

ERNW Newsletter 24 / Oktober 2008

Liebe Partner, liebe Kollegen,

willkommen zur 24ten Ausgabe des ERNW-Newsletters mit dem Thema:

TrueCrypt – Eine Einführung

Version 1.0 vom 05. Oktober 2008

von: Michael Maria Schaefer, mschaefer@ernw.de

Crypto ist in! Noch nie war es so einfach Daten zu ver- und entschlüsseln, ohne die verwendeten Technologien vollständig zu durchdringen. Im Speziellen erfreuen sich die Technologien großer Beliebtheit, bei denen der Prozess des Ver- oder Entschlüsselns transparent, das heisst für den Benutzer *unsichtbar* abläuft.

Ein freies Open-Source Produkt, um das man bei der näheren Betrachtung von transparenter Daten (-träger) Ver- und Entschlüsselung nicht herumkommt, ist *TrueCrypt*.

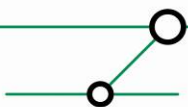
Vor Kurzem in der Version 6.0a erschienen, bietet TrueCrypt mittlerweile eine Vielzahl von Features und Funktionen und deckt ein weites Anwendungsfeld ab.

Dieser Newsletter soll einen Überblick verschaffen, sowie den Einstieg in benutzerfreundliche Verschlüsselung von Daten geben.



INHALTSVERZEICHNIS

1	WAS IST TRUECRYPT?	3
2	WAS KANN TRUECRYPT?	3
2.1	Container und Partitionen.....	4
2.2	Keyfiles	5
2.3	Glaubhafte Bestreitbarkeit (Hidden Volumes)	5
2.4	Traveler Mode.....	6
3	INTEROPERABILITÄT	7
4	KRITISCHE BETRACHTUNG	7
5	SCHLUSSBEMERKUNG	8



1 WAS IST TRUECRYPT?

TrueCrypt geht aus dem Projekt *Encryption for the Masses* (E4M) hervor, dessen Entwicklung im Jahre 2000 mit der Version 2.02a eingestellt wurde. Im Februar 2004 griff das TrueCrypt Projekt das Ziel von E4M wieder auf und veröffentlichte die Version 1.0. Damals kämpfte man noch mit Problemen wie die korrekte Größenanzeige von eingebundenen Datenträgern und elementaren Funktionen. Die so genannten *Hidden Volumes* oder den *Traveler Mode* folgten auch erst deutlich später.

Auch die Unterstützung für Windows-ferne Betriebssysteme und Hardwareplattformen jenseits von i386 wurden erst nach und nach in späteren Versionen nachgereicht.

Heute ist TrueCrypt in der Version 6.0a als freie Software erhältlich und unterstützt neben Windows 2000, den 32- und 64-Bit Versionen von Windows Vista, Windows XP, Windows Server 2008 und Windows Server 2003 auch Mac OS X 10.4 und 10.5, sowie Linux (Kernel 2.4 und 2.6).

Die Software arbeitet vollkommen transparent. Einmal ins System eingebunden ist ein verschlüsselter Bereich wie jeder beliebige interne oder externe Datenträger ansprechbar. Die hierbei erzielte Geschwindigkeit der Lese- und Schreibzugriffe hängt stark mit den verwendeten Algorithmen zusammen, die der Benutzer bei der Erstellung verschlüsselter Bereiche selber wählen kann. Ein wichtiger Punkt ist die Interoperabilität und in dieser Hinsicht hat TrueCrypt eine Vorbildfunktion. Volumes können auf allen unterstützten Plattformen verwendet werden, unabhängig davon, auf welcher Plattform sie erstellt wurden. Die Voraussetzung dafür ist natürlich, dass das verwendete Dateisystem auch von der jeweiligen Plattform unterstützt wird, hierfür trägt jedoch der Benutzer die Verantwortung.

