SSL/TLS 보안 및 취약점 동향

한성대학교 컴퓨터공학부
윤재웅

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

개요

- SSL(Secure Sokets Layer) / TLS(Transport Layer Security) 란?

- 클라이언트와 서버 사이에 교환되는 데이터를 안전하게 보호하기 위하여 공개키 인증서를 통한 사용자 인증, 비밀키 암호 시스템을 통한 데이터의 기밀성을 제공한다.

버전

- SSL v2.0

1994년 Netscape사에 의해서 Netscape 웹브라우저를 통한 안전한 통신을 위하여 최초로 제안

- SSL v3.0

IETF(Internet Engineering Task Force)에서 제안

이후로도 지속적인 수정 및 보안

당시 사실상의 웹 보안의 표준

버전

- TLS v1.1

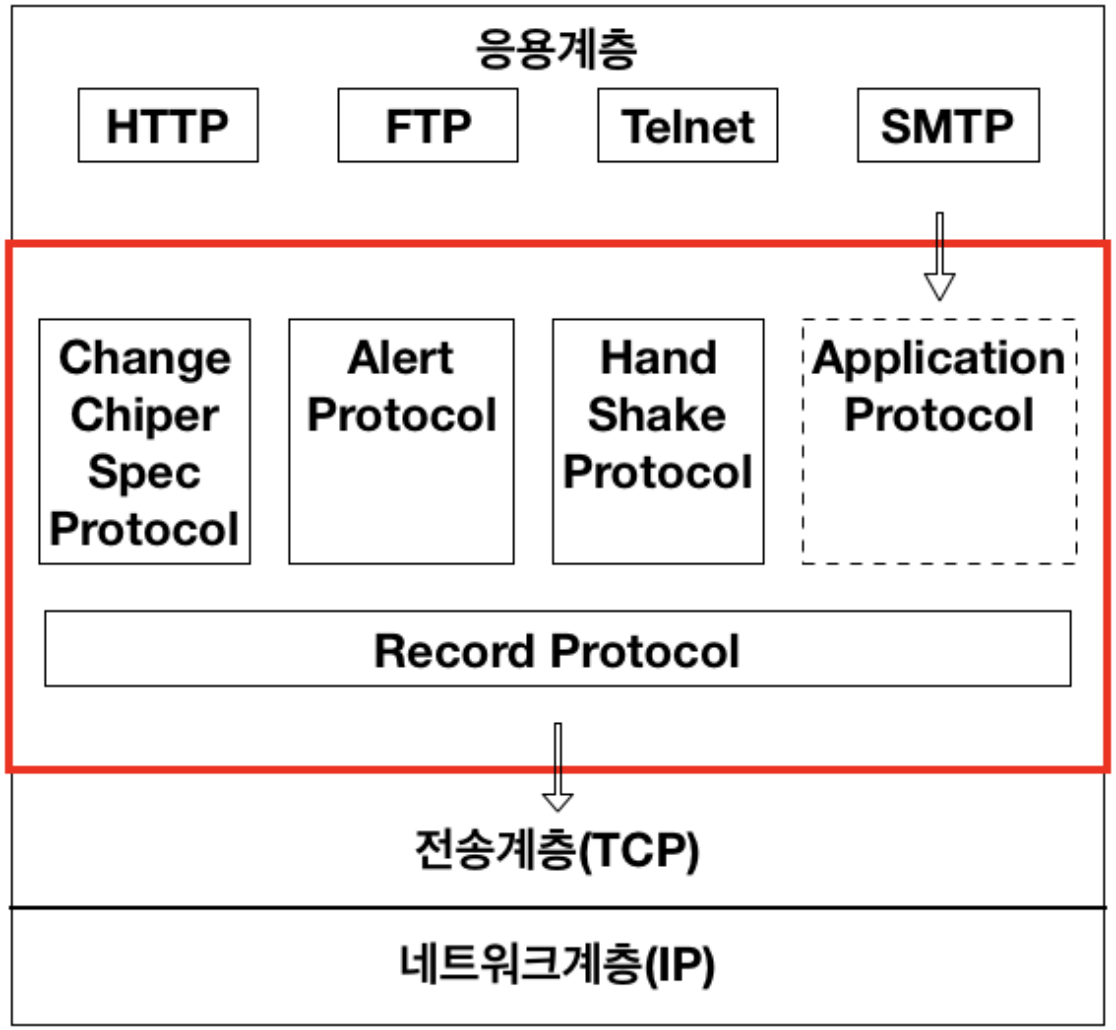
 1999년 SSL v3.0을 참고로 RFC 2246으로 표준화 됨(SSL v3.1에 해당)

