EPT: EDNS Privacy Tunnel for DNS

Lanlan Pan[1], Jie Chen[1], Anlei Hu[2] and Xuebiao Yuchi[3]

[1] Geely Automobile Research Institute, Zhejiang 315336, China
[2] China Internet Network Information Center, Beijing 100190, China
[3] Chinese Academy of Sciences, Beijing 100190, China
abbypan@gmail.com

Abstract. DNS privacy concerns are growing. Recursive resolvers such as ISP DNS and Google Public DNS are serving massive clients, which could fingerprint individual users and analysis the domain interest of users easily. In order to mitigate user privacy leaks on recursive resolvers, in this paper we propose an EDNS privacy tunnel (EPT) extension for DNS. EPT can hide the query domain name from recursive resolvers through public key encryption, avoid big data analysis on individual users, defense against censorship and lying recursive resolvers.

Keywords: DNS; Privacy; Censorship; Hijack; ECS; EPT.

1 Introduction

Individual user privacy is raising global attention nowadays. Domain name system (DNS) is a critical internet service, however, it is weak at the privacy protection for individual users.

Figure 1 shows an example of default DNS traffic flow. As a domain query agent for the client, recursive resolver knows about the client's IP address (client IP), the query domain name (qname) and the response data (answer). Obviously, recursive resolver could fingerprint individual users and analysis the domain interest of individual users easily[1-3].

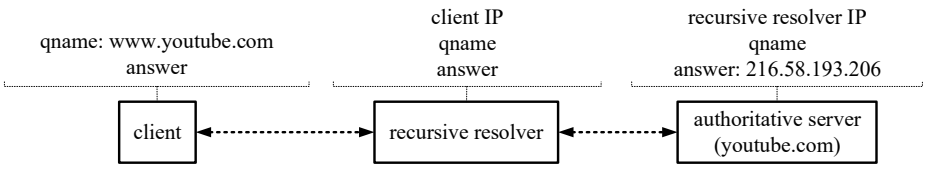

Figure 1. DNS Traffic.

Public recursive resolvers such as Google Public DNS and OpenDNS are not close enough to many users since they couldn't deploy servers among each country and each ISP's network. To bring the web content as close to the users as possible, Google proposes an EDNS client subnet (ECS) extension to carry part of the client's IP address in

the DNS packets for authoritative nameserver [4]. As Figure 2 shows, ECS leaks client subnet information on the resolution path to the authoritative servers. ECS raises individual user's privacy concerns, makes DNS communications less private, and the potential for massive surveillance is greater [5].

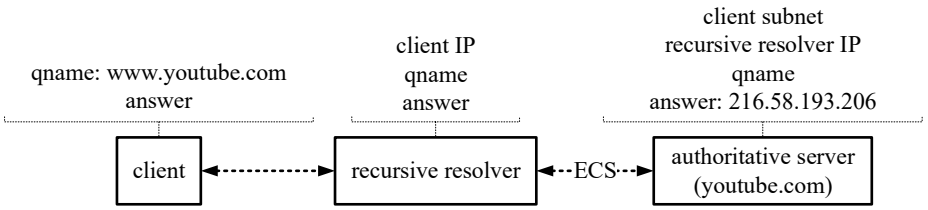

Figure 2. DNS Traffic with ECS Extension.

Therefore, it is important to design a suitable individual user privacy preservation mechanism, especially to defense in-path censorship such as recursive resolver's individual user fingerprinting and lying response. In this paper, we introduce an EDNS privacy tunnel (EPT) extension to address the problem. EPT takes advantage of the public key encryption to hide the query domain from recursive resolvers, defense against censorship and lying recursive resolvers, improve individual user privacy on DNS traffic effectively.

The remainder of this paper is organized as follows. In section 2, we give a brief overview of existing DNS privacy protection technologies. In section 3, we describe the EPT extension in detail. From section 4 to section 6, we discuss privacy improvement, concerns about security and operation. In section 7, we show our experiment. Finally, in section 8, we conclude the paper.

