RFC 8446 : TLS 1.3

Description et éléments d'analyse d'impact sur les SI

Olivier Levillain Franck Rouxel

Conférence ESSI

Une brève histoire de SSL/TLS

Motivation pour une nouvelle version

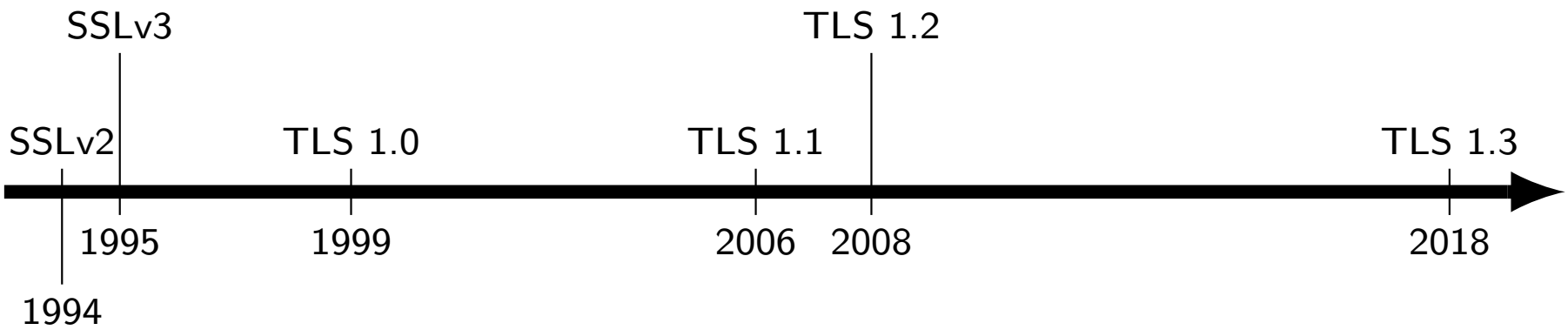
Impact de TLS sur l'analyse de flux

Conclusion

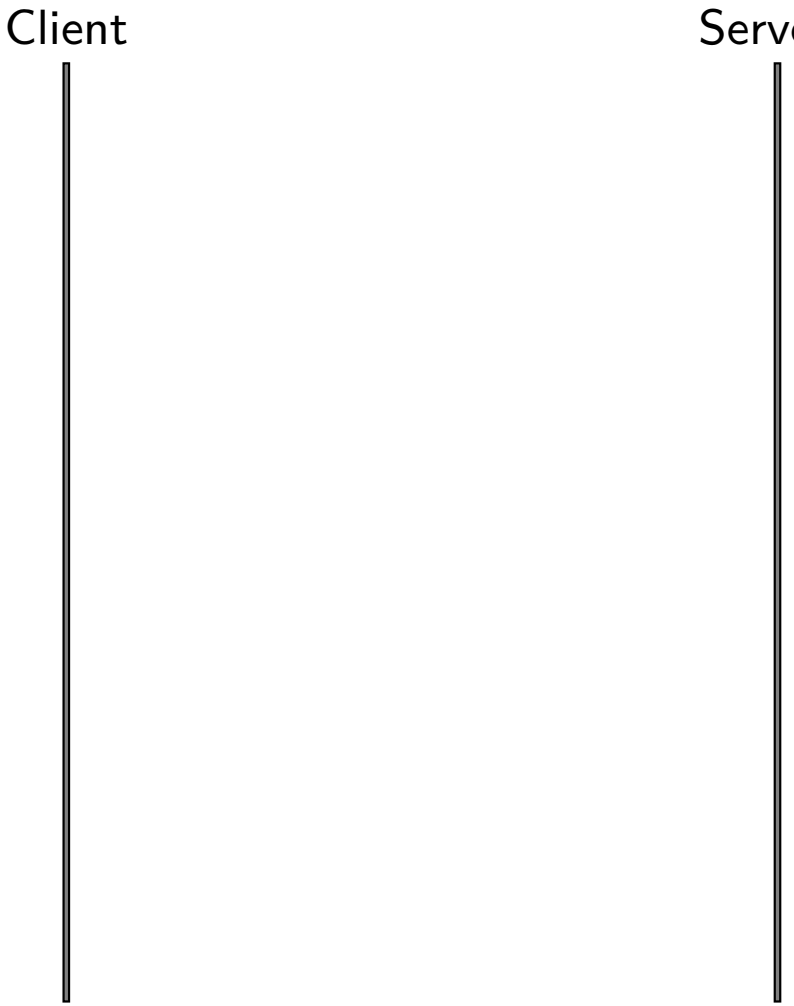
SSL/TLS : un pilier de la sécurité d'Internet

- Le schéma `https://` inventé par Netscape en 1995
  - début du commerce en ligne
  - SSL/TLS est aujourd'hui omiprésent
- Objectifs de sécurité
  - authentification du serveur (et du client)
  - protection en confidentialité et en intégrité des données
  - anti-rejeu
- Évolution des usages dans le monde du web
  - HTTP2 impose en pratique TLS
  - mise en avant des sites en HTTPS dans les moteurs de recherche
  - politique pro-active des navigateurs

