Rapport Labo 4 - Cryptographie

Auteur : Harun Ouweis

8 Questions

1. Pourquoi devons-nous transmettre une chaîne de certificats dans les deux applications (email et TLS) ?

Réponse : Transmettre une chaîne de certificats dans les applications d'email et TLS permet de garantir la validité et la confiance des certificats utilisés. Une chaîne de certificats contient le certificat final ainsi que les certificats intermédiaires jusqu'au certificat racine. Cela permet à l'application de vérifier que chaque certificat de la chaîne a été signé par une autorité de certification de confiance. En validant toute la chaîne, on s'assure que le certificat utilisé est bien légitime et qu'il a été émis par une autorité reconnue et de confiance.

2. Comment avez-vous configuré nginx ? Donnez votre fichier de configuration.

Fichier de configuration :

```
# generated 2024-06-14, Mozilla Guideline v5.7, nginx 1.17.7, OpenSSL 1.1.1k,
intermediate configuration, no OCSP
# https://ssl-
config.mozilla.org/#server=nginx&version=1.17.7&config=intermediate&openssl=1.1.1k
&ocsp=false&guideline=5.7
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    location / {
        return 301 https://$host$request_uri;
    }
}

server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;

    ssl_certificate /etc/nginx/ssl/Harun-TLS-Chain.crt;
    ssl_certificate_key /etc/nginx/ssl/IP.key;
    ssl_session_timeout 1d;
    ssl_session_cache shared:MozSSL:10m;  # about 40000 sessions
    ssl_session_tickets off;

    # curl https://ssl-config.mozilla.org/ffdhe2048.txt > /etc/nginx/ssl/dhparam
    ssl_dhparam /etc/nginx/ssl/dhparam;

    # intermediate configuration
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-
```

```
ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-
SHA384:DHE-RSA-CHACHA20-POLY1305;
    ssl_prefer_server_ciphers off;

    # HSTS (ngx_http_headers_module is required) (63072000 seconds)
    add_header Strict-Transport-Security "max-age=63072000" always;

    location / {
        root /var/www/labo-crypto.com/public;
        index index.html;
    }
}
```

Comment je l'ai configuré et pourquoi :

Je me suis basé sur les recommandations de configuration de [ssl-config.mozilla.org] pour configurer Nginx selon la donnée. Voici les principales modifications et ajouts effectués :

1. Les chemins des certificats et des clés ont été spécifiés pour utiliser les certificats créés et les clés générées. Harun-TLS-Chain.crt est le certificat en chaîne qui inclut le certificat du serveur ainsi que les certificats intermédiaires. IP.key est la clé privée associée au certificat du serveur.

2. Le chemin vers le fichier de paramètres Diffie-Hellman a été ajusté pour refléter l'emplacement où le fichier a été téléchargé `(/etc/nginx/ssl/dhparam).` Ce fichier renforce la sécurité en utilisant des groupes Diffie-Hellman sécurisés pour l'échange de clés.

3. Cette section configure l'emplacement racine du serveur web, en spécifiant où les fichiers du site web sont stockés `(/var/www/labo-crypto.com/public)` et quel fichier utiliser comme page d'index `(index.html)`. Cela permet au serveur Nginx de servir le contenu web correctement.

