[redacted]

[redacted]

Untersuchung TrueCrypt

Arbeitspaket 1

Funktionale Unterschiede zwischen Microsoft Windows und Linux Version

[redacted]

Version:	1.0
Datum:	15. September 2010

Historie

Version	Autor	Kommentar	Datum
0.1	[redacted]	Initiale Dokumentversion erstellt	09.08.10
0.5	[redacted]	Überarbeitete Fassung nach Kick-Off-Meeting	26.08.10
0.9	[redacted]	Überarbeitete Fassung nach Telefonkonferenz	31.08.10
0.91	[redacted]	Überarbeitete Fassung nach Telko vom 6.9.2010	08.09.10
0.92	[redacted]	Überarbeitete Fassung nach Kommentaren	09.09.10
1.0	[redacted]	Überarbeitete Fassung nach Kommentaren	15.09.10

Inhaltsverzeichnis

1 Einleitung

1.1 Einführung

Ziel des Projektes ist es, genaue Kenntnisse über den Aufbau und die Funktionsweise sowie über die Sicherheit des Produktes „TrueCrypt“ zu erhalten und die Weiterentwicklung des Produktes vorzubereiten. Als erster Schritt dafür ist eine Analyse der Funktionen und Möglichkeiten von TrueCrypt und die Erstellung einer Übersicht über die funktionalen Unterschiede notwendig, welche zwischen der MS-Windows- und Linux-Version von TrueCrypt bestehen. Diese Unterschiede sind in verschiedenen Bereichen der Software zu finden und können unter anderem die graphische Oberfläche, die Kommandozeilenwerkzeuge oder den Pre-Boot-Mechanismus betreffen.

Die folgende Dokumentation beschreibt die vorgenommene Analyse der MS Windows und Linux Version von TrueCrypt und stellt die gefundenen Unterschiede in einer kategorisierten und eindeutig durchnummerierten Tabelle dar. Es wird die Funktion benannt, eine detailliertere Beschreibung gegeben und gegebenenfalls Unterschiede zwischen den Versionen beschrieben. Ein vollständiges, teilweises oder gar nicht Vorhandensein wird mit entsprechenden Symbolen gekennzeichnet

(✓,-,✗) .

1.2 Verwendete Begriffe

Begriff	Erläuterung
Sparse-Datei	Eine Datei, die aus „Löchern“ – Sequenzen von Nullbytes und den eigentlichen Daten besteht. Die Nullbytesequenzen werden nicht gespeichert und benötigen somit keinen Speicherplatz.
Volume	Ein zusammenhängend adressierbarer Block auf einem Speichermedium, der für ein oder mehrere Dateisysteme benutzt werden soll, z.B. Festplatte, Festplattenpartition, USB-Speichermedium, Container-Datei. Auf diesem Volume werden die Dateien von TrueCrypt verschlüsselt abgelegt.

2 Methodik

Um die Funktionen besser testen und vergleichen zu können, wurden zwei virtuelle Maschinen mit Windows XP und Linux erstellt. Als Linux-Variante wurde Ubuntu als eine der am weitesten verbreiteten Distributionen in der Version 10.04 gewählt. Dies ist eine LTS-Version (Long Term Support) mit 5 Jahren Support, sodass die Ergebnisse relativ lange verwendbar sein werden. Die Resultate sind im Prinzip auch auf andere Linux-Varianten übertragbar, insbesondere auf Debian, auf dem Ubuntu basiert, das aber bei der Aufnahme von Programmversionen in eine stabile Version sehr konservativ und auch wesentlich aufwändiger in der Konfiguration ist. Nachträglich wurden diese Tests erneut mit MS Windows 7 durchgeführt und die Resultate in die Tabelle aufgenommen. Als zu testende TrueCrypt Version wurde die zum Erstellungszeitpunkt aktuellste Version (7.0[1]) gewählt und auf den betreffenden Betriebssystemen installiert. Hierbei traten keine gravierenden Unterschiede oder Probleme auf.

Als erstes wurden die beiden graphischen Oberflächen untersucht und verglichen, wobei auch hier keine nennenswerten Unterschiede auffielen. Lediglich die Einträge in der Menüleiste wiesen unterschiedliche Funktionen auf, welche in einem späteren Schritt mit näheren Beschreibungen aus der TrueCrypt Dokumentation in die unten stehende Tabelle eingefügt wurden.

Im zweiten Schritt wurden parallel in beiden Betriebssystemen auf den ersten Blick erkennbare Funktionen getestet. Dazu gehörten unter anderem die Erstellung von verschlüsselten Container-Dateien in unterschiedlichen Größen und mit unterschiedlichen Formaten und Algorithmen, die Verschlüsselung einer kompletten Partition und die Nutzung von Keyfiles. Da alle in diesem Schritt getesteten Funktionen direkt in beiden Betriebssystemen verifiziert wurden, konnten bestehende Unterschiede eindeutig identifiziert werden.

Um den kompletten Funktionsumfang von TrueCrypt zu identifizieren und weiterführende Informationen über bereits bekannte Funktionen zu erhalten, wurde in einem weiteren Schritt die offizielle TrueCrypt Dokumentation[2] vollständig analysiert. Einige neu identifizierte Funktionen wurden in den virtuellen Maschinen getestet, sowie alle festgestellten Unterschiede in der Tabelle vermerkt und beschrieben.

Es wurde zusätzlich eine grobe Quellcodeanalyse durchgeführt, wobei unter anderem die Quellen der MS Windows und Linux Version mit dem Tool „WinMerge[3]“ verglichen wurden. Die Ergebnisse wurden ebenfalls in der Tabelle vermerkt.

Zuletzt konnten noch einige weiterführende Informationen in diversen Foren und durch die Suchmaschine Google gefunden werden.

---

[1] http://www.truecrypt.org/downloads

[2] http://www.truecrypt.org/docs/

[3] http://winmerge.org/

3 Versionsvergleich

In diesem Abschnitt werden die TrueCrypt Versionen für MS Windows und Linux gegenübergestellt. In 3.1 (Gegenüberstellung) werden die Funktionen aufgelistet und die Unterstützung der jeweiligen Version durch entsprechende Symbole dargestellt. In 3.2 (Erläuterung) erfolgt dann die detaillierte Beschreibung der einzelnen Punkte.