2 WAS KANN TRUECRYPT?

Dem Benutzer wird eine Vielzahl von Anwendungsmöglichkeiten geboten. Wahlweise können komplette (System-) Partitionen oder Teilbereiche verschlüsselt werden oder gar ganze Teilbereiche innerhalb verschlüsselter Sektionen versteckt werden. Darüber hinaus bietet TrueCrypt mittlerweile ein ganzes Arsenal an kryptographischen Algorithmen und Hashfunktionen bis hin zur Möglichkeit, einen verschlüsselten Datenbereich auf einem Rechner zu nutzen, auf dem keine Version von TrueCrypt installiert ist, den so genannten *Traveler Mode*. Seit Version 5.0 steht den Benutzern sämtlicher unterstützter Betriebssysteme eine intuitiv gestaltete grafische Benutzeroberfläche zur Verfügung, die auch dem ungeübten Kryptographen das unkomplizierte Verschlüsseln ermöglicht.

Unter Linux war lange Zeit nur eine konsolenbasierte Nutzung möglich. Seit Version 5.0 steht nun auch hier eine grafische Oberfläche zur Verfügung. Mit dem Versionssprung auf 5.0 hat sich unter Linux ohnehin einiges getan. War bis dato noch ein eigenes Kernel-Modul für den Betrieb notwendig, läuft TrueCrypt nun komplett im Userspace. Für Ubuntu und OpenSuse bieten die Entwickler Pakete zum Download an. Sofern kein eigenes Paket angeboten wird, müssen Nutzer anderer Distributionen momentan in den meisten Fällen auf den Source Code zurückgreifen und selber kompilieren.



2.1 Container und Partitionen

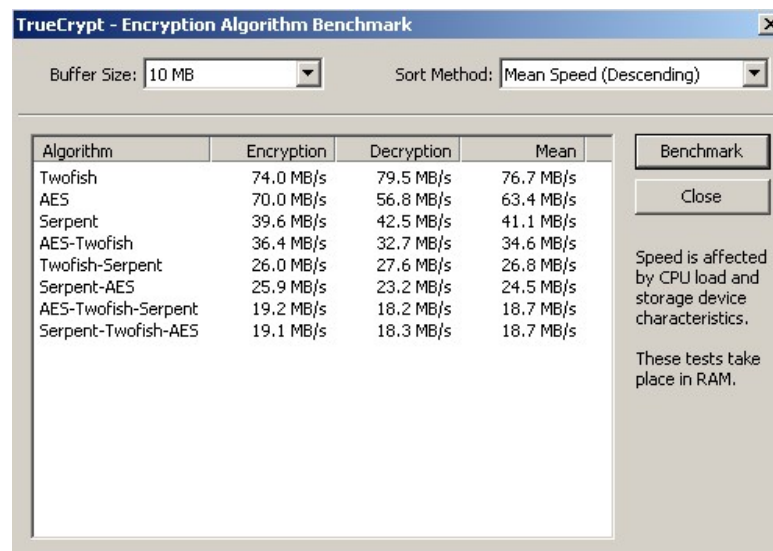
TrueCrypt kennt zwei Arten von verschlüsselten Datenbereichen. Wahlweise kann entweder eine ganze Partition verschlüsselt oder ein so genannter *Container* angelegt werden. Ein *Container* beschreibt einen verschlüsselten Teilbereich innerhalb eines bereits vorhandenen Dateisystems.

Möchte man beispielsweise einen USB-Stick mit einem verschlüsselten und einem unverschlüsselten Bereich ausstatten, ist dieses Feature sehr nützlich, da Windows (im Gegensatz zu Linux und Mac OS X) auf einem *removable media* nicht mehr als eine Partition unterstützt.

Mit Hilfe der grafischen Oberfläche können mit wenigen Klicks Container erstellt oder ganze Partitionen verschlüsselt werden. Ebenso einfach funktioniert das Einhängen von diesen Datenbereichen. Auch eine Konfiguration zum automatischen Mounten (nach Eingabe des zugehörigen Passwortes und/oder des entsprechenden *Keyfiles* versteht sich) ist möglich.

