Mise au point sur le HTTPS

freetux

Date de publication : 26 juin 2015
Dernière modification : 26 juin 2015

Introduction

À l'heure actuelle, n'importe quelle donnée est épiée, stockée, étudiée, analysée, triée, classée et utilisée contre nous. Le chiffrement de l'information est et restera le seul rempart pour protéger nos données secrètes (mots de passe, compte en banque, etc.), nos données privées (idées politiques, habitudes de consommations, etc.) et nos données personnelles (date de naissance, adresse physique, courriel, etc.).

La technique de chiffrement la plus connue est le SSL (*Secure Sockets Layer*) maintenant appelé TLS (*Transport Layer Security*) qui est utilisé pour chiffrer les communications entre notre ordinateur et un site Web. Celui-ci se reconnaît au `https://` de l'URL du site que vous souhaitez visiter. Dans la conscience collective, la simple présence du cadenas que vous affiche votre navigateur vous certifie que tout est sûr et que personne ne lira les données qui transitent. Quand on voit une barre verte en plus, là on se dit que c'est le *summum* de la sécurité et qu'il n'y a rien de plus fiable. Même la NSA ne pourra pas les lire. Ouf ! Dans le cas où votre navigateur vous affiche une « Alerte de sécurité » sur un site en `https://` soit les gens fuient en pensant se faire pirater soit ils cliquent sur « Je comprends les risques » sans les lire… *A contrario*, quand c'est juste noté `http://`, là on se dit que c'est pas chiffré et que tout le monde peut lire ce qui passe dans le Réseau (enfin j'espère que la plupart des gens pensent cela…). Donc le monde est divisé en deux options : `http://` pas sécurisé, `https://` sécurisé si pas d'alerte du navigateur, finalement c'est simple le chiffrement.

Seulement il y a un hic.

Les coulisses du https

Le hic c'est ce qu'il existe une chose encore plus dangereuse que le manque de sécurité, c'est l'excès de confiance en la sécurité d'un système. Je m'explique. Si vous utilisez une technologie qui n'est pas sécurisée (que ça soit en informatique ou dans le monde physique), vous agirez d'une certaine façon. Si vous utilisez une technologie que vous savez sécurisée (parce que vous savez comment elle fonctionne par exemple), vous agirez d'une autre façon (plus librement). Enfin, si vous utilisez une technologie que vous croyez sécurisée (parce qu'on vous dit ou vous montre que c'est sécurisé sans vous expliquer comme elle fonctionne) mais qu'en fait non, vous vous retrouvez en danger ou exposés.

De très mauvaises habitudes se sont installées dans la tête des gens et malheureusement les développeurs des logiciels n'ont pas forcement aidé à les changer.

En effet, au même titre qu'un cadenas à clé ou qu'une serrure de porte, il existe plusieurs technologies, certaines datant de Louis XVI, d'autres du début du XIX^e^siècle ou des bien plus récentes datant du début de l'année. Les algorithmes de chiffrement fonctionnent de la même façon : certains sont vieux et dépassés alors que d'autres sont récents. Qui utiliserait une porte datant de Louis XVI pour sa maison ? Qui utiliserait une technique de chiffrement datant de 10 ans pour son ordinateur ?

Quand vous allez sur un site Web, votre navigateur vous dit que la connexion est chiffrée est que les certificats (les clés qui permettent de chiffrer) ont été signés — ou certifiés — par une autorité qu'il connait. Par exemple, Firefox connaît l'autorité de certification de Gandi, alors tous les certificats que Gandi va signer seront valides sur votre navigateur. Par contre, les certificats SSL de mes sites Web sont signés par ma propre autorité, vous aurez donc une erreur de sécurité de votre navigateur vous disant que l'autorité est inconnue, ce qui est logique. En effet, mon autorité de certification personnelle n'est pas présente dans Firefox ou d'autre navigateurs par défaut.
Trois questions peuvent alors se poser : qui sont ces autorités de certifications ? Comment une autorité de certification arrive à être connue des navigateurs Web ? Et comment les autorités de certification signe des certificats de clients ?
Pour répondre dans l'ordre, tout le monde peut être une autorité de certification, moi-même j'en suis une (voir mon article sur le sujet ici). Pour être présent dans les navigateurs Web il faut respecter une trèèèès long liste de conditions (pour Firefox, voir ici) et aligner pas mal d'argent pour des audits par exemple. Il en existe une bonne centaine autorisée dans votre navigateur. Enfin, pour faire signer ses certificats par une autorité de certification, il suffit de payer l'autorité

