Web Security

PART II: TLS/SSL

Dr. Bheemarjuna Reddy Tamma

IIT HYDERABAD

Note: This is revised version of slide deck of Prof. Dan Boneh (Stanford) with material from various Internet sources

Outline

- How SSL/TLS protocols work
- Various attacks on SSL/TLS variants
- TLS 1.3

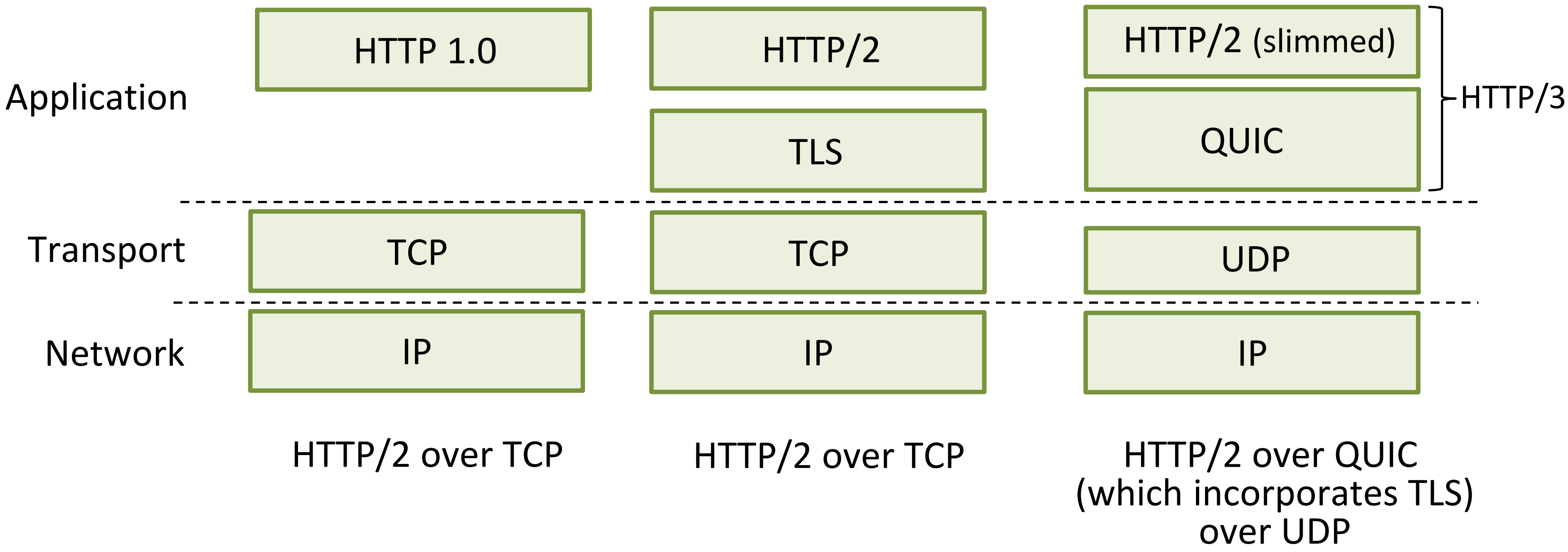
Transport Layer Security (TLS)

- Widely deployed security protocol above the transport layer
  - Supported by almost all browsers, web servers: https (port 443)
  - Primarily used with TCP (reliability and in-sequence delivery)
  - Datagram TLS (DTLS) variant for use with UDP/SCTP/SRTP/CAPWAP
- Provides:
  - confidentiality: via *symmetric encryption*
  - integrity: via *cryptographic hashing*
  - authentication: via *public key cryptography*

all techniques we have studied!

