# Cybersecurity - Homework 10

Vlad Turno (1835365)

December 29, 2025

## 1) Introduction

*TLS* is a cryptographic protocol that ensures communication over untrusted networks by providing confidentiality as data is encrypted, integrity as data cannot be altered and authentication since communicating parts have to prove their identities.
*TLS* operates at a level between the transport layer and the application layer, therefore is application-agnostic and it secures the data stream regardless of the application protocol.
The *TLS Handshake* extablishes a shared cryptographic connection before the application data is shared, by performing a key exchange mechanism and a certificate validation process.

## 2) Configuration

Now I dump the *TLS* negotiation parameters obtained from the usage of OpenSSL API compared to the ones given by SSLLabs:

```
$ openssl s_client -connect cloudflare.com:443 -cipher ALL -tls1_3
CONNECTED(00000003)
depth=2 C = US, O = Google Trust Services LLC, CN = GTS Root R4
verify return:1
depth=1 C = US, O = Google Trust Services, CN = WE1
verify return:1
depth=0 CN = cloudflare.com
verify return:1
---
Certificate chain
 0 s:CN = cloudflare.com
   i:C = US, O = Google Trust Services, CN = WE1
   a:PKEY: id-ecPublicKey, 256 (bit); sigalg: ecdsa-with-SHA256
   v:NotBefore: Nov 14 20:28:36 2025 GMT; NotAfter: Feb 12 21:28:32 2026 GMT
 1 s:C = US, O = Google Trust Services, CN = WE1
   i:C = US, O = Google Trust Services LLC, CN = GTS Root R4
   a:PKEY: id-ecPublicKey, 256 (bit); sigalg: ecdsa-with-SHA384
   v:NotBefore: Dec 13 09:00:00 2023 GMT; NotAfter: Feb 20 14:00:00 2029 GMT
 2 s:C = US, O = Google Trust Services LLC, CN = GTS Root R4
   i:C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
   a:PKEY: id-ecPublicKey, 384 (bit); sigalg: RSA-SHA256
   v:NotBefore: Nov 15 03:43:21 2023 GMT; NotAfter: Jan 28 00:00:42 2028 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIID+zCCA6GgAwIBAgIRAO15rhrc6Ar2ET4r0vg6x7UwCgYIKoZIzj0EAwIwOzEL
MAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczEMMAoG
A1UEAxMDV0UxMB4XDTI1MTExNDIwMjgzNloXDTI2MDIxMjIxMjgzMlowGTEXMBUG
A1UEAxMOY2xvdWRmbGFyZS5jb20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAARs
NzD+heIbqfl8Nx3tPfDjQFtvT2HQDF+Xuarx5rVKjBgN95X/CiQ/KtjcSt7+EFXq
vTSmuPeX/AWVWVlf1T2vo4ICpjCCAqIwDgYDVR0PAQH/BAQDAgeAMBMGA1UdJQQM
MAoGCCsGAQUFBwMBMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFBuX4yUWU95RWpzp
XYbue1nsaUYTMB8GA1UdIwQYMBaAFJB3kjVnxP+ozKnme9mAeXvMk/k4MF4GCCsG
```

```
AQUFBwEBBFIwUDAnBggrBgEFBQcwAYYbaHR0cDovL28ucGtpLmdvb2cvcy93ZTEv
N1hrMCUGCCsGAQUFBzAChhlodHRwOi8vaS5wa2kuZ29vZy93ZTEuY3J0MHcGA1Ud
EQRwMG6CDmNsb3VkZmxhcmUuY29tghFucy5jbG91ZGZsYXJlLmNvbYITKi5ucy5j
bG91ZGZsYXJlLmNvbYIaKi5zZWNvbmRhcnkuY2xvdWRmbGFyZS5jb22CGHNlY29u
ZGFyeS5jbG91ZGZsYXJlLmNvbTATBgNVHSAEDDAKMAgGBmeBDAECATA2BgNVHR8E
LzAtMCugKaAnhiVodHRwOi8vYy5wa2kuZ29vZy93ZTEvQUhXaFA3WnZmZUkuY3Js
MIIBBQYKKwYBBAHWeQIEAgSB9gSB8wDxAHYAyzj3FYl8hKFEX1vB3fvJbvKaWc1H
CmkFhbDLFMMUWOcAAAGahEUtZAAABAMARzBFAiEA0jUY6kkzMZgtV+NJOk3mnPPh
6ySCEEkxxDO8J1lB3pkCIFU0G/16A6CX2auzcGtU5KUzF7cVy65tBj5pUP/Jderj
AHcADleUvPOuqT4zGyyZB7P3kN+bwj1xMiXdIaklrGHFTiEAAAGahEUtGwAABAMA
SDBGAiEAqiaro/ITLMdh7OlMSdLvO08UeenLAvFdEJw9CXAoK9oCIQCaxjlEnicz
