IETF: DoH Discovery & Privacy I-Ds Initial thoughts to aid EDDI discussions

EDDI London 1st November 2019 meeting

Andy Fidler, Chris Box, Dave Cleland

IETF Encrypted DNS discovery and privacy related I-Ds

- Presently there are seven I-Ds covering Encrypted DNS discovery, privacy and policy aspects, spread across four different IETF groups.

- DNS Ops:
  https://tools.ietf.org/html/draft-ietf-dnsop-resolver-information-00

- DPRIVE:
  https://tools.ietf.org/html/draft-pauly-dprive-adaptive-dns-privacy
  https://tools.ietf.org/html/draft-pauly-dprive-oblivious-doh
  https://tools.ietf.org/html/draft-reddy-dprive-dprive-privacy-policy-00#section-9
  https://tools.ietf.org/html/draft-reddy-dprive-bootstrap-dns-server-05

- DoH:
  https://tools.ietf.org/html/draft-peterson-doh-dhcp-01

- ADD:
  https://datatracker.ietf.org/doc/draft-grover-add-policy-detection/

- Some of the draft IDs share common approaches, others appear not to.

- It would be beneficial to have some alignment and consolidation discussions at IETF 106 in Singapore.

Overall early BT comments on current draft I-Ds:

- Consideration needs to be given to how Encrypted DNS discovery will work in the home environment where many ISPs deploy stub resolvers in Customer Premise Equipment (CPE) / hubs.
    - For example for BT Broadband, we presently deploy a stub resolver in our Smart hubs. The Smart Hub is aware of the BT DNS recursive resolver public IP address via RADIUS. However devices connected to the hub will only see the private IP address of hub stub resolver and get advised off this via DHCP, e.g. the hub uses 192.168.1.254 as the stub address for DNS. Hence browsers won't be able to determine who's providing the DNS resolution and their DoH capabilities.
    - Also are there scenarios to consider around CPE having DoH capabilities and if so what certificate provisioning challenges will exist here?
- We welcome I-D's planning to detect the presence of existing ISP content filtering / malware and Enterprise policies. However detection is only half the answer, what about best practice around policy, customer experience and informed consent implementation aspects?
    - Plus clarity is needed on whether canary domain detection will only apply in case of default ON, what about manual entries?
    - Will discovery be one-time or on-going and what about context awareness – home, work and public wifi environments?
- Discovery and policy approaches need to considered layered client options – e.g. option for customers to use their ISP DoH servers when connected to ISP networks, but when on 3rd party wi-fi networks have the option to use 3rd party DoH resolvers if their ISP does not provide an open DoH capability.
- I-Ds should consider the impact on existing ISP on-net content caching, particular in terms of ECS support.
- I-Ds should consider impact on load balancing, TLS session / key management, resilience and disaster recovery.

Early comments on draft-ietf-dnsop-resolver-information-00

- Focusses on DNS resolver functionality discovery – e.g. support for DoH, DoT, DNSSEC.
- Based on information returned as a JSON object.
- Appears not to cover subsequent client / browser policy behaviour based on DoH information.
- Appears not to cover gathering information on stub/resolver privacy policies.
- Appears not to cover authenticity of stub / resolver response.

Early comments on draft-pauly-dprive-adaptive-dns-privacy-00 & draft-pauly-dprive-oblivious-doh

- Defines this resolution algorithm, to be used in priority order, for resolving a particular hostname X:

  1. Exclusive Direct Resolver, such as a resolver provisioned by a VPN, with domain rules that include X.
  2. Direct Resolver, such as a local router, with domain rules that are known to be authoritative for X.
  3. DoH Servers that have been designated by X's domain. This is likely to mean the DoH server belonging to the CDN.
  4. Oblivious DoH queries using multiple DoH Servers. If this resolution fails, Privacy-Sensitive Connections will fail.
  5. The default Direct Resolver, generally the resolver provisioned by the local router, is used as the last resort.

- Uses Web Provisioning Domain (WebPvD): a JSON object describing resolver information. It can be retrieved from a DoH server, and included in Router Advertisements. For clients with both wifi and mobile connections, there could be one PvD for each interface.

- Oblivious DoH allows client IP addresses to be disassociated from queries via proxying. Will this have any impacts on load-balancing and TLS session management? It will certainly add latency, but how much is an open question.

- Discourages use of ECS feature for privacy reasons but acknowledges that sharing subnet information may result in better targeted DNS resolution. Could the answer here be to start using the client prefix option already defined in RFCs to allow customers to chose the balance between privacy and performance? Or a way o automatically chose an ECS prefix length that's appropriate to the user's preferences and activity.

Early comments on draft-reddy-dprive-dprive-privacy-policy-00

- Mechanism for DNS server to communicate its privacy policy to a client.
- Based on JSON response so seems to be compatible with dnsop-resolver-information.
- Response is cryptographically signed so covers off authenticity angle, but how will this work at the application layer and what about trust anchors?
- But appears not to consider how clients will use this information.

Early comments on draft-reddy-dprive-bootstrap-dns-server-05

- Mechanism for automatically bootstrapping endpoints (hosts, hubs) to discover and authenticate – DoT and DoH servers provided by a local network.
- Also considers bootstrapping for IoT devices.
- How does this align with other I-Ds?

Early comments on draft-peterson-doh-dhcp-01

- DHCP option and router advertisement extension to inform clients of presence of a DoH server.
- Different to dnsop-resolver-information approach.
- Appears not to include in this draft security / authenticity aspects, e.g. attack could inject DHCP messages.

Early comments on draft-grover-add-policy-detection

- Specifies behaviour expected from DNS with regard to DNS queries for special-use domain name.
- Use of reserved canary domains to determine presence of existing ISP based content filtering or enterprise policies.
- If policy exists the resolver must return NXDOMAIN, if policy not present DNS look up will be successful.
- I-D appears not to cover how clients / browsers will use this information to make policy / DoH enablement decisions.
- BT welcomes I-D's planning to detect the presence of existing ISP content filtering / malware and Enterprise policies.
- However detection is only half the answer, what about best practice around policy, customer experience and informed consent implementation aspects?
- Plus clarity is needed on whether canary domain detection will only apply in case of default ON, what about manual entries?

Conclusion & next steps

- Presently we have 7 different I-Ds tackling aspects around Encrypted DNS discovery, privacy and policy across 4 IETF working groups.
- It appears that there is not one I-D which addresses all aspects – discovery, authenticity, privacy and policy.
- Encourage EDDI members to review the current drafts and discuss via EDDI mail reflector / Git hub.
- Should the IETF pause the various encrypted DNS discovery work until it is sorted out which single WG has responsibility for the work?
- Should the proposed IETF ABCD BoF / WG have in its charter the scope to define a single complete encrypted DNS discovery protocol, covering the following aspects:
    - Encrypted DNS discovery with context awareness across broadband, mobile, public wifi and enterprise networks.
    - Ability to verify the authenticity of Encrypted DNS resolvers.
    - Ability to determine the privacy policies of Encrypted DNS resolvers.
    - Ability to detect the presence of existing ISP content filtering and enterprise policies.
    - Ability for clients/customers to make informed decisions around choice of Encrypted DNS resolvers.
    - Ability for clients to support context awareness options e.g. Resolver A for broadband and Resolver B for public wifi.
    - Applicable to browsers and going forward CPE, mobile applications and IoT devices.