Transport Layer Security (TLS)

- TLS provides an API that *any* application can use
- HTTP view of TLS:

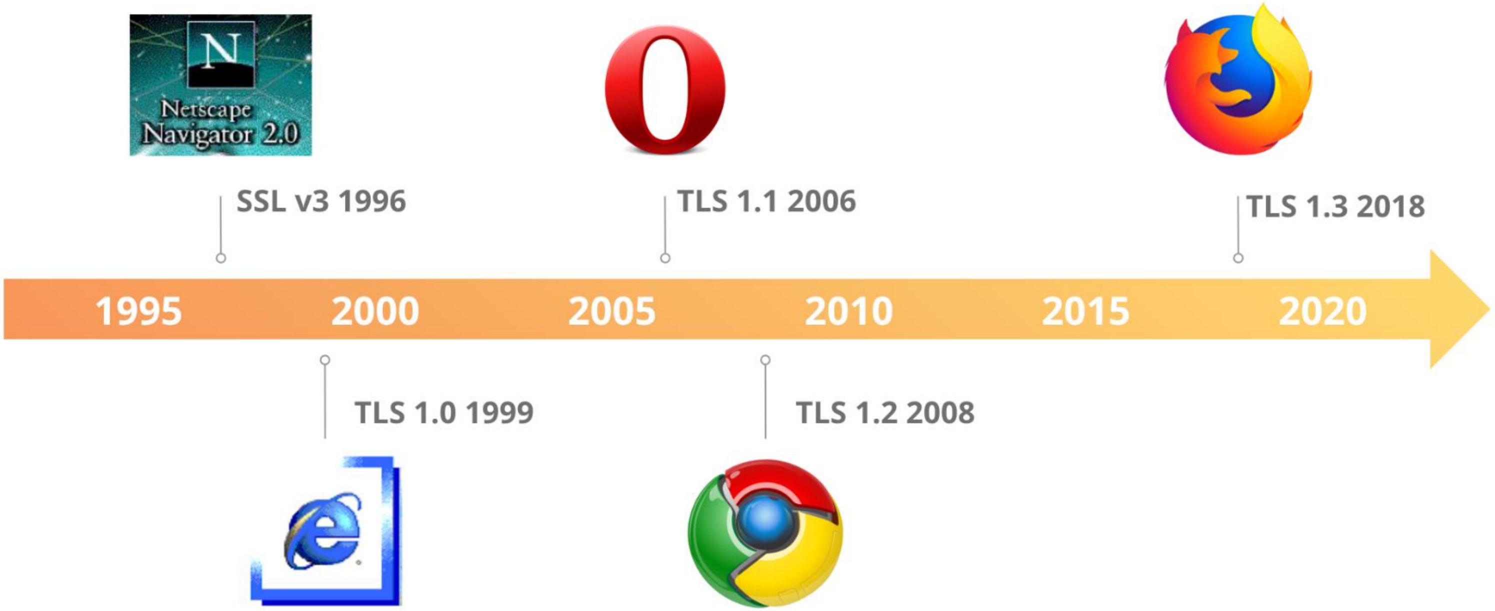


HTTP/2 over TCP

HTTP/2 over TCP

HTTP/2 over QUIC (which incorporates TLS) over UDP

SSL/TLS Variants



1995 2000 2005 2010 2015 2020

SSL v3 1996

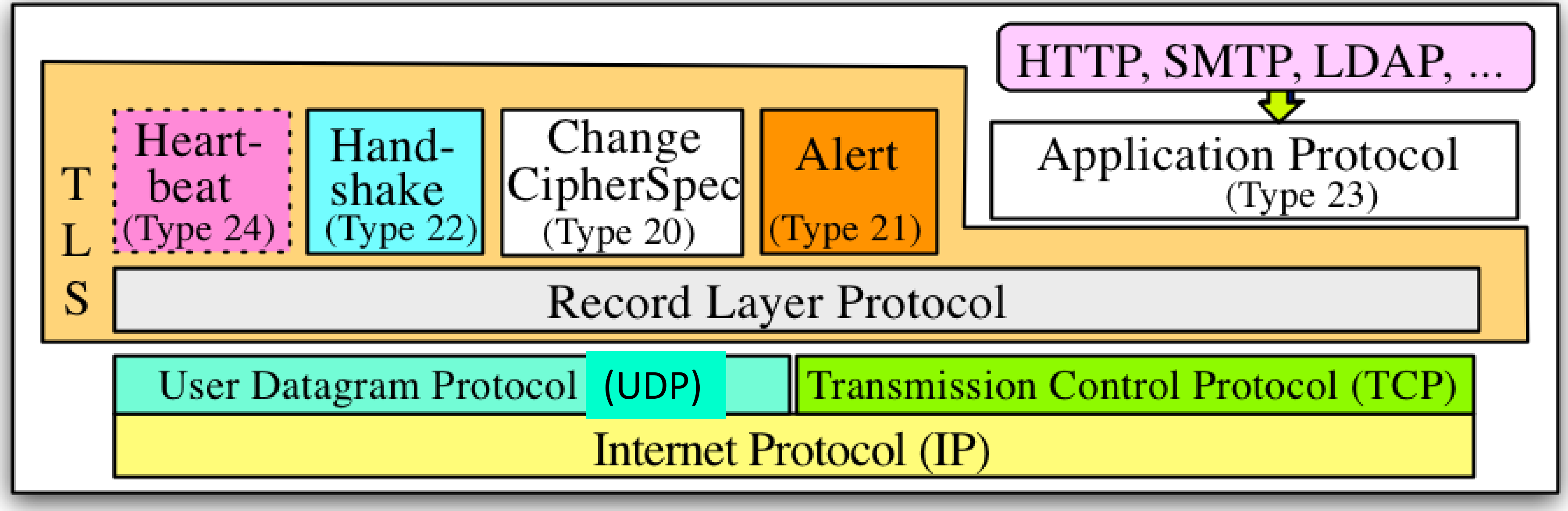
TLS 1.0 1999

TLS 1.1 2006