3.1 Gegenüberstellung

ID	Kategorie	Funktion	Windows XP	Windows 7	Ubuntu 10.04
3.2.1	Verschlüsselung	Erstellen einer verschlüsselten Container-Datei	✓	✓	✓
3.2.2	Verschlüsselung	Erstellen einer verschlüsselten Partition (ohne Systemdateien)	✓	✓	✓
3.2.3	Verschlüsselung	Verschlüsseln der Systempartition oder -festplatte (Systemverschlüsselung)	✓	✓	✗
3.2.4	Verschlüsselung	Existierende Partition verschlüsseln	✗	✓	✗
3.2.5	Sicherheit	Volume umschlüsseln	✗	✗	✗
3.2.6	Sicherheit	Passwort ändern	✓	✓	✓
3.2.7	Sicherheit	Volume-Header sichern / wiederherstellen	✓	✓	✓
3.2.8	Sicherheit	Algorithmus für Headerschlüsselberechnung ändern	✓	✓	✓
3.2.9	Sicherheit	Erstellen einer TrueCrypt Rescue Disk	✓	✓	✗
3.2.10	Sicherheit	Versteckte Volumes	✓	✓	-

ID	Kategorie	Funktion	Windows XP	Windows 7	Ubuntu 10.04
3.2.11	Sicherheit	Schutz für versteckte Volumes	✓	✓	✓
3.2.12	Sicherheit	Verschiedene Verschlüsselungsalgorithmen	✓	✓	✓
3.2.13	Sicherheit	Verschiedene Hash-Algorithmen	✓	✓	✓
3.2.14	Sicherheit	Eingänge des Zufallszahlengenerators	-	-	-
3.2.15	Sicherheit	Kryptografischer 'Mode of Operation'	✓	✓	✓
3.2.16	Authentisierung	Security Tokens und Smartcards	✓	✓	✓
3.2.17	Authentisierung	Benutzung / Erstellung von Keyfiles	✓	✓	✓
3.2.18	Authentisierung	Multi-Faktor-Authentisierung	✓	✓	✓
3.2.19	Authentisierung	Pre-Boot-Authentication	✓	✓	✗
3.2.20	Authentisierung	Revoke Authentication	✗	✗	✗
3.2.21	Performance	Pipelining während Ver- und Entschlüsselung	✓	✓	✗
3.2.22	Performance	AES Hardware Beschleunigung	✓	✓	✓
3.2.23	Benutzerfreundlichkeit	Sprachunterstützung	✓	✓	✗
3.2.24	Benutzerfreundlichkeit	Hotkeys	✓	✓	✗

ID	Kategorie	Funktion	Windows XP	Windows 7	Ubuntu 10.04
3.2.25	Benutzerfreundlichkeit	Benutzen von Favoriten	✓	✓	✓
	Benutzerfreundlichkeit	Verwalten von Favoriten	✓	✓	✓
3.2.26	Benutzerfreundlichkeit	Ausführen von TrueCrypt ohne Administratorrechte	-	-	-
3.2.27	Benutzerfreundlichkeit	Portable Version	✓	✓	✗
3.2.28	Benutzerfreundlichkeit	Trennen der Volumes bei Energiesparmodus (Standby, Ruhezustand)	✓	✓	✗
3.2.29	Benutzerfreundlichkeit	Sicherer Ruhezustand	✓	✓	✗
3.2.30	Benutzerfreundlichkeit	Passwort Caching	✓	✓	✓
3.2.31	Benutzerfreundlichkeit	Grafisches Benutzer Interface (GUI)	✓	✓	-
		Kommandozeileninterface (CLI)	-	-	-
3.2.32	Benutzerfreundlichkeit	Verschiedene Dateisysteme	-	-	-
3.2.33	Quellcode	Unterschiede im Quellcode	-	-	-
3.2.34	Quellcode	Nicht unterstützte Funktionsklassen	-	-	-

3.2 Erläuterung

3.2.1 Erstellen einer verschlüsselten Container-Datei

Diese Funktion erstellt eine verschlüsselte Datei, welche als Container fungiert und nach dem Einbinden wie ein normaler Datenträger behandelt werden kann. Unter Windows können diese zusätzlich als dynamisch eingestellt werden, d.h. belegen im leeren Zustand nur den tatsächlich benötigten Platz für die internen Verwaltungsinformationen und wachsen beim Speichern von Dateien in dem Volume entsprechend mit. Beim Löschen schrumpfen diese allerdings nicht wieder und sie besitzen auch andere Nachteile (z.B. Performance, Sichtbarkeit von leeren Bereichen nach außen).

Das Erstellen von verschlüsselten Container-Dateien ist in allen getesteten Versionen verfügbar.

3.2.2 Erstellen einer verschlüsselten Partition (ohne Systemdateien)

Diese Funktion erstellt eine verschlüsselte Partition auf einem internen oder externen Medium. Die Partition enthält kein Betriebssystem.

Das Erstellen von verschlüsselten Partitionen ist in allen getesteten Versionen verfügbar.

3.2.3 Verschlüsseln der Systempartition oder -festplatte (Systemverschlüsselung)

Diese Funktion verschlüsselt die Systempartition (-festplatte) und somit das komplette Betriebssystem. Das Verschlüsseln kann abgebrochen und fortgesetzt werden. Vor dem Bootvorgang muss sich der Benutzer per Volume-Passwort authentisieren. Im Anschluss daran wird das Betriebssystem geladen.

Diese Funktion ist nur unter den beiden Windows Versionen möglich, unter der Linux Version wurde diese Funktion noch nicht implementiert.

Gründe diesbezüglich werden in Abschnitt 4.1.1 aufgezeigt.

3.2.4 Existierende Partition verschlüsseln

Mit dieser Funktion kann eine existierende unverschlüsselte Partition, welche schon Daten enthält, verschlüsselt werden, ohne dass diese Daten dabei verloren gehen.

Das Verschlüsseln von existierenden Partitionen ist erst ab Windows Vista und unter Linux gar nicht möglich.

