TrueCrypt

aus Wikipedia, der freien Enzyklopädie

Gesichtet (+/-)

TrueCrypt ist ein freies Open-Source-Programm zur Verschlüsselung von Festplatten, Teilen davon oder Wechseldatenträgern. Es läuft unter Windows XP (32-Bit/64-Bit), Windows 2000, Windows Server 2003 und Vista (32-Bit/64-Bit). Verschiedene Versionen für Linux gibt es seit Release 4.0. Seit Version 4.2 ist es auch möglich, unter Linux verschlüsselte Partitionen zu erstellen, davor war nur das Benutzen von unter Windows erstellten Partitionen möglich. Seit Version 5.0 steht Truecrypt auch für Mac OS X 10.4 und 10.5 zu Verfügung, allerdings bisher ohne die Möglichkeit versteckte Container („hidden volumes“) zu erstellen.

TrueCrypt	
	
Basisdaten	
Entwickler:	TrueCrypt Foundation
Aktuelle Version:	5.1a (17. März 2008)
Betriebssystem:	Linux, Windows und Mac OS X
Kategorie:	Datenträgerverschlüsselung
Lizenz:	TrueCrypt License
Deutschsprachig:	Ja (Windows)
Website:	truecrypt.org

Inhaltsverzeichnis

- 1 Funktionen
  - 1.1 Algorithmen
  - 1.2 Container
  - 1.3 Konzept der glaubhaften Bestreitbarkeit

- 1.4 „Traveler Mode“
- 1.5 Verschlüsselung von Systempartitionen
- 2 Geschichte
- 3 Geplante Merkmale in zukünftigen Versionen
- 4 Alternativen
- 5 Weblinks
- 6 Einzelnachweise

Funktionen

Algorithmen

TrueCrypt bietet Verschlüsselung mit folgenden Algorithmen: AES, Twofish und Serpent. Es stehen neben der Wahl eines einzelnen Algorithmus auch vorgegebene Kaskadierungen mehrerer Algorithmen zur Wahl.

Container

TrueCrypt kennt zwei Arbeitsweisen im Umgang mit verschlüsselten Daten:

1. Die gesamte Partition wird verschlüsselt, was einerseits bedeutet, dass die Partition neu formatiert wird, und anderseits, dass *TrueCrypt* immer im Hintergrund aktiv ist, wenn auf diese Partition zugegriffen wird.
2. *TrueCrypt* kennt so genannte *Container*, die aus Sicht des Betriebssystems aus einer beliebigen, einzelnen Datei bestehen. Innerhalb dieses *Containers* verwaltet *TrueCrypt* ein Dateisystem. Diese *Container* sind insbesondere geeignet, um auf einer ansonsten nicht verschlüsselten Partition einen privaten verschlüsselten Bereich für sensible Daten anzulegen. Zum Lesen und Schreiben mountet *TrueCrypt* diese Datei. Unter Windows wird hierzu ein neues virtuelles Laufwerk erstellt, unter Linux wird der Container in einen beliebigen Ordner eingehängt. Durch Zugriff auf die gemountete Datei erlangt der Benutzer Zugang zu den unverschlüsselten Daten und kann durch einfache Kopieroperationen auf das TrueCrypt-Laufwerk bzw. in das Mountverzeichnis Verschlüsselungen vornehmen. Bei der Speicherung von Backups, insbesondere auf CD/DVD, ist Vorsicht geboten, da eine Beschädigung des Volume-Header-Bereiches (die

ersten 1024 Bytes) dazu führt, dass der Container nicht mehr gemountet werden kann. Truecrypt bietet daher eine Funktion zum Sichern und Wiederherstellen des Kopfdatenbereiches. Einzelne defekte Sektoren führen nur dazu, dass die betreffenden Zuordnungseinheiten im enthaltenen Dateisystem nicht mehr gelesen werden können.

Konzept der glaubhaften Bestreitbarkeit

Ein besonderes Sicherheitsmerkmal von *TrueCrypt* ist das Konzept der glaubhaften Bestreitbarkeit (engl. *plausible deniability*). Das bedeutet, dass es sehr schwierig ist, die Existenz verschlüsselter Daten nachzuweisen. Dazu gibt es zwei Funktionen:

1. TrueCrypt-Container (*Volumes*) können nicht erkannt werden, da sie keinen eigenen Kopfdatenbereich haben und nur aus zufälligen Bitfolgen zu bestehen scheinen. Sie sind damit von normalen Partitionen oder Dateien voller Zufallszahlen nicht zu unterscheiden. Der Angreifer wird dort jedoch verschlüsselte Daten vermuten. Hier setzt die zweite Funktion an:
2. Versteckte Container (*Hidden Volumes*) können innerhalb des freien Speicherplatzes eines anderen verschlüsselten Volumes versteckt werden. Wird man z. B. gezwungen, das Passwort für das Volume herauszugeben, gibt man nur das Passwort für das äußere Volume her, das versteckte und mit einem anderen Passwort verschlüsselte Volume bleibt unentdeckt. So sieht ein Angreifer nur unwichtige Alibi-Daten, die vertraulichen Daten sind verschlüsselt im freien Speicherplatz des verschlüsselten Volumes verborgen.[1]

„Traveler Mode“

Seit Version 3.1 unterstützt TrueCrypt auch einen sogenannten „Traveler Mode“, womit das Programm nicht mehr installiert werden muss (siehe auch Portable Software). Dadurch kann es z. B. von USB-Sticks gestartet werden. Für den „Traveler Mode“ werden auf den Windows-Rechnern jedoch Administrator-Rechte benötigt. Alternativ ist der Start unter einem CD-basierten Betriebssystem auf Windowsbasis wie Windows PE oder Bart PE möglich. Da diese Systeme von sich aus nicht auf die Festplatte schreiben, sondern lediglich im Hauptspeicher agieren, ist eine hohe Sicherheit gewährleistet.

