Notes from Bangkok

DNS OARC Workshop 30

ICANN DNS Symposium 2019

Dave Knight - dns-wg – RIPE 78

Notes from Bangkok

INTRO

- ICANN held a series of meetings in Bangkok this month
  - May 06-09 Global Domains Division Industry Summit
  - May 09 Registry Operations Workshop
  - May 10-11 DNS Symposium
- DNS OARC 30 was held in the same venue May 12-13

SUMMARY

- Each meeting lasted two days and there was a total of
  - 47 presentations
  - 5 lightning talks
  - 2 panel discussions
  - No talks duplicated there, or here at RIPE!

- There’s a lot to get through!

IDS

- **Keynote: 30 Years .TH | Prof. Kanchana**
  - » A history of the Internet in Thailand and specifically the .TH TLD

- **Keynote: DNS Stakeholders and Protocol Stability | David Dagon**
  - » The implications of the rearrangement of how DNS has traditionally worked.
  - » Recursives move from the ISP to the cloud, the stub moves to the application.
  - » ECS leaks and breaks anonymity networks. DoH is also going to reveal private information.
  - » DoH subverts ability to apply local policy in DNS.
  - » Changes to DNS have significant impact on privacy.

Notes from Bangkok

IDS

- **On the Implementation of the EU NIS Directive | Jim Reid**
  - European Union Network and Information Security Directive
  - We've spoken a lot about GDPR, this will likely impact us all too.
  - Aims to improve cybersecurity across the EU.
  - Covered the UK approach to NIS and raised concerns with their threshold based approach and how it applies to DNS.
  - A parked domain hoster is `big` by domain count, but those domains are
  - probably less important than BBC, which has few.

- **Client Side Debugging | Petr Špaček**
  - Lowering DNS resolver support costs
  - Sometimes resolution breaks and users call support.
  - Described automated diagnostics and tools built to ease this burden and
  - help users to perform self-diagnostics. Motivated by the Turris router,
  - but you can use it too!

Notes from Bangkok

IDS

- **DNS-Magnitude | Alexander Mayrhofer**
  - What is the magnitude of a domain? How popular is it?
  - How often is it queried, by how many resolvers?
  - This is a good input for machine learning algorithms.
  - Discussed how analysis was done and interesting things that came out of it.

- **DNS Resolver Centrality | Joao Damas**
  - Wanted an idea of how centralized resolution is around certain bits of infrastructure
  - Measurements with their ad based network, a small number of resolvers serve most
  - end users on the Internet. Will continue to provide stats on an ongoing basis.

- **New Security Framework for Home Gateways | Jacques Latour**
  - Motivated by the Dyn attack and the threat of IoT botnets
  - Started a project with various participating organizations to build a framework for a secure home gateway. Are working on a prototype, documentation and code are available

Notes from Bangkok

IDS

- **CrypTech Open Source HSM for DNSSEC | Phil Roberts**
  - » Described cryptech, an open source HSM and described how it can be used for DNSSEC
- **DNSSEC in Small Linux Devices | Fernando López**
  - » Described the challenges of managing e.g. firmware updates on IoT devices and the role for DNSSEC
- **ICANN Research Projects | Paul Hoffman**
  - » An overview of research projects going on at ICANN, e.g.
    - † trends in IPv6 deployment
    - † looking at conversations between recursives and root servers
    - † analysing latencies toward picking good placements for root server
    - † looking at how browsers interact with dns
    - † how popular is this domain?
    - † Identifier Technology Health Indicators!
    - † ..and other data collection efforts

Notes from Bangkok

IDS

- **Session: Future of KSK Rollover | Paul Hoffman**
  - Paul led a mic-line discussion of what future KSK Rolls should look like
  - We can have an even more useful discussion on the mail list:
  - https://mm.icann.org/mailman/listinfo/ksk-rollover

- **Keynote: Lessons Learnt from Avalanche | Stewart Garrick**
  - The work of the Shadowserver Foundation, a not for profit security organization
  - Avalanche was a botnet based malware delivery platform and money muling network.
  - Takedown involved a lot of DNS analysis and domain sinkholes.