3.2.5 Volume umschlüsseln

Beim Umschlüsseln des Volumes wird der Schlüssel mit dem die Daten verschlüsselt sind geändert. Dazu muss jeder Datenblock des Volumes gelesen, mit dem alten Schlüssel entschlüsselt, mit dem neuen Schlüssel verschlüsselt und dann wieder gespeichert werden.

TrueCrypt bietet in keiner der getesteten Versionen die Umschlüsselung des Volumes an.

3.2.6 Passwort ändern

TrueCrypt bietet eine Funktion, die es erlaubt, das Volume-Passwort zu ändern. Dabei wird der Header des Volumes mit dem unter anderem aus dem Passwort abgeleiteten Schlüssel neu verschlüsselt und gespeichert.

Danach kann das Volume nur noch mit dem neuen Passwort entschlüsselt werden.

Wurde jedoch der alte Volume-Header vorher gesichert, so kann er danach wiederhergestellt werden, und das neue Passwort kann durch das alte überschrieben werden.

Die Passwortänderung kann nur im inaktiven Zustand erfolgen, d.h. das Volume muss getrennt sein.

In allen getesteten Versionen ist die Änderung des Volume-Passworts möglich.

3.2.7 Volume-Header sichern / wiederherstellen

Der Volume-Header enthält alle benötigten Daten, die nötig sind um zusammen mit den Authentisierungsmerkmalen (Passwort, Keyfiles, Smartcard) den Volumeschlüssel zu berechnen, mit dem das Volume verschlüsselt ist.

TrueCrypt bietet die Möglichkeit den Volume-Header zu sichern, um ihn bei Bedarf wiederherstellen zu können. Vor dem Sichern des Headers muss eine Authentisierung an dem Volume durchgeführt werden. Vor dem Wiederherstellen des Headers muss eine Authentisierung mit den zum Zeitpunkt der Sicherung gültigen Authentisierungsmerkmalen erfolgen. Es wird nicht geprüft, ob der zurückgeschriebene Header zu dem Volume selber passt. Spielt man ein falsches Backup ein, kann man zwar das Volume später einbinden, da die Daten aber mit dem falschen Volumeschlüssel entschlüsselt werden, ist das Volume dann selber nicht lesbar.

Bei Fehlern (technische Fehler im Bereich des Headers) kann dann der zuvor gesicherte Volume-Header wiederhergestellt werden. Nach der Wiederherstellung des Volume-Headers sind die Authentisierungsmerkmalen zum Zeitpunkt der Sicherung gültig. Diese Funktion kann also auch dazu genutzt werden, eine Passwortänderung rückgängig zu machen.

Für das Sichern / Wiederherstellen des Headers sind keine Administratorrechte erforderlich.

Die Sicherung / Wiederherstellung des Volume-Headers ist in allen getesteten Versionen verfügbar.

3.2.8 Algorithmus für Headerschlüsselberechnung ändern

Der Algorithmus für die Headerschlüsselberechnung eines Volumes kann beim Formatieren gewählt werden und kann nachträglich geändert werden. Der entsprechenden Informationen des Volume-Headers wird dabei neu berechnet. Beim Einbinden des Volumes ermittelt TrueCrypt durch Ausprobieren aller möglichen Algorithmenkombinationen (Ableitung des Volumeschlüssels sowie der verwendete Verschlüsselungsalgorithmus) die richtigen Parameter.

Der Algorithmus für die Headerschlüsselberechnung kann in allen getesteten Versionen geändert werden.

3.2.9 Erstellen einer TrueCrypt Rescue Disk

Diese Disk ermöglicht es eine verschlüsselte Systempartition (-festplatte) und das darauf befindliche Betriebssystem zu reparieren, falls aus folgenden Gründen nicht darauf zugegriffen werden kann:

- Fehler im TrueCrypt-Bootloader
- Der TrueCrypt-Bootloader steht im Verdacht, manipuliert worden zu sein.
- Der TrueCrypt-Bootloader soll nicht auf der Festplatte gespeichert sein.
  (z.B. um den Einsatz von Truecrypt zu verschleiern)
- Der Master Key oder andere wichtige Daten sind beschädigt
- Windows ist beschädigt und/oder startet nicht richtig und ein Reparaturprogramm, welches die Verschlüsselung nicht unterstützt, soll gestartet werden
- Backup des „First Drive Track“ (Master Boot Record)
- Die Verschlüsselung soll entfernt werden, ohne das System neu installieren zu müssen

Wird das System von der Rescue Disk gestartet, hat der Nutzer die Möglichkeit die verschlüsselte Systemfestplatte nach Eingabe des korrekten Passwortes zu entschlüsseln, danach können ggf. Reparaturen am System vorgenommen werden. Ferner können Sicherung und Restaurierung des Volume-Headers durchgeführt werden.

Die Erstellung einer TrueCrypt Rescue Disk ist unter beiden Windows-Versionen verfügbar. Unter Linux ist die Verschlüsselung der Systempartition nicht möglich und daher die Erstellung der Rescue Disk nicht erforderlich.

3.2.10 Versteckte Volumes

Versteckte Volumes dienen dazu innerhalb eines regulären Volumes ein weiteres (verstecktes) Volume zu erstellen. Die Existenz eines solchen versteckten Volumes kann nicht nachgewiesen werden, der User kann also dessen Existenz bestreiten.

Versteckte Volumes werden in allen getesteten Versionen unterstützt.

Bei Verwendung der Systemverschlüsselung ist es möglich, ein weiteres, verstecktes Betriebssystem innerhalb der Systempartition anzulegen. Für jedes System wird ein separates Passwort bei der Pre-Boot-Authentication verwendet.

Versteckte Betriebssysteme sind nur unter den Windows Versionen möglich.

3.2.11 Schutz für versteckte Volumes

Bei der Verwendung von versteckten Volumes kann es beim Beschreiben des äußeren Volumes zum versehentlichen Überschreiben des inneren Volumes und somit zu dessen Zerstörung kommen. TrueCrypt bietet eine Möglichkeit zum Schutz des inneren Volumes. Dazu muss beim Einbinden des äußeren Volumes die entsprechende Funktion aktiviert und zusätzlich die Authentisierung für das innere Volume durchgeführt werden. Sind beide Authentisierungen gültig, bindet TrueCrypt nur das äußere Volume ein, liest aber die Längeninformation aus dem Header des inneren Volumes aus. Somit ist die Größe des inneren Volumes bekannt und ein möglicher Schreibzugriff in diesen Bereich wird zurückgewiesen.

