**DNS 차단과 HTTPS 프로토콜**

2018년 5월 2일 - 문화체육관광부에서 방송통신위원회, 경찰청과 협동해 불법 웹툰 사이트 등 저작권 침해 방지 대책 발표

1. 저작권 침해사이트를 심의

2. DNS 스푸핑 기법을 이용해 차단 -> 최종적으로 SNI필드 감청 기법을 도입

부적절한 사이트 접속을 차단!

**알아둘 용어**

Internet Services Provider(ISP) : 인터넷 서비스 공급자. KT, SKT와 같은 통신사

Internet Protocol Address(IP Address) : 인터넷 통신에서 사용하는 주소값

Domain Name System(DNS) : 도메인네임 ex) naver.com, daum.net 을 해당 서버의 IP로 바꿔주는 시스템. 이 시스템을 운영하는 서버를 DNS 서버라고 한다.

Transport Layer Security(TLS) : Secure Socket Layer에 기반한 기술로 인터넷 통신의 신뢰성을 다루는 규약을 묶어 정리한 것

HyperText Transfer Protocol(HTTP) : 클라이언트와 서버 사이 요청/응답 프로토콜

**DNS 스푸핑**

물리적으로 DNS서버보다 가까운 곳에 위치해 대기하다가 통신에 끼어드는 방법이다. 원래 보내지는 패킷이 자신을 향한 것이 아니면 열어보면 안되지만 설정을 바꿔 들어오는 모든 패킷을 읽고, 특정한 DNS로 향하는 패킷이 확인될 경우 자신이 만든 가짜 패킷으로 이를 대체, 송신하여 상대방이 자신의 패킷을 진짜처럼 취급하게 하여 상대방과 통신하는 방법이다.

정부에서는 국내 ISP와 협력하여 패킷을 확인하고 불법 사이트의 도메인으로 향하는 패킷을 막는 방법을 사용하겠다는 뜻이다. 하지만 이는 DNS 서버를 국외로 설정하는 방법으로 쉽게 뚫리게 된다.