2 DNS Privacy Protection Technologies

As Figure 3 shows, existing DNS privacy protection technologies are hard to provide user privacy protection on recursive resolvers that support ECS.

- Encrypting DNS Traffic

DNS traffic encrypt solutions such as DNS over TLS [6], DNS over DTLS [7], DNSCurve [8], DNSCrypt [9] and Confidential DNS [10] can prevent eavesdropping on the DNS resolution path. However, none of these solutions are workable for individual user de-identification on recursive resolver.

- Reducing Information Leakage to DNS Server

Root loopback[11] and qname minimization[12] can hide domain query information from Root and TLD, while they are not designed for reducing client subnet information leakage on recursive resolver and authoritative server.

- EncDNS

EncDNS [13] encapsulates encrypted messages in standards-compliant DNS messages, which is a lightweight privacy-preserving name resolution service compared to conventional third-party resolvers. EncDNS encapsulates encrypted queries within the question name field of a standard DNS query in binary form. Encrypted replies are encapsulated within the data section of a TXT resource record. Therefore, compared with normal DNS packets, EncDNS packets may encounter some problem to bypass middleboxes such as firewall and IDS. Another privacy concern is that EncDNS server can track the activities of a client if the client uses the same key pair in multiple EncDNS queries.

- ODNS

ODNS [14] architecture is similar with EncDNS, it uses ODNS resolver's public key to encrypt a symmetric session key. The session key is responsible for encrypt query domain, and decrypt the OPT record of the response. The problem of ODNS is mostly on operational. Recursive resolvers should support forwarding EDNS query, and they never remove specific response packets without A record but contains OPT record. The firewalls on the whole resolution path never drop the specific response package.

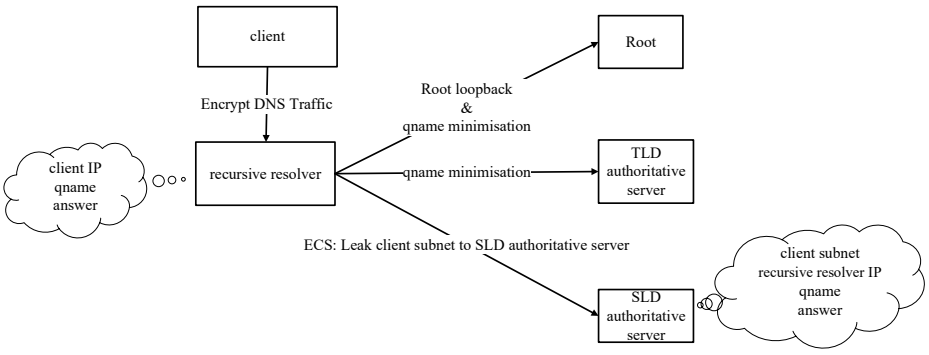

Figure 3. DNS Privacy Leak.

3 EDNS privacy tunnel (EPT) Extension

EDNS privacy tunnel (EPT) is an EDNS extension [15], resolution path is similar with EncDNS and ODNS, while deployment is similar with DNSCrypt.
EPT can be added into DNS queries sent by local forwarding resolvers. EPT is only defined for the Internet (IN) DNS class and the qtype is A or AAAA.

3.1 Structure

EPT is structured as follows:

- **OPTION-CODE**, 2 octets, defined in RFC6891. It should be assigned by the IANA.

- **OPTION-LENGTH**, 2 octets, defined in RFC6891, contains the length of the payload (everything after OPTION-LENGTH) in octets.
- **Payload**, contains encrypted <qname, xor_IP, salt> information. qname is the original query domain, xor_IP is a random generated IP, salt is a random generate string for encryption.

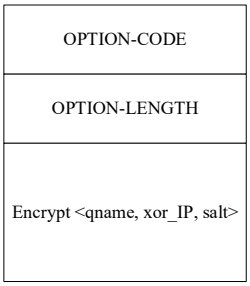

Figure 4. EPT Structure.