- TLS v1.2

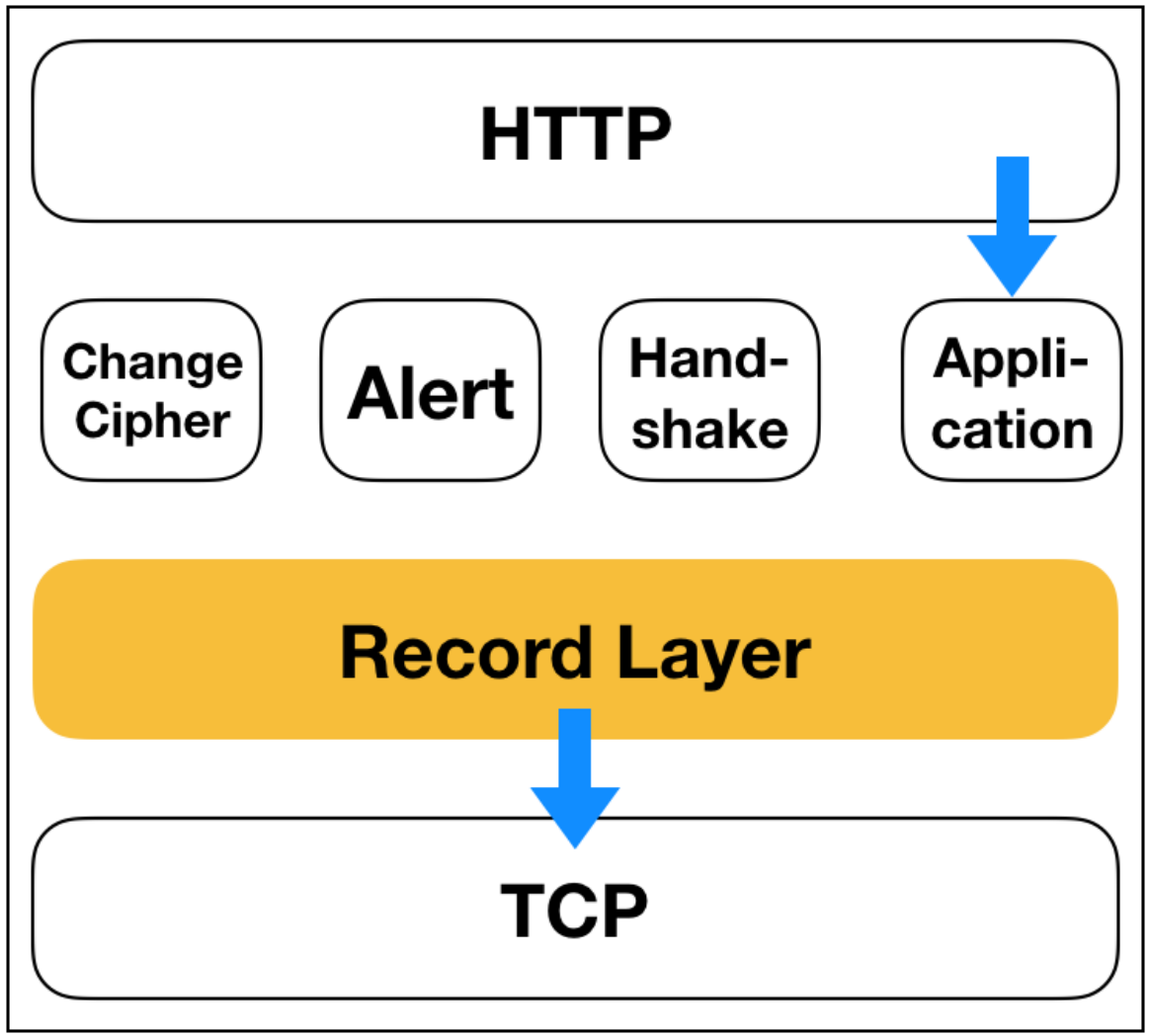
 RFC 5246, 2008

- TLS v1.3

구조 및 동작


응용계층
HTTP
FTP
Telnet
SMTP
Change Chiper Spec Protocol
Alert Protocol
Hand Shake Protocol
Application Protocol
Record Protocol
전송계층(TCP)
네트워크계층(IP)

Record Layer Protocol

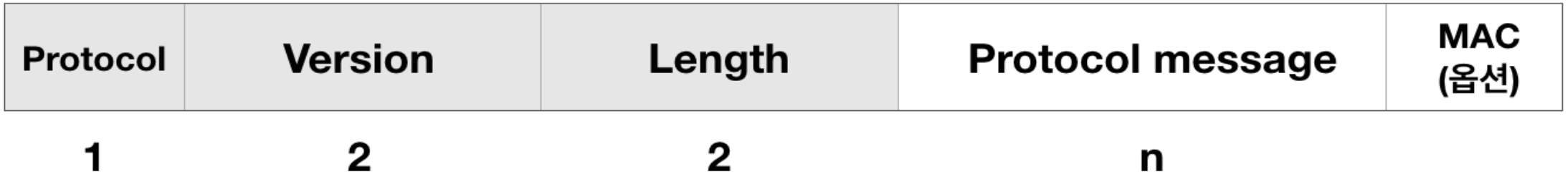


Record Layer 프로토콜은

- ChangeCipherSpec Protocol
- Alert Protocol
- Handshake Protocol
- Application Protocol

네 개의 프로토콜 바로 밑에 위치하고 있습니다.

Record Layer Protocol



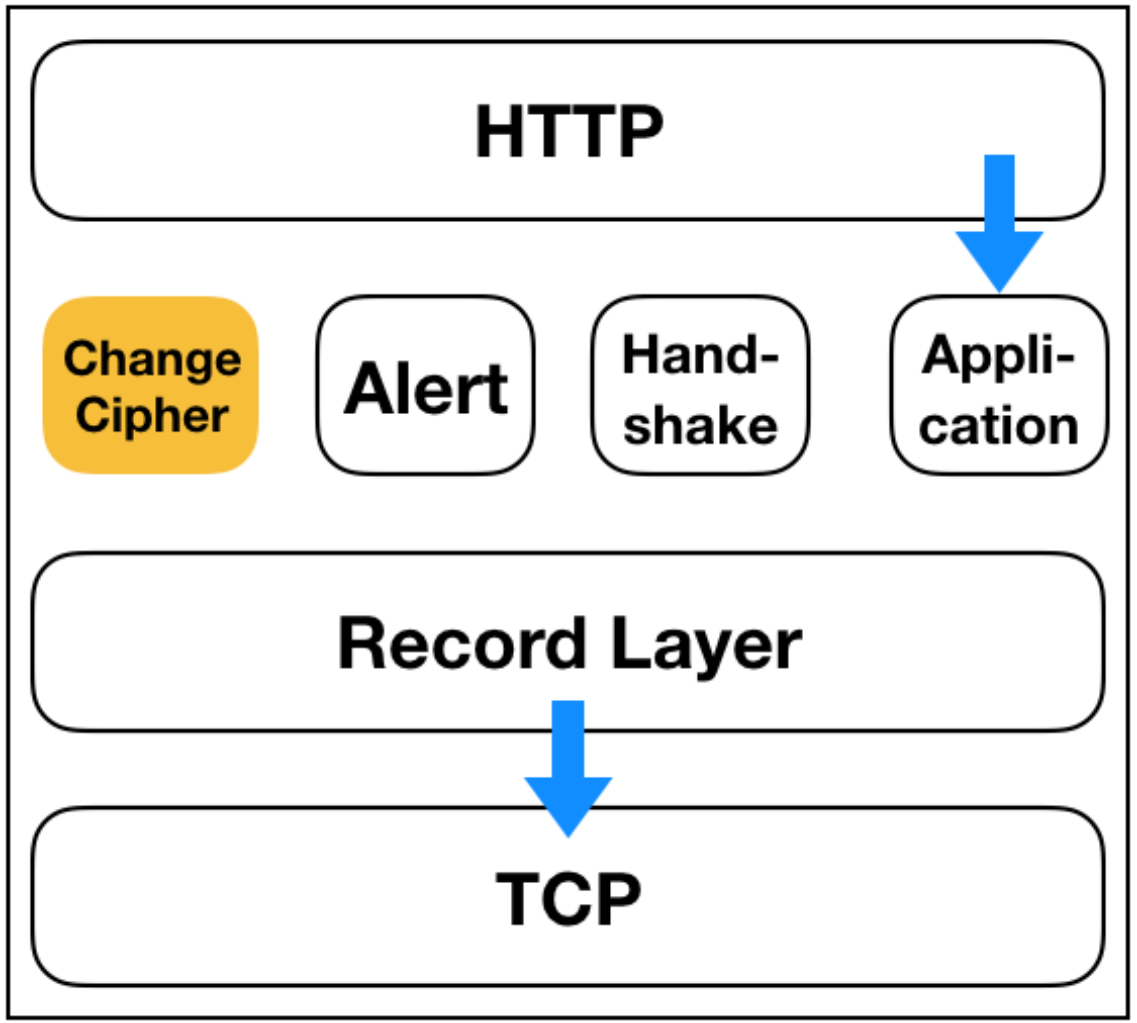
- **Protocol**
  Record Layer 프로토콜이 감싸고 있는 프로토콜이 무엇인지 표시

