[redacted]

[redacted]

Untersuchung TrueCrypt

Arbeitspaket 3

Angriffsszenarien und Bedrohungsanalyse

[redacted]

Version:	1.0
Datum:	16. November, 2010

Historie

Version	Autor	Kommentar	Datum
0.1	[redacted]	Initiale Dokumentenversion erstellt	20.09.10
0.2		Modifizierte Vorgehensweise	01.10.10
0.3		Deutlichere Darstellung und Strukturierung	06.10.10
0.4		Angriffsbaum System, Annahmen, Entwurf Zusammenfassung	14.10.10
0.5	[redacted]	Zusammenfassung, bleibende Angriffe, Software-Lebenszyklus, Erläuterungen Annahmen, spezielle Angriffe explizit erwähnt, SSD	26.10.10
0.6		Referenzen, Anmerkungen BSI	02.11.10
0.7	[redacted]	Review	04.11.10
0.9		Kommentare aus Review eingearbeitet	05.11.10
1.0		Version zur Abnahme	16.11.10

Inhaltsverzeichnis

1 Methodik

1.1 Angriffsbaum

In diesem Dokument werden die Bedrohungen analysiert, die auf das Festplattenverschlüsselungsprogramm TrueCrypt einwirken können. Dabei werden zusätzlich auch Angriffe auf ein allgemeines Produkt „Festplattenverschlüsselung" betrachtet, die jedoch durch TrueCrypt in seiner momentanen Implementierung abgewehrt werden oder durch Besonderheiten in der Implementierung gar nicht erst auftreten können. Diese erweiterten Angriffe können jedoch – da das Ziel „Festplattenverschlüsselung" unscharf ist – unvollständig sein.

Zuerst werden alle zu schützenden primären Werte (*Assets*) und die bedrohten Eigenschaften dieser Werte gesammelt. Durch den konkreten Einsatz einer Festplattenverschlüsselung ergeben sich aus deren Konstruktion weitere sekundäre zu schützenden Werte, mit denen genauso verfahren wird.

Ausgehend von diesen Werten wird für jeden Wert ein Teil-Angriffsbaum erstellt. Dabei werden zunächst alle bedrohten Eigenschaften dieser Werte betrachtet, und dann strukturiert alle Möglichkeiten erfasst, um diese Eigenschaften anzugreifen.

Die Strukturierung wird dabei in jeder Ebene so allgemein gewählt, dass einerseits gewährleistet bleibt, dass keine Angriffe übersehen werden, andererseits die notwendige Übersichtlichkeit hergestellt wird.

Ein Knoten stellt jeweils ein Angriffsziel dar. Um den in einem mit UND bezeichneten Knoten beschriebenen Angriff durchzuführen, müssen alle in den Kindknoten dargestellten Ziele erreicht werden.

Falls ein Knoten ein ODER-Knoten ist (dies ist der weitaus häufigere Fall, daher wird hier nicht gesondert beschriftet) dann sind die Kindknoten dieses Knotens die verschiedenen unabhängigen Möglichkeiten, dieses Angriffsziel zu erreichen.

Bei der Erstellung von aus einzelnen Knoten ausgehenden Verzweigungen wird dabei jeweils nach passenden Kriterien gegliedert, wie: Ort, physikalischen (die Hardware betreffende) und logischen (Software/Daten betreffende), eingesetzten Algorithmen/Technologien, durch Datenstrukturen vorgegebene Kategorien, betreffend eines Zeitpunktes bzw. einer Zeitdauer, indirekt/direkt, Anzahlen.

Bei jedem Angriff werden mögliche Gegenmaßnahmen bzw. Anforderungen genannt, um diesen abzuwehren oder Annahmen gemacht, die erfüllt sein müssen, damit der Angriff nicht zutrifft. Dies können einerseits schon von TrueCrypt erbrachte, oder noch nicht erbrachte, aber wünschenswerte Leistungen sein. Andererseits wird auch auf anderweitige Maßnahmen verwiesen, wie z.B. organisatorische, oder durch das Betriebssystem erbrachte, mit deren Hilfe der Angriff abgewehrt werden kann oder muss.

Diese Anforderungen werden dann gesammelt.

Falls ein Angriff auf einen Wert durch einen bestimmten Angriff oder eine Kategorie von Angriffen auf einen anderen Wert ermöglicht wird, wird der Baum an dieser Stelle

abgebrochen und entsprechend verwiesen. Genauso wird verfahren bei an unterschiedlichen Stellen auftauchenden identischen oder bei zu langen Angriffsbäumen.

1.2 Angriffspotential

Für die Blätter wird jeweils das Angriffspotential abgeschätzt. Dies geschieht in Anlehnung an die Bewertung in den Common Criteria (AVA_VAN) (Siehe Anhang A). Es wird dabei die Vorbereitung und die Durchführung eines Angriffs nach den Faktoren Gesamtzeit (Time), Expertise des Angreifers, den notwendigen Zugriff auf den Evaluationsgegenstand (Window of Opportunity, W.o.O.) und notwendige Ausrüstung (Equipment) bewertet und aufsummiert. An geeigneten Stellen wird auch eine mathematische Aufwandsabschätzung angegeben.

Mit Hilfe dieser Informationen können nun optimale Angriffspfade gefunden werden.

Dabei ist zu beachten, dass TrueCrypt einer Open-Source-Lizenz unterliegt, sodass das Design von TrueCrypt selbst grundsätzlich als öffentlich bekannt anzunehmen ist und somit jedem Angreifer mit der notwendigen Expertise zugänglich ist. Für hardwarebasierte, eng mit geschlossenen Betriebssystemen oder auf unbekannten Sicherheitslücken arbeitende Angriff können dennoch nicht-öffentliche Kenntnisse vonnöten sein, was auch an den entsprechenden Stellen in die Bewertung mit einfließt.

1.3 Zusammenfassung

Abschließend werden die Annahmen diskutiert, die wünschenswert bzw. vorgesehen sind, aber in TrueCrypt derzeit noch nicht implementiert sind.

Die erfolgreichen Angriffe werden dann gesammelt und Empfehlungen hinsichtlich deren Abwehr gegeben.

2 Angreifermodell

Zuerst wird unterschieden zwischen internem und externem Angreifer.

Der externe Angreifer hat Zugriff auf das verschlüsselte System bzw. den verschlüsselten Datenträger im ausgeschalteten, d.h. inaktiven Zustand. Er kann auch an ein System mit aktivierter Festplattenverschlüsselung gelangen, welches aber gegen direkten Zugriff gesichert ist, d.h. etwa durch einen passwortgeschützten Bildschirmschoner.(*** siehe 6.1)

Desweiteren kann er den Software-Lebenszyklus angreifen, also Installationsdateien beim Download manipulieren usw.

Der interne Angreifer hat zusätzlich zu den Eigenschaften des externen Angreifers noch Zugriff auf das System mittels eines eigenen Benutzerzugangs.

Insbesondere der Administrator und der Geheimnisträger selbst seien vertrauenswürdig.

Die Spanne im Angriffspotential reicht von wenig motivierten Tätern mit wenig Ausrüstung, wie „der neugierige Kollege", über Amateur-Hacker bis hin zu mit großen finanziellen Mitteln ausgestatteten Tätern, wie sie im Zusammenhang mit Industriespionage, organisiertem Verbrechen und Geheimdiensten auftreten.

3 Bedrohte Werte und Eigenschaften

3.1 Bedrohter primärer Wert

Es sollen unter Verschluss zu haltenden Daten bearbeitet werden. Diese sind als primärer Wert bedroht. Genau genommen sind folgende Eigenschaften bedroht:

- W1 Daten
  - E1 Vertraulichkeit
    - E1.1 Teile der Daten selbst
    - E1.2 Die Information, ob ein Datenträger nur Zufallsdaten oder verschlüsselte Daten enthält. (Unterscheidbarkeit)
    - E1.3 Informationen über die Menge an Daten
    - E1.4 Informationen über Änderungen an Daten
    - E1.5 Die Information, ob ein bestimmtes – vorgegebenes – Datum auf dem Datenträger enthalten ist.
  - E2 Integrität
  - E3 Verfügbarkeit

3.2 Bedrohte sekundäre Werte

Um den primären Wert zu schützen, werden die Daten auf einem Datenträger verschlüsselt gespeichert und auf einem verschlüsselten System bearbeitet. (Näheres zum Aufbau von TrueCrypt siehe AP4).

Dadurch ergeben sich sekundäre Werte mit Eigenschaften, die zu schützen sind, und zwar:

- W2 Volume-Schlüssel
  - E4 Vertraulichkeit
- W3 Header-Schlüssel
  - E5 Vertraulichkeit
- W4 Authentifizierungsmerkmale
  - W4.1 Passwort
    - E6 Vertraulichkeit
  - W4.2 Smartcard
    - E7 Besitz
  - W4.3 PIN

E8 Vertraulichkeit

E9 Vertraulichkeit des Smartcard-Keyfiles

W5 System (schließt Konfigurationsdaten mit ein)

E10 Integrität

E11 Vertraulichkeit (RAM, Temporäre Dateien, Swap usw.)

E12 Verfügbarkeit

W6 Algorithmen

E13 Vertraulichkeit

W7 Software-Lebenszyklus

W7.1 Installation

E13.1 Integrität

W7.2 Update

E13.2 Integrität

W7.3 Reparaturen

E13.3 Vertraulichkeit

W7.4 Deinstallation

E13.4 Vertraulichkeit

4 Annahmen und Anforderungen

Folgende Annahmen und Anforderungen müssen vorausgesetzt werden bzw. ergeben sich aus dem Baum. Mit (*) markierte können entweder nicht mit der momentanen Version von TrueCrypt erfüllt werden und benötigen eine Erweiterung bzw. Zusatzsoftware oder sind anderweitig problematisch, siehe dazu Kapitel 6.1 .

