# Privacy Preserved Achievement Method for OCSP Status and Supported Protocols in Full-DoH Architecture

Anonymous Author(s)

***Abstract*—Currently,Efforts to protect privacy information through encrypted DNS communications are becoming increasingly active. The encryption of DNS, standardized by the Internet Engineering Task Force (IETF), predominantly uses Transport Layer Security (TLS). However, the use of TLS for encrypting DNS communications results in the leakage of privacy information during the certificate revocation process. This paper proposes a new method for certificate revocation verification in encrypted DNS communications, presents a way to enhance the protection of privacy information, and outlines a research plan for further investigation.**

***Index Terms*—domain name system, privacy, certification, security**

## I. Introduction

Traditionally, the Domain Name System (DNS), which serves as a starting point for users accessing the internet, communicated in plaintext, without consideration for the protection of privacy information. Therefore, attackers who can intercept communications on the DNS transmission path can determine when and what content a user is attempting to access. For example, if a user made a hospital appointment due to an illness, an attacker could potentially identify the hospital of interest based on the domain name.

Currently, the protection of privacy in DNS communications is recognized as an important issue [1]. Standards such as QNAME Minimization (Q-min) [2], DNS over TLS (DoT) [3], DNS over HTTPS (DoH) [4], and DNS over QUIC (DoQ) [5] have been established to enhance privacy protection in DNS communications. However, the privacy protection measures implemented by these standards are still an issue.

QNAME Minimization (Q-min) reduces the risk of leaking private information by not transmitting the Fully Qualified Domain Name (FQDN) as a DNS query from full-service resolvers to authoritative DNS servers until necessary. However, Q-min is not perfect for privacy protection because it still sends the FQDN, which becomes privacy-sensitive information, in plaintext to the authoritative DNS servers during the final stage of name resolution.

DoT, DoH, and DoQ protect privacy by encrypting communication contents. The issue with these protocols resides in the certificate verification process of the Transport Layer Security (TLS) handshake, which is required to initiate encrypted communication. During the TLS handshake, the client receives a server certificate from the DNS server and determines whether the DNS server is a legitimate communication partner by verifying the certificate against the following three points: (1)Verify the integrity of the certificate. (2)Verify the expiration date of the certificate. (3)Verify the Revocation Status of Certificates. In these protocols, especially in the point of (3)Verify the Revocation Status of Certificates, the protection of privacy is not guaranteed.

The verification of certificate revocation primarily involves three options: (A) obtaining a Certificate Revocation List (CRL), (B) using the Online Certificate Status Protocol (OCSP) to retrieve status [6], and (C) forgoing the verification of revocation.

If option (A) is selected, the client will incur bandwidth costs proportional to the size of the CRL, and the user experience for name resolution will be significantly compromised [7].

If option (B) is selected, it is necessary to resolve the Fully Qualified Domain Name (FQDN), which is private information, in plaintext. This is because, at this stage of verification, encrypted communication has yet to commence between the client and the DNS server. When a full-service resolver performs name resolution of domain names in plaintext to retrieve OCSP status information, the leakage of institutional privacy becomes problematic [8].

If option (C) is selected, there is a risk of initiating communication with an entity impersonating a legitimate authoritative DNS server, depending on the situation. DNS Security Extensions(DNSSEC) is effective for detecting DNS authoritative servers that are impersonating others [9]. Due to the chain of trust in DNSSEC, clients can detect fraud. However, once a DNS query is sent to an impersonating authoritative DNS server, private information is exposed. Therefore, DNSSEC alone is insufficient in terms of preventing the transfer of private information to attackers, and verification of certificates in TLS handshake becomes crucial.

Usually, the private key of a certificate is protected to prevent leakage to third parties, and there is no need to revoke the certificate unless the private key is compromised. However, incidents have occurred where the private key is leaked due to unauthorized access, compromising the trustworthiness of the certificate. For instance, in 2011, DigiNotar, a certification authority in the Netherlands, was hacked, leading to the risk of issuing fraudulent certificates, which necessitated the revocation of their certificates [10]. To achieve complete privacy protection in DNS communications, including verification of

certificate revocation, the existing protocols are insufficient.

## II. PROPOSED METHOD

We propose a novel method to ensure privacy protection in the verification of certificate revocation during encrypted DNS communication. Previous studies introduced a technique that injects the server's supported encryption methods into the NS records [11]. By enhancing this method with the OCSP status, we eliminate potential privacy leaks that may occur during certificate revocation checks in the TLS handshake, thereby achieving perfect privacy protection in encrypted DNS communications.

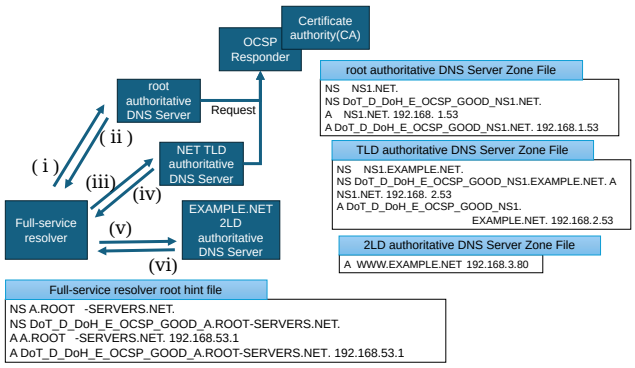


Fig. 1. Overview of the Proposed Method.