ZR2ZbJAWsFtgZLQrBLVtFzKzvXgKo+BZeTAKBggqhkjOPQQDAgNIADBFAiEAkjZE
gH04OJ1o6XVbkHFizlrjuZLYYxPt1OW4zjKsVjMCIBT6ZZABfDQVIjBCKmcmTRMV
fsdx2bveFBHl/vr2SjKd
```

```
-----END CERTIFICATE-----
subject=CN = cloudflare.com
issuer=C = US, O = Google Trust Services, CN = WE1
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2911 bytes and written 328 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 86F514A96EA6B7E7976B585EC347099E1585F9624E693FDA2AB79EDF9D5D7CA8
    Session-ID-ctx:
    Resumption PSK: 2371B3F28972747088933B15DF4B64AA8937418AFEE0B00EE43D7CDF5416E13
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 64800 (seconds)
    TLS session ticket:
    0000 - c5 9d ec d6 ec 8c 3a e3-c5 37 1f f8 6f f3 dd d4
......:..7..o...
    0010 - b6 53 c9 d8 5f a9 45 c3-07 d6 3d a0 0f 19 49 a2
.S.._.E...=...I.
    0020 - 21 5a 73 ba 6d 93 03 db-c7 b5 8b f9 f3 5e 8f 3d
!Zs.m........^.=
    0030 - 92 59 1f fa e2 24 12 ec-fb fa 04 a1 1b 1a 86 16
.Y...$..........
    0040 - b6 38 33 6f 71 0b 49 c4-af 92 68 d6 f4 71 ce 57
.83oq.I...h..q.W
```

```
    0050 - a2 a2 21 a2 18 f9 dc 15-ea c7 6b 7a a5 4c 60 ec
..!.......kz.L`.
    0060 - 7b fc a9 64 ca a6 7d d0-47 92 6b b0 8d dd f4 a8
{..d..}.G.k.....
    0070 - 09 79 44 02 3c 7b dc b1-af 9c 16 a9 46 7d 21 d9
.yD.<{......F}!.
    0080 - 39 58 de 96 8c 1b 6e 10-d8 f8 bf d7 a3 29 fd d0
9X....n......)..
    0090 - 1f 51 2b 28 95 4e e8 eb-bd 5d e6 07 f7 17 9e d8
.Q+(.N...]......
    00a0 - af e5 56 48 4f b6 1d 2c-a8 ca 78 29 2f 84 e8 6d
..VHO..,..x)/..m
    00b0 - 18 b0 48 a9 3a 5b 4b 76-22 6e 54 92 e7 30 f4 31
..H.:[Kv"nT..0.1
    00c0 - 09 79 0b 81 fe f4 c7 b0-ce bf 12 a1 cd 61 f6 79
.y...........a.y

    Start Time: 1767039742
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 14336
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 60E2557392CAF410F7543D56545AD9C6007DAC3A65845B097586DCF3394DE618
    Session-ID-ctx:
    Resumption PSK: 9D644C727792FC120FC862E4D114E8DAC78F451F9C85E4F44B05E4F8EFC4937
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 64800 (seconds)
    TLS session ticket:
    0000 - c5 9d ec d6 ec 8c 3a e3-c5 37 1f f8 6f f3 dd d4
......:..7..o...
    0010 - 74 78 f7 07 1a d2 55 77-f9 ee 7c b7 d1 3f 79 1e
tx....Uw..|..?y.
    0020 - e7 0a 5e 0f e0 b3 af cf-80 af 17 91 46 7e c4 bd
..^.........F~..
    0030 - c2 f2 ee 91 02 e0 41 61-56 a6 34 d2 07 3e a2 f4
......AaV.4..>..
    0040 - cd f7 43 b8 b6 2e 05 61-e2 60 d4 7d be bb 22 a6
..C....a.`.}..".
    0050 - 59 40 d6 a1 1e 10 82 6d-1d b5 b8 3d 5d 96 71 30
Y@.....m...=].q0
    0060 - 87 cc b9 51 f3 c6 73 dd-34 db f7 c4 4a 45 51 d9
...Q..s.4...JEQ.
    0070 - 70 3a 79 72 e9 19 21 0a-52 bb f4 ad 40 51 73 b4
p:yr..!.R...@Qs.
    0080 - 48 4c 5d 98 4c c6 ab 54-b4 0b 61 39 75 17 31 f0
HL].L..T..a9u.1.
    0090 - ff 21 c3 72 ab ba 05 76-14 f8 e7 00 05 c5 5e b8
.!.r...v......^.
    00a0 - 3a 6e f3 65 58 f2 6d be-4d ef 1d f2 df e6 62 c0
:n.eX.m.M.....b.
```

```
    00b0 - 25 a0 26 e9 98 fe 7e 06-b3 8e ed f4 a3 db d1 4a
%.&...~........J
    00c0 - 6f 4f 73 cd e7 7a bf 23-c6 08 e4 b7 88 0a 21 30
oOs..z.#......!0

    Start Time: 1767039742
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 14336
---
read R BLOCK
closed
```

```
Server Key and Certificate #1
