L'Inria et Microsoft publient une implémentation de référence de TLS

A l'occasion du Paris Open Source Summit, qui se tient en ce moment dans la capitale, Microsoft et l'Inria, qui, depuis le milieu des années 2000, ont ouvert un laboratoire commun à Saclay, sur le campus de l'Ecole Polytechnique, dévoilent une implémentation sécurisée de TLS, le protocole de sécurisation des échanges le plus répandu sur Internet. Un protocole notamment employé dans le HTTPS, qui sécurise une large part des communications sur le Web.

Ce sont en fait deux jeux de code (MiTLS et flexTLS) que les deux partenaires ont **placés en Open Source (sous licence Apache)**, afin d'aider les chercheurs et experts en sécurité à créer leur propre implémentation sécurisée de TLS. Le premier code est donc une implémentation « *vérifiée* » de TLS. Le second offre un outil permettant de tester les implémentations du protocole. Ces résultats font partie des travaux que mène le laboratoire de Saclay sur la conception de systèmes dont il possible de prouver mathématiquement la sécurité.

C'est cette même équipe de chercheurs issus des labs de Microsoft et de l'Inria qui a mis au jour, ces derniers mois, les failles Triple Handshake, Freak et Logjam, des failles se logeant dans TLS. « *Nous ne les avons pas trouvées parce nous cherchions des attaques contre TLS*, explique aujourd'hui Cédric Fournet, un chercheur de Microsoft dans un billet de blog. *C'était un effet de bord de nos recherches.* » Par ailleurs, l'éditeur affirme que les recherches menées par ses équipes, en partenariat avec l'Inria, influencent l'évolution du protocole TLS, dont la prochaine version est attendue en 2016. « *Pour moi, c'est même l'aspect essentiel* », dit Karthikeyan Bhargavan, un des chercheurs de l'Inria impliqués sur MiTLS.

La sécurité du chiffrement mise à l'épreuve

Lancé au départ comme un projet de recherche de court terme visant à évaluer comment des implémentations académiques de TLS pouvaient être exploitées sur des systèmes en production, MiTLS s'est transformé en projet pluri-annuel, du fait de l'importance des failles découvertes.

Ces derniers mois, de nombreuses recherches ont montré la fragilité des protocoles de sécurisation des échanges sur Internet. Ou de leur implémentation. Ainsi, en octobre, un des algorithmes centraux utilisés pour le chiffrement sur Internet, SHA-1, était jugé insuffisamment sécurisé contre des attaques par force brute. Un peu plus tôt dans l'année, une étude pointait la faiblesse d'un algorithme d'échange de clefs (Diffie-Hellman), utilisé dans les principaux protocoles de sécurisation d'Internet. Deux études auxquelles avait également participé l'Inria. Plus récemment, une étude de l'université de Boston a montré comment les failles de NTP, le protocole de synchronisation qui permet de caler l'horloge locale d'ordinateurs sur une référence, peuvent être exploitées pour mettre en péril des certificats TLS.

A lire aussi :

Le chiffrement source de multiples failles de sécurité

Paris Open Source Summit : fluctuat nec mergitur

Crédit photo : isak55 / Shutterstock