A proposal of DoH-based domain name resolution architecture including authoritative DNS servers

Satoru Sunahara
Chitose Institute of Science and Technology
Hokkaido, Japan.
s-sunaha@photon.chitose.ac.jp

Yong Jin
Tokyo Institute of Technology
Tokyo, Japan.
yongj@gsic.titech.ac.jp

Katsuyoshi Iida
Hokkaido University
Hokkaido, Japan.
iida@iic.hokudai.ac.jp

***Abstract*—In addition to cache poisoning attacks, the privacy leakage has become a critical issue in DNS nowadays. Especially, the communication between the DNS full-service resolver and the authoritative DNS servers may go through multiple ISP networks. Thus, if the communication path contains areas with different privacy policies, the security and privacy in DNS domain name resolution cannot be guaranteed. To mitigate cache poisoning attacks and protect the privacy of the Internet users, we propose a novel architecture that encrypts all DNS communications with DoH. In the proposed architecture, in addition to the communication between the end clients and the DNS full-service resolvers, that between the DNS full-service resolvers and the authoritative DNS servers is also covered by DoH. As a result, not only the risk of cache poisoning attacks can be dramatically mitigated on DNS full-service resolver but also the risk of eavesdropping on DNS traffic can be reduced. Moreover, the proposed architecture is the first approach to pure DoH-based domain name resolution including DNS authoritative DNS servers.**

***Keywords*—DNS, DNS over HTTPS, DoH, privacy, and privacy.**

I. Introduction

Cache poisoning attacks have been a critical security threat in Domain Name System (DNS) [1] based domain name resolution for a long time. Recently, privacy leakage of the Internet users during DNS-based domain name resolution has become another critical issue. In the conventional DNS architecture, an organization network normally has one or more DNS full-service resolvers for providing domain name resolution service to the internal users. Moreover, many public DNS servers (DNS full-service resolvers) are also available for providing domain name resolution service to the Internet users. Since the conventional non-encrypted User Datagram Protocol (UDP) based domain name resolution is vulnerable to cache poisoning attacks and privacy leakage [2], which cannot be guaranteed by DNS Security Extensions (DNSSEC) [3] due to the low deployment rate and non-encrypted DNS traffic, DNS over TLS (DoT) [4] and DNS over HTTPS (DoH) [5], which encrypts DNS communication for the purpose of privacy protection and cache poisoning attack mitigation have been standardized. The major public DNS servers, such as Quad9, Cloudflare, google, etc, started DoT and DoH services.

However, the current DoT and DoH services are mainly adopted in DNS full-service resolvers so that only a part of DNS communication is encrypted. Figure 1 shows the current DNS architecture including the conventional UDP-based and DoT/DoH-based domain name resolution. The communication between DNS full-service resolvers and authoritative DNS servers is still in plaintext, thus there is a risk of privacy leakage by eavesdropping. For example, if an Internet user is using a DNS full-service resolver operated by an organization administrator, the administrator can capture the DNS traffic between the DNS full-service resolver and the authoritative DNS servers so that the user's privacy can be leaked. Similarly, when the Internet users use the DNS full-service resolvers of the ISP, there is also the same privacy risk.

In addition, it is technically possible for ISPs to rewrite DNS responses for advertisment or blocking [6]. Therefore, DNS Query Name Minimization [7] was proposed to improve the privacy of the Internet users during DNS domain name resolution between DNS full-service resolver and authoritative DNS servers. Conventionally, DNS full-service resolvers query the original FQDN which is the privacy information to all the necessary authoritative DNS servers. By using the Query Name Minimization method, only the minimized part of the original FQDN will be queried from the DNS full-service resolvers to each necessary authoritative DNS server step by step to protect the users' privacy as much as possible. However, this feature neither can mitigate the risk of cache poisoning attacks nor can solve the privacy concern completely.

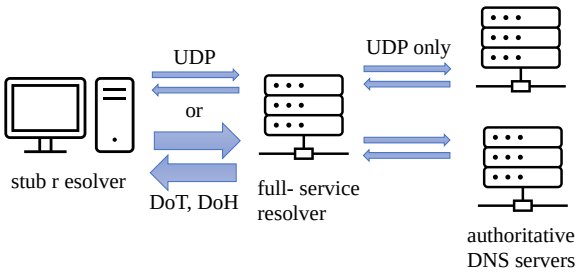

Fig. 1. Current DNS architecture.

Accordingly, in addition to the risk of cache poisoning attacks, if the communication path contains networks with different privacy policies or eavesdropping device, the privacy will be leaked. Therefore, we believe that it is important to encrypt all communication paths in DNS-based domain name resolution in order to mitigate the risk of cache poisoning attacks and avoid the leakage of privacy information, which may

further derive inappropriate information manipulation, such as advertising display and blocking. Above all, we therefore propose a novel architecture of pure DoH-based domain name resolution including not only DNS full-service resolvers but also authoritative DNS servers. DoH has been standardized as an encrypted DNS-based domain name resolution protocol for the communication between the end clients and the DNS full-service resolvers. Therefore, in this research we extend the DoH protocol to the communication between the DNS full-service resolvers and the DNS authoritative servers.

