ADD
Internet-Draft
Intended status: Informational
Expires: January 14, 2021

A. Campling
419 Consulting Limited
N. Kowalewski
Deutsche Telekom
G. Scalone
Vodafone
C. Box
BT Group
A. Winfield
Sky

July 13, 2020

Practical Observations from Encrypted DNS Deployments by Network Operators
draft-campling-operator-observations-00

Abstract

The following document includes observations regarding a variety of implementations of recursive DNS capabilities that are important to network operators in terms of delivering DNS services to their (several tens of millions of) customers. It highlights some of the challenges that need to be addressed to allow the widespread adoption of encrypted DNS by the end-users of network operators.

The information is intended to aid the development of discovery mechanisms for protocols such as DNS-over-HTTPS. It clearly defines problems that need technical solutions to allow the deployment of encrypted DNS by the largest number of operators to the largest number of users in the shortest possible timeframe with little or no disruption to the user experience.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 14, 2021.

1. Introduction

The IETF has developed many protocols to improve the security and reliability of DNS over UDP or TCP (Do53) [RFC1035] including DNS over TLS (DoT) [RFC7858], DNS over HTTPS (DoH) [RFC8484] and DNS Security Extensions (DNSSEC) [RFC2535]. To enable the broadest adoption of these technologies, there are issues for consideration of any discovery solutions that are proposed to the Adaptive DNS Discovery [ADD] working group.

Many network operators, including Internet Service Providers (ISPs), whether using fixed or mobile networks, would like to ensure that their encrypted DNS services can be seamlessly discovered and used by applications and operating systems that support encrypted DNS, particularly DoH, in order that encrypted DNS can be deployed to the widest possible community of users. They would particularly like to ensure that any proposed DNS discovery mechanisms take into account ISP use-cases such as DNS forwarders on CPE (Customer Premises Equipment or routers), the use of DNS for CDNs (Content Delivery Networks) with local content caches and the non-public nature of most ISP DNS services.

This document has taken observations and experiences from a number of network operators that have been actively working on adding support for encrypted DNS to their networks. It is intended to make clear the requirements needed by any discovery mechanism developed by the ADD group. It collates and succinctly describes common problems faced by existing stakeholders in adopting encrypted DNS mechanisms.

This document also presents some background information that is relevant to describing the issues and explains concerns around

current proposed solutions. It should also be noted that, in many European countries, some regulations are specific to ISPs. One such requirement is that their customers should be able to connect to the Internet with any home router of their choice even if a router is provided by the ISP as part of its service. Therefore new proocols cannot be accommodated simply by requiring ISP customers to upgrade their routers.

2. Rationale

This document is intended provide information to aid interested parties in developing discovery mechanisms for protocols such as DoH to allow their adoption with minimal disruption to the end user experience, maximising the number of users that can enjoy an easy upgrade path towards DNS encryption.

The information provided will help interested paries develop discovery mechanisms that avoid the unnecessary exclusion of the majority of customers of a significant number of ISPs (including the major ones in Europe that serve several tens of millions of customers) from easy access to this new technology using the secure by design, same-provider auto-upgrade mechanisms.

Such discovery choices will ensure that easy access to encrypted DNS is not dependent on the Internet access network architecture and on the ease of upgrade of any CPE. In addition, it will ensure that users are not forced to change their DNS resolver to a third party, potentially via manual configuration by the user, possibly losing functionality in the process.

3. The 'Same Provider Auto-Upgrade' Model

Both Google Chrome and Microsoft Windows (and perhaps other client software in the future) currently deploy encrypted DNS through a 'same provider auto-upgrade' (SPAU) model. This approach results in the client not needing to prompt the user to change to a different resolver operator to enjoy an encrypted connection. Instead the client will rather try to determine whether an encrypted channel exists for communication with the same resolver operator that the user currently employs for unencrypted DNS resolution. If such a channel can be found, the client will automatically upgrade the connection from the original unencrypted one to the new encrypted one; otherwise, the client will continue sending DNS queries unencrypted.

