CSCI-UA 480: Computer Networks Assignment 5

Kai Liao

December 5, 2020

1 SSL clients

1.1 HTTP request to www.google.com

```
[b'HTTP/1.1 200 OK',
 b'Date: Sun, 29 Nov 2020 06:11:08 GMT',
 b'Expires: -1',
 b'Cache-Control: private, max-age=0',
 b'Content-Type: text/html; charset=ISO-8859-1',
 b'P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."',
 b'Server: gws',
 b'X-XSS-Protection: 0',
 b'X-Frame-Options: SAMEORIGIN',
 b'Set-Cookie: 1P_JAR=2020-11-29-06; expires=Tue, 29-Dec-2020 06:11:08 GMT; pat'
 b'h=/; domain=.google.com; Secure',
 b'Set-Cookie: NID=204=VvQ46ni7qNa_4L-VXIMerjsJYy5Wxt7NBX4wzYUYag_qHHyk8nlLDyuz'
 b'2ApDkEoAl0ObaXpbgjs-47RJe9YC5Jsiufc3LJug7vyMpkCVpnOHxpJkJJ6jX95R78P2d9cy_zO3'
 b'MA7XTOZxFmFnnPhHIkajQj7lnwWjoEAemNzVfEU; expires=Mon, 31-May-2021 06:11:08 G'
 b'MT; path=/; domain=.google.com; HttpOnly',
 b'Alt-Svc: h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443";'
 b' ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443'
 b'"; ma=2592000; v="46,43"',
 b'Accept-Ranges: none',
 b'Vary: Accept-Encoding',
 b'Transfer-Encoding: chunked',
 b'',
 b'454e',
 b'<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang='
 b'"en"><head><meta content="Search']
```

1.2 HTTP request to www.amazon.com

```
[b'HTTP/1.1 200 OK',
 b'Content-Type: text/html;charset=UTF-8',
 b'Transfer-Encoding: chunked',
 b'Connection: keep-alive',
 b'Server: Server',
 b'Date: Sun, 29 Nov 2020 06:12:23 GMT',
 b'x-amz-rid: 6Z8TN87TNA1A6SQ4V6M3',
 b'Set-Cookie: session-id=130-0967678-6589315; Domain=.amazon.com; Expires=Mon,'
 b' 29-Nov-2021 06:12:23 GMT; Path=/; Secure',
 b'Set-Cookie: session-id-time=2082787201l; Domain=.amazon.com; Expires=Mon, 29'
 b'-Nov-2021 06:12:23 GMT; Path=/; Secure',
```

```
 b'Set-Cookie: i18n-prefs=USD; Domain=.amazon.com; Expires=Mon, 29-Nov-2021 06:'
 b'12:23 GMT; Path=/',
 b'Accept-CH: ect,rtt,downlink',
 b'Accept-CH-Lifetime: 86400',
 b'X-UA-Compatible: IE=edge',
 b'Content-Language: en-US',
 b'Cache-Control: no-cache',
 b'Pragma: no-cache',
 b'Expires: -1',
 b'X-XSS-Protection: 1;',
 b'X-Content-Type-Options: nosniff',
 b'Vary: Accept-Encoding,User-Agent,Content-Type,Accept-Encoding,X-Amzn-CDN-Cac'
 b'he,X-Amzn-AX-Treatment,User-Agent',
 b'Strict-Transport-Security: max-age=47474747; includeSubDomains; preload',
 b'X-Frame-Options: SAMEORIGIN',
 b'X-Cache: Miss from cloudfront',
 b'Via: 1.1 837618b47e5c2bb0a75ec63765498']
```

1.3 HTTP request to www.nytimes.com

```
[b'HTTP/1.1 301 Moved Permanently',
 b'Connection: close',
 b'Content-Length: 232',
 b'Server: Apache',
 b'Cache-Control: public, max-age=300',
 b'Location: https://www.nytimes.com/',
 b'Content-Type: text/html; charset=iso-8859-1',
 b'X-Origin-Time: 2020-11-29 06:10:08 UTC',
 b'Accept-Ranges: bytes',
 b'Date: Sun, 29 Nov 2020 06:13:25 GMT',
 b'Age: 197',
 b'X-Served-By: cache-ewr18129-EWR',
 b'X-Cache: HIT',
 b'X-Cache-Hits: 1',
 b'X-Timer: S1606630406.974604,VS0,VE1',
 b'Vary: Fastly-SSL',
 b'Set-Cookie: nyt-a=oOE_TDHPZYuMkvLnJdKM6l; Expires=Mon, 29 Nov 2021 06:13:25 '
 b'GMT; Path=/; Domain=.nytimes.com; SameSite=none; Secure',
 b'Set-Cookie: nyt-gdpr=0; Expires=Sun, 29 Nov 2020 12:13:25 GMT; Path=/; Domai'
 b'n=.nytimes.com',
 b'x-gdpr: 0',
 b'Set-Cookie: nyt-purr=cfhhcfhhhck; Expires=Mon, 29 Nov 2021 06:13:25 GMT; Pat'
 b'h=/; Domain=.nytimes.com; SameSite=Lax; Secure',
 b'X-Frame-Options: DENY',
 b'onion-location: https://www.nytimes3xbfgragh.onion/index.html',
 b'X-API-Version: F-GL',
 b'x-nyt-route: legacy-gke',
 b"Content-Security-Policy: upgrade-insecure-requests; default-src data: 'unsaf"
 b"e-inline' 'unsafe-eval'"]
```

