Regard critique sur TLS

Olivier Levillain

ANSSI/CyberEdu

Journée CyberEdu à Nantes
19 avril 2018

Table des matières

Table des matières

Une question d'entretien classique

Un certificat électronique...

- ... est un fichier de données
- ... est un programme exécutable
- ... contient une clé privée
- ... peut être chiffré avec RSA
- ... garantit l'identité de son porteur

Une question d'entretien classique

Un certificat électronique...

- ... est un fichier de données
- ... est un programme exécutable
- ... contient une clé privée
- ... peut être chiffré avec RSA
- ... garantit l'identité de son porteur

Une entrée en matière intéressante pour en arriver à la définition d'un certificat

Une question d'entretien classique

Un certificat électronique...

- ... est un fichier de données
- ... est un programme exécutable
- ... contient une clé privée
- ... peut être chiffré avec RSA
- ... garantit l'identité de son porteur

Une entrée en matière intéressante pour en arriver à la définition d'un certificat

Les réponses sont souvent étonnantes... même de la part de personnes ayant mis en place des IGC

De la rigueur dans les termes

Un certificat est donc une association entre une **identité** et une **clé publique**, garantie par la **signature** une autorité

De la rigueur dans les termes

Un certificat est donc une association entre une **identité** et une **clé publique**, garantie par la **signature** une autorité

Un certificat (électronique) est donc un fichier contenant

- une identité
- une clé publique
- une signature d'une autorité liant les deux éléments précédents
- quelques autres éléments détaillés plus loin

De la rigueur dans les termes

Un certificat est donc une association entre une **identité** et une **clé publique**, garantie par la **signature** une autorité

Un certificat (électronique) est donc un fichier contenant

- une identité
- une clé publique
- une signature d'une autorité liant les deux éléments précédents
- quelques autres éléments détaillés plus loin

En dehors du cas particulier des certificats auto-signés, un certificat met donc en jeu **deux** biclés

Autres éléments d'un certificat

Encadrement de l'usage de la clé publique

- dates de validité
- description de l'usage
  - chiffrement, signature, etc.
  - autorité de certification, IPsec, TLS, etc.
- précisions de la portée
  - noms alternatifs
  - profondeur de la chaîne
  - contraintes sur les noms
  - etc.

Autres éléments d'un certificat

Encadrement de l'usage de la clé publique

- dates de validité
- description de l'usage
  - chiffrement, signature, etc.
  - autorité de certification, IPsec, TLS, etc.
- précisions de la portée
  - noms alternatifs
  - profondeur de la chaîne
  - contraintes sur les noms
  - etc.

Informations liées à la révocation

- adresse des listes de révocation
- adresse des serveurs OCSP

Autres éléments d'un certificat

Encadrement de l'usage de la clé publique

- dates de validité
- description de l'usage
  - chiffrement, signature, etc.
  - autorité de certification, IPsec, TLS, etc.
- précisions de la portée
  - noms alternatifs
  - profondeur de la chaîne
  - contraintes sur les noms
  - etc.