Versteckte Volumes sollten nicht in Sparse-Dateien erstellt werden. Unter Windows wird dies automatisch erzwungen, unter Linux nicht.

Der Schutz für versteckte Volumes ist in allen Versionen verfügbar, allerdings muss unter Linux die Prüfung auf Sparse-Dateien manuell erfolgen.

3.2.12 Verschlüsselungsalgorithmen

Folgende Algorithmen stehen für die Verschlüsselung zur Verfügung:

- AES
- Serpent
- TwoFish
- AES-TwoFish
- AES-TwoFish-Serpent
- Serpent-AES
- Serpent-TwoFish-AES
- TwoFish-Serpent

Die genannten Verschlüsselungsalgorithmen sind in allen getesteten Versionen, auch bei der Systemverschlüsselung unter Windows verfügbar.

3.2.13 Hash-Algorithmen

Folgende Hash-Algorithmen stehen für den Zufallszahlengenerator und die Ableitung des Schlüssels für die Headerverschlüsselung zur Verfügung:

- RIPEMD-160
- SHA-512
- Whirlpool

Die genannten Hash-Algorithmen sind in allen getesteten Versionen nutzbar.

Bei der Systemverschlüsselung unter Windows ist ausschließlich RIPEMD-160 verfügbar.

3.2.14 Zufallsquellen

Der Zufallszahlengenerator bezieht Zufallsdaten aus folgenden Quellen:

- Mausbewegung
- Tastenanschläge

Abhängig vom verwendeten Betriebssystem werden weiter Zufallsquellen genutzt. Deren Auswahl kann der Anwender nicht beeinflussen.

MS Windows:

- CryptoAPI
- Netzwerkstatistiken
- Verschiedene Win32-Handles

- Zeitvariablen
- Zähler

Linux:

- Werte aus dem Betriebssystem-RNG (/dev/random und /dev/urandom)[4]

Unter allen getesteten Versionen sind verschiedene, betriebssystemabhängige Zufallsquellen für den Zufallszahlengenerators vorhanden.

3.2.15 Kryptografischer „Mode of Operation“

Der einzige von TrueCrypt verwendete kryptografische Betriebsmodus ist XTS.

XTS wird in allen getesteten Versionen verwendet.

3.2.16 Security Tokens und Smartcards

TrueCrypt unterstützt PKCS #11[5] (2.0 oder höher) kompatible Smartcards und Security Tokens und kann darauf befindliche Keyfiles direkt benutzen oder eigene Keyfiles auf dem Token / der Smartcard ablegen. Die Eingabe des PIN Codes, mit dem üblicherweise der Zugriff auf den Token / die Smartcard geschützt wird erfolgt über die Tastatur des Computers. Es war nicht möglich, die PIN über die externe Tastatur einzugeben, da zumindest für den getesteten Class3 Reader[6] ein spezielles Kommando dazu benötigt wird, welches scheinbar in Truecrypt nicht implementiert wurde. Es sollte jedoch mit wenig Aufwand möglich sein, diese Funktion nachzurüsten. Ob dennoch Kartenleser existieren, mit denen die PIN-Eingabe am Leser möglich ist, kann nicht ausgeschlossen werden, es wurden jedoch keine Hinweise diesbezüglich gefunden.

Voraussetzung für die Benutzung ist ein installierter PKCS #11 (2.0 oder höher) Softwarestack. Dieser steht dem Pre-Boot-Manager aber nicht zur Verfügung, sodass derartige Hardware nicht für Systemverschlüsselung eingesetzt werden kann. Unter Windows muss beispielsweise die Siemens CardOS API installiert werden, falls eine CardOS Karte benutzt werden soll. Bei Aktivierung der Auto-Detect-Library-Option unter Windwos wird eine vorhandene PKCS#11-Bibliothek automatisch gefunden und verwendet. Unter Linux müssen die Pakete: *opensc, pcsc-lite, pcsc-tools, pkcs11-helper* installiert sein und die Treiber[7] heruntergeladen und installiert werden.

Die Benutzung von Security Tokens und Smartcards ist in allen Versionen verfügbar, allerdings nicht für Systemverschlüsselung.

Anmerkungen:

---

[4] Diese werden unter anderem auch mit Entropie aus Linuxtreibern, z.B. Netzwerktreiber, gefüllt, wobei nur bei /dev/random der Entropiegehalt überwacht wird. In AP4 wird geklärt, welcher dieser beiden wofür verwendet wird.

[5] http://www.rsa.com/rsalabs/node.asp?id=2133

[6] Reiner SCT cyber*Jack*® e-com http://www.reiner-sct.com/content/view/6/17/

[7] http://www.hidglobal.com/driverDownloads.php?techCat=19&prod_id=186#

- Jeder rechtmäßige Benutzer des Tokens ist prinzipiell in der Lage die Daten aus dem Token auszulesen und sich so Kopien zu erzeugen. Bei Rückgabe des Token kann man also nicht davon ausgehen, dass der User keine Kopie mehr besitzt**. Dieses ist aber eine prinzipbedingte Einschränkung einer Festplattenverschlüsselung und könnte nur verhindert werden, wenn die Festplattenverschlüsselung durch die Smartcard erfolgen würde, was aus Performancegründen nicht möglich ist.**

3.2.17 Benutzung / Erstellung von Keyfiles

Jede existierende Datei (.txt, .exe, .mp3, …) kann als TrueCrypt-Keyfile verwendet werden. Zusätzlich kann TrueCrypt Keyfiles mit zufälligem Inhalt erzeugen.

Es ist möglich, einem verschlüsselten Volume mehrere Keyfiles zuzuordnen. Diese müssen dann zur Authentisierung alle gleichzeitig vom Benutzer zur Verfügung gestellt werden. Das Verändern der Keyfilekonfiguration kann nachträglich geschehen, dazu wird der Volume-Header neu geschrieben.