Darüber hinaus ist es möglich ganze Systempartitionen zu verschlüsseln. Hierzu wird der TrueCrypt eigene Bootloader installiert, der während dem Bootvorgang das entsprechende Passwort zur Entschlüsselung der Systempartition abfragt. Die Verschlüsselung der Systempartition, die momentan nur unter Windows möglich ist, kann im laufenden Betrieb durchgeführt werden. Eine Neuinstallation ist nicht notwendig. Der Verschlüsselungsvorgang kann sogar inmitten unterbrochen und zu einem späteren Zeitpunkt fortgesetzt werden.

Zur Verschlüsselung an sich stehen die kryptographischen Algorithmen *AES*, *Serpent* und *Twofish* zur Auswahl, welche auch beliebig kombiniert werden können. Wie bereits angesprochen konvergiert die Geschwindigkeit der Operationen im verschlüsselten Bereiche stark mit der Komplexität und Rechenintensität des verwendeten Algorithmus.



TrueCrypt - Encryption Algorithm Benchmark

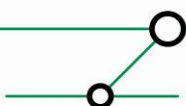
Buffer Size: 10 MB Sort Method: Mean Speed (Descending)

Algorithm	Encryption	Decryption	Mean
Twofish	74.0 MB/s	79.5 MB/s	76.7 MB/s
AES	70.0 MB/s	56.8 MB/s	63.4 MB/s
Serpent	39.6 MB/s	42.5 MB/s	41.1 MB/s
AES-Twofish	36.4 MB/s	32.7 MB/s	34.6 MB/s
Twofish-Serpent	26.0 MB/s	27.6 MB/s	26.8 MB/s
Serpent-AES	25.9 MB/s	23.2 MB/s	24.5 MB/s
AES-Twofish-Serpent	19.2 MB/s	18.2 MB/s	18.7 MB/s
Serpent-Twofish-AES	19.1 MB/s	18.3 MB/s	18.7 MB/s

Buttons: Benchmark, Close

Speed is affected by CPU load and storage device characteristics.
These tests take place in RAM.

Integrierter Benchmark gibt einen Überblick zur erwartenden Performance



2.2 Keyfiles

Um Zugriff auf einen wie auch immer verschlüsselten Bereich zu beschränken, gibt es ein weit verbreitetes Mittel – das Passwort. TrueCrypt bietet darüber hinaus die Möglichkeit von so genannten *Keyfiles*. ...

Keyfiles stellen eine Option dar, die sowohl exklusiv als auch in Kombination mit einem Passwort verwendet werden kann. Auch eine Verwendung mehrerer *Keyfiles* ist möglich. So lässt sich die Sicherheit von Wissen (Passwort) und Besitz (*Keyfiles(s)* auf externem Datenträger) kombinieren und das Sicherheitslevel maximieren. Prinzipiell kann jede beliebige Datei als *Keyfile* verwendet werden. Bei der Definition des *Keyfiles* kann auch ein ganzer Ordner angegeben werden. Es werden dann entsprechend alle in diesem Ordner befindlichen Dateien verwendet.

Da TrueCrypt (sofern möglich) das erste MB ausliest und verwendet, sollte beachtet werden, dass sich im Falle einer Veränderung des Dateiinhalts das Volume nicht mehr entschlüsseln lässt. Man sollte sich darüber bewusst sein, dass auch bei der Kombination von *Keyfiles* und Passwort der Verlust von bereits einer der Komponenten dazu führt, dass die Daten nicht mehr entschlüsselt werden können. Das nachträgliche Entfernen von *Keyfiles* und eine damit verbundene Neu-Verschlüsselung sind zwar möglich, selbstverständlich wird für diesen Vorgang jedoch erneut einmalig das entsprechende *Keyfile* benötigt.

