Avec Riffle, le MIT conçoit une alternative au réseau Tor

Les réseaux d'anonymisation comme Tor ou I2P ne sont pas sans failles. Des chercheurs de l'institut de technologie du Massachusetts (MIT) et de l'École Polytechnique Fédérale de Lausanne (EPFL) ont donc planché sur une alternative : Riffle. L'outil agrège plusieurs techniques cryptographiques pour mieux protéger l'anonymat de ses utilisateurs. Et ce tant qu'il reste un serveur non compromis.

Comme d'autres, Riffle utilise une série de serveurs (mixnet) qui enrobent un message dans plusieurs couches de chiffrement. Mais, à la différence de Tor (le *« routeur oignon »*), chaque serveur du mixnet du MIT et de l'EPFL permute l'ordre de réception des messages avant de les transmettre à un autre serveur, et ainsi de suite. Pour un intrus, il devient donc plus difficile de lier les flux entrants et sortants. De plus, Riffle vérifie chaque connexion initiale sur tous les serveurs du réseau (*« verifiable shuffle »*), et s'appuie également sur un procédé d'authentification pour vérifier le reste.

Dix fois plus rapide ?

C'est grâce à la combinaison de ces techniques déjà connues, que Riffle protégerait mieux l'anonymat de ses utilisateurs, et la sécurité de leurs données, que ne le font ses prédécesseurs. Par ailleurs, le transfert d'un fichier volumineux entre utilisateurs se ferait dix fois plus rapidement qu'avec les réseaux d'anonymisation existants…

Les chercheurs du MIT et de l'EPFL en feront la démonstration lors du Privacy Enhancing Technologies Symposium (PETS) qui aura lieu à Darmstadt, en Allemagne, du 19 au 22 juillet 2016.

Lire aussi :

Un gourou du chiffrement lance PrivaTegrity, une alternative à Tor
Hornet, un réseau d'anonymisation à la mode Tor en haut débit
Vuvuzela, une messagerie qui fait du bruit pour garantir l'anonymat