Keyfiles können auch auf PKCS-11 Security Tokens und Smart Cards gespeichert werden. Somit lässt sich eine 2-Faktor-Authentisierung realisieren.

Diese Funktion ist in allen Versionen verfügbar, allerdings nicht für Systemverschlüsselung.

Anmerkungen:

- Keyfiles können nicht für Systemverschlüsselung verwendet werden, da zum Zeitpunkt des Bootens bei der Passwortabfrage noch kein Treiber geladen ist, der Zugriff auf diese Dateien ermöglichen würde.

3.2.18 Multi-Faktor-Authentisierung

TrueCrypt unterstützt die Verwendung von Security Tokens und Smartcards. Somit lässt sich eine 2-Faktor-Authentisierung realisieren. Dies gilt jedoch nicht für die Systemverschlüsselung (siehe auch Abschnitt 3.2.17).

Die 2-Faktor-Authentisierung lässt sich in allen getesteten Versionen, allerdings nicht für Systemverschlüsselung unter Windows nutzen.

3.2.19 Pre-Boot-Authentication

Bei der Verwendung der Systemverschlüsselung muss sich der Benutzer durch die Eingabe des Volume-Passworts authentisieren, bevor das Betriebssystem gebootet wird. Dieser Vorgang wird als Pre-Boot-Authentication bezeichnet.

Diese Funktion ist unter beiden MS Windows Versionen verfügbar. Unter Linux steht die Pre-Boot-Authentication nicht zur Verfügung, da die Systemverschlüsselung durch TrueCrypt nicht möglich ist (siehe Abschnitt 4.1.1).

3.2.20 Revoke Authentication

Revoke Authentication bezeichnet den Vorgang, einem rechtmäßigen Benutzer nachträglich das Recht zu entziehen, die Festplatte zu entschlüsseln. Ein Revoke Authentication kann bei einer

Festplattenverschlüsselung nur durch eine Umschlüsselung des Volumes bewirkt werden. Die von Truecrypt zur Verfügung gestellte Funktion Passwort ändern (siehe Abschnitt 3.2.5) ist jedoch wirkungslos, da ein rechtmäßiger Benutzer in der Lage ist den Volume-Header und somit indirekt auch den Schlüssel zu sichern und später wiederherzustellen.

TrueCrypt bietet in keiner getesteten Version einen Mechanismus für das Zurückziehen der Authentisierung.

3.2.21 Pipelining während Ver- und Entschlüsselung

Ab Version 5.0 verwendet TrueCrypt zur Beschleunigung der Ver- und Entschlüsselung sogenanntes Pipelining (asynchrone Bearbeitung).

Pipelining kommt in beiden MS Windows Versionen zum Einsatz. Unter Linux ist dies nicht möglich (siehe Abschnitt 4.1.2)**.**

3.2.22 AES Hardwarebeschleunigung

TrueCrypt kann ab Version 7.0 die AES Hardwarebeschleunigung aktueller Intel (Core i5/i7) Prozessoren nutzen, wodurch die Ver- und Entschlüsselung um den Faktor 4 bis 8 schneller durchgeführt wird.

Die AES Hardwarebeschleunigung ist in allen getesteten Versionen verfügbar.

3.2.23 Sprachunterstützung

Es sind Third-Party-Sprachpakete (Language Packs) verfügbar, die die TrueCrypt GUI in anderen Sprachen darstellen. Diese Sprachpakete werden durch XML-Dateien zur Verfügung gestellt und unter MS Windows direkt im Programmordner abgelegt. Im Einstellungsmenü erfolgt dann die Sprachauswahl. In einigen Sprachpaketen ist auch die Übersetzung des Benutzerhandbuchs enthalten. Die deutsche Übersetzung ist bis auf kleine Lücken nahezu vollständig.

Die Windows Versionen von TrueCrypt bieten diese Sprachunterstützung an. In der Linuxversion ist sie nicht verfügbar (siehe Abschnitt 4.1.3)**.**

3.2.24 Hotkeys

Es können spezielle Systemweite Tastenkombinationen mit TrueCrypt-Funktionen belegt werden, z.B. „Alle Volumes trennen“.

Die Benutzung von Systemweiten Hotkeys ist nur unter den getesteten MS-Windows Versionen, jedoch nicht unter Linux möglich (siehe Abschnitt 4.1.4)**.**

3.2.25 Benutzen/Verwalten von Favoriten

Es können favorisierte Volumes festgelegt und bei Bedarf gemeinsam eingebunden werden. Weiterhin ist es möglich, festgelegte Volumes einzubinden, sobald sich der Benutzer beim Betriebssystem angemeldet hat.

Unter Windows besteht zusätzlich noch die Möglichkeit, diverse Mountoptionen anzugeben. Hierzu zählen: Einbinden des Volumes, wenn sein Host-Gerät angeschlossen wird, Einbinden beim Anmelden, nicht einbinden, wenn die „Favoriten einbinden“ Tastenkombination gedrückt wird, öffnen einer Explorer Fensters bei erfolgreichem Einbinden und als „read-only“ einbinden.

Das Festlegen von favorisierten Volumes wird von allen Versionen unterstützt. Das automatische Einbinden von Volumes durch TrueCrypt bei Benutzeranmeldung ist hingegen nur unter Windows möglich, unter Linux kann das aber durch entsprechende Skripte die selbe Funktionalität erzielt werden.

3.2.26 Ausführen von TrueCrypt ohne Administratorrechte

TrueCrypt kann von jedem Benutzer, auch ohne Administratorrechte, ausgeführt werden. Voraussetzung dafür ist, dass TrueCrypt zuvor auf dem System von einem Administrator bzw. root installiert wurde.

Unter Windows kann ein normaler Benutzer dann TrueCrypt Container-Dateien erstellen, Volumes (außer das Systemvolume) einbinden, Daten darauf schreiben, davon lesen und selbst eingehängte Volumes wieder trennen. Er kann auch favorisierte Volumes beliebig einhängen und (auch solche, die von anderen Benutzern eingebunden wurden) trennen. (Dies kann aber in der Konfiguration des Betriebssystemes unterbunden werden, siehe [8])

Bei Unixsystemen muss zusätzlich eine Benutzergruppe angelegt werden, welcher alle Benutzer angehören müssen, die TrueCrypt verwenden. Für diese Gruppe muss vom Administrator „sudo“ eingerichtet werden, welches dann TrueCrypt mit root-Rechten startet.