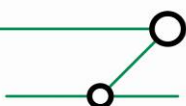
TrueCrypt bringt auch eigene Tools zur Erstellung von entsprechenden Dateien mit. Die vermutlich einfachste Variante zur Erstellung ist jedoch das Füllen einer Datei mit Zufallswerten (unter Linux z.B. mittels */dev/urandom*). Die Entwickler geben an, dass ein *Keyfile* stets mindestens 30 Byte groß sein sollte, um Brute Force Attacken zu erschweren.

2.3 Glaubhafte Bestreitbarkeit (Hidden Volumes)

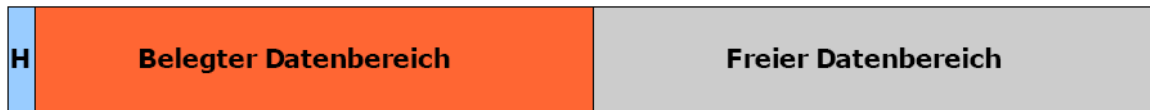
Ein spezielles Sicherheitsmerkmal, welches bei TrueCrypt Einzug hielt, ist das Prinzip der Glaubhaften Bestreitbarkeit (*plausible deniability*). Die Umsetzung dieses Konzepts beruht auf der Tatsache, dass die Existenz von verschlüsselten Daten und im Speziellen eines TrueCrypt Volumes gar nicht oder nur schwer nachweisbar ist.

Es wird davon ausgegangen, dass ein verschlüsselter Bereich zwar eigentlich nicht von einem Speicherbereich mit zufälligen Bitmustern unterschieden werden kann, im Falle einer entsprechenden Vermutung kann man aber unter Umständen zu der Herausgabe eines Passwortes gezwungen werden. In Großbritannien existiert beispielsweise seit dem Jahr 2007 ein entsprechendes Gesetz, auf dessen Grundlage die Nicht-Herausgabe eines Passwortes mit einer Freiheitsstrafe von bis zu fünf Jahren bestraft werden kann. Um einer solchen (oder ähnlichen) Situation entgehen zu können, implementiert TrueCrypt die so genannten *Hidden Volumes*.

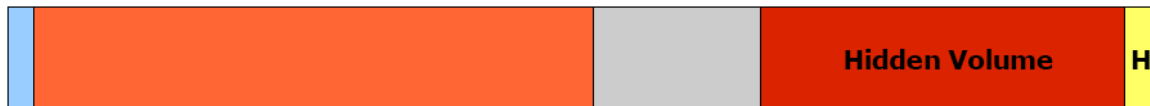
Genau betrachtet sind die *Hidden Volumes* nichts weiter als ein versteckter Container innerhalb des freien Bereichs eines normalen verschlüsselten Volumes.



TrueCrypt Container



Hidden Volume in Standard Container



Wird nun das äußere Volume gemountet, so bleibt das innere, versteckte Volume (welches im Übrigen mit einem separaten Passwort gesichert werden muss) unsichtbar und dessen Existenz wird als mit *impossible to prove* (nicht nachweisbar) beschrieben. Dies rührt daher, dass auch freier Bereich in einem TrueCrypt Volume immer mit Zufallswerten aufgefüllt ist und darüber hinaus die Informationen über das Dateisystem des äußeren Volumes bei der Erstellung des versteckten Bereichs nicht verändert werden.

In dem äußeren Bereich können nun vermeintlich geheime Daten abgelegt werden, wohingegen die wirklich privaten Daten in dem *Hidden Volume* versteckt werden. Im Falle des Falles kann somit das Passwort für den äußeren Container herausgegeben werden und die wirklich privaten Daten bleiben unentdeckt. Im praktischen Gebrauch wird übrigens in Abhängigkeit vom eingegebenen Passwort entweder der äußere oder der versteckte, innere Bereich gemountet. Auch um sicher zu stellen, dass beim Beschreiben des Standard Volumes nicht aus Versehen Teile es versteckten Bereichs überschrieben werden (wie gesagt: Das äußere Volume *weiß nichts* von der Existenz des *Hidden Volumes*), gibt es ein Flag, welches beim Mounten gesetzt werden kann und in dessen Folge beide Passwörter abgefragt werden um bei anschließenden Operationen immer zu verifizieren, dass nicht versehentlich in den versteckten Bereich geschrieben wird.

