

TrueCrypt

Martin Massat
03. Mai 2011
IAV 10-12

- Was ist TrueCrypt?
- Wofür brauche ich TrueCrypt?
- Verschlüsselungsmethoden
- Verschlüsselungsalgorithmen
- Praxisbeispiel
- Alternativen
- Quellen

Gliederung

- kostenloses Programm zum Erstellen und Verwalten verschlüsselter Container/Volumes
- bietet eine anwenderfreundliche On-the-fly Verschlüsselung
- Quellcode ist zwar verfügbar, TrueCrypt gilt allerdings nicht als Open-Source-Software
- mittlerweile verfügbar für Windows ab 2000, Mac OS X ab 10.4 und Linux ab Kernel 2.4

Download: truecrypt.org/downloads

Was ist TrueCrypt?

Ich habe ein Benutzerkennwort in meinem Betriebssystem eingerichtet, also bin ich auf der sicheren Seite?

Falsch! Jeder könnte leicht die Festplatte ausbauen und die Daten auf einem anderem System auslesen!

- Vertrauliche Firmendaten
- Persönliche Dokumente
- Versand von vertraulichen oder geheimen Daten über das Internet

TrueCrypt versucht diese Sicherheitsanforderungen möglichst anwenderfreundlich in einer Software zu verpacken.

Wofür brauche ich TrueCrypt?

Verschlüsselte Containerdatei

- Verschlüsseltes Laufwerk, welches als Datei gespeichert wird
- Zum Lesen/Schreiben wird die Containerdatei gemountet

Verschlüsselte Partition/Laufwerk

- Verschlüsselte Nicht-Systempartition auf einem internen oder externen Laufwerk
- Vorhandene Daten müssen vor dem Verschlüsseln zwischengespeichert werden

Verschlüsselte Systempartition

- TrueCrypt Bootloader
- Bietet die höchste Sicherheit

Verschlüsselungsmethoden

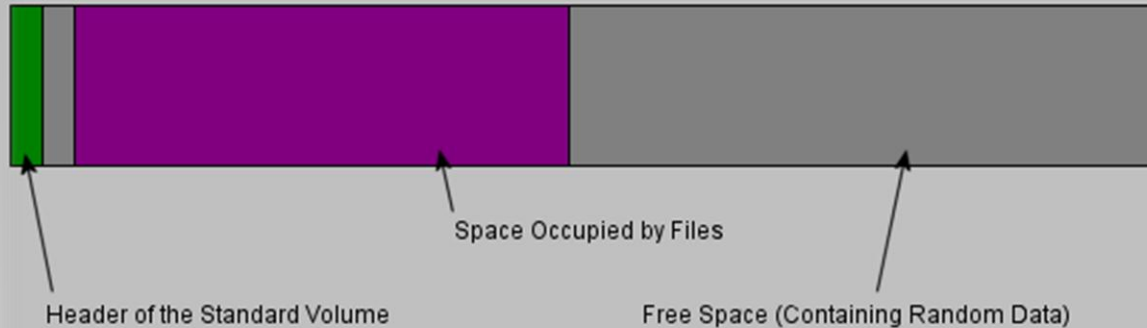
Konzept der glaubhaften Abstreitbarkeit:
Sicherheitsmerkmal von Truecrypt zur Auffindung
von versteckten Daten bzw. dem Nachweis dieser.

- TrueCrypt Container haben keinen eigenen
Kopfdatenbereich
- > Versteckter Container (Hidden Volume)

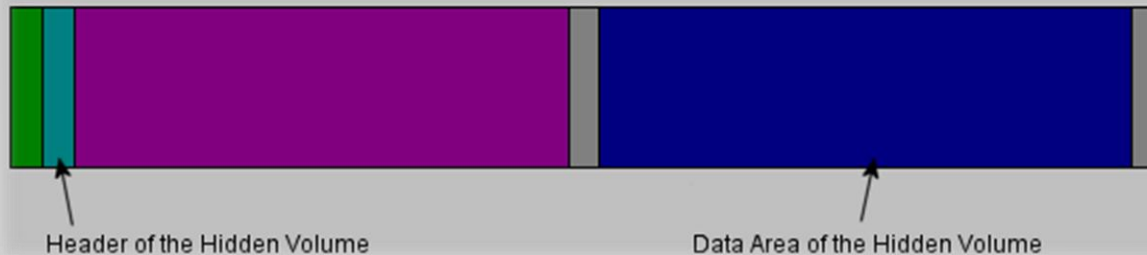
Verschlüsselungsmethoden

Versteckter Container (Hidden Volume)

A standard TrueCrypt volume



The standard TrueCrypt volume after a hidden volume was created within it



Verschlüsselungsmethoden



AES-256

Rijndael

Serpent

Twofish

128-bit Blockgröße

256-bit Schlüssellänge

Verschlüsselungsalgorithmen



Praxisbeispiel

Transparente Projekte

- [FreeOTFE](#)
- [DiskCryptor](#)
- [CrossCrypt](#)
- [dm-crypt](#)
- [SecurStick](#)
- [GNU Privacy Guard](#)

Closed- Source Produkte

- [Jetico Bestcrypt](#)
- [Free CompuSec](#)
- [SafeGuard Easy](#)
- [PGP Whole Disk Encryption](#)
- [DriveCrypt](#)
- [BitLocker](#)
- [EFS](#)
- [PGP](#)
- [FileVault](#)

Alternativen

- <http://www.truecrypt.org>
- <http://de.wikipedia.org/wiki/TrueCrypt>
- [http://de.wikipedia.org/wiki/Advanced Encryption Standard](http://de.wikipedia.org/wiki/Advanced_Encryption_Standard)
- <http://www.webcitation.org/query?url=g1.globo.com/English/noticia/2010/06/not-even-fbi-can-de-crypt-files-daniel-dantas.html>

Quellen