Subject         cloudflare.com
Fingerprint SHA256: 708b5398ef8d4c2e9c47d9a9c3628e731db80d5cf38c9d729d10df862f04935
Pin SHA256: zdbR4Y5bRi7BsB4HvKpPPFxukBbKnkt7JDDSgf467dc=
Common names    cloudflare.com
Alternative names       cloudflare.com ns.cloudflare.com *.ns.cloudflare.com *.seco
Serial Number   00cab07e5f69b82ffc0e84b20a2af26f80
Valid from      Fri, 14 Nov 2025 20:28:27 UTC
Valid until     Thu, 12 Feb 2026 21:26:01 UTC (expires in 1 month and 14 days)
Key     RSA 2048 bits (e 65537)
Weak key (Debian)       No
Issuer  WR1
AIA: http://i.pki.goog/wr1.crt
Signature algorithm     SHA256withRSA
Extended Validation     No
Certificate Transparency        Yes (certificate)
OCSP Must Staple        No
Revocation information  CRL, OCSP
CRL: http://c.pki.goog/wr1/7AItB636UoU.crl
OCSP: http://o.pki.goog/s/wr1/yrA
Revocation status       Good (not revoked)
CRL ERROR: IOException occurred
DNS CAA         Yes
policy host: cloudflare.com
issuewild: pki.goog; cansignhttpexchanges=yes flags:0
issue: letsencrypt.org flags:0
iodef: mailto:tls-abuse@cloudflare.com flags:0
issuewild: digicert.com; cansignhttpexchanges=yes flags:0
issue: ssl.com flags:0
issuewild: comodoca.com flags:0
issue: digicert.com; cansignhttpexchanges=yes flags:0
issuewild: letsencrypt.org flags:0
issue: comodoca.com flags:0
issuewild: ssl.com flags:0
issue: pki.goog; cansignhttpexchanges=yes flags:0
Trusted         Yes


Additional Certificates (if supplied)
Certificates provided   3 (4095 bytes)
Chain issues    None
#2
```

```
Subject         WR1
Fingerprint SHA256: b10b6f00e609509e8700f6d34687a2bfce38ea05a8fdf1cdc40c3a2a0d0d0e4
Pin SHA256: yDu9og255NN5GEf+Bwa9rTrqFQ0EydZ0r1FCh9TdAW4=
Valid until     Tue, 20 Feb 2029 14:00:00 UTC (expires in 3 years and 1 month)
Key     RSA 2048 bits (e 65537)
Issuer  GTS Root R1
Signature algorithm     SHA256withRSA
#3
Subject         GTS Root R1
Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e
Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
Valid until     Fri, 28 Jan 2028 00:00:42 UTC (expires in 2 years)
Key     RSA 4096 bits (e 65537)
Issuer  GlobalSign Root CA
Signature algorithm     SHA256withRSA

Certification Paths
1       Sent by server  cloudflare.com
Fingerprint SHA256: 708b5398ef8d4c2e9c47d9a9c3628e731db80d5cf38c9d729d10df862f04935
Pin SHA256: zdbR4Y5bRi7BsB4HvKpPPFxukBbKnkt7JDDSgf467dc=
RSA 2048 bits (e 65537) / SHA256withRSA
CRL ERROR: IOException occurred
2       Sent by server  WR1
Fingerprint SHA256: b10b6f00e609509e8700f6d34687a2bfce38ea05a8fdf1cdc40c3a2a0d0d0e4
Pin SHA256: yDu9og255NN5GEf+Bwa9rTrqFQ0EydZ0r1FCh9TdAW4=
RSA 2048 bits (e 65537) / SHA256withRSA
CRL ERROR: IOException occurred
3       In trust store  GTS Root R1   Self-signed
Fingerprint SHA256: d947432abde7b7fa90fc2e6b59101b1280e0e1c7e4e40fa3c6887fff57a7f4c
Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
RSA 4096 bits (e 65537) / SHA384withRSA


Server Key and Certificate #1
Subject         cloudflare.com
Fingerprint SHA256: dad41622d84a85573e24d9e669060486567025905 5a635a01f6ed7ea971007a
Pin SHA256: 0Jy8yqiKAxmg2xlvRhjVy+iIXEB6HQbEBO6+ANndTqw=
Common names    cloudflare.com
Alternative names       cloudflare.com ns.cloudflare.com *.ns.cloudflare.com *.seco
