HTTP-HTTPS

Célian Butré

Janvier 2021

Plan

Protocoles de communications

L'existence de protocoles de communications implique :

Protocoles de communications

L'existence de protocoles de communications implique :

- L'existence de communications simples

Protocoles de communications

L'existence de protocoles de communications implique :

- L'existence de communications simples
- L'existence de communications cryptées

Protocoles simples

Protocoles simples

- Protocoles universels

Protocoles simples

- Protocoles universels
- Protocoles personnels

Protocoles simples

- Protocoles universels
- Protocoles personnels
- Analogie du téléphone

Protocoles simples

- Protocoles universels
- Protocoles personnels
- Analogie du téléphone
- Données + Analyse = Information = Communication

Protocoles cryptés

Protocoles cryptés

- Nécessité d'encryption

Protocoles cryptés

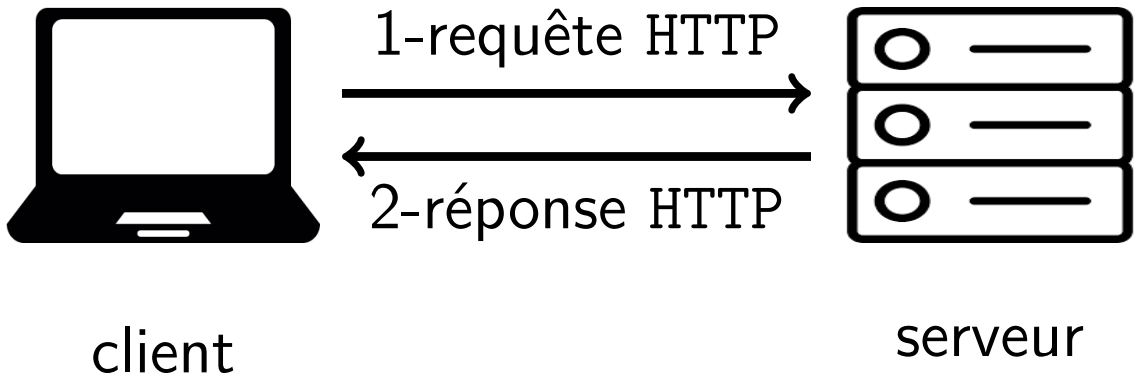
- Nécessité d'encryption
- RSA : clef publique - clef privée

Protocoles cryptés

- Nécessité d'encryption
- RSA : clef publique - clef privée
- Analogie de la boîte aux lettres

Le Protocole HTTP

Le Protocole HTTP



Contexte

Contexte

- Tim Berners-Lee : CERN

Contexte

- Tim Berners-Lee : CERN
- World Wide Web

Contexte

- Tim Berners-Lee : CERN
- World Wide Web
- Protocole HTTP

Description du protocole HTTP

Description du protocole HTTP

1. la méthode employée pour effectuer la requête (PUT, GET, DELETE, ETC.)

Description du protocole HTTP

1. la méthode employée pour effectuer la requête (PUT, GET, DELETE, ETC.)
2. l'URL de la ressource

Description du protocole HTTP

1. la méthode employée pour effectuer la requête (PUT, GET, DELETE, ETC.)
2. l'URL de la ressource
3. la version du protocole utilisé par le client (souvent HTTP 1.1)

Description du protocole HTTP

1. la méthode employée pour effectuer la requête (PUT, GET, DELETE, ETC.)
2. l'URL de la ressource
3. la version du protocole utilisé par le client (souvent HTTP 1.1)
4. le navigateur employé (Firefox, Chrome) et sa version

Description du protocole HTTP

1. la méthode employée pour effectuer la requête (PUT, GET, DELETE, ETC.)
2. l'URL de la ressource
3. la version du protocole utilisé par le client (souvent HTTP 1.1)
4. le navigateur employé (Firefox, Chrome) et sa version
5. le type du document demandé (par exemple HTML)

Exemple d'échange suivant le protocole HTTP

Algorithme 1 : Protocole HTTP.

```
GET /mondossier/monFichier.html HTTP/1.1
User-Agent : Mozilla/5.0
Accept : text/html



HTTP/1.1 200 OK
Date: Sat, 5 nov 1955 14:15:00 GMT
Server: Apache/2.0.54 (Debian GNU/Linux) DAV/2 SVN/1.1.4
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=ISO-8859-1
<un document HTML qui prend beaucoup trop de place>
</un document HTML qui prend beaucoup trop de place>
```

