature which can signal back to root what trust anchors are in use
- Data since its recent deployment suggests as many as 5% are still running outdated statically-configured trust anchors
  - this is worrying, as the operators running this latest code ought to be the most clueful/careful
- Significant risk of breaking DNS resolution for visible proportion of Internet users
- Best course of action seems to be to pause, and gather more data to better understand what is going on here
  - data being gathered in other ways too, including OARC DITL collection
  - insight from ICANN's Recursive Resolver Testbed
- Please check your trust anchors and watch this space !

2017 Root KSK Rollover

- ICANN statement on postponement:
  - https://www.icann.org/news/announcement-2017-09-27-en
- Duane Wessels' presentation on RFC8145 data:
  - https://indico.dns-oarc.net/event/27/session/1/contribution/11/material/slides/0.pdf
- Matt Larson's presentation on rollover plans:
  - https://indico.dns-oarc.net/event/27/contribution/35/material/slides/0.pptx
- Video of this and discussion:
  - https://www.youtube.com/watch?v=zP2-IGTt3Fw?t=1h25m45s

Measuring DNSSEC Deployment

- DNSSEC deployment in the .gov domain is steady around 84%
  - mostly using SHA-1 and SHA-256 algorithms
  - some open questions around periodic salt changes and appliance use of NSEC3
- Rootcanary.org project quantifies the quality of DNSSEC validation in the wild
  - e.g. which crypto algorithms are working or not

DNS, CDNs, Anycast, Traffic Engineering

- LinkedIn case study of how effectively their use of internal and external CDNs scales their traffic and protects their infrastructure
- *RUMDNS* as tool for traffic steering, using Big Data to decide RData responses
- ISI's *Verfploeter* tool provides alternative approach to measuring B-root anycast catchments
  - passive vantage points using IPv4 pings
  - comparison against RIPE Atlas measurements
- PCH's use of *TSDB*/*Prometheus* telemetry on their public anycast resolver cloud

Abuse Prevention, Detection, Mitigation

- Experiences of running a live traffic attack exercise against a national ccTLD
- Measurement of deployment and effectiveness of Response Rate-Limiting
  - ~17% of zone servers exhibit rate-limiting behaviors
- Service monitoring at Salesforce
- Detecting DGA-based Botnets using DNS traffic
- Improving responsible reporting

DNS and IPv6 Migration

- How T-Mobile has used DNS64/NAT64/464XLAT to migrate its US mobile customers to IPv6
  - now 89% with tail of corner-cases
  - works well with Happy Eyeballs
  - techniques to detect and mitigate failure scenarios
- There remain a bunch of issues with MTU size and UDP fragmentation when using DNS over IPv6
  - *really* needs to be fixed for IPv6-only DNS to work
  - may need protocol transport fixes

Performance and Maintainability Improvements in BIND

- BIND legacy is a million lines of code since 9.0 in 1998 !
- Quantitative measurement of code complexity shows it is **very** high by any standards
- ISC has been analyzing and re-visiting performance and platform assumptions
- Various projects to break up and move functions, and address performance bottlenecks

Understanding Caching

- Analysis of caching of “core” domains
  - top 100 account for 67% of traffic; top 1000 ~= 90
  - overall cache hit rate ~91%
  - but drops to just 33% for DNSSEC
- Study of priming queries 2016 vs 2017
  - roughly 2kq/s seen at K-Root
  - 95% of these are not useful
  - most junk traffic generated by small number of outliers
  - need to distribute/cache root zone more aggressively !

Running Root on Loopback

- In theory there are a number of potential advantages from running your own local copy of the Root (RFC 7706)
  - but also challenges if vendors were to ship this as default
- CZ.NIC study compared RFC7706 against RFC8189 Aggressive Caching as an alternative approach
  - used testbed, and OARC's "*drool*" traffic generation tool
  - suggested RFC8189 may have some advantages
  - higher hit rate of >98% vs <94% for local root
  - stimulated a *lot* of discussion...

New Protocol Feature Deployment

- DNS Privacy Clients
  - DNS-over-TLS, RFC 7858
  - summary of available API, CLI, mobile clients
  - detail on Sinodun's *stubby* client
- Persistent DNS sessions (RFC7766)
- Performance impact of using CNAME chains vs ALIAS records

OARC Software Tools

- OARC's disparate set of DNS measurement, collection and testing tools had undergone major transformation over past year+½
- See https://www.dns-oarc.net/oarc/software
  - taken over ownership of DNSCAP, PacketQ
- New tools of note:
  - *drool* - a tool to replay DNS traffic
  - *CheckMyDNS* – integrated framework and UI for DNS resolver testing
- Open-source hosted at https://github.com/DNS-OARC with automated build and test environment

Lightning Talks

- .SE DNSSEC Algorithm Rollover
- Practical Metazones
- Understanding traffic sources seen at .NZ
- .*internal* – RFC1918 for names
- RFC5074 deprecation...

Death of Lookaside Validation ☠

- ISC's DLV (DNSSEC Lookaside Validation – RFC5074) was a public benefit service to help with initial DNSSEC deployment
  - stitched across holes in the signed delegation tree
  - arguably its time of usefulness has long since passed
  - but always lingering fear something might break if turned off...
- Turned off live on stage at OARC27 !
- Nothing broke !
- You might want to check for and clean up any dangling DLV config in your named.conf however...

Until Next Time...

- OARC27 Presentations Video
  - https://www.youtube.com/channel/UctgW_wIPdA_WBmMKX79JT4g/videos
  - most of OARC team are at NANOG71 ☺
- OARC28 will be in spring 2018
  - we're hoping for somewhere in the LAC region
- OARC29 will be co-located with RIPE76 and CENTR-Tech
  - Amsterdam, October 13-14th
- Thank you NANOG team for all your co-location help !

Questions ?

Why Become an OARC Member ?

- Access to and participation in the world's premier community of DNS technical experts
- Influence development of open tools and services to support your infrastructure operations
- Ability to share and analyze a unique dataset perspective into global DNS operations
- Use of community co-ordination resources to respond to incidents and threats
- Support a trusted neutral party free of vested interests in the DNS space