TrueCrypt

TrueCrypt	
Développeur	TrueCrypt Foundation
Première version	2 février 2004
Dernière version	7.2 (28 mai 2014)
État du projet	Abandonné par ses auteurs originaux, géré par d'autres logiciels.
Écrit en	C++, C et assembleur/WxWidgets
Environnements	Multiplate-forme
Langues	Multilingue
Type	Chiffrement de disque
Licence	TrueCrypt Collective License (http://www.truecrypt.org/license.php)
Site web	www.truecrypt.org (http://www.truecrypt.org)

TrueCrypt est à la fois un format de système de fichier chiffré, notamment géré par Linux dans son module dm-crypt depuis la version 3.13[1, 2], et un logiciel de chiffrement à la volée fonctionnant sur Microsoft Windows XP/2000/2003/Vista (32-bit et 64-bit)/7, Mac OS X et GNU/Linux, ce dernier étant à l'origine de ce système de fichier.

TrueCrypt est gratuit et son code source est disponible bien qu'il n'ait pas le statut de logiciel libre. Le logiciel tc-play, pour Linux, est par contre un logiciel libre sous Licence BSD, dont la version 1.0 est sortie en mai 2013 et qui est compatible avec TrueCrypt[3].

TrueCrypt permet de créer un disque virtuel chiffré (*volume TrueCrypt*) contenu dans un fichier et de le monter comme un disque physique réel. TrueCrypt peut aussi chiffrer une partition entière ou un périphérique, par exemple une disquette ou une clé USB. Le chiffrement est automatique, en temps réel et transparent.

Tout ce qui sera stocké dans un volume TrueCrypt sera entièrement chiffré, y compris noms de fichiers et répertoires. Les volumes TrueCrypt se comportent, une fois montés, comme des disques durs physiques. Il est ainsi possible, par exemple, d'en réparer le système de fichiers avec *Check Disk*, ou de défragmenter les volumes créés par TrueCrypt.

TrueCrypt n'est plus maintenu par ses auteurs originaux depuis le 28 mai 2014, mais plusieurs alternatives reprenant le code du logiciel (*forks*), dont VeraCrypt, ont vu le jour depuis, ainsi que différents projets d'hébergement des anciennes versions de TrueCrypt.

Sommaire

Historique

Origines de TrueCrypt

TrueCrypt est basé sur le logiciel E4M **(en)** (Encryption for the Masses (chiffrement pour les masses)). E4M était un logiciel gratuit open source très populaire de chiffrement à la volée (*on the fly encryption*, ou OTFE) dont la première version date de 1997. Ce logiciel a cessé d'être maintenu en 2000 quand son auteur, Paul Le Roux, a commencé à développer une version payante d'OTFE. La première version de TrueCrypt a été dévoilée le 2 février 2004. C'était à cette époque le seul logiciel de chiffrement à la volée open source disponible pour Windows XP et permettant le déni plausible.

La version 1.0 fonctionnait sous W98/ME et 2000/XP. La version 1.0a a supprimé la prise en charge de W98/ME, l'auteur du pilote pour W98 n'ayant pas donné l'autorisation d'utiliser son code dans des projets dérivés d'E4M. Remarque : Les auteurs de Scramdisk **(en)** et d'E4M ont échangé leurs codes respectifs (l'auteur de Scramdisk a fourni le pilote pour W9x, et l'auteur d'E4M a fourni le pilote pour WNT), permettant la création ultérieure du partagiciel Scramdisk NT. Il existe également des controverses quant à l'origine de certaines parties du code, l'auteur d'E4M ayant apparemment récupéré du code sous licence propriétaire appartenant à un de ses employeurs[4].