TLS 1.2 2008

TLS 1.3 2018

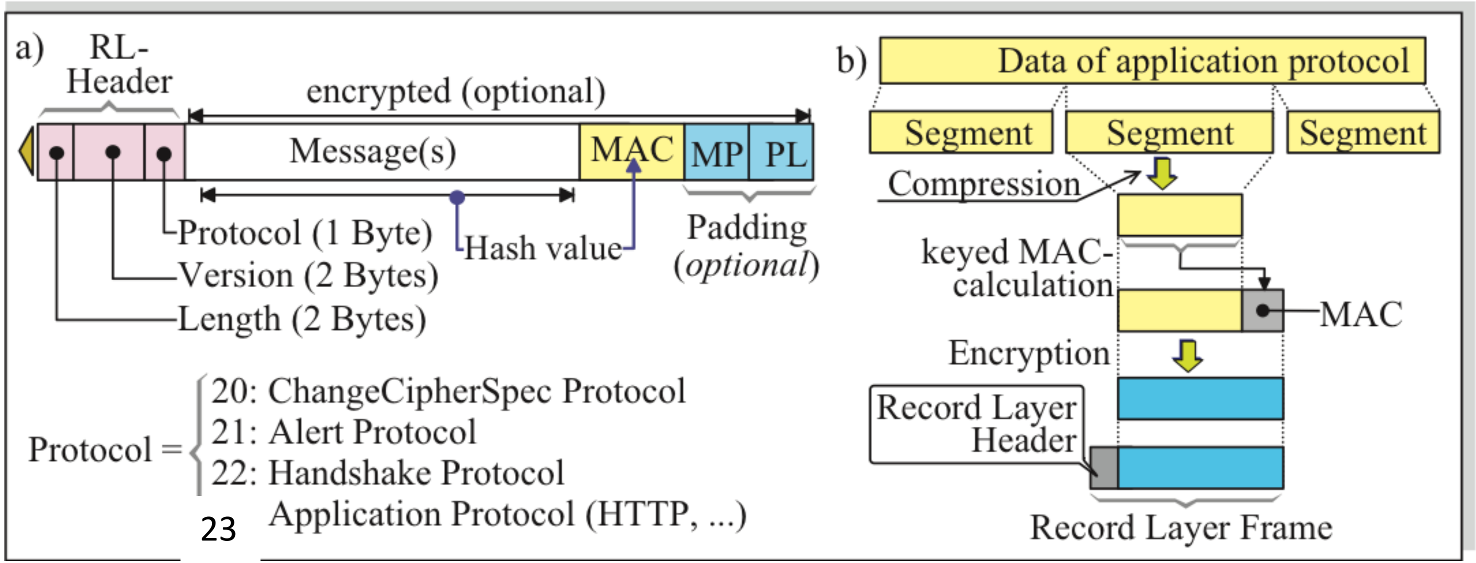
Layered Architecture of TLS



https://www.fehcom.de/qmail/smtptls.html

TLS: Record Layer

- RL is the workhorse of TLS
  - *fragment* the application data into segments
  - Compression of segments
  - Integrity by adding MAC, padding (if needed), Encryption
  - Finally, adding required RL Header



