CT 모니터를 이용한 DNS 다운그레이드 공격 완화 기법

황명빈, 김현수, 권태경

서울대학교

auddl1020@snu.ac.kr, wayles@snu.ac.kr, tkkwon@snu.ac.kr

Mitigating DNS Downgrade Attacks through CT Monitors

Myungbin Hwang, Hyunsoo Kim, Ted “Taekyoung” Kwon

Seoul National Univ.

요 약

Domain Name System(DNS)은 중요한 인터넷 인프라로서, DNS의 보안 취약점은 심각한 데이터 유출로 이어질 수 있다. 기존 DNS 통신은 암호화되지 않아 중간자 공격에 노출되었으나, 최근 DNS over TLS(DoT), DNS over HTTPS(DoH) 등의 보안 프로토콜이 도입되어 통신의 기밀성과 무결성을 강화하였다. 그러나 이러한 방식도 다운그레이드 공격의 가능성이 여전히 존재한다. 이는 DNS 리졸버가 DoH 연결 실패 시 평문 통신으로 전환하는 opportunistic privacy profile에서 비롯된다. 본 논문에서는 Certificate Transparency(CT) 로그의 모니터를 활용하여 CT 로그에 기록된 DoT/DoH 리졸버의 인증서를 사전에 검증하고 갱신함으로써 중간자 공격 및 다운그레이드 공격을 방지하는 방법을 제안한다. 이 방법은 DNS의 보안을 향상시키고 프라이버시를 보호하는 데 기여할 것이다.

Ⅰ. 서 론

많은 인터넷 응용 프로그램 및 서비스들이 Domain Name System (DNS) 정보를 기반으로 동작하므로 DNS에 대한 공격은 광범위한 프라이버시 침해 및 데이터 유출로 이어질 수 있다. 그러나 기존 DNS 프로토콜에서는 클라이언트와 DNS 리졸버, DNS 리졸버와 DNS 네임 서버 간 정보를 평문 형태로 전송하므로 제 3자에 의한 도청, 위변조 등 중간자 공격의 위험이 존재하였다. 이러한 취약점을 해결하기 위하여 클라이언트와 DNS 리졸버 사이에는 사용자의 프라이버시를 강화할 수 있는 DNS over TLS(DoT)[1]와 DNS over HTTPS(DoH)[2]을 통해 데이터 기밀성(Confidentiality), 무결성(Integrity), 그리고 리졸버의 인증(Authentication)을 제공하였고, DNS 리졸버와 DNS 네임 서버 사이에는 데이터의 무결성과 인증을 제공할 수 있는 DNS Security Extension(DNSSEC)[3]이 도입되었다. DoT, DoH는 DNS 쿼리 전송을 위해 각각 TLS와 HTTPS 프로토콜을 이용하여 DNS 요청과 응답을 암호화함으로써 중간자 공격을 방지한다.

그러나 DoT, DoH, DNSSEC에 대한 다운그레이드 공격이 여전히 가능하다. [4][5][6] 본 논문에서는 중간자 공격 발생 시 사용자에게 많은 피해를 줄 수 있는 클라이언트와 DNS 리졸버 간의 통신, 그중에서도 상대적으로 많이 사용되고 있는 DoH 프로토콜의 다운그레이드 공격에 집중하였다. [7] DNS 리졸버들은 기본적으로 DoH 연결에 실패하면 DNS 통신을 중지하는 strict privacy profile 대신 평문으로 통신을 이어가는 opportunistic privacy profile을 채택하고 있다. 이를 이용하여 공격자는 그림 1에서와 같이 DoH 리졸버의 IP 주소에 대한 DNS 요청이나 클라이언트와 DoH 리졸버 간 TCP 트래픽 자체를 차단한다. 혹은 DoH 리졸버에 대한 잘못된 IP를 전달하거나 위조된 TCP RST 패킷을 전달하여 DoH 리졸버와의 TCP 연결을 해제한다. 위와 같은 방식으로 DoH 리졸버에 대한 연결에 실패하면 opportunistic privacy profile에 의해 클라이언트는 평문으로 DNS 통신을 수행하게 된다. [6]