Versions du protocole

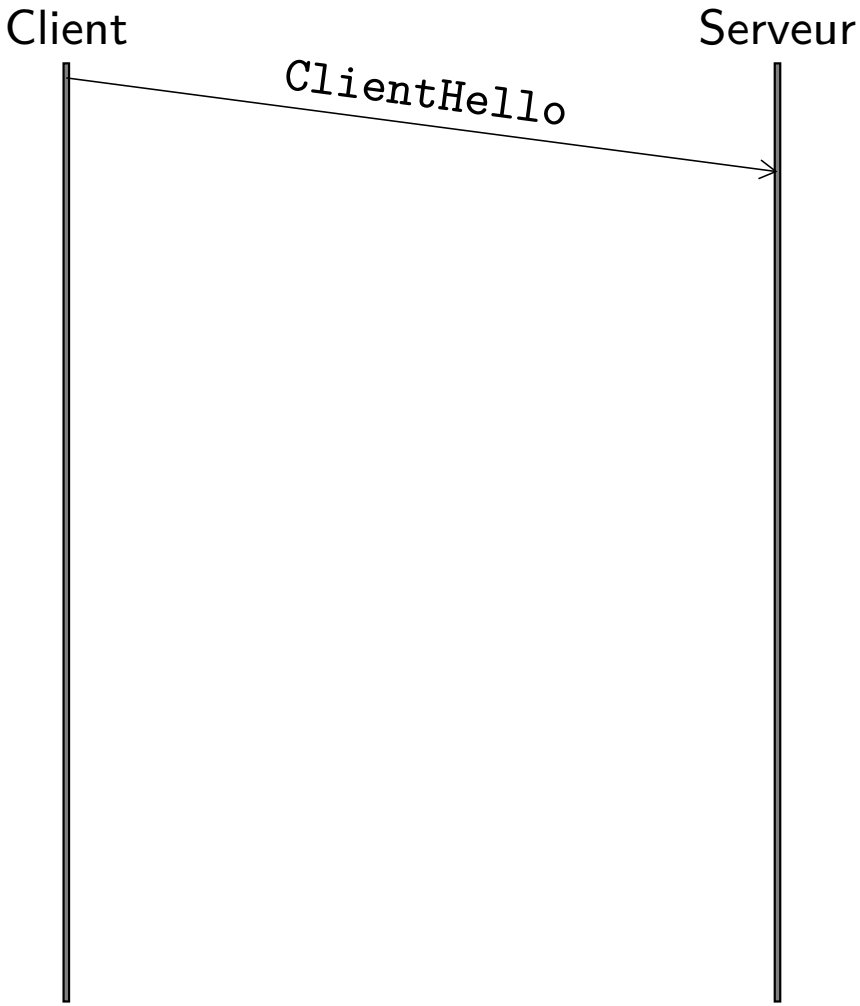


Fonctionnement du protocole



Hypothèses

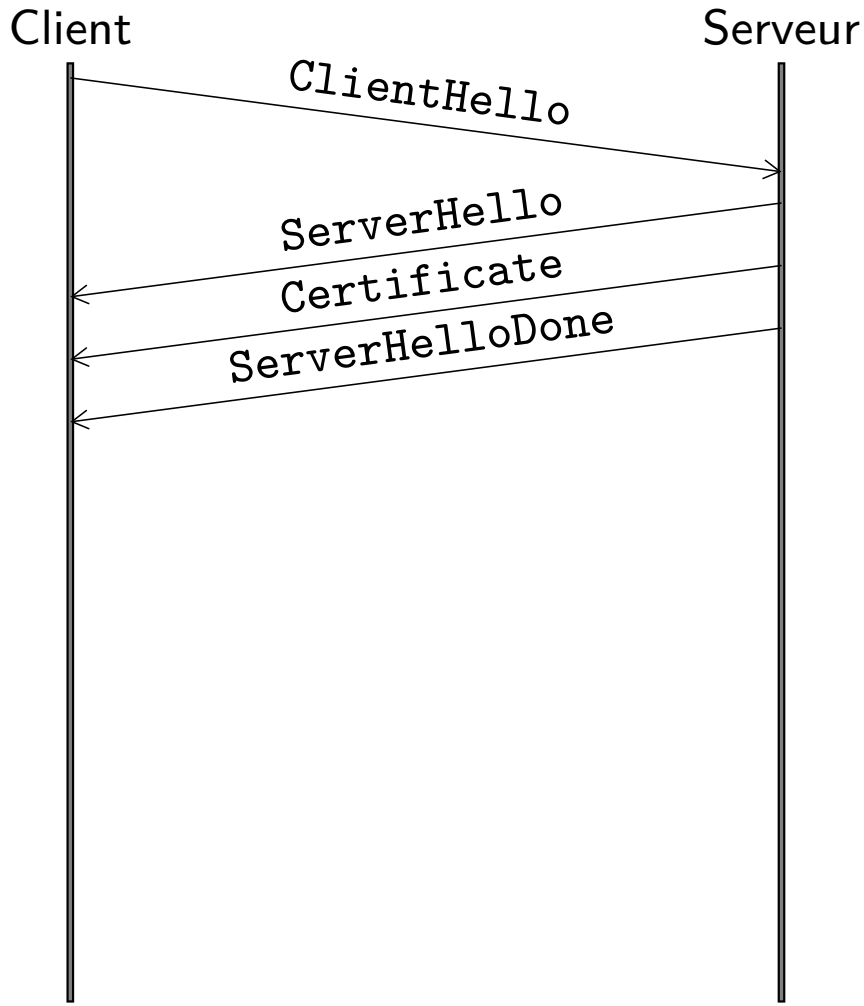
Fonctionnement du protocole



Hypothèses

- Version : SSLv3 - TLS 1.2

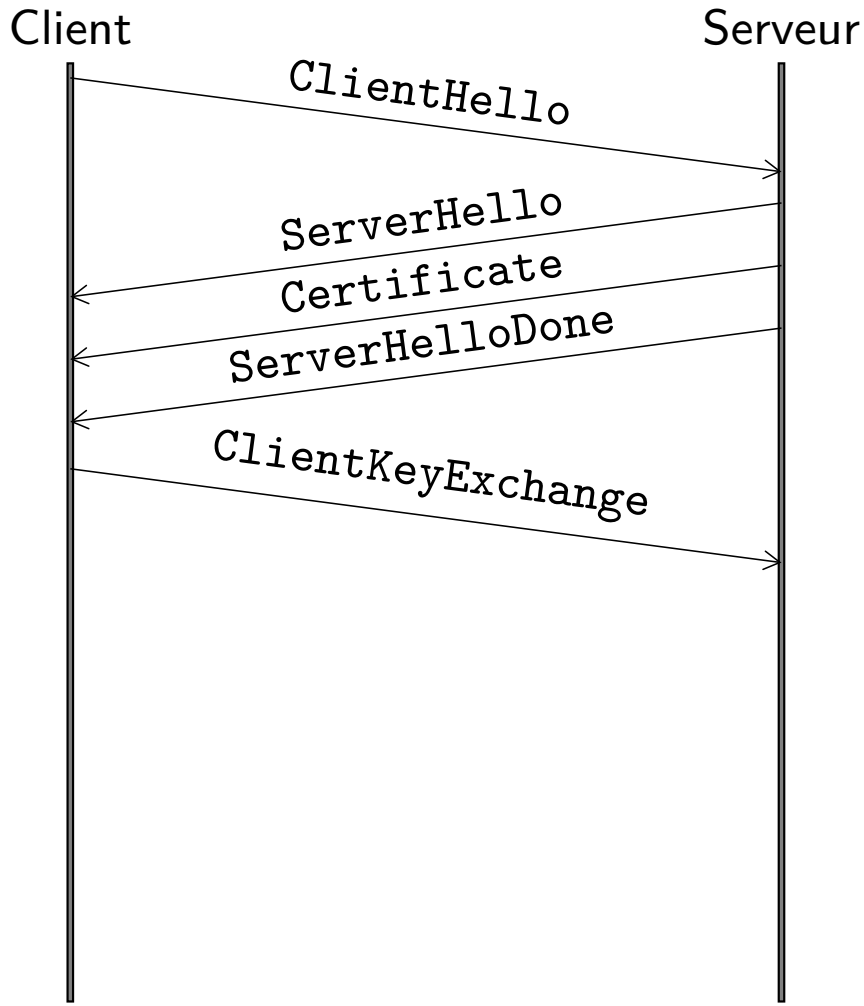
Fonctionnement du protocole



Hypothèses

- Version : SSLv3 - TLS 1.2
- Algorithme d'échange de clé : chiffrement RSA

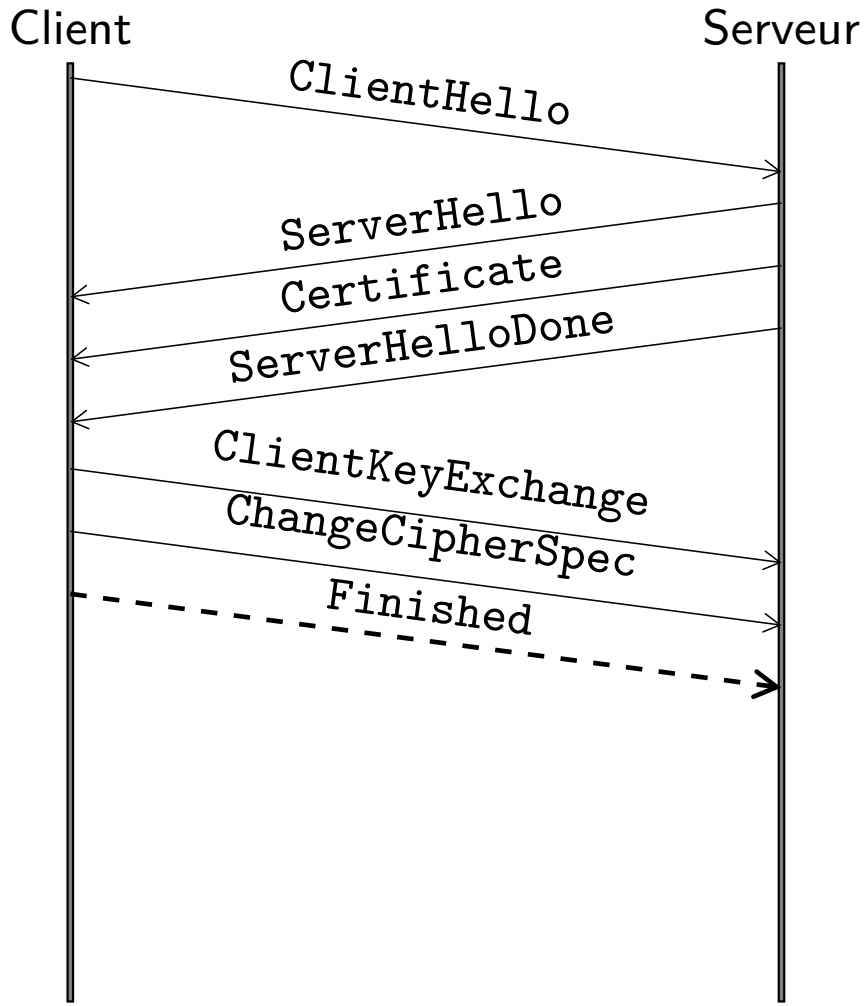