Four Phases of TLS Handshake Protocol

- **Phase-1**

  Both ends agree upon Cipher Suite

  - TLS_**RSA**_WITH_**AES**_256_CBC_**SHA**256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - AEAD_**AES**_256_GCM_**SHA**384 (TLS 1.3)

- **Phase-2**

  Server sends its digital Cert signed by a CA

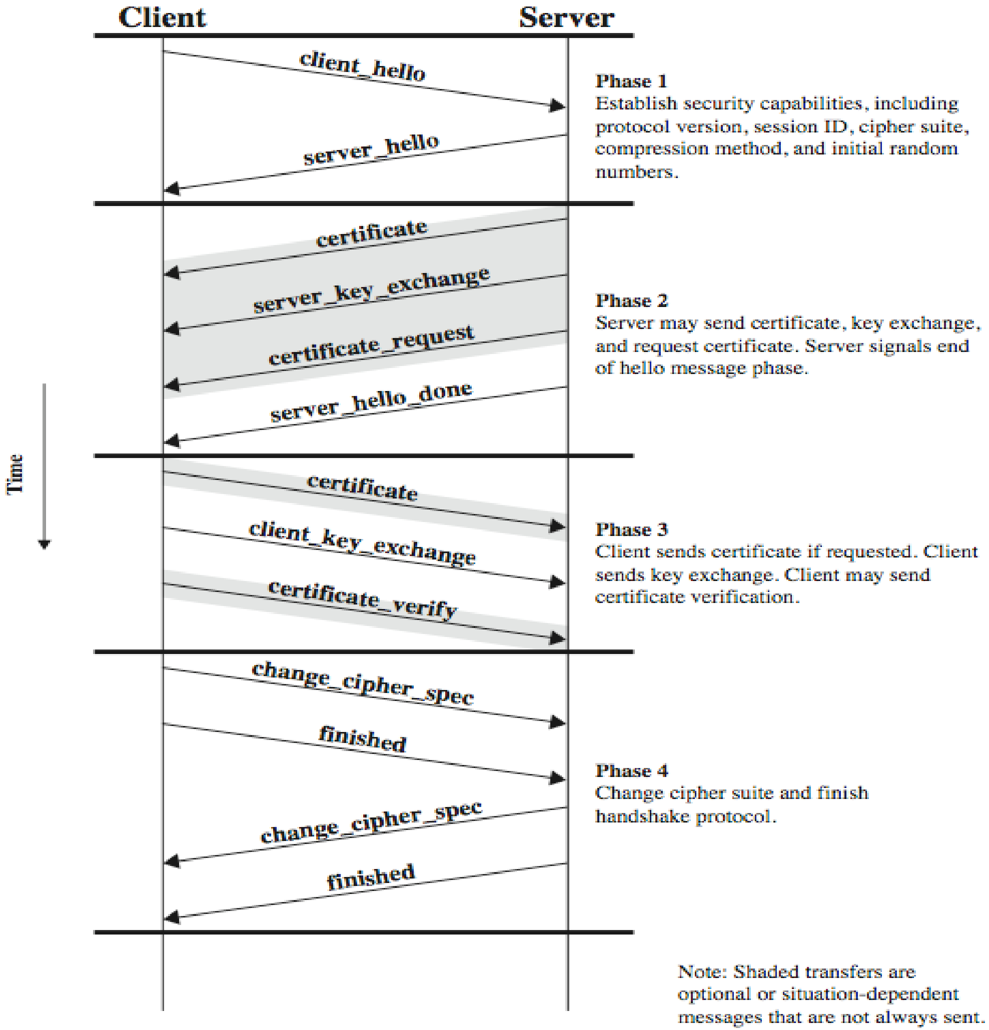
- **Phase-3**

  Client sends a secret master key encrypted with Server's public key

  Client may also send a signed hash of all of its previous messages in Cert_Verify msg

