

Python, TLS et les délais de garde

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 Avril 2009

<http://www.bortzmeyer.org/python-tls-timeout.html>

J'ai besoin de munir un client HTTP existant, écrit en Python, de TLS. Je ne veux pas seulement faire des connexions chiffrées mais aussi accéder à des informations sur le certificat du serveur, notamment le nom de la CA qui l'a signé. Comme le but du projet <<http://www.dnswitness.net/>> est d'interroger pas mal de serveurs HTTP, souvent non répondants (il est fréquent qu'un serveur réponde en HTTP et "timeoute" en HTTPS et on ne peut pas le savoir avant d'essayer), il faut pouvoir mettre des délais de garde sur la connexion.

Il y a plusieurs solutions en Python (en dépit de la règle "*There should be one— and preferably only one—obvious way to do it.*" du PEP 20 <<http://www.python.org/dev/peps/pep-0020/>>) mais aucune parfaite pour ce besoin. Voyons les solutions.

python-gnutls <<http://pypi.python.org/pypi/python-gnutls>> : pratiquement pas documenté, peut-être pas maintenu, ne permet pas de mettre un délai maximum (car il fonctionne avec des prises non-bloquantes, on récupère un `gnutls.errors.OperationWouldBlock: Function was interrupted`).

Python OpenSSL <<http://pyopenssl.sourceforge.net/>>. Pas mieux : si on met un "timeout", il plante également tout de suite avec un `OpenSSL.SSL.WantReadError`.

Le module SSL <<http://docs.python.org/library/ssl.html>> de la bibliothèque standard. Il nécessite Python 2.6 et je voudrais bien que mon code marche en 2.5. Il ne semble pas permettre de récupérer les méta-données du certificat.

TLSSlite <<http://trevp.net/tlsslite/>>. Ne semble pas capable de récupérer le nom du signataire.

Donc, toujours pas de solution pour faire du TLS avec "timeout". Le programme qui l'appellera étant multi-"threadé", je ne peux pas utiliser les signaux Unix. Je suis donc toujours à la recherche de la solution géniale. Pour les utilisateurs de Stack Overflow <<http://www.bortzmeyer.org/stack-overflow.html>>, j'ai lancé une récompense de 100 points <<http://stackoverflow.com/questions/675130/tls-connection-with-timeouts-and-a-few-other-difficulties>> sur cette question.