SUBJECT: DoH public comment
FROM: Martin Hunek <[redacted]
TO: [redacted]
DATE: 09/01/2021 00:52
ATTACHMENTS (20210109-005235-0000060): [redacted]

Good afternoon,

I would like to provide a comment on DNS over HTTPS RFC8484 (later DoH) implementation in Mozilla Firefox.

I work as Network/System administrator for campus network and also for two regional ISPs.

First of all let me say that I do not have any reservations against security of DoH protocol itself. What is, let say, problematic is way it is used in Mozilla Firefox. By introduction of third party DoH providers you are introducing data about users DNS queries to a third party whom would not have access to it previously. To make a matter worst, by having direct connection made from browser to DoH provider, you make such queries directly identifiable with browser instance. In contrast, in classical plain-text DNS, the query is identifiable with application only inside the machine, with machine only inside network segment between client machine and first DNS resolver (either caching or recursive). After that query is identifiable just with that network segment and with CGNAT in public internet it is either identifiable with shared IP or more probably just with ISP.

You may say that DoH is more secure because it encrypts content of DNS query and you would be right. However if you are connected on same network segment and you forces network equipment to give you a copy of packets, you are capable of tracking users in that segment even without DNS queries. Same goes for ISP. As ISP in my country (Czech Republic), I'm required by law to collect connections' metadata - flow data. So I know source address, destination address and source and destination port. If I want I can collect also packet size, frequency of flow, TTL etc. This will give me quite a picture of what traffic it is and what user agent / operating system is in use by client.

So ones again as ISP I know:
- Who is communicating in my network. (CPE specific)
- Who he/she is communicating with.
- Which type of service it is used.
- I can guess which operating system is being used on both ends.

If you want to hide this kind of information from me (as ISP), you had to use some kind of VPN with encapsulation and encryption. And even inside it you had to transfer padded data and also some random flows.

Long story short, even without DNS data I know (had to) with whom client is communicating. Also please be advised that when the internet shifts to IPv6, there will be plenty addresses for every single service to have its unique address. This contrasts with current CGNAT IPv4 world in which services are sharing common address. If so, specificity of tracking by flow data would became even higher, so less I need clients DNS queries to identify his/her browsing habits.

Now we can look at it by DoH providers' point of view:
So far it has not any information about traffic which is not addressed to it. But after introduction of DoH, it will get every single query in non-interrupted session. This means that all queries can be grouped as single user, or even more specific - single application instance.

Even as ISP, I can't do such specific grouping. I can easily identify/group queries coming from single CPE (router). But it usually has caching resolver in it, so I don't see every query from every machine in customer network. Even more, I can't tell which PC in customer network initiated query or which application has done it.

Now form the users point of view:
Until DoH, user knew that its ISP could have his aggregated DNS queries and that it can be visible inside his/her network. But he/she has contractual agreement with ISP and most likely both reside under the same jurisdiction. At least in Europe ISP cannot sell collected without consent given by user (thanks to GDPR).

From DoH on, user still knows that ISP would have flow data, but also that some DoH provider with whom user doesn't have contractual agreement and which might be under different jurisdiction, will get every single non-aggregated DNS query. This DoH still cannot sell such information, at least because of TRR policy (contract with Mozilla), but it would have information which it would not have prior DoH. We might or might not trust that Cloudflare, Google and others would not abuse this information for their own business, however if there would came some government agency with lawful order to give them users data and to be quiet about it, would they get the data? How it helps user privacy then?

Don't get me wrong, I think that there can be use-case when it can be beneficial. There might be countries which abuses DNS blocking to block access to some domains, and in that case this might help. However in my country when there was a crusade against internet gambling government agreed upon that DNS blocking is sufficient to ISP to do. But if that everybody would use third party DoH resolver without blocking, than the government would force us to use deep packet inspection or to block whole IP addresses. This would not be as easy to bypass and to cheap to do. This way it would hurt both users and ISPs.