Mit (**) markierte Punkte werden in Kapitel 4.1 kurz näher erläutert.

A1 Der System-Administrator ist vertrauenswürdig.

A2 Das Volume muss vor oder bei dem Formatieren sicher gelöscht werden.

A2.1 Es darf insbesondere kein Quickformat verwendet werden.

A3 Auf dem Datenträger wurden vor dem Einsatz der Festplattenverschlüsselung und auch während des Einsatzes nie sensible Daten im Klartext gespeichert.

A4 ATA-TRIM ist deaktiviert.

A5 Die Kryptoalgorithmen sind sicher.

A5.1 Die Kryptoalgorithmen sind korrekt implementiert.

A5.2 Es wird ein sicherer Kryptoalgorithmus verwendet.

A5.3 Es wird ein sicherer Betriebsmodus verwendet.

A5.4 Die Kryptoalgorithmen werden innerhalb ihrer Parameter eingesetzt

A6 Umschlüsseln (*)

A6.1 Durch Mitzählen der verschlüsselten Datenmenge wird rechtzeitig ein Umschlüsseln erzwungen. Der Zähler wird sicher gespeichert.(*)

A6.2 Wird eine Verschleierung von Änderungen gewünscht, muss das Volume vollständig umgeschlüsselt werden.

A6.3 Beim Entzug von Zugriffsrechten auf ein Volume wird dieses Volume vollständig umgeschlüsselt.

A7 Der Datenträger wird durch Siegel vor unbemerkter Benutzung geschützt.(**)

A8 Es wird eine Integritätssicherung durchgeführt.(*) (**)

A8.1 Es wird eine blockweise Integritätssicherung durchgeführt.(*)

A8.2 Es wird eine vollständige Integritätssicherung durchgeführt.(*)

A9 Es wird verhindert, dass mehrere Versionen eines Datenträgers mit dem gleichen Schlüssel vorhanden sind.

A9.1 Es werden nur physikalische Datenträger benutzt, also keine Container.

A9.2 Physikalische Datenträger werden nicht bitweise geklont.

A10 Es sind sicher verwahrte Backups der Header vorhanden. (**)

A11 Unnötige Anzeigen werden unterbunden.(*)

A11.1 Die Anzeige von Schlüsselmaterial wird unterbunden.

A11.2 Die Anzeige von Zufallsmaterial wird unterbunden.

A12 Es wird ein sicherer Zufallsgenerator verwendet. (**)

A13 Sicherer Umgang mit Authentisierungsmerkmalen.

A13.1 Es werden sichere Passwörter verwendet.

A13.2 Passwörter werden sicher behandelt.

A14 Es wird eine passend zertifizierte Smartcard verwendet.

A15 Es wird ein zertifizierter Smartcard-Leser eingesetzt. (**)

A15.1 Die Verbindung zwischen Rechner und Smartcard ist sicher. (**)

A15.2 Die Benutzer sind geschult im Umgang mit dem Smartcard-Leser.

A15.3 Die Smartcard wird nur für Festplattenverschlüsselung benutzt.

A16 Das Betriebssystem ist sicher.(*)

A16.1 Das Betriebssystem setzt eine Benutzertrennung zuverlässig durch.

A16.2 Es ist keine relevante Sicherheitslücke in Betriebssystem oder Drittsoftware vorhanden.

A16.3 Das Betriebssystem oder Drittsoftware schützt vor Angriffen über das Netz.

A17 Innerhalb des Volumes sind die Zugriffsrechte geeignet beschränkt.

A18 Es werden nur die Funktionen benutzt, die keine Administratorrechte seitens des Benutzers erfordern.

A19 Ein benutzter Passwort-Cache ist nach Benutzern getrennt.

A20 Angriffe über externe Schnittstellen werden verhindert.

A20.1 Erweiterungssteckplätze sind gegen Zugang von außen logisch oder physikalisch abgesichert.

Dies kann z.B. durch Deaktivieren der Treiber oder physikalisches Unbrauchbarmachen sichergestellt werden.

A20.2 Firewire-Anschlüsse sind gegen Zugang von außen logisch oder physikalisch abgesichert.

Stichwort: Treibereinstellungen/IOMMU

A20.3 Der Docking-Port wird behandelt wie alle darüber verfügbaren Anschlüsse

A20.4 Docking-Stationen werden genauso behandelt wie der zugehörige PC.

A21 Das Booten von anderen Quellen als der eingebauten Festplatte ist im BIOS deaktiviert.

A21.1 Das BIOS ist mit einem Passwort vor Veränderung geschützt.

A21.2 Der Veränderungsschutz des BIOS lässt sich nicht durch ein Masterpasswort umgehen.

A21.3 Es wird ein Rechner verwendet, bei dem das Rücksetzen der BIOS-Einstellungen nicht trivial möglich ist.

A21.4 Das Laden eines Erweiterungs-BIOS ist im BIOS abgeschaltet.

A22 Vor jedem Start wird die physikalische Integrität des Rechners und aller mit ihm verbundener weiterer Komponenten durch den Benutzer überprüft, z.B. durch Siegel.

A22.1 Der Benutzer stellt sicher, dass er ein ihm bekanntes System vor sich hat.

A22.2 Der Benutzer versichert sich, dass alle Komponenten des Systems unverändert sind.

A22.3 Der Benutzer überprüft vor jedem Systemstart die Integrität der Schnittstellen.

A23 Der Benutzer ist geschult im sicheren Umgang mit dem System.

A24 Bei Abwesenheit des Benutzers muss dafür gesorgt werden, dass keine sensiblen Daten und Schlüssel im RAM mehr gespeichert sind. (***,siehe 6.1)

A24.1 Beim regulären Herunterfahren müssen Daten und Schlüssel aus dem RAM gelöscht werden. (*)

A24.2 Nach ungesichertem Ausschalten und Abstürzen muss der Benutzer den ausgeschalteten Rechner mehrere Minuten beaufsichtigen.

A25 Die Speichermodule werden mittels Kleber fixiert und isoliert. (*)

A26 Zur Abwehr von Cache-Timing-Angriffen auf AES wird eine Hardwarebeschleunigung eingesetzt.

A27 Geheim zu haltende Algorithmen müssen entweder vom System getrennt sein oder durch einen öffentlichen Kryptoalgorithmus geschützt werden. (*)

A28 Das System ist verschlüsselt.

A28.1 Der Auslagerungsspeicher wird verschlüsselt.

A28.2 Alle möglichen Orte für temporäre Dateien sind verschlüsselt.

A29 Bei der Deinstallation dürfen keine Informationen bezüglich der verarbeiteten sensiblen Daten mehr im System enthalten sein.

A29.1 Bei der Deinstallation wird der Swap sicher gelöscht.

A29.2 Es müssen alle freien Bereiche innerhalb des verschlüsselten Volumes vor der Deinstallation sicher gelöscht sein.

A30 Alle zu installierenden Dateien werden zuvor per Signatur auf ihre Integrität geprüft.

A31 Der Quelltext wurde vollständig auf Fehler und Hintertüren untersucht.

A32 Es wird ein von einer vertrauenswürdigen Instanz kompilierter oder verifizierter Binärcode verwendet.

4.1 Erläuterungen

Zu A2.1 (Quickformat)

Es wird von TrueCrypt die Option „Quickformat" angeboten. Wenn sie aktiviert ist, werden nur die Verwaltungsinformationen für das Dateisystem verschlüsselt geschrieben. Der weitere (freie) Platz wird nicht berührt. Die dort enthaltenen Rückstände bzw. die Tatsache, dass dieser Platz vom Angreifer als unverschlüsselt erkennbar sein kann, führt zu unten beschriebenen Angriffen.

Wenn die Option deaktiviert ist, überschreibt TrueCrypt vor dem eigentlichen Formatieren das Volume mit Zufallsdaten. Tatsächlich fordert TrueCrypt die darauf folgende eigentliche Formatierung unabhängig davon vom System immer als Quickformat an.

Das System schreibt dann nur die für das Dateisystem nötigen Verwaltungsinformationen auf das Volume, ohne sich um den freien Speicherplatz zu kümmern.

Der Hintergrund ist, dass so der freie Speicher sowohl bei Betrachtung von außerhalb als auch von innerhalb des Volumes mit (Pseudo-)Zufall belegt ist und so eine Nutzung dieses freien Speichers durch ein verstecktes Volume erst möglich wird. Bei

der direkten Voll-Formatierung durch das System würde der freie Platz innerhalb des Volumes mit Nullen belegt sein.

Zu A7 (Schutz vor unbemerkter Benutzung durch Siegel)

Der Datenträger muss so versiegelt werden, dass jegliche Manipulation an der Hardware und jeder Zugriff auf die Daten erkannt wird. Dies kann z.B. durch ein Siegel an den Schnittstellen geschehen oder in einem entsprechenden Umschlag. Je nach Einsatzszenario muss dann das Siegel nach jeder rechtmäßigen Benutzung neu angebracht werden.

Zu A8 (Integritätssicherung)

Dies kann z.B. blockweise passieren, wie die Verwendung eines integritätssichernden Betriebsmodus oder eines RAIDs inherhalb des verschlüsselten Volumes, schützt dann aber nicht gegen alle aufgeführten Angriffe. Umfassendere Integritätssicherung kann durch zusätzliche Software stattfinden. Darüber hinaus kann ein Dateisystem mit aktivierter Integritätssicherung wie ZFS verwendet werden. Siehe dazu auch AP4.

Zu A10 (Headerbackup)

Es muss ein Headerbackup verfügbar sein, das so verwahrt sein muss, dass nur (wenige) Berechtigte darauf Zugriff haben.

Zu A12 (Zufallszahlengenerator)

Der Zufallszahlengenerator muss für kryptografische Anwendungen geeignet sein. Die genaue Konstruktion des TrueCrypt-Zufallszahlengenerators und dessen Eignung wird näher in AP4 und AP5 betrachtet.

