RFC 4255 : Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 avril 2006. Dernière mise à jour le 3 septembre 2007

Date de publication du RFC : Janvier 2006

https://www.bortzmeyer.org/4255.html

On le sait, le protocole SSH dépend, pour la sécurité du client, d'une vérification de la clé publique du serveur, lors de la première connexion. Cette vérification étant rarement faite, notre RFC propose un moyen de l'automatiser via le DNS.

Voici une session SSH typique, la première fois qu'on se connecte à `foobar.example.org` :

```
% slogin foobar.example.org
The authenticity of host 'foobar.example.org (172.19.1.33)' can't be established.
RSA key fingerprint is 38:e8:5b:3f:25:41:e2:ca:fa:4e:71:38:b8:db:f0:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'foobar.example.org,172.19.1.33' (RSA) to the list of known hosts.
Last login: Sun Apr  2 17:45:12 2006 from ludwigvi.sources.org
NetBSD 3.99.17 (XEN3_U) #5: Sat Mar 25 19:01:14 CET 2006
```

Comme je ne m'étais jamais connecté depuis cette machine, la clé publique du serveur (dont l'**empreinte**, le résumé par une fonction de hachage cryptographique, est `38:e8:5b:...`) n'était pas stockée (sur Unix, dans `/.ssh/known_hosts`). Comme SSH est sensible aux attaques d'un **intermédiaire**, une machine qui intercepte la requête du client et prétend être le serveur, il demande une vérification manuelle.

En théorie, je devrais vérifier (par téléphone, par échange d'empreintes signées avec PGP, etc) la clé publique du serveur. En pratique, quasiment personne ne le fait. Comme souvent en cryptographie, on a des techniques formidables et un facteur humain qui fait perdre toute la sécurité qu'aurait pu donner la cryptographie.

Notre RFC propose donc une solution : de distribuer les clés publiques des serveurs SSH via le DNS. Comme celui-ci, par défaut, n'offre aucune sécurité, cela implique évidemment DNSSEC.

Notre RFC normalise donc un nouveau type de données, le SSHFP, qui stocke les empreintes des clés publiques. Par exemple :

```
foobar.example.org.  SSHFP 2 1 38e85b3f2541e2cafa4e7138b8dbf0d1
```

me permettra de vérifier que je me suis bien connecté vers le bon serveur.

À l'heure d'aujourd'hui, si on veut supprimer cette agaçante question affichée plus haut, il faut utiliser un client SSH comme OpenSSH, dans une version très récente, et activer l'option `VerifyHostKeyDNS` dans le fichier de configuration. Pour publier les clés dans le DNS, le plus simple est sans doute d'utiliser `ssh-keygen -r $DOMAIN` ou bien le programme sshfp <http://www.xelerance.com/software/sshfp/>. (Merci à Phil Regnauld pour les détails pratiques. sshfp devrait être remplacé par hash-slinger <http://people.redhat.com/pwouters/hash-slinger/>.)

Si vous voulez voir des enregistrements SSHFP en vrai, il en existe un sur `anoncvs.netbsd.org`, le serveur CVS anonyme du projet NetBSD :

```
% dig SSHFP anoncvs.netbsd.org
...
;; ANSWER SECTION:
anoncvs.netbsd.org. 86400 IN SSHFP 1 1 198C34A92FC0B2AB1DA52B688C2F191D2D960C09
```

(Ou bien, avec le DNS Looking Glass <https://www.bortzmeyer.org/dns-lg.html>, en <https://dns.bortzmeyer.org/anoncvs.netbsd.org/SSHFP>.)

Quelques détails pratiques sur l'utilisation de SSHFP figurent dans « "*How to get OpenSSH to see DNSSEC AD flags on SSHFP lookups with glibc*" <http://bd.hauke-lampe.de/dnssec/how-to-get-dnssec-a html> ». Un autre client SSH qui a SSHFP est GateOne <https://github.com/liftoff/GateOne> (voir la discussion <https://github.com/liftoff/GateOne/issues/12>). Sur leur sécurité avec OpenSSH, voir « "*On the safety of SSHFP records*" <http://fanf.livejournal.com/118060.html> ». Sur leur production et leur publication lorsqu'on a beaucoup de machines, voir « "*On collecting SSH host keys for SSHFP DNS records*" <http://jpmens.net/2012/02/01/on-collecting-ssh-host-keys-for-ssh > ». Sur les limites et certains problèmes de cette technique, voir, du même auteur, « "*VerifyHostKeyDNS=maybe*" <http://jpmens.net/2011/02/18/verifyhostkeydnsmaybe/> ». Un exemple de publication est « "*SSHFP tutorial : how to get SSHFP records, DNSSEC, and VerifyHostKeyDNS=yes to work*" <http://fanf.livejournal.com/130577.html> » de Tony Finch.