II. Proposed Architecture

As shown in Fig. 1, the conventional DNS architecture allows plaintext to be used for communication between the end clients and the DNS full-service resolvers and so does in the communication between the DNS full-service resolver and the authoritative DNS servers.

In Fig. 2, we illustrate the proposed DoH-based domain name resolution architecture, which completely uses DoH for all DNS communications. In other words, all authoritative name servers must support DoH in the proposed architecture. The end clients can communicate securely by just switching the configured DNS full-service resolver to the one which only supports DoH-based domain name resolution. The procedure of the proposed architecture is described in the following.

(1) The stub resolver in the end client sends DNS query to the DNS full-service resolver using DoH.
(2) If the DNS full-service resolver has no DNS resource records cached for the domain name, the DNS full-service resolver iteratively queries the DNS authoritative servers using DoH for the domain name resolution.
(3) Each DNS authoritative server replies corresponding referral information to the DNS full-service resolver using DoH and until the DNS full-service resolver obtains the final DNS response. In this example, we only illustrate one more pair (4) and (5).
(6) The DNS full-service resolver replies to the final DNS response to the end client using DoH.

With the above procedure, by using the proposed DoH-based domain name resolution architecture, both the risk of cache poisoning attacks and privacy leakage of the Internet users can be reduced dramatically. Table I shows the comparison of the proposal with the conventional methods regarding the security and privacy of the DNS architecture. One concern we have to clarify is that the proposed architecture can mitigate the risk of cache poisoning attacks and privacy leakage, it cannot guarantee that the DNS full-service resolvers are not compromised. As a solution, the collaboration of the DNSSEC and the proposed architecture is possible so that the end client can avoid using faked DNS resource records.

Another concern is the performance issue of the proposed architecture. The proposed architecture has a higher communication cost than the conventional method. In the conventional method, a pair of UDP query-and-response is completed within a round trip time between the full-service resolver and the authoritative DNS server. On the other hand, the proposed architecture requires Transmission Control Protocol (TCP) three-way handshake, TLS handshake and negotiation, HTTPS communication, and TCP disconnection. From the perspective of practical usage, it is necessary to confirm whether the proposed method will cause network congestion on wired and wireless network environment.

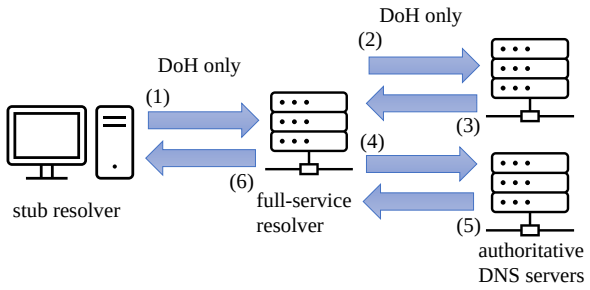

Fig. 2. DoH-based domain name resolution architecture.

TABLE I
Comparison of Security and Privacy Enhancements

Method	Integrity protection	Privacy protection	Scope
DNSSEC [3]	Protect	Does not protect	Stub resolver – Authoritative DNS server
DoT [4] DoH [4]	Protect	Protect	Stub resolver – Full-service resolver
Query Name Minimization[7]	Does not protect	Minimize the leakage of privacy information	Full-service resolver – Authoritative DNS server
Proposed method	Protect	Protect	Full-service resolver – Authoritative DNS server

In addition, it is necessary to cope with Denial of Services (DoS) attacks. By deploying the DoH service, the network administrators must deal with TCP, TLS, and HTTPS-based DoS attacks; SYN flood attacks, HTTP GET/POST flood attacks, and slow HTTP DoS attacks, etc. A common way to block these attacks is to deploy a firewall or intrusion prevention system (IPS). We have to confirm that firewalls and IPS can protect such kind of attacks. For example, enabling DoH may bypass some of the filtering done by ISPs and organizations. In the conventional methods, the DNS traffic can be read in plaintext, thus it was technically possible to detect and block the DNS traffic bound for the suspicious destinations in advance. However, the conventional method is not applicable to DoH-based name resolutions due to the traffic is encrypted. Therefore, the users may lose some security filtering as the cost of privacy protection with DoH. To solve this problem, we have to develop new security systems using techniques such as machine learning [8].

III. Design of Prototype Implementation

In the previous section, we have proposed DoH-based domain name resolution architecture including authoritative DNS

servers. This section describes the local experimental network, the current implementation and the future work.

A. Construction of a local experimental network

We constructed a local experimental network environment on one physical server in order to implement and evaluate the proposed architecture. The minimum virtual configuration consists of one end client, one DNS full-service resolver, and two authoritative DNS servers. Figure 3 shows network configuration of the prototype system. In this environment, all authoritative DNS servers contain digital certificates and support DoH. More importantly, the full-service resolver is configured with root.hints" file that only contains the experimental root authoritative DNS server of the proposed system and uses the NAT functionality ofiptables" to pass UDP-based DNS queries to DoH proxy. Table II summarizes the parameters of the prototype system. We plan to evaluate the scalability performance by increasing the number of DNS queries from end clients, the number of authoritative DNS servers, and volume of zone size, etc.