1.4 HTTP request to www.facebook.com

```
[b'HTTP/1.1 302 Found',
 b'Location: https://www.facebook.com/unsupportedbrowser',
```

```
 b'Strict-Transport-Security: max-age=15552000; preload',
 b'Content-Type: text/html; charset="utf-8"',
 b'X-FB-Debug: jjey610MBws/FCGsES3J7xdTfxIy+7ecU5Rr/VOXD3RktJ6LvkOC5LrStVPD+en/'
 b'9QIe4p4C8dYa3VnVEHBffg==',
 b'Date: Sun, 29 Nov 2020 06:14:27 GMT',
 b'Alt-Svc: h3-29=":443"; ma=3600,h3-27=":443"; ma=3600',
 b'Connection: keep-alive',
 b'Content-Length: 0',
 b'',
 b'']
```

1.5 Changing recv bytes

We increase 1024 bytes to 4096 bytes, and initiate the same HTTP request to www.google.com The output does change. The notable difference is the last html code that our request returns.

```
 b'<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang='
 b'"en"><head><meta content="Search the world\'s information, including webp'
 b'ages, images, videos and more. Google has many special features to help you '
 b'find exactly what you\'re looking for." name="description"><meta content='
 b'"noodp" name="robots"><me']
```

Since we receive more bytes here, we receive more text in the last html code.

2 SSL certificates

2.1 Certificate from Google

```
{'OCSP': ('http://ocsp.pki.goog/gts1o1core',),
 'caIssuers': ('http://pki.goog/gsr2/GTS1O1.crt',),
 'crlDistributionPoints': ('http://crl.pki.goog/GTS1O1core.crl',),
 'issuer': ((('countryName', 'US'),),
            (('organizationName', 'Google Trust Services'),),
            (('commonName', 'GTS CA 1O1'),)),
 'notAfter': 'Jan 26 07:39:18 2021 GMT',
 'notBefore': 'Nov  3 07:39:18 2020 GMT',
 'serialNumber': 'E5895014FFA656CF02000000008055FE',
 'subject': ((('countryName', 'US'),),
             (('stateOrProvinceName', 'California'),),
             (('localityName', 'Mountain View'),),
             (('organizationName', 'Google LLC'),),
             (('commonName', 'www.google.com'),)),
 'subjectAltName': (('DNS', 'www.google.com'),),
 'version': 3}
```

2.2 Certificate from Amazon

```
{'OCSP': ('http://ocsp.digicert.com',),
 'caIssuers': ('http://cacerts.digicert.com/DigiCertGlobalCAG2.crt',),
 'crlDistributionPoints': ('http://crl3.digicert.com/DigiCertGlobalCAG2.crl',
                           'http://crl4.digicert.com/DigiCertGlobalCAG2.crl'),
 'issuer': ((('countryName', 'US'),),
            (('organizationName', 'DigiCert Inc'),),
            (('commonName', 'DigiCert Global CA G2'),)),
 'notAfter': 'Jul 10 12:00:00 2021 GMT',
```

```
 'notBefore': 'Jul 13 00:00:00 2020 GMT',
 'serialNumber': '05F9903B912F1A009CADC806652BDA18',
 'subject': ((('countryName', 'US'),),
             (('stateOrProvinceName', 'Washington'),),
             (('localityName', 'Seattle'),),
             (('organizationName', 'Amazon.com, Inc.'),),
             (('commonName', 'www.amazon.com'),)),
 'subjectAltName': (('DNS', 'amazon.com'),
                    ('DNS', 'amzn.com'),
                    ('DNS', 'uedata.amazon.com'),
                    ('DNS', 'us.amazon.com'),
                    ('DNS', 'www.amazon.com'),
                    ('DNS', 'www.amzn.com'),
                    ('DNS', 'corporate.amazon.com'),
                    ('DNS', 'buybox.amazon.com'),
                    ('DNS', 'iphone.amazon.com'),
                    ('DNS', 'yp.amazon.com'),
                    ('DNS', 'home.amazon.com'),
                    ('DNS', 'origin-www.amazon.com'),
                    ('DNS', 'buckeye-retail-website.amazon.com'),
                    ('DNS', 'huddles.amazon.com'),
                    ('DNS', 'p-nt-www-amazon-com-kalias.amazon.com'),
                    ('DNS', 'p-yo-www-amazon-com-kalias.amazon.com'),
                    ('DNS', 'p-y3-www-amazon-com-kalias.amazon.com')),
 'version': 3}
```