All fields of EPT are in network byte order.

3.2 Resolution

Similar with EncDNS, there is a special-use second level domain "myept.com" (EPT_SLD) for EPT. EPT authoritative server of "myept.com" is responsible for analyzing the EPT query and packing the EPT response.
EPT authoritative server selects an asymmetric cryptography algorithm such as RSA, and generates a pair of public key (K_{pub}) and private key (K_{priv}) of the selected algorithm for asymmetrical encryption of EPT tunnel data. As Table 1 shows, the information of the public key can be published as a TXT RR of "myept.com".

Table 1. RSA Example of EPT Public Key Information.

TXT RR of EPT_SLD myept.com
myept.com. 3600 IN TXT "EPT=RSA1024 https://file.myept.com/ept_public_key.pem"

As Table 2 shows, EPT client can get the EPT public key file through the file URL. The format of public key file follows IETF Public-Key Cryptography Standards (PKCS). EPT authoritative server should update new key pairs at regular intervals, offer the public key. EPT client should update the latest public key of EPT authoritative server through TXT record query timely.

Table 2. Example of EPT Public Key File Content.

https://file.myept.com/ept_public_key.pem
-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK6TS3kY6T2mDgAijP/1k4+Tsa

QCAwmu32pNCNDP86X9W9gbWC86fO1QuVIr2PhXUExktQSMJUbTe4lQM6K7QZXXrE
xfqinWNEFyib2X9g65eRKAROrMUBk2Vy+SwaHNKWu0H1kLv8cWNxKZ4lG/9pm7mX
qr39XqTzCnpjwc2sgwIDAQAB
-----END PUBLIC KEY-----

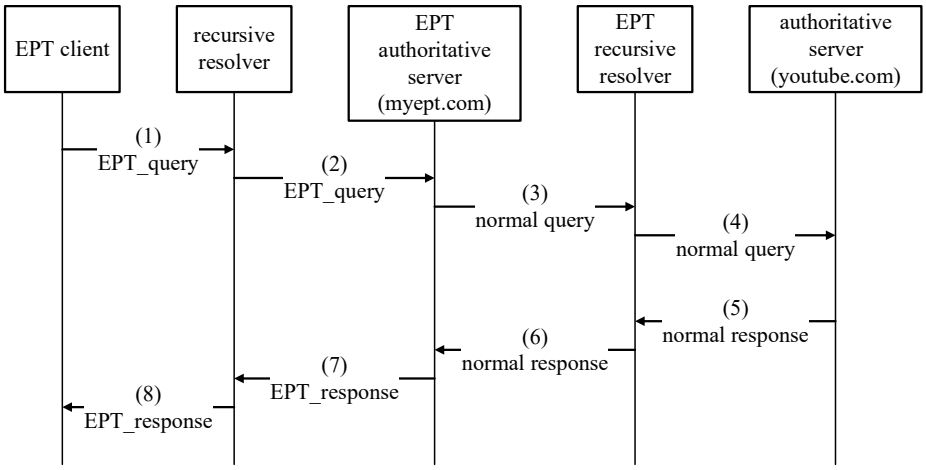

Figure 5. EPT Resolution.

Figure 5 shows the overview of EPT resolution. The steps of EPT resolution are detailed as follows:

(1) EPT client wants to query {qname: "www.youtube.com", qtype: "A"}. EPT client generates random xor_IP and random salt string, then encrypts <qname, xor_IP, salt> with K_{pub} as EPT_payload, and a md5 hash EPT_qname.

$$\text{xor\_IP} = \text{“202.38.64.10”}$$

$$\text{s} = \text{join(“,”, qname, xor\_IP, salt)}$$

$$\text{EPT\_payload} = \text{Asymmetrical\_Encrypt}(K_{pub}, \text{s})$$

$$\text{EPT\_SLD} = \text{“myept.com”}$$

$$\text{EPT\_qname} = \text{join(“.”, md5\_hex(s), EPT\_SLD)}$$

EPT client sends an EPT query {qname: EPT_qname, qtype: "A", additional: EPT_payload} to recursive resolver. The recursive resolver should support RFC6891 and forward the query with EPT_payload.

