Rough Notes of the EDDI Meetup at DNS-OARC

San Francisco, 9th February 2020

Agenda

Link to a recording of part one: https://youtu.be/a-8Vp5ezsVo

- Agenda Bash
- Introductions (15m)
- EDDI Overview –Glenn Deen (5m)
- Deployments (40m)
    - Erik Bishop, Comcast (20m)
    - Nic Leymann, DT (20m)
- Tommy Jenson Microsoft (30m)
- Coffee Break (30min)

Link to a recording of part two: https://m.youtube.com/watch?v=l6CJj6H2z-U

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Introductions

- Thanks to DNS-OARC for all their help and support in allowing the meeting to take place, facilitate the live streaming
- The anti-trust guidelines were displayed and highlighted – see also https://www.encrypted-dns.org/legal-privacy
- Glenn reminded people to be kind and respectful

EDDI Overview

(See GitHub for the slides - https://github.com/Encrypted-DNS-Deployment-Initiative/Reference/blob/master/meetings/2.9.20-DNS-OARC32-San%20Francisco/Agenda%20EDDI%202.9.20.pdf)

The goal of EDDI is to ensure the smooth introduction and reliable operation at scale of DNS encryption operation. It overlaps with the IETF list on technical issues but extends into policy issues too, will also develop best practices for deployment. All interactions are public.

Deployments: Nic Leymann, DT

Nic summarized the key components of the Nic Leymann DNS deployment

- It spans two platforms, one each for its fixed and mobile networks.
- Running at approximately 2.5m requests per second, around 90% of the total volume from the DT network from non-Enterprise customers
- Currently testing DoT and DoH, with employees initially
- There is more DoT traffic on the mobile network as Android devices will use it
- DoH is only enabled on a subset of servers at present
- The lack of an automatic discovery mechanism for DoH resolver is likely to limit its adoption to more tech-capable users
- Are preparing the whole DNS platform to support DoT and DOH but it's early days
- Need to produce an updated policy document

Question responses

- Need to decide how to handle scenarios such as coffee shop and how to educate customers regarding which DNS will be in operation
- Access to the DT DoH server? It's currently an open resolver.
- How does the DT OSS align with DNS provision, is this being tested too?
- What code base is being used? DNS Dist and Power DNS, no problems to date but still pretty low volumes. Expects some learning around TCP optimization.

Deployments: Erik Bishop, Comcast

- Comcast was the first US ISP to be added to the Microsoft DoH list
- Sees a total of around 600 billion queries per day on DNS
- Launched DoH and DoT trials in October 2019, has just completed phase 1 of the trial
- Seeing around 3,000 queries per second on the server side so far
- Expects to have a production live service in Q2 2020

Question responses

- Thoughts about client subnet deployment? Still learning, to cover this in due course after evaluation of the early data
- The key focus in phase 1 of the trial was functionality, learning about loading etc
- Measurements on connection re-use etc? More a focus for phase 2

Tommy Jensen, Microsoft

See GitHub for Tommy's slides - https://github.com/Encrypted-DNS-Deployment-Initiative/Reference/blob/master/meetings/2.9.20-DNS-OARC32-San%20Francisco/Microsoft%20Windows%20DoH%20client.pdf

- Summarised the Windows DoH design principles
- The first milestone will be auto-promotion, which is not intended to be a long-term solution (ie it can be replaced when a discovery mechanism is available)
- If encrypted DNS is selected for a server, it will not revert to Do53 if DoH is not available
- May still add support for DoT but DoH is a better fit for a number of scenarios
- The DoH behavior is per server so different servers can be configured differently – or they could all be configured for DOH only
- Support for CPE-based deployments is to be determined, potentially through the IETF working group

- Release timeline? To be confirmed
- No option to configure a custom resolver yet
- Currently the auto-promotion is binary – ie it's on for everyone on off for everyone that uses a specific resolver
- Still thinking about user dialogue
- Any thoughts on how to communicate about DNS within the security awareness scheme? It may happen over time but there's a long way to go, are open to ideas
- How to be certain about the security of the auto-promote list? Microsoft will maintain the list manually to ensure its security in the period before discovery is addressed.
- Anything on timelines? The DoH client has already had some preliminary testing but nothing yet on timings, it will however be disabled by default.
- Working with captive portals? This remains a challenge, are looking for solutions.
- By implementing DoH in the o/s, the hope is that application developers will not see the need to implement their own DNS stack and controls
- At present it will not be possible for enterprises to support deployment of their own DoH resolvers within Windows – hoping that this will come form the IETF working group
- Will DoH be deployed on the Microsoft Active Directory servers? Doesn't believe that there are plans to deploy at present.

Early AoB - Glenn

1. See the following information from BT on its trial open DoH resolvers
    - Available as a trial service at https://doh.bt.com/dns-query/ with test page at http://splashpage.doh.bt.com
    - Built on and working with OpenXchange / PowerDNS.
    - Supporting only IPv4 and RFC8484 implementation.
    - Shortly planning to enable DNSSEC validation.

    - Others are encouraged to use the trial service whilst it's available.

2. See the GitHub 30th January for a presentation of early test results of DoH resolvers by BT - https://github.com/Encrypted-DNS-Deployment-Initiative/Reference/blob/master/meetings/1.30.20-London/EDDI%20Jan%20Update%20on%20BT%20DoH%20trials%20Issue%201%20300120.pdf

IETF Activity

See slides 15-16 for a summary of the draft working group charter etc at https://github.com/Encrypted-DNS-Deployment-Initiative/Reference/blob/master/meetings/2.9.20-DNS-OARC32-San%20Francisco/Agenda%20EDDI%202.9.20.pdf

- Adaptive DNS Discovery working group draft charter displayed, is now out for public comment from the IESG over the next two weeks - see https://mailarchive.ietf.org/arch/msg/add/4MjK0HQhbDncUCCG8yChIapyBpA
- It will be discussed by the IESG on 20th February
- Glenn Deen and David Lawrence have been proposed as the working group co-chairs

- The working group is intended to focus on resolver discovery and resolver selection as well as the provision of informational documents covering potential implementations for different client-side use cases
- There's an expectation of a working group meeting at IETF 107 in Vancouver (if this doesn't happen there should at least be another BoF at IETF 107)

Use Cases and Taxonomy

- Several decades of creative operational uses of DNS need capturing …. contribute yours!
- GitHub: https://github.com/Encrypted-DNS-Deployment-Initiative/Use-Cases
- Taxonomy: https://github.com/Encrypted-DNS-Deployment-Initiative/Use-Cases/blob/master/Taxonomy.md
- Format: Template based on RFC7744 to be posted in the GitHub repository

- Please help to document use cases on GitHub.
- How granular? Both high level and more granular, important to start and then others can contribute
- The next EDDI meeting in London will brainstorm use cases, then share these more widely to get other contributions
- Comments on the taxonomy on GitHub also appreciated

Next Steps and Future Meetups

Meetups

- London –March 2, 2020
- IETF107 Vancouver side meeting March 22-26
- IETF108 Madrid
- More to come in 2020

  Past meetings & materials: https://github.com/Encrypted-DNS-Deployment-Initiative/Reference

Offers to host future meetings most welcome.
Possible

AoB

- Important to keep communications open

EDDI Links

- EDDI: https://www.encrypted-dns.org/
- Mailing List: https://www.encrypted-dns.org/mailing-list
- Archive: http://lists.encrypted-dns.org/scripts/waENCDNS.exe?A0=ENCRYPTED-DNS
- GitHub: https://github.com/Encrypted-DNS-Deployment-Initiative