TrueCrypt kann unter allen Versionen ohne Administratorrechte, wenn auch mit teilweise eingeschränktem Funktionsumfang, ausgeführt und benutzt werden.

Anmerkungen:

- Die Festplattenverschlüsselung entscheidet nur, ob die Daten zu Authentisierung des Volumes vorliegen und gültig sind.
- Jeder Nutzer der sich erfolgreich authentisieren kann, startet die transparente Ver- bzw. Entschlüsselung und kann die Festplatte im Betrieb wie eine unverschlüsselte Festplatte nutzen.
- **Daher kann eine Festplattenverschlüsselung prinzipbedingt keine Rechte innerhalb des Dateisystemes durchsetzen.** Das können nur entsprechende Mechanismen des Betriebssystems.
- Die Festplattenverschlüsselung ist prinzipbedingt auch nicht in der Lage, das Einbinden der Festplatte auf bestimmte Punkte (Mountpoints) oder Systeme zu beschränken.

[8] http://www.truecrypt.org/docs/?s=multi-user-environment

3.2.27 Portable Version

TrueCrypt kann auch im sogenannten „Portable-Modus“ ausgeführt werden, wodurch die Installation von TrueCrypt entfällt. Allerdings muss der Benutzer über Administratorrechte verfügen, um TrueCrypt im „Portable-Modus“ ausführen zu können.

TrueCrypt kann auf zwei unterschiedliche Arten im „Portable-Modus“ betrieben werden. Erstens, nach Entpacken des TrueCrypt Installers und Auswahl von „Extract“ anstatt „Install“ oder zweitens durch die Erstellung einer sogenannten „Traveler Disk“. Diese „Traveler Disk“ ist kein TrueCrypt-Volume sondern ein unverschlüsseltes Volume, was die TrueCrypt-Programmdateien beinhaltet.

Die Portable Version ist nur für die beiden MS Windows Versionen verfügbar. Unter Linux steht diese nicht zur Verfügung (siehe Abschnitt 4.1.5)**.**

3.2.28 Trennen der Volumes bei Energiesparmodus (Standby, Ruhezustand)

TrueCrypt kann beim Wechsel in einen Energiesparmodus (Standby / Suspend to RAM, Ruhezustand / Suspend to Disk) automatisch alle verbundenen Volumes trennen.

Diese Funktion ist nur in den getesteten Windows Versionen verfügbar.

3.2.29 Sicherer Ruhezustand

Beim Wechsel in den Ruhezustand (Suspend to disk) wird der RAM-Inhalt in ein Hibernationfile auf die Festplatte geschrieben. Dieses Hibernationfile ist üblicherweise auf der Systempartition gespeichert. Bei Verwendung der Systemverschlüsselung ist somit auch der Inhalt des Hibernationfiles verschlüsselt. Das Reaktivieren des Rechners entspricht aus Hardwaresicht zunächst einem regulären Bootvorgang, bei dem dann das bootende Windows-System das Hibernationfile wieder in den Speicher lädt. Daher muss sich der Benutzer dann wie beim regulären Bootvorgang per Pre-Boot-Authentication authentisieren.

Diese Funktion wird nur von den getesteten MS Windows Versionen unterstützt. Unter Linux ist sie nicht möglich, da die Systemverschlüsselung durch TrueCrypt nicht verfügbar ist (siehe Abschnitt 4.1.6)**.**

3.2.30 Passwort Caching

TrueCrypt erlaubt es, alle Daten von erfolgreichen Authentisierungen im TrueCrypt-Treiber zu cachen. Bei aktiviertem Passwort Caching können Volumes erneut eingebunden werden, ohne dass die Authentisierungsdaten (Passwort / Keyfile / Smartcard) erneut einzugeben sind. TrueCrypt versucht dabei das einzubindende Volume mit den alten Daten aus dem Cache einzubinden, erst wenn das nicht erfolgreich ist, wird der Dialog der Passworteingabe angezeigt.

Das Cachen der Volume-Passwörter wird in allen getesteten Versionen unterstützt.

Anmerkungen:

- Der Passwort-Cache wird unter Windows von allen angemeldeten Benutzern gemeinsam genutzt.

3.2.31 Grafisches Benutzer Interface (GUI) / Kommandozeileninterface (CLI)

Die Bedienung von TrueCrypt erfolgt in der Regel über die Grafische Programmoberfläche (GUI), kann aber sowohl unter Linux als auch unter Windows auch über die Kommandozeile (CLI) gesteuert werden. Somit ist es möglich den Einsatz von TrueCrypt zu automatisieren, z.B. durch den Einsatz von Skripten.

Die folgende Tabelle zeigt die aus Benutzersicht wichtigsten, von TrueCrypt zur Verfügung gestellten Funktionen und ob sich diese Funktionen über die jeweilige GUI (MS Windows oder Linux) und das jeweilige CLI (MS Windows oder Linux) bedienen lassen.

Funktionen, die in auf einem der beiden Betriebssysteme grundsätzlich nicht unterstützt werden, z.B. Systempartition verschlüsseln unter Linux, sind hier nicht aufgelistet, da in diesem Dokument die Windows und Linux Versionen verglichen wurden und nicht die Unterschiede zwischen GUI und CLI.