(2) Recursive resolver sends the above EPT query to the EPT authoritative server.

(3) EPT authoritative server decrypts the EPT_payload with K_{priv}, extracts the <qname, xor_IP, salt> information.

$$\text{s} = \text{Asymmetrical\_Decrypt}(K_{priv}, \text{EPT\_payload})$$

$$\text{(qname, xor\_IP, salt)} = \text{split(“,”, s)}$$

EPT authoritative server sends a normal query {qname: “www.youtube.com”, qtype: “A”} to EPT recursive resolver.

(4) EPT recursive resolver sends the above normal query to authoritative server of “www.youtube.com”.

(5) Authoritative server of “www.youtube.com” returns a normal response {qname: “www.youtube.com”, qtype: “A”, answer: “216.58.193.206”} to EPT recursive resolver.

(6) EPT recursive resolver forwards the normal response to EPT authoritative server.

(7) EPT authoritative server calculates the EPT_answer from the answer of normal response and xor_IP, then builds up the EPT_response {qname: EPT_domain, qtype: “A”, answer: EPT_answer, additional: EPT_payload}. EPT authoritative server sends the EPT_response to recursive resolver.

$$\text{EPT\_answer} = \text{xor}(\text{answer}, \text{xor\_IP}) = \text{“18.28.129.196”}$$

(8) Recursive resolver sends the EPT_response to EPT client. EPT client recovers the answer.

$$\text{answer} = \text{xor}(\text{EPT\_answer}, \text{xor\_IP}) = \text{“216.58.193.206”}$$

4 Privacy Improvement

Figure 6 shows an example of EPT traffic flow.

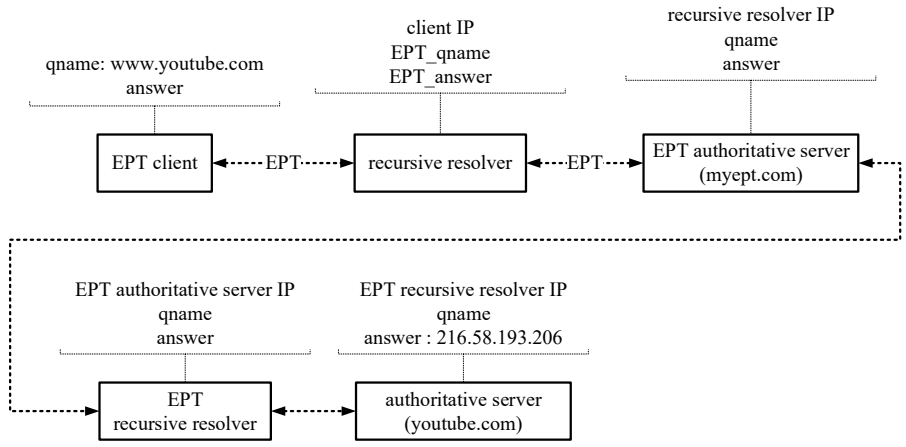

Figure 6. DNS Traffic with EPT Extension.

4.1 Hiding Qname and Answer from Recursive resolver

As a domain query agent for clients, some recursive resolver shares queries log with third-parties in ways not known or obvious to end-users. With EPT extension, recursive resolver knows about the client’s IP address (client IP), the EPT query domain name

(EPT_qname) and the EPT response data (EPT_answer). However, recursive resolver can't know the query domain name (qname) and the response data (answer). Therefore, compare with Figure 1 and Figure 2, recursive resolver could not analysis the domain interest of users because of it lacks the information about qname and answer.