Zu A15 (Smartcard-Leser)

Der Smartcard-Leser muss dem für die Festplattenverschlüsselung erforderlich Schutzgrad entsprechen. Insbesondere muss er gegen Abhören und Manipulation gesichert sein. Dies kann im einfachsten Falle durch eine geeignete anderweitige Zertifizierung sichergestellt werden.

Zu A15.1 (sichere Verbindung)

Die Verbindung sowohl zwischen System und Smartcard-Leser sowie zwischen Smartcard-Leser und Smartcard müssen geeignet manipulations- und abhörsicher sein, z.B. durch markiertes Kabel bzw. geeignete mechanische Bauweise u.ä.

5 Angriffsszenarien

5.1 Angriffsbaum Daten (W1)

B 1 Vertrauliche Informationen erhalten (E1)

B 1.1 Teile der Daten selbst auslesen (E1.1)

B 1.1.1 Angriff auf Volume

B 1.1.1.1 Bestehende Rückstände

Wenn ein Datenträger vor dem Einsatz der Verschlüsselungssoftware unverschlüsselt eingesetzt wurde, können Rückstände auf dem Datenträger verbleiben.

B 1.1.1.1.1 Für das Betriebssystem sichtbare Rückstände

Es können Rückstände auf der für das Betriebssystem sichtbaren logischen Sektorstruktur vorliegen.

Bewertung: Hierzu liegen gängige vollautomatische Analysewerkzeug als Open Source vor (z.B. PhotoRec[1]).

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0	2	0	1	0	3

Gegenmaßnahme: Quickformat verhindern bzw. „sicheres Löschen".

Annahmen: A2 Das Volume muss vor oder bei dem Formatieren sicher gelöscht werden.
A2.1 Es darf insbesondere kein Quickformat verwendet werden.

B 1.1.1.1.2 Für das Betriebssystem nicht sichtbare Rückstände

Wenn die Firmware einer Festplatte einen defekten Sektor vermutet, kann sie den Zugriff darauf umleiten auf einen Reservesektor. Der Originalsektor wird ab diesem Zeitpunkt unsichtbar für Betriebssysteme, auf diesem Sektor vorhandene Daten werden auf den neuen Sektor kopiert, bleiben aber auf Dauer auf dem alten Sektor erhalten.
Bewertung: Es ist mit speziellen ATA-/Firmwarebefehlen oder mit Hardware-Lesegeräten möglich, diese Sektoren auszulesen. Die erforderlichen Kenntnisse und die Spezialausrüstung stehen Festplattenherstellern bzw. Datenrettungsfirmen zur Verfügung.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
2	8	5	3	7	25

Gegenmaßnahmen: Sensible Daten nie im Klartext speichern; Spezielle Löschbefehle an die Festplatte zum Löschen auch dieser versteckten Sektoren.

Annahme: A3 Auf dem Datenträger wurden vor dem Einsatz der Festplattenverschlüsselung und auch während des Einsatzes nie sensible Daten im Klartext gespeichert.

B 1.1.1.2 Neue Rückstände

Durch Fehler in der Verschlüsselungssoftware könnten Klartextrückstände auf das Volume gelangen.

1 http://www.cgsecurity.org/wiki/PhotoRec

Annahme: A5.1 Die Kryptoalgorithmen sind korrekt implementiert.

B 1.1.1.3 Brechen des Verschlüsselungsalgorithmus

Der Verschlüsselungsalgorithmus selbst könnte gebrochen werden.

Bewertung: Bis jetzt sind keine praktisch relevanten Angriffe auf AES bekannt.

Annahme: A5.2 Es wird ein sicherer Kryptoalgorithmus verwendet.

B 1.1.2 Erlangen des Volume-Schlüssels

Siehe B 4

B 1.1.3 Durch Manipulation des auslesenden Systems

siehe B 9.1

B 1.2 Zufallsdaten von verschlüsselten Daten unterscheiden (E1.2)

B 1.2.1 Brechen des Kryptoalgorithmus (Known Ciphertext-Angriff)

Bewertung: Keine praktisch nutzbaren Angriffe auf AES bekannt.

Annahme: A5.2 Es wird ein sicherer Kryptoalgorithmus verwendet.

B 1.2.2 Brechen der Betriebsart des Kryptoalgorithmus

Je nach Betriebsart ergeben sich unabhängig von der damit verwendeten Blockchiffre weitere Angriffe.

B 1.2.2.1 ECB

Es können sowohl einfache Muster in bestehenden Daten erkannt werden als auch über Einschleusen von Daten trivial eigene Muster platziert werden.

Bewertung: Für TrueCrypt nicht zutreffend, da es dort nicht verwendet wird.

B 1.2.2.2 CBC mit schlechter Wahl des IV

Siehe B 1.5.2 Watermarking

Bewertung: Für TrueCrypt mit neuen Volumes nicht zutreffend.
Annahme: Es wird ein sicherer Betriebsmodus verwendet.

B 1.2.2.3 LRW brechen

Kann gebrochen werden, wenn im Betriebsmodus LRW der Schlüssel auf dem verschlüsseltem Volume gespeichert wird. Dies kann hauptsächlich durch Auslagern von Speicherinhalten passieren.

Gegenmaßnahme: LRW vermeiden oder Auslagern verhindern.

Annahme: A5.3 Es wird ein sicherer Betriebsmodus verwendet.

B 1.2.2.4 XTS: Zu viele verschlüsselte Daten

Bewertung: Für XTS sind Einheiten mit maximal 2^20 Blöcken zugelassen, also für AES mit 128-Bit-Blöcken ca. 17 MB[2]. Je nach verlangter Sicherheit wird empfohlen, insgesamt maximal 1 TB mit dem gleichen Schlüssel zu verschlüsseln.[3] [4]

Dies ist lediglich eine Abschätzung für die Betriebsart XTS und (außer bezüglich der Blockgröße) unabhängig vom tatsächlichen Algorithmus.

Annahme: A5.4 Die Kryptoalgorithmen werden innerhalb ihrer Parameter eingesetzt.

B 1.2.2.5 Zu viele verschlüsselte Daten

Wenn zu viele Daten mit dem gleichen Schlüssel verschlüsselt werden, kann dies einen Angriff erleichtern. Dies müsste TrueCrypt mitzählen und diesen Zähler sicher speichern, z.B. in einem Trusted Platform Modul (TPM) oder in einem integritätsgesicherten Bereich. Dabei muss auch beachtet werden, dass ein vollständiges Rücksetzen des gesamten Volumes den Zähler nicht rücksetzt oder zumindest als Manipulation erkannt wird.

Annahme: A6.1 Durch Mitzählen der verschlüsselten Datenmenge wird rechtzeitig ein Umschlüsseln erzwungen. Der Zähler wird sicher gespeichert.

B 1.3 Informationen über Füllstand/leere Bereiche erlangen (E1.3)

B 1.3.1 Quickformat

Bei Anwendung von Quickformat auf eine Festplatte, die Nullen oder anderen offensichtlich Klartext enthält, können Rückschlüsse auf den Füllstand geschlossen werden. Zu Anfang ist nämlich nur ein kleiner Bruchteil der als Klartext erkennbaren Daten mit Verwaltungsinformationen des Dateisystems überschrieben. Für jede neu angelegte und beschriebene Datei wird der entsprechende bis dahin im Schlüsseltext als leer erkennbare Bereich mit quasi-zufälligen Daten belegt und ist so als belegt erkennbar. Je mehr dieser beschriebenen Bereiche vom Dateisystem im Laufe der Zeit als gelöscht markiert wird, desto weniger Informationen über den Füllstand kann also ein Angreifer erhalten.

Annahmen: A2 Das Volume muss vor oder bei dem Formatieren sicher gelöscht werden.
A2.1 Es darf insbesondere kein Quickformat verwendet werden.

---

2 NIST Special Publication (SP) 800-38E

3 IEEE Std 1619-2007

4 Moses Liskov and Kazuhiko Minematsu. Comments on XTS-AES. 2008. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/XTS/XTS_comments-Liskov_Minematsu.pdf

B 1.3.2 TRIM

Mittels des ATA-TRIM-Kommandos können Speicherseiten innerhalb von größeren Flash-Blöcken als gelöscht markiert werden. Dies gilt nur für SSD, die über ATA angebunden sind, nicht jedoch für USB-Datenträger.

Das Betriebssystem macht ohne Verschlüsselung gegenüber der SSD jede freie Speicherseite bekannt. TrueCrypt reicht das TRIM-Kommando unter Windows *nur bei der Systemverschlüsselung* an den darunterliegenden Datenträger durch. Linux unterstützt dies für den Krypto-Devicemapper (dm-crypt) generell noch nicht, jedoch für andere Funktionen des Devicemappers, sodass mit einer Unterstützung in näherer Zukunft gerechnet werden kann.

Üblicherweise werden dann die freien Seiten sofort gelöscht, um das spätere Beschreiben zu beschleunigen. Laut Standard ist der Inhalt einer solchen Seite dann undefiniert. Es muss aber damit gerechnet werden, dass für einen Angreifer auch ohne spezielle Kenntnisse der speziellen Hardware jeder freie Block bekannt ist (weil ein Lesezugriff darauf z.B. immer in dem gleichen, oder einem beliebigen, aber als nicht zufällig erkennbarem Muster resultiert)

Gegenmaßnahme: TRIM deaktivieren.

Annahme: A4 ATA-TRIM ist deaktiviert.

B 1.4 Informationen über Änderungen erhalten (E1.4)

XTS ist wie LRW ein Narrow-Block-Betriebsmodus. d.h. Änderungen sind in diesem Fall mit der Granularität einer AES-Blockgröße, also 128 Bit = 16 Byte nachverfolgbar.

Bei ECB sind sogar gleiche Blöcke erkennbar.