- **Version**
  SSL/TLS의 버전을 표시

- **Protocol Message**
  Record Layer 프로토콜이 감싸고 있는 프로토콜의 내용

- **MAC**
  Protocol Message 내용의 MAC 값
  메시지 인증 기능을 사용할 경우 사용되므로 이 필드의 사용은 옵션

ChangeCipherSpec Protocol



ChangeCipherSpec 신호

- SSL/TLS 통신을 하려면 양 편이 암호화 통신을 할 때 사용할 암호화 알고리즘들, 즉 비밀키 알고리즘과 메시지 다이제스트 알고리즘을 정하는 신호

통신을 하는 양 편에 ChangeCipherSpec 신호를 알리기 위해 사용됩니다.

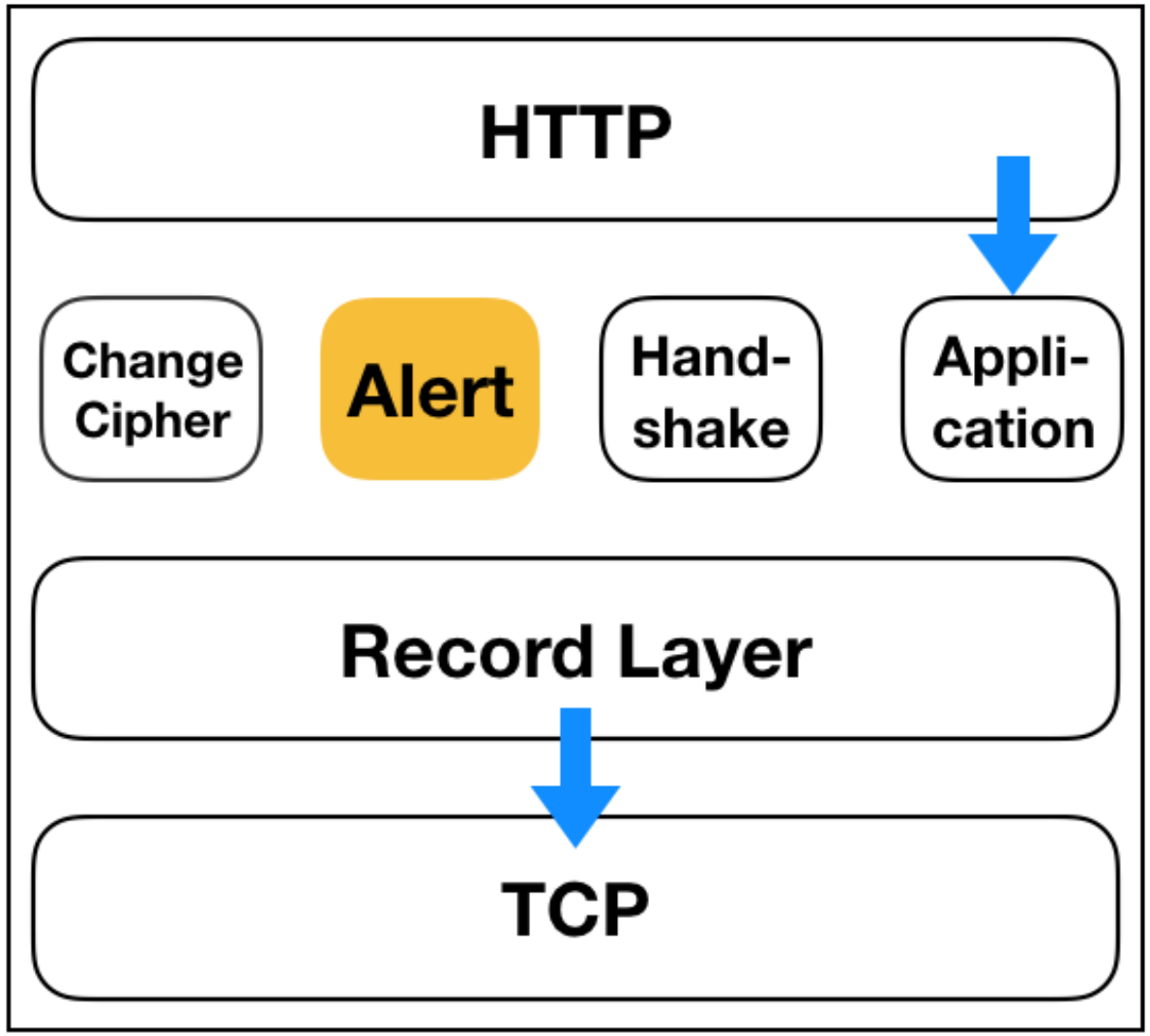
ChangeCipherSpec Protocol

- **Protocol**
ChangeCipherSpec임을 나타내는 20

- **Version**
SSL 3.0

- **Protocol Message**
ChangeCipherSpec Protocol 내용의 바이트의 값은 언제나 1

Alert Protocol



Alert 신호

- SSL/TLS 통신을 하는 양 쪽 누군가 한태 에러나, 주의 같은 정상적이지 않은 상황이 발생했을 때 이를 상대방에게 알리기 위해서 사용

통신을 하는 양 편에 Alert 신호를 알리기 위해 사용

Alert Protocol

21	3	0	0	2	Level	Description

Protocol **Version** **Length** **Message (1 Byte 씩 2 Field)**

- **Protocol**

Alert 임을 나타내는 21

- **Version**

SSL 3.0

