RFC 5656 : Elliptic-Curve Algorithm Integration in the Secure Shell Transport Layer

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 15 décembre 2009

Date de publication du RFC : Décembre 2009

https://www.bortzmeyer.org/5656.html

Les algorithmes de cryptographie de la famille des courbes elliptiques prennent de plus en plus d'importance, concurrençant les traditionnels RSA et DSA. Ce RFC spécifie l'utilisation de certains de ces algorithmes dans le protocole SSH.

Il y a déjà plusieurs RFC qui utilisent les courbes elliptiques : les RFC 4050 [1], RFC 4492, RFC 5349, etc. SSH n'est donc pas, et de loin, le premier protocole IETF à en bénéficier. Mais il est plus répandu et l'intégration des courbes elliptiques leur donnera donc une bien meilleure exposition.

Outre des avantages techniques comme des clés de faible taille (voir la section 1 du RFC pour des chiffres précis), l'intérêt des courbes elliptiques est que, compte-tenu du risque toujours existant de percées soudaines en cryptanalyse, il est prudent de garder « plusieurs fers au feu ». Si une nouvelle méthode de factorisation en nombres premiers apparait, menaçant RSA, la disponibilité d'algorithmes utilisant les courbes elliptiques fournira une solution de repli.

Notre RFC 5656 étend donc SSH, tel qu'il est spécifié dans les RFC 4251 et RFC 4253. Pour davantage d'information sur les courbes elliptiques, il renvoie à « "*SEC 1 : Elliptic Curve Cryptography*" <http://www.secg.org/download/aid-780/sec1-v2.pdf> » et « "*SEC 2 : Recommended Elliptic Curve Domain Parameters*" <http://www.secg.org/download/aid-386/sec2_final.pdf> ».

La section 3 de notre RFC attaque les détails pratiques de l'algorithme ECC. Le format des clés (section 3.1), l'algorithme utilisé pour la signature (nommé ECDSA), avec la fonction de hachage SHA-2 et l'encodage de la signature y sont normalisés.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4050.txt

Un protocole d'échange de clés utilisant les courbes elliptiques, ECDH, occupe la section 4. Un autre, ECMQV, figure en section 5 (mais seul ECDH est obligatoire dans SSH).

Le tout est enregistré dans le registre des paramètres SSH <https://www.iana.org/assignments/ssh-parameters>, tel que décrit en section 6. Comme le terme de « courbes elliptiques » désigne une famille, pas un seul algorithme, il faut ensuite préciser l'algorithme exact utilisé. Trois courbes elliptiques sont ainsi mise en avant, nommées `nistp256`, `nistp384` et `nistp521`. Un mécanisme utilisant l'OID de la courbe est prévu pour celles sans nom (section 6.1). Ces courbes peuvent être utilisées pour ECDSA (section 6.2), ECDH (section 6.3) et ECMQV (section 6.4). Ainsi, le nom complet de l'algorithme utilisé pour ECDSA avec la courbe `nistp256` est `ecdsa-sha2-nistp256`.

Comment vont faire les mises en œuvres de SSH avec ces nouveaux algorithmes et interopéreront-elles avec les anciennes ? Oui, répond la section 8 : le protocole SSH a toujours prévu un mécanisme de négociation des algorithmes utilisés et les programmes ignorent simplement les algorithmes inconnus (section 8.2). La section 8 couvre d'autres problèmes concrets comme les performances des nouveaux algorithmes (en général meilleure que celle de RSA ou DSA, en raison de la taille plus faible des clés).

Une très riche section 9 analyse en détail les caractéristiques de sécurité des courbes elliptiques et leur résistance à la cryptanalyse. D'abord, il faut bien retenir que « courbes elliptiques » désigne une famille, pas un seul algorithme. Certains membres de la famille sont plus vulnérables que d'autres, par exemple à des attaques comme la descente de Weil <http://www.cs.bris.ac.uk/~nigel/weil_descent.html>. Il faut donc considérer avec prudence une courbe qui n'est pas listée dans la section 10 (qui résume la liste des courbes utilisées pour SSH).

Ppur les courbes ainsi spécifiées, il n'existe pas actuellement d'autres attaques que la force brute. Les seules exceptions concernent les algorithmes pour ordinateurs quantiques (comme celui de Shor). Or, ces ordinateurs ont déjà le plus grand mal, à l'heure actuelle, à additionner 2 + 2 et le RFC note qu'il est peu probable qu'ils deviennent une menace réelle dans les prochaines années. Les lois de la physique et celle de l'ingéniérie ne sont pas faciles à faire plier !

La section 10 rassemble les caractéristiques des courbes obligatoires (section 10.1) et recommandées (section 10.2), donnant pour chacune l'OID attribué. Toutes sont dérivées de normes NIST. Ainsi, `nistp256` a l'OID `1.2.840.10045.3.1.7`. Tous ces algorithmes sont enregistrés dans le registre SSH <https://www.iana.org/assignments/ssh-parameters>, suivant le RFC 4250.

La mise en œuvre la plus répandue de SSH, OpenSSH, a intégré ces algorithmes à courbes elliptiques sa version 5.7 <http://marc.info/?l=openssh-unix-dev&m=129583391525629&w=2dans>, livrée en janvier 2011 (voir un résumé en <http://pthree.org/2011/02/17/elliptic-curve-cryptograph>). Il y a quelques années, un interview d'un des développeurs <http://www.securityfocus.com/columnists/375> indiquait qu'un des problèmes était celui des brevets logiciels (il parlait aussi de l'absence de normalisation, ce qui n'est plus vrai avec la sortie de notre RFC).