We will explain the specific process we propose. Figure 1 is an overview diagram of the method we suggest. The host exemplified in Figure 1 includes a full-service resolver subject to privacy protection, root authority servers, TLS, second-level domain (2LD) authority servers, a Certificate Authority (CA), and an OCSP responder operated by the CA. Our proposed method assumes that authoritative DNS servers preliminarily inquire about the certificate status of the domains listed in the NS records from the OCSP responder, and this OCSP status is recorded in the NS records. In the example of Figure 1, the root authoritative DNS server has registered the encryption protocol supported by the TLD authoritative server and its OCSP status in the NS records. The NS records indicate that DoT is disabled (DoT_D), DoH is enabled (DoH_E), and the OCSP_GOOD signifies that the certificate has not been revoked. The TLD authoritative DNS server has registered the supported encryption protocols and OCSP information of the 2LD authoritative servers in the NS records. The root hint file of the full-service resolver includes the encryption protocols and OCSP information supported by the root authoritative DNS server.

If these prerequisites are met, the following processes are available: (i) the full-service resolver initiates a TLS connection request with the root authoritative DNS server, (ii) receives the certificate, checks for revocation using the OCSP information from the root hint file, and if there are no issues, receives the NS record of the TLD authoritative server, which includes the corresponding encryption method and registered OCSP status, (iii) initiates a TLS connection request with the TLD authoritative DNS server, (iv) receives the certificate, verifies revocation with the OCSP information received from the root authoritative DNS server and that of the TLD authoritative DNS server, and if there are no issues, receives the NS record of the 2LD authoritative server, which includes the corresponding encryption method and registered OCSP status, (v) initiates a TLS connection request with the 2LD authoritative DNS server and (vi) receives the certificate, verifies revocation with the OCSP information received from the TLD authoritative DNS server and that of the 2LD authoritative DNS server, and if there are no issues, receives the A record. Furthermore, even as the domain name deepens, as long as the full-service resolver can receive OCSP information from the delegating authoritative DNS server as described, it is not necessary to resolve OCSP information in plaintext, thereby achieving the protection of privacy information.

## III. RESEARCH PLAN

In this paper, we introduced issues of privacy leakage occurring during the TLS handshake in encrypted DNS communications, along with methods for addressing these issues. The proposed method requires an extension to existing NS records, and the impact of this extension on existing communications has not yet been verified. Therefore, this study necessitates the initial creation of a verifiable prototype environment. In this prototype environment, we plan to verify that there is no impact on existing communications, including DNSSEC, and also to assess the performance.

## REFERENCES


[1] T. Wicinski, "DNS Privacy Considerations," IETF RFC9076, July 2021.
[2] S. Bortzmeyer, R. Dolmans, and P.E. Hoffman, "DNS query name minimisation to improve privacy." IETF RFC9156, November 2021.
[3] S. Dickinson, D.K. Gillmor, and T. Reddy.K, "Usage profiles for DNS over TLS and DNS over DTLS." IETF RFC8310, March 2018.
[4] P.E. Hoffman and P. McManus, "DNS queries over HTTPS (DoH)." IETF RFC8484, October 2018.
[5] C. Huitema, S. Dickinson, and A. Mankin, "DNS over dedicated QUIC connections." IETF RFC9250, May 2022.
[6] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol." IETF RFC6960, June 2013.
[7] Y. Liu, W.Tome, L. Zhang, D.Choffnes, D.Levin, B. Maggs, A. Mislove, A. Schulman and C. Wilson, "An End-to-End Measurement of Certificate Revocation in the Web's PKI," In Proceedings of the 2015 Internet Measurement Conference (IMC '15),
[8] B. Imana, A. Korolova, and J. Heidemann, "Institutional privacy risks in sharing DNS data." In Proceedings of the Applied Networking Research Workshop (ANRW '21). Association for Computing Machinery, pp 69–75, July 2021.
[9] P.E. Hoffman, "DNS Security Extensions(DNSSEC)." IETF RFC9364, February 2023.
Association for Computing Machinery, pp 183 - 196, October 2015.
[10] Microsoft Security Advisory "Fraudulent Digital Certificates Could Allow Spoofing." https://learn.microsoft.com/en-us/security-updates/SecurityAdvisories/2011/2607712, accessed on 20 April 2024.
[11] S. Sunahara, Y. Jin, and K. Iida. "Authoritative DNS Server Discovery Method to Enhance DNS Privacy Preservation." In Proceedings of the on CoNEXT Student Workshop 2023 (CoNEXT-SW '23). Association for Computing Machinery, pp 31–32.