4.2 Mitigating Client Subnet Leakage to Authoritative server

As Figure 2 shows, ECS extension leaks the client subnet information to authoritative server, the domain query action become personally identifiable. With EPT extension, authoritative server only knows about EPT recursive resolver IP, the query domain name (qname) and the response data (answer). Therefore, compare with Figure 2, authoritative server could not analysis the domain interest of users because of it lacks the client subnet information.

4.3 Privacy Preservation on EPT Failure Traffic

To make EPT extension work, the recursive resolver should support RFC6891 EDNS extension, and forward the EPT_query packet to EPT authoritative server. However, as Figure 7 shows, some recursive resolver may replace the EPT extension with ECS, cause a failed query to EPT authoritative server. In this case, EPT authoritative server knows about the client's IP address (client IP), the EPT query domain name (EPT_qname), but it can't know about the query domain name (qname) to generate a normal query. Therefore, EPT authoritative server could not analysis the domain interest of users because of it lacks the information about qname.

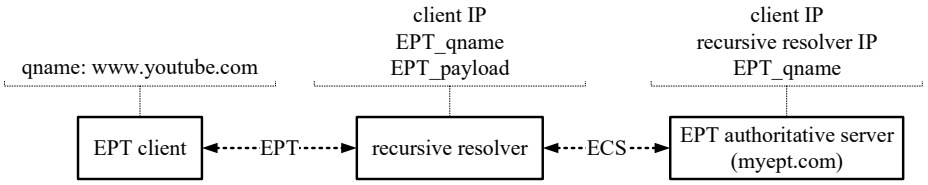

Figure 7. EPT Failure Traffic.

4.4 Combating Targeted Censorship

On default DNS traffic flow, recursive resolver is easy to make targeted client censorship. Even worse, it is fragile to targeted client subnet censorship on the resolution path from recursive resolver to authoritative server when recursive resolver sends the ECS query.

Since EPT hide the qname from recursive resolver and hide the client subnet from authoritative server, EPT will be stronger to defense against the targeted DNS censorship attack. EPT can help to avoid getting lie response on special domain from recursive resolver, and add difficulty on target censorship by the AS-level adversary. If EPT_answer is banned by recursive resolver casually, client can simply generate a new EPT query with different xor_IP and salt to address the problem.

4.5 Anonymous

Compared to VPN and Tor, EPT is focus on preserving the end user privacy on DNS traffic.
On VPN communication scenario, the DNS traffic of each end user is in plain-text to VPN service provider. On the contrary, EPT service provider can't know about end user's DNS queries.
Even in the Tor anonymity network, an AS-level adversary can monitor egress traffic between the exit relay and exit relay's DNS resolver, or the DNS resolver itself [16]. Tor end user can't control the exit relay's DNS resolver configuration because of the multiple anonymity hops relay. However, EPT end user can easily change in the EPT service set, send the EPT query through VPN, the AS-level adversary will be hard to figure out the exact exit relay like Tor.

5 Security

5.1 Hijack

Plain text DNS traffic is naturally in risk of hijacking. The defense capability to hijack depends on the global deployment of DNS traffic encryption and DNSSEC.

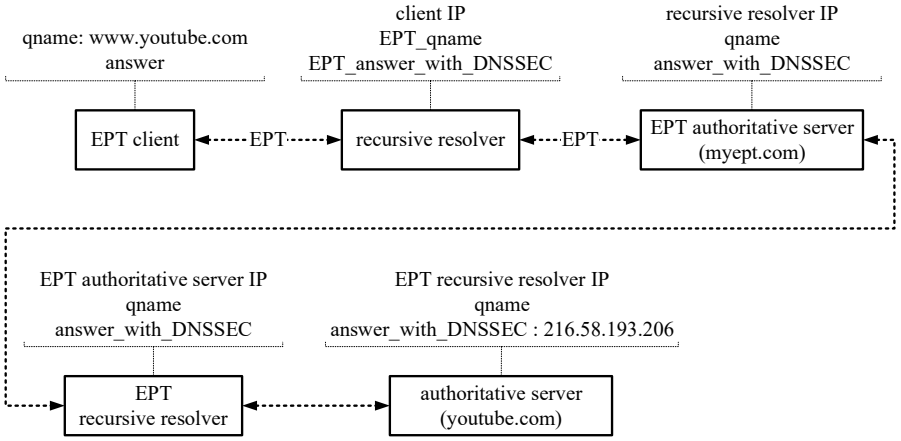

Figure 8. EPT with DNS over TLS and DNSSEC.