Fonctionnement du protocole



Hypothèses

- Version : SSLv3 - TLS 1.2
- Algorithme d'échange de clé : chiffrement RSA

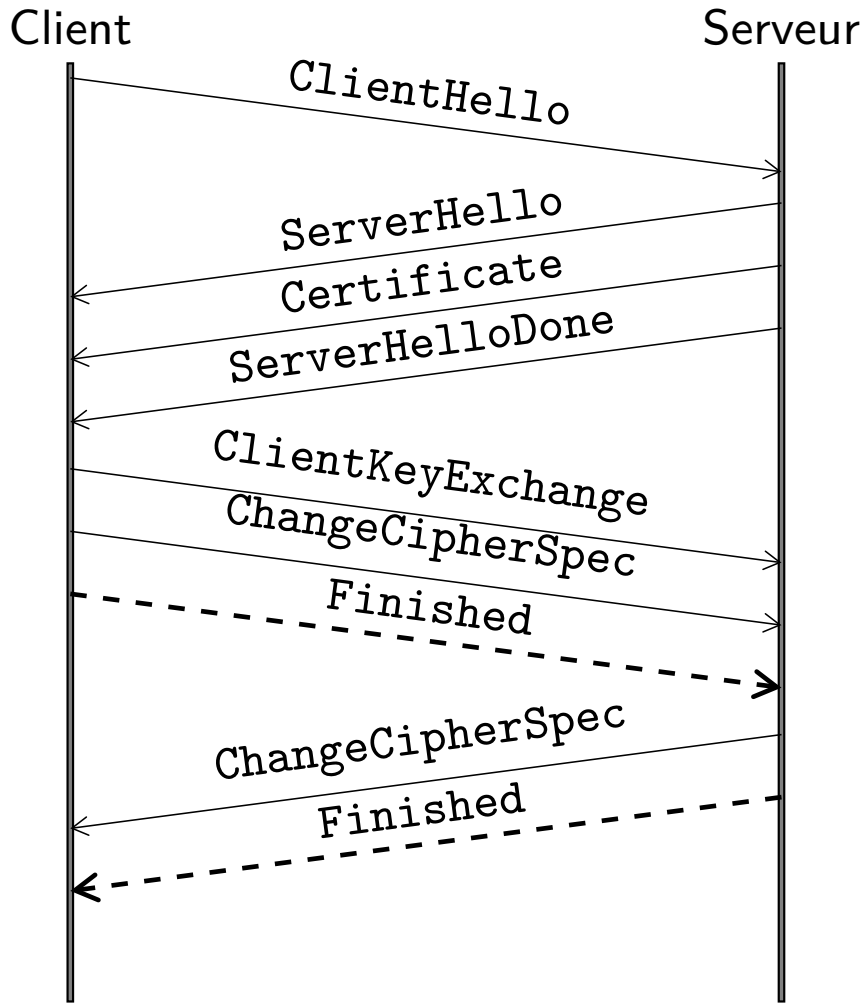
Fonctionnement du protocole



Hypothèses

- Version : SSLv3 - TLS 1.2
- Algorithme d'échange de clé : chiffrement RSA

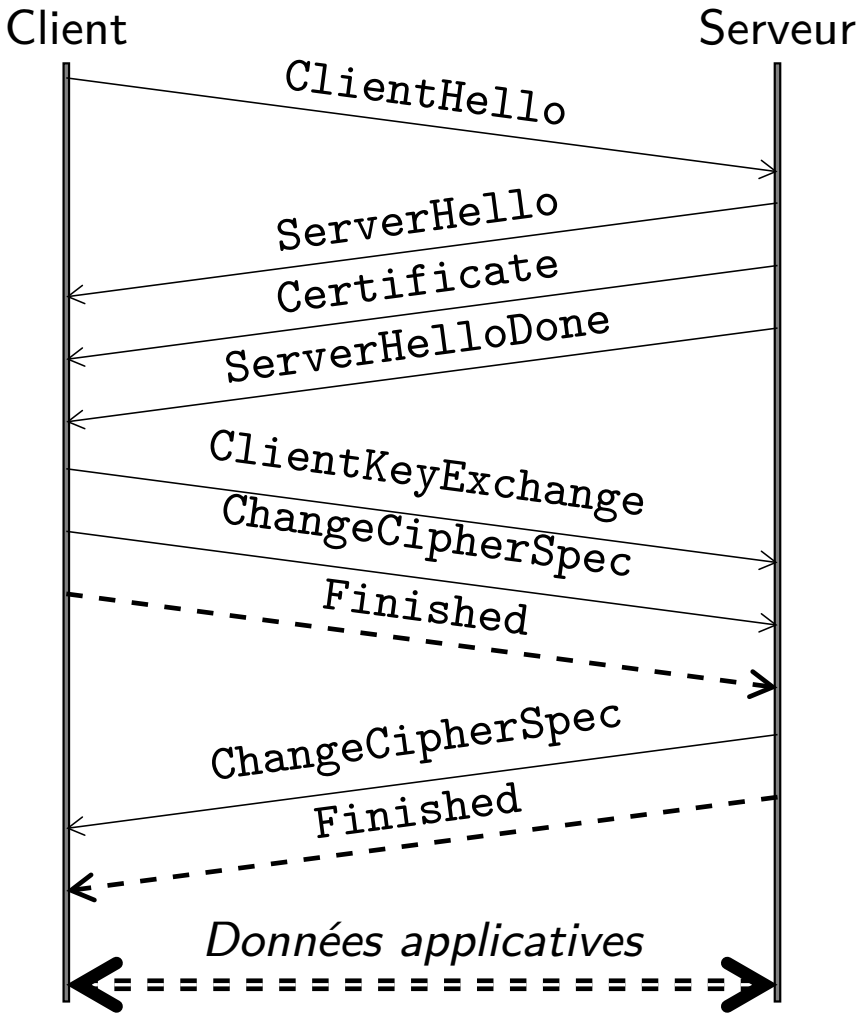
Fonctionnement du protocole



Hypothèses

- Version : SSLv3 - TLS 1.2
