***Нємкова Олена Анатоліївна. / Nyemkova E.A.***

*доктор технічних наук, професор /DCs, Prof.*

*ORCID: 0000-0003-0690-2657*

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

*аспірант / postgraduate*

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

*Національний університет «Львівська політехніка», Львів, Бандери, 12, 79013*

**Браузерне розширення на основі QUIC та RDAP: Швидкий та зручний доступ до децентралізованих Handshake доменів**

**Ключові слова:***DNS (Система доменних імен), Handshake, RDAP, QUIC, децентралізація, безпека, конфіденційність*

**Вступ.**

Cистема доменних імен (DNS) в своїй традиційній формі виконує ключову роль в роботі інтернету, перетворюючи зрозумілі для людей доменні імена в машинні IP-адреси. Втім, DNS має ряд вроджених недоліків, пов'язаних з її централізованою природою. Покладаючись на ієрархічну структуру серверів [1], DNS може бути вразливою до цензури, атак з перехопленням даних або технічних збоїв у ключових точках ієрархії. Це може призвести до примусової недоступності сайтів, порушень конфіденційності користувачів чи навіть масштабних відключень певних частин мережі [2].

Протокол Handshake прагне вирішити ці проблеми, представляючи децентралізований підхід до управління доменними іменами. Використовуючи технологію блокчейн, Handshake розподіляє повноваження з управління доменами верхнього рівня (TLD) між численними учасниками мережі, усуваючи єдині точки відмови чи контролю [3]. Однак, наразі популярні браузери не мають вбудованої можливості розпізнавати домени Handshake. Цей недолік ускладнює широке впровадження протоколу, оскільки значна частина користувачів все ще покладається на традиційні веб-браузери [4]. Саме тут браузерне розширення, здатне спрощувати процес розпізнавання доменів Handshake, може відіграти значну роль.

**Функціонал розширення.**

Ключовим завданням браузерного розширення є перехоплення запитів з браузера та визначення, чи належить введений домен до мережі Handshake. Якщо так, розширення ініціює процес розпізнавання, який дещо відрізняється від традиційного DNS. Ідеальний сценарій передбачає співпрацю з реєстраторами доменів Handshake для формування актуальної бази даних про адреси відповідних серверів RDAP (Registration Data Access Protocol).

RDAP є сучасним протоколом, який замінює застарілий WHOIS, забезпечуючи стандартизований та зручніший формат для роботи з реєстраційними даними доменів [5]. Використовуючи RDAP, розширення отримує інформацію про відповідний домену неймсервер або неймсервери безпосередньо, обминаючи ієрархічну структуру традиційного DNS та потенційні проблеми, пов'язані з нею.

Для ефективної взаємодії з неймсерверами розширення може використовувати протокол QUIC (Quick UDP Internet Connections). Завдяки низці оптимізацій, QUIC здатен знизити затримки під час встановлення з'єднання (handshaking) та пришвидшити передачу даних [6], забезпечуючи плавніший користувацький досвід у порівнянні з традиційним DNS. Використання шифрування у QUIC також додає додатковий рівень безпеки для передачі даних. За відсутності підтримки протоколу QUIC кінцевим неймсервером, може використовуватись UDP (для даних малого розміру) або TCP (для даних, перевищуючих розмір стандартного пакету UDP) [7].

**Принцип роботи розширення.**

При введенні користувачем доменного імені у браузері, процес роботи розширення виглядає наступним чином:

1. Визначення приналежності домену до типу Handshake.
2. Отримання адреси відповідного RDAP-сервера (через співпрацю з реєстратором чи динамічне виявлення).
3. Запит до RDAP-сервера для отримання адреси авторитетного неймсервера (або неймсерверів) для домену.
4. Комунікація з неймсервером за протоколом QUIC/UDP/TCP та отримання необхідних даних.
5. Передача отриманої інформації (IP-адреси) браузеру.



*рис.1 – Спрощена схема роботи браузерного розширення*

**Переваги та недоліки.**

Оскільки браузерне розширення працює безпосередньо з запитами браузера, можуть виникнути певні проблеми із сумісністю з функціями шифрування DNS, такими як DoH (DNS over HTTPS) та DoT (DNS over TLS). DoH і DoT інкапсулюють DNS-запити в безпечні HTTPS або TLS-з'єднання, що ускладнює для розширення ідентифікацію та перехоплення DNS-запитів для подальшого аналізу [8]. Це може стати перешкодою для користувачів, які орієнтовані на конфіденційність і використовують шифрування DNS.

Втім, описане розширення забезпечує зручний користувацький досвід і за правильної конфігурації може використовуватись спільно з протоколами DoH/DoT. Воно усуває потребу в складних налаштуваннях, знижує вхідний технічних поріг для недосвідчених користувачів, роблячи Handshake домени більш доступним для широкої аудиторії.

**Висновки.**

Традиційна система доменних імен (DNS) має вбудовані недоліки, пов'язані з її централізованим характером. Протокол Handshake прагне вирішити ці проблеми, використовуючи децентралізований підхід до управління доменами верхнього рівня. Спеціалізоване браузерне розширення, здатне перехоплювати DNS-запити та взаємодіяти з неймсерверами Handshake, може значно спростити використання доменів Handshake у звичайних веб-браузерах. Використання сучасних протоколів, таких як RDAP та QUIC, дає змогу підвищити конфіденційність, безпеку передачі та розпізнавання даних.

**Література:**

[1] Graham-Cumming J. Cloudflare outage on July 17, 2020. Cloudflare Blog. Cloudflare, Inc.; 2020 Jul 18. URL: <https://blog.cloudflare.com/cloudflare-outage-on-july-17-2020>

[2] Dooley M., Rooney T. Introduction to the Domain Name System (DNS). In: Cryptography and Network Security (7th ed.). Hoboken, NJ: Wiley-IEEE Press; 2017: p. 29-55. DOI: 10.1002/9781119328292.ch2

[3] About Handshake – Namebase Learning Center. Seattle: Namebase; c2023. URL: <https://learn.namebase.io/about-handshake/about-handshake>

[4] Rajendran B., Palaniappan D. A Universal Domain Name Resolution Service – Need and Challenges - Study on Blockchain Based Naming Services. In: 2022 IEEE Region 10 Symposium (TENSYMP); 2022 Aug 4-7; Mumbai, India. Piscataway, NJ: IEEE; 2022. DOI: 10.1109/TENSYMP54529.2022.9864361

[5] Gañán C. H. WHOIS sunset? A primer in Registration Data Access Protocol (RDAP) performance. In: 14th IFIP,2021 Aug 18-20: Guildford, United Kingdom: Springer; 2021. р. 72–87. DOI: 78-3-903176-40-9

[6] Nepomuceno T. C. C., Nepomuceno K. T. C. Quantifying Webpage Performance: A Comparative Analysis of TCP/IP and QUIC Communication Protocols for Improved Efficiency. Data. 2023; 8(8):134. DOI: 10.3390/data8080134

[7] Kosek M., Schumann L., Marx R. DNS privacy with speed?: evaluating DNS over QUIC and its impact on web performance. In: Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22); 2022 Oct 25–27; Nice, France. New York, NY: ACM; 2022. p. 44-50. DOI: 10.1145/3517745.3561445

[8] Hounsel A., Borgolte K., Schmitt P., Holland J., Feamster, N. Analyzing the costs (and benefits) of DNS, DoT, and DoH for the modern web. In: Proceedings of the Applied Networking Research Workshop (ANRW '19); 2019 Jul; Montreal, Canada. New York, NY: ACM; 2019. p. 20-22. DOI: 10.1145/3340301.3341129