As Figure 8 shows, EPT is fully compatible with DNS over TLS and DNSSEC.

- DNS over TLS can be deployed at every resolution path on the EPT query chain.
- Suppose that EPT recursive resolver and authoritative server have enabled DNSSEC, EPT authoritative server can make the qname query with DNSSEC option, and validate the DNSSEC answer of qname which is generated by authoritative server.

- Suppose that recursive resolver has enabled DNSSEC, EPT client can make the EPT_qname query with DNSSEC option, and validate the DNSSEC answer of EPT_qname which is generated by EPT authoritative server.

5.2 DDoS Attack

Similar with pseudo-random sub-domain attack, recursive resolver and EPT authoritative server may encounter error EPT_payload with some random error string. Since recursive resolver doesn't have enough information to find out the correct EPT_payload, it may directly drop the EPT_query flood in case it could not afford the attack. EPT authoritative server may decrypt a lot of error EPT_payload, exhausting CPU.
To mitigate the DDoS attack influence more effectively, recursive resolver and EPT authoritative server can only accept an EPT_query which is from encrypt connection, or from TCP connection. They can also deploy some response rate limitation policy on the query source IP. EPT authoritative server should set short TTL for EPT_response. Further, as Table 1 shows, recursive resolver doesn't need to cache EPT_response if it finds the EPT TXT record of EPT_SLD.

6 Operation

6.1 Deployment

The key point of EPT is to separate client IP and qname information. Therefore, recursive resolver and EPT authoritative server should not share query log with each other. Otherwise, they could spell out the <client, qname, answer> privacy elements. Similar, recursive resolver and EPT recursive resolver should not share query log with each other.
EPT recursive resolver can enable qname minimisation [12] to prevent the qname leakage to the Root and TLD server.
EPT deployment on the client side is similar with DNSCrypt [9]. Client should install an EPT proxy resolver on local machine. EPT proxy resolver is responsible to make a control on the local DNS traffic, encrypt selective normal query to EPT_query, decrypt EPT_response to normal answer. EPT proxy resolver can configure multiple EPT authoritative servers.

6.2 Cache Size of Recursive Resolver

EPT_queries behave similar on recursive resolver to disposable domain. Disposable domains are likely generated automatically, characterized by a "one-time use" pattern, and appear to be used as a way of "signaling" via DNS queries [17].
Basically, recursive resolver can use traditional cache aging heuristic policy to deal with the EPT_response cache issue. Besides, recursive resolver can also make some more optimization, as described in [17].

Further, as Figure 9 shows, to reduce cache size, recursive resolver could remove the EPT extension of EPT_response packet. As the EPT_qname is generated by md5 hash function, the probability of EPT_qname collision is very low.
To lighten the burden of EPT authoritative server, EPT extension is optional in EPT_response packet. EPT client must record the <EPT_qname, xor_IP> information to retrieve response from the EPT_response packet without EPT extension. EPT_response without EPT extension is almost the same with normal response. Therefore, it won't trigger the drop policy for the abnormal response packets without A record on recursive resolver, and it will be very easy to bypass middleboxes such as firewall and IDS.