Serial Number   00ed79ae1adce80af6113e2bd2f83ac7b5
Valid from      Fri, 14 Nov 2025 20:28:36 UTC
Valid until     Thu, 12 Feb 2026 21:28:32 UTC (expires in 1 month and 14 days)
Key     EC 256 bits
Weak key (Debian)       No
Issuer  WE1
AIA: http://i.pki.goog/we1.crt
Signature algorithm     SHA256withECDSA
Extended Validation     No
Certificate Transparency        Yes (certificate)
OCSP Must Staple        No
Revocation information  CRL, OCSP
CRL: http://c.pki.goog/we1/AHWhP7ZvfeI.crl
OCSP: http://o.pki.goog/s/we1/7Xk
Revocation status       Good (not revoked)
CRL ERROR: IOException occurred
DNS CAA         Yes
policy host: cloudflare.com
issuewild: pki.goog; cansignhttpexchanges=yes flags:0
issue: letsencrypt.org flags:0
```

```
iodef: mailto:tls-abuse@cloudflare.com flags:0
issuewild: digicert.com; cansignhttpexchanges=yes flags:0
issue: ssl.com flags:0
issuewild: comodoca.com flags:0
issue: digicert.com; cansignhttpexchanges=yes flags:0
issuewild: letsencrypt.org flags:0
issue: comodoca.com flags:0
issuewild: ssl.com flags:0
issue: pki.goog; cansignhttpexchanges=yes flags:0
Trusted         Yes

Protocol Details
Secure Renegotiation    Supported
Secure Client-Initiated Renegotiation   No
Insecure Client-Initiated Renegotiation         No
BEAST attack    Not mitigated server-side (more info)
TLS 1.0: 0xc013
POODLE (SSLv3)  No, SSL 3 not supported (more info)
POODLE (TLS)    No (more info)
Zombie POODLE   No (more info)   TLS 1.2 : 0xc009
GOLDENDOODLE    No (more info)   TLS 1.2 : 0xc009
OpenSSL 0-Length        No (more info)   TLS 1.2 : 0xc009
Sleeping POODLE         No (more info)   TLS 1.2 : 0xc009
Downgrade attack prevention     Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression     No
RC4     No
Heartbeat (extension)   No
Heartbleed (vulnerability)      No (more info)
Ticketbleed (vulnerability)     No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)       No (more info)
OpenSSL Padding Oracle vuln.
(CVE-2016-2107)         No (more info)
ROBOT (vulnerability)   No (more info)
Forward Secrecy         With modern browsers (more info)
ALPN    Yes   h2 http/1.1
NPN     Yes   h2 http/1.1
Session resumption (caching)    No (IDs assigned but not accepted)
Session resumption (tickets)    Yes
OCSP stapling   Yes
Strict Transport Security (HSTS)        Yes
max-age=15780000; includeSubDomains
HSTS Preloading         Chrome  Edge  Firefox  IE
Public Key Pinning (HPKP)       No (more info)
Public Key Pinning Report-Only  No
Public Key Pinning (Static)     No (more info)
Long handshake intolerance      No
TLS extension intolerance       No
TLS version intolerance         No
Incorrect SNI alerts    No
Uses common DH primes   No, DHE suites not supported
DH public server param (Ys) reuse       No, DHE suites not supported
ECDH public server param reuse  No
Supported Named Groups  x25519, secp256r1, secp384r1, secp521r1 (server preferred o
SSL 2 handshake compatibility   Yes
0-RTT enabled   No

Miscellaneous
Test date       Mon, 29 Dec 2025 17:06:18 UTC
Test duration   108.837 seconds
```

```
HTTP status code          301
HTTP forwarding           https://www.cloudflare.com
HTTP server signature     cloudflare
 Server hostname          –
```