- **Domain Reputation Lists as a Tool Against Domain Abuse | Joe Wein**
  - Described how they create URI blocklists and how to use them

- **Building DNS Firewalls With Response Policy Zones | Paul Vixie**
  - How to build a DNS firewall with RPZ, and why you'd want to

IDS

- **ICANN’s Domain Abuse Activity Reporting | Samaneh Tajalizadehkhoob**
  - » Described ICANN's system for reporting on domain registration and abuse data across TLD registries and registrars. Seeks to understand threat activity to help operators.
  - » Consumes data from many sources, does analysis and has APIs to make reporting available.

- **Anomaly Detection in DNS Traffic | Maciej Andziński**
  - » Looking for resolvers demonstrating unusual behaviour
  - » Doing statistical analysis of queries captured at CZ nameservers
  - » Exercising resolvers using RIPE Atlas

- **The Role of Domains and DNS in Large Scale Abuse | Carel Bitter**
  - » A look at the types of domains used to send spam, how their reputation is
  - » managed and DNS based authentication techniques used and abused.

IDS

- **On DoH Dilemma | Vittorio Bertola**
  - The impact of DNS over HTTPS. How DoH is different from traditional resolution.
  - Thoughts on the pros and cons of DoH given various scenarios. It's mostly bad.

- **A UK ISP View on DNS over HTTPS | Andrew Fidler**
  - Concerned by the subversion of local policy re content filtering, customer assistance redirects, on-net content caches, mandated filtering, etc
  - Call for collaboration with DoH implementors to work on these problems

- **Benefits and Hazards of Non-Local DNS Resolution | Paul Vixie**
  - Some history of how name resolution has worked on the Internet.
  - DoH is presented as an end run around local policy and the latest salvo in the war for the resolution path.

IDS

- **Panel: Applications Performing Their Own DNS Resolution | Paul Hoffman**
  - Discussion of various deployment scenarios
  - Paul Vixie spoke of a future RPZ which distributes policy as a bloom filter rather than a catalog
  - Warren Kumari gave an update on how Chrome will DoH

- **On the Recent DNS/IMAP Hijacking Campaign | Bill Woodcock**
  - A very candid and thorough explanation of a recent state-sponsored attack which PCH fell victim to.
- **Trends in TLD Abuse | Ralf Weber**
  - Description of how they gather DNS data from recursives and do analysis
  - Looking at that data for evidence of malicious domains across TLDs
- **DNS – A Phishing Chokepoint | Carel Bitter**
  - The domain is a good place to break phishing attacks
  - Looking at patterns in domain names and other metadata indicators to predict whichwill be used for phishing before we see a phish

DNS OARC

- **DNS Recursive Resolver Delegation Selection in the Wild | Dr. Kyle Schomp**
  - » Want to know how resolvers choose an authority to aid decision making around server deployments, etc
  - » Capture data at authority servers, measure rtt to querying resolvers, did analysis
  - » Most resolvers prefer low latency authority, some query every ns, some query only one
- **Developing a Testbed For Interactions Between Resolvers and the Root | Paul Hoffman**
  - » Building A test framework made out of lots of virtualbox VMs filled with nameservers to simulate behaviour of resolution at the root - code available
- **The Modality of Mortality in Domain Names | Paul Vixie**
  - » Set out to determine the quality of DNS content, are new domains mostly bad?
  - » Used passive dns infrastructure to look at domains from creation to death, how long, types of death.
  - » Some TLDs see significantly higher early death rates than others

DNS OARC

- **DNS Security: Past, Present, and Future (It’s Not Easy) | Ralf Weber**
  - A history of security issues in and around the DNS

- **Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path | Chaoyi Liu**
  - Investigated interception of dns queries in a numer of networks
  - Sending queries to public resolvers and checking to see who actually performs the query
  - Looked into what's going on when queries are intercepted

- **Multi-signer DNSSEC Models | Shumon Huque et al**
  - The traditional multi-provider model doesn't work well with widely used, but non-standard DNS features
  - DNSSEC with multiple providers where these features are used requires multiple signers
  - Approaches for this were described. There is a draft.

