DNS와 SNI를 이용한 인터넷 검열

윤재웅* 김경호** 서화정**

*한성대학교 컴퓨터공학부

**한성대학교 IT 융합공학부

Internet Censorship using DNS and SNI

Jae-Woong Yun*

*School of Computer Engineering, Hansung University.

Kyung-Ho Kim** Hwa-Jeong Seo**

**Division of IT convergence Engineering, Hansung University.

요 약

방송통신심위위원회가 2000년대에 들어서면서 ISP(Internet Service Provider)와 협력하여 HTTP 차단, DNS(Domain Name System) 차단을 이용하여 불법 정보를 담고 있는 사이트를 차단하기 시작했다. 올해 2월 새로운 인터넷 접속차단 정책인 SNI(Server Name Indication) 필드 차단 방식을 도입했다. 주요 논란점은 차단 과정에서 불법적으로 패킷의 일부분(Header)을 해킹한다는 것이다. 이에 본 논문에서는 DNS 암호화 기반 표준으로 제정된 DNSSEC, DNS-over-TLS, DNS-over-HTTPS을 살펴보고, TLS 1.3에서 제안된 SNI 암호화인 ESNI(Encryption SNI)에 대해 확인해 보도록 한다.

I. 서론

검열에 대한 차단 방식으로는 세 가지로 정리할 수 있다[1].

첫 번째, IP 차단으로 HTTP 평문 통신을 이용해 IP 주소로 연결되는 웹 서버에 불법 사이트가 하나뿐이라도 서버에 존재하는 여러 사이트를 모두 차단한다.

두 번째, DNS 차단은 ISP마다 관리하는 DNS 서버에 불법 사이트의 IP 주소가 들어올 때 차단안내페이지의 IP 주소를 알려주는 파밍(Pharming) 기법의 차단 방식이다.

세 번째, 현재 시행중인 SNI 차단으로 SNI는 TLS의 확장이다. 현재 통용되고 있는 TLS 프로토콜을 통한 HTTPS 암호화 통신을 한다더라도, 여전히 최초에 어떤 서버의 무슨 사이트와 통신할 것인지를 알려주는 SNI는 암호화되지 않은 평문으로 노출을 이용한 차단이다.

본 논문에서는 DNS 암호화 표준으로 제정된 DNSSEC, DNS-over-TLS, DNS-over-HTTPS을 살펴보고, TLS 1.3에서 제안된 SNI 암호화인 ESNI에 대해 알아본다[2][3].

II. HTTP

HTTP 통신은 평문 통신하기 때문에 IP를 차단하는 방식으로 웹 서버 전체가 차단된다.

2.1 HTTPS

TLS 프로토콜로 HTTP 통신을 암호화한 HTTPS 통신에서 클라이언트와 웹 서버 간 통신은 암호화되기 때문에 중간에서 확인 할 수 없다[4]. 이로써 HTTP 통신으로 인한 IP 차단을 우회할 수 있다.

III. DNS

3.1 DNSSEC

DNSSEC(DNS Security Extension)은 DNS의 보안 확장이며, DNS 서버의 각 수준에서 요

청에 디지털 서명을 하도록 하며 신뢰 체인을 형성해 조회의 각 단계에서 요청의 무결성을 검증한다. 하지만 전송되는 패킷 자체는 암호화 되더라도 패킷의 목적지 정보는 암호화 되지 않은 평문으로 노출되어 사생활 보호를 보장하지 못하는 문제점이 있다.

3.2 DNS-over-TLS

DNS-over-TLS(DoT)는 클라이언트와 DNS 서버간의 TLS 프로토콜 기반 암호화된 통신을 통해 DNS 요청을 근본적으로 감청 할 수 없게 만들뿐만 아니라 중간자 공격을 차단함으로써 DNS 스푸핑 공격의 가능성을 줄인다[6].

3.3 DNS-over-HTTPS

DNS-over-HTTPS(DoH)는 DNS 요청을 평문이 아닌 HTTPS를 통해 DNS 정보에 접근한다[6]. 이를 통하여 DoH는 DNS 요청을 HTTP 요청인 것처럼 위장하기 때문에 높은 보안성 효과가 있으며 높은 확장성을 제공한다.

3.3 DoT와 DoH의 비교

DoT는 TCP를 기본 연결 프로토콜로 사용하고 TLS 암호화 및 인증을 통해 계층화 하는 반면 DoH는 HTTPS 및 HTTP/2를 사용하여 연결한다[6].

DoT는 자체 전용 포트인 853을 사용하며 DNS 요청 자체는 암호화되기 때문에 요청한 내용을 알 수는 없지만 사용하는 전용 포트 번호 때문에 DoT를 사용하고 있다는 것을 알 수 있다. 반면, DoH는 기존 HTTPS 트래픽의 표준 포트인 443을 사용하므로 HTTPS 통신과 DoH 통신을 구분할 수 없다. 즉, DoT와는 다르게 사용하고 있다는 것을 숨길 수 있다.

IV. SNI

SNI는 TLS 프로토콜의 확장이며 이를 이용하면 동일한 IP 주소 여러 개의 인증서를 사용할 수 있게 된다. 따라서 동일 IP의 여러 호스트 인증이 가능하게 된다.

4.1 ESNI

ESNI는 2018년 TLS 1.3에서 제안된 SNI 암호화이며[3]. DNS 통신을 이용해서 공개키를 배포하고 이 공개키를 이용하여 SNI를 암호화한다. 그리고 공개키 방식인 DH(Diffie-Hellman) 이용하여 공개키로부터 공유키를 유도한다. 서버는 자신의 개인키와 클라이언트의 공개키를 사용하여 공유키를 유도하여 복호화한다.

문제점은 HTTPS 기반의 웹 서버와 DNS 서버 상호간에 동기화가 잘 이루어져야 한다는 것이다. SNI 암호화에 사용되는 키의 만료기간으로 인한 갱신이 요구되는데 이러한 갱신이 이 두 서버에 동시에 반영되어야 한다. 일반적으로 웹 서버의 경우 ISP가 직접 관리하지만, DNS 서버는 ISP 제공 서버 혹은 외부의 네임 서버를 사용하는 경우가 많기 때문에 어려움이 예상된다.

V. 결론

각각의 기술이 아닌 ESNI와 TLS 1.3, DNSSEC, DoT/DoH와 같이 사용되면 인터넷상의 감시와 검열로 부터 자유로워 질 것으로 예상된다. 하지만 사생활과 인권을 중요시하는 '보안(Security)' 측면과 네트워크상의 트래픽의 '가시성(Visibility)' 측면의 문제에 관해서도 생각해 보아야할 문제다.

[참고문헌]

[1] 임철민, "정부 HTTPS 불법사이트 차단 논란 4대 쟁점 분석", ZDNet Korea, 2019

[2] A. Ghedini, You get TLS 1.3! You get TLS 1.3! Everyone gets TLS 1.3!, May 2018

[3] A. Ghedini, Encrypt it or lose it: how encrypted SNI works, Cloudflare, September 2018

[4] M. Martin, Everyday Cryptography: Fundamental principles and applications, second edition, Oxford University Press, 2017

[5] Keith Shaw, What is DNS and how does it work?, Network World, April 2018

[6] P. Nohe, What is the difference between DNS over TLS & DNS over HTTPS?, The TLS Store, December 2018