Informations liées à la révocation

- adresse des listes de révocation
- adresse des serveurs OCSP

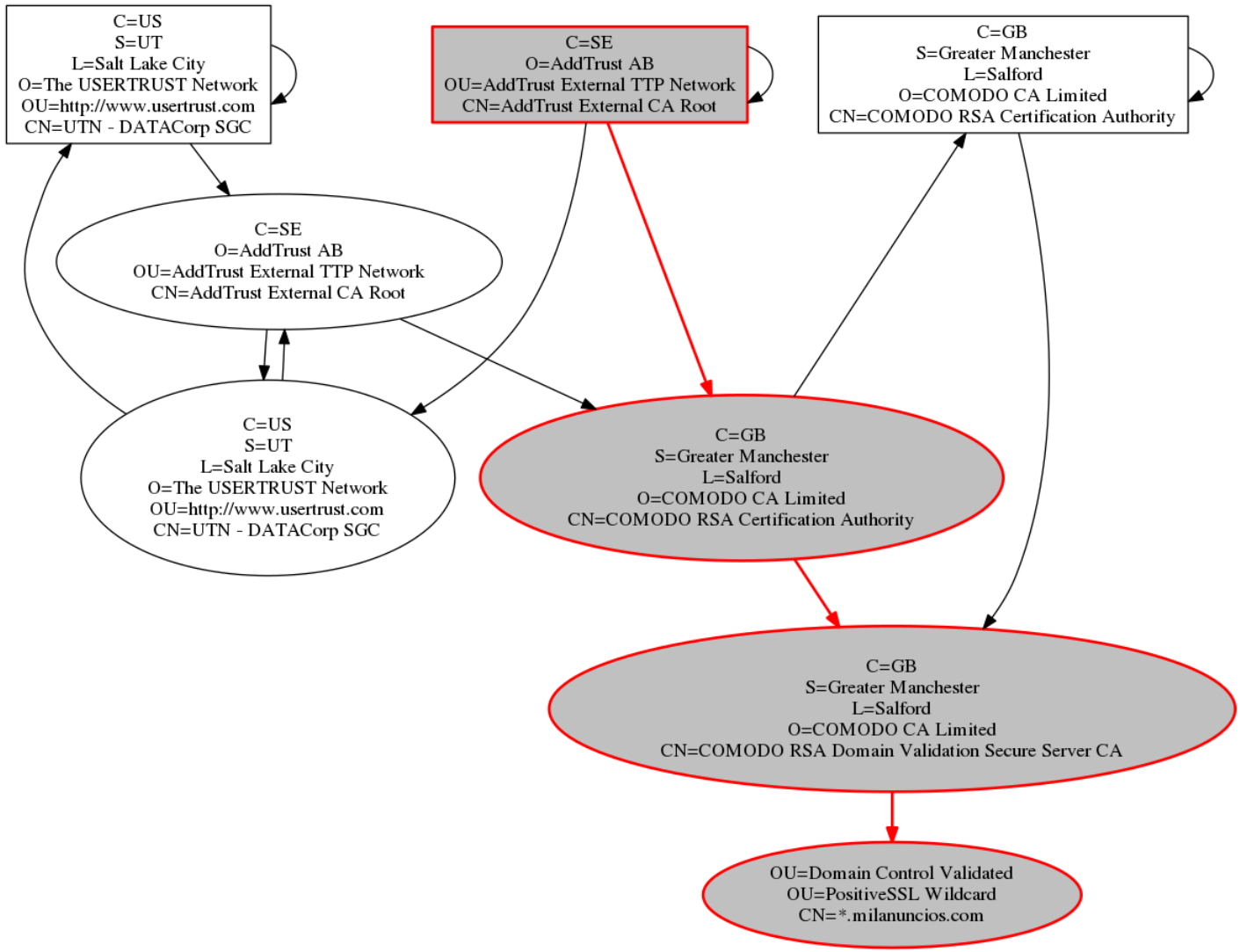
Informations techniques

- émetteur
- numéro de série
- identifiant de la clé

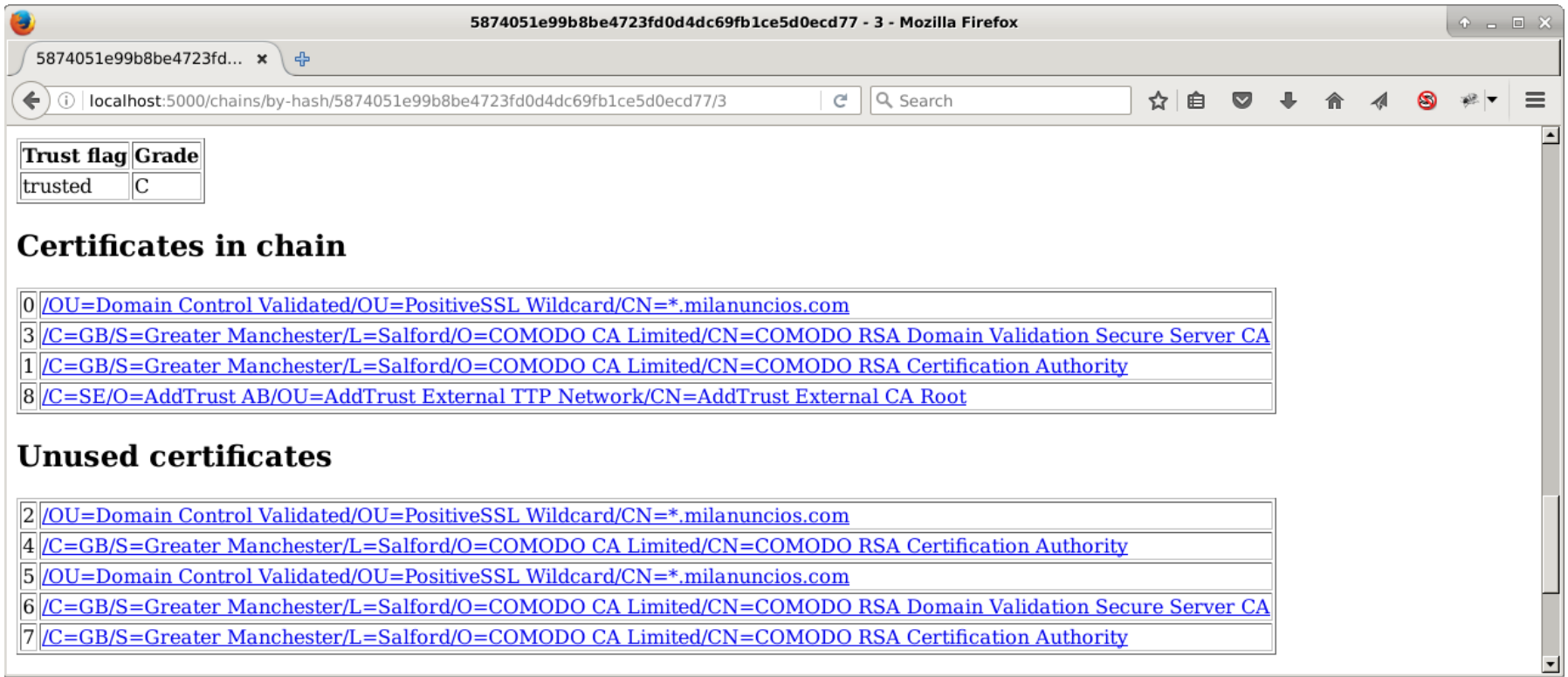
Qu'est-ce qu'une IGC ?

- Chaque certificat concerne deux biclés
- Le long de la chaîne, la clé publique du certificat *du dessus* correspond à la clé privée qui a servi à signer le certificat *du dessous*
- En bas de la chaîne, le certificat terminal
- Au milieu, des éventuels certificats d'autorités intermédiaires pour lesquels l'usage de la clé publique est de signer des certificats
- En haut, un auto-signé (autorité racine)

Exemple de chaînes de certification TLS (1/2)



Exemple de chaînes de certification TLS (2/2)



Qu'est-ce qu'un certificat auto-signé

Un certificat auto-signé est un certificat où la clé privée utilisée pour la signature est le pendant de la clé publique contenue dans le certificat

À quoi cela sert-il ?

Qu'est-ce qu'un certificat auto-signé

Un certificat auto-signé est un certificat où la clé privée utilisée pour la signature est le pendant de la clé publique contenue dans le certificat

À quoi cela sert-il ?

- à distribuer de manière simple une clé publique d'autorité, accompagnée de ses attributs

Qu'est-ce qu'un certificat auto-signé

Un certificat auto-signé est un certificat où la clé privée utilisée pour la signature est le pendant de la clé publique contenue dans le certificat

À quoi cela sert-il ?

- à distribuer de manière simple une clé publique d'autorité, accompagnée de ses attributs
- à prouver que l'émetteur possède la clé privée associée à la clé publique annoncée (discutable)

Qu'est-ce qu'un certificat auto-signé

Un certificat auto-signé est un certificat où la clé privée utilisée pour la signature est le pendant de la clé publique contenue dans le certificat

À quoi cela sert-il ?

