L’audit du logiciel de chiffrement TrueCrypt est relancé

Les développements du logiciel de chiffrement de disque **TrueCrypt** avaient été interrompus après une annonce de ses développeurs sur la vulnérabilité de l’outil, en mai 2014. Le projet d’audit initié à l’automne 2013, après les premières révélations d’Edward Snowden sur la surveillance de masse menée par la NSA américaine, avait donc été suspendu. Mais l’un des initiateurs de l’audit, le cryptologue **Matthew Green**, a annoncé le 18 février 2015 l’ouverture prochaine d’une **seconde phase** portant sur la crytographie de la version 7.1a de TrueCrypt, fiable d’après ses promoteurs.

Une cryptanalyse de TrueCrypt 7.1a va débuter

Le projet d’audit de TrueCrypt a bénéficié d’un financement participatif de **70 000 dollars**. L’entreprise **iSEC Partners** a été chargée de la première phase (« Open Crypto Audit ») centrée sur le code du noyau, le programme d’amorçage et le pilote du système de fichier. Elle a été finalisée il y près d’un an. Le rapport du 14 février 2014 ne fait état d’aucun souci majeur dans le code source, mais l’annonce de la fin des développements au printemps de la même année a chamboulé l’audit…

Finalement, après des mois d’hésitation, les initiateurs du projet ont trouvé un plan B. Pour la seconde phase de l’audit, les consultants de **Cryptography Services (NCC Group)** ont été engagés afin assurer une cryptanalyse de la version originale de TrueCrypt 7.1a, qui sert de base à de nouveaux *forks*. Les donateurs du projet devront toutefois encore patienter pour en savoir plus. Le *« calendrier de réalisation de l’audit n’est pas encore »* précisé, a indiqué par voie de communiqué Cryptography Services.

Lire aussi :
CipherShed relance le projet TrueCrypt
Un malware résistant à un formatage de disque dur : l’œuvre de la NSA ?