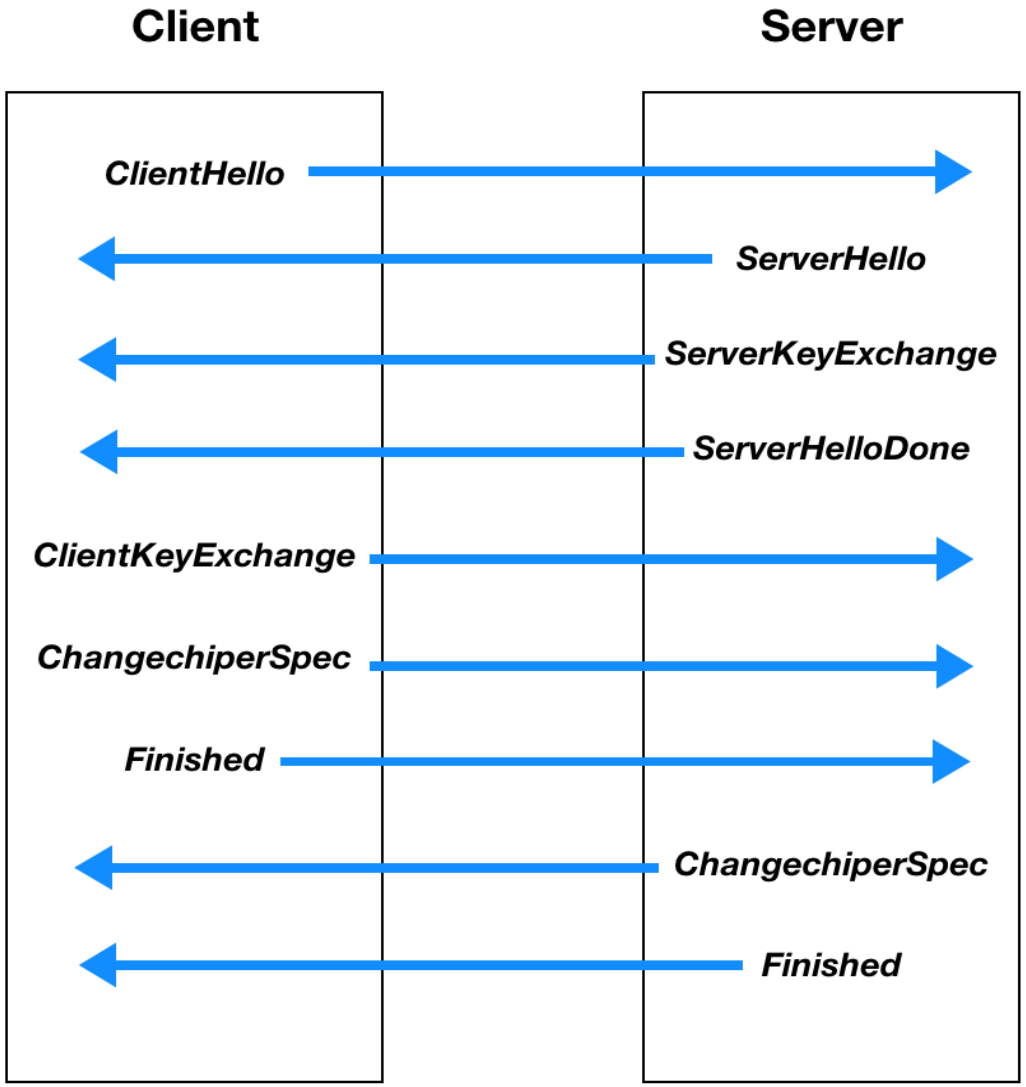
- **Protocol Message (Level, Description)**

Warning(1) – 주의를 해야 하는 문제가 발생 -> 연결 종료하지 않음
Fatal(2) – 매우 중대한 문제가 발생 -> 연결 종료

Alert Protocol

값	의미	설명
0	CloseNotify	상대방에게 연결을 종료 하겠다고 알립니다.
10	UnexpectedMessage	상대방에게 지금 받은 메시지는 적당하지 않은 메시지라는 것을 알립니다.
20	BadRecordMAC	상대방에게 지금 받은 메시지의 내용과 MAC이 일치하지 않는다고 알립니다.
30	DecompressionFailure	상대방에게 지금 받은 메시지의 데이터의 압축을 풀지 못한다는 것을 알립니다.
40	HandShakeFailure	HandShake 협상을 할 수 없다고 상대방에게 알립니다.
41	NoCertificate	자신에게는 인증서가 없다는 것을 상대방에게 알립니다.
42	BadCertificate	상대방에게 받은 인증서의 형식이 맞지 않거나, 인증 할 수 없는 인증서일때 이를 상대방에게 알립니다.
43	UnSupportedCertificate	상대방에게 지금 받은 인증서는 지원 할 수 없는 인증서 형식임을 알립니다.
44	CertificateRevoked	상대방에게 지금 받은 인증서는 발급자로부터 철회되었다는 것을 알립니다.
45	CertificateExpired	상대방에게 지금 받은 인증서는 사용 기간이 지났음을 알립니다.
46	CertificateUnkown	상대방에게 지금 받은 인증서에 알 수 없는 문제가 있다는 것을 알립니다.
47	IllegalParamerter	상대방에게 지금 받은 메시지는 형식에 맞지 않다는 것을 알립니다.