Bei CBC ist nur noch erkennbar, ab welchem 16-Byte-Block sich ein Sektor geändert hat.

Bei Wide-Block-Betriebsmodi (nicht in TrueCrypt implementiert) ist das nur auf Sektorebene möglich.

B 1.4.1 Mindestens 2 Abbilder von Volume mit gleichem Schlüssel erlangen

B 1.4.1.1 Ein einziges Volume

Wenn ein Angreifer zweimal Zugriff auf ein Volume erlangt, kann er Änderungen zwischen diesen beiden Zugriffen nachverfolgen.

Gegenmaßnahmen: probabilistic encryption, vollständig umschlüsseln.

Annahme: A6.2 Wird eine Verschleierung von Änderungen gewünscht, muss das Volume vollständig umgeschlüsselt werden.

B 1.4.1.2 Mehrere Volumes

Es liegen unterschiedliche Datenträger vor, die aber mit dem gleichen Volume-Schlüssel verschlüsselt sind. (i.A. weil sie alle von einem einzigen Ur-Volume geklont wurden.

Gegenmaßnahme: Klonen verhindern, Umschlüsseln, Container (besonders anfällig) verbieten

Annahmen: A9 Es werden keine Container benutzt, physikalische Datenträger werden nicht bitweise geklont.

B 1.5 Watermarking (E1.5)

B 1.5.1 ECB

Siehe B 1.2.2.1

B 1.5.2 CBC mit schlechter Wahl des IV

Wenn im Modus CBC der Initialisierungsvektor durch einen ungeeigneten Algorithmus erzeugt wird, kann der Angreifer anhand des Schlüsseltextes nachweisen, dass eine von ihm zuvor speziell konstruierte Datei im Volume gespeichert wurde.

Bewertung: Bei TrueCrypt nur zutreffend bei alten Volumes.

Annahme: A5.3 Es wird ein sicherer Betriebsmodus verwendet.

B 2 Manipulation der Daten (E2)

B 2.1 Manipulation des auslesenden Systems

Siehe B 9.1

B 2.2 Daten direkt manipulieren (UND)

B 2.2.1 heimlicher Zugriff auf Volume

B 2.2.1.1 Systemverschlüsselung

siehe B 9.1.1.3.1.1

B 2.2.1.2 Verschlüsselung eines externen Datenträgers

Annahme: A7 Der Datenträger wird durch Siegel vor unbemerkter Benutzung geschützt.(**) Oder: A8 Es wird eine Integritätssicherung durchgeführt.(*) (**)

B 2.2.1.3 Verschlüsselung eines Containers

Annahme: A9 Es werden keine Container verschlüsselt.

B 2.2.2 Daten manipulieren

B 2.2.2.1 Erlangen von Schlüsseln

Siehe B 4 Angriffsbaum Schlüssel

B 2.2.2.2 Daten durch Zufall ersetzen

Der Angreifer kann Blöcke im Schlüsseltext ersetzen, wobei er aber keinen Einfluss darauf hat, wie diese Blöcke im Klartext aussehen.

B 2.2.2.2.1 Bekannte feste Blöcke zerstören

Der Angreifer kann bestimmte Blöcke zerstören, die aufgrund ihres Ortes bestimmte Auswirkungen haben werden. (z.B. Dateisystemstrukturen)

Bewertung: Nur in Ausnahmefällen hilfreich für den Angreifer.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0	6	0	1	0	7

Annahme: A8.1 Es wird eine blockweise Integritätssicherung durchgeführt

B 2.2.2.2.2 Blöcke in Abhängigkeit von geänderten Blöcken zerstören

Der Angreifer kann bestimmte Blöcke zerstören, von deren Lage er durch Änderungen (siehe B 1.4) erfahren hat.

Bewertung: Nur in Ausnahmefällen hilfreich für den Angreifer.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
1	6	0	1	0	8

Annahme: A8.1 Es wird eine blockweise Integritätssicherung durchgeführt.

B 2.2.2.2.3 Einzelne Zeichen erzwingen

Falls ein Entschlüsselungs-Orakel zur Verfügung steht, dann können durch Brute-Force-Blockänderung des Schlüsseltextes einige (wenige) Zeichen im Klartext erzwungen werden, während der Rest zufällig bleibt.

Für das erzwingen von n Bits werden im Durchschnitt 2^n Anfragen an das Orakel benötigt.

Bewertung: In der Praxis ist dies kaum möglich, da aus normalen Vorgängen kein Entschlüsselungs-Orakel mit der erforderlichen Anzahl an Frage-Antwort-Paaren erzeugt werden kann, ohne einen Angriff, der von vorn herein wesentlich mächtiger ist.

Gegenmaßnahme: Zugangsgelegenheiten beschränken, Integritätssicherung

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
2	6	0	**	1	**

Annahme: A8.1 Es wird eine blockweise Integritätssicherung durchgeführt.

B 2.2.2.2.4 Bits kippen

In der Betriebsart CBC kann durch Kippen von Schlüsseltext-Bits eines Blocks das entsprechende Klartext-Bit des nächsten Blocks gekippt werden. Dabei muss in Kauf genommen werden, dass der Klartext des ersten Blocks durch Zufall ersetzt wird.

Gegenmaßnahme: Integritätssicherung, CBC vermeiden.

Annahme: A5.3 Es wird ein sicherer Betriebsmodus verwendet.

B 2.2.2.3 Daten wählbar ersetzen

B 2.2.2.3.1 Daten selektiv in einen früheren Zustand versetzen (UND)

Der Angreifer kann einzelne Datenblöcke in einen früheren Zustand ersetzen

Bewertung: Kann in speziellen Fällen erfolgreich sein: Falls etwa dem Angreifer die Auswirkung gewisser Änderungen bekannt ist, kann er diese Änderungen u.U. zu seinem Vorteil selektiv auswählen.

B 2.2.2.3.1.1 Volume-Abzug erlangen

B 2.2.2.3.1.2 Rückgängig zu machende Änderungen abwarten

B 2.2.2.3.1.3 Zweiten Volume-Abzug erlangen

B 2.2.2.3.1.4 Vergleichen und passende Blöcke zurückschreiben

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
1	7	0	2	0	10

Annahmen: A8.2 Es wird eine vollständige Integritätssicherung durchgeführt, bzw.: A6.2 Wird eine Verschleierung von Änderungen gewünscht, muss das Volume vollständig umgeschlüsselt werden.

B 2.2.2.3.2 Blöcke untereinander ersetzen („Copy&Paste-Angriff")

B 2.2.2.3.2.1 Einzelne Blöcke ersetzen (ECB)

Der Angreifer kann beliebige der 128-Bit-Schlüsseltextblöcke der Blockchiffre durch beliebige andere Schlüsseltextblöcke ersetzen. (Analog bei anderer Bitlänge der Chiffre)

B 2.2.2.3.2.2 Intervalle ersetzen (CBC)

Der Angreifer kann einen Sektor bzw. ein beliebiges 128-Bit-Block-Intervall eines Sektors durch ein gleich langes anderes Intervall ersetzen, wenn er in Kauf nimmt, dass der erste 128-Bit-Block des Zielintervalls und – wenn das Intervall nicht bis zur Sektorgrenze des Zielsektors reicht – der darauffolgende 128-Bit-Block zu für ihn nicht vorhersehbarem Zufall entschlüsselt.

Annahme: A5.3 Es wird ein sicherer Betriebsmodus verwendet.

B 3 Zugriff verhindern (E3)

Der Angreifer will verhindern, dass der Nutzer Zugriff auf die Daten hat.

B 3.1 Beschädigung Daten

Der Angreifer kann die Festplatte überschreiben. Hierbei kann er Daten, oder Headerdaten überschreiben

B 3.1.1 Header beschädigen

Wenn der Angreifer den Header beschädigt, kann er schnell den Zugriff auf alle Daten der Partition verhindern.

Bewertung: Hier kann – im Unterschied zum unverschlüsselten Datenträger – ein Angreifer durch Überschreiben einer sehr kleinen Datenmenge (in entsprechend kurzer Zeit) eine große Datenmenge unrekonstruierbar zerstören..

Gegenmaßnahme: Backup der Headerdaten an einem anderen, nicht vom Angreifer erreichbaren Ort.

Annahme: A10 Es sind sicher verwahrte Backups der Header vorhanden.

B 3.1.2 Daten beschädigen

Der Angreifer kann die Daten auf dem Volume verändern / löschen.

Hierbei ist es irrelevant, ob er die verschlüsselten Daten oder die unverschlüsselten Daten löscht.

Bewertung: Dieser Angriff trifft auf einen unverschlüsselten Datenträger genauso zu und ist daher als irrelevant zu betrachten.

Gegenmaßnahme: Backup der Daten, an einem Ort, der nicht vom Angreifer erreichbar ist. In der Regel sollte es sich um ein verschlüsseltes Image des Volumes handeln.

B 3.2 Beschädigung Hardware

Der Angreifer kann die Hardware physikalisch zerstören. Bewertung: Dieser Angriff trifft auf ein unverschlüsseltes System genauso zu und ist daher als nicht relevant zu betrachten.

5.2 Angriffsbaum Volume-Schlüssel (W2)

B 4 Volume-Schlüssel erlangen (E4)

B 4.1 Angriff bei Erzeugung

B 4.1.1 Bei Erzeugung angezeigte Schlüsselteile ausspähen

Nach der Schlüsselerzeugung wird der Anfang der Schlüssel als Hexadezimalcode auf dem Bildschirm angezeigt. Dies können vom Angreifer ausgespäht werden

Bewertung: Der angezeigte Teil ist zu kurz, um praktisch ausnutzbar zu sein:

Schlüssellänge: 512 Bit = 128 Hex-Ziffern

Unter Windows werden 32 Hex-Ziffern = 128 Bit angezeigt.

Unter Linux werden 26 Hex-Ziffern = 104 Bit angezeigt.