The current implementation of this model is as follows:

- Out of band, the client software vendor discovers ISPs running DoH services (in the case of Google Chrome, ISPs will more likely apply for inclusion through Google's announced process). The vendor records the existing (Do53) resolver IP addresses, and adds them to a hard-wired table that maps those existing Do53 IP addresses to the DoH service that the vendor discovered to be associated with those resolver IPs.

- When the client starts for the first time, and thereafter whenever it detects a network change, it checks the resolver configuration of the local host. If the configured resolver matches one of the IPs listed in the above table, the client auto-upgrades to use the DoH service instead.

The above method ensures that users are only upgraded to DoH when the vendor is sure that the DoH service is the same service as the Do53 service already used.

4. The Problem with Auto-Upgrade and Forwarders

Automatic upgrades that rely upon the user device being able to know and compare the address of the resolver that is serving the device can fail in some home network environments where the CPE is acting as a DNS proxy. To do this, the CPE will run software like DNSMASQ which acts as a proxy between the client and the DNS resolver, also providing DHCP services and performing DNS caching as well as forwarding. This is often paired with a home network architecture that uses RFC1918 [RFC1918] private IP addresses.

In circumstances where private IP addresses are used, any auto-upgrade on the user device that compares the IP address of the device's DNS resolver against a list of known public DNS resolvers will fail because the client DNS resolver is a RFC1918 private address of the CPE device and not the public address of the actual DNS resolver operated by the network operator.

As can be seen, the existing SPAU model doesn't work with the DNS-forwarder, private IP approach commonly used by network operators. Given that this approach allows for the implementation of the best privacy practices and best latency/engineering reqirements, it shouldn't change, therefore the SPAU model needs to be adapted to work with it.

5. Why DNS Discovery Needs to Support Forwarders

5.1. Loss of Functionality if CPE Doesn't Support DNS Forwarders

If the CPE is upgraded to announce the public resolver to clients, the following functionality will be lost

- Caching/Proxy on the CPE - This leads to more load on the ISP's DNS platform because every client talks directly to the public resolvers (not only the clients which are auto-upgraded to DoH but also all other clients).

- Local DNS routing and resilience - Some deployments segment the user base into regions, with CPE in each region receiving a different IPv4 and IPv6 address for the DNS server, improving latency and load balancing, as well as helping with cyber resilience compared to a single address for a typical anycast implementation.

- Addressing local clients via their names - Often the CPE assigns the name configured to a client to the client's IP address on the CPE (for example, if the hostname is set to 'myhost' on a home network to reach this host on that network under that name). This will not work if the clients communicate directly with a resolver in the carrier network nor would it for auto-upgraded clients because, even if they fallback to Do53, they will still ask a resolver in the carrier network and not the CPE - and in both cases private network details will be leaked.

- The CPE is the only network element that is aware of the local network topology. If the local network information is lost it is not possible to differentiate devices. The Discovery mechanism alone is not enough to solve this use case as additional logic is required on the DoH server to send back the request to the CPE. By using EDNS0 (Extension Mechanisms for DNS) [RFC2671] it is possible for a client running on the CPE to pass EDNS0 information to the ISP's DNS and provide, to the opted-in customers, information on the client that performed the request. This in turn allows the execution, for example, of parental controls on devices belonging to children (there are various ways of doing this that preserves privacy, for example by providing information only about the required filtering profile or by providing only a locally generated ID to distinguish between devices without necessarily identifying them).

- Similar to the above use-case, some CPE can be configured to perform filtering directly, relying on a DNS forwarder's ability to intercept and modify DNS queries to do so. Moving queries to the network DoH server removes this capability, allowing more data

to leave the local network, even if a resolver is available to perform similar filtering.

5.2. Why Not Just Upgrade the CPE to Stop Forwarding?

It may seem easier to simply ignore the loss of functionality detailed above and just upgrade the CPE to stop DNS forwarding. However, such a software upgrade programme, or even the wholesale replacement of CPE, is not without its own challenges.