Handshake Protocol



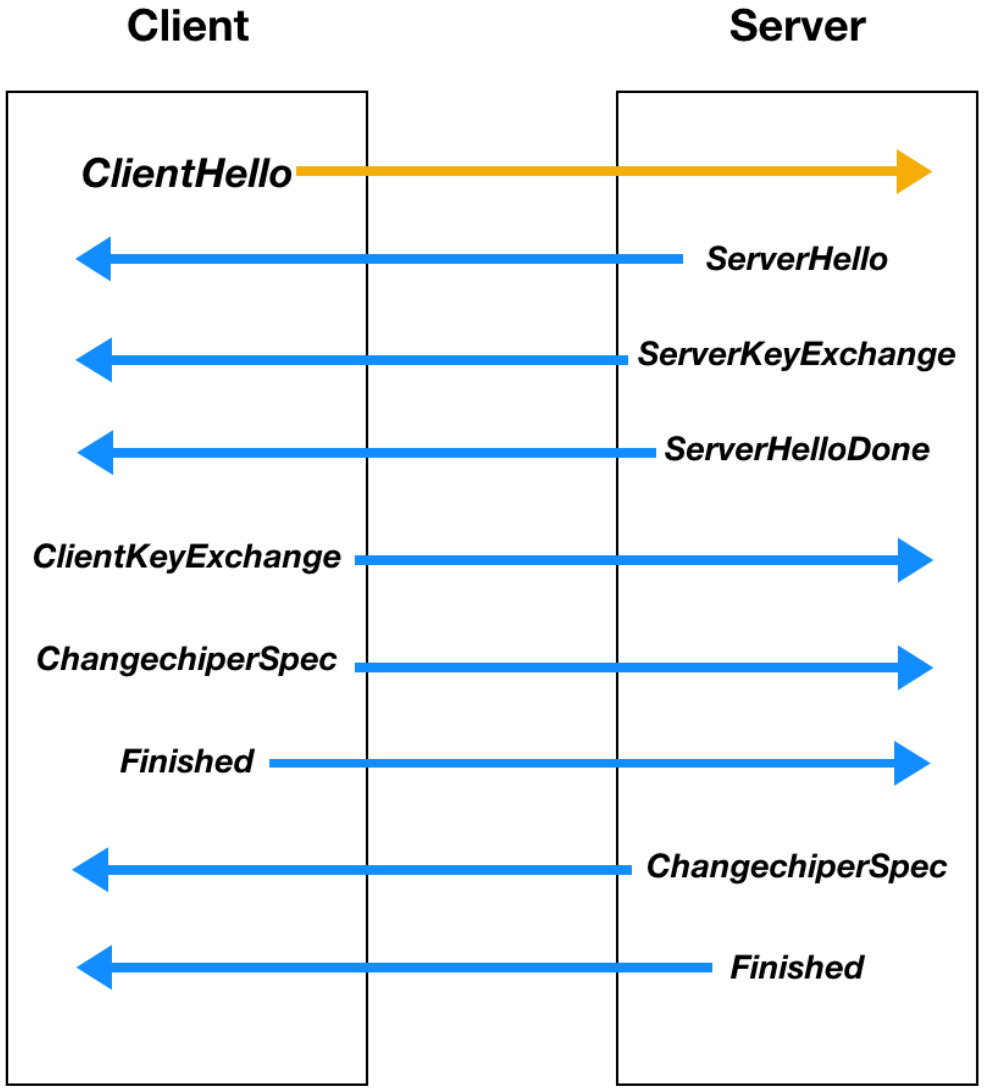
SSL/TLS 통신의 대부분의 메시지가 여기에 해당

- 개략적 통신 순서

1. 클라이언트와 서버의 암호화 통신을 위한 준비 작업을 위한 단계

2. 실제의 암호화 통신

Handshake Protocol



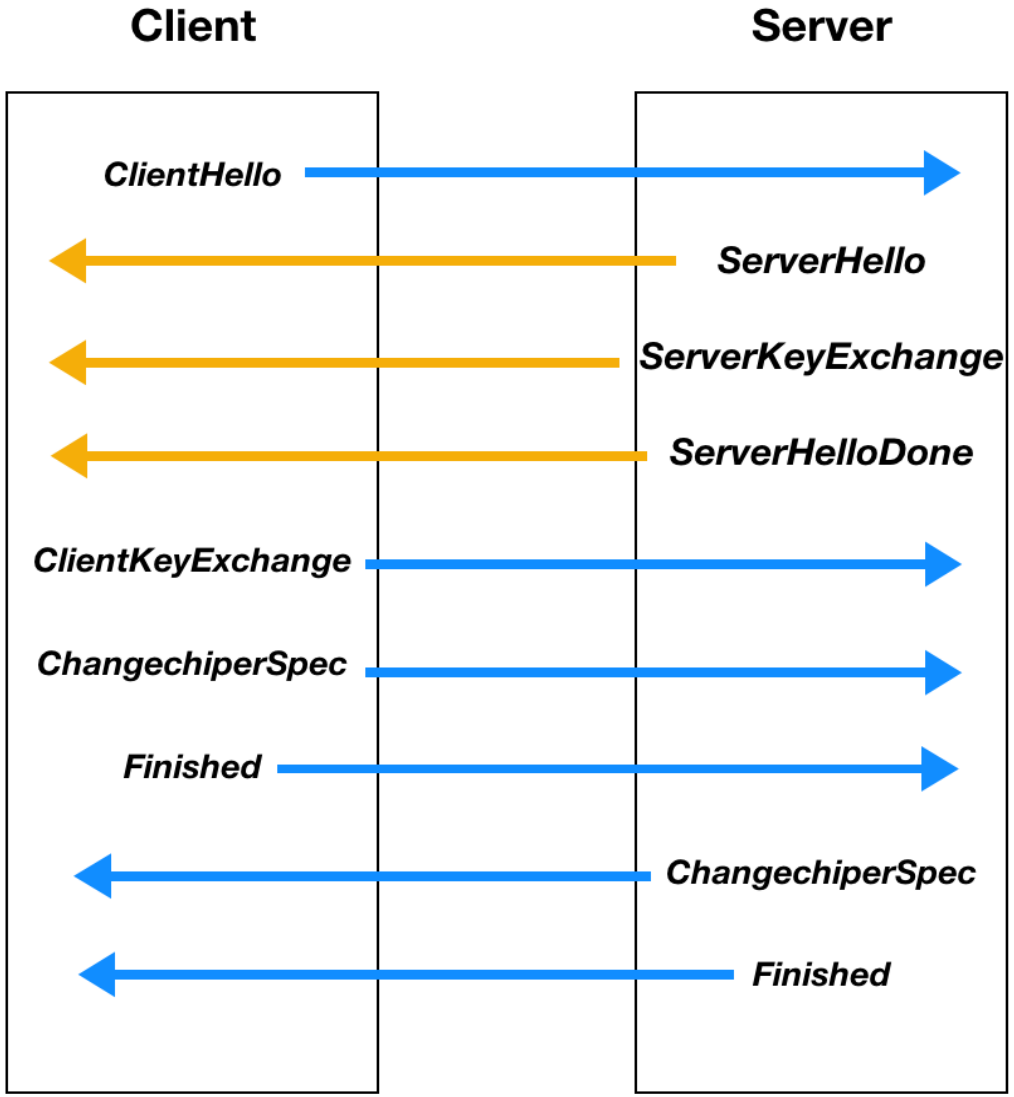
- ClientHello
클라이언트가 메시지를 보냄으로 통신 시작한다.

- 자신이 지원 할 수 있는 암호화 알고리즘의 리스트를 이 메시지를 통해 서버에게 알립니다.

Handshake Protocol

필드	설명
Version	지원 할 수 있는 SSL버전을 표시
RandomNumber	Seed로 사용될 32바이트의 랜덤 수 입니다. 클라이언트가 제공하는 이 랜덤 수와 서버가 자체적으로 만드는 랜덤 수를 Seed로 사용 합니다. 하지만 이 랜덤 수는 그리 중요하지는 않습니다.
SessionID	SSL 세션을 나타내는 세션 ID입니다. 지금은 새로운 세션을 시작하는 것 이으로 의미가 없으며, 빈 공간으로 놔둡니다.
CipherSuites	클라이언트가 지원할 수 있는 암호화 알고리즘의 리스트입니다.
CompressionMethod	클라이언트가 지원할 수 있는 압축 알고리즘의 리스트입니다.

Handshake Protocol



- **ServerHello**

서버는 클라이언트에게 응답을 보냅니다.
서버는 받은 ClientHello 메시지 안의 암호화 알고리즘 중에서 자신이 지원 가능한 알고리즘을 선정해 ServerHello 메시지에 넣어서 클라이언트에게 보냅니다.