- à distribuer de manière simple une clé publique d'autorité, accompagnée de ses attributs
- à prouver que l'émetteur possède la clé privée associée à la clé publique annoncée (discutable)
- ~~à amorcer la confiance dans l'infrastructure~~

Gestion de la confiance

Dans une infrastructure à clé publique classique

- il existe des autorités de confiance à la racine des chemins de certification
- chaque maillon du chemin correspond à une signature valide
- il faut faire confiance par délégation aux autorités intermédiaires

Certains éléments sont techniques

- algorithmes cryptographiques et tailles de clés
- contraintes sur l'usage
- protection adéquate des clés (confidentialité et intégrité)
- qualité de l'implémentation (BERserk en novembre 2014)

Les IGC ne sont pas magiques

Attention cependant, les IGC ne font que réduire et déplacer le problème de la distribution des clés !

Exemples concrets de la diffusion des autorités racines

- CD d'installation de distribution
- mises à jour des OS et des navigateurs

Les IGC ne sont pas magiques

Attention cependant, les IGC ne font que réduire et déplacer le problème de la distribution des clés !

Exemples concrets de la diffusion des autorités racines

- CD d'installation de distribution
- mises à jour des OS et des navigateurs
- mais là encore, on ne fait que déplacer le problème !

Table des matières

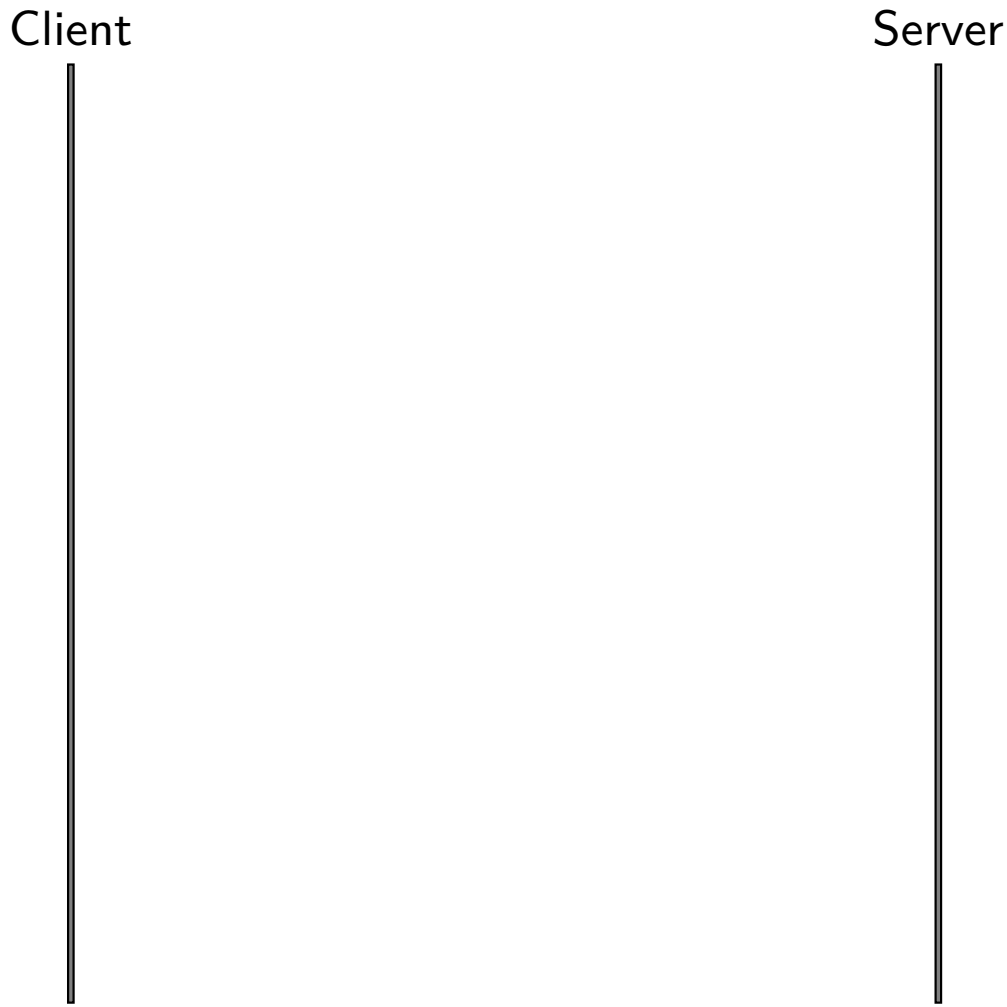
SSL/TLS : un pilier de la sécurité d'Internet

- Le schéma `https://` inventé par Netscape en 1995
  - début du commerce en ligne
- Omniprésence de SSL/TLS aujourd'hui
  - HTTPS, bien au-delà du commerce en ligne
  - Une méthode générique pour sécuriser d'autres protocoles (SMTP, IMAP, LDAP...)
  - VPN SSL
  - EAP TLS

