Authoritative DNS Server Discovery Method to Enhance DNS Privacy Preservation

Satoru Sunahara*
Chitose Institute of Science and Technology
Chitose, Hokkaido, Japan
Hokkaido University
Sapporo, 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.hokkudai.ac.jp

ABSTRACT

Plaintext-based DNS domain name resolution poses significant privacy risks. Therefore, encrypting DNS communication across all pathways is essential for privacy preservation. The IETF has standardized DoT, DoH, and DoQ to achieve encryption between end terminals and DNS full-service resolvers. Currently, an Internet-Draft has been published for encrypted communication between DNS full-service resolvers and authoritative DNS servers. However, the probing policy on the Internet-Draft prioritizes compatibility and conducts plaintext communication until it discovers authoritative DNS servers that support encrypted communication. Therefore, the Internet-Draft's probing policy does not provide complete privacy preservation. In this paper, we propose a novel authoritative DNS server discovery approach that achieves privacy preservation while ensuring compatibility.

CCS CONCEPTS

• **Security and privacy → Privacy-preserving protocols**.

KEYWORDS

DNS, Privacy preservation, Encrypted DNS Authoritative Server, Server Discovery, NS Records

ACM Reference Format:
Satoru Sunahara, Yong Jin, and Katsuyoshi Iida. 2023. Authoritative DNS Server Discovery Method to Enhance DNS Privacy Preservation. In *Proceedings of the CoNEXT Student Workshop 2023 (CoNEXT-SW '23), December 8, 2023, Paris, France.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3630202.3630228

1 INTRODUCTION

Plaintext-based DNS domain name resolution poses significant privacy risks. Even today, the communication between DNS full-service resolvers and authoritative DNS servers remains in plaintext, thereby exposing institutional privacy to potential leaks [3].

To enhance privacy preservation in DNS, the IETF has standardized Query Name Minimization (Q-min) [1]. Q-min mitigates the threat of privacy leakage by minimizing the use of Fully Qualified Domain Names (FQDN), which could be privacy-sensitive information, in queries sent to authoritative DNS servers. However, Q-min still sends FQDN in plaintext to authoritative DNS servers during the final stage of name resolution, potentially risking privacy information leakage along that path. Therefore, Q-min's privacy preservation is not enough.

Encrypting all DNS communication between end terminals, DNS full-service resolvers, and authoritative DNS servers is essential to guarantee absolute privacy preservation in DNS domain name resolution since it provides the benefit of protection against eavesdropping threats for all users and organizations relying on DNS.

The IETF has published an Internet-Draft for encrypted communication between DNS full-service resolvers and authoritative DNS servers [2]. However, the probing policy still includes a process in which FQDNs are sent in plaintext, making privacy preservation imperfect. Specifically, the probing policy prioritizes compatibility, sending plaintext-based DNS queries simultaneously until an authoritative DNS server that supports encrypted communication is found. Moreover, even if it successfully identifies an authoritative DNS server that supports encrypted communication, there remains the possibility of the same plaintext communication occurring during the interval between a domain name resolution session and a new one.

Therefore, to achieve complete privacy preservation in DNS domain name resolution, a method for discovering authoritative DNS servers that support encrypted communication while considering both privacy preservation and compatibility is essential.

2 PROPOSED METHOD

In this paper, we propose a method that reconciles compatibility and privacy preservation by adding a dummy DNS Name Server (NS) record indicating the support information of encrypted communication of each authoritative DNS server in each zone's parent authoritative DNS server.

Generally, when a DNS full-service resolver receives a DNS query, it refers to the NS records in the pre-configured root.hints file. It then receives NS records from authoritative DNS servers for root, top-level domain (TLD), second-level domain (SLD), and so on, indicating the delegation destination authoritative DNS servers and proceeding with the domain name resolution.

*The author is associated with two institutions.

CoNEXT-SW '23, December 8, 2023, Paris, France

ACM ISBN 979-8-4007-0452-9/23/12.
https://doi.org/10.1145/3630202.3630228

In this paper, we propose a method that allows a DNS full-service resolver to discover authoritative DNS servers that support encrypted communication by adding "a dummy NS record indicating the support information of encrypted communication of each authoritative DNS server" in addition to the delegation NS records. The dummy NS record consists of 3 elements: (1) the FQDN of the delegated authoritative DNS server, (2) a string indicating encryption support information, and (3) a non-existed top-level domain name.

For example, to indicate that "ns1.example.com" supports DNS over TLS (DoT) and DNS over HTTPS (DoH) but not DNS-over-QUIC (DoQ), a dummy NS record like "example.com NS ns1.example.com.TEHEQD.invalid" is added to the parent zone "com." Here, the "TEHEQD" represents (T for DoT, E for Enable, H for DoH, Q for DoQ, and D for Disable), indicating the availabilities of DoH and DoT. In addition, the non-existed top-level domain will be configured in the DNS full-service resolver to avoid unnecessary DNS queries.