Annahme: A11.1 Die Anzeige von Schlüsselmaterial wird unterbunden.

B 4.1.1.1 Ausspähen durch elektromagnetische Abstrahlung

B 4.1.1.2 Optisch ausspähen

B 4.1.2 Rekonstruktion des Zufalls bei Schlüsselerzeugungen

Die genaue Bewertung ist abhängig von AP5.

Annahme: A12 Es wird ein sicherer Zufallsgenerator verwendet.

B 4.1.2.1 Zufallsgenerator schwächen

Der Angreifer kann den Zufallsgenerator im Vorfeld der Schlüsselerzeugung so schwächen, dass er die Schlüssel vorhersagen kann.

B 4.1.2.2 Angezeigten Zufallspool ausspähen

Bei der Erzeugung von Zufallszahlen wird ein Teil des Zufallspools als Hexadezimalcodes auf dem Bildschirm angezeigt. Dieser könnte vom Angreifer ausgespäht werden.

Bewertung: Es werden zu bestimmten Zeitpunkten alle 320 Bytes des Zufallspools angezeigt. Je nach nachfolgendem Zufall-

seingang kann dies eine starke Schwächung des Generators darstellen.

Annahme: A11.2 Die Anzeige von Zufallsmaterial wird unterbunden.

B 4.1.2.2.1 Ausspähen durch elektromagnetische Abstrahlung

B 4.1.2.2.2 Optisch ausspähen

B 4.2 Angriff zu einer späteren Zeit

B 4.2.1 Angriff auf Volume

B 4.2.1.1 Schlüssel aus Volume-Header

B 4.2.1.1.1 Aktuelle Header-Daten erlangen

B 4.2.1.1.1.1 Header-Schlüssel erlangen

Siehe B 5 Angriffsbaum Header-Schlüssel

B 4.2.1.1.2 Alternative Header-Daten erlangen

Der Angreifer kann einen Header mit bekannten Authentisierungsmerkmalen erlangen.

B 4.2.1.1.2.1 Wiederherstellen von früher rechtmäßig erlangtem Zugriff

Der Angreifer hatte früher rechtmäßig Zugang zu einem Volume. Danach wurden die Authentifizierungsmerkmale geändert, um dem Angreifer den Zugang zu entziehen.
Wenn der Angreifer zuvor ein Header-Backup angefertigt hat, kann er dieses zurückspielen, um wieder auf das Volume zugreifen zu können

Bewertung: Dies funktioniert mit Standardfunktionen in TrueCrypt.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0	3	0	4	0	7

Annahme: A6.3 Beim Entzug von Rechten wird ein Volume vollständig umgeschlüsselt.

B 4.2.1.1.2.2 Rückstände

Ein alter Header könnte in versteckten Sektoren vorhanden sein.

Siehe B 1.1.1.1.2 Für das Betriebssystem nicht sichtbare Rückstände

B 4.2.1.2 Aus Volume-Daten

Der Schlüssel soll durch einen Angriff auf den Kryptoalgorithmus aus den Daten gewonnen werden.
Bewertung: Momentan kein praktisch anwendbarer Angriff bekannt.

Annahme: A5.2 Es wird ein sicherer Kryptoalgorithmus verwendet.

B 4.2.2 Angriff auf System (UND)

Der Schlüssel muss prinzipbedingt ständig im RAM gespeichert sein, während das Volume aktiv ist.

B 4.2.2.1 Teile der Speichers erlangen

Siehe Angriffsbaum B 9.2 Vertrauliche Informationen aus System erhalten (E11)

B 4.2.2.2 Schlüssel extrahieren

Aus diesen Speicherteilen kann nun der Schlüssel extrahiert werden.
Bewertung: Es gibt fertige, frei herunterladbare Tools, um Schlüssel aus einem Speicherabzug zu extrahieren.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0	5	0	4	0	9

B 4.2.3 Berechtigter Besitz

Ein Innentäter besitzt notwendigerweise alle nötigen Authentifizierungsmerkmale für das Systemvolume, um das System überhaupt starten zu können. Damit kann er auch den Schlüssel ableiten.

Gegenmaßnahmen: Mit dem Einsatz eines TPM kann es für den Innentäter erschwert werden, den vollständigen Schlüssel direkt zu erhalten.

Bewertung: Der Angriff kann prinzipbedingt nicht direkt abgewehrt werden.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0	3	0	1	0	4

5.3 Angriffsbaum Header-Schlüssel (W3)

B 5 Header-Schlüssel erlangen (E5)

B 5.1 Angriff bei Erzeugung

Bei jeder Änderung von Authentifizierungsmerkmalen wird ein neuer Header-Schlüssel erzeugt. Die Erzeugung kann angegriffen werden, analog zu B 4.1 .

B 5.2 Angriff bei Benutzung

B 5.2.1 Kryptoalgorithmus brechen

Bewertung: Momentan ist kein praktisch anwendbarer Angriff bekannt.

Annahme: A5 Die Kryptoalgorithmen sind sicher.

B 5.2.2 Authentisierungsmerkmal(e) angreifen

B 5.2.2.1 Passwort angreifen

siehe B 6 Angriffsbaum Passwort

B 5.2.2.2 Smartcard angreifen

siehe B 7 Angriffsbaum Smartcard

5.4 Angriffsbaum Authentifizierungsmerkmale (W4)

5.4.1 Angriffsbaum Passwort (W4.1)

B 6 Passwort erlangen (E6)

B 6.1 Vom Benutzer

B 6.1.1 Passworteingabe ausspähen

Die Eingabe des Passworts durch den Benutzer kann ausgespäht werden.

B 6.1.1.1 Intern

####### B 6.1.1.1.1 Keylogger

Siehe B 9.1 Manipulation System

####### B 6.1.1.1.2 Pre-Boot-Authentication-Passwort im Tastaturpuffer

Das Pre-Boot-Passwort wird beim Eingeben im Tastaturpuffer gespeichert. Wenn es dort nicht explizit gelöscht wird, kann es auch später während des Betriebs noch lesbar sein.

Bewertung: Diese Lücke betrifft nur TrueCrypt-Versionen bis einschließlich 5.0. Sie ist seit Version 5.1 behoben.

B 6.1.1.2 Extern

####### B 6.1.1.2.1 Optisch

####### B 6.1.1.2.2 Elektromagnetische Abstrahlung

####### B 6.1.1.2.3 Analyse Stromverbrauch

####### B 6.1.1.2.4 Akustisch

B 6.1.1.3 Durch Hardwaremanipulation

####### B 6.1.1.3.1 Keylogger

Bewertung: Hardware-Keylogger sind frei und günstig erhältlich.

Gegenmaßnahmen: Verwendung einer Smartcard, bauliche Abschirmung, verdeckte Eingabe.

Annahme: A14 Es wird eine passend zertifizierte Smartcard verwendet.

B 6.1.2 Notiertes Passwort

Der Benutzer könnte das Passwort notiert haben, dies ist umso wahrscheinlicher, je komplizierter das Passwort ist und je häufiger es gewechselt wird.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0	0	0	4	0	4

Annahme: A13.2 Passwörter werden sicher behandelt.

B 6.1.3 Mehrfach verwendetes Pawsswort

Der Benutzer könnte das gleiche Passwort für andere Dienste benutzt haben, die leichter zu brechen oder direkt unter der Kontrolle eines Angreifers stehen.

Annahme: A13.2 Passwörter werden sicher behandelt.

B 6.1.4 Social Engineering

Der Angreifer könnte z.B. vortäuschen, berechtigt zu sein, etwa Administrator, Vorgesetzter usw. und von einem Benutzer das Passwort fordern.

Annahme: A13.2 Passwörter werden sicher behandelt.

B 6.2 Direkt

B 6.2.1 Über Tabellen

Wenn aus Passwörtern Schlüssel generiert werden, ist es oftmals möglich, bestimmte Brute-Force-Angriffe durch Tabellen zu beschleunigen. (z.B. über rainbow tables)

Hier werden einmalig mit großem Aufwand die Menge aller in Frage kommenden Passwörter jeweils durch die entsprechenden Krypto-Algorithmen passend verarbeitet, und die Ergebnisse geschickt komprimiert in große Tabellen gespeichert. Später kann die Zeit zum Erlangen eines Passworts aus dieser Menge mit diesen Tabellen stark reduziert werden.

Dieser Angriff ist hier irrelevant, da TrueCrypt ein „Salt" verwendet. Dies ist eine Zahl, die zusammen mit dem Passwort in die Berechnung des Schlüssels eingeht. Sie wird unverschlüsselt gespeichert und darf auch dem Angreifer bekannt sein. Diese Zahl wird für jedes Passwort zufällig neu gewählt. Der Effekt ist, dass der Angreifer für

jedes Salt eine neue Tabelle anlegen müsste, was den Einsatz von Tabellen ad absurdum führt.

B 6.2.2 Über Wörterbuchangriff/Brute Force

Vom Angreifer können automatisiert systematisch alle Wörter und bestimmte Kombinationen aus einem Wörterbuch durchprobiert werden.
Bewertung: Je nach Komplexität des Passwortes möglich.

Die Anzahl der möglichen Zeichen setzt sich zusammen aus der Anzahl der Kleinbuchstaben, Großbuchstaben, Umlaute, Ziffern und Sonderzeichen (Näherung): 26+26+7+10+26=95

Damit ergibt sich eine maximale Entropie von ca. 6,5 Bit pro Zeichen bei völlig zufällig gewähltem Passwort.

Jedes Passwort wird mit PBKDF2 1000-mal (Systemverschlüsselung) bzw. 2000-mal (Volumeverschlüsselung) gehasht. Die damit verbundene Erweiterung des Sicherheitsvorsprungs gegen Durchprobieren ist äquivalent zu einer Verlängerung des Passworts um ca. 10 bzw. 11 Bit

Für eine Sicherheit von 80 Bits benötigt man daher ein völlig zufälliges Passwort mit 11 Zeichen.