	GUI		CLI	
Funktion	**Windows**	**Linux**	**Windows**	**Linux**
Volume erstellen	✓	✓	✗	✓
Volume Eigenschaften anzeigen	✓	✓	✗	✓
Volume / Datenträger auswählen	✓	✓	✓	✓
Volume einbinden / trennen	✓	✓	✓	✓
Keyfile zum einbinden verwenden	✓	✓	✓	✓
Cache sicher löschen	✓	✓	✓	✗
Volume Passwort ändern	✓	✓	✗	✓
Keyfiles zu Volume hinzufügen / davon entfernen	✓	✓	✗	✗
Keyfiles erzeugen	✓	✓	✗	✓
Volume Header sichern / wiederherstellen	✓	✓	✗	✓

	GUI		CLI	
Algorithmus für Headerschlüsselableitung ändern	✓	✓	✗	✓
Verwaltung von Favoriten	✓	✓	✗	✗
Verwaltung von Security Tokens	✓	✓	✗	✓

Die wichtigsten Funktionen aus Benutzersicht sind in allen Versionen über die GUI bedienbar. Die Bedienung per Kommandozeile ist unter den Windowsversionen stark eingeschränkt. Unter Linux ist TrueCrypt fast vollständig per Kommandozeile bedienbar.

Anmerkungen:

- Ist für das Kommando eine Passworteingabe nötig, wird unter Windows der grafische Authentisierungsdialog angezeigt. Unter Linux wird ein entsprechender X-Dialog geöffnet und falls keine grafische Oberfläche zur Verfügung steht erfolgt die Abfrage des Passwortes per stdin.
- Es ist unter Linux und Windows möglich die Authentisierungsdaten (Passworte) auf der Kommandozeile mit zu übergeben. Davon wird aber explizit abgeraten, da Betriebssystemfunktionen die alten Befehle und die Passworte in der History speichern könnten.

3.2.32 Verschiedene Dateisysteme

Eine transparente Festplattenverschlüsselung agiert in in Art transparent, dass nach erfolgreicher Authentisierung die Festplatte transparent entschlüsselt wird und das Betriebssystem darauf genau wie auf eine unverschlüsselte Festplatte zugreifen kann. Daher ist diese Verschlüsselung im Prinzip unabhängig von dem auf der entschlüsselten Festplatte verwendeten Dateisystem.

Bei der Anlage von verschlüsselten Partitionen unterstützt TrueCrypt den Benutzer dadurch, dass es gleichzeitig die Formatierung durchführt. Unter Windows kann zwischen den Dateisystemen FAT und NTFS gewählt werden, unter Linux kann FAT, Ext2, Ext3 und Ext4 gewählt werden. Im Gegensatz zu Windows ist unter Linux die Clustergröße nicht einstellbar. Unter Linux kann dafür auch ein Volume ohne Dateisystem erstellt werden, auf das dann manuell beliebige Dateisysteme mit beliebigen Parametern geschrieben werden können.

Unter allen getesteten Versionen sind die betriebssystemtypischen Dateisystem benutzbar.

3.2.33 Unterschiede im Quellcode

Der Quellcode wird in AP4 (Softwareanalyse) im Detail analysiert. Daher wird an dieser Stelle nur ein grober Überblick der Dateien und Verzeichnisse gegeben.

Ein Großteil des Codes der Windows- und Linux-Version sind identisch. Dies betrifft alle Dateien in folgenden Verzeichnissen:

- ./Boot
- ./Common
- ./Crypto
- ./Driver (ohne ./Fuse)
- ./Format
- ./Mount
- ./Platform (ohne ./Unix)
- ./Release
- ./Resources/Text

Zusätzlich zu den oben genannten Verzeichnissen sind bei der Linuxversion noch folgende Verzeichnisse

- ./Build/*
- ./Core
- ./Driver/Fuse
- ./Main/*
- ./Platform/Unix
- ./Resources/Icons
- ./Volume

und Dateien vorhanden:

- ./Build/Makefile
- ./Makefile

Bei der Windows Version sind hingegen folgende Verzeichnisse:

- ./Setup

und Dateien vorhanden:

- ./TrueCrypt.sln
-

Es sind sowohl identische, als auch betriebssystemabhängige Quellcodedateien vorhanden.

3.2.34 Nicht unterstützte Funktionsklassen

In den Quellcodeverzeichnissen existieren Funktionsklassen, welche jedoch in der betreffenden Version nicht unterstützt werden.

Linux:

- Hotkey

- BootEncryption
- Language

4 Nicht vorhandene Funktionen

In diesem Kapitel werden die Ursachen für das Nichtvorhandensein von TrueCrypt-Funktionen in der entsprechenden Version erläutert. Diese Ursachen werden voraussichtlich während der Bearbeitung von AP4 (Softwareanalyse) im Detail erfasst und an dieser Stelle dokumentiert.

4.1 Linux

In den folgenden Abschnitten werden die nicht vorhandenen Funktionen der Linux-Version genauer betrachtet.

4.1.1 Systemverschlüsselung

Die Systemverschlüsselung durch TrueCrypt ist aktuell unter Linux nicht möglich, da die TrueCrypt-Entschlüsselungstreiber vor dem Bootvorgang nicht geladen werden können.

Dieses Problem kann jedoch durch den Einsatz von zusätzlicher Software umgangen werden. Das Projekt Keyrona (http://www.keyrona.org) bietet beispielsweise die Möglichkeit mittels einer Initrd die Systempartition mittels TrueCrypt zu verschlüsseln. Die Bootpartition, auf der das Kernelimage und das Initrd abgelegt sind, bleibt dabei unverschlüsselt.

4.1.2 Pipelining

Die Ursachen für das Fehlen des Pipelinings in der Linux-Version werden während der Bearbeitung von AP4 (Softwareanalyse) erfasst.

4.1.3 Sprachunterstützung

Die Ursachen für das Fehlen der Sprachunterstützung in der Linux-Version werden während der Bearbeitung von AP4 (Softwareanalyse) erfasst.

4.1.4 Hotkey-Unterstützung

Die Ursachen für das Fehlen der Hotkeyunterstützung in der Linux-Version werden während der Bearbeitung von AP4 (Softwareanalyse) erfasst.

4.1.5 Portable Version

Die Ursachen für das Fehlen einer portablen Linux-Version werden während der Bearbeitung von AP4 (Softwareanalyse) erfasst.

4.1.6 Sicherer Ruhezustand

Die Ursachen für das Fehlen des Sicheren Ruhezustandes unter Linux ist in erster Linie das Fehlen der Systemverschlüsselung. Da bei dieser Funktion nicht Mechanismen aus dem BIOS, sondern Mechanismen des Betriebssystemes genutzt werden, kann davon ausgegangen werden, dass, sobald eine Systemverschlüsselung unter Linux möglich, ist auch der Ruhezustand unterstützt wird.