- **Phase-4**

  Handshake is completed and a secure connection is established



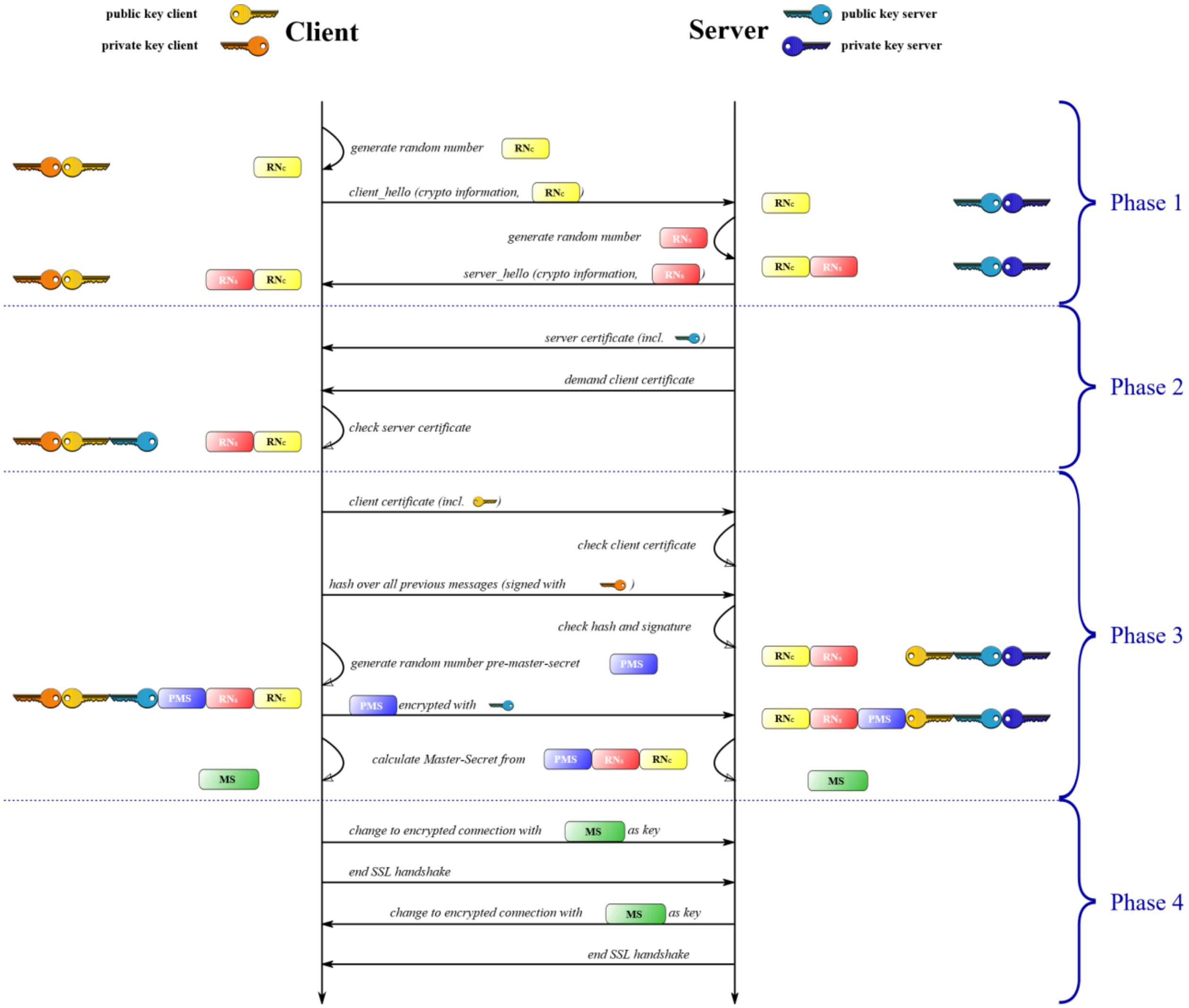
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