B. Current implementation and the future work

We chose Ubuntu22.04 LTS as the server OS for the local experimental network environment and used Kernel-based Virtual Machine (KVM) as a hypervisor in order to build the virtual machines. We prepared Ubuntu22.04 and Windows11 as end clients. Ubuntu22.04 uses "dnsperf" for load testing while Windows11 uses web browsers for the evaluation. We used bind9 [9] for the DNS full-service resolver and the authoritative DNS servers. However, even bind9 could provide DoH service to the end client it has no functionality of DoH-based name resolution as a DNS full-service resolver. Therefore, we developed a proxy using python that converts the DNS traffic from UDP to DoH and vice versa between the DNS full-service resolver and the authoritative DNS servers. We realized the proxy functionality by combining the dnslib [10] and the Linux command "curl HTTP request".

One of the research issues of the proposed architecture is to clarify how many physical servers are required to maintain the performance. As a performance evaluation, we plan to compare the performance among DoT, DoH and the proposed architecture. PowerDNS [11] has an experimental implementation of DoT encryption for communication between DNS full-service resolvers and authoritative DNS servers, which we will use for verification in the future.

Based on the result of empirical evaluations, we plan to estimate how many physical servers are required in high load servers, such as the root servers and TLD servers. Moreover, we also plan the deployment of the proposed architecture within the current DNS environment.

IV. Summary

In this paper, we proposed a DoH-based domain name resolution architecture including the authoritative DNS servers. This approach allows us to protect user privacy all along the DNS communication path. We built a prototype environment for this architecture and indicated the direction of future research. From the perspective of the practical usage, we described the further research plan in terms of the increased communication costs, increased burden on name server administrators, and the impact of existing security measures.

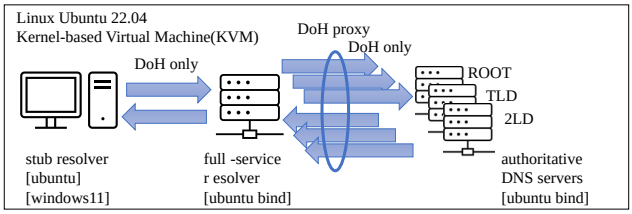

Fig. 3. A prototype of DoH-based domain name resolution architecture.

TABLE II
THE PARAMETERS IN THE PROTOTYPE SYSTEM

role	IP/subnet	remarks
stub resolver	192.168.53.5/16	Resolve names on 192.168.53.10
full-service resolver	192.168.53.10/16	Server certificate required Proxying with nat in iptables bind9: root hint file ROOT-SERVERS 192.168.53.20
root authoritative DNS	192.168.53.20/16	Server certificate required
TLD authoritative DNS	192.168.53.30/16	Server certificate required
2LD authoritative DNS	192.168.53.50/16	Server certificate required

Acknowledgements

This work was partially supported by JSPS KAKENHI (Grants-in-Aid for Scientific Research) Grant Number 19K20254.

References

[1] Z. Yan, and J.H. Lee, "The road to DNS privacy," *Future Generation Computer Systems*, vol. 112, pp. 604–611, Nov. 2020. doi: 10.1016/j.future.2020.06.012

[2] D.W. Kim, and J. Zhang, "You are how you query: Deriving behavioral fingerprints from DNS traffic," in *Proc. Int'l Conf. Security and Privacy in Communication Systems (SecureComm 2015)*, part of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 164, pp. 348–366, Oct. 2015. doi: 10.1007/978-3-319-28865-9˙19

[3] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS security introduction and requirements," *IETF RFC 4033*, Mar. 2005.

[4] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman, "Specification for DNS over transport layer security (TLS)," *IETF RFC7858*, May 2016.

[5] P. Hoffman, and P. McManus, "DNS queries over HTTPS (DoH)," *IETF RFC8484*, Oct. 2018.

[6] N. Weaver, C. Kreibich, and V. Paxson, "Redirecting DNS for ads and profit," in *Proc. USENIX Workshop on Free and Open Communications on the Internet (FOCI 11)*, Aug. 2011, 6 pages.

[7] S. Bortzmeyer, "DNS query name minimisation to improve privacy," *IETF RFC7816*, Mar. 2016.

[8] R. Mitsuhashi, Y. Jin, K. Iida, T. Shinagawa, and Y. Takai, "Malicious DNS Tunnel Tool Recognition using Persistent DoH Traffic Analysis ," *IEEE Trans. Network and Service Management,* advanced publication, 9 pages, Oct. 2022. doi: 10.1109/TNSM.2022.3215681

[9] Internet Systems Consortium, Inc., "BIND 9 - Versatile, classic, complete name server software" (online), available from https://www.isc.org/bind/

[10] PaulC, "dnslib" (online), available from https://github.com/paulc/dnslib

[11] PowerDNS.COM BV, "PowerDNS" (online), available from https://www.powerdns.com/