et respecter quelques conditions (plus ou moins strictes selon l'autorité).
Maintenant, une dernière question peut/doit se poser : et la sécurité dans tout ça ?
Il est justement ici le problème. Dans tout ce que j'ai dit plus haut, la force des certificats (directement liée à la sécurité des échanges) est secondaires pour les faire signer et reconnaître par votre navigateur. Par ailleurs, les protocoles acceptés par le serveur hébergeant un site sont totalement indépendants de l'autorité. Finalement, ce que l'internaute voit, c'est qu'une autorité soi-disant (re)connue par votre navigateur a signé les clés de chiffrement du site que vous visitez. À première vue, vous n'avez aucune idée du chiffrement qui est utilisé derrière. La seule information que cela vous donne, c'est que vous vous trouver bien sur le bon site. Pour tester la sécurité des sites que vous visitez régulièrement (banque, sites d'administration, Webmail, etc.), vous pouvez vous rendre sur ce site : https://www.ssllabs.com/ssltest/ et rentrer le nom du domaine en question : particuliers.societegenerale.fr, le site de Pôle Emploi ou celui des impôts par exemple.
Ce site analyse en profondeur le niveau de sécurité des technologies de chiffrement utilisées par le serveur que vous souhaitez joindre, indépendamment de l'autorité. Et là, le monde est beaucoup moins rose. Beaucoup de serveurs présentent de grosses failles de sécurité comme Poodle permettant à un attaquant de déchiffrer sans problème un flux de donnée normalement chiffré.

Ce que je pense du modèle de certification SSL

Personnellement, je trouve qu'il serait bien que les développeurs des navigateurs Web permettent d'avertir les utilisateurs, via un code couleur par exemple, des niveaux de chiffrements que proposent les sites qu'ils consultent. Cela aura comme conséquence une plus grande visibilité des risques et donc une meilleure sensibilisation des Internautes. Si ces informations commencent à devenir grand public, les administrateurs réseaux réagiront rapidement pour rectifier le tir, c'est sûr. Un très bon exemple est celui de Heartbleed qui a été beaucoup médiatisé. Très rapidement (enfin pas pour tous...) la plupart des serveurs importants ont procédé à la mise à jour. Cependant, Heartbleed permettait à une personne d'attaquer directement le serveur d'une banque ou n'importe quel site de commerce en ligne par exemple. Les failles encore possibles sur de nombreux sites actuellement permettent d'attaquer les utilisateurs et non les serveurs. Du coup les entreprises derrières sont beaucoup moins pressées. Ça n'est pas comme si elles se préoccupaient de leurs clients/internautes...

Certains me diront que pour les gens sur Windows XP utilisant encore Internet Explorer 6 ou 8, ils ne pourront plus aller sur les sites « sécurisés » vu que

ces deux versions de IE ne prennent pas en charge les technologies récentes. Bah tant pis, un mal pour un bien comme on dit. La proportion de personnes sur XP + IE est tout de même relativement faible, et si on en trouve encore, il faut les inviter à passer sur GNU/Linux, c'est le bon moment de migrer. Mais il ne faut pas, sous prétexte que quelques personnes risquent d'avoir des problèmes d'accès, ne rien faire pour autant. Il y aura peut-être quelques difficultés au début, mais elles seront vite résolues. Surtout, je n'ai pas envie d'être obligé de me connecter à des sites pas sécurisés, juste parce qu'il y a encore quelques personnes sur des très vieilles version qui ne sont plus compatibles avec les nouvelles technologies…Un dernier contre-exemple, les personnes utilisant Internet Explorer sur Windows XP doivent représenter 0,1 % des Internautes. En parallèle, 6 % d'internautes sont aveugles ou mal-voyants et sont obligés d'avoir des sites Web accessibles pour qu'ils puissent les utiliser. Tous les sites sont-ils vraiment accessibles ? Loin de là. Mais pour le coup, tout le monde s'en fout…

Plus généralement, je trouve que tout le système actuel est bancal. Il faut arrêter de se focaliser sur la seule existence d'une autorité de certification et d'afficher un beau bandeau vert alors que les technologies de chiffrement derrières sont pourries. Certes, elles sont importantes mais pas obligatoires pour assurer la sécurité des données qui transitent sur le Net. Ça n'est pas parce qu'un site n'a pas d'autorité qu'il n'est pas sécurisé. Et ça n'est pas parce qu'un site s'est payé une autorité reconnue qu'il est sécurisé pour autant. Il faut nuancer ces messages. Si un navigateur Web dit sur le site d'une banque ce message : « l'autorité de certification est valide, mais ce serveur utilise des technologies anciennes et vulnérables à plusieurs failles de sécurité, vos données ne sont donc plus sécurisées », en une semaine tous les serveurs importants se mettent à jour. Sûr.