- Algorithme d'échange de clé : chiffrement RSA

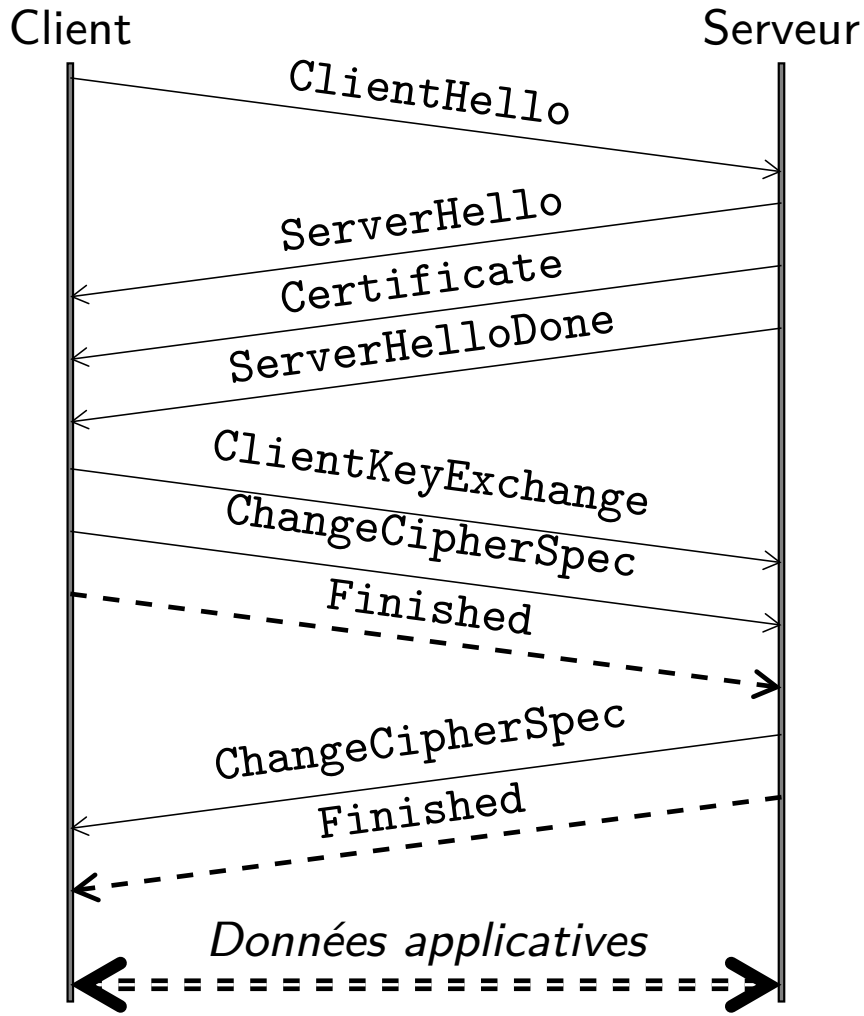
Fonctionnement du protocole



Hypothèses

- Version : SSLv3 - TLS 1.2
- Algorithme d'échange de clé : chiffrement RSA
- Ni erreur ni incompatibilité

Fonctionnement du protocole



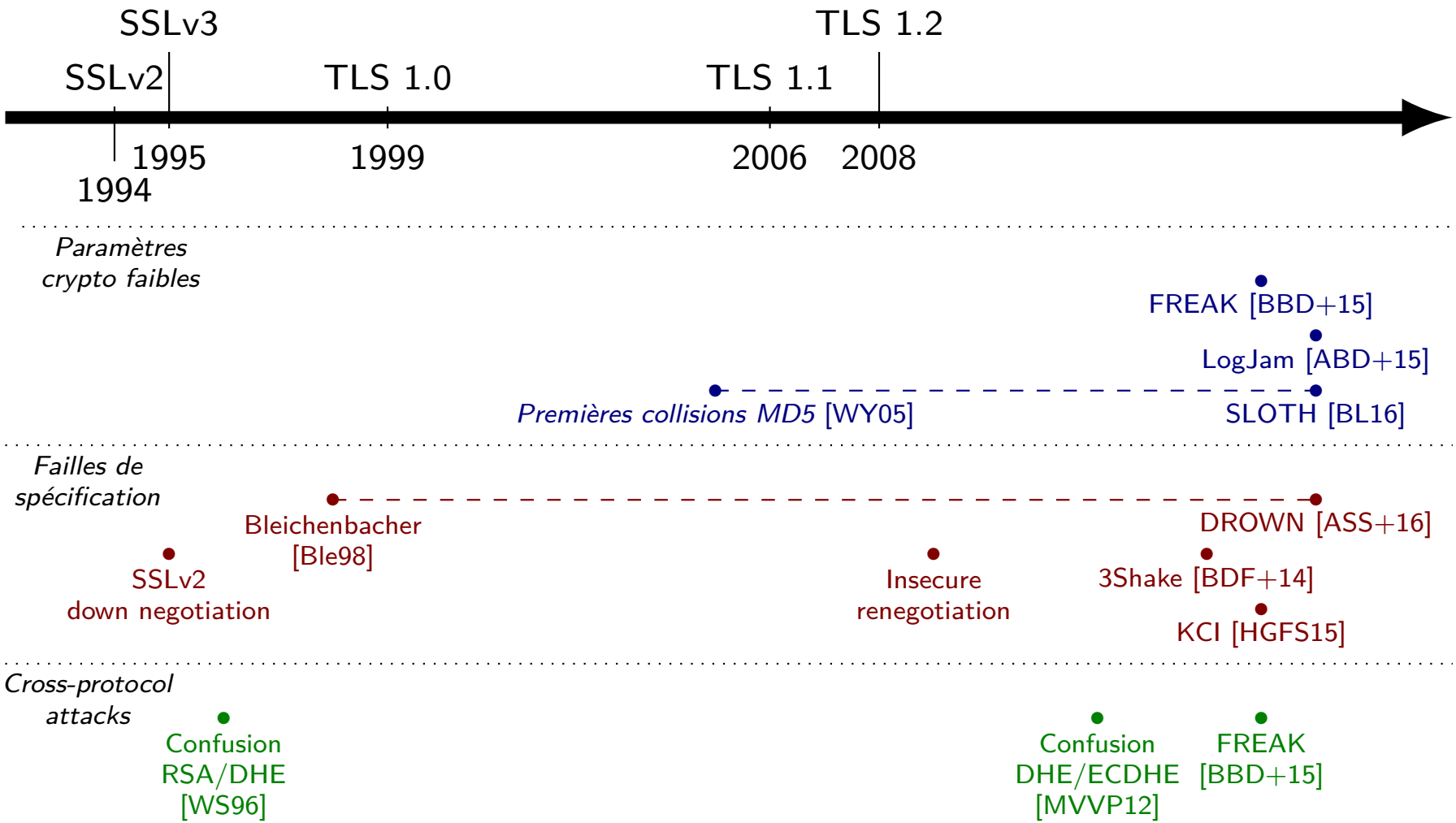
Hypothèses

- Version : SSLv3 - TLS 1.2
- Algorithme d'échange de clé : chiffrement RSA
- Ni erreur ni incompatibilité

