

Exercise: SSL/TLS





HTTPS (HTTP sur SSL/TLS) permet sécuriser les communications entre un serveur Web et un navigateur. La figure ci-dessous présente des paquets capturés chez un client web (navigateur) qui accède au site www.google.tn (la première colonne donne les numéros des paquets capturés).

Le navigateur calcule une clé secrète K (master key) et l'envoi au serveur dans un canal sécurisé.

No.	Time	Source	Destination	Protocol	Length	Info
15	0.545613000	192.168.1.4	193.95.57.20	DNS	73	Standard query 0xae9a A www.google.tn
16	0.566743000	193.95.57.20	192.168.1.4	DNS	475	Standard query response 0xae9a A 193.95.13.57 A 193.95.13.59 A 193.95.13.16 A 193.95.13.20 A 193.95.13.21
17	0.566937000	192.168.1.4	193.95.57.20	DNS	73	Standard query 0xb442 AAAA www.google.tn
18	0.588446000	193.95.57.20	192.168.1.4	DNS	247	Standard query response 0xb442 AAAA 2a00:1450:4002:808::2083
19	0.588768000	192.168.1.4	193.95.13.57	TCP	74	33866 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=665582 TSecr=0 WS=128
20	0.606281000	193.95.13.57	192.168.1.4	TCP	74	http > 33866 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1400 SACK_PERM=1 TSval=3726931217 TSecr=665582
21	0.606325000	192.168.1.4	193.95.13.57	TCP	66	33866 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=665586 TSecr=3726931217
22	0.606450000	192.168.1.4	193.95.13.57	HTTP	555	GET /7qws_rd=cr6eindm6xVobpMc0ZsAH9-4jQBA HTTP/1.1
23	0.634240000	193.95.13.57	192.168.1.4	TCP	66	http > 33866 [ACK] Seq=1 Ack=490 Win=30080 Len=0 TSval=3726931245 TSecr=665586
24	0.709940000	193.95.13.57	192.168.1.4	HTTP	622	HTTP/1.1 302 Found (text/html)
25	0.709963000	192.168.1.4	193.95.13.57	TCP	66	33866 > http [ACK] Seq=490 Ack=557 Win=30336 Len=0 TSval=665612 TSecr=3726931318
26	0.712178000	192.168.1.4	193.95.13.57	TCP	74	35164 > https [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=665613 TSecr=0 WS=128
27	0.729075000	193.95.13.57	192.168.1.4	TCP	74	https > 35164 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1400 SACK_PERM=1 TSval=3726931339 TSecr=665612
28	0.729109000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=665617 TSecr=3726931339
29	0.729289000	192.168.1.4	193.95.13.57	TLSv1.2	271	Client Hello
30	0.749978000	193.95.13.57	192.168.1.4	TCP	66	https > 35164 [ACK] Seq=1 Ack=206 Win=30080 Len=0 TSval=3726931361 TSecr=665617
31	0.772947000	193.95.13.57	192.168.1.4	TLSv1.2	1454	Server Hello
32	0.772969000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=206 Ack=1389 Win=32128 Len=0 TSval=665628 TSecr=3726931378
33	0.774449000	193.95.13.57	192.168.1.4	TCP	726	[TCP segment of a reassembled PDU]
34	0.774472000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=206 Ack=2049 Win=34944 Len=0 TSval=665628 TSecr=3726931378
35	0.778457000	193.95.13.57	192.168.1.4	TLSv1.2	1454	Certificate
36	0.778478000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=206 Ack=3437 Win=37888 Len=0 TSval=665629 TSecr=3726931378
37	0.778498000	193.95.13.57	192.168.1.4	TLSv1.2	181	Server Key Exchange
38	0.778505000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=206 Ack=3552 Win=37888 Len=0 TSval=665629 TSecr=3726931378
39	0.781434000	192.168.1.4	193.95.13.57	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
40	0.781548000	192.168.1.4	193.95.13.20	TCP	74	49127 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=665630 TSecr=0 WS=128
41	0.802681000	193.95.13.20	192.168.1.4	TCP	74	http > 49127 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1400 SACK_PERM=1 TSval=3726925424 TSecr=665630
42	0.802712000	192.168.1.4	193.95.13.20	TCP	66	49127 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=665635 TSecr=3726925424
43	0.802875000	192.168.1.4	193.95.13.20	OCSP	583	Request
44	0.818375000	193.95.13.57	192.168.1.4	TLSv1.2	410	New Session Ticket, Change Cipher Spec, Hello Request, Hello Request, Application Data, Application Data
45	0.855801000	192.168.1.4	193.95.13.57	TCP	66	35164 > https [ACK] Seq=333 Ack=3896 Win=48576 Len=0 TSval=665640 TSecr=3726931437