Arrêt du développement

Le 28 mai 2014, le site officiel de TrueCrypt annonce la fin du développement en prétextant la fin du support de Windows XP par Microsoft. Il affirme par ailleurs que le logiciel est compromis et demande d'utiliser à la place le logiciel commercial BitLocker de Microsoft, pourtant connu pour fournir des portes dérobées aux services de renseignement[5] et ne permettant pas une interopérabilité (ne fonctionnant que sous Windows) comme le permet TrueCrypt. Le site web renvoie vers la version 7.2 qui révèle, après un audit rapide par la communauté informatique, qu'il est impossible de chiffrer de nouvelles données, tout en signalant par une fenêtre surgissante que TrueCrypt est compromis. La communauté informatique soupçonne que les développeurs ont été piratés voire contactés par les services de renseignement[6, 7, 8, 9].

Selon Gibson Research Corporation **(en)**, les développeurs anonymes de TrueCrypt n'ont pas souhaité poursuivre le développement après une dizaine d'années consacrées au sujet, car "il n'y avait plus d'intérêt" à sa poursuite[10]. Le projet initial visait à l'époque à combler le manque d'outil de chiffrement en standard sur Windows XP[10].

Reprises du projet

Un site web situé en Suisse, truecrypt.ch[11], affirme vouloir relancer le projet, en tirant les leçons de la fin énigmatique du projet initial. Le projet sera situé en Suisse, pour se soustraire à l'influence des services de renseignement américains, l'équipe de développement ne sera plus anonyme et le projet sera « réellement open-source ».

Il existe également des projets visant à héberger les anciennes versions complètes et à soutenir le développement des *forks* :

- CipherShed **(en)**, *fork* complet de TrueCrypt[12].
- Truecrypt.ch, s'occupe d'héberger les anciennes versions complètes et soutient le développement de *CipherShed*[12, 13]. Le site est hébergé en Suisse, dans le but d'éviter la possibilité d'une éventuelle intervention ou l'ingérence des services de renseignement ou de la police fédérale des États-Unis, comme cela pourrait être le cas dans d'autres pays.
- L'équipe d'audit de sécurité de l'Université Concordia au Canada, qui continue à distribuer les anciennes versions complètes.
- VeraCrypt

Fonctionnalités

Présentation

TrueCrypt se destine principalement au stockage chiffré des données, non à leur transmission de façon sécurisée comme peut le faire PGP. TrueCrypt ne gère pas le problème de la transmission de la clef (le mot de passe) qui doit être transmis sur un autre canal par Diffie-Hellman ou similaire en cas d'envoi d'un volume contenant des données à un destinataire. La taille des volumes (de quelques Mio à plusieurs Gio/Tio) peut dans certains cas ne pas se prêter commodément à un transport autre que physique.

En tant que logiciel de chiffrement à la volée, TrueCrypt ne protège pas d'éventuelles failles de sécurité. Il convient donc une fois un volume ouvert (on dit aussi « monté ») de vérifier les droits d'accès à ce disque (chevaux de Troie, droits utilisateurs, partage réseau...) tout comme de l'accès physique à la machine.

Il ne s'agit pas là de failles de sécurité : Truecrypt n'a pas pour objet de protéger contre des accès une fois un volume ouvert.

Une analogie serait un coffre-fort dans des bureaux. Le coffre fermé, seuls ceux qui connaissent la clef peuvent l'ouvrir, mais une fois ouvert tout le monde peut accéder à son contenu. Il convient donc de protéger l'accès au coffre quand il est ouvert et de veiller avec qui partager la clef.

Une fois ce principe acquis, Truecrypt fait preuve d'une solidité intéressante[14]. La version 6.0a a d'ailleurs été qualifiée au niveau élémentaire le 17 août 2009 par l'ANSSI (durée de validité d'un an)[15].