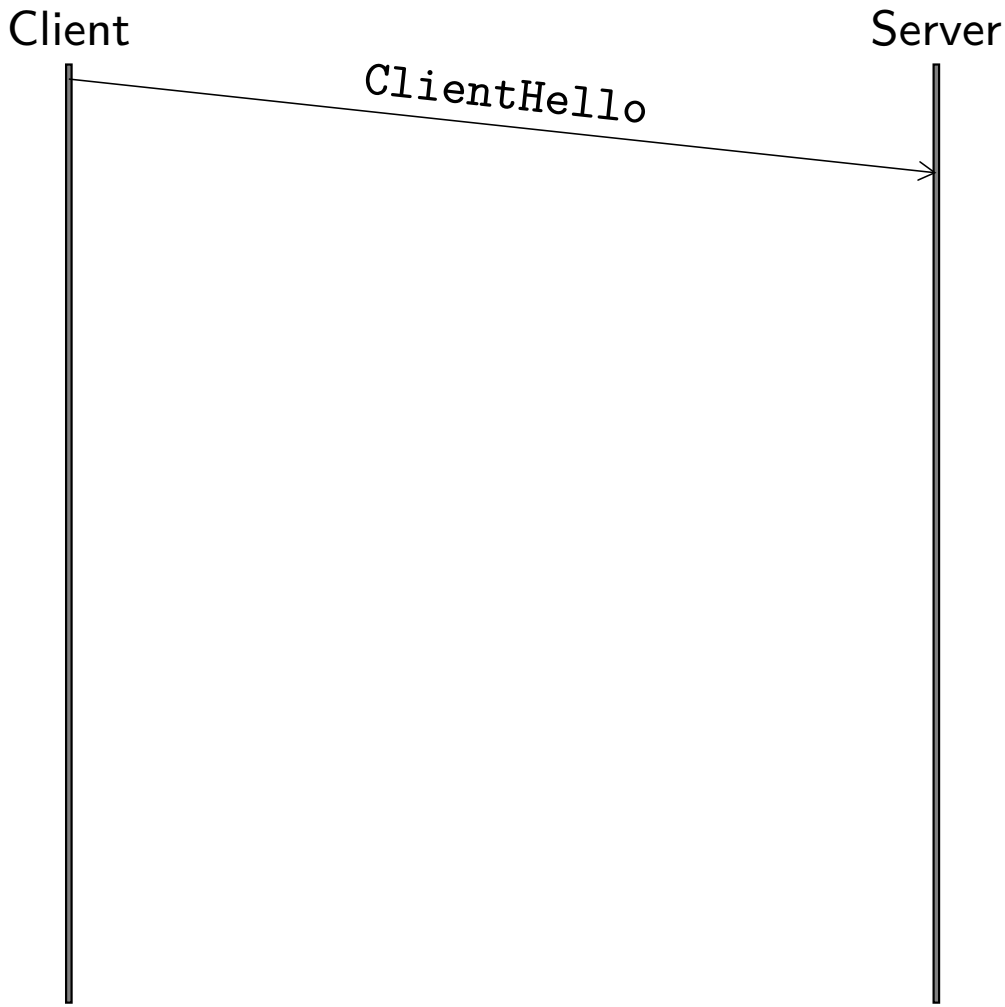
SSL/TLS : un pilier de la sécurité d'Internet

- Le schéma `https://` inventé par Netscape en 1995
  - début du commerce en ligne
- Omniprésence de SSL/TLS aujourd'hui
  - HTTPS, bien au-delà du commerce en ligne
  - Une méthode générique pour sécuriser d'autres protocoles (SMTP, IMAP, LDAP...)
  - VPN SSL
  - EAP TLS
- SSL (*Secure Sockets Layer*) ou TLS (*Transport Layer Security*) ?
  - SSLv2 (1995) et v3 (1996) conçu par Netscape
  - TLS 1.0 (2001) ou SSLv3.1, maintenu par l'IETF
  - De nouvelles révisions depuis : 1.1 (2006), 1.2 (2008) et 1.3 (2016 ?)

