Le rituel des sessions de signature de clés PGP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 août 2007

`https://www.bortzmeyer.org/pgp-session.html`

Année après année, le rituel ne change pas : les sessions de signature réciproque des clés PGP suivent toujours le même cérémonial, inattendu dans une communauté de "*geeks*".

PGP repose sur la notion de **réseau de confiance**. On signe les clés des gens dont on a pu vérifier l'identité et ils signent la vôtre. De proche en proche, on peut en général trouver le chemin `<http://www.kim-minh.com/#a-2>` qui mène de la clé d'une personne à la clé de n'importe quelle personne (au fait, l'**ID** de ma clé est `0xCCC66677` et son empreinte est `F42D 259A 35AD BDC8 5D9B FF3E 555F 5B15 CCC6 6677`).

Mais cela suppose qu'on se rencontre dans le monde réel pour vérifier les identités. C'est le rôle des sessions PGP ou "*key signing parties*". Le principe ? Prenons l'exemple de celle qui s'est tenue à la réunion IETF 69 à Chicago en juillet 2007 (mais toutes ces sessions se ressemblent).

Les participants envoient préalablement leur clé publique à l'organisateur. Il calcule les **empreintes** des clés (typiquement avec `gpg --fingerprint`) et les imprime. Lors de la session, il distribue le papier à tout le monde. Les clés elles-mêmes ont été recupérées sur le réseau et importées dans le trousseau (typiquement avec `gpg --import`). L'organisateur lit successivement chaque empreinte et la personne à qui appartient la clé confirme que c'est la bonne empreinte. On sait alors que les clés distribuées sont bien celles envoyées par les participants.

Il reste à vérifier les identités des participants. Un algorithme simple serait que chacun vérifie successivement l'identité de chacun. C'est ainsi qu'on procédait autrefois. Mais cet algorithme est en $o(n\hat{\}2)$. On utilise désormais un algorithme parallèle. Les participants sont rassemblés en deux rangs qui se font face à face, chacun vérifie l'identité de son vis-à-vis. Puis on se décale d'un cran, avec passage des personnes d'extrémité dans l'autre rang, et on recommence (en essayant de ne pas éclater de rire devant le joli ballet que ça représente).

Ah, au fait, comment vérifie t-on l'identité ? Typiquement par un document officiel d'identité. C'est loin d'être parfait car je ne sais pas à quoi est censé ressembler un permis de conduire de l'Illinois, et je suis perplexe devant les cartes d'identité japonaises en jolis caractères. Mais c'est mieux que rien.

On peut alors signer les clés sur son portable (typiquement avec `gpg --sign-key`), ou bien une fois rentré chez soi, et les envoyer ensuite au titulaire, ou à un serveur de clés public. La première méthode est recommandée, car elle permet de valider également l'adresse électronique indiquée dans la clé.

Chaque étape du rituel a été minutieusement étudiée. N'oublions pas que les participants n'ont aucune raison de faire confiance à l'organisateur et qu'il faut donc que tout le processus soit **transparent**. Pas question, donc, que seul l'organisateur fasse la vérification des identités.

Voici les instructions qui avaient été envoyées aux participants pour la session PGP en question : <http://www1.ietf.org/mail-archive/web/ietf-announce/current/msg03926.html>. Il y a bien sûr d'autres façons de faire <http://www.keysigning.org/methods/sassaman-projected>.