DNS 통신 암호화를 위한 IETF 표준기술 비교 분석

김평수
한국공학대학교
pskim@tukorea.ac.kr

Comparative Analysis of Encrypted DNS Communication Standards at the IETF

Pyung Soo Kim
Tech University of Korea

요 약

본 논문에서는 기존의 평문 기반의 DNS의 보안 취약성을 해결하고자 국제표준화 기구인 IETF에서 개발된 대표적 DNS 통신 암호화 표준기술을 소개하고 기본설계측면, 성능 및 적용 이슈 측면, 개발 및 확산 현황 측면에서 비교 분석을 수행한다.

Ⅰ. 서 론

DNS에서 "라스트 마일(last mile)"은 사용자 기기와 DNS 리졸버 사이의 네트워크 구간을 의미한다. 이 부분은 암호화되지 않은 DNS 쿼리가 로컬 라우터, ISP 및 기타 중개 노드를 통과하기 때문에 감시 및 조작에 특히 취약하다. 암호화된 DNS 프로토콜은 DNS 쿼리가 사용자 기기에서 DNS 리졸버로 안전하게 전송되도록 보장하여 이 라스트 마일을 보호하고, 전송 중 제3자가 트래픽을 가로채거나 수정하는 것을 방지한다. 암호화된 DNS가 없으면 라스트 마일은 심각한 개인 정보 보호 위험을 초래하며, 특히 공용 Wi-Fi 핫스팟이나 기업 네트워크와 같이 네트워크 트래픽이 모니터링되는 환경에서 더욱 그렇다[1]-[6]. 본 논문에서는 국제표준화 기구인 IETF에서 개발된 대표적 DNS 통신 암호화 표준기술을 소개하고 다양한 측면에서 비교 분석을 수행한다.

Ⅱ. 본론 및 결론

<표 1> 정리했듯이, IETF에서 개발된 대표적 DNS 통신 암호화 표준으로는 DNS over TLS(DoT), DNS over DTLS(DoDT), DNS over HTTPS(DoH), DNS over QUIC(DoQ)이 있다. 이 표준 기술들에 대해서 <표 2>에서는 기본 설계 측면에서 비교 분석하고, <표 3>에서는 성능 및 적용 이슈 측면에서 비교 분석하고, <표 4>에서는 개발 및 적용 확산 측면에서 비교 분석을 한다.

표 1. 대표적 DNS 통신 표준 기술

기술	RFC	표준명	IETF WG
DNS with Plaintext	RFC 1035	Domain names - implementation and specification	DNS
DNS over TLS	RFC 7858	Specification for DNS over Transport Layer Security (TLS)	DPRIVE
	RFC 8094	DNS over Datagram Transport Layer Security (DTLS)	DPRIVE
DNS over HTTPS	RFC 8484	DNS Queries over HTTPS (DoH)	DOH
DNS over QUIC	RFC 9250	DNS over Dedicated QUIC Connections	DPRIVE

표 2. 기본 설계 측면에서의 비교

항목	DoT	DoDT	DoH	DoQ
IETF 표준	RFC 7858	RFC 8094	RFC 8484	RFC 9250
기반 전송 계층	TCP	UDP	TCP	UDP
응용계층 프로토콜	없음	없음	HTTPS	없음
Fallback 지원 (대체수단/옵션)	지원	지원	미지원	지원
표준 TLS 암호화	사용	사용	사용	사용
포트 번호	853	853	443	853

표 3. 성능 및 적용 이슈 측면에서의 비교

항목	DoT	DoDT	DoH	DoQ
DNS 트래픽 분석 방지	부분적 가능	부분적 가능	가능	부분적 가능
DNS 트래픽 블록 가능성	용이함	용이함	어려움	용이함
주요 제약점	TCP의 내재적 제약점 (3-way handshake, HOL Blocking)	Experimental standard (제한된 구현)	오버헤드로 인한 늦은 응답시간 네트워크 가시성 이슈, TCP의 내재적 제약점	가장 최근에 개발된 표준 기술로 확산 초기 단계
DNS 클라이언트 변경 최소화	부분적가능	불가능	가능	불가능
DNS 쿼리 처리 시간 (응답속도)	보통	우수	미흡	매우 우수

표 4. 개발 및 적용 확산 측면에서의 비교

항목	DoT	DoDT	DoH	DoQ
확산 현황 (대중성)	상대적으로 성숙된 솔루션	제한된 구현	점차적으로 확산되나, 가시성문제로 제한적	가장 최근 기술로 확산 초기 상황
DNS 클라이언트 개발 현황	우수	미흡	보통	보통
DNS 클라이언트 개발 현황	(OS 지원) Windows, Android (전용SW) Stubby, Unbound	-	(브라우저) 파이어폭스, 크롬 (OS지원) Windows Server 2022	(전용SW) AdGuard NextDNS (오픈소스) quicdoq, doqclient
DNS 리졸버/서버 개발 현황	우수	미흡	우수	보통
DNS 리졸버/서버 개발 사례	Quad9 Cloudflare Google AdGuard PowerDNS DNS4EU	RouteDNS	Cloudflare Google Amazon PowerDNS DNS4EU	Cloudflare AdGuard PowerDNS DNS4EU (오픈소스)Unbound

Acknowledgement

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-학·석사연계ICT핵심인재양성의 지원(IITP-2025-RS-2022-00156326, 50%)과 정부(과학기술정보통신부)의 재원으로 ICT 표준화포럼 과제의 지원(2025-FM-02, 50%)을 받아 수행된 연구임

참 고 문 헌

[1] 김평수, “안전한 웹사이트 접속을 위한 IETF 표준 기술 동향 분석,” 한국통신학회지 정보와통신, vol.36, no.6, pp. 32-40, 2019

[2] 이웅희, 허준번, “TLS기반 패킷 검사 우회 표준 기술 분석 및 미래 전술네트워크 운용 가능성 연구,” 한국통신학회논문지, vol.47, no.9, pp. 1370-1380, 2022

[3] M. Lyu, H. H. Gharakheili, V. Sivaraman, "A Survey on DNS Encryption: Current Development, Malware Misuse, and Inference Techniques", ACM Computing Surveys, vol. 55, no. 8, pp. 1 - 28, 2023.

[4] G. Hu and K. Fukuda, "Privacy Leakage of DNS over QUIC: Analysis and Countermeasure," 2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Osaka, Japan, 2024, pp. 518-523.

[5] J. Sengupta, M. Kosek, J. Fries, S. Ferlin-Reiter and V. Bajpai, "On Cross-Layer Interactions of QUIC, Encrypted DNS and HTTP/3: Design, Evaluation, and Dataset," IEEE Transactions on Network and Service Management, vol. 21, no. 3, pp. 2992-3007, June 2024.

[6] A. Aydeger, S. Hoque, E. Zeydan, K. Dev, "Analysis of Robust and Secure DNS Protocols for IoT Devices", Proceedings of the 2025 IEEE International Conference on Communications (ICC 2025), Montreal, Canada, June 8 - 12, 2025