Pourquoi le certificat de la CNIL n'est pas reconnu et autres belles histoires au coin du feu en hiver

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 mars 2016

https://www.bortzmeyer.org/cnil-et-x509.html

Tout le monde, surtout les gens qui ne savent pas distinguer ROT13 de SHA-256, l'a constaté et largement commenté sur les rézosocios : le site de la CNIL a un problème de certificat. Que s'est-il donc passé ? C'est de leur faute ? Ce sont des gros nuls, doublés de feignants ? Les certificats servent-ils à quelque chose ?

Pour commencer, essayez ces deux liens : et . Avec le certificat installé aujourd'hui, le premier lien devrait déclencher une erreur de sécurité (genre « *"The certificate is only valid for the following names : www.cnil.fr [...]"* »), le second lien va marcher avec certaines machines, mais, avec d'autres, vous aurez un avertissement de sécurité (comme « *"The certificate is not trusted because the issuer certificate is unknown"* »).

Avant de répondre aux questions que je posais plus haut, revenons au rôle des certificats (si vous lisez le X.509 en codé en DER sans l'aide d'un ordinateur, et en faisant les calculs RSA de tête, vous pouvez sauter ce paragraphe). La communication avec le site de la CNIL utilise le protocole HTTPS, qui est HTTP avec en prime la sécurité qu'apporte la cryptographie. Celle-ci, fournie par un mécanisme nommé TLS (et que certains conservateurs s'obstinent à nommer de son nom du siècle précédent, SSL), permet d'éviter l'écoute de votre conversation par un tiers indiscret. Elle fournit également une certaine authentification du site distant, vous garantissant (en théorie) que vous allez bien sur le site de la CNIL. (Les deux fonctions, confidentialité et authentification, sont en fait liées : sans l'authentification, vous pourriez parler à l'Homme du Milieu, qui pourrait alors lire vos communications.) Le certificat est une clé cryptographique, celle qu'utilise le serveur distant pour chiffrer ses communications avec vous, agrémenté d'une série de noms (la norme technique des certificats, X.509, les appelle « sujets »), de quelques métadonnées et signé par une Autorité de Certification. Cette signature par une AC vous garantit que le certificat est bien celui de la CNIL et pas un certificat qu'un plaisantin a généré lui-même, en y mettant comme nom celui de la CNIL.

Deux points sont particulièrement à retenir dans ce résumé très simplifié : le certificat indique les noms possibles pour le site Web, et il ne sera accepté que s'il est signé par une AC elle-même « acceptée ». Or, le nouveau site de la CNIL a **deux** problèmes, portant sur ces deux points.

Premier problème, dans la liste des noms (les « sujets ») du certificat, on ne trouve pas `cnil.fr`. Si on se connecte à , on aura donc systématiquement une erreur du genre :

(Dans la version française du navigateur, « Le certificat n'est valide que pour les noms suivants : www.cnil.fr [...])

Comment trouver cette liste ? Le navigateur Web peut vous la donner. Sur Firefox, cliquer sur le cadenas, demander "*More information*" puis "*View certificat*" et, dans la liste des attributs du certificat, sélectionner "*subject*" et "*Subject Alt Name*" :

Une méthode plus "*geek*" est d'utiliser OpenSSL en ligne de commande :

```
% openssl s_client -connect cnil.fr:443  | openssl x509 -text
...
Subject: C=FR, O=COMMISSION NAT INFORMATIQUE ET LIBERTE, OU=0002 11000012200025, L=PARIS, CN=www.cnil.fr/ser
...
X509v3 Subject Alternative Name:
   DNS:www.cnil.fr, DNS:piwik.cnil.fr, DNS:backoffice.cnil.fr, DNS:www.jeunes.cnil.fr, DNS:www.educnum.fr
```

On voit bien que `cnil.fr` ne figure pas dans les noms. Cette erreur là (car, oui, à mon avis, c'est une erreur de la part de la CNIL, qui permet les connexions à `https://cnil.fr/` mais ne présente pas de quoi l'authentifier) explique le premier problème.

Le second problème, maintenant. Il ne se produit qu'avec certains systèmes. Par exemple, le Firefox sur ma Debian affiche :

```
www.cnil.fr uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.

(Error code: sec_error_unknown_issuer)
```

Ici, le problème est tout différent. Rappelez-vous que le certificat doit être signé par une Autorité de Certification (le "*issuer*" du message ci-dessus). Chaque logiciel qui se connecte avec le protocole TLS a un **magasin** stockant les AC (Autorités de Certification) qu'il reconnait. (Parfois, le magasin est global au système d'exploitation, ou bien à une bibliothèque logicielle particulière, et le navigateur Web ne fait qu'utiliser ce magasin qu'on lui a fourni.) Qui décide de ce qu'on met dans le magasin ? Eh bien, c'est ça qui est drôle, personne. Il n'existe pas d'autorité qui décide de ce qu'on met ou pas dans ce magasin. Chaque gestionnaire d'un magasin d'AC (donc, chaque navigateur Web, ou système d'exploitation) a ses propres critères (parfois documentés - ici, la politique de Mozilla <`https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/`>, parfois opaques, parfois arbitraires) pour décider. Résultat, deux magasins n'ont jamais le même contenu. On peut donc avoir un certificat qui est accepté par une machine et refusé par une autre, ou même accepté par un navigateur Web et refusé par un autre sur la même machine.

C'est ce qui est arrivé à la CNIL. Leur certificat est signé par l'AC Certinomis <`https://www.certinomis.fr/`> et certains n'ont pas le certificat de l'AC dans leur magasin (ou, peut-être, n'ont qu'un autre certificat de cette AC). C'est un problème fréquent, et qui n'est pas réellement de la faute de la CNIL. (À noter que la version HTTPS de mon blog a souvent le même problème <`https://www.bortzmeyer.org/https-blog.html`>, en raison de son utilisation de l'AC CAcert <`https://www.bortzmeyer.org/cacert.html`>.)

Ce petit incident est donc l'occasion de rappeler quelques règles de fonctionnement du système X.509, qui est derrière l'authentification des sessions TLS :

— La notion d'AC « officielle » ou d'AC « reconnue » n'a aucun sens. Chacun choisit les AC de son magasin.
— Qu'une AC soit absente d'un magasin ne signifie pas (contrairement à ce que prétendent des ignorants <https://twitter.com/zataz/status/705430910498381825>) que les gérants du site Web soient incompétents ou négligents. Ils ne contrôlent pas les AC utilisées par les **clients**.