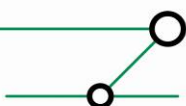
Seit Version 6 können auch Systempartitionen versteckt werden. Im TrueCrypt Kontext spricht man von *Hidden Operating Systems*.

2.4 Traveler Mode

Unter Windows ist eine Funktion verfügbar, welches es ermöglicht TrueCrypt Volumes auch auf Systemen einzubinden, auf denen zuvor kein TrueCrypt installiert ist. Der *Traveler Mode* kann auf zwei Arten verwendet werden. Es sei hier direkt der Hinweis gegeben, dass für den *Traveler Mode* Administrator Rechte auf dem Zielsystem notwendig sind.

Die einfachste Variante ist es, das entsprechende TrueCrypt Binary (truecrypt.exe) auf einen unverschlüsselten Teil des Datenträgers (z.B. ein USB Stick) zu kopieren und dieses dann auf dem System, wo das verschlüsselte Volume eingebunden werden soll, aufzurufen.

Eine weitere Möglichkeit bietet der Assistent zur Erstellung eines Datenträgers im Traveler Mode. Der Assistent erstellt zusätzlich zu dem Binary und einigen Systemdateien eine *autorun.inf*, die alle erforderlichen TrueCrypt Parameter bei einem Autostart setzt, so dass dem Benutzer nur noch ein Passwort abgefragt wird und der Datenträger anschließend im System eingebunden ist und verwendet werden kann.



3 INTEROPERABILITÄT

Ein schon zu Beginn genanntes Argument für TrueCrypt ist die Interoperabilität. Wie bereits erwähnt ist TrueCrypt für diverse Windows Versionen, Linux und Mac OS X erhältlich. Seit Version 5.0 steht für alle Plattformen auch die gleiche grafische Benutzeroberfläche zur Verfügung.

In praktischen Tests hat sich gezeigt, dass die Interoperabilität zwischen den Systemen durchaus mit *gut* bewertet werden kann, auch wenn es noch kleine Schönheitsfehler gibt, über die man sich bewusst sein sollte wenn man TrueCrypt Plattform übergreifend nutzen möchte. Im Speziellen ist die Abwärtskompatibilität nicht immer gegeben. *Hidden Volumes* die beispielsweise mit TrueCrypt 5.1a unter Linux erstellt wurden, können unter Umständen auf der selben Plattform mit der letzten Version des 4er Release 4.3a nicht gemountet werden, auch wenn kryptographische Algorithmen verwendet wurden, die auch unter 4.3a verfügbar sind. Unter Windows hingegen lässt sich das gleiche Volume problemlos einbinden.

Im Gegenzug erwies sich TrueCrypt unter Windows Vista als ein wenig widerspenstig, wenn es darum ging *Hidden Volumes* zu erstellen. Entsprechende Bugs scheinen bei den Entwicklern aber bekannt zu sein.

Die Verwendung von Volumes die unter anderen Betriebssystemen erstellt wurden, funktioniert in der Praxis sehr gut. Es gilt zu beachten, dass das entsprechende Dateisystem selbstredend vom Betriebssystem unterstützt werden muss, mit dem man das Volume nutzen möchte. Auch wenn TrueCrypt von Haus aus nur FAT (und NTFS unter Windows) als Option für die Formatierung anbietet, ist es theoretisch wie praktisch kein Problem, das Volume unformatiert zu lassen und ein anderes Dateisystem zu verwenden. Die entsprechende Formatierung muss dann natürlich manuell auf dem eingebundenen Volume vollzogen werden. Die einzige Einschränkung hierbei ist, dass das äußere Volume eines *Hidden Volume* stets mit FAT formatiert werden muss.