In der Praxis hat jedoch ein von Benutzern gewähltes Passwort mit 40 Zeichen, das sogar bestimmten Regeln zur Zusammensetzung genügt, lediglich eine Entropie von gut 60 Bits[5], verbunden mit PBKDF2 also entsprechend rund 70 Bits.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0...	5	0	1	2...6	**8...**

Annahme: A13.1 Es werden sichere Passwörter verwendet.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
19...	5	0	1	6	**31...**

5.4.2 Angriffsbaum Smartcard (W4.2)

B 7 Schlüsselmaterial von Smartcard erlangen (E9)

B 7.1 Schlüsselmaterial direkt aus Smartcard in Besitz des Angreifers (UND) (E7)

B 7.1.1 Smartcard erlangen

Der Angreifer kann physikalischen Besitz der Smartcard erlangen.

5 NIST Special Publication 800-63, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

B 7.1.2 Zugriff auf Daten

####### B 7.1.2.1 PIN erlangen

Siehe B 8 Angriffsbaum PIN

####### B 7.1.2.2 Direkter Angriff auf Smartcard

Bewertung: Abhängig vom konkret verwendeten Typ

Annahme: A14 Es wird eine passend zertifizierte Smartcard verwenden.

B 7.2 Angriff ohne Besitz der Smartcard

B 7.2.1 Benutzung an eigenem Leser

Die Smartcard wird in den Leser eingesetzt, der üblicherweise dafür benutzt wird.

####### B 7.2.1.1 Hardwareschnittstelle für Smartcard manipulieren

######## B 7.2.1.1.1 Verbindung zu Smartcard-Leser manipulieren

Der Angreifer könnte die Verbindung zwischen Smartcard-Leser und Rechner abhören oder gar manipulieren.

Gegenmaßnahmen: Verbindung absichern (z.B. durch Verschlüsselung oder organisatorische Maßnahmen); Verbindung prüfen.

Annahme: A15.1 Die Verbindung zwischen Leser und Rechner ist sicher.

######## B 7.2.1.1.2 Smartcard-Leser manipulieren

Ein Angreifer könnte den Smartcard-Leser so manipulieren, dass er den Schlüssel an ihn übermittelt oder speichert.

Annahmen: A15 Es wird ein zertifizierter Smartcard-Leser benutzt.
A15.2 Die Benutzer sind geschult im Umgang mit dem Smartcard-Leser.

B 7.2.2 Benutzung an fremdem Leser

Der Benutzer benutzt die Smartcard an einem fremden Leser, dieser kann unter der Kontrolle des Angreifers stehen.

Beispiel: Mehrfach verwendete Smartcard, z.B. bei Zutrittskontrolle. Dann kann mit der Meldung „Benutzen sie die 'andere' PIN" der Benutzer möglicherweise dazu gebracht werden, die Festplatten-PIN einzugeben.

Gegenmaßnahme: Separate Smartcard nur für Festplattenverschlüsselung; oder: Benutzerschulung.

Annahme: A15.2 Die Benutzer sind geschult im Umgang mit dem Smartcard-Leser.

5.4.3 Angriffsbaum PIN (W4.3)

B 8 PIN erlangen (E8)

B 8.1 PIN mitlesen

B 8.1.1 PIN durch Seitenkanal erlangen

Die PIN kann über einen Seitenkanal abgehört werden.

Siehe B 6.1.1.2

Annahmen: A15 Es wird ein zertifizierter Smartcard-Leser eingesetzt, A15.2 Die Benutzer sind geschult im Umgang mit dem Smartcard-Leser.

B 8.1.2 PIN intern abhören

Der Angreifer könnte den Smartcard-Leser so manipulieren, dass die PIN aufgezeichnet wird.

Annahmen: A15 Es wird ein zertifizierter Smartcard-Leser eingesetzt. A15.2 Die Benutzer sind geschult im Umgang mit dem Smartcard-Leser.

B 8.2 Benutzer dazu bringen, PIN über vom Angreifer kontrollierte Geräte einzugeben

Der Benutzer wird auf fremden Geräten/Rechnern aufgefordert, seine PIN einzugeben.

Gegenmaßnahme: Schulung der Benutzer: Eingabe nur an vorgesehenem Leser und nur dann, wenn notwendig.

Annahmen: A15 Es wird ein zertifizierter Smartcard-Leser eingesetzt. A15.2 Die Benutzer sind geschult im Umgang mit dem Smartcard-Leser.

5.5 Angriffsbaum System (W5)

B 9 System angreifen

B 9.1 System manipulieren (E10)

B 9.1.1 Manipulation vor Ort

B 9.1.1.1 Im aktiven, nicht gesperrten Zustand

Ein Innentäter habe einen eigenen Benutzerzugang am System des anzugreifenden Geheimnisträgers. Dann ergeben sich *zusätzlich* weitere Angriffsmöglichkeiten für den Innentäter.

B 9.1.1.1.1 Sicherheitslücke in Betriebssystem bzw. anderer Software mit erhöhten Rechten

Der Angreifer könnte sich erhöhte Rechte beschaffen. Hier kann die Verschlüsselung nicht schützen.

Annahme: A16.2 Es ist keine relevanten Sicherheitslücke in Betriebssystem oder Drittsoftware vorhanden.

B 9.1.1.1.2 Über Schnittstellen zu privilegierten Teilen von TrueCrypt

B 9.1.1.1.2.1 Linux

Unter Linux gibt es für den normalen Benutzer 2 mögliche Schnittstellen zu Teilen von TrueCrypt, die mit erhöhten Rechten laufen. Dies ist einerseits der über sudo gestartete CoreService-Prozess und andererseits die FUSE-Schnittstelle zum TrueCrypt-Treiber.

B 9.1.1.1.2.1.1 CoreService angreifen

Sämtliche Funktionalitäten, für die erhöhte Rechte erforderlich sind, werden mittels eines selbst entwickelten Serialisierungsverfahrens von einer mit erhöhten Rechten laufenden Instanz vom CoreService angefordert. Diese Instanz wird zuvor mittels sudo gestartet.

Die Möglichkeiten, Angriffe über diese Schnittstelle durchzuführen hängt so stark von der konkreten Implementierung ab, dass hier nur die bereits durch die Analyse bekannten Schwächen aufgezählt und kategorisiert werden können.

Abgetrennt aus Gründen der Übersichtlichkeit. Siehe Angriffsbaum B 11

B 9.1.1.1.2.1.2 Fuse-Schnittstelle angreifen

Die Fuse-Schnittstelle erzeugt neben der Datei `volume` auch eine Datei `control`, über die auf TrueCrypt zugegriffen werden kann.

In AP4 wird dazu ein Angriff beschrieben, der eine Race Condition nutzt.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
1	6	0	2	6	15

B 9.1.1.1.2.2 Windows

B 9.1.1.1.2.2.1 UAC

Für bestimmte Aktionen (Authentifizierungsmerkmale ändern, NTFS formatieren...) muss

der Benutzer schon volle Administrator-Rechte haben.

Annahme: A18 Es werden nur die Funktionen benutzt, die keine Administratorrechte seitens des Benutzers erfordern.

B 9.1.1.1.2.2.2 Treiber

B 9.1.1.1.2.2.2.1 Passwort-Cache

Die Passwörter aller Benutzer werden in einem gemeinsamen Cache abgelegt und werden automatisch benutzt, auch von nicht berechtigten Benutzern.

Gegenmaßnahmen: Cache deaktivieren

Annahme: A19 Ein benutzter Passwort-Cache ist nach Benutzern getrennt.

B 9.1.1.1.2.2.2.2 Codeschwächen

Hier können mangels einer vollständigen Codeanalyse nur Beispiele aufgezählt werden.

B 9.1.1.1.2.2.2.2.1 Unsichere Stringfunktionen

B 9.1.1.1.2.2.2.2.2 Off-by-One Overflows

B 9.1.1.1.2.2.2.2.3 ...

B 9.1.1.2 Im aktiven, aber gesperrten Zustand

Das System läuft, die Festplattenverschlüsselung ist aktiv, aber das System ist durch eine Sperre wie z.B. Bildschirmschoner geschützt. Hier ist auch Suspend-to-RAM einzuordnen.

B 9.1.1.2.1 System herunterfahren

Der Angreifer fährt das System herunter, um einen Angriff nach B 9.1.1.3 durchzuführen

B 9.1.1.2.2 Angriff über Schnittstellen des Systems

B 9.1.1.2.2.1 Firewire

Durch einfaches anschließen eines 2. PC an die Firewire-Schnittstelle und Laden einer frei verfügbarer Software kann direkt lesend und schreibend auf den kompletten Arbeitsspeicher zugegriffen werden.

Gegenmaßnahmen: Schnittstellenkontrolle; durch IOMMU oder Deaktivieren von Firewire insgesamt

bzw. der DMA-Funktion. Physikalische Sperrung der Firewire-Schnittstelle.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
1	5	0	1	1	8

Annahme: A20 Es werden Maßnahmen getroffen, um Angriffe über externe Schnittstellen zu verhindern.

B 9.1.1.2.2.2 USB

Der Angreifer könnte Sicherheitslücken in der USB-Implementierung ausnutzen

Bewertung: Wurde auf nicht-PC-System schon durchgeführt, siehe Playstation-3-Hack[6] Dies ist aber keine prinzipielle Angreifbarkeit sondern erfordert eine Lücke im Betriebssystem.

Annahme: A16 Das Betriebssystem ist sicher.

B 9.1.1.2.2.3 eSATA

Der Angreifer kann per DMA über den eSATA-Port auf den Speicher zugreifen. Dafür ist jedoch im Gegensatz zu Firewire eine extra für diesen Zweck entwickelte Spezialhardware samt Software nötig.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
10	8	2	1	9	30

B 9.1.1.2.2.4 Ethernet

Dies ist eine Remote-Schnittstelle, die nicht unmittelbar Zugang gewährt. Daher stellt dies einen Angriff aus der Ferne dar, siehe dazu B 9.1.2.2 .