3. Fournissez le résultat du scan de testssl sur votre serveur ainsi que des commentaires, si nécessaire.

Résultat du scan :

```
□[1m
#############################################################
    testssl.sh       3.2rc3 from □[m□[1mhttps://testssl.sh/dev/□[m
□[1m    (□[m□[0;37mbcb2ef3 2024-06-28 15:04:12□[m□[1m)□[m
□[1m
      This program is free software. Distribution and
             modification under GPLv2 permitted.
      USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

       Please file bugs @ □[m□[1mhttps://testssl.sh/bugs/□[m
□[1m
#############################################################□[m

 Using "OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)" [~94
```

```
ciphers]
 on DESKTOP-ORI6T24:/usr/bin/openssl
 (built: "Feb 16 08:51:30 2024", platform: "debian-amd64")


□[7m Start 2024-06-28 16:40:47                -->> 10.190.133.22:44309
(10.190.133.22) <<--□[m

 rDNS (10.190.133.22):   --
 Service detected:       HTTP


□[1m□[4m Testing protocols □[m□[4mvia sockets except NPN+ALPN □[m

□[1m SSLv2      □[m□[1;32mnot offered (OK)□[m
□[1m SSLv3      □[m□[1;32mnot offered (OK)□[m
□[1m TLS 1      □[mnot offered
□[1m TLS 1.1    □[mnot offered
□[1m TLS 1.2    □[m□[1;32moffered (OK)□[m
□[1m TLS 1.3    □[m□[1;32moffered (OK)□[m: final
□[1m NPN/SPDY   □[mnot offered
□[1m ALPN/HTTP2 □[m□[0;32mh2□[m, http/1.1 (offered)

□[1m□[4m Testing cipher categories □[m

□[1m NULL ciphers (no encryption)                      □[m□[1;32mnot offered
(OK)□[m
□[1m Anonymous NULL Ciphers (no authentication)        □[m□[1;32mnot offered
(OK)□[m
□[1m Export ciphers (w/o ADH+NULL)                     □[m□[1;32mnot offered
(OK)□[m
□[1m LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      □[m□[0;32mnot offered
(OK)□[m
□[1m Triple DES Ciphers / IDEA                         □[mnot offered
□[1m Obsoleted CBC ciphers (AES, ARIA etc.)            □[mnot offered
□[1m Strong encryption (AEAD ciphers) with no FS       □[mnot offered
□[1m Forward Secrecy strong encryption (AEAD ciphers)  □[m□[1;32moffered (OK)□[m


□[1m□[4m Testing server's cipher preferences □[m

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher
Suite Name (IANA/RFC)
-----------------------------------------------------------------------------
-----------------------------------------
□[4mSSLv2□[m
 -
□[4mSSLv3□[m
 -
□[4mTLSv1□[m
 -
□[4mTLSv1.1□[m
 -
□[4mTLSv1.2□[m (no server order, thus listed by strength)
```

```
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH□[0;32m 253□[m   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 x9f     DHE-RSA-AES256-GCM-SHA384         DH□[0;32m 2048□[m    AESGCM      256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
 xcca8   ECDHE-RSA-CHACHA20-POLY1305       ECDH□[0;32m 253□[m   ChaCha20    256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 xccaa   DHE-RSA-CHACHA20-POLY1305         DH□[0;32m 2048□[m    ChaCha20    256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH□[0;32m 253□[m   AESGCM      128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 x9e     DHE-RSA-AES128-GCM-SHA256         DH□[0;32m 2048□[m    AESGCM      128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
□[4mTLSv1.3□[m (no server order, thus listed by strength)
 x1302   TLS_AES_256_GCM_SHA384            ECDH□[0;32m 253□[m   AESGCM      256
TLS_AES_256_GCM_SHA384
 x1303   TLS_CHACHA20_POLY1305_SHA256      ECDH□[0;32m 253□[m   ChaCha20    256
TLS_CHACHA20_POLY1305_SHA256
 x1301   TLS_AES_128_GCM_SHA256            ECDH□[0;32m 253□[m   AESGCM      128
TLS_AES_128_GCM_SHA256

□[1m Has server cipher order?     □[mno
 (limited sense as client will pick)

□[1m□[4m Testing robust forward secrecy (FS)□[m□[4m -- omitting Null
Authentication/Encryption, 3DES, RC4 □[m

