TrueCrypt finalement mieux sécurisé que prévu

TrueCrypt est malaimé. Abandonné par ses développeurs pour des suspicions de failles, il a depuis fait l'objet de diverses alertes de sécurité.

La branche recherche IT de **l'Institut Fraunhofer** vient remettre les choses à leur place. À cet effet, un audit complet a été réalisé sur le code source de TrueCrypt, à la demande du **BSI**, le bureau fédéral allemand dédié à la sécurité informatique. Le rapport de cet audit peut être téléchargé depuis cette page web.

En résumé, TrueCrypt est bien plus sécurisé qu'il n'y paraît. Le dernier problème en date, relevé par le **Project Zero de Google**, permet une escalade de privilèges via TrueCrypt. Un souci touchant en fait tous les pilotes système, et qui ne permet pas ici d'accéder à la version en clair de données chiffrées.

Certes, un virus présent sur la machine pourra accéder aux informations stockées, puisque les données sont visibles sous leur forme déchiffrée une fois l'utilisateur connecté. TrueCrypt propose toutefois **un excellent niveau de protection lorsque le volume chiffré n'est pas monté**. D'autres failles ont été trouvées dans TrueCrypt, mais ne sont pas exploitables dans la pratique.

Une offre trop bien sécurisée ?

Des résultats qui ne font que renforcer l'idée selon laquelle le développement de ce projet n'a pas été abandonné pour cause de sécurité défaillante, mais pour la raison inverse, le niveau de sécurité des données apporté par TrueCrypt posant **un sérieux problème** aux forces de sécurité souhaitant accéder au contenu d'un ordinateur.

Un petit souci a toutefois été noté dans la génération des nombres aléatoires. Ce bug ne sera pas corrigé dans TrueCrypt, puisque son développement a été stoppé, mais des solutions comme **VeraCrypt** ont depuis repris le flambeau.

À lire aussi :
L'audit de TrueCrypt ne décèle pas de backdoor délibérée
TrueCrypt baisse le rideau sur le chiffrement des données
CipherShed relance le projet TrueCrypt