B 9.1.1.2.2.5 Wlan/Bluetooth

Analog zu Ethernet, siehe B 9.1.2.2 .

B 9.1.1.2.2.6 Cardbus/Expresscard

B 9.1.1.2.2.6.1 Einsatz einer Firewire-Karte

Durch Einstecken einer Firewire-Adapter-Karte kann ein Angriff nach B 9.1.1.2.2.1 durchgeführt werden.
Gegenmaßnahmen siehe dort.

B 9.1.1.2.2.6.2 Einsatz einer speziell entwickelten Karte

6 http://www.heise.de/security/meldung/Source-Code-des-PS3-Hacks-veroeffentlicht-1070859.html

Es wurde bereits entsprechende Hardware entwickelt[7], die durch einen eigenen Prozessor selbständig lesend und schreibend auf Speicherinhalte zugreifen kann. Dafür ist keine Treiberunterstützung seitens des Betriebssystems erforderlich.

Gegenmaßnahme: Schnittstellenkontrolle (IOMMU einsetzen oder Steckplatz deaktivieren durch logische oder physikalische Maßnahmen)

Annahme: A20.2 Der Erweiterungssteckplatz ist gegen Zugang von außen logisch oder physikalisch abgesichert.

B 9.1.1.2.2.7 Docking-Port

Eine an den Docking-Port anschließbare Docking-Station kann alle inB 9.1.1.2.2 aufgeführten sonstigen Schnittstellen enthalten, wobei bei manchen Modellen zusätzlich PCI-/PCI-Express-Erweiterungskarten eingebaut werden können. Die möglichen Angriffe darauf sind analog zu den Angriffen auf die entsprechenden externen Schnittstellen B 9.1.1.2.2.6 .

Zusätzlich veraltete Anschlüsse wie Parallelports und Serielle Ports sind zu vernachlässigen.

Annahmen: A20.3 Der Docking-Port wird behandelt wie alle darüber verfügbaren Anschlüsse. A20.4 Docking-Stationen werden genauso behandelt wie der zugehörige PC.

B 9.1.1.3 Im ausgeschalteten Zustand

B 9.1.1.3.1 Bootloader manipulieren

Ein Angreifer kann den Bootloader manipulieren, um das System anzugreifen.

Bewertung: Spezielle Programme wie Evil-Maid sind sowohl fertig als Image als auch im Quelltext frei verfügbar[8] und können so auch angepasst werden.

B 9.1.1.3.1.1 Zugriff auf Festplatte

B 9.1.1.3.1.1.1 Booten von externem Medium

B 9.1.1.3.1.1.1.1 Standardeinstellung

7 http://actes.sstic.org/SSTIC09/Compromission_physique_par_le_bus_PCI/SSTIC09-article-C-Devine-G-Vissian-Compromission_physique_par_le_bus_PCI.pdf

8 http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html

Annahmen: A21 Das Booten von anderen Quellen als der eingebauten Festplatte ist im BIOS deaktiviert.

A21.1 Das BIOS ist mit einem Passwort vor Veränderung geschützt.

B 9.1.1.3.1.1.1.2 Zugriff auf BIOS

B 9.1.1.3.1.1.1.2.1 BIOS-Masterpasswort

Einige BIOS-Hersteller vergeben ein Generalpasswort.

Annahme: A21.2 Der Veränderungsschutz des BIOS lässt sich nicht durch ein Masterpasswort umgehen.

B 9.1.1.3.1.1.1.2.2 CMOS physikalisch löschen

Der Angreifer öffnet das Systemgehäuse und setzt über einen Jumper die BIOS-Konfigurationsdaten zurück.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0	6	2	2	0	10

Es gibt Rechner, bei denen diese Methode nicht anwendbar ist.

Annahmen: A22.2 Es wird ein Rechner verwendet, bei dem das Rücksetzen der BIOS-Einstellungen nicht trivial möglich ist.

A22 Vor jedem Start wird die physikalische Integrität des Rechners durch den Benutzer überprüft.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
2	6	2	**	0	**

B 9.1.1.3.1.1.1.3 BIOS austauschen

Der Angreifer könnte das Speichermodul des BIOS zurücksetzen/austauschen. Bewertung:

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
2	8	2	3	6	21

Annahme: A22 Vor jedem Start wird die physikalische Integrität des Rechners durch den Benutzer überprüft.

B 9.1.1.3.1.1.2 Booten von (versteckter) Expresscard/Cardbus bzw. PCI/PCIe-Karte mit Erweiterungs-BIOS

Das BIOS führt bei jedem Start sämtliche auf Erweiterungskarten vorhandenen BIOS-Ergänzungen aus.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
6	8	0	1	7	22

B 9.1.1.3.1.1.2.1 Direkt

Gegenmaßnahmen: Erweiterungs-BIOS abschalten, Port physikalisch blockieren. *Annahme: A22* Vor jedem Start wird die physikalische Integrität des Rechners durch den Benutzer überprüft. A22.3 Der Benutzer überprüft vor jedem Systemstart die Integrität der Schnittstellen.

B 9.1.1.3.1.1.2.2 Über Docking-Station

Annahme: A20.4 Docking-Stationen werden genauso behandelt wie der zugehörige PC.

Annahme: A21.4 Das Laden eines Erweiterungs-BIOS ist im BIOS abgeschaltet.

B 9.1.1.3.1.1.3 Physikalischer Lese-/Schreibzugriff auf Festplatte

Die Festplatte wird ausgebaut und darauf mittels eines eigenen PC zugegriffen

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
1	3	0	1	3	8

Annahme: A22 Vor jedem Start wird die physikalische Integrität des Rechners durch den Benutzer überprüft.

B 9.1.1.3.2 Über Manipulation des System-Volumes (UND)

B 9.1.1.3.2.1 Zugriff auf Festplatte

siehe B 9.1.1.3.1.1

B 9.1.1.3.2.2 Logische Manipulation

B 9.1.1.3.2.2.1 Volume-Schlüssel erlangen

Siehe B 4

B 9.1.1.3.2.2.2 Ohne Kenntnis des Schlüssels

B 9.1.1.3.2.2.2.1 Ausführbare Daten manipulieren

B 9.1.1.3.2.2.2.1.1 Zufällig ändern

B 9.1.1.3.2.2.2.1.2 Sicherheitsfunktionen können möglicherweise unbemerkt deaktiviert werden.

Bewertung: Nur in Ausnahmefällen erfolgreich.

Siehe B 2.2.2.2 Daten durch Zufall ersetzen.

Annahmen: siehe dort.

B 9.1.1.3.2.2.2.1.3 Update rückgängig machen

B 9.1.1.3.2.2.2.1.4 Angreifer kann Updates rückgängig machen, die eine anderweitig ausnutzbare Sicherheitslücke betreffen.

Siehe B 2.2.2.3.1 Daten selektiv in einen früheren Zustand versetzen (UND)

Annahmen: siehe dort.

B 9.1.1.3.2.2.2.2 Konfigurationen manipulieren

B 9.1.1.3.2.2.2.2.1 Zufällig ändern

Ein Angreifer kann eine Konfigurationsdatei ungültig machen. Bestimmte Programme könnten hierdurch in eine unsichere Standardkonfiguration zurückfallen.

Siehe B 2.2.2.2 Daten durch Zufall ersetzen

Annahmen: siehe dort.

B 9.1.1.3.2.2.2.2.2 Rückgängig machen

B 9.1.1.3.2.2.2.3 Ein Angreifer kann Konfigurationsänderungen rückgängig machen, die die Sicherheitsfunktionen betreffen.

Siehe B 2.2.2.3.1 Daten selektiv in einen früheren Zustand versetzen (UND)

Annahmen: siehe dort.

B 9.1.1.3.3 Hardware manipulieren

B 9.1.1.3.3.1 Austausch

B 9.1.1.3.3.1.1 Komplett

Der Angreifer könnte das System gegen ein identisches austauschen.

Annahme: Der Benutzer stellt sicher, dass er ein ihm bekanntes System vor sich hat.

B 9.1.1.3.3.1.2 Teilweise

B 9.1.1.3.3.1.2.1 Intern

Der Angreifer könnte interne Komponenten austauschen.

Annahme: A22 Vor jedem Start wird die physikalische Integrität des Rechners durch den Benutzer überprüft.

B 9.1.1.3.3.1.2.2 Extern

Der Angreifer könnte Tastatur, Kartenleser oder Bildschirm gegen von ihm kontrollierte Geräte austauschen.

Annahme: A22.2 Der Benutzer versichert sich, dass alle Komponenten des Systems unverändert sind.

B 9.1.1.3.3.2 Veränderung bestehender Hardware

B 9.1.1.3.3.2.1 Firmwareveränderungen

Ein Angreifer könnte Software verändern, die direkt in Speicherbausteinen im System gespeichert ist.

B 9.1.1.3.3.2.1.1 System-BIOS verändern

Ein Angreifer kann das System-BIOS verändern.

B 9.1.1.3.3.2.1.1.1 Eigenes System booten

Der Angreifer kann das BIOS aus seinem eigenen System heraus ändern.

Siehe B 9.1.1.3.1.1.1

B 9.1.1.3.3.2.1.1.2 System öffnen

Der Angreifer kann das System öffnen und den BIOS-Chip direkt umprogrammieren/austauschen.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
7	8	0	2	6	23

Annahme: A22 Vor jedem Start wird die physikalische Integrität des Rechners durch den Benutzer überprüft.

B 9.1.1.3.3.2.1.2 Erweiterungs-BIOSe hinzufügen

Das System-BIOS führt beim Systemstart jedes Erweiterungs-BIOS auf eingesteckten Erweiterungskarten aus. Dort kann der Angreifer eigenen Code unterbringen.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
7	8	0	2	6	23

Annahme: A22 Vor jedem Start wird die physikalische Integrität des Rechners durch den Benutzer überprüft.