TrueCrypt offre deux niveaux de dissimulation des données :

1. Rien ne permet d'identifier formellement un volume TrueCrypt. Il s'agit concrètement d'un fichier de taille quelconque, de nom quelconque avec une extension quelconque (le contenu des volumes TrueCrypt ne peut pas être distingué de données aléatoires et rien ne permet de les relier à TrueCrypt. Leur taille est libre, ils peuvent porter le nom.extension décidé par l'utilisateur). Toutefois, le logiciel propose d'utiliser l'extension .tc afin d'ouvrir TrueCrypt avec un simple double-clic sur ceux-ci. Attention au cas d'une partition ou d'un volume entier chiffré : il est si peu distinguable d'un volume non initialisé ou effacé que Windows peut par exemple en proposer le formatage à l'utilisateur !
2. Au même titre que FreeOTFE, une des fonctionnalités les plus notables est qu'il possède deux niveaux de chiffrement imbriquables, permettant ainsi le déni plausible, ce qui peut s'avérer utile dans le cas où l'utilisateur se voit requis (par la force, par la loi...) de révéler son mot de passe : il est ainsi possible de créer un second volume chiffré caché à l'intérieur du volume principal (accessible à l'aide de son propre mot de passe et non accessible à l'aide du mot de passe du volume principal).

Les algorithmes de chiffrement mis en œuvre dans TrueCrypt comprennent AES, Serpent et Twofish. Il est également possible d'utiliser en cascade différents algorithmes comme AES+Twofish+Serpent.

Les versions 5.0 et ultérieures du logiciel utilisent les algorithmes de chiffrement en mode XTS, plus fiable que le mode LRW, lui-même plus sûr que le mode CBC.

TrueCrypt permet également :

- l'utilisation en application portable, sur clef USB par exemple, c'est-à-dire sans installation sur l'ordinateur de l'utilisateur. Cette utilisation portable nécessite tout de même d'être connecté avec un compte Administrateur pour pouvoir monter les pilotes (Windows).
- de créer des volumes dynamiques sur des disques NTFS. Ces volumes grossissent pour s'adapter aux données qu'y stocke l'utilisateur, jusqu'à une taille maximum fixée par lui. Utiliser de tels volumes fait chuter les performances et la sécurité, comme expliqué dans la documentation du logiciel.
- de changer le mot de passe du volume ou son *keyfile* sans perdre les données.
- de restaurer les en-têtes de volume :
  - Cela pourrait être utile en cas d'écrasement physique ayant occasionné un dommage sur l'en-tête du volume ;
  - Restaurer un ancien en-tête de volume permet de repartir avec le mot de passe qui était valide avec cet en-tête de volume.

Volume caché

TrueCrypt implémente, en théorie, le déni plausible en imbriquant deux niveaux de chiffrement. Même si l'utilisateur est forcé de révéler le mot de passe du volume principal, rien ne permet ensuite de prouver l'existence ou la non-existence du volume caché à l'intérieur du volume principal, sachant que le volume éventuellement imbriqué apparaîtra comme une suite de caractères aléatoires indiscernables qui remplissent l'espace disponible du premier volume.

En effet, l'ensemble du volume étant chiffré, y compris l'espace vide, les données et pointeurs chiffrés par un autre mot de passe ne sont pas discernables de ce dernier. Une différence importante entre l'espace réservé et l'espace apparemment utilisé peut éventuellement éveiller les soupçons, mais restera inattaquable si les dates des fichiers du premier volume sont récentes : il est normal qu'un volume récent ne soit encore que peu rempli. L'utilisation la plus classique est d'utiliser le volume principal pour placer des fichiers pseudo-sensibles (photos personnelles, copies de pièces administratives...) leurrant celui qui forcerait à révéler le mot de passe principal. Les dossiers réellement sensibles sont placés dans un volume imbriqué.

Un volume caché est utilisé de la même manière qu'un volume standard de TrueCrypt. Il peut être créé dans n'importe quel type de volume de TrueCrypt, c'est-à-dire un volume fichier ou une partition (la seconde exigeant des privilèges d'administrateur).