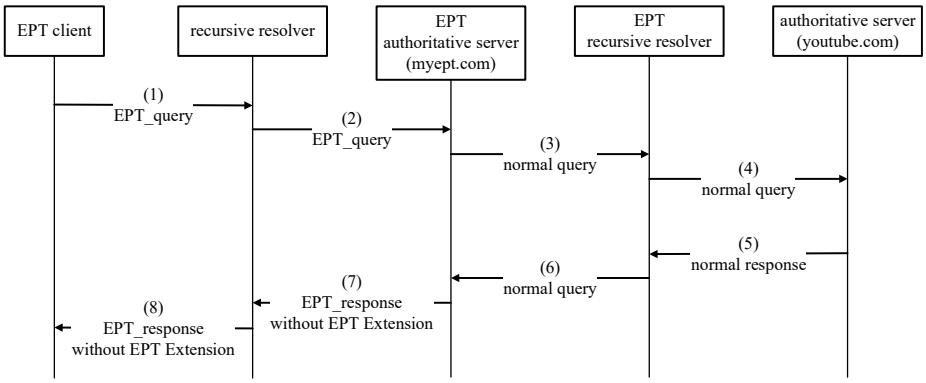

Figure 9. EPT Response without EPT Extension.

6.3 Response Latency

Every EPT_qname will encounter cache miss on recursive resolver. Therefore, recursive resolver should forward each EPT_query to EPT authoritative server. Response latency will rise, since there will be additional latency on the <recursive resolver, EPT authoritative server, EPT recursive resolver> resolution path. If the common additional latency is less than 100ms, it is acceptable for many privacy sensitive users.
Moreover, to reduce response latency, EPT authoritative server can act the role of EPT recursive resolver, communicate with authoritative server directly.

7 Experiment

Our experiment code can be found in [18].
The compatibility issue of EPT extension is that recursive resolver should support RFC6891. The EPT extension is mandatory in EPT_query packet, recursive resolver should send the EPT_query packet to EPT authoritative server without any modification.
Table 3 shows our EDNS support test on some famous public recursive resolvers. Public recursive resolvers may send some modified queries to EPT authoritative server when they receive the EPT_query.

- All of them remove the EPT extension from original EPT_query, then send a UDP query with zero EDNS data length for the EPT_qname, just indicate the EDNS payload size they can support. VerisignDNS is more special, it changes uppercase and lowercase characters of EPT_qname and send the UDP EDNS queries for these modified qnames.
- Except Quad9 and Cloudflare, most of them will send a UDP query without EDNS extension for the EPT_qname.
- Only Cloudflare will try to send TCP queries with zero EDNS data length for the EPT_qname.
- Only GoogleDNS will send UDP ECS queries for the EPT_qname, it will undermine privacy protection of EPT extension because EPT authoritative server will know about the client subnet information for specific qname.

Table 3. EDNS Support on Public Recursive Resolvers.

Recursive resolver	UDP+EDNS (Payload Size)	UDP	TCP+EDNS (Payload Size)	ECS
GoogleDNS (8.8.8.8)	Y (4096)	Y	N	Y
Quad9 (9.9.9.9)	Y (1680)	N	N	N
Cloudflare (1.1.1.1)	Y (1452)	N	Y (1452)	N
OpenDNS (208.67.222.222)	Y (1280)	Y	N	N
VerisignDNS (64.6.64.6)	Y (1280)	Y	N	N
114DNS (114.114.114.114)	Y (4096, 512)	Y	N	N
AliDNS (223.5.5.5)	Y (512)	Y	N	N

As the length of EPT_qname is hash fixed, EPT doesn't have the qname length problem as ODNS [14].

EPT authoritative sever can choose many popular asymmetric cryptography algorithms. Most of the time, the length of <qname, xor_IP, salt> will less than 256 bytes, and RSA2048 is workable. Except RSA, as Table 4 shows, Elliptic Curve Integrated Encryption Scheme (ECIES) can be another choice for the encryption on longer <qname, xor_IP, salt> [19].

Table 4. ECIES Example of EPT Public Key Information.