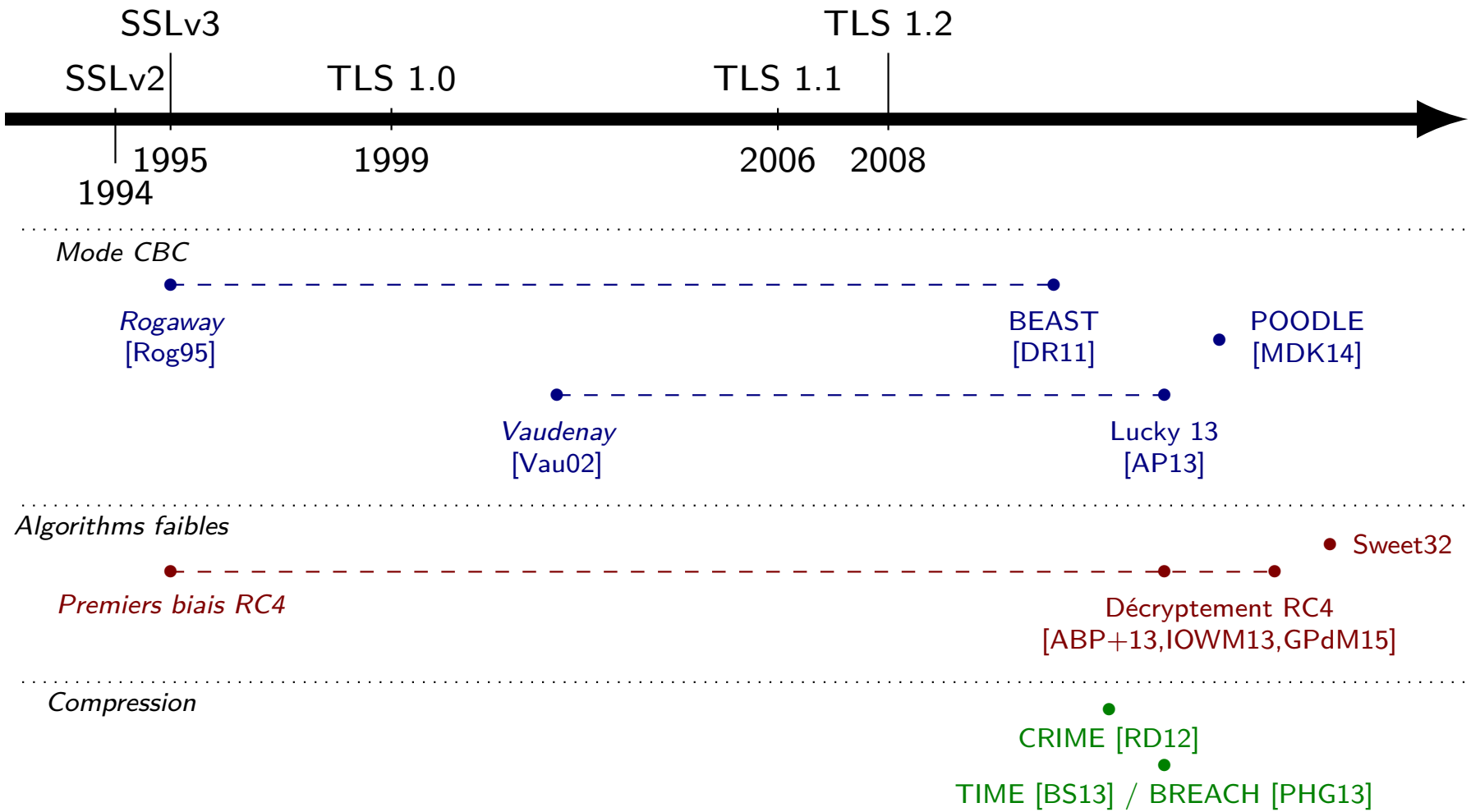
Il existe des variantes

- échange de clé DHE
- reprise de session
- échange de clé symétrique
- ...

Failles du *Handshake Protocol*



Attaques contre *Record Protocol*



Problèmes de sécurité et solutions

Pas de *forward security* systématique

Algorithmes symétriques faibles

Fonctionnalités dangereuses/complexes

- compression
- renégociation

Problèmes de sécurité et solutions

Pas de *forward security* systématique

- utilisation de (EC)DHE...
- ... sur des groupes nommés

Algorithmes symétriques faibles

- ~~RC4~~, ~~Mac-then-CBC~~
- ~~MD5~~, ~~SHA-1~~
- il faut garder uniquement des modes AEAD

Fonctionnalités dangereuses/complexes

- ~~compression~~
- ~~renégociation~~
- il faut les supprimer

Problèmes de sécurité et solutions

Pas de *forward security* systématique

- utilisation de (EC)DHE...
- ... sur des groupes nommés

Algorithmes symétriques faibles

- ~~RC4~~, ~~Mac-then-CBC~~
- ~~MD5~~, ~~SHA-1~~
- il faut garder uniquement des modes AEAD

Fonctionnalités dangereuses/complexes

- ~~compression~~
- ~~renégociation~~
- il faut les supprimer

Une pile TLS 1.2 *bien configurée* peut déjà presque faire l'affaire

Autres propriétés

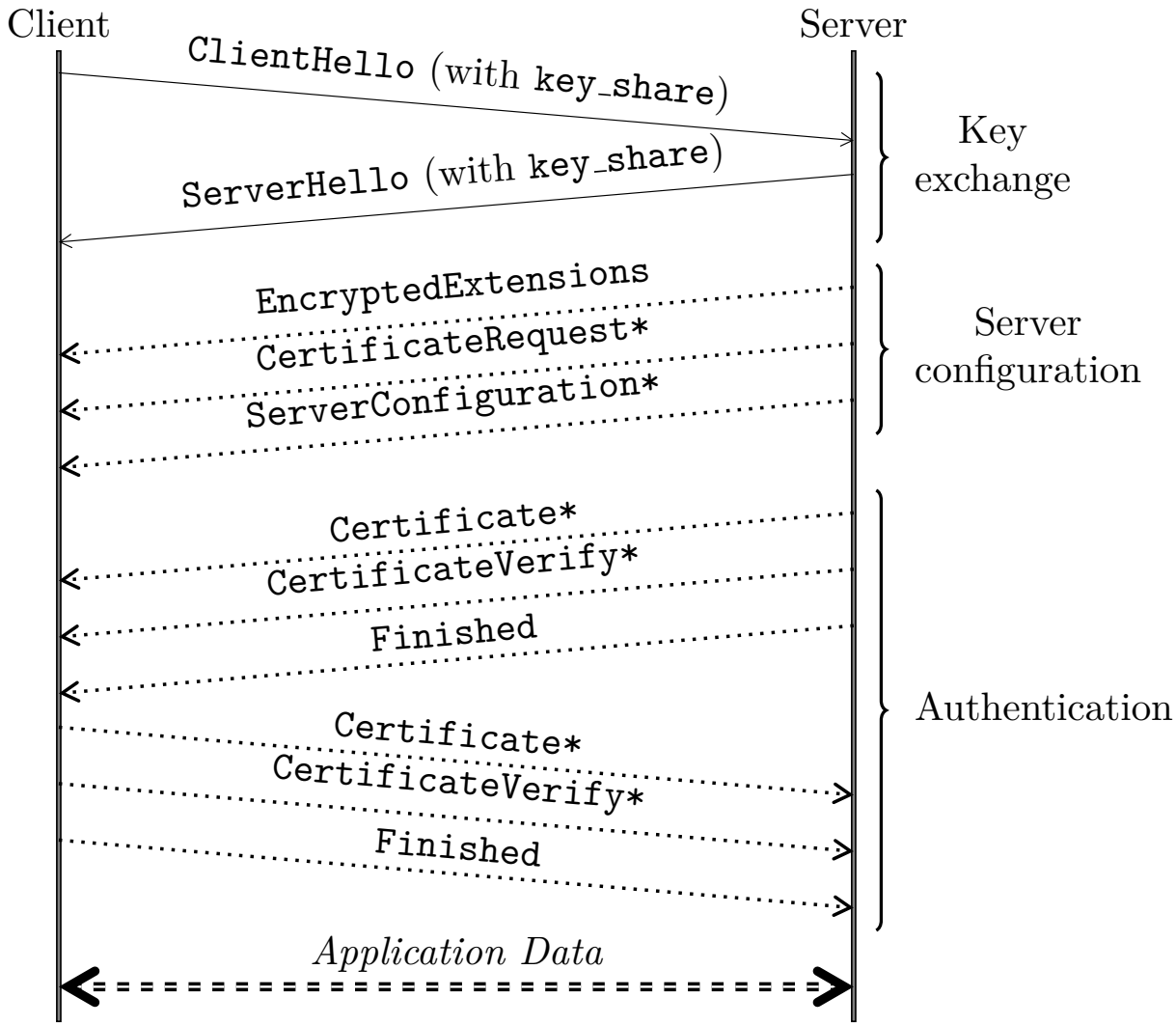
TLS est lent

- mode 1 RTT (échange DHE non authentifié dès les premiers messages)
- *TCP Fast Open*
- reprise de session
- mode 0 RTT

Trop d'informations en clair

- certificats client/serveur
- extensions
- *Server Name Indication*
- *Encrypt all the things !*

TLS 1.3 : flot de messages standard



TLS 1.3 : la solution à tous les problèmes ?

Hypothèses pour garantir les objectifs de sécurité

- utiliser des algorithmes et des clés décentes dans les certificats
- refuser des paramètres faibles dans les certificats
- question plus générale de la confiance dans l'IGC

TLS 1.3 : la solution à tous les problèmes ?

Hypothèses pour garantir les objectifs de sécurité

- utiliser des algorithmes et des clés décentes dans les certificats
- refuser des paramètres faibles dans les certificats
- question plus générale de la confiance dans l'IGC

Hypothèses si on doit vivre avec des versions antérieures

- TLS 1.2 minimum
- échange de clé ECDHE
- mode AEAD

TLS 1.3 : la solution à tous les problèmes ?