The communication flow using the proposed method is as follows. Initially, the DNS full-service resolver receives a DNS query from an end terminal and references the root.hint file to locate a root authoritative DNS server that supports encrypted communication. If it discovers a root authoritative DNS server that supports encrypted communication, it sends the DNS query over encrypted communication. The root authoritative DNS server sends NS records indicating the delegation destination and encryption support information to the DNS full-service resolver by the dummy NS record in the "authoritative section" of the DNS response in addition to the real delegation destinations. The DNS full-service resolver searches for the TLD authoritative DNS servers supporting encrypted communication from the NS records and, if found, sends the DNS query over encrypted communication. This process is repeated iteratively for SLD authoritative DNS servers and beyond, ultimately resulting in the DNS full-service resolver sending the result back to the end terminal. Through the above procedure, all DNS communication paths are encrypted, and privacy will be preserved.

3 EXPERIMENT

To evaluate the compatibility and privacy preservation feature in the proposed method, we constructed a prototype experimental environment. Figure 1 illustrates the system configuration of the experimental environment, and we will highlight the key implementation points in the following.

(1) Enable encrypted communication on all DNS servers.
(2) Add a dummy NS record indicating the status of encrypted communication to authoritative DNS servers.
(3) Develop the capability to search for authoritative DNS servers that support encrypted communication.
(4) Enable DNS full-service resolvers to engage in encrypt-ed communication with authoritative DNS servers.

In order to demonstrate the real-world applicability of the proposed method, it's important to confirm that it works seamlessly with the already standardized DNSSEC and does not pose compatibility issues when used in conjunction with Q-min. Ideally, the points (3) and (4) should be implemented in the bind9 for DNS full-service resolvers. However, due to the complexity and high difficulty level of bind9 customization, a DNS Proxy is developed in the prototype environment.

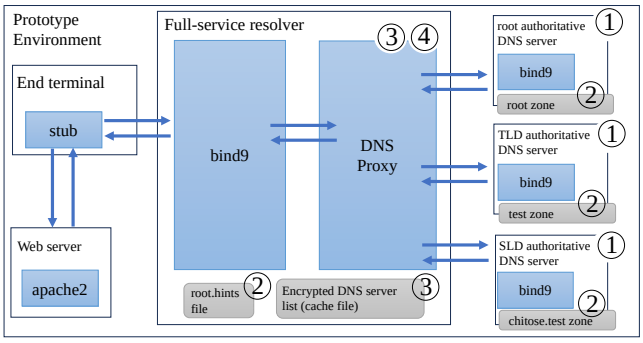

Figure 1: Prototype Environment Overview.

4 RESULTS AND RESEARCH PLAN

To achieve privacy preservation in DNS communication, it is necessary to encrypt all DNS traffic. In this paper, we proposed an authoritative DNS server discovery method that considers both compatibility and privacy preservation. The wide deployment of this method will enhance DNS domain name resolution privacy.

At the present stage, the implementation of the DNS-Proxy has been completed in the prototype environment. By adding a dummy of the NS record indicating support for encrypted communication of child authoritative DNS servers to the parent authoritative DNS server, We confirmed that the authoritative DNS servers that support encryption could be discovered as expected, and the domain name resolution could be encrypted in all DNS communication.

Our next steps involve verifying that there are no critical issues when using the proposed method in conjunction with DNSSEC and Q-min. Additionally, we will confirm that our method can initiate encrypted communication more rapidly than the probing policy proposed in the Internet-Draft.

We also plan to submit our proposed method as information for discussion before the expiration of the IETF's dprive-unilateral-probing Internet-Draft (3 March 2024).

ACKNOWLEDGEMENTS

This work was partly supported by JSPS KAKENHI Grant Number 23K17623.

REFERENCES

[1] Stéphane Bortzmeyer, Ralph Dolmans, and Paul E. Hoffman. 2021. DNS query name minimisation to Improve Privacy. IETF RFC9156. https://doi.org/10.17487/RFC9156
[2] Daniel Kahn Gillmor, Joey Salazar, and Paul E. Hoffman. 2023. Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS. https://datatracker.ietf.org/doc/draft-ietf-dprive-unilateral-probing/, (Accessed on 20 Sep. 2023).
[3] Basileal Imana, Aleksandra Korolova, and John Heidemann. 2021. Institutional Privacy Risks in Sharing DNS Data. In *Proceedings of the Applied Networking Research Workshop* (Virtual Event, USA) *(ANRW '21)*. Association for Computing Machinery, New York, NY, USA, 69–75. https://doi.org/10.1145/3472305.3472324