TXT RR of EPT_SLD myept.com
myept.com. 3600 IN TXT "EPT=ECIES,Curve:secp256k1,KDF:PBKDF2,Symmetric:AES-256-GCM,MAC:HMAC-SHA256 https://file.myept.com/ept_public_key.pem"

8 Conclusion

This paper is an extended version of an earlier poster paper presented at the IEEE Trustcom 2018[20]. Plain text DNS traffic is weak at user privacy protection. Clients are hard to avoid recursive resolver's big data analysis on query log, not to mention censorship and lies without DNSSEC support. User privacy protection requires additional costs. EPT is to defense against user domain interest censorship and avoid selective domain hijack. EPT can provide end-user privacy enhancement on recursive resolver and authoritative server. The biggest reality problem of EPT deployment is the support of existed recursive resolvers. We plan to deploy the EPT into real world DNS traffic in the future.

References

1. Imana, B., Korolova, A., & Heidemann, J. (2018, February). Enumerating privacy leaks in DNS data collected above the recursive. In *NDSS: DNS Privacy Workshop*.
2. Siby, S., Juarez, M., Vallina-Rodriguez, N., & Troncoso, C. (2018). DNS Privacy not so private: the traffic analysis perspective.
3. Bradshaw, S., & DeNardis, L. (2019). Privacy by Infrastructure: The Unresolved Case of the Domain Name System. *Policy & Internet*, *11*(1), 16-36.
4. Contavalli, C., W. van der Gaast, and D. Lawrence. W. Kumari: Client Subnet in DNS Queries. RFC7871. 2016.
5. Kintis, Panagiotis, et al.: Understanding the Privacy Implications of ECS. Detection of Intrusions and Malware, and Vulnerability Assessment. Springer International Publishing, 2016. 343-353.
6. Hu, Z., et al.: Specification for DNS over Transport Layer Security (TLS). RFC 7858. 2016.
7. Reddy, Tirumaleswar, D. Wing, and P. Patil. DNS over Datagram Transport Layer Security (DTLS). No. RFC 8094. 2017.
8. Dempsky, M.: Dnscurve: Link-level security for the domain name system. Work in Progress, draft-dempsky-dnscurve-01 (2010).
9. DNSCrypt, https://dnscrypt.org/.
10. Wijngaards, W., and G. Wiley.: Confidential DNS. IETF Draft.(https://tools.ietf.org/html/draft-wijngaards-dnsop-confidentialdns-03) (2015).
11. Kumari, W., and P. Hoffman.: Decreasing Access Time to Root Servers by Running One on Loopback. RFC 7706. 2015.
12. Bortzmeyer, S.: DNS Query Name Minimisation to Improve Privacy. RFC7816. 2016.
13. Herrmann, D., Fuchs, K. P., Lindemann, J., & Federrath, H. (2014, September). Encdns: A lightweight privacy-preserving name resolution service. In European Symposium on Research in Computer Security (pp. 37-55). Springer, Cham.
14. Schmitt, P., Edmundson, A., & Feamster, N. (2018). Oblivious DNS: Practical Privacy for DNS Queries. arXiv preprint arXiv:1806.00276.
15. Damas, Joao, Michael Graff, and Paul Vixie: Extension mechanisms for DNS (EDNS (0)). RFC 6891. 2013.
16. Greschbach, B., Pulls, T., Roberts, L. M., Winter, P., & Feamster, N. (2016). The Effect of DNS on Tor's Anonymity. arXiv preprint arXiv:1609.08187.
17. Chen, Y., Antonakakis, M., Perdisci, R., Nadji, Y., Dagon, D., & Lee, W. (2014, June). DNS noise: Measuring the pervasiveness of disposable domains in modern DNS traffic. In

Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on (pp. 598-609). IEEE.
18. dns_test_ept, https://github.com/abbypan/dns_test_ept.
19. Martínez, V. G., & Encinas, L. H. (2010, August). A Comparison of the Standardized Versions of ECIES. In Information Assurance and Security (IAS), 2010 Sixth International Conference on (pp. 1-4). IEEE.
20. Pan, L., Yuchi, X., Wang, J., & Hu, A. (2018, August). A Public Key Based EDNS Privacy Tunnel for DNS. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1722-1724). IEEE.