# 3) Assessments

Comparison of parameters observed during an active TLS handshake using OpenSSL with the broader configuration and policy analysis produced by SSL Labs. Both tools targeting cloudflare.com as host.

## 3.1) TLS Version and Cipher Suite

**OpenSSL**: A TLS 1.3 handshake was successfully negotiated using the cipher suite TLS_AES_256_GCM_SHA384 with no early data (0-RTT) used.

**SSL Labs**: Support for TLS 1.3 and TLS 1.2 only, with all legacy protocol versions disabled. The server advertises exclusively modern AEAD cipher suites.

Both tools agree on the use of modern TLS versions and strong cipher suites. OpenSSL confirms the server's preferred configuration as actually negotiated by a client, while SSL Labs enumerates the full set of supported policies. No downgrade paths or weak ciphers were observed.

## 3.2) Key Exchange and Forward Secrecy

**OpenSSL**: The handshake employed ephemeral elliptic-curve Diffie-Hellman key exchange (ECDHE) using the X25519 curve. Forward secrecy is therefore provided by design in TLS 1.3.

**SSL Labs**: forward secrecy is enabled for all modern clients. Supported elliptic curves include X25519, secp256r1, secp384r1 and secp521r1. Finite-field Diffie-Hellman cipher suites are not supported.

There is full consistency between the protocol-level and policy-level assessments. The exclusive use of ECDHE with modern curves ensures strong forward secrecy and resistance to retrospective decryption.

## 3.3) Certificate Chain

**OpenSSL**: The server presented a valid ECDSA leaf certificate for cloudflare.com, signed by a Google Trust Services intermediate certificate and ultimately anchored in a globally trusted root CA. Certificate verification completed successfully with no errors.

**SSL Labs**: Complete and correctly ordered certificate chain, widespread trust across major platforms, and active Certificate Transparency logging. The leaf certificate is short-lived and uses modern signature algorithms. Revocation information is available via OCSP and CRL.

OpenSSL verifies the cryptographic correctness and trust of the certificate chain, while SSL Labs extends the evaluation to ecosystem-level properties such as revocation mechanisms and transparency. Minor CRL fetch errors reported by SSL Labs do not affect overall trust.

## 3.4) ALPN/OCSP Stapling

**OpenSSL**: No ALPN protocol was negotiated during the observed handshake, and no OCSP stapled response was included.

**SSL Labs**: SSL Labs confirms that ALPN is enabled and supports h2 and http/1.1. OCSP stapling is enabled and functioning correctly. Session tickets and HSTS are also supported.

The apparent discrepancy arises from client behavior rather than server misconfiguration. OpenSSL reports only extensions explicitly requested during the handshake, whereas SSL Labs verifies server-side capability across multiple simulated clients.