Choix cryptographiques d'OpenBSD

Bruno Martin
Bruno.Martin@unice.fr

29 janvier 2016

Nombre d'étudiants souhaités : 1

Description du sujet

Le système d'exploitation `OpenBSD` a fait un certain nombre de choix inhabituels quant à ses composant cryptographiques. Les développeurs de ce système sont à l'initiative de la conception d'utilitaires largement distribués dans le monde `UNIX` ou `linux` comme `OpenSSH` ou de librairies comme `LibreSSL` qui propose une alternative à `openSSL`. L'étudiant, doté d'une certaine autonomie, devra comprendre le fonctionnement du chiffre `ChaCha20` et de son utilisation en conjonction à `Poly1305` pour le calcul d'un MAC comme proposition de standard dans la librairie `TLS`. Une petite étude de sa sécurité pourra être faite selon le temps disponible.

Lieu

Pas de possibilité de bureau.

Prérequis

Avoir de bonnes notions de mathématiques discrètes, d'informatique fondamentale et un certain goût pour l'algèbre.

Informations complémentaires

- `http://tools.ietf.org/html/draft-agl-tls-chacha20poly1305-04`
- `http://www.openbsd.org/papers/rubsd2013-mikeb-en.pdf`
- D.J. Bernstein, *The Poly1305-AES Message-Authentication Code*, FSE, LNCS 3557, Springer Verlag, 2005