Generell empfiehlt es sich bei Verwendung auf den unterschiedlichsten Systemen darauf zu achten, dass jeweils die aktuellste Version von TrueCrypt verwendet wird. Tests in der Praxis haben gezeigt, dass bei diesem Szenario die Schnittmenge der plattformübergreifend funktionierenden Funktionen maximal ist.

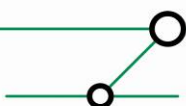
4 KRITISCHE BETRACHTUNG

Bei aller Crypto-Euphorie muss man sich ins Bewusstsein rufen, dass auch der stärksten Datenverschlüsselung umgebungsbedingte Grenzen gesetzt sind. Dessen ist man sich auch bei TrueCrypt bewusst und gibt entsprechende Hinweise, die man bei dem Umgang unbedingt beachten sollte.

Hierzu ist es wichtig zu wissen, dass mit den gewählten Authentifizierungsdaten wie Passwort und *Keyfile* lediglich der TrueCrypt Header verschlüsselt wird, in welchem wiederum der *Masterkey* für die eigentliche Verschlüsselung der Nutzdaten zu finden ist.

Umstrukturierung des Dateisystems durch Defragmentierung oder Journaling kann es einem Angreifer u.U. ermöglichen, auch nach Erneuerung eines TrueCrypt Headers (z.B. Ändern des Passwortes) durch Datenwiederherstellung in den Besitz eines entsprechenden alten Headers zu gelangen. Mit Hilfe eines kompromitierten Passwortes kann der Angreifer nun einen Masterkey extrahieren, mit dessen Hilfe sich die Nutzdaten wieder entschlüsseln lassen. Im Falle von kompromitierten Authentifizierungsdaten ist es also stets ratsam, diese nicht bloß zu ändern, sondern einen komplett neuen Container zu erstellen. Die damit verbundene Neu-Verschlüsselung der Nutzdaten schützt vor unbefugtem Zugriff durch alte Header.

Darüber hinaus sollte man sich dessen bewusst sein, dass produktiv genutzte Daten unverschlüsselt im Arbeitsspeicher abgelegt sind und z.B. durch unvorhergesehenen dumps



zum Vorschein kommen können. Auch Mechanismen wie suspend-to-disk schreiben evtl. genutzte Daten in unverschlüsselter Form auf die Festplatte.

5 SCHLUSSBEMERKUNG

TrueCrypt hat sich im Laufe der Jahre zu einem mächtigen und ausgereiften Werkzeug zur Datenverschlüsselung entwickelt. Speziell die Möglichkeit der plattformübergreifenden Nutzung macht es zu einer attraktiven Alternative gegenüber anderen vorherrschenden Produkten. Andere etablierte Produkte wie z.B. *dm-crypt* oder *AxCrypt* bieten zwar ebenfalls interessante Features, sind aber meist auf die Nutzung unter einem bestimmten Betriebssystem beschränkt.

Die Homepage des TrueCrypt Projekt bietet eine hervorragende Dokumentation, die weit über die Behandlung dieses Artikels hinausgeht. Speziell für Interessierte der kryptographischen Funktionsweisen empfiehlt sich ein Blick in die technische Dokumentation.

Jenseits der vollständigen Implementierung von angesprochenen Funktionen und dem Ausmerzen kleinerer Bugs und Inkompatibilitäten hat man sich für die Zukunft ehrgeizige Ziele gesetzt. Mit der Version 6 wurde die Unterstützung für paralleles Rechnen eingeführt, so dass auf Multi-Core Systemen ein deutlicher Leistungszuwachs erzielt werden konnte. Darüber hinaus arbeitet man an der Unterstützung für hardwareseitige Sicherheitsmodule und dem Verschlüsseln von Rohdaten auf optischen Datenträgern wie CDs und DVDs.

Mit freundlichen Grüßen,

[Michael Maria Schaefer].

ERNW GmbH
Michael Maria Schaefer
Security Research

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel: +49 6221 480390
Fax: +49 6221 419008
Mob: +49 151 16227564
Email : info@ernw.de
www.ernw.de