Verschlüsselung von Systempartitionen

Seit Version 5.0 unterstützt TrueCrypt auch die „Full System Encryption“ bzw. „Whole Disk Encryption“ (auch bekannt als *Pre-Boot-Authentication*) genannte vollständige Verschlüsselung von Windows-Systempartitionen oder auch der gesamten Festplatte, auf der sich eine Systempartition befindet. Unterstützt werden zurzeit Windows XP, Windows Vista und Windows Server 2003, jeweils in den 32- oder 64-Bit-Ausführungen[2]. Ist die gesamte Systempartition verschlüsselt, erscheint vor dem Starten des Betriebssystems ein spezieller TrueCrypt-Bootloader, der zur Passworteingabe auffordert[3]. Ein Vorteil dieses Verfahrens ist, dass sowohl Temp-, Swap- als auch Hibernation (Ruhezustand)-Dateien verschlüsselt auf der Partition abgelegt werden.

Es ist möglich, bereits vorhandene Systempartitionen und -festplatten im laufenden Windows-Betrieb zu verschlüsseln, diese Verschlüsselung zu unterbrechen und zu einem späteren Zeitpunkt fortzusetzen.

Zu Beginn des Verschlüsselungsvorgangs einer Systempartition oder -festplatte erstellt TrueCrypt eine Rescue Disk[4]. Dieses ermöglicht das Entschlüsseln der verschlüsselten Systempartition bzw. das Wiederherstellen des TrueCrypt-Bootloaders..

Geschichte

TrueCrypt basiert auf Encryption for the Masses (E4M), dessen Entwicklung im Jahr 2000 eingestellt worden war. Anfang 2004 wurde das Programm als *TrueCrypt* weiterentwickelt. Ein Nachteil dieser schrittweisen Entwicklung ist die nicht einheitliche Lizenz. Der Quellcode des Programms ist zwar offen, allerdings besitzen einzelne Programmteile unterschiedliche teilweise autorenspezifische Lizenzen, die dann in der *TrueCrypt Collective License* zusammengefasst werden. Damit ist es zum Beispiel nicht ohne weiteres möglich, eine Abspaltung unter einer üblichen freien Lizenz (wie der GPL) durchzuführen. Eine Vereinheitlichung der Lizenz steht zurzeit nicht in Aussicht, da hierzu die Zustimmung aller beteiligten Urheber nötig wäre. Allerdings kann man laut Lizenz Teile der Software bzw. des Quellcodes verwenden und in eigenen Projekten

benutzen, wenn Lizenz und Urheber im Programm/Projekt angegeben werden.

Geplante Merkmale in zukünftigen Versionen

Für spätere Versionen des Programms ist zudem eine Truecrypt-API zur Ansteuerung der Software durch andere Programme, die Rohverschlüsselung von CDs und DVDs und die Unterstützung kryptografischer Tokens angekündigt[5].

Alternativen

Transparente Ver- und Entschlüsselung von Daten bieten neben TrueCrypt außerdem AxCrypt, CrossCrypt, dm-crypt, FreeOTFE, PGP Whole Disk Encryption sowie die kommerziellen Closed-Source-Produkte Jetico Bestcrypt, FREE CompuSec, SafeGuard Easy und DriveCrypt. Das Programm FileVault ist seit Version 10.3 in Apples Betriebssystem Mac OS X integriert.

GNU Privacy Guard und PGP sind ebenfalls Verschlüsselungsprogramme, die jedoch nicht transparent arbeiten und häufiger zum Verschlüsseln und digitalen Signieren von Daten oder E-Mails eingesetzt werden.

Einige Produkte arbeiten als *Full-Disk-Encryption-Software*. Damit kann man sowohl einzelne Partitionen verschlüsseln, als auch eine komplette Festplatte inklusive der Systempartition. Des Weiteren lässt sich eine sogenannte *Pre-Boot-Authentication* installieren, d. h. es erscheint eine Passwortabfrage, bevor das eigentliche Betriebssystem bootet. Ohne das korrekte Passwort wird das System nicht hochgefahren, da die auf der Festplatte enthaltenen Daten komplett verschlüsselt sind.

Weblinks

- Offizielle Website (Englisch)

Einzelnachweise

1. ↑ TrueCrypt Foundation: *Hidden Volume*, Artikel mit weiterführenden

Informationen auf truecrypt.org, 2006, englisch
2. ↑ TrueCrypt Foundation: *Features*, Übersicht über die Eigenschaften der Programmversion
3. ↑ TrueCrypt Foundation: *System Encryption*, Dokumentation
4. ↑ TrueCrypt Foundation: *TrueCrypt Rescue Disk*, Dokumentation
5. ↑ TrueCrypt Foundation: *Future*, geplante Veränderungen