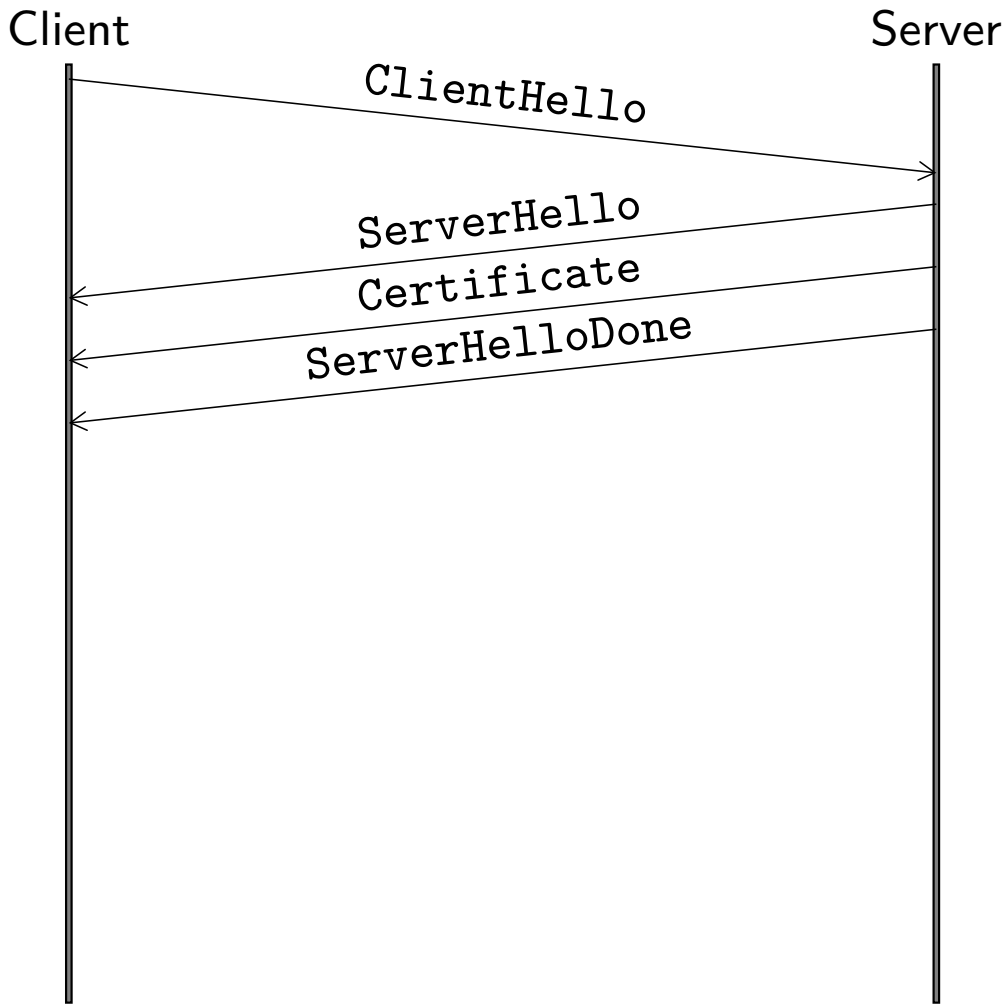
Fonctionnement du protocole



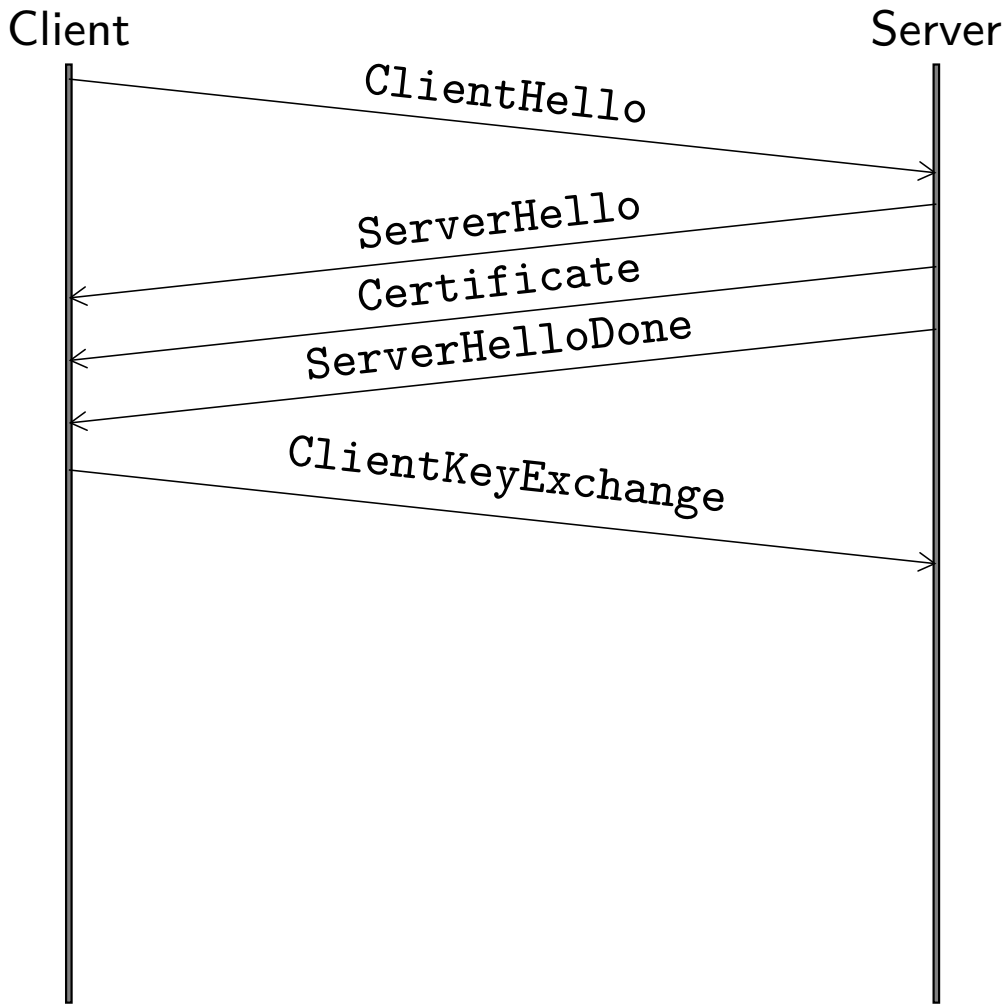
Fonctionnement du protocole



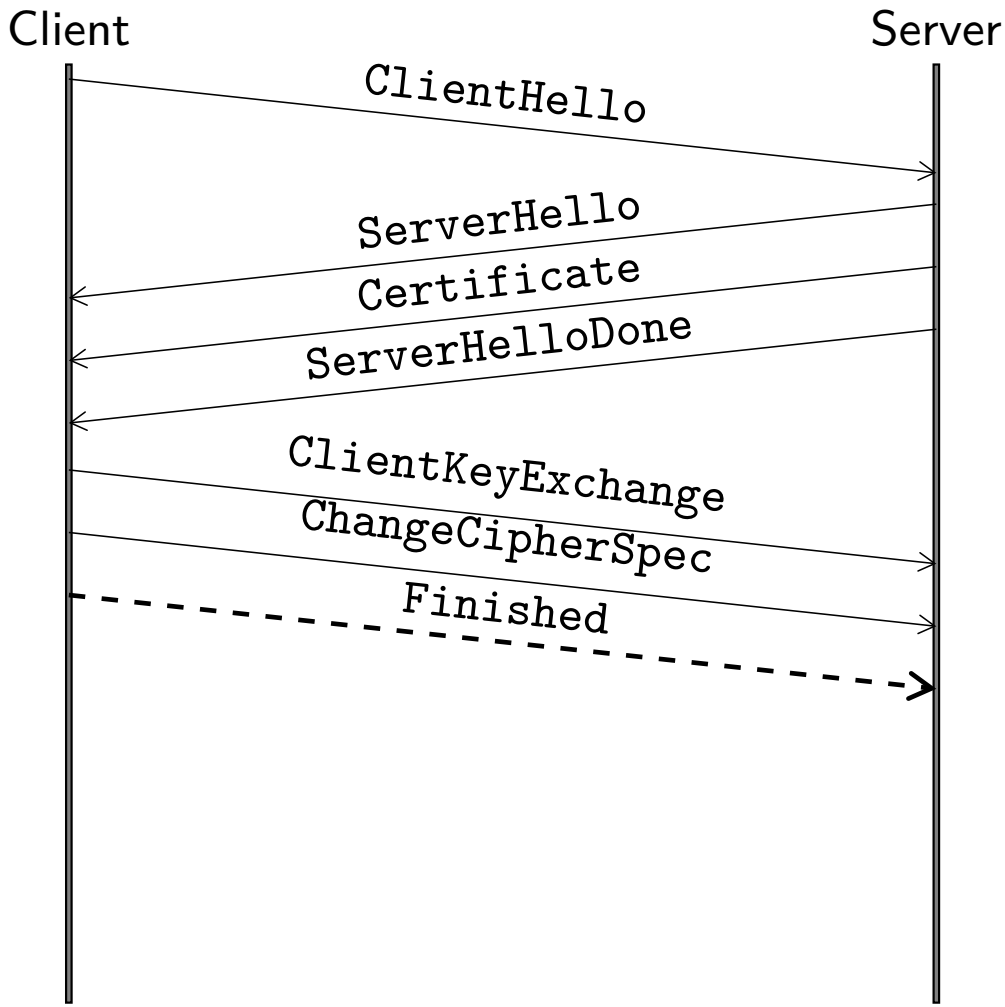
Fonctionnement du protocole



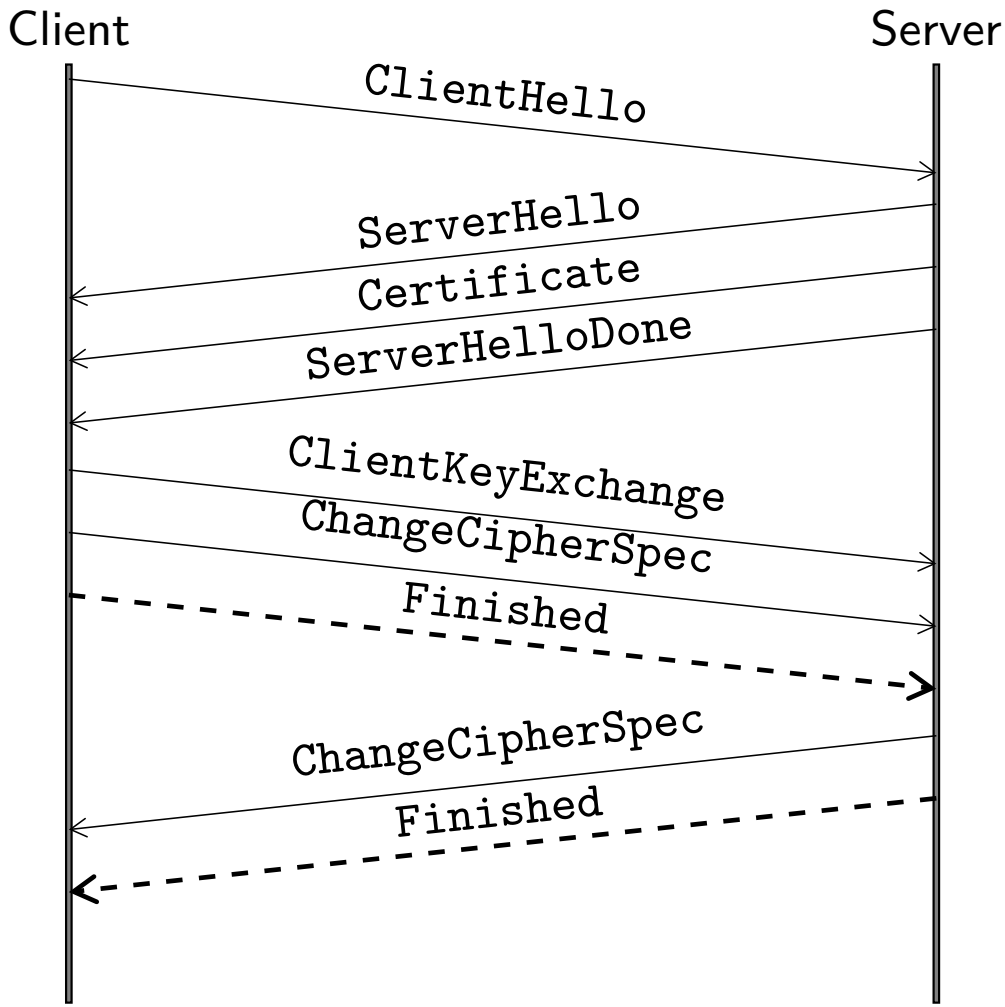
Fonctionnement du protocole



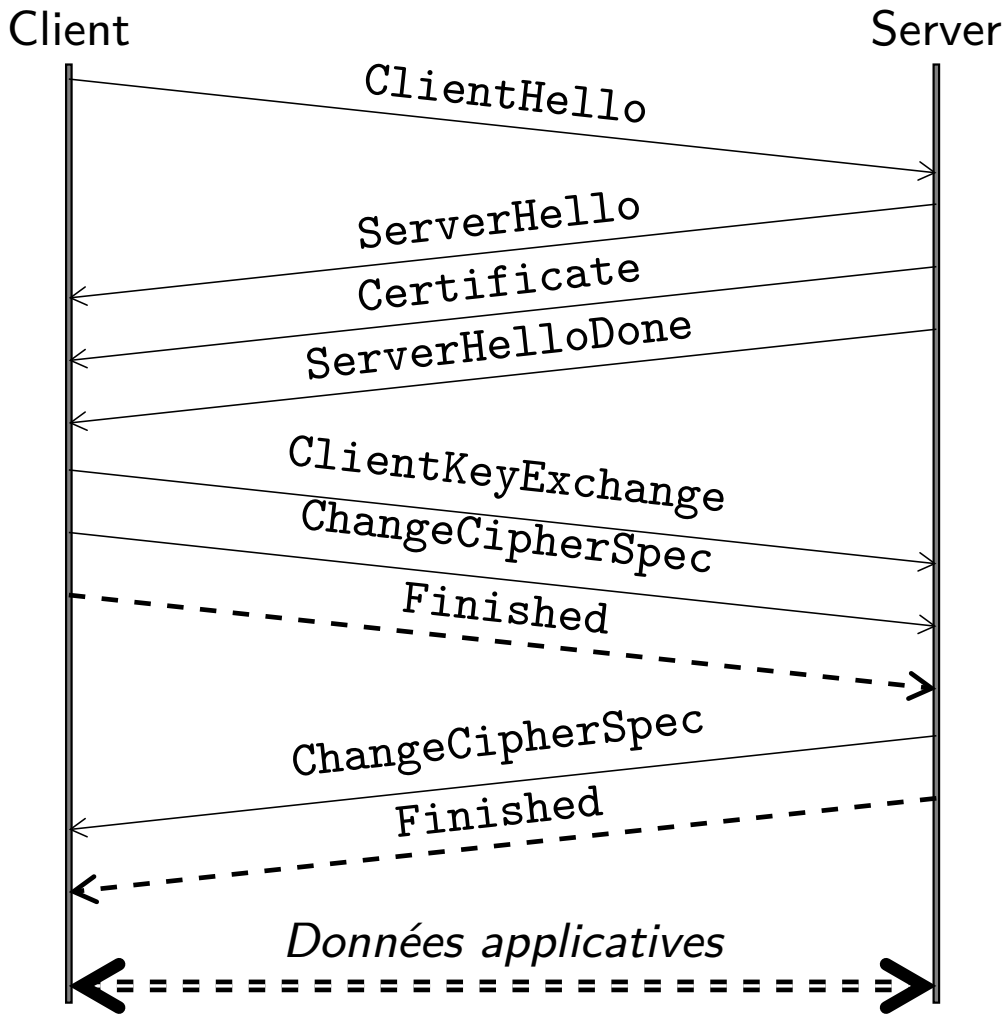
Fonctionnement du protocole



Fonctionnement du protocole



Fonctionnement du protocole



Quelques chiffres sur SSL/TLS

- Plus de 50 RFC
- 5 versions du protocole pour le moment
- Plus de 300 suites cryptographiques
- Plus de 20 extensions
- Quelques fonctionnalités *intéressantes*
  - compression
  - renégociation
  - reprise de session (2 méthodes)
- Une douzaine d'implémentations bien connues
- Et combien de piles maison ?