5 ASE_INT.NfD – Security Target Introduction

5.1 ST / TOE Reference

Der zu evaluierende Gegenstand ist die Software

TrueCrypt in Version 7.0 vom 19.07.2010 erstellt durch die TrueCrypt Developers Association.

5.2 TOE Overview

5.2.1 Usage and major security features of the TOE

Das TOE ist ein Softwaresystem für die Erstellung und Verwaltung von verschlüsselten Datenträgern – Verschlüsselungssoftware. Als Datenträger sind dabei beispielsweise Festplatten, USB-Sticks, Containerdatei, usw. zu verstehen – Volumes. Das vollständige Dateisystem dieser Datenträger wird vom TOE auf Blockebene verschlüsselt, also neben Dateien und Verzeichnissen auch Metadaten und ungenutzter Speicher. Die Ver- und Entschlüsselung erfolgt hierbei automatisch, d.h. transparent und on-the-fly, also ohne Benutzerinteraktion. Ohne die Verwendung des entsprechenden Passworts oder Schlüssels können die Daten auf diesen Datenträgern nicht gelesen oder geschrieben werden. Für die Verschlüsselung selbst steht eine Vielzahl der gebräuchlichsten Algorithmen zur Verfügung.

Das TOE bietet folgende Sicherheitsleistungen:

- Verschlüsselung
- Authentisierung
- Abstreitbarkeit[9]

5.2.2 TOE Type

Im Allgemeinen ist das TOE eine Softwareapplikation – „software application“. Genauer: Das TOE ist eine Verschlüsselungssoftware, die zum Erstellen und Verwalten von verschlüsselten Datenträgern (Volumes) eingesetzt wird und dem autorisierten Anwender Zugriff auf die gespeicherten Daten gewährt.

5.2.3 Required non-TOE hardware/software/firmware

Voraussetzungen für die Nutzung von TrueCrypt sind:

- Rechnersystem
- Betriebssystem
  - MS Windows 7, Vista, XP, Server 2008, Server 2003 (32 / 64 Bit), Windows 2000
  - Linux (Kernel 2.4, 2.6; mit Devicemapper)

[9]Der Benutzer streitet erfolgreich ab, dass eine Verschlüsselung verwendet wird.

- Mac OS X 10.4, 10.5, 10.6

- Datenträger
  - Festplatte
  - USB-Stick
  - etc.

5.3 TOE Description

5.3.1 Physical Scope

Das TOE ist ein reines Softwareprodukt, das als Binärdatei oder Quellcode zur Verfügung steht. Weiterhin sind Benutzerdokumentation und FAQs vorhanden. Für die Verwendung des TOE ist ein Rechnersystem und eines der unter Abschnitt 5.2.3 Required non-TOE hardware/software/firmware dargestellten Betriebssysteme notwendig.

5.3.2 Logical Scope

Im folgenden Abschnitt werden die vom TOE zur Verfügung gestellten Sicherheitsleistungen dargestellt.

Verschlüsselung	Das TOE wird verwendet, um verschlüsselte Volumes zu Erstellen und zu Verwalten. Durch das Einbinden dieser Volumes wird dem autorisierten Anwender der Zugriff auf die gespeicherten Daten gewährt. Die Dateien, die in dem Volume gespeichert sind, können dabei wie ganz gewöhnliche Dateien behandelt werden. Der Anwender kann sie lesen, schreiben, kopieren, verschieben, etc. Die Ver-, Entschlüsselung wird dabei transparent und on-the-fly durchgeführt. Nicht autorisierte Benutzer können hingegen das Volume nicht einbinden und erhalten somit auch keinen Zugriff auf die Dateien, die in dem Volume gespeichert sind. Bei der Erstellung eines Volumes wird der sogenannte Volume-Header angelegt. Dieser verschlüsselte Volume-Header beinhaltet neben wichtigen Informationen wie der Größe des Volumes, Byte Offset des Datenbereichs auch die geheimen Master-Keys, die zur Verschlüsselung der einzelnen Blöcke verwendet wird. Die Bereiche des Volume-Headers, die sensitive Daten enthalten, z.B. Master-Keys, sind wiederum mit dem sogenannten Header-Key verschlüsselt. Der Header-Key wird vom Volume-Passwort, das der Anwender selbst vergeben kann, einem Keyfile oder beidem abgeleitet. Für die Verschlüsselung des Volumes stellt das TOE folgende Algorithmen zur Verfügung: • AES

	• Serpent • Twofish • AES-Twofish • AES-Twofish-Serpent • Serpent-AES • Serpent-Twofish-AES • Twofish-Serpent Folgender, vereinfachter Zusammenhang lässt sich beschreiben: • Anwender autorisiert sich durch Passworteingabe, Keyfile oder beides • Das TOE entschlüsselt den Volume-Header und erhält Zugriff auf den Master-Key • Das TOE ver- und entschlüsselt die entsprechenden Blöcke mit dem Master-Key
Verschlüsselung der Systempartition (nur MS Windows)	Das TOE bietet für MS Windows Betriebssysteme die Möglichkeit der Verschlüsselung der Systempartition, d.h. der Partition auf welcher Windows installiert ist und von welcher es bootet. Dadurch wird ein hohes Maß an Sicherheit erzielt, da dabei alle von Windows erzeugten Dateien (Swapfile, Hibernationfile, temporäre Dateien) mit verschlüsselt werden. Die hierbei zum Einsatz kommenden Verschlüsselungsalgorithmen entsprechen denen für die Verschlüsselung von Standarddatenträgern. Bei Verschlüsselung der Systempartition wird der Einsatz der Pre-Boot-Authentication notwendig.
Authentisierung	Die Authentisierung der Anwender erfolgt durch Passwort, Keyfile, Security Token oder SmartCards.
Pre-Boot-Authentication (nur MS Windows)	Pre-Boot-Authentication kommt bei Verwendung einer verschlüsselten Systempartition unter MS Windows zum Einsatz. Dabei erfolgt vor dem Starten des Betriebssystems die Authentisierung des Benutzers durch Passworteingabe.