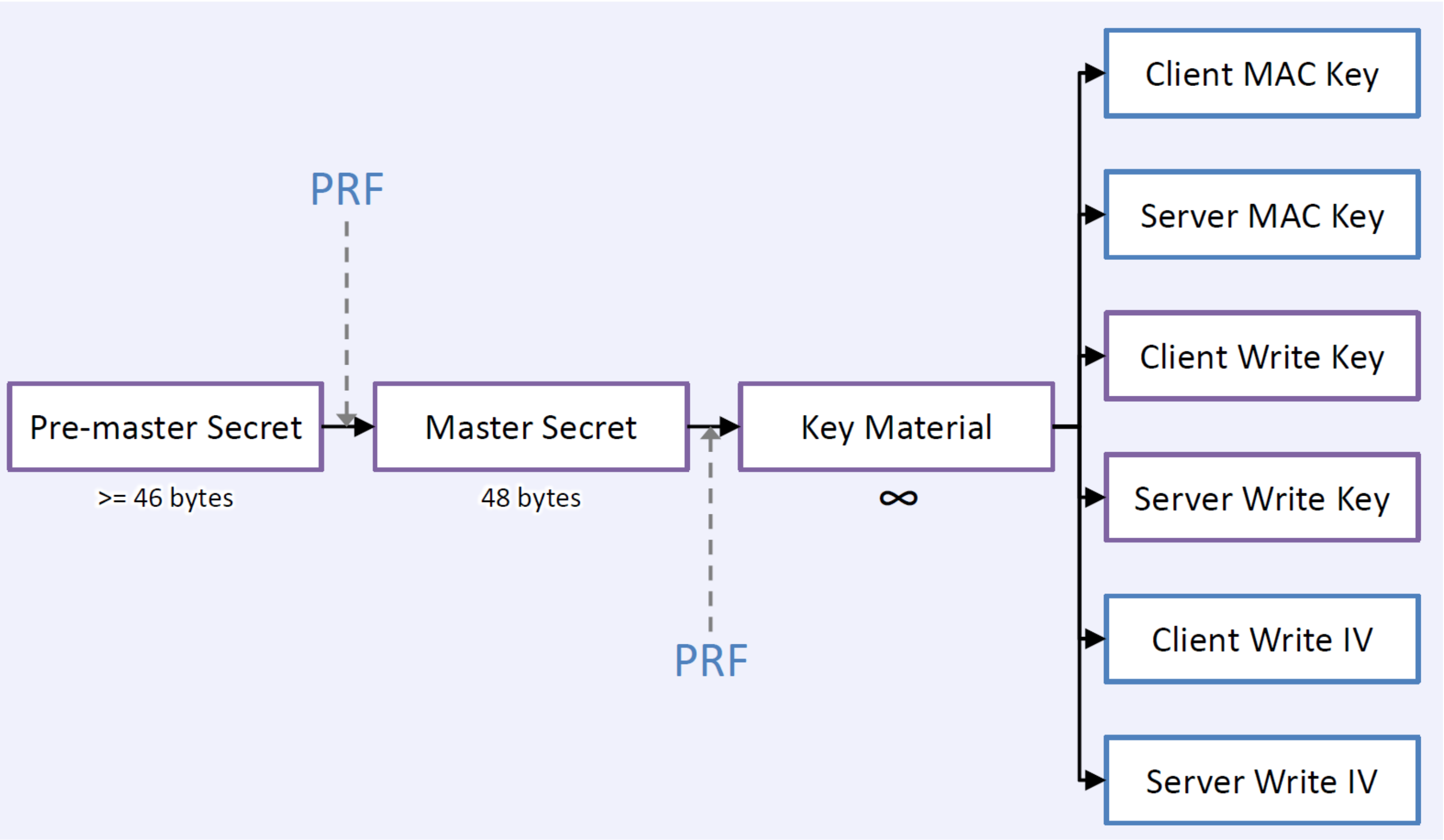
Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.