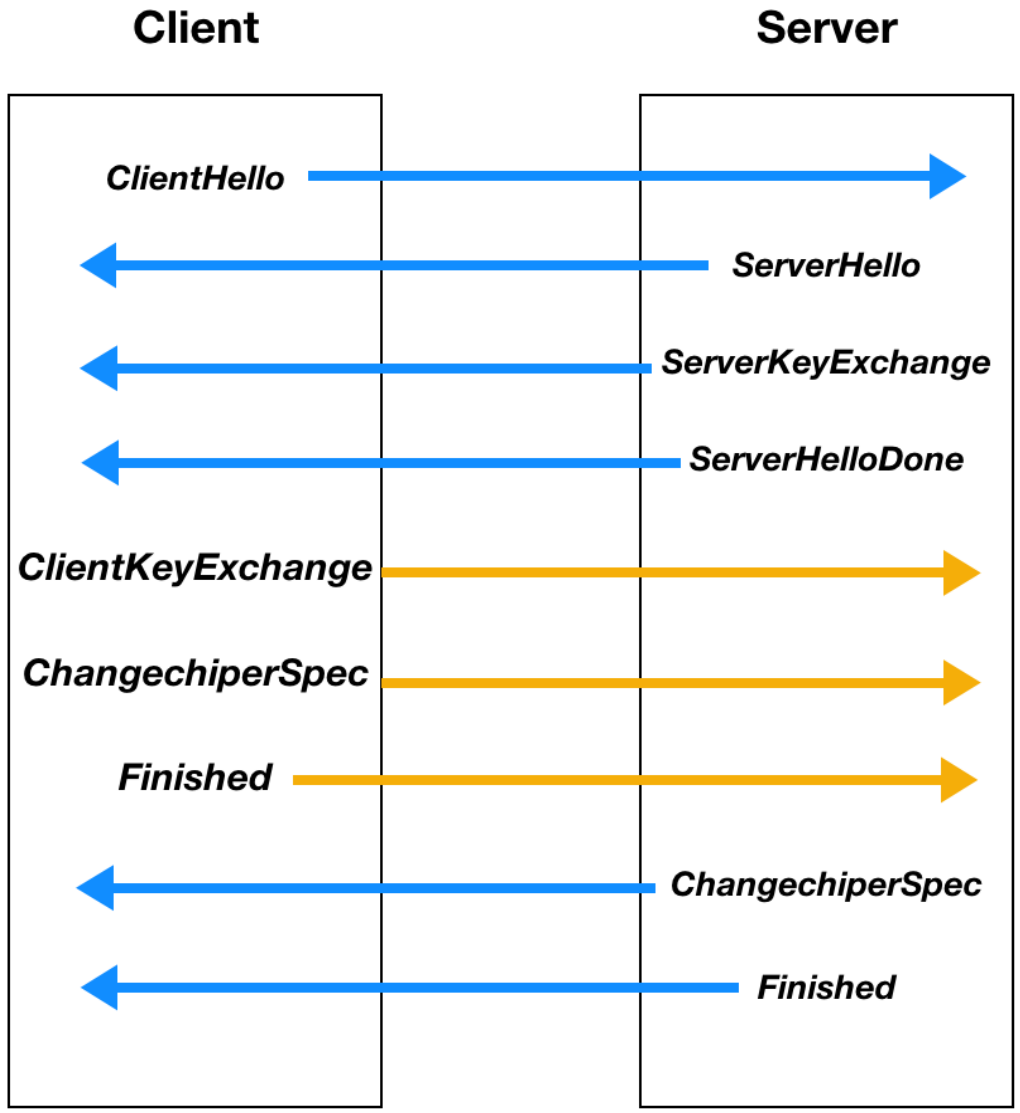
- **ServerKeyExchange**

서버는 메시지 안에 자신의 공개키를 넣어서 클라이언트에게 보냅니다.

- **ServerHelloDone**

서버는 자신의 초기화 협상 단계가 끝났다는 것을 클라이언트에게 메시지를 통해 알립니다.

Handshake Protocol



- **ClientKeyExchange**

암호화 통신 때 클라이언트와 서버 간의 데이터를 암호화/복호화 하는데 사용될 비밀키를 생성합니다.

클라이언트는 ServerKeyExchange 메시지를 통해 얻은 서버의 공개키로 비밀키를 암호화해서 ClientKeyExchange 메시지에 넣어 서버에게 전송합니다.

- **ChangeCipherSpec**

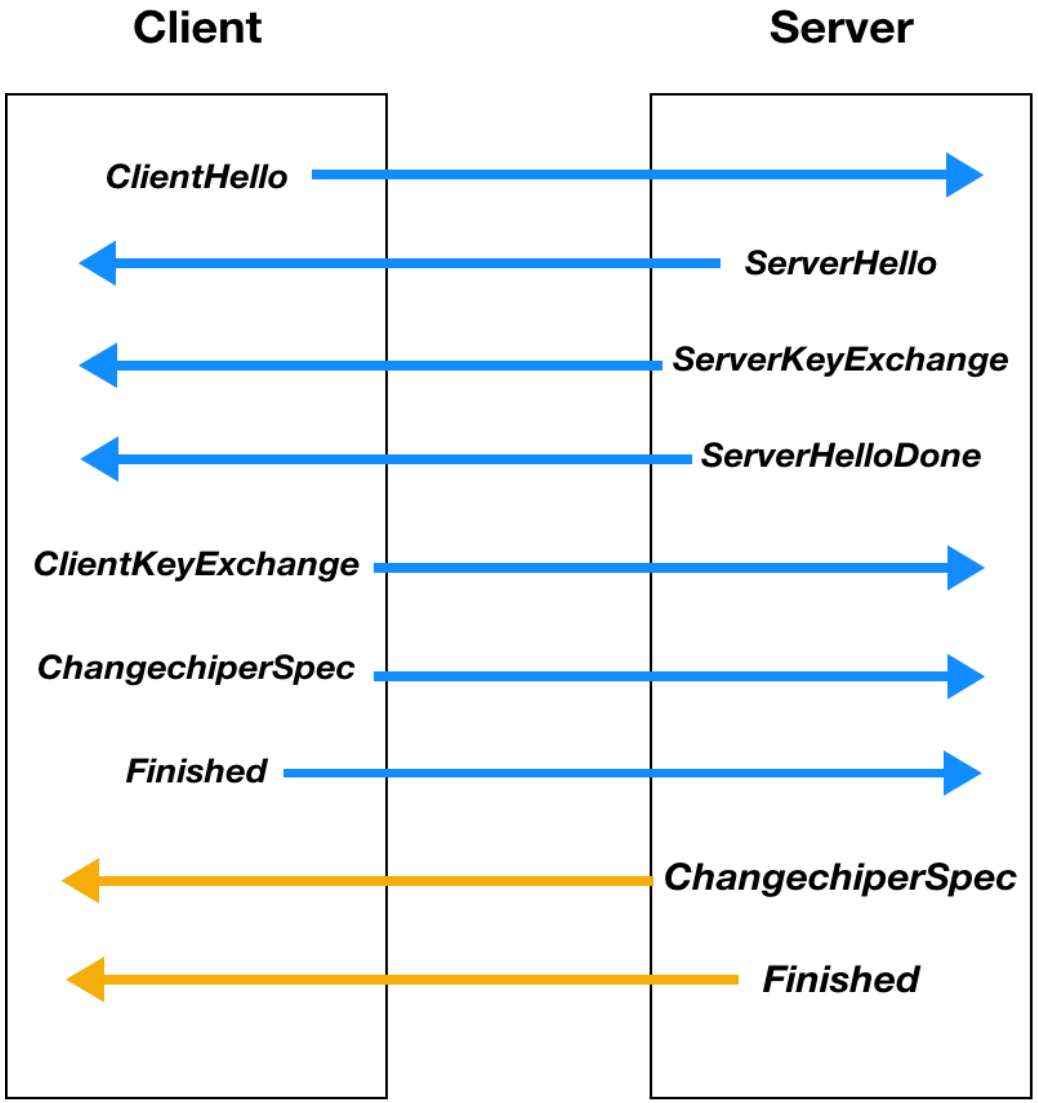
클라이언트는 메시지를 보냄으로 해서 지금까지 정해진 암호화 파라미터(암호화 알고리즘, 비밀키)를 실제로 적용합니다.