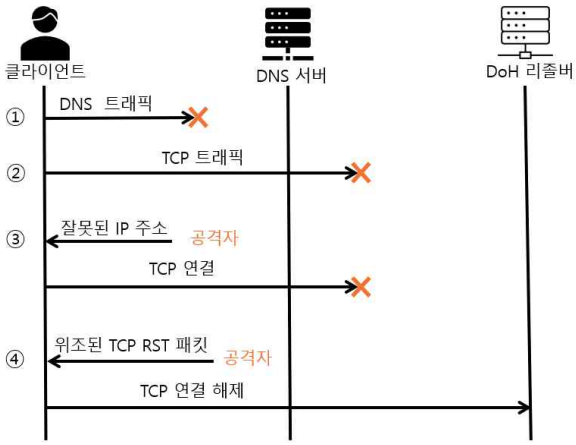

그림 1. DoH 다운그레이드 공격 방식 [6]

본 논문에서는 Certificate Transparency(CT)[8] 로그의 모니터(Monitor)를 활용하여 DoT/ DoH 프로토콜을 기존 DNS 프로토콜로 다운그레이드하는 공격을 방지하는 방법을 제안한다.

Ⅱ. 본론

TLS 혹은 HTTPS 서버의 인증서(Certificate)는 발급되는 과정에서 CT 로그에 기록되며 CT 모니터는 로그에 기록된 인증서 발급, 변경 등의 정보를 확인하여 악의적인 인증서 발급, 인증서 부정 사용 등의 위협을 탐지하는 auditor의 역할을 수행한다. DoT/DoH 리졸버는 클라이언트와 TLS, HTTPS 연결 후 DNS 쿼리를 수행하므로 보안 세션 수립에 필요한 인증서를 Certificate Authority(CA)로부터 발급받으며, 이때 CA는 발급한 인증서를 CT 로그에 전송한다. 즉, DoT/DoH 리졸버의 인증서를 CT 모니터를 통해 확인할 수 있다. DNS 다운그레이드 공격은 DoT/DoH 리졸버와의 연결을 차단함으로써 해당 프로토콜을 지원하지 않는 것으로 판단,

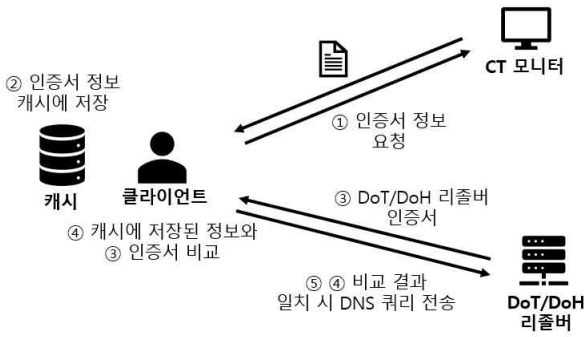

그림 2. CT 모니터를 통해 DoT/DoH 리졸버의 인증서를 검증하는 과정

평문으로 쿼리를 전송하도록 하므로, DNS 클라이언트가 사전에 DoT/DoH 리졸버의 인증서 정보를 알고 검증할 수 있다면 공격을 방지할 수 있을 것이다.

그림 2는 CT 모니터를 통해 DoT/DoH 리졸버의 인증서를 검증하는 과정을 도시한다. 우선, DNS 쿼리를 요청하는 클라이언트는 애플리케이션 단에서 신뢰하는 CT 모니터의 연결 정보를 내장하고 있음을 가정한다. 이는 마치 신뢰하는 Root 인증서가 소프트웨어, OS에 함께 패키징 되어 있는 것과 유사하다. 다음으로 DNS 쿼리를 보낼 DoT/DoH 리졸버가 정해지면, 클라이언트는 CT 모니터로부터 해당 DoT/DoH 리졸버의 인증서를 받아 캐시에 저장한다. 이후 DNS 정보가 필요할 때, 캐시에 저장된 정보를 바탕으로 DoT/DoH 리졸버에 연결을 시도한다. 연결 과정에서 리졸버로부터 받은 인증서를 캐시에 저장된 인증서와 비교하여 같으면 DNS 통신을 수행한다. 만약 두 인증서가 다르다면 중간자 공격이 있는 것으로 판단하고 이에 대한 대응으로 넘어갈 수 있을 것이다.

