Server Name Indication

Server Name Indication (**SNI**), qui peut se traduire par « **indication du nom du serveur** », est une extension du protocole TLS[1]. Avec l'extension SNI, le client indique le nom d'hôte (*hostname*) avec lequel il tente de démarrer une négociation TLS. Cela permet au serveur de présenter plusieurs certificats pour la même adresse IP (mais des noms d'hôte différents), et donc de mutualiser des hébergements pour des sites sécurisés en https.

Tous les navigateurs web ne supportent pas le SNI. Lorsque le navigateur ne supporte pas le SNI, le serveur fournit le certificat par défaut, et un avertissement au sujet du certificat se produit donc le plus souvent.

Sommaire

1 Problème initial
2 En quoi SNI résout ce problème ?
3 Déploiement
4 Références

Problème initial

Lorsqu'un client initie une connexion TLS, il demande un certificat électronique au serveur web ; une fois que le serveur a renvoyé le certificat, le client l'examine et compare le nom de domaine qu'il essaye de joindre avec le ou les noms inclus dans le certificat. Si une correspondance est trouvée, la connexion continue comme d'habitude. Sinon, l'utilisateur est généralement prévenu d'un problème et la connexion est alors interrompue, puisqu'un tel problème peut signaler une tentative d'attaque de l'homme du milieu. Cependant, certaines applications autorisent l'utilisateur à passer outre l'avertissement, et se connecter tout de même, l'utilisateur prenant alors seul la responsabilité de la confiance envers le certificat concerné.

Il est possible à un certificat électronique de couvrir plusieurs noms DNS. La norme X.509 v3 ajoute un champ *subjectAltName* qui permet à un certificat de préciser plusieurs noms DNS, et de préciser les jokers (wildcards). Cependant, cela est peu pratique, voire impossible à déployer, par exemple lorsque l'on ne connaît pas d'avance la liste des noms de domaines qui seront hébergés sur la même adresse IP.

L'hébergement virtuel permet à des noms DNS multiples d'être hébergés sur un seul serveur (généralement un serveur web) sur la même adresse IP. Pour cela, le serveur utilise le nom de domaine présenté par le client dans le cadre du protocole (par exemple l'entête Host: du protocole HTTP). Cependant, en HTTPS, le *handshake* TLS advient avant que le serveur n'aie reçu d'entêtes HTTP. Il n'est donc pas possible que le serveur présente le certificat correspondant au nom de domaine demandé.

En pratique, cela signifie qu'un serveur HTTPS ne peut servir qu'un seul domaine (ou un petit groupe de domaine si on utilise X.509 v3) sur une adresse IP donnée. Assigner des adresses IP supplémentaires pour chaque site augmente le coût d'hébergement, car les assignation d'adresses IP doivent être justifiées auprès du registre Internet régional et que la pénurie d'adresses IPv4 augmente le problème. Conséquence de cela, les sites web ne sont pas invités à utiliser des communications sécurisées.

En quoi SNI résout ce problème ?

L'extension du protocole TLS, nommée SNI (Server Name Indication), répond à ce problème en envoyant le nom DNS du domaine dans le cadre de la négociation TLS[2]. Cela permet au serveur de choisir le domaine virtuel plus tôt et donc de présenter au navigateur le bon certificat contenant le bon nom DNS. Par conséquent, avec des clients sachant utiliser SNI, une adresse IP unique peut être utilisée pour servir un groupe de domaines pour lequel il ne serait pas facile d'obtenir un certificat commun.

Déploiement

En 2004, un correctif ajoutant TLS/SNI à OpenSSL a été créé par le projet EdelKey[3]. En 2006, ce correctif a été inclus dans la branche principale de OpenSSL, et porté sur l'ancienne version de OpenSSL 0.9.8 en 2007.

Pour pouvoir implémenter correctement SNI, l'application doit en avoir connaissance, et passer le nom de domaine à sa bibliothèque TLS. La complication augmente quand on sait que de nombreux logiciels client ou serveur utilisent TLS sous forme d'un composant extérieur (une bibliothèque ou un greffon), dépendant du système d'exploitation. En 2013, la plupart des navigateurs et bibliothèques TLS implémentent correctement SNI, mais un grand nombre d'utilisateurs ont toujours une combinaison d'application et de logiciel client incompatibles avec SNI [4]

Références

1. section de 3.1 de la norme RFC4366 qui décrit les extensions du TLS (https://tools.ietf.org/html/rfc4366#section-3.1)
2. {en} "TLS Server Name Indication" (http://journal.paul.querna.org/articles/2005/04/24/tls-server-name-indication/). Paul's Journal.
3. {en} http://www.edelweb.fr/EdelKey/
4. Statistiques de navigateurs (http://www.w3counter.com/globalstats.php) en Juillet 2013, 20 % des utilisateurs sont sous Windows XP, dont le navigateur Internet Explorer n'implémente pas SNI à cause de la bibliothèque TLS de Windows XP.