- *메시지는 지금까지 정한 암호화 파라미터를 사용하겠다는 확답입니다.*

- **Finished**

암호화 파라미터들의 협상을 종료하겠다는 신호로 서버에게 메시지를 보냅니다.

Handshake Protocol



- **ChangeCipherSpec**

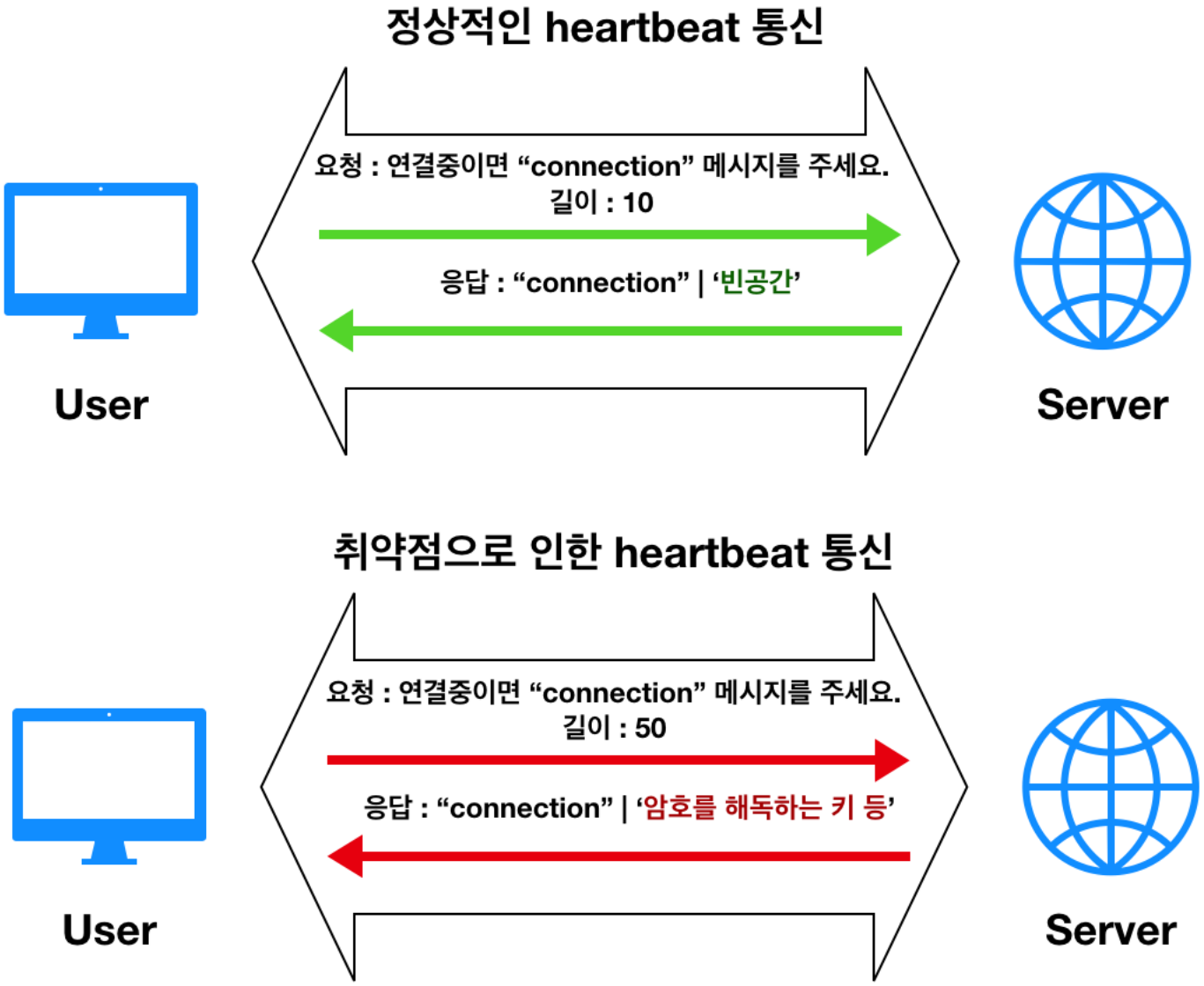
지금까지 정해진 암호화 파라미터들 (암호화 알고리즘, 비밀키)을 실제로 적용합니다.

- 지금까지 정한 암호화 파라미터를 정말로 사용하겠다는 화답 메시지이다.

- **Finished**

암호화 파라미터들의 협상을 종료하겠다는 신호로 클라이언트에게 메시지를 보냅니다.