인증서가 변경, 만료될 수 있으므로, 본 논문에서는 두 가지 방식으로 CT 모니터로부터 인증서 정보를 업데이트한다. 우선 CT 모니터에서 받은 인증서의 만료 날짜를 기준으로 그로부터 일정 시간 이전에 CT 모니터로부터 다시 인증서 정보를 받아 캐시를 업데이트할 수 있다. 이때 만료 날짜부터 얼마나 이전에 갱신할지 그 시간을 일정 범위 내에서 랜덤으로 결정함으로써 동시에 다수의 클라이언트 애플리케이션이 CT 모니터에게 새로운 인증서 갱신을 요청하는 것을 방지한다. 다음으로, DoT/DoH 리졸버로부터 받은 인증서 정보가 캐시에 저장된 정보와 다른 경우, 다운그레이드 공격이 아닌 정상적인 상황에서 인증서가 변경되었을 가능성이 있으므로 CT 모니터로부터 정보를 다시 받아와 캐시를 갱신한다. 캐시 정보가 변경되었으므로 두 인증서를 한 번 더 비교하고 새로 가져온 정보와 일치하면 DNS 통신을 지속하고 일치하지 않으면 종료한다. 본 논문에서는 CT 모니터에 대한 검증과 클라이언트와 CT 모니터 간 전달되는 정보에 대한 무결성은 보장된다고 가정하였다.

일반적으로 클라이언트가 사용하는 DNS 리졸버는 정해져 있으며 캐시에 인증서 정보를 저장해놓은 뒤 만료 기간 직전, 혹은 리졸버로부터 받은 인증서가 다를 때에만 CT 모니터에 쿼리를 보내게 되므로 CT 모니터에 대한 트래픽이 증가하는 문제를 방지할 수 있다.

Ⅲ. 결론

본 논문에서는 CT 모니터를 활용하여 DNS 다운그레이드 공격을 완화하는 방법을 제안하였다. DoT와 DoH 프로토콜은 클라이언트와 DNS 리졸버 간 요청과 응답이 평문으로 진행되어 중간자 공격에 취약하다는 점을 개선하기 위해 고안되었으나 여전히 다운그레이드 공격이 가능하다는 문제점이 존재한다. 이러한 문제점은 DoT/DoH 리졸버에서 사용하는 TLS/HTTPS 인증서에 대한 정보를 미리 알고 있다면 개선 가능하다. 따라서 본 논문에서는 CT 모니터를 이용하여 DoT/DoH 리졸버의 인증서 정보를 저장한 뒤 연결 과정에서 비교하여 중간자 공격 및 다운그레이드 공격을 막음으로써 프라이버시를 향상하는 방법을 제시하였다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00220985).

참 고 문 헌

[1] Hu, Zi, et al. "RFC 7858: Specification for DNS over transport layer security (TLS)." (2016).

[2] Hoffman, Paul, and Patrick McManus. "Rfc 8484: Dns queries over https (doh)." (2018).

[3] Hoffman, P. "RFC 9364: DNS Security Extensions (DNSSEC)." (2023).

[4] Lee, Sangtae, Youngjoo Shin, and Junbeom Hur. "Return of version downgrade attack in the era of TLS 1.3." Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies. 2020.

[5] Huang, Qing, Deliang Chang, and Zhou Li. "A comprehensive study of {DNS-over-HTTPS} downgrade attack." 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20). 2020.

[6] Heftrig, Elias, Haya Shulman, and Michael Waidner. "Downgrading {DNSSEC}: How to Exploit Crypto Agility for Hijacking Signed Zones." 32nd USENIX Security Symposium (USENIX Security 23). 2023.

[7] García, Sebastián, et al. "Large scale measurement on the adoption of encrypted DNS." arXiv preprint arXiv:2107.04436 (2021).

[8] Laurie, Ben, Adam Langley, and Emilia Kasper. "RFC 6962: Certificate Transparency." (2013).