2.3 Cetficate from NYTimes

```
{'OCSP': ('http://ocsp.sectigo.com',),
 'caIssuers': ('http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt',),
 'issuer': ((('countryName', 'GB'),),
            (('stateOrProvinceName', 'Greater Manchester'),),
            (('localityName', 'Salford'),),
            (('organizationName', 'Sectigo Limited'),),
            (('commonName',
              'Sectigo RSA Domain Validation Secure Server CA'),)),
 'notAfter': 'Apr  6 00:00:00 2022 GMT',
 'notBefore': 'Jan  3 00:00:00 2020 GMT',
 'serialNumber': 'B947803967139F666A54B56C27B852B5',
 'subject': ((('commonName', 'nytimes.com'),),),
 'subjectAltName': (('DNS', 'nytimes.com'),
                    ('DNS', '*.api.dev.nytimes.com'),
                    ('DNS', '*.api.nytimes.com'),
                    ('DNS', '*.api.stg.nytimes.com'),
                    ('DNS', '*.blogs.nytimes.com'),
                    ('DNS', '*.blogs.stg.nytimes.com'),
                    ('DNS', '*.dev.nyt.com'),
                    ('DNS', '*.dev.nyt.net'),
                    ('DNS', '*.dev.nytimes.com'),
                    ('DNS', '*.newsdev.nyt.net'),
                    ('DNS', '*.newsdev.nytimes.com'),
                    ('DNS', '*.nyt.com'),
                    ('DNS', '*.nyt.net'),
                    ('DNS', '*.nytco.com'),
```

```
                    ('DNS', '*.nytimes.com'),
                    ('DNS', '*.payflow.sbx.nytimes.com'),
                    ('DNS', '*.sbx.nytimes.com'),
                    ('DNS', '*.stg.newsdev.nyt.net'),
                    ('DNS', '*.stg.newsdev.nytimes.com'),
                    ('DNS', '*.stg.nyt.com'),
                    ('DNS', '*.stg.nyt.net'),
                    ('DNS', '*.stg.nytimes.com'),
                    ('DNS', '*.timestalks.com'),
                    ('DNS', 'nyt.com'),
                    ('DNS', 'nyt.net'),
                    ('DNS', 'nytco.com'),
                    ('DNS', 'timestalks.com'),
                    ('DNS', 'www.homedelivery.nytimes.com')),
 'version': 3}
```

2.4 Certificate from Facebook

```
{'OCSP': ('http://ocsp.digicert.com',),
 'caIssuers': ('http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServerCA.crt',),
 'crlDistributionPoints': ('http://crl3.digicert.com/sha2-ha-server-g6.crl',
                           'http://crl4.digicert.com/sha2-ha-server-g6.crl'),
 'issuer': ((('countryName', 'US'),),
            (('organizationName', 'DigiCert Inc'),),
            (('organizationalUnitName', 'www.digicert.com'),),
            (('commonName', 'DigiCert SHA2 High Assurance Server CA'),)),
 'notAfter': 'Jan 30 23:59:59 2021 GMT',
 'notBefore': 'Nov  2 00:00:00 2020 GMT',
 'serialNumber': '0AA94B5AFA70A370979AC50647EFAC9C',
 'subject': ((('countryName', 'US'),),
             (('stateOrProvinceName', 'California'),),
             (('localityName', 'Menlo Park'),),
             (('organizationName', 'Facebook, Inc.'),),
             (('commonName', '*.facebook.com'),)),
 'subjectAltName': (('DNS', '*.facebook.com'),
                    ('DNS', '*.facebook.net'),
                    ('DNS', '*.fbcdn.net'),
                    ('DNS', '*.fbsbx.com'),
                    ('DNS', '*.m.facebook.com'),
                    ('DNS', '*.messenger.com'),
                    ('DNS', '*.xx.fbcdn.net'),
                    ('DNS', '*.xy.fbcdn.net'),
                    ('DNS', '*.xz.fbcdn.net'),
                    ('DNS', 'facebook.com'),
                    ('DNS', 'messenger.com')),
 'version': 3}
```

2.5 Meaning of crlDistributionPoints, notAfter, and notBefore

crlDistributionPoints are the locations where CRL and certificates are stored on the Internet. CRL is a certificate revocation list which stores list of certificates that are valid but are revoked [1]. notBefore: Certificate is not valid before this date. notAfter: certificate is not valid after this date.