Hypothèses pour garantir les objectifs de sécurité

- utiliser des algorithmes et des clés décentes dans les certificats
- refuser des paramètres faibles dans les certificats
- question plus générale de la confiance dans l'IGC

Hypothèses si on doit vivre avec des versions antérieures

- TLS 1.2 minimum
- échange de clé ECDHE
- mode AEAD

Quid de l'implémentation ?

Des objectifs de sécurité contradictoires

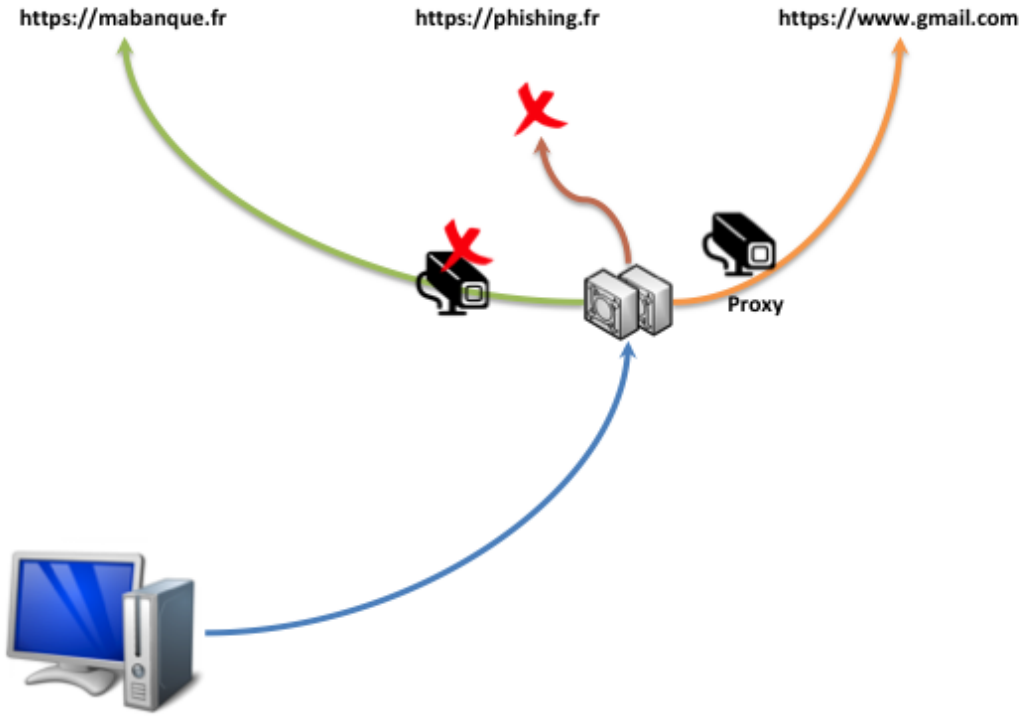
Dans certains systèmes d'information

- flux protégés avec TLS...
- ... mais besoin d'inspecter les flux clairs
  - détection de contenu malveillant
  - prévention des fuites d'information (DLP)
- ... avec une exception pour les échanges liés à la vie privée
  - comptes bancaires

Caractérisation des connexions HTTPS nécessaires

- connexions à ne pas surveiller
- connexions à bloquer
- connexions à inspecter

Fonctionnement classique des outils



Avec TLS $\leq$ 1.2

- vérification du certificat par un équipement en coupure
- politique appliquée en fonction de l'identité observée

Limitations de l'architecture

Fragilité de l'aiguillage basé sur le certificat

- prise en compte des *SubjectAltName*s ?
- quid d'une renégociation ?
- méthode de la double connexion...

Limitations de l'architecture

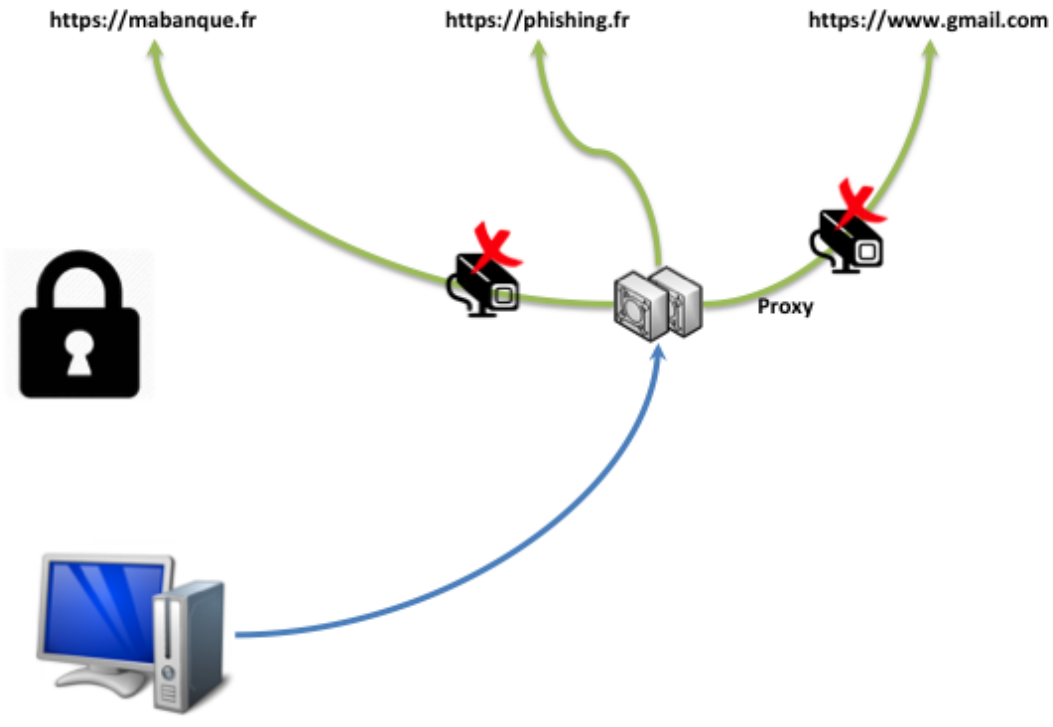
Fragilité de l'aiguillage basé sur le certificat

- prise en compte des *SubjectAltName*s ?
- quid d'une renégociation ?
- méthode de la double connexion...

Restrictions imposées par la pile TLS de l'équipement

- fonctionnalités non supportées menant à des coupures
  - extensions
  - certificats clients / U2F
- baisse du niveau de sécurité possible (inhérent au modèle avec rupture de TLS)
  - suites cryptographiques supportées
  - mauvaise vérification du certificat

Fonctionnement classique des outils



Incompatibilité avec TLS ≤ 1.3

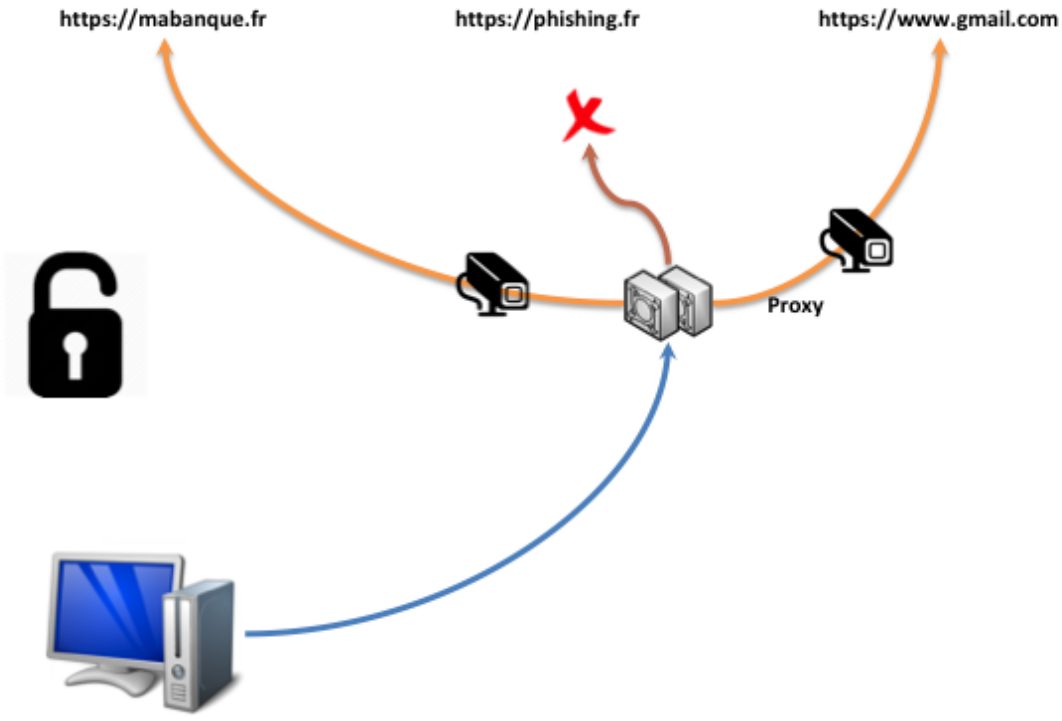
- le certificat n'est plus en clair
- plus d'aiguillage possible sans se placer en coupure