Jusqu'aux versions 4.x, un volume caché pouvait seulement être créé dans un volume principal en FAT32. Le système de fichiers NTFS stocke en effet diverses données dans le volume entier (par opposition au système FAT). Quant à lui, lorsque le volume principal est un fichier (et non une partition ou un périphérique), il peut être stocké sur n'importe quel système de fichiers. Depuis les versions 5.0 et ultérieures, le volume caché peut être hébergé au sein d'un volume de type NTFS (dans ce cas, la taille du volume caché ne pourra excéder la moitié de celle du volume externe). Dans tous les cas, il faudra veiller au remplissage du volume normal afin de ne pas écrire sur le volume caché. Exemple, dans un volume de 20 Gio avec un volume caché de 5 Gio, il ne faut pas remplir le volume normal à plus de 15 Gio.

TrueCrypt dispose d'une option de protection des volumes cachés lors de l'ouverture d'un volume normal. Cette option permet d'éviter de remplir trop le volume normal et d'écrire ainsi sur le volume caché mais nécessite les clefs des deux volumes.

Algorithmes supportés

TrueCrypt supporte les algorithmes de chiffrement suivants :

- AES-256
- Serpent (256-bit)
- Twofish (256-bit).

et les fonctions de hachage cryptographiques suivantes :

- RIPEMD-160
- SHA-512
- Whirlpool.

Accélération matérielle

TrueCrypt 7.0a sait utiliser l'accélération matérielle au chiffrement/déchiffrement (AES) des processeurs Intel qui en disposent (AES-NI). Par exemple une mesure sur le Intel Core i5-2500K montre qu'activer cette accélération quadruple la vitesse de chiffrement en la portant à 2,3 Go/s[16].

Sécurité

Attaques

Truecrypt a été la cible de plusieurs attaques telles que la *Cold Boot attack* ou les *keyloggers*. L'idée est de récupérer la clef pour ensuite lire ou écrire les données à volonté. Ces attaques ne passent pas par des failles du logiciel lui-même, mais par des failles de protection de la machine, par exemple :

- des failles de protection physique de la machine : exemple de *Cold Boot attacks*, Firewire ;
- des failles de l'environnement logiciel de l'ordinateur : faille de sécurité dans le système d'exploitation, virus, session non verrouillée à l'insu d'un utilisateur ayant ouvert un volume, copie d'écran à distance par X Window, etc.

La clef (ou mot de passe) est par nature sensible à une attaque de type *brute force* consistant à tester une à une toutes les combinaisons possibles. On veille donc à en choisir une de taille (comme une *passphrase*[17]) et/ou de complexité (comme les initiales des mots d'une phrase longue) appropriée à la nature des données à protéger.

Si rien actuellement ne permet d'identifier formellement un fichier comme étant un volume, au moins deux caractéristiques peuvent faire suspecter qu'un fichier est un volume Truecrypt : l'absence d'en-tête de fichier et le fait que sa taille soit un multiple de 512. Des logiciels tel que *TCHunt* permettent d'établir une liste de fichiers suspects.

Audit global du logiciel en 2013

À la suite des révélations d'Edward Snowden sur les programmes de surveillance de masse américains et britanniques en 2013, et en particulier le programme *Bullrun* de la NSA qui vise à « casser » ou contourner les principaux systèmes de chiffrement utilisés sur Internet[18, 19], plusieurs internautes ont, à la mi-octobre 2013, lancé un projet d'audit de sécurité du logiciel[20, 21].

Ce projet vise à[22] :

- réaliser une cryptanalyse et un audit de sécurité du code source de la version actuelle du Truecrypt (TC 7.1a) ;
- résoudre le problème de licence libre ;
- mettre à disposition de l'ensemble des internautes une application sure pour une majorité de systèmes d'exploitations.

Le 28 décembre 2014, un article de *Der Spiegel* indique que le logiciel TrueCrypt posait des « problèmes majeurs » à la NSA en 2012 dans sa volonté de casser ou contourner le chiffrement[23].