Une petite piste d'amélioration

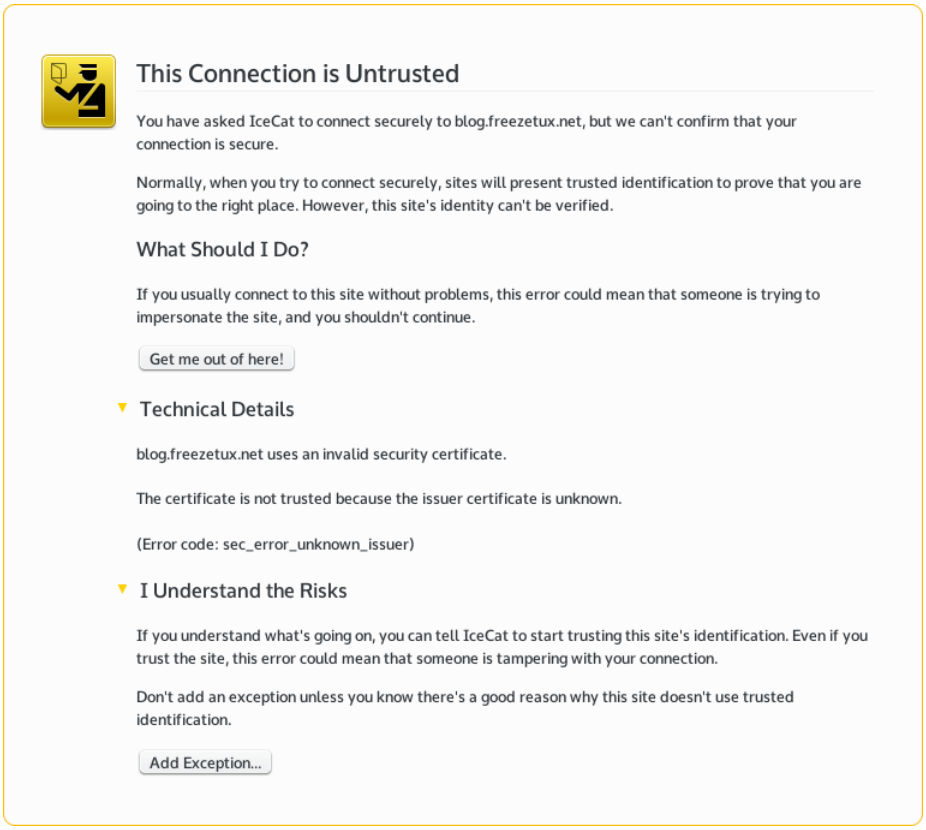
Petit exemple de ce qui pourrait se faire du côté des navigateurs pour les sites ayant une autorité reconnue (utilisation du code couleur de SSLlabs) :

- protocoles et certificats sûrs :
  

- vulnérabilité Poodle (par exemple) :
  

- procoles dépassés, failles nombreuses :
  

En attendant, je vous invite aussi à installer sur votre navigateur Web cette extension vous affichant via un code couleur la fiabilité des technologies de chif-



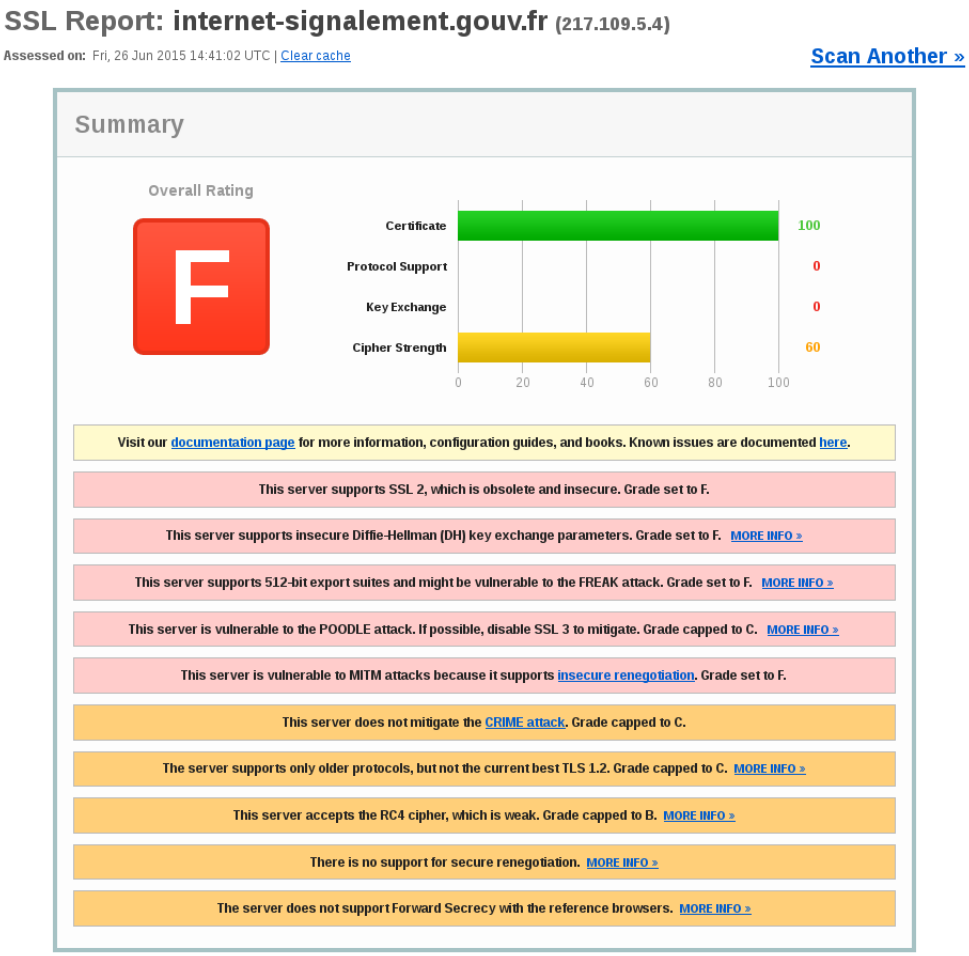
Un exemple de message de Icecat (équivalent de Firefox) avertissant que l'autorité de mon blog n'est pas connue. Pourtant, en mettant à part l'autorité, mon serveur est irréprochable d'un point de vue de la sécurité des certificats et des protocoles de chiffrement comme le montre SSLlabs. Pourquoi je devrais subir une alerte aussi stricte ? Le message d'information de cette image est à mon avis très mauvais et informe mal les internaute sur les risques liés. À cause de lui, je ne peux pas mettre tous les sites en `https` exclusif afin de m'adapter à ceux qui ne savent pas quoi faire avec un tel message et feront demi-tour sans regarder le site...