Inspection des flux et TLS 1.3 (1/3)

Choix 1 : ne plus inspecter les flux

- \+ simple !
- − ne répond plus au cahier des charges initial
- ▶ pas forcément toujours stupide (que dit l'analyse de risques ?)

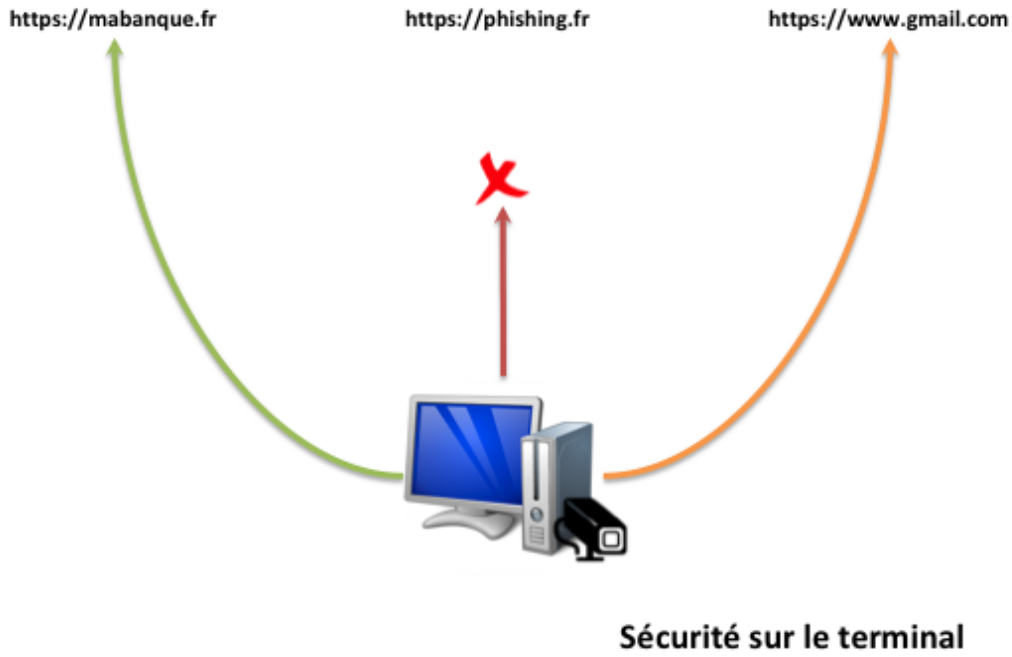
Inspection des flux et TLS 1.3 (2/3)



Choix 2 : décapsuler tous les flux

+ aiguillage de nouveau possible (et robuste)
− ressources nécessaires plus importantes
− fermer les yeux sur les communications privées est plus difficile

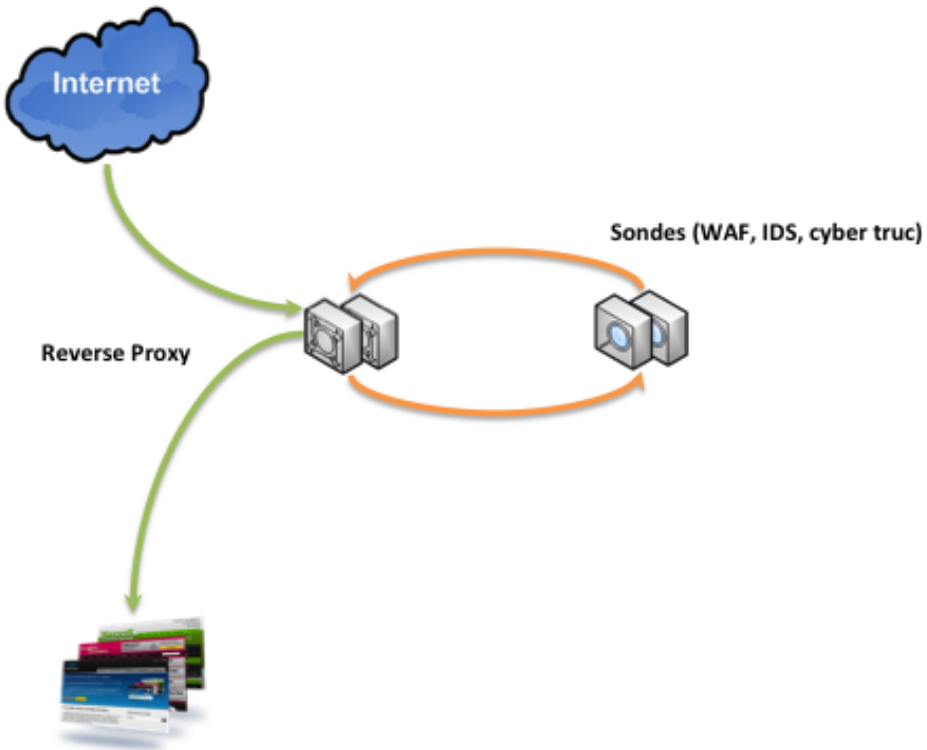
Inspection des flux et TLS 1.3 (3/3)