Exemple d'échange suivant le protocole HTTP

1 - -	Information
2 - -	Succès
3 - -	Redirection
4 - -	Erreur du client Web
5 - -	Erreur du serveur

Le protocole HTTPS

Le protocole HTTPS

HTTP + Sécurité = HTTPS

Le protocole HTTPS

HTTP + Sécurité = HTTPS

Sécurité = Protocole TLS

Motivation

Problèmes du Protocole HTTP

Motivation

Problèmes du Protocole `HTTP`

- Communications interceptables et non-cryptées

Motivation

Problèmes du Protocole `HTTP`

- Communications interceptables et non-cryptées
- Aucune preuve de l'authenticité du serveur receveur

Protocole TLS

Le protocole TLS garantit :

Protocole TLS

Le protocole TLS garantit :

* L'authentification du serveur

Protocole TLS

Le protocole TLS garantit :

* L'authentification du serveur
* L'encryption des données échangées

Protocole TLS

Le protocole TLS garantit :

* L'authentification du serveur
* L'encryption des données échangées
* L'intégrité des données

Protocole TLS

Le protocole TLS garantit :

* L'authentification du serveur
* L'encryption des données échangées
* L'intégrité des données
* (optionnel) L'authentification du **client**

Description du protocole HTTPS

Description du protocole HTTPS

$$\texttt{TLS}(\texttt{HTTP}) = \texttt{HTTPS}$$

Description du protocole HTTPS

TLS(HTTP) = HTTPS

Le protocole TLS est appliqué directement à la requête HTTP et encrypte

Description du protocole HTTPS

TLS(HTTP) = HTTPS

Le protocole TLS est appliqué directement à la requête HTTP et encrypte

- ✓ URL

Description du protocole HTTPS

TLS(HTTP) = HTTPS

Le protocole TLS est appliqué directement à la requête HTTP et encrypte

- ✓ URL
- ✓ Paramètres de la requête

Description du protocole HTTPS

TLS(HTTP) = HTTPS

Le protocole TLS est appliqué directement à la requête HTTP et encrypte

- ✓ URL
- ✓ Paramètres de la requête
- ✓ Les cookies transmis

Description du protocole HTTPS

TLS(HTTP) = HTTPS

Le protocole TLS est appliqué directement à la requête HTTP et encrypte

- ✓ URL
- ✓ Paramètres de la requête
- ✓ Les cookies transmis
- × Le nom du domaine accédé