취약점 동향

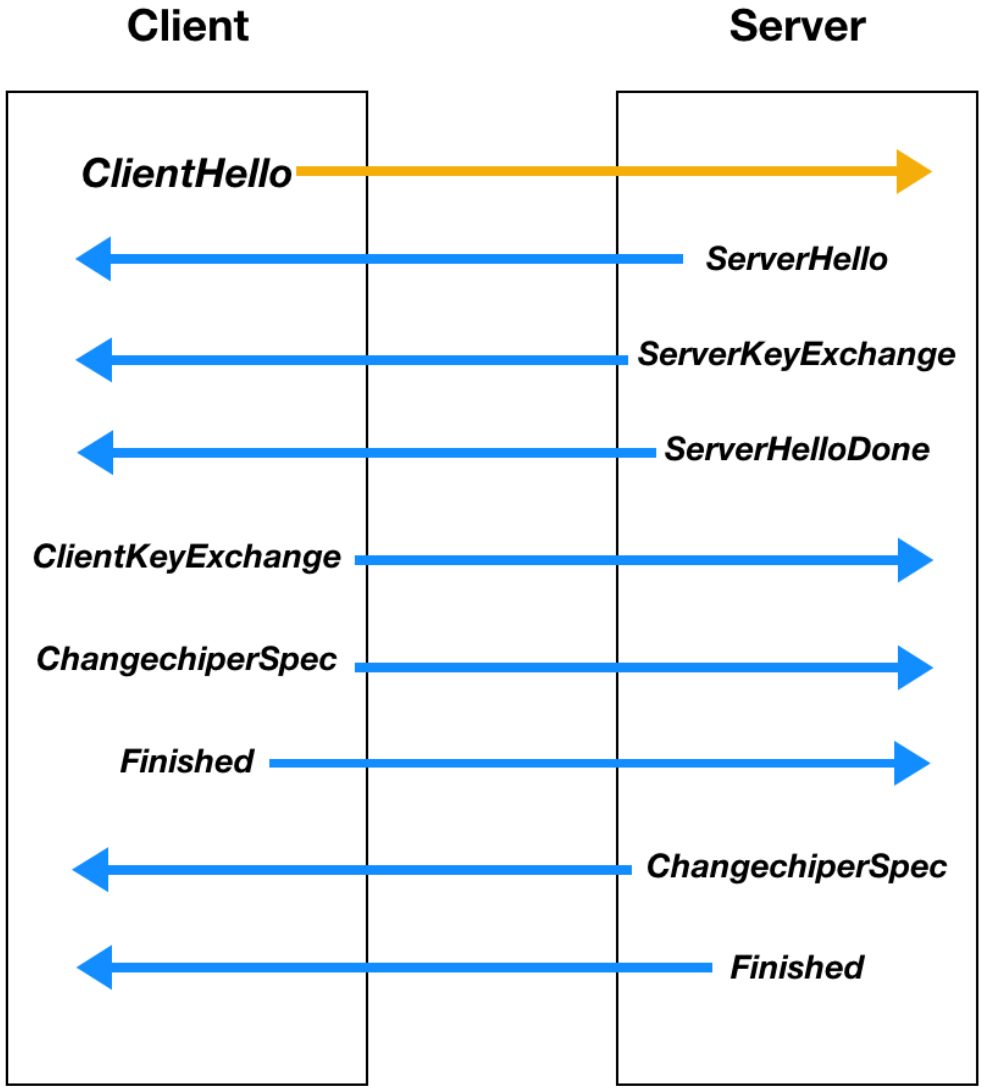


'하트블리드(HeartBleed)' 취약점이란?

HeartBleed란 OpenSSL 1.0.1 버전에서 발견된 매우 위험한 취약점 입니다. OpenSSL을 구성하고 있는 TLS/DTLS의 HeartBeat 확장규격에서 발견된 취약점으로, 해당 취약점을 이용하면 서버와 클라이언트 사이에 주고받는 정보들을 탈취할 수 있습니다.

- OpenSSL은 정해진 규격의 네트워크 보안 프로토콜을 범용 라이브러리로 구현하기 위한 목적으로 만들어졌으며, SSL이나 TLS를 이용한 암호화를 구현할 수 있습니다.
- 강력한 암호화 기능을 제공하기 때문에, 보안이 중요한 대형 포털서비스, 이메일 서비스, 금융권 등에서 데이터 통신 시 OpenSSL을 사용하고 있습니다.

취약점 동향



- **사이퍼 스턴팅 (Cipher Stunting)**

디지털 지문을 조작하는 취약점

최초 Handshake 요청인 클라이언트 헬로(Client Hello) 패킷 (SSL/TLS 버전, 세션 ID, 암호화 관련 옵션, 확장자, 압축 방법과 관련된 정보)의 변종 수가 갑자기 폭팔적으로 늘어나는 현상이 일어납니다.

공격자들은 사이퍼 패킷의 각종 정보들을 무작위로 가져다 쓰면서 디지털 지문의 양을 늘리고 내용을 바꿨습니다. 이로 인해 클라인언트 헬로 패킷의 디지털 지문 수가 기하급수적으로 증가하기 시작 했습니다.

공격자들의 최종 목표는 단일 컴퓨터나 단일 네트워크로부터 발생하는 트래픽을 수만 개 내지는 수천 만 개의 사용자 장비로 보이도록 둔갑시키는 것입니다.

TLS v1.3

1. 보안성 강화

Handshake 단계에서 인증서를 암호화하고, 무결성을 검증함으로써 중간자 공격을 통해 협상 내용을 취약하게 변경하는 다운 그레이드 공격 방어가 가능합니다.

2. 성능 향상

Handshake 과정에서 2-RTT(Round Trip Time)를 거처야 했으나, 이 과정을 단순화 시켜 1-RTT로 감소시켜 성능을 향상시켰다.

3.프라이버시 강화

TLS의 확장인 SNI(Server Name Indication), 정보를 암호화 하는 ESNI(Encrtption SNI) 드래프트 나와있는 상태입니다.

ESNI를 적용하면 접속지 정보가 암호화되므로, 국가 검열 등의 이슈에서 자유로워 질 수 있으며 사용자에게 큰 프라이버시를 제공하게 됩니다.

TLS v1.3

- SSL/TLS의 이전 버전에 결함이 발견되어 새로운 버전이 발표되더라도, 호환성 문제나 관리의 문제 등으로 인해 이전 버전을 허용하는 경우가 많다.

- 실제로 TLS v1.1 이하의 경우 보안성 이슈로 지원을 중지하고 있다. PCI(Payment Card Industry) 협의회에서는 2018년 6월까지 사용을 중지하도록 했고, IETF에서도 TLS v1.0과 v1.1 사용 금지에 대한 드래프트를 내 놓았다.

- Chrome. Firefox, Edge, Safari, Explorer 등 주요 웹브라우저들도 2020년에 TLS v1.0과 v1.1에 대한 지원을 중지한다고 발표했다.

감사합니다.