□[0;32m FS is offered (OK) □[m          TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256 ECDHE-RSA-AES256-GCM-SHA384
                             DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-
POLY1305 DHE-RSA-CHACHA20-POLY1305
                             TLS_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
□[1m Elliptic curves offered:     □[m□[0;32mprime256v1□[m □[0;32msecp384r1□[m
□[0;32msecp521r1□[m □[0;32mX25519□[m □[0;32mX448□[m
□[1m DH group offered:            □[m□[0;32mffdhe2048□[m
□[1m TLS 1.2 sig_algs offered:    □[m□[1;33mRSA+SHA1□[m RSA+SHA224 RSA+SHA256
RSA+SHA384 RSA+SHA512 RSA-PSS-RSAE+SHA256
                             RSA-PSS-RSAE+SHA384 RSA-PSS-RSAE+SHA512
□[1m TLS 1.3 sig_algs offered:    □[mRSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-
PSS-RSAE+SHA512

□[1m□[4m Testing server defaults (Server Hello) □[m

□[1m TLS extensions (standard)    □[m"renegotiation info/#65281" "EC point
formats/#11" "next protocol/#13172"
                             "supported versions/#43" "key share/#51" "max
fragment length/#1"
                             "application layer protocol negotiation/#16"
"extended master secret/#23"
□[1m Session Ticket RFC 5077 hint □[mno -- no lifetime advertised
□[1m SSL Session ID support       □[myes
□[1m Session Resumption           □[mTickets no, ID: yes
□[1m TLS clock skew□[m               Random values, no fingerprinting possible
□[1m Certificate Compression      □[mnone
```

```
□[1m Client Authentication          □[mnone
□[1m Signature Algorithm            □[m□[0;32mSHA256 with RSA□[m
□[1m Server key size                □[mRSA □[0;32m4096□[m bits (exponent is 65537)
□[1m Server key usage               □[mDigital Signature, Key Encipherment
□[1m Server extended key usage      □[mTLS Web Server Authentication, TLS Web
Client Authentication
□[1m Serial                         □[m7450FD15DAAAAAA1E629279604FD8C918065FD2C
(OK: length 20)
□[1m Fingerprints                   □[mSHA1
14395EBF75D34EBBA154EF0B9734CB774CD2CDEB
                                SHA256
CF9D0D43838E6C95823BC03EA0F3D95BCF1C1B4E8B11150DA03CC31D142B5F2F
□[1m Common Name (CN)               □[m□[3mIP □[m
□[1m subjectAltName (SAN)           □[m□[3m10.190.133.22 □[m
□[1m Trust (hostname)               □[m□[0;32mOk via SAN□[m
□[1m Chain of trust□[m                 □[0;32mOk   □[m□[0;35m□[m
□[1m EV cert□[m (experimental)         no
□[1m Certificate Validity (UTC)     □[m□[0;32m380 >= 60 days□[m (2024-06-14 12:58
--> 2025-07-14 12:58)
□[1m ETS/"eTLS"□[m, visibility info  not present
□[1m Certificate Revocation List    □[m--
□[1m OCSP URI                       □[m--
                                □[0;31mNOT ok --□[m neither CRL nor OCSP URI
provided
□[1m OCSP stapling                  □[mnot offered
□[1m OCSP must staple extension     □[m--
□[1m DNS CAA RR□[m (experimental)      □[1;33mnot offered□[m
□[1m Certificate Transparency       □[m--
□[1m Certificates provided□[m          2
□[1m Issuer                         □[m□[3mHarun-TLS□[m (□[3mHEIG-VD□[m from
□[3mCH□[m)
□[1m Intermediate cert validity     □[m#1: □[0;32mok > 40 days□[m (2034-06-14
11:01). □[3mHarun-TLS□[m <-- □[3mHEIG-VDRoot□[m
□[1m Intermediate Bad OCSP□[m (exp.) □[0;32mOk□[m


□[1m□[4m Testing HTTP header response @ "/" □[m

□[1m HTTP Status Code             □[m  200 OK
□[1m HTTP clock skew                □[m-2 sec from localtime
□[1m Strict Transport Security      □[m□[0;32m730 days□[m=63072000 s□[0;36m, just
this domain□[m
□[1m Public Key Pinning             □[m--
□[1m Server banner
□[mnginx/□[33m1□(B□[m.□[33m1□(B□[m□[33m4□(B□[m.□[33m0□(B□[m
(□[33m□[1mUbuntu□(B□[m)
□[1m Application banner             □[m--
□[1m Cookie(s)                      □[m(none issued at "/")