- 1. Que représentent les paquets 15, 16, 17 et 18 ?**
La requête et réponse auprès du serveur DNS. Demande d'établissement de connexion du client auprès du serveur DNS qui transmet cette requête au serveur du site www.google.tn
- 2. Que représentent les paquets 19, 20 et 21 ?**
Établissement de la poignée de main en 3 étapes (3 way handshake),
établissement de la connexion TCP
- 3. Que représentent les paquets 26, 27 et 28 ?**
Établissement de connexion sécurisée
- 4. Sur son navigateur l'utilisateur a tapé l'adresse**
<http://www.google.tn> ou <https://www.google.tn> ?
<https://www.google.tn> .

5. Préciser, à l'aide d'un schéma, les différents messages échangés pour établir une connexion sécurisée entre le client et www.google.tn !

CLIENT 192.168.1.4		SERVEUR 193.95.13.57
15-16-17-18 Requête DNS Recherche de la destination à travers le serveur DNS		
19-20-21 Établissement de la connexion TCP 3 étapes		
SYNC  Dans la première étape, le client établit une connexion avec un serveur. Il envoie un segment avec SYN et informe le serveur qu'il veut commencer une communication, et quel doit être son numéro de séquence.		
SYNC/ACK  Dans cette étape, le serveur répond à la demande du client avec le signal SYN-ACK défini. ACK vous aide à signifier la réponse du segment qui est reçu et SYN signifie quel numéro de séquence il doit pouvoir commencer avec les segments.		
ACK  Dans cette dernière étape, le client accuse réception de la réponse du serveur et ils créent tous les deux une connexion stable pour commencer le processus de transfert de données.		
ESTABLISHED, On peut maintenant commencer l'initialisation d'une connexion SSL		
INITIALISATION DE LA CONNEXION SSL		
22  Le client (192.168.1.4): envoie un paquet qui comporte: le protocole SSL qu'il supporte (Version). Un session ID Liste des modes de chiffrement (RSA-MD5) qu'il va supporter. Et étant poli il ne va oublier de dire HELLO		

23 -24

Le serveur (193.93.15.57): analyse les informations que le client à envoyé

Il vérifie la version SSL
Génère un session ID
Sélectionne le mode de chiffage.
Il envoie le certificat (la clé publique).
Et lui aussi pour être poli il va dire: HELLO



25

Le client (192.168.1.4): reçoit le certificat et le valide, après vérification de la validité et l'authenticité auprès de l'autorité certifiante (vérifier la signature présente à la fin du certificat). Il a une liste de certificats pré-utilisés de différentes autorités.

Sur Google chrome: paramètres avancées , Security, gérer les certificats, autorités de certifications intermédiaires) =

D'où l'importance d'avoir un navigateur à jour !

A savoir: à chaque fois qu'on reçoit le message qui nous demande d'accepter un certificat = le certificat sera ajouté à cette liste.

Va créer un numéro (clé) aléatoire (Premaster Security) et l'envoyer au serveur en le chiffrant avec la clé publique du serveur (et que le serveur est capable de le déchiffrer)



26 -27

Client et serveur font un calcul de clé et une communication symétrique (A clé unique) est faite entre eux, car la communication asymétrique est impossible: (seul le serveur possède un certificat et le client n'a pas de pair de clés).



28

ÉCHANGES DE MESSAGES CHIFFRÉS

Pourquoi on n'utilise pas directement le chiffrement asymétrique pour sécuriser les communications HTTPS ? Donner deux raisons.

A cause de la lenteur d'exécution, et des algorithmes de chiffrement et de déchiffrement qui sont assez complexes

La clé K (Premaster key) est-elle envoyée au serveur dans un canal sécurisé et authentifié ? expliquer ?

Oui. Elle chiffrée asymétriquement par le client et le serveur

Pourquoi certains anciens navigateurs web ne peuvent pas utiliser HTTPS ?

Manque d'une BD, et possibilité de chiffage pas assez importante

À votre avis, la clé privée du serveur web est stockée en clair ou protégé par mot de passe ? Expliquer.

Protégée par un mot de passe. Elle est confidentielle (parce qu'elle est faite pour déchiffrer et signer les messages)

Il est possible d'utiliser un certificat client stocké sur le navigateur pour l'échange HTTPS. Donnez un avantage et un inconvénient de procéder ainsi.

Avantage: Identifier le client, permet l'authentification auprès du serveur

Inconvénient: si faille dans le navigateur, l'attaquant a accès à toutes vos communications