Accueil

> « I trust – oh, what's the file encrypter – TrueCrypt, which I consider the best of three bad alternatives.
>
> J'ai confiance en – comment s'appelle ce logiciel de chiffrement – TrueCrypt, que je considère comme la meilleure des trois mauvaises solutions. »

— Bruce Schneier, le 12 décembre 2013 à la Columbia Law School où il était invité par Eben Moglen[24].

La version 6.0a a reçu un Certificat de Sécurité de Premier Niveau (CSPN) par l'Agence nationale de sécurité des systèmes d'information[25].

En septembre 2013, le cryptographe Bruce Schneier affirme qu'il utilise TrueCrypt depuis qu'il a commencé à travailler sur les documents diffusés par Edward Snowden et conseille de se méfier des solutions commerciales[26].

Licence

La licence collective TrueCrypt ne remplit pas les critères de la définition de l'Open Source et n'a donc pas été approuvée par l'Open Source Initiative. Ce logiciel n'est pas considéré comme libre par plusieurs grandes distributions GNU/Linux (Debian[27], Ubuntu[28], Fedora[29], openSUSE[30], Gentoo[31]). Il est en revanche parfaitement possible de l'utiliser sur ces distributions.

Notes et références

1. « dm-crypt: Linux kernel device-mapper crypto target - IV generators » (https://code.google.com/p/cryptsetup/wiki/DMCrypt), cryptsetup, 11 janvier 2014 (consulté le 13 juin 2014)
2. « index : kernel/git/stable/linux-stable.git - path: root/drivers/md/dm-crypt.c » (https://git.kernel.org/cgit/linux/kernel/git/stable/linux-stable.git/tree/drivers/md/dm-crypt.c?id=refs/tags/v3.13), Kernel.org cgit, 20 janvier 2014 (consulté le 13 juin 2014) voir ligne de commentaire 241
3. **(en)** BWALEX, « TC-play » (https://github.com/bwalex/tc-play), github (consulté le 10 juin 2014)
4. « He Always Had a Dark Side » (https://mastermind.atavist.com/he-always-had-a-dark-side), 24 mars 2016 (consulté le 29 juillet 2016)
5. **(en)** « Microsoft Hands Cops a Crowbar for BitLocker » (http://www.technewsworld.com/story/62825.html) (consulté le 10 juin 2014)
6. Warnung auf offizieller Seite: "Truecrypt ist nicht sicher" (http://www.heise.de/newsticker/meldung/Warnung-auf-offizieller-Seite-Truecrypt-ist-nicht-sicher-2211037.html)
7. What Happened To TrueCrypt? Encryption Software Development Ends Abruptly As InfoSec Community Searches For Answers - Cammy Harbison May 28, 2014 (http://www.idigitaltimes.com/articles/23222/20140528/what-happened-truecrypt-encryption-software-development-ends-hacked-defaced.htm)
8. True mystery of the disappearing TrueCrypt disk encryption software - Naked Security (http://nakedsecurity.sophos.com/2014/05/28/true-mystery-of-the-disappearing-truecrypt-disk-encryption-software/)
9. Is this the end of popular encryption tool TrueCrypt ? - Washington Post