□[1m Security headers               □[m□[0;33m--□[m
□[1m Reverse Proxy banner           □[m--


□[1m□[4m Testing vulnerabilities □[m
```

```
□[1m Heartbleed□[m (CVE-2014-0160)                □[1;32mnot vulnerable (OK)□[m,
no heartbeat extension
□[1m CCS□[m (CVE-2014-0224)                       □[1;32mnot vulnerable (OK)□[m
□[1m Ticketbleed□[m (CVE-2016-9244), experiment.  □[1;32mnot vulnerable (OK)□[m,
no session ticket extension
□[1m ROBOT                                          □[m□[1;32mServer does not support
any cipher suites that use RSA key transport□[m
□[1m Secure Renegotiation (RFC 5746)              □[m□[1;32msupported (OK)□[m
□[1m Secure Client-Initiated Renegotiation     □[m□[0;32mnot vulnerable (OK)□[m
□[1m CRIME, TLS □[m(CVE-2012-4929)                   □[0;32mnot vulnerable (OK)□[m
□[1m BREACH□[m (CVE-2013-3587)                    □[0;33mpotentially NOT ok,
"gzip" HTTP compression detected.□[m - only supplied "/" tested
                                                  Can be ignored for static pages or if
no secrets in the page
□[1m POODLE, SSL□[m (CVE-2014-3566)               □[1;32mnot vulnerable (OK)□[m,
no SSLv3 support
□[1m TLS_FALLBACK_SCSV□[m (RFC 7507)              □[0;32mNo fallback possible
(OK)□[m, no protocol below TLS 1.2 offered
□[1m SWEET32□[m (CVE-2016-2183, CVE-2016-6329)    □[1;32mnot vulnerable (OK)□[m
□[1m FREAK□[m (CVE-2015-0204)                     □[1;32mnot vulnerable (OK)□[m
□[1m DROWN□[m (CVE-2016-0800, CVE-2016-0703)      □[1;32mnot vulnerable on this
host and port (OK)□[m
                                                  make sure you don't use this
certificate elsewhere with SSLv2 enabled services, see
                                                  https://search.censys.io/search?
resource=hosts&virtual_hosts=INCLUDE&q=CF9D0D43838E6C95823BC03EA0F3D95BCF1C1B4E8B1
1150DA03CC31D142B5F2F
□[1m LOGJAM□[m (CVE-2015-4000), experimental      common prime with 2048 bits
detected: □[3mRFC7919/ffdhe2048□[m (□[0;32m2048 bits□[m),
                                                  but no DH EXPORT ciphers
□[1m BEAST□[m (CVE-2011-3389)                        □[0;32mnot vulnerable (OK)□[m,
no SSL3 or TLS1
□[1m LUCKY13□[m (CVE-2013-0169), experimental     □[1;32mnot vulnerable (OK)□[m
□[1m Winshock□[m (CVE-2014-6321), experimental    □[1;32mnot vulnerable (OK)□[m
□[1m RC4□[m (CVE-2013-2566, CVE-2015-2808)        □[0;32mno RC4 ciphers detected
(OK)□[m


□[1m□[4m Running client simulations □[m□[1m□[4m(HTTP) □[m□[1m□[4mvia sockets
□[m

 Browser                      Protocol  Cipher Suite Name (OpenSSL)       Forward
Secrecy
--------------------------------------------------------------------------------
--------------
 Android 6.0                  TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256
□[0;32m256 bit ECDH (P-256)□[m
 Android 7.0 (native)         TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256
□[0;32m256 bit ECDH (P-256)□[m
 Android 8.1 (native)         TLSv1.2   ECDHE-RSA-AES128-GCM-SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Android 9.0 (native)         TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Android 10.0 (native)        TLSv1.3   TLS_AES_128_GCM_SHA256
```

```
□[0;32m253 bit ECDH (X25519)□[m
 Android 11 (native)          TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Android 12 (native)          TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Chrome 79 (Win 10)           TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Chrome 101 (Win 10)          TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Firefox 66 (Win 8.1/10)      TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Firefox 100 (Win 10)         TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 IE 6 XP                      No connection