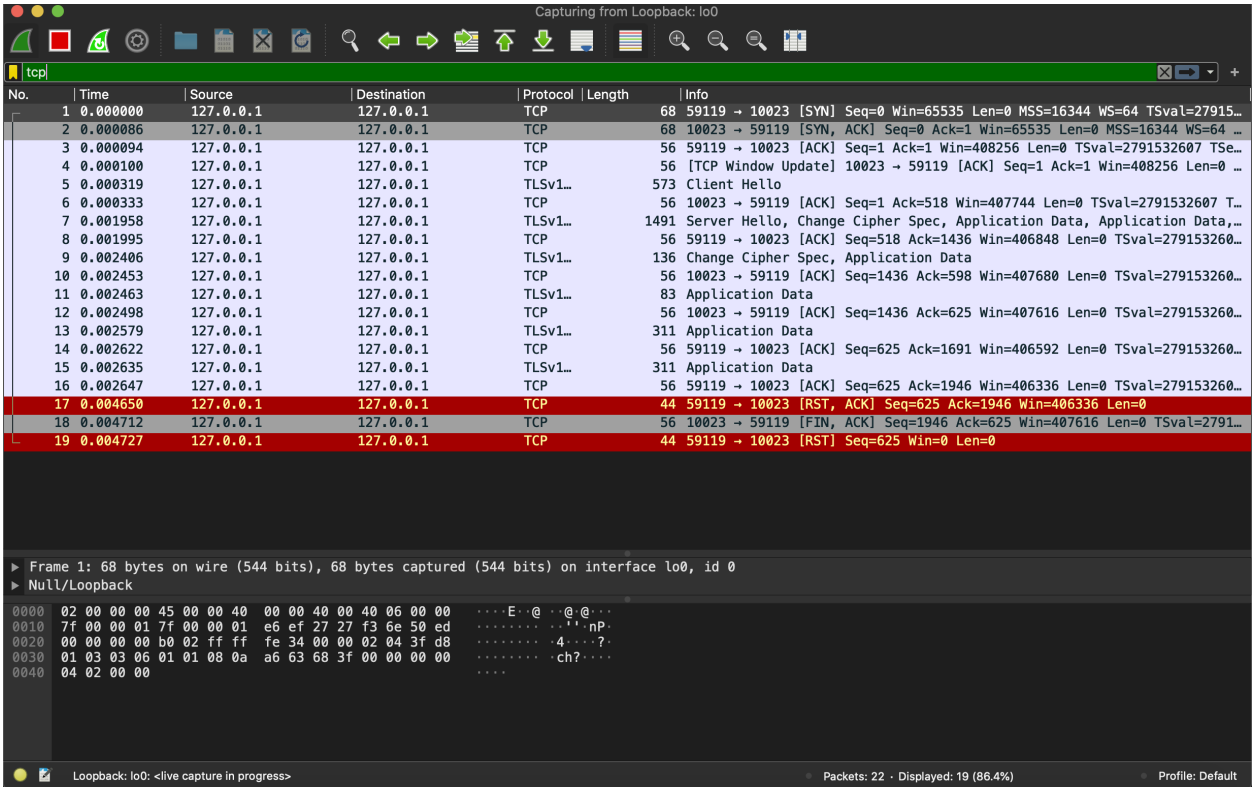

Figure 1: Packets exchanged between SSL client and server

3 SSL server

`ssl_server.py` : server using self-signed certificate
`cert.pem` : self-signed certificate
`ssl_client.py` : client connected to server

Run the server first using:

```
python3 ssl_server.py
```

Then run the client using:

```
python3 ssl_client.py
```

4 The mechanics of SSL

The first three lines the in the figure are the TCP handshake. The client sends SYN to the server which is on listen mode. The server responds with SYN+ACK. The client then respones with ACK.

TLS handshake consists of Client Hello, Server Hello, and Change Ciper Spec from both. Client Hello serves to indicate the cipher suites available, the TLS version that the client supports, and random bytes. Server Hello serves to decide the cipher suite and TLS version, and generate a random integer. The Change Ciper Spec from both client and server serves to change the encryption to symmetric key encryption [2].

References

[1] Abobe Illustrator. *What is a CRL.*

[2] Apporv munshi. *TLS v1.2 handshake overview.*