Now for questions:
I would not comment on TRR, I'm not lawyer.

Privacy and security:
2: I can use DNS data to detect malware node by monitoring queries. Maybe DoH provider should be allowed to do the same (at least for well-known malware domains).

3: Almost useless. I can hide data processing from any auditor, only thing I need is packet duplication on any switch in the way. But of coarse, this at least force them to hide it better.

4: Government can force DoH provider to remain silent about monitoring which are currently done. Contract is less then law under which jurisdiction DoH provider is. Again even more useless than previous point.

Online Safety:
As ISP I'm required to provide network neutrality, so I cannot block or provide any advantage over another site that it is not agreed with user. Same should be the case with DoH provider. For parental control or company policy, enabling/disabling DoH in Firefox should require administrative privileges. Reasoning is simple. If I'm under parental control, if it should work, I should not be able to change system DNS resolver. Same should be the case for DoH in Firefox. If I'm root/Administrator, then I should be able to tell which resolver should be used. If I'm not than it is up to sysadmin or netadmin to tell.

1: OK

2: From top of my head: DoH provider can block its competitor. For example Google might block Yahoo. It is not DNS providers' (of any kind) job to block any domain - it should be neutral.

3: IP based blocking, however this might harm other services on same IP address. DNS blocking is the easiest, the most specific way for ISP. You as a browser vendor may use your own list of pages or you may standardize HTML header to indicate non-family friendly site.

4: Not a lawyer.

5: Don't use DNS for that. Make a list and check against it when family-friendly blacklist is enabled. Again require administrative privileges do toggle it on/off.

Ecosystem:
Huge problem with DoH. In both ISPs I'm working for, we use split-horizon DNS. This means that for internal users we give RFC1918 replies, for outside users we provide our public address and without some internal domains. When you introduce third-party DNS resolver to this mix, you will cripple systems and services which are not publicly accessible. In our case IP authentication for IPTV services which had to be made before CGNAT. For some time we even had our public range not accessible from inside of our network. This means that if third-party resolver is used, all internal services would not be accessible. This could be also used as policy enforcement to users not to use third party resolvers.

1: Not in most of the Europe (EU). We don't have huge DNS blacklists and classical DNS provide sufficient anonymity outside of local network segment.

2: Government block lists. However it is not huge problem in EU.

3: DoH is not only one secure DNS protocol out there. It is useful for users under heavy DNS based censorship. However from ISP point of view it is better to support DNS-over-TLS (RFC7858) because it make more sense. It does have lower overhead and it makes no sense to ISP to hide DNS traffic in HTTPS. Also it is not affected by lack of detection method in DoH URL and it can and already is in some system resolvers supported. I do support DoT on our resolvers, I'm not so sure with DoH. I know that it is more appealing for web browser vendor, but it is not so hot for ISP.

4: In very specific. In public hotspot case it can help very slightly. For "complete security" you need some sort of VPN. DoH is only useful for users under heavy DNS based censorship (government or private company policy). For other use cases, it will either not help significantly or by introducing third party to communication it will hurt user privacy.

5: Yes. We use NAT64/DNS64 in our network and by enabling DoH by third-party provider, user would not be provided with DNS64 and because of that it would loose connectivity to IPv4 internet. It may cripple IPv4aaS services which are DNS based. What would also break is split-horizon DNS for internal domains.

If you want from ISP higher support for this protocol or you want not to brake these systems then try to initiate DoH first with resolvers used by operating system. Then if ISP supports DoH, all things would work as intended. If you are getting NXDOMAIN replies (or internal addresses) on known to work domain names, then try to do DoH on external provider and if there is a difference, then advise user to use DoH for that network connection. This way it may serve for those under censorship and would not hurt those which are not.

Also if you want to help, enforce DNSSEC validation in both your selected DoH providers and in your browser as DoH client. It may mitigate more substantial problem of current internet - the false replies and poisoned caches.

Sincerely,
Martin Hunek

--
[redacted]