La force du certificat (auto-signé)

Pierre Bettens

pbettens@heb.be

octobre 2015
v0.2

— Le site est en https donc c'est sécurisé.
— Oui et non.

Un site en *https* signifie que la communication entre le serveur — le site web auquel l'utilisateur accède — et le client — le navigateur internet — est chiffrée. Si cette communication est chiffrée, elle ne pourra pas être lue par un tiers. Le mot de passe de ton compte, le numéro de ta carte visa, la recette de la tarte à mastelles, la photo de ta b… bagnole. Tout ça circule de manière chiffrée en `https` ou en clair si c'est simplement en `http`.

Pour mettre en place une communication *tls* (anciennement *ssl*), il faut deux ingrédients.

Le premier ingrédient permet effectivement que la communication entre les deux parties soit chiffrée. C'est de la cryptographie asymétrique avec génération de clés privées et publiques et partage de la clé publique. Dès lors que la taille des clés et la méthode de chiffrement sont valables, la communication ne sera pas déchiffrée (en un temps raisonnable et avec des moyens raisonnables bla bla). Grâce à ces clés, on peut faire deux choses:

- vérifier l'identité d'un interlocuteur. En effet s'il me donne sa clé publique et s'il prétend être qui il prétend, il détient alors la clé privée et je peux lui envoyer un challenge;
- établir un canal de communication sécurisé temporaire pour s'échanger une clé de session qui chiffrera toute la suite de la communication.

Le deuxième ingrédient se résume en une seule question :

> **« Mon interlocuteur est-il bien qui il prétend être ? »**.

Il est en effet possible qu'une personne malveillante substitue son site web au site web auquel je voulais me connecter afin de dérober mes secrets ! C'est là qu'entre en jeu l'autorité de certification.

Le rôle de **l'autorité de certification** est simplement de garantir l'identité de l'interlocuteur. Plus précisément la validité du couple identité / clé publique. Si je tente une connexion *https* au site `secure.example.org` l'autorité de certification pourra me dire si c'est effectivement avec le « bon » site `secure.example.org` que je communique. Si c'est le cas, nous échangerons nos clés et nous communiquerons de manière chiffrée. Sinon, mon navigateur me préviendra du danger.

Il existe différents types de certificats. La question du jour s'intéresse à la confiance que l'on peut leur faire[1]. On parle bien ici de la confiance que l'on a en l'autorité qui me garantit qu'une autre personne est digne de confiance. On pourrait s'intéresser à qui sont ces autorités mais ce n'est pas l'objet.

Le premier type de certificat que l'on rencontre est le **certificat auto-signé**. À l'allure ci-dessous, je garantis que je suis bien qui je prétends être.

— C'est qui ?
— C'est moi.
— Qui ça moi ?
— Ben moi, ouvre !

```
Émis pour
Nom commun (CN)             secure.example.org
Organisation (O)            ACME
Unité d'organisation (OU)   ACME
```

[1] Faire confiance en une autorité de certification, c'est croire: 1/ qu'elle n'accorde pas de faux certificat à des tiers (voir Microsoft en tunisie, l'affaire Ben Ali), 2/ qu'elle vérifie correctement l'identité des demandeurs, 3/ qu'elle ne fait pas les attaques *man in the middle* elle-même car elle est très bien placée pour le faire.

```
Numéro de série             AA:BB:11:22:CC:DD:33:44::EE

Émis par
Nom commun (CN)             secure.example.org
Organisation (O)            ACME
Unité d'organisation (OU)   AME

Période de validité
...
```

En fonction du navigateur, le message d'alerte sera différent. Google Chrome donnera toujours un avertissement qu'il sera « difficile » d'ignorer tandis que Mozilla Firefox proposera d'ajouter une exception permanente.

- Avec Google Chrome si le certificat change un jour, je n'en suis pas informé car je dois ignorer l'avertissement à chaque connexion. Je suis donc dans une « situation dangereuse » à chaque fois. Le choix de Google de ne pas autoriser l'enregistrement d'une exception pousse à l'abandon des certificats auto-signé. Est-ce un aspect sécuritaire ou commercial ?
- Avec Mozilla Firefox, si je décide de faire confiance au site web une première fois en ajoutant l'exception, il me préviendra si, soudain, le certificat change. Je dois faire confiance lors de la première connexion.

Un certificat auto-signé n'est pas **nécessairement** une mauvaise solution ni une solution dangereuse. Je suis sûr que la connexion est chiffrée et je serai informé — si j'utilise Mozilla Firefox et s'il ne le fait pas dès la première connexion — si quelqu'un usurpe l'identité du site.

L'important, pour que la communication soit confidentielle, c'est d'être sûr de l'identité de mon interlocuteur. C'est d'être sûr que la clé publique présentée est bien la sienne. Un meilleur moyen que le certificat auto-signé serait simplement l'affichage — avec surveillance — de l'empreinte de cette clé sur la place publique. Le canal de communication de la clé doit être sécurisé mais pas confidentiel.

Dans le cadre de l'école, les **valves papiers** font très bien l'affaire. Je ne dois pas faire confiance à une société tierce et je suis certain que la clé est la bonne puisque je le vérifie moi-même.

C'est bien dans le choix du type de certificat que se passe toute la réflexion. Je n'ai pas besoin de la même sécurité lorsqu'il s'agit du site d'une banque ou d'un site de commerce en ligne, d'un site de porn / rencontre, d'un site de *elearning*...

Les **autres types de certificats** sont garantis par une autorité de certification tierce et la « force » de la garantie dépend simplement du prix que l'on veut bien payer ! En fonction de ce prix, l'autorité de certification fera des vérifications de l'identité du demandeur plus ou moins poussées. Des navigateurs comme Google Chrome et l'ignorance des utilisateurs m'imposent d'utiliser un tel certificat pour éviter l'affichage d'un avertissement à chaque connexion.

Pour les certificats les moins chers, l'autorité se contente de vérifier que le demandeur a bien la main sur le domaine. L'une des trois méthodes utilisée est:

- demande d'ajout d'un enregistrement DNS (il faut avoir la main sur la zone concernée);
- demande d'ajout d'une adresse mail particulière (il faut avoir la main sur la zone ou sur le serveur de mail);
- demande d'ajout d'un fichier texte particulier à la racine du domaine à protéger (il faut avoir la main sur l'hébergement)

Pour les certificats plus chers et donc plus surs, le demandeur devra montrer des preuves de domiciliation, de propriété du nom de domaine… et l'autorité de certification pourra offrir des garanties sur les transactions financières.

À partir de ±300€ / an, l'autorité de certification fournit la « **green bar** » gage d'une vérification poussée.

On aura alors des certificats à l'allure suivante:

```
Émis pour
Nom commun (CN)             secure.example.org
Organisation (O)            ACME
Unité d'organisation (OU)   ACME
Numéro de série             AA:BB:11:22:CC:DD:33:44::EE

Émis par
Nom commun (CN)             VeriSign Class 3 Secure Server CA - G3
Organisation (O)            VeriSign, Inc
Unité d'organisation (OU)   VeriSign Trust Network

Période de validité
...
```

Le plus simple est de faire confiance à son navigateur. Le plus simple n'est jamais le plus sécurisé. Lorsque le navigateur accepte un certificat TLS, c'est bien. Je peux ne pas me poser de question. Lorsqu'il le refuse, rien n'empêche de le regarder et de l'accepter en fonction du site web qu'il chiffre.

Crédit photo par Pitivier et ses amis chez Live2times. Qui donc que la septième compagnie pour représenter l'autorité ?

Merci aux collègues qui ont accepté de relire.

Article publié sur notes · de · pit