0. Steve Gibson, « And then the TrueCrypt developers were heard from! » (https://www.grc.com/misc/truecrypt/truecrypt.htm) , *TrueCrypt Latest Release Repository*, Gibson Research Corporation, 30 mai 2014 (consulté le 30 mai 2014)
1. truecrypt.ch (http://www.truecrypt.ch/)
2. « CipherShed : le successeur de TrueCrypt bientôt disponible » (http://www.numerama.com/magazine/30643-ciphershed-le-successeur-de-truecrypt-bientot-disponible.html), sur *Numerama*, 20 septembre 2014 (consulté le 20 septembre 2014)
3. **(en)** « New name announced - TCnext » (https://truecrypt.ch/2014/07/new-name-announced/), sur *truecrypt.ch*, 8 juillet 2014 (consulté le 20 septembre 2014)
4. cf. Korben, « TrueCrypt à l'épreuve du FBI » (http://korben.info/truecrypt-a-lepreuve-du-fbi.html)
5. Qualification de la v6.0a au niveau élémentaire par l'ANSSI (http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/p_32_TrueCrypt_version_6.0a.html)
6. Llano A8-3850 VS Core i3-2105 (2011) (http://www.ginjfo.com/dossiers/tests-materiel/composants/processeurs/llano-a8-3850-vs-core-i3-2105-20110816?page=5)
7. Considérant que, par définition, la longueur d'une phrase est supérieure ou égale à celle d'un mot.
8. **(en)** James Ball, Julian Borger et Glenn Greenwald, « Revealed: How US and UK spy agencies defeat internet privacy and security », *The Guardian*, 6 septembre 2013 (lire en ligne (https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security))
9. Comment la NSA peut contrecarrer le chiffrement des communications (http://www.numerama.com/magazine/26916-comment-la-nsa-peut-contrecarrer-le-chiffrement-des-communications.html) Numerama 6 septembre 2013

0. **(en)** « Is TrueCrypt truly secure? Let's have a fundraiser to find out - Fundraising efforts to provide source code auditing for encryption software TrueCrypt have already raised over $46,000 », *Infoworld*, 22 octobre 2013 (lire en ligne (http://www.infoworld.com/t/encryption/truecrypt-truly-secure-lets-have-fundraiser-find-out-229254))
1. **(en)** « Verify, then trust », *The Economist*, 18 octobre 2013 (lire en ligne (http://www.economist.com/blogs/babbage/2013/10/computer-security))
2. Site du projet istruecryptauditedyet.com (http://istruecryptauditedyet.com)
3. Jacob Appelbaum, Aaron Gibson, Christian Grothoff, Andy Müller-Maguhn, Laura Poitras, Michael Sontheimer et Christian Stöcker, Inside the NSA's War on Internet Security (http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html)*, spiegel.de, 28 décembre 2014*
4. Eben Moglen + Bruce Schneier (December 12, 2013) (https://archive.org/details/schneier) - archive.org
5. « Certification » (http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/certificat_cspn_2008_03.html)
6. https://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance
7. « Debian Bug report logs - #364034 » (http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=364034).
8. « Bug #109701 in Ubuntu » (https://bugs.edge.launchpad.net/ubuntu/+bug/109701).
9. « TrueCrypt licensing concern » (http://lists.freedesktop.org/archives/distributions/2008-October/000276.html)

0. « non-OSI compliant packages in the openSUSE Build Service » (http://lists.opensuse.org/opensuse-buildservice/2008-10/msg00055.html).
1. « Gentoo bug 241650 » (http://bugs.gentoo.org/show_bug.cgi?id=241650).

Voir aussi

Articles connexes

Autres systèmes de fichiers chiffrés

- Encrypting File System
- FreeOTFE
- Geli
- BitLocker Drive Encryption, version de Microsoft, connue pour sa porte dérobée grâce à l'outil COFEE fourni par Microsoft
- Acid Cryptofiler
- LUKS

Chiffrement

- Chiffrement à la volée
- OpenSSL

Liens externes

- **(en)** Site officiel (http://www.truecrypt.org)
- **(en)** « Accueil du projet TrueCrypt » (https://sourceforge.net/projects/truecrypt/), sur *SourceForge.net*.
- **(en)** Site du projet d'audit de sécurité du logiciel en 2013 (http://istruecryptauditedyet.com/)

Ce document provient de « https://fr.wikipedia.org/w/index.php?title=TrueCrypt&oldid=143293223 ».

La dernière modification de cette page a été faite le 7 décembre 2017 à 19:41.