Notes from Bangkok

DNS OARC

- **A Story on Unsupported DNSSEC Algorithms | Matthijs Mekking**
  - We remove no longer supported DNSSEC algorithms from the nameserver, what goes wrong?
  - Tested many implementations of authority, resolver and signer.
  - Overall things look good, but some quirkiness and crashes were found.
- **Signing with offline KSK in Knot DNS 2.8 | Jaromír Talíř**
  - Some history on how CZ was signed and the challenges with the method
  - Described new improved process using Knot DNS signer
- **Seeing the effects of DNS Flag Day in action | Willem Toorop**
  - Presented some measurement taken around DNS Flag day to determine resolver uptake

DNS OARC

- **DNS flag day 2019 panel discussion | Petr Špaček et al.**
  - Some background presented on Flag Day and measurements taken
  - The panel discussed how they perceived Flag Day, lessons learned, and should we have another one?

- **The road to the Ultimate Stub-resolver | Ólafur Guðmundsson**
  - Some history of stub resolvers, concluding in the observation that they still give you very little
  - Want to make CDN services faster, need faster resolution
  - Described a new approach using dnsdist in front of a resolver farm which is faster and works better

- **OpenINTEL - Creating a "long-term memory" for the global DNS | Willem Toorop**
  - Wanted to measure lots of the global DNS, Unlike passiveDNS this uses active measurement
  - Some examples of using this to learn about DNSSEC deployment, DNS resilience, weird things seen in TXT records

DNS OARC

- **DNSKEY Flood what does that tell us about resolvers | Ray Bellis**
  - Work motivated by the KSK roll, will resolvers do 5011 correctly?
  - Looked at root server data for 8145 signalling and DNSKEY query behaviour

- **What part of “NO” is so hard to understand? | Geoff Huston**
  - Investigated surprising repeated queries seen during a different experiment
  - Using ads to query for things which don't exist, see more than half of tests generating more than one query
  - Described the various reasons why this is happening

- **Incentivizing the adoption of (new) standards | Maarten Wullink**
  - Motivated by the success of incentivized DNSSEC adoption in .nl
  - Want to repeat for IPv6, etc
  - Described how incentives for things are made in .nl domain pricing, and how adoption is measured

DNS OARC

- **Measures against cache poisoning attacks using IP fragmentation in DNS | Kazunori Fujiwara**
  - Described how IP fragmentation is used to attack pMTUd and the resolver cache
  - Proposed some methods to protect against this

- **Flamethrower: A flexible tool for DNS load and functional testing | Jan Včelák**
  - An alternative to dnsperf, TCP support! realistic query patterns!
  - Easily built into CI/CD
  - Code is available

- **Hyper-hyper-local root serving | Ray Bellis**
  - Ray built the tiniest, but very high performance nameserver for locally serving just the root zone

DNS OARC

- **respdiff: Regression and interoperability testing for the Internet | Petr Špaček**
  - » Describes the challenge of closing the gap between RFC compliance and making things work on the real Internet
  - » respdif! tool to generate and send queries to many nameservers than gather and compare responses
  - » Code is available

- **Lightning Talks**
  - » Identifier Technology Health Indicators | Paul Hoffman
  - » Oh, another DoH | Jaromír Talíř
  - » DNSCrypt | Brian Hartvigsen
  - » DNS Flag Day: kiwi flavour | Sebastian Castro
  - » Whither DANE? | Shumon Huque

LINKS

Agendas, slide decks and webcast archives at…

DNS OARC 30

https://indico.dns-oarc.net/event/31/timetable/

ICANN DNS Symposium

https://www.icann.org/ids

UPCOMING OARC WORKSHOPS

- **DNS OARC 31**
  - Austin, TX   10/31 - 11/01
  - https://indico.dns-oarc.net/event/32/

- **Moving to 3 meetings annually in 2020**
  - Adding a 1 day meeting in February
  - Meetings held ~ Feb / May / Oct
  - Co-locating with e.g. NANOG / RIPE / ICANN IDS