Les piles SSL/TLS maison (1/3)

Que répond un serveur si vous lui proposez les suites crypto `AES128-SHA` et `ECDH-ECDSA-AES128-SHA` ?

Les piles SSL/TLS maison (1/3)

Que répond un serveur si vous lui proposez les suites crypto `AES128-SHA` et `ECDH-ECDSA-AES128-SHA` ?

A `AES128-SHA`

Les piles SSL/TLS maison (1/3)

Que répond un serveur si vous lui proposez les suites crypto `AES128-SHA` et `ECDH-ECDSA-AES128-SHA` ?

A `AES128-SHA`

B `ECDH-ECDSA-AES128-SHA`

Les piles SSL/TLS maison (1/3)

Que répond un serveur si vous lui proposez les suites crypto `AES128-SHA` et `ECDH-ECDSA-AES128-SHA` ?

A `AES128-SHA`

B `ECDH-ECDSA-AES128-SHA`

C une alerte

Les piles SSL/TLS maison (1/3)

Que répond un serveur si vous lui proposez les suites crypto `AES128-SHA` et `ECDH-ECDSA-AES128-SHA` ?

A `AES128-SHA`

B `ECDH-ECDSA-AES128-SHA`

C une alerte

D la réponse D (`RC4_MD5`)

Les piles SSL/TLS maison (1/3)

Que répond un serveur si vous lui proposez les suites crypto `AES128-SHA` et `ECDH-ECDSA-AES128-SHA` ?

A `AES128-SHA` (`0x002f`)

B `ECDH-ECDSA-AES128-SHA` (`0xc005`)

C une alerte

D la réponse D (`RC4_MD5`) (`0x0005`)

Le pire, c'est qu'on peut l'expliquer :

- une suite cryptographique est un entier sur 16 bits
- pendant longtemps, les seules valeurs utilisées étaient `00 XX`
- du coup, pourquoi considérer l'octet de poids fort ?

Les piles SSL/TLS maison (2/3)

- En 2010, Google propose plusieurs extensions, *False Start* et *Snap Start*
- Après plusieurs mois, Internet se montre intolérant à *Snap Start*
- L'expérimentation est abandonnée en 2012

Les piles SSL/TLS maison (2/3)

- En 2010, Google propose plusieurs extensions, *False Start* et *Snap Start*
- Après plusieurs mois, Internet se montre intolérant à *Snap Start*
- L'expérimentation est abandonnée en 2012

- Un an plus tard, le même problème resurgit dans un autre contexte
- Sur la liste de diffusion IETF (`tls@ietf.org`), on apprend finalement la raison : le `ClientHello` est trop gros...

Les piles SSL/TLS maison (3/3)

Examinons le début d'un `ClientHello` de 258 octets

16	03	01	01	02

TLS

Type	Version	Longueur
HS	*TLS 1.0*	*258*

SSLv2

Longueur	*Pad.*	Type
5635	...	*CH*

Un `ClientHello` TLS dont la taille est comprise entre 256 et 511 peut être confondu avec un `ClientHello` SSLv2 !

Les piles SSL/TLS maison (3/3)

Examinons le début d'un `ClientHello` de 258 octets

16	03	01	01	02

TLS

Type	Version	Longueur
HS	*TLS 1.0*	*258*

SSLv2

Longueur	*Pad.*	Type
5635	...	*CH*

Un `ClientHello` TLS dont la taille est comprise entre 256 et 511 peut être confondu avec un `ClientHello` SSLv2 !

Tout est bien qui finit bien

- Google a finalement proposé une extension pour ajouter du bourrage au `ClientHello`...

Table des matières

Absence de TLS

Un cas classique de problème lié à TLS est l'absence de TLS !

- URL en `http` et non `https`
- serveur ne proposant pas STARTTLS
- problème des pages web avec du contenu mixte
- pages de *login* en `http`

Absence de TLS

Un cas classique de problème lié à TLS est l'absence de TLS !

- URL en `http` et non `https`
- serveur ne proposant pas STARTTLS
- problème des pages web avec du contenu mixte
- pages de *login* en `http`

Contre-mesures

- forcer TLS côté client (HSTS, configuration client mail...)
- durcir le fonctionnement des navigateurs

Qualité de la connexion ?

Il existe des faiblesses dans TLS

Qualité de la connexion ?

Il existe des faiblesses dans TLS

- SSLv2 doit être proscrit

Qualité de la connexion ?

Il existe des faiblesses dans TLS

- SSLv2 doit être proscrit
- SSLv3 et TLS 1.0 permettent des attaques sur le mode CBC

Qualité de la connexion ?

Il existe des faiblesses dans TLS

- SSLv2 doit être proscrit
- SSLv3 et TLS 1.0 permettent des attaques sur le mode CBC
- de manière générale, les suites reposant sur CBC sont faibles

Qualité de la connexion ?

Il existe des faiblesses dans TLS

- SSLv2 doit être proscrit
- SSLv3 et TLS 1.0 permettent des attaques sur le mode CBC
- de manière générale, les suites reposant sur CBC sont faibles
- les suites reposant sur RC4 aussi...

Qualité de la connexion ?

Il existe des faiblesses dans TLS

- SSLv2 doit être proscrit
- SSLv3 et TLS 1.0 permettent des attaques sur le mode CBC
- de manière générale, les suites reposant sur CBC sont faibles
- les suites reposant sur RC4 aussi...
- l'échange clé par chiffrement RSA (PKCS#1 v1.5) est difficile à implémenter correctement

Qualité de la connexion ?