B 9.1.1.3.3.3 Zusätzliche Geräte/Bausteine einbauen

B 9.1.1.3.3.3.1 Zur automatischen Manipulation im laufenden Betrieb

Siehe B 9.1.1.2 Manipulation im laufenden Betrieb.

Annahme: A22 Vor jedem Start wird die physikalische Integrität des Rechners durch den Benutzer überprüft.

B 9.1.1.3.3.3.2 Zusätzliche Datenträger einbauen

Der Angreifer könnte zusätzliche Datenträger in das System einbauen. Dies kann auch von außen passieren, z.B. durch Verstecken eines Miniatur-USB-Datenspeicher in einem USB-Port.

Annahme: A22.3 Vor jedem Start wird die Integrität der Schnittstellen durch den Benutzer überprüft.

B 9.1.2 Manipulation aus der Ferne

B 9.1.2.1 Manipulation des Systems durch Manipulation eines Datenträgers

Ein Datenträger gelangt in vorübergehenden Besitz eines Angreifers. Der Angreifer kann ihn manipulieren, um Zugriff zum System zu erhalten.

B 9.1.2.1.1 Manipulation an der Hardware des Datenträgers

B 9.1.2.1.1.1 Angriff auf die Schnittstelle des Systems

Der Angreifer manipuliert den Datenträger so, dass automatisiert über die Schnittstelle (USB, Firewire, eSATA) ein Angriff auf das System durchgeführt wird.

####### B 9.1.2.1.1.1.1 Zusätzlicher Datenträger

Der Angreifer könnte unter Verwendung eines USB-Hub-Chip einen zweiten USB-Datenspeicher in das Gehäuse des Datenträgers einbauen. (analog Firewire bzw. eSATA) Dies kann er für einen Angriff nutzen nach B 9.1.2.1.2.1.1 ‚Fehler: Referenz nicht gefundenB 9.1.2.1.2.2.2.1

Annahmen siehe dort.

B 9.1.2.1.2 Durch Manipulation der Daten des Datenträgers

B 9.1.2.1.2.1 Angriff über Benutzer

####### B 9.1.2.1.2.1.1 Partition hinzufügen

Es wird auf dem Datenträger eine zusätzliche Partition untergebracht, die als interessante Daten bzw. interessante Software getarnte Schadsoftware enthält. Der Benutzer soll nun dazu gebracht werden, diese (z.B. aus Neugier) auszuführen.

Annahme: A23 Der Benutzer ist geschult im sicheren Umgang mit dem System.

B 9.1.2.1.2.2 Fehler/Eigenschaften der Software ausnutzen

####### B 9.1.2.1.2.2.1 Verschlüsselungssoftware

######## B 9.1.2.1.2.2.1.1 Headerbereich

Bewertung: Bei TrueCrypt sind Header voll verschlüsselt. Darum ist die Möglichkeit eines gezielten Angriffs auf die dahinterliegenden Mechanismen unwahrscheinlich.

Annahme: A5.1 Die Kryptoalgorithmen sind korrekt implementiert.

######## B 9.1.2.1.2.2.1.2 Datenbereich

Bewertung: Bei Korrektheit der Implementation der Krypto-Algorithmen auszuschließen.

Annahme: A5.1 Die Kryptoalgorithmen sind korrekt implementiert.

####### B 9.1.2.1.2.2.2 Betriebssystem

######## B 9.1.2.1.2.2.2.1 Partition hinzufügen

Bewertung: hohes Risiko (siehe z.B. LNK-Lücke[9] bei Stuxnet)

Gegenmaßnahme: Betriebssystem absichern; nur vollständig verschlüsselte Datenträger zulassen; bei verschlüsselten Datenträgern keine weiteren Partitionen einbinden; Austausch von Datenträgern verhindern. Physikalische Manipulation des Datenträgers verhindern.

Annahme: A16 Das Betriebssystem ist sicher.

######## B 9.1.2.1.2.2.2.2 Datenträger bootbar machen

Gegenmaßnahme: Booten von externem Datenträger verhindern

Annahme: A21 Das Booten von anderen Quellen als der eingebauten Festplatte ist im BIOS deaktiviert.

######## B 9.1.2.1.2.2.2.3 Fehler über Partitionstabelle

Bewertung: Es sind keine Angriffe bekannt, die Fehler in Partitionstabellen ausnutzen.

9 http://www.heise.de/security/meldung/Microsoft-bestaetigt-USB-Trojaner-Luecke-1039915.html

Annahme: A16 Das Betriebssystem ist sicher.

B 9.1.2.2 Manipulation über Netzwerk

B 9.1.2.2.1 Booten über Netzwerk

Der Angreifer kann bei aktivierter Funktion „Booten von Netzwerk" nach einem Angriff auf das Netzwerk Schadsoftware über das Netzwerk booten.

Annahme: A21 Das Booten von anderen Quellen als der eingebauten Festplatte ist im BIOS deaktiviert.

B 9.1.2.2.2 Betrieb an Netzwerk

TrueCrypt selbst hat keine direkten Netzwerkfunktionen.

Annahme: A16.3 Die Sicherheit im Netzwerk muss während des Betriebs durch das Betriebssystem bzw. andere Sicherheitssoftware (Firewall, elektronische Signaturen etc.) sichergestellt werden.

B 9.2 Vertrauliche Informationen aus System erhalten (E11)

B 9.2.1 Durch Manipulation des Systems

Auf das System kann Schadcode gebracht werden, der über verschiedene Kanäle Informationen nach außen leitet.

Siehe Angriffsbaum B 9.1 : Manipulation des Systems

B 9.2.2 Lokaler Angriff im ausgeschalteten Zustand

B 9.2.2.1 Zugriff auf die Festplatte (UND)

B 9.2.2.1.1 Auf Festplatte lesend zugreifen

Siehe Angriffsbaum B 9.1.1.3.1.1

B 9.2.2.1.2 Vertrauliche Informationen erhalten

Siehe Angriffsbaum B 1

B 9.2.2.2 Rückstände des Systems auslesen (ODER)

B 9.2.2.2.1 RAM

####### B 9.2.2.2.1.1 Vor Sekunden bis Minuten ausgeschaltet (Cold-Boot)

Entgegen früheren Annahmen hält RAM den Großteils des Speicherinhalts je nach Temperatur einige Sekunden bis Minuten. Mit Kältespray kann diese Zeit maximiert werden.[10]

10 J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino. Lest We Remember: Cold Boot Attacks on Encryption Keys. http://citp.princeton.edu/memory/

Gegenmaßnahmen: Wichtige Daten beim Herunterfahren im RAM überschreiben; wichtige Daten so kurz wie möglich im RAM speichern; Bei Abwesenheit immer System sauber herunterfahren bzw. in einen verschlüsselten Suspend-Modus versetzen.

B 9.2.2.2.1.1.1 Booten von extern

Siehe Angriffsbaum B 9.1.1.3.1.1.1

Bewertung: Es existieren fertige USB-Sticks, um einen Speicherabzug zu erstellen.

Gegenmaßnahmen: Booten von extern verhindern, Reset des RAM beim Booten durch BIOS.

Annahme: A21 Das Booten von anderen Quellen als der eingebauten Festplatte ist im BIOS deaktiviert.

B 9.2.2.2.1.1.2 Austausch der Festplatte

Der Angreifer tauscht die Festplatte gegen eine eigene, von der er booten kann.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
1	3	0	1	2	7

Annahme: A22 Vor jedem Start wird die physikalische Integrität des Rechners durch den Benutzer überprüft.

B 9.2.2.2.1.1.3 Physikalischen Zugriff auf Speicher

Der Angreifer kann die Speichermodule direkt ausbauen und in einem eigenen Rechner auslesen.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
1	8	0	1	2	12

Gegenmaßnahme: Kühlen und Ausbauen physikalisch so erschweren, dass bis zum erneuten Einbau in einen anderen Rechner so viel Zeit vergeht, dass der RAM-Inhalt verfällt.

Annahme: A25 Die Speichermodule werden mittels Kleber fixiert und isoliert.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
1	8	0	**	2	**

B 9.2.2.2.1.1.4 Zugriff über interne physikalische Manipulation

Der Angreifer kann über andere interne Schnittstellen den Rechner unter seine Kontrolle bringen und einen Speicherabzug anfertigen. z.B. Austausch des BIOS, interne Busse usw.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
1	6	4	1	6	18

Annahme: A24 (***) Bei Abwesenheit des Benutzers muss dafür gesorgt werden, dass keine sensiblen Daten im RAM sind.

B 9.2.2.2.1.2 Vor längerer Zeit ausgeschaltet

Bewertung: Für normalen Speicher irrelevant, höchstens in hier nicht verwendeten Krypto-Beschleunigern[11].

B 9.2.2.2.2 Swap

Der Angreifer kann sensible Daten vom Swap lesen.

Gegenmaßnahmen: Sensible Daten als nicht auslagerbar markieren; besser: Swap verschlüsseln.

Annahme: A28.1 Der Auslagerungsspeicher wird verschlüsselt.

B 9.2.2.2.3 Temporäre Dateien

Bei der Bearbeitung von sensiblen Daten werden u.U. temporäre Dateien angelegt. Ein Angreifer könnte diese auslesen.

Annahmen: A28.2 Alle möglichen Orte für temporäre Dateien sind verschlüsselt.

B 9.2.3 Lokales Auslesen in aktivem, aber gesperrten Zustand

B 9.2.3.1 Angriff durch Ausschalten

Siehe B 9.2.2

B 9.2.3.2 Auslesen über außen zugängliche Schnittstellen

B 9.2.3.2.1 Auslesen über DMA

B 9.2.3.2.1.1 Firewire

Siehe B 