frement utilisées sur le site que vous visitez. Vous pourrez via cette même extension, interdire d'utiliser certaines technologies considérées comme peu fiables (RC4, SSL2, SSL3…), au risque de ne plus pouvoir visiter beaucoup de sites. Si vous souhaitez aller plus loin, demander des comptes aux administrateurs du site.

En guise de conclusion…

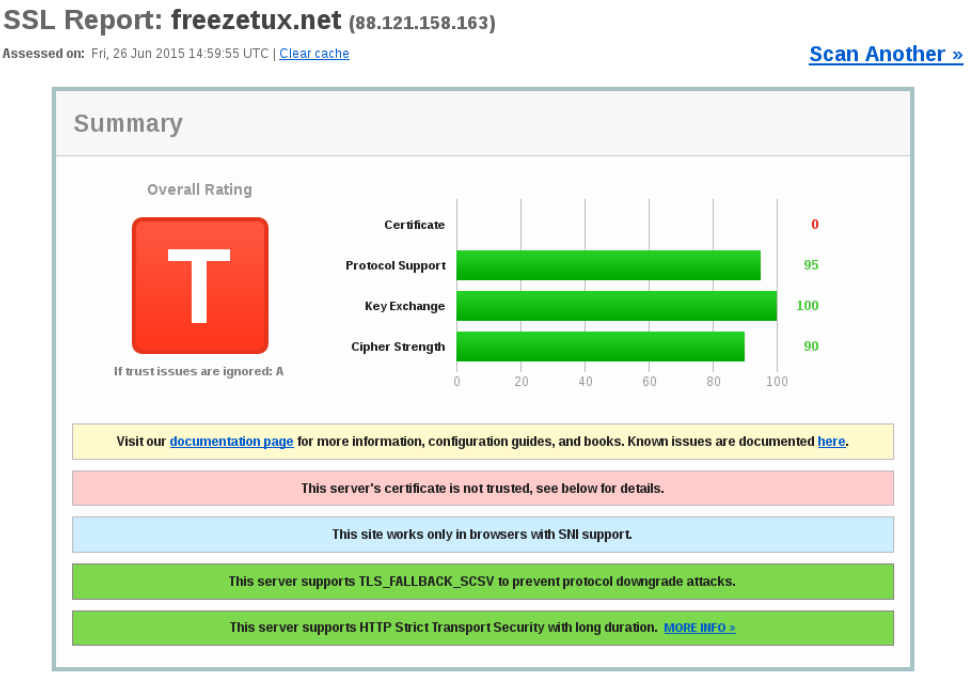
Vous préférez lequel ?

- La sécurité sur la plateforme Pharos du ministère de l'Intérieur…



- … ou la sécurité sur mes sites Web, même si mon autorité de certification n'est pas reconnue par votre navigateur ? (Je trouve SSLlabs très binaire

d'ailleurs pour le critère de l'autorité...)



Ne vous fiez pas à ce qu'on vous dit, allez voir par vous-même si vous pouvez faire confiance en une technologie. ;-)

Lire et voir ailleurs

- Conférence d'Aeris à Pas sage en Seine sur « SSL/TLS pour les nuls »