 IE 8 Win 7                   No connection
 IE 8 XP                      No connection
 IE 11 Win 7                  TLSv1.2   DHE-RSA-AES256-GCM-SHA384
□[0;32m2048 bit DH  (ffdhe2048)□[m
 IE 11 Win 8.1                TLSv1.2   DHE-RSA-AES256-GCM-SHA384
□[0;32m2048 bit DH  (ffdhe2048)□[m
 IE 11 Win Phone 8.1          No connection
 IE 11 Win 10                 TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
□[0;32m256 bit ECDH (P-256)□[m
 Edge 15 Win 10               TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
□[0;32m253 bit ECDH (X25519)□[m
 Edge 101 Win 10 21H2         TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Safari 12.1 (iOS 12.2)       TLSv1.3   TLS_CHACHA20_POLY1305_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Safari 13.0 (macOS 10.14.6)  TLSv1.3   TLS_CHACHA20_POLY1305_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Safari 15.4 (macOS 12.3.1)   TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 Java 7u25                    No connection
 Java 8u161                   TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
□[0;32m256 bit ECDH (P-256)□[m
 Java 11.0.2 (OpenJDK)        TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m256 bit ECDH (P-256)□[m
 Java 17.0.3 (OpenJDK)        TLSv1.3   TLS_AES_256_GCM_SHA384
□[0;32m253 bit ECDH (X25519)□[m
 go 1.17.8                    TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m
 LibreSSL 2.8.3 (Apple)       TLSv1.2   ECDHE-RSA-CHACHA20-POLY1305
□[0;32m253 bit ECDH (X25519)□[m
 OpenSSL 1.0.2e               TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
□[0;32m256 bit ECDH (P-256)□[m
 OpenSSL 1.1.0l (Debian)      TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
□[0;32m253 bit ECDH (X25519)□[m
 OpenSSL 1.1.1d (Debian)      TLSv1.3   TLS_AES_256_GCM_SHA384
□[0;32m253 bit ECDH (X25519)□[m
 OpenSSL 3.0.3 (git)          TLSv1.3   TLS_AES_256_GCM_SHA384
□[0;32m253 bit ECDH (X25519)□[m
 Apple Mail (16.0)            TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
□[0;32m256 bit ECDH (P-256)□[m
```

```
 Thunderbird (91.9)           TLSv1.3   TLS_AES_128_GCM_SHA256
□[0;32m253 bit ECDH (X25519)□[m


□[1m□[4m Rating (experimental) □[m

□[1m Rating specs□[m (not complete)  SSL Labs's 'SSL Server Rating Guide'
(version 2009q from 2020-01-30)
□[1m Specification documentation
□[mhttps://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
□[1m Protocol Support □[m(weighted)  100 (30)
□[1m Key Exchange □[m    (weighted)  90 (27)
□[1m Cipher Strength □[m (weighted)  90 (36)
□[1m Final Score                  □[m93
□[1m Overall Grade                □[m□[1;32mA+□[m

□[7m Done 2024-06-28 16:41:51 [  67s] -->> 10.190.133.22:44309 (10.190.133.22)
<<--□[m
```

Explication du scan :

J'ai pu tiré les points positifs suivants :

Protocoles : Seuls TLS 1.2 et TLS 1.3 sont activés. Chiffrement : Aucune suite de chiffrement faible n'est offerte. Forward Secrecy : Offert. Certificat : Utilisation d'une clé de 4096 bits et validité de plus de 60 jours. Compatibilité : Compatible avec les navigateurs modernes. Vulnérabilités : Pas de vulnérabilités connues détectées. Note : Le serveur obtient une note globale de A+, ce qui est excellent et indique une configuration de sécurité très forte.

4. Quelle durée de validité avez-vous choisie pour le certificat du serveur TLS ? Pourquoi ?

Réponse : J'ai choisi une durée de validité de 395 jours (soit 1 an et 1 mois) afin de m'aligner sur les pratiques recommandées en cours. Une durée de validité relativement courte permet de réduire le risque en cas de compromission du certificat, car un nouveau certificat devra être émis régulièrement, limitant ainsi la durée pendant laquelle un certificat compromis pourrait être utilisé.