Choix 3 : déporter l'inspection sur les équipements terminaux

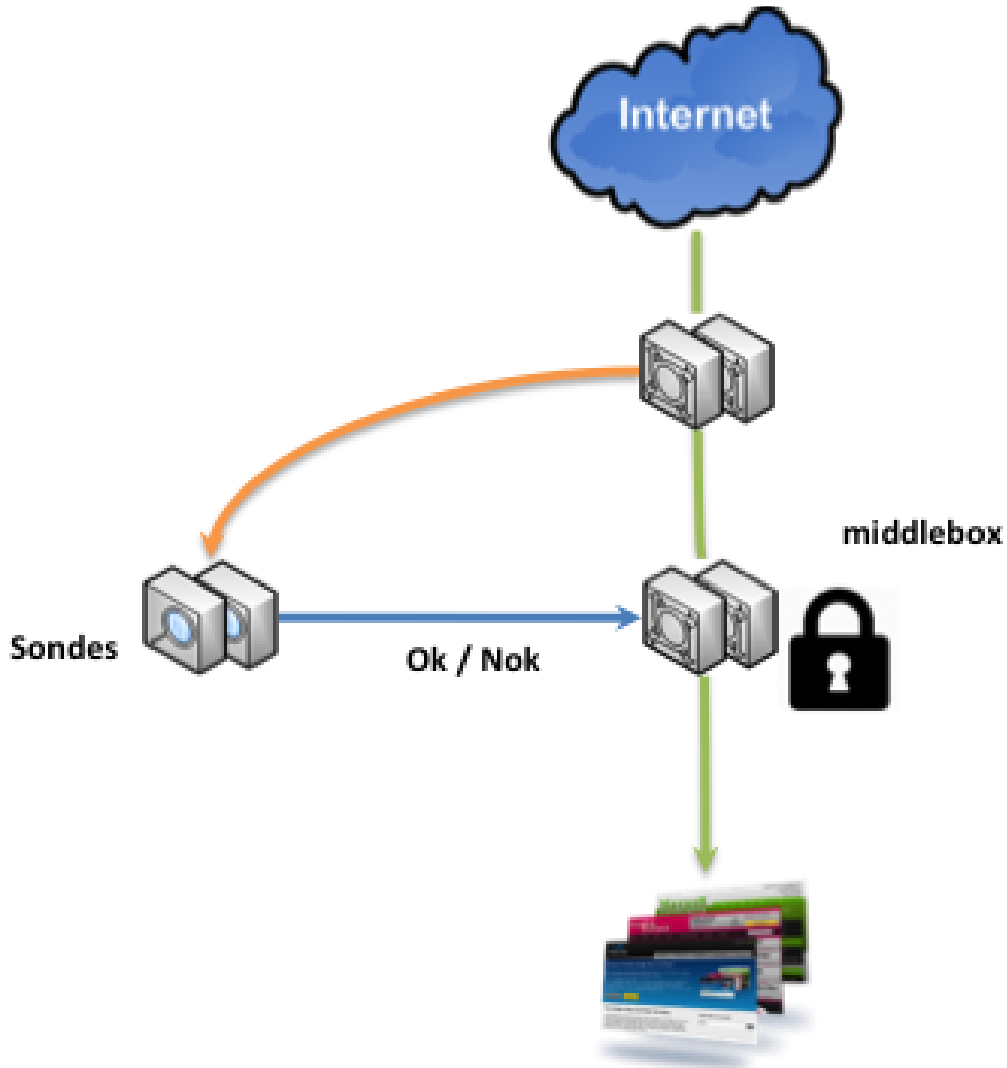
- \+ flexibilité et répartition de la charge
- − journalisation et centralisation
- − quelles garanties en cas de compromission du poste ?

Étude de cas : sécurité des services hébergés

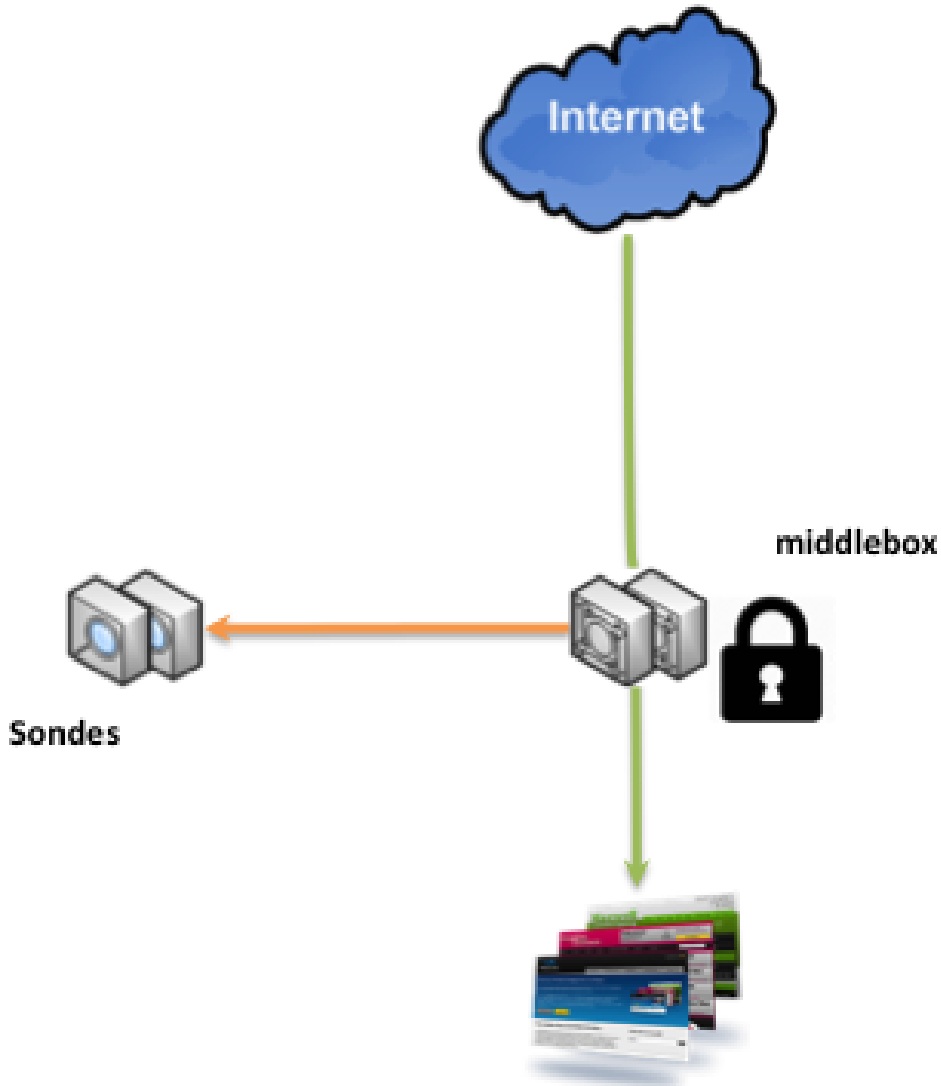


- *reverse proxy* pour décapsuler
- attention aux flux en clair
- compatible avec TLS 1.*
- ... sauf pour certains aspects
  - certificats clients
  - U2F (lien entre TLS et le flux applicatif)

Architectures suspectes (inspection sans coupure du flux)



Architectures suspectes (inspection sans coupure du flux)



Architectures suspectes (inspection sans coupure du flux)

Pour fonctionner, ces équipements imposent des contraintes sur la configuration du serveur

- Version TLS 1.2 max
- Chiffrement RSA imposé
- Diffie-Hellman *éphémère* statique

Fragilité intrinsèque

- absence de *forward secrecy*
- incompatibilité avec les versions et fonctionnalités récentes

Mieux vaut conserver une architecture saine et robuste...

TLS 1.3 : un nouvel espoir

Parmi les failles présentées, nombreuses sont celles issues de la conception

- la crypto obsolète, retirée dans TLS 1.3 : PKCS#1 v1.5, RC4, CBC...
- certains problèmes de l'automate : la négociation a été repensée

Cependant, TLS 1.3 ne résout pas

- les défauts dans les méthodes de développement
- les soucis de compatibilité : les versions précédentes de TLS sont encore là pour un certain temps
- la complexité du standard
  - X.509
  - 0-RTT
  - l'authentification tardive du client
  - des astuces sordides pour contrer les *middle boxes*

Une remise en cause nécessaire de certaines architectures

Certains usages et certains produits ne fonctionnent plus avec TLS 1.3

- pas ou peu d'outils disponibles et compatibles
- remise en cause du fonctionnement actuel
- tentation d'utiliser des solutions sordides (DH statique, TLS 1.2 forcé)

Une remise en cause nécessaire de certaines architectures

Certains usages et certains produits ne fonctionnent plus avec TLS 1.3

- − pas ou peu d'outils disponibles et compatibles
- − remise en cause du fonctionnement actuel
- − tentation d'utiliser des solutions sordides (DH statique, TLS 1.2 forcé)
- \+ niveau de sécurité des communications
- \+ remise en cause du fonctionnement actuel pour des solutions plus robustes et plus élégantes ?

Une remise en cause nécessaire de certaines architectures

Certains usages et certains produits ne fonctionnent plus avec TLS 1.3

- − pas ou peu d'outils disponibles et compatibles
- − remise en cause du fonctionnement actuel
- − tentation d'utiliser des solutions sordides (DH statique, TLS 1.2 forcé)
- \+ niveau de sécurité des communications
- \+ remise en cause du fonctionnement actuel pour des solutions plus robustes et plus élégantes ?

Un nouvel équilibre à trouver entre

- la protection des flux
- les capacités d'inspection

Questions ?

Merci pour votre attention