public key client
private key client
Client
Server
public key server
private key server
generate random number RN_c
RN_c
client_hello (crypto information, RN_c)
RN_c
generate random number RN_s
server_hello (crypto information, RN_s)
RN_s RN_c
RN_c RN_s
Phase 1
server certificate (incl.)
demand client certificate
check server certificate
RN_s RN_c
Phase 2
client certificate (incl.)
check client certificate
hash over all previous messages (signed with)
check hash and signature
RN_c RN_s
generate random number pre-master-secret PMS
PMS RN_s RN_c
PMS encrypted with
RN_c RN_s PMS
calculate Master-Secret from PMS RN_s RN_c
MS
MS
Phase 3
change to encrypted connection with MS as key
end SSL handshake
change to encrypted connection with MS as key
end SSL handshake
Phase 4

Key Generation in TLS 1.2



Pre-master Secret

>= 46 bytes

PRF

Master Secret

48 bytes

PRF

Key Material

∞

Client MAC Key

Server MAC Key

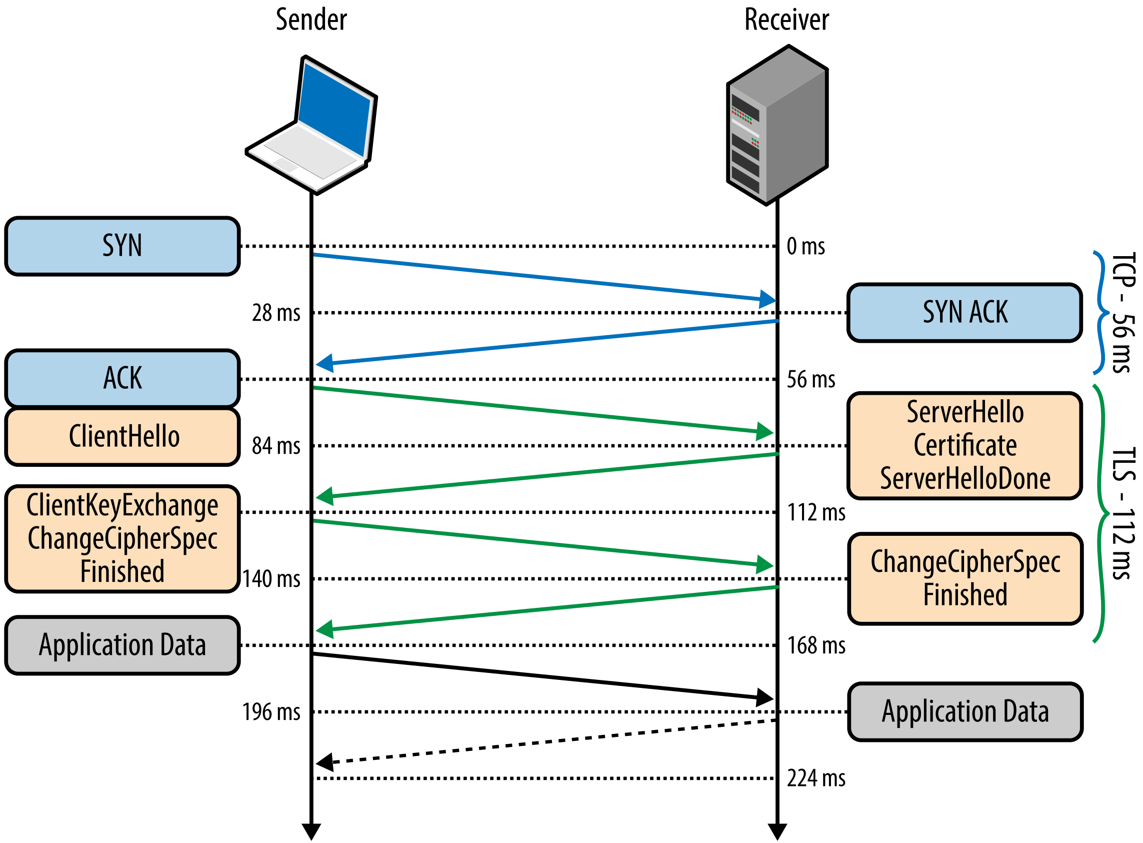
Client Write Key

Server Write Key

Client Write IV

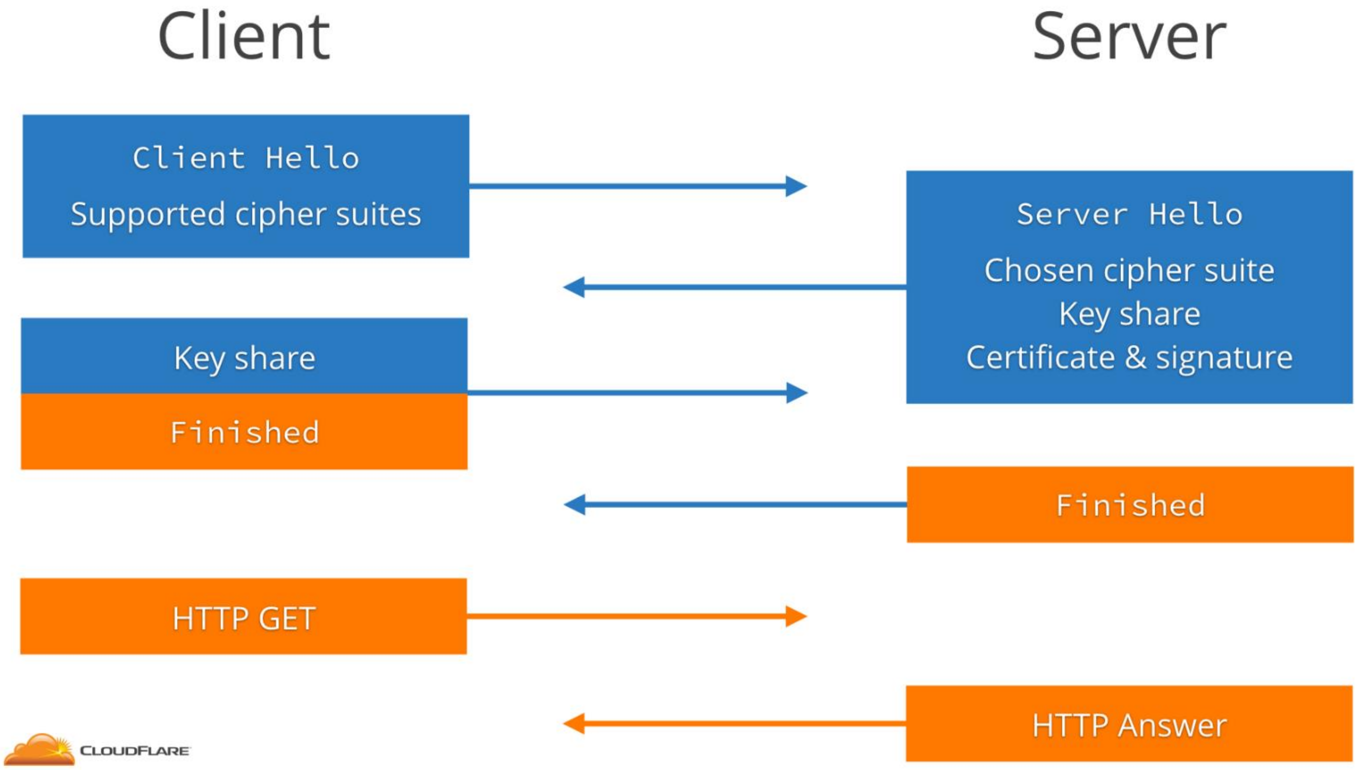
Server Write IV

Full TLS 1.2 handshake with timing information



Reference

TLS 1.2 (ECDHE)



Client

Server

Client Hello

Supported cipher suites

Server Hello

Chosen cipher suite

Key share

Certificate & signature

Key share

Finished

Finished

HTTP GET

HTTP Answer

Diffie–Hellman key exchange - Wikipedia

References

- https://en.wikipedia.org/wiki/Transport_Layer_Security
- RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2 (ietf.org)
- Networking 101: Transport Layer Security (TLS) - High Performance Browser Networking (O'Reilly) (hpbn.co)
- SSL/TLS beginner’s tutorial. This is a beginner’s overview of how… | by German Eduardo Jaber De Lima | Talpor | Medium
- Tutorial: SMTP Transport Layer Security (fehcom.de)
- Diffie–Hellman key exchange - Wikipedia