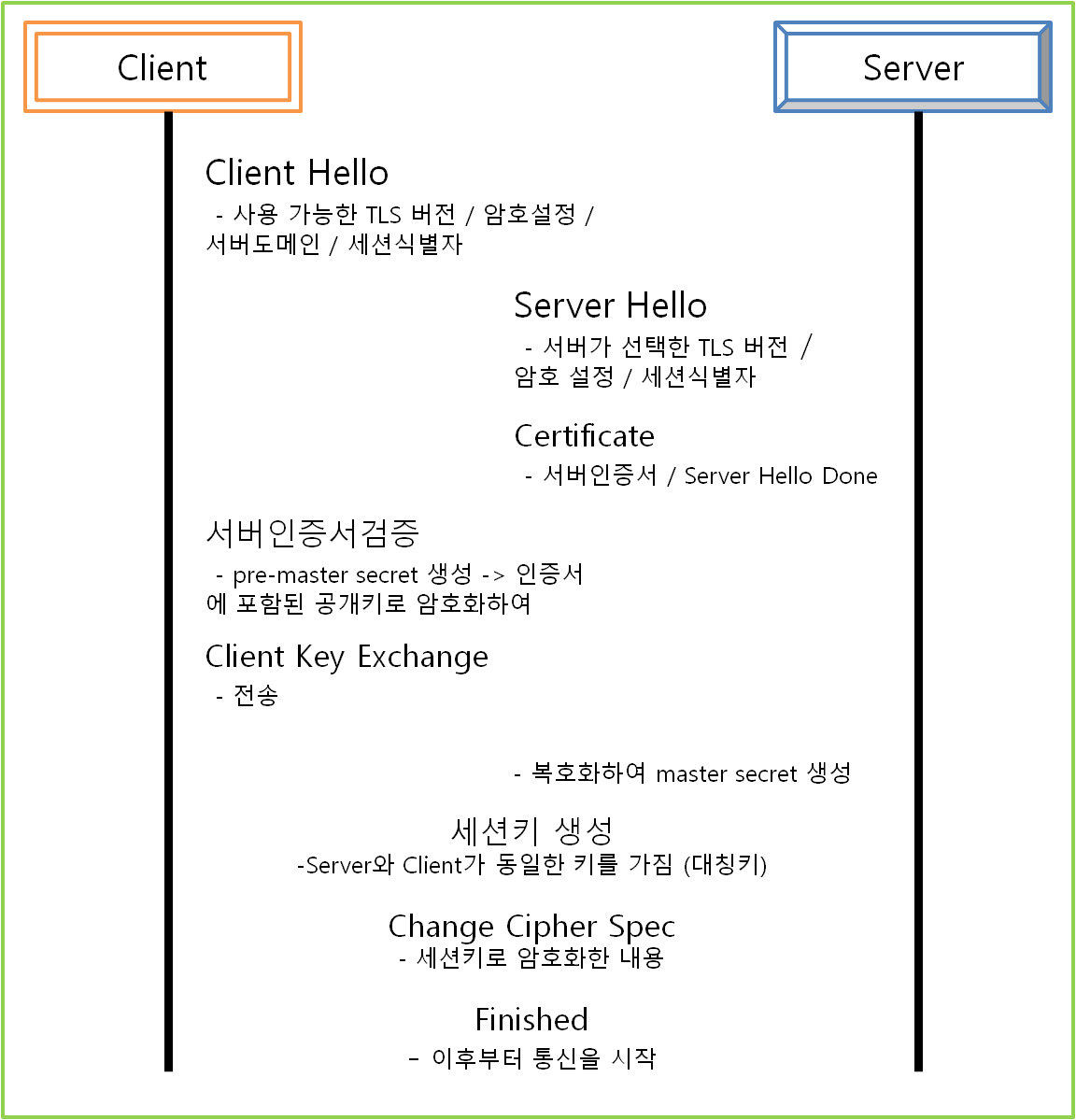
**SNI필드? 그 전에 TLS**

TLS는 인터넷 통신에서

1. 사용자가 신뢰할만한지

2. 통신 내용이 암호화되었는지

이런 통신 보안 규약을 묶어 정리한 것이다. TLS 통신에서는 신원확인과정(Handshake)을 거치는데 다음과 같이 이뤄진다



<TLS의 Handshake 과정, Server에서 Client의 인증서를 요구하기도 한다>

통신을 위해 미리 전송해야 할 내용이 많다 -> 속도가 느림 / 부하가 커서 DDoS 공격에 취약함

HTTPS는 HTTP에서 TLS를 사용하는 방식으로 보안이 강화된 HTTP 버전이다.

특히 인증서가 중요하게 기능하는데 인증기관이 인증서를 손쉽게 발급하는 바람에 Extended Validation SSL이 등장했는데 인증서를 허위로 발급하지 못하도록 강력한 규제를 거쳤을 때 인증받을 수 있는 제도이다. 크롬에서 연결했을 때 주소창에 초록색으로 보안 연결됐다고 알려주면 EVSSL 연결이다.

**SNI?**

HTTPS 통신상 같은 IP주소와 TCP포트를 사용하는 서버에서 여러 인증서를 쓸 수 있게 해주는 기능이다. IPv4 체계는 2^32개의 주소 발급이 가능한데 현대에 필요로 하는 주소 개수에 못 미치기 때문에 DHCP처럼 하나의 주소를 공유해 사용하는 방법 등 대책이 요구되고 있는데 서버도 마찬가지이다. TLS통신을 위해 특정 IP 주소에 접근했을 때 어느 도메인에 접근하려는지 알 수 없어 어느 도메인의 인증서를 건네주어야 할지 알 수 없는 상황을 피하기 위해 도입된 대책이다. 통신할 때 SNI필드라는 곳에 접근하려는 도메인의 주소를 담아서 전송하는 방식을 사용하며, TLS 규약에 포함되어있지 않다가 2018년 초안이 TLS 1.3에 포함되었다. TLS에 포함되어있지 않을 때는 암호화규정이 없어 평문으로 전송되었지만 1.3버전에 포함되면서 Encrypted SNI가 개발되고 있다고 한다. ESNI는 SNI필드도 암호화하도록 규정한다. ESNI는 서버 공개키가 전달되는 순간을 DNS통신 단계로 앞당겨 SNI필드도 암호화하는 방식이다.

정부에서는 현재의 평문으로 전송되는 SNI필드를 확인해 불법 사이트로 연결되는 도메인을 차단하고자 한다.

**DNS에 대해**

Forward Zone( : 도메인주소 -> IP주소)과 Reverse Zone(: IP주소 -> 도메인주소)이 있다.

네트워크 연결은 DNS서버에 질의하고 질의한 내용을 응답 받는 방식으로 이뤄지는데 이 과정에서 응답 방식이 두 시나리오로 나뉘게 된다.

daum.net에 연결하는 시나리오로 예를 들자

**Authoritative Answer**

DNS서버가 질의 받은 IP - 도메인의 레코드(정보)를 Forward와 Reverse 모두 가지고 있을 때이다.



**Non-Authoritative Answer**

DNS서버가 질의 받은 IP - 도메인에 대해 Forward 혹은 Reverse에 대한 정보가 없을 때로 일반적인 가정에서 연결했을 때의 과정이다.

