***Павлюк Олександр-Юрій Святославович / Pavliuk O.- I. S.***

*аспірант / postgraduate*

*Lviv Polytechnic National University, S. Bandery St. 12, Lviv, 79013*

*ORCID ID: 0009-0008-6985-203X*

**Enhancing Web Performance and Security using HTTPS DNS Records and DNS-over-HTTPS Synergy**

The modern web relies heavily on the Domain Name System (DNS) to translate human-readable domain names (like www.example.com) into the IP addresses that computers use to communicate. While seemingly simple, the traditional DNS system faces significant challenges regarding both performance and security. Users experience latency due to the multiple recursive lookups often required to resolve a domain name. Furthermore, traditional DNS queries are typically unencrypted, making them vulnerable to eavesdropping and manipulation. This exposure allows attackers to intercept and alter DNS responses, potentially redirecting users to malicious websites or stealing sensitive information. Even worse, unencrypted DNS queries reveal a user's browsing history to anyone monitoring the network, raising serious privacy concerns.

To address these critical shortcomings, several key technologies have emerged: HTTPS DNS records (a specialized type of Service Binding (SVCB) record), DNS-over-HTTPS (DoH), and Encrypted ClientHello (ECH).

This article argues that the synergistic combination of HTTPS DNS records and DoH significantly improves both web performance and security. By securing DNS lookups and providing optimized connection information, these technologies create a faster, more private, and more secure browsing experience. We will explore how these technologies work, examine their individual benefits, and demonstrate how their combined use creates a powerful solution for the challenges facing the traditional DNS system.
**Technology Overview**

* **HTTPS records** are a specialized type of **Service Binding (SVCB)** record designed specifically for HTTPS services [1]. These records provide clients with comprehensive information about how to connect to a web server. An HTTPS record includes the hostname and port of the server, the supported HTTP versions (e.g., HTTP/2, HTTP/3), and crucial security parameters, including configuration details for Encrypted ClientHello (ECH). By providing this information directly in the DNS response, HTTPS records optimize the HTTPS connection process, reducing latency and enabling support for ECH.

*Table 1. HTTPS DNS packet structure*

|  |  |
| --- | --- |
| **Element** | **Description** |
| TCP Header | Contains information for reliable, ordered delivery of data between applications. Includes source and destination ports, sequence |
| \* ClientHello | The client initiates the handshake, advertising supported ciphers, TLS versions, and extensions |
| \* (Other Handshake) | Further exchanges (key exchange, etc) |
| Encrypted Data |  |

* **DNS-over-HTTPS (DoH)** enhances user privacy and security by encrypting DNS queries. Instead of sending queries in plain text over traditional protocols like UDP or TCP, DoH encapsulates them within HTTPS traffic [2]. This prevents eavesdroppers, such as ISPs or network administrators, from viewing or manipulating DNS requests. DoH offers increased privacy, protection against DNS-based attacks like tampering and spoofing, and the potential to bypass censorship in some situations.
* **Encrypted ClientHello (ECH)** is a feature of the TLS protocol that encrypts the Server Name Indication (SNI) field within the TLS handshake [3]. The SNI is a crucial piece of information that tells the server which website the client is trying to access. Without ECH, this information is sent in plain text, revealing the user's browsing history to anyone monitoring the network. ECH encrypts the SNI, protecting user privacy by hiding the websites they visit.

These technologies work together synergistically to enhance both web performance and security. DoH ensures that HTTPS record lookups are themselves secure and protected from manipulation. The HTTPS record then provides the client with all the necessary information to establish an efficient and secure HTTPS connection, including the configuration needed to use ECH. As an example, let’s explore a connection process with **DoH and SVCB applied**:

1. A user attempts to visit https://www.example.com.
2. The browser, configured to use DoH, sends a DNS query for www.example.com over HTTPS to a DoH resolver. This query, including the domain name, is encrypted.
3. Because the query is encrypted, eavesdroppers cannot see which website the user is trying to access. The query is also protected from tampering.
4. The DoH resolver performs the DNS lookup, potentially retrieving an HTTPS record (SVCB record) for www.example.com. Critically, the HTTPS record itself is fetched securely via DoH.
5. The DoH resolver returns the HTTPS record to the browser, *encrypted* within the HTTPS response. This record contains all the information needed for a secure and optimized connection, including the server's IP address, supported protocols (like HTTP/2 or HTTP/3), and ECH configuration.
6. The browser uses the information in the HTTPS record to establish a direct, secure HTTPS connection to the server. If ECH is configured, the SNI is encrypted as well. The connection is faster because the browser has all the necessary details upfront, avoiding additional lookups or redirects.

**Summary and Conclusion**

The combination of HTTPS DNS records, DNS-over-HTTPS (DoH), and Encrypted ClientHello (ECH) offers significant improvements in web performance, user privacy, and overall security:

* **Privacy:** DoH encrypts DNS queries, preventing eavesdropping and protecting user privacy. Traditional DNS queries are sent in the clear.
* **Security:** DoH protects against DNS manipulation and spoofing. Traditional DNS is highly vulnerable to these attacks.
* **Performance:** The HTTPS record provides all the necessary information for a secure connection in a single, secure DNS lookup, reducing latency. Traditional DNS often requires multiple lookups and may involve redirects.
* **End-to-End Security:** With DoH and HTTPS records, the entire process, from DNS lookup to HTTPS connection, is secured. This end-to-end security is a significant improvement over the vulnerable traditional approach.

**REFERENCE LIST**

[1] Bishop, M., P. McManus, and A. Wilk. "Service Binding and Parameter Specification for the HTTP/HTTPS Schemes." Internet Engineering Task Force, RFC 9460, 2023. https://datatracker.ietf.org/doc/html/rfc9460.

[2] Hoffman, P., Y. Nir, and P. E. Davies. "DNS Queries over HTTPS (DoH)." Internet Engineering Task Force, RFC 8484, 2018. https://datatracker.ietf.org/doc/html/rfc8484.

[3] Rescorla, E., M. Thomson, and C. Huitema. "Encrypted ClientHello." Internet Engineering Task Force, RFC 9146, 2022. <https://datatracker.ietf.org/doc/html/rfc9146>.

[4] Zirngibl, J., P. Sattler, and G. Carle. "A First Look at SVCB and HTTPS DNS Resource Records in the Wild." 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Delft, Netherlands, 2023, 470–74. [https://doi.org/10.1109/EuroSPW59978.2023.00058](https://www.google.com/search?q=https://doi.org/10.1109/EuroSPW59978.2023.00058&authuser=5).