Il existe des faiblesses dans TLS

- SSLv2 doit être proscrit
- SSLv3 et TLS 1.0 permettent des attaques sur le mode CBC
- de manière générale, les suites reposant sur CBC sont faibles
- les suites reposant sur RC4 aussi...
- l'échange clé par chiffrement RSA (PKCS#1 v1.5) est difficile à implémenter correctement
- il ne faut pas utiliser les options de compression

Qualité de la connexion ?

Il existe des faiblesses dans TLS

- SSLv2 doit être proscrit
- SSLv3 et TLS 1.0 permettent des attaques sur le mode CBC
- de manière générale, les suites reposant sur CBC sont faibles
- les suites reposant sur RC4 aussi...
- l'échange clé par chiffrement RSA (PKCS#1 v1.5) est difficile à implémenter correctement
- il ne faut pas utiliser les options de compression
- les paramètres RSA/DH/ECDH doivent être correctement dimensionnés

Qualité de la connexion ?

Il existe des faiblesses dans TLS

- SSLv2 doit être proscrit
- SSLv3 et TLS 1.0 permettent des attaques sur le mode CBC
- de manière générale, les suites reposant sur CBC sont faibles
- les suites reposant sur RC4 aussi...
- l'échange clé par chiffrement RSA (PKCS#1 v1.5) est difficile à implémenter correctement
- il ne faut pas utiliser les options de compression
- les paramètres RSA/DH/ECDH doivent être correctement dimensionnés

Solution

- TLS 1.2 avec des suites récentes (GCM) et ECDHE
- TLS 1.3 (qui ne permet que ces suites)

Problème d'implémentation

Morceaux choisis dans les piles TLS

- 2002 : Mauvaise interprétation de l'extension X.509 *Basic Constraints* (IE)
- 2008 : contournement de la validation de certificats (OpenSSL)
- 2009 : confusion liée à la présence de caractères nuls dans les certificats (divers)
- 2011 : Mauvaise interprétation de l'extension X.509 *Basic Constraints* (iOS)
- 2014 : `goto fail` Apple
- 2014 : contournement de la validation de certificats (GnuTLS)
- 2014 : *Heartbleed* et *EarlyCCS* (OpenSSL)
- 2015 : FREAK et *LogJam* (nombreuses piles)

Problème d'implémentation

Morceaux choisis dans les piles TLS

- 2002 : Mauvaise interprétation de l'extension X.509 *Basic Constraints* (IE)
- 2008 : contournement de la validation de certificats (OpenSSL)
- 2009 : confusion liée à la présence de caractères nuls dans les certificats (divers)
- 2011 : Mauvaise interprétation de l'extension X.509 *Basic Constraints* (iOS)
- 2014 : `goto fail` Apple
- 2014 : contournement de la validation de certificats (GnuTLS)
- 2014 : *Heartbleed* et *EarlyCCS* (OpenSSL)
- 2015 : FREAK et *LogJam* (nombreuses piles)

Solutions ?

- plus de tests
- une meilleure spécification
- des méthodes de développement plus sérieuses

Côté crypto ?

Soucis d'aléa dans la génération des clés

- bug OpenSSL dans Debian
- problèmes de génération d'aléa sur des équipements réseau
- *Return of the Coppersmith Attack*

Côté crypto ?

Soucis d'aléa dans la génération des clés

- bug OpenSSL dans Debian
- problèmes de génération d'aléa sur des équipements réseau
- *Return of the Coppersmith Attack*

Gestion des certificats

- absence de la vérification des certificats
- émission frauduleuse de certificats (Diginotar)

Côté crypto ?

Soucis d'aléa dans la génération des clés

- bug OpenSSL dans Debian
- problèmes de génération d'aléa sur des équipements réseau
- *Return of the Coppersmith Attack*

Gestion des certificats

- absence de la vérification des certificats
- émission frauduleuse de certificats (Diginotar)

Solutions ?

- une meilleure compréhension des enjeux et des hypothèses crypto par les développeurs
- une bonne protection des secrets
- la mise en oeuvre de moyens de révocation
- *Certificate Transparency*
- le *certificate pinning*

Que protège réellement TLS ?

TLS n'est qu'un élément de la sécurité

Que protège réellement TLS ?

TLS n'est qu'un élément de la sécurité

- dans certains cas, la connexion TLS n'est que le premier maillon d'une chaîne
  - *Content Delivery Networks* avec HTTP
  - suite de rebonds avec SMTP

Que protège réellement TLS ?

TLS n'est qu'un élément de la sécurité

- dans certains cas, la connexion TLS n'est que le premier maillon d'une chaîne
  - *Content Delivery Networks* avec HTTP
  - suite de rebonds avec SMTP
- TLS ne protège que le tunnel, pas l'objet transmis
  - différence avec *Subresource Integrity* et S/MIME

Que protège réellement TLS ?

TLS n'est qu'un élément de la sécurité

- dans certains cas, la connexion TLS n'est que le premier maillon d'une chaîne
  - *Content Delivery Networks* avec HTTP
  - suite de rebonds avec SMTP
- TLS ne protège que le tunnel, pas l'objet transmis
  - différence avec *Subresource Integrity* et S/MIME
- la pile TLS vit dans un système...

Que protège réellement TLS ?

TLS n'est qu'un élément de la sécurité

- dans certains cas, la connexion TLS n'est que le premier maillon d'une chaîne
  - *Content Delivery Networks* avec HTTP
  - suite de rebonds avec SMTP
- TLS ne protège que le tunnel, pas l'objet transmis
  - différence avec *Subresource Integrity* et S/MIME
- la pile TLS vit dans un système...
- ... et sert à une application

Conclusion

- TLS est une brique importante
- Mais la sécurité ne se résume pas à des communications sécurisées
- Il faut prendre en compte la sécurité dans tous les aspects
- Au-delà des aspects techniques, quid de la perception et de l'organisationnel
- Au-delà de la prévention, il faut penser à la réaction et à la reprise après incident

Questions ?

Merci de votre attention.