The following is based on information from various large European ISPs, all of which use a DNS forwarder in their CPE. This configuration applies to operators in multiple countries, each of which has many millions of customers, so is a fair reflection of the envirnment in which any DNS discovery process needs to operate.

- Non-standard CPE - Whilst many ISPs provide their customers with CPE, some customers will elect to use alternative equipment which will not accept software upgrades

- Multiple hardware variants - ISPs typically endeavour to maintain support for legacy CPE. Upgrading the CPE software therefore requires complex and lengthy quality assurance processes to accommodate the many device variants, with some of the larger ISPs having 20-30 variants of devices.

- Large, dispersed customer bases - Cycle times to replace CPE are lengthy due to the costs and numbers involved, and the outcome of any upgrade programme is uncertain due to the aversion of some customers to replace their existing equipment

In summary, the timeframe for non-critical software updates of ISP-supplied CPE can be lengthy. In addition, any such upgrades will only apply to the ISP-supplied CPE so will at best only ever reach between 60-80% of the customer base for many of the largest European ISPs. A replacement programme will also take an extended period without a guaranteed outcome, and that is without considering the cost.

5.3. The Advantage of Supporting Forwarding

The above is intended to illustrate why it is more effective to ensure that DNS discovery methods, including those that support the SPAU model, are developed that work with the hardware and software environments in common use by network operators.

6. Alternative Solutions

Some may be tempted to suggest that the simplest solution to address the issues noted in this document would be for users to connect to global DNS resolvers. Aside from the loss of functionality and significant reduction in user choice that this would imply, it would also result in the further, forced, centralisation of Internet infrastructure, a policy outcome which is out of scope for the ADD working group. It would also, of course, result in the personal data of very large numbers of users to shared with additional parties simply to provide encrypted DNS functionality.

A better approach would be to address the underlying issues so that client software is able to auto-discover and connect to encrypted resolvers on existing network wherever these are available, giving users a seamless upgrade, maintaining full functionality and maximising choice.

7. Extending the Use Case

TO DO

The information in this document is largely based on input from a number of large European network operators, augmented with knowledge of the operations of others, mainly in Europe but with some from North America. It would be beneficial to extend this document with data from additional ISPs to complement the existing content and also to extend the narrative with examples of additional working practices relating to the operation of DNS where possible. This would provide valuable information to inform the development of DNS discovery approaches that will benefit a far broader set of users than would otherwise be possible.

To this end, additional contributions are welcomed as these would ensure that the document is fully representative of the significant use cases globally.

8. Acknowledgements

In addition to the authors, this document is the product of an informal group of experts including the following people:

Andy Fidler, BT plc

Neil Cook, Open-Xchange

Nic Leymann, Deutsche Telekom

Ralf Weber, Akamai

Vittorio Bertola, Open-Xchange

9. Informative References

[ADD] IETF, "Adaptive DNS Discovery (ADD) Working Group", February 2020, <https://datatracker.ietf.org/wg/add/about/>.

[EDDI] EDDI, "Encrypted DNS Deployment Initiative", July 2020, <https://www.encrypted-dns.org/>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[RFC2535] Eastlake 3rd, D., "Domain Name System Security Extensions", RFC 2535, DOI 10.17487/RFC2535, March 1999, <https://www.rfc-editor.org/info/rfc2535>.

[RFC2671] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, DOI 10.17487/RFC2671, August 1999, <https://www.rfc-editor.org/info/rfc2671>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

Authors' Addresses

Andrew J Campling
419 Consulting Limited

Email: Andrew.Campling@419.Consulting
URI: https://www.419.Consulting/

Normen B Kowalewski
Deutsche Telekom

Email: Normen.Kowalewski@Telecom.DE
URI: https://www.Telecom.DE/

Gianpaolo A Scalone
Vodafone

Email: Gianpaolo-Angelo.Scalone@Vodafone.Com
URI: https://www.Vodafone.Com/

Chris Box
BT Group

Email: Chris.Box@BT.Com
URI: https://www.BT.Com/

Alister Winfield
Sky

Email: Alister.Winfield@Sky.UK
URI: https://www.Sky.Com/