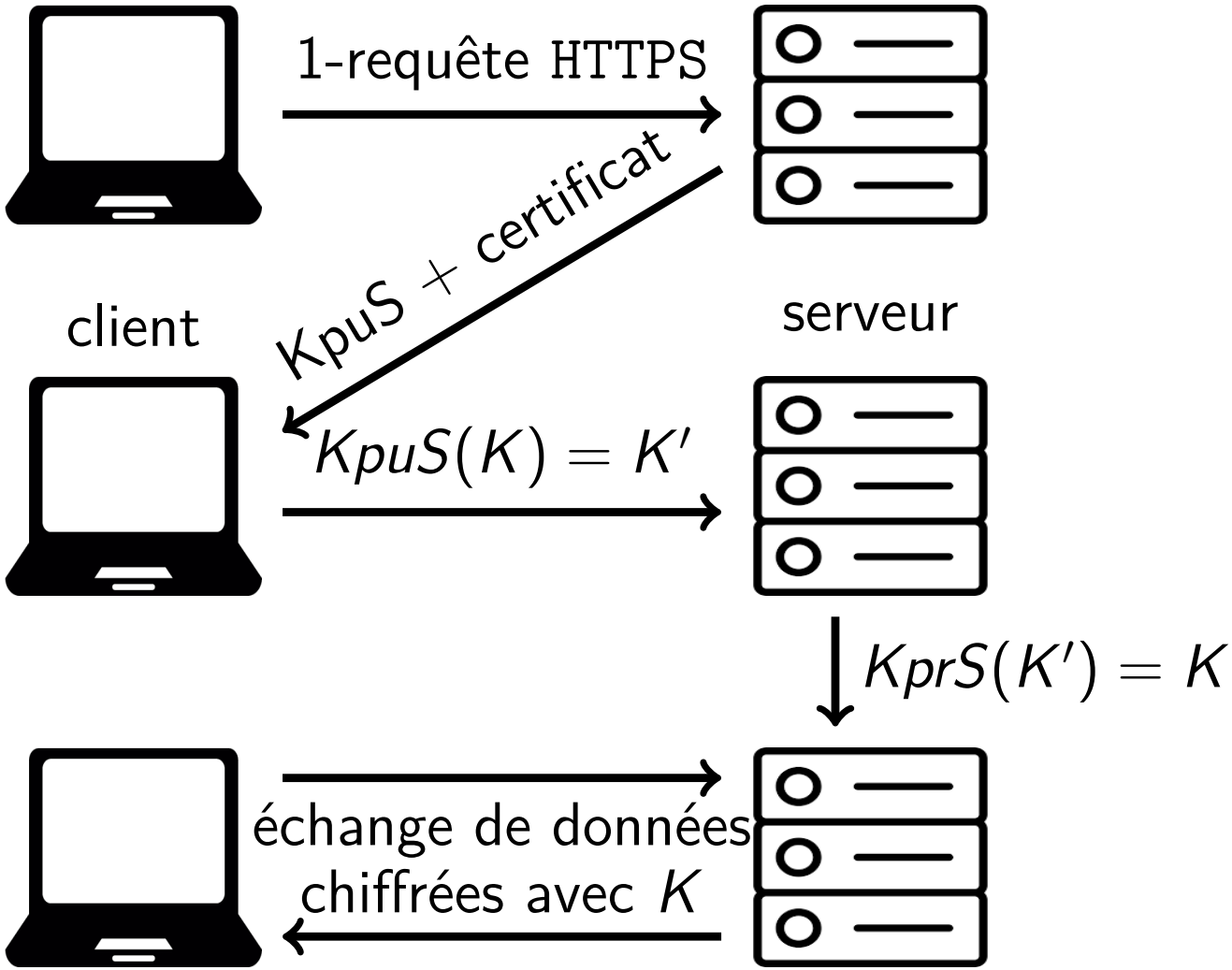
Description du protocole HTTPS

TLS(HTTP) = HTTPS

Le protocole TLS est appliqué directement à la requête HTTP et encrypte

- ✓ URL
- ✓ Paramètres de la requête
- ✓ Les cookies transmis
- × Le nom du domaine accédé
- × Les ports utilisés (et donc l'addresse IP)

Exemple du protocole HTTPS



Article sur les Couches de Transports Securise **WikipediaTLS**

Article sur les Couches de Transports Securise. https://fr.wikipedia.org/wiki/Transport_Layer_Security.

Article sur les Protocoles de Transferts d'HyperText **WikipediaHTTP**

Article sur les Protocoles de Transferts d'HyperText. https://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol.

Article sur les Protocoles de Transferts d'HyperText Securise **WikipediaHTTPS**

Article sur les Protocoles de Transferts d'HyperText Securise. https://en.wikipedia.org/wiki/HTTPS.

Bref Histoire sur les Protocoles de Transferts d'HyperText **HTTPHistory**

Bref Histoire sur les Protocoles de Transferts d'HyperText. https://hpbn.co/brief-history-of-http.

Roche : Cours sur la sécurisation des communications **PixeesSecurisation**

D. Roche. *Cours sur la sécurisation des communications*. https://pixees.fr/informatiquelycee/n_site/nsi_term_archi_secu.html.

Scott : Why the Web Is Such a Mess **TomScottCookies**

Tom Scott. *Why the Web Is Such a Mess*. https://www.youtube.com/watch?v=OFRjZtYs3wY&ab_channel=TomScott.

Wikepedia Tim Berners Lee **WikepediaTBL**

Wikepedia Tim Berners Lee.
https://en.wikipedia.org/wiki/Tim_Berners-Lee.

Wikipedia CERN **WikepediaCERN**

Wikipedia CERN. https://en.wikipedia.org/wiki/CERN.

Wikipedia World Wide Web **WikipediaWWW**

Wikipedia World Wide Web.
https://en.wikipedia.org/wiki/World_Wide_Web.

Le Logo Client **LogoClient**

Le Logo Client.
https://www.flaticon.com/free-icon/server_165130.

Le Logo Serveur **LogoServeur**

Le Logo Serveur.
https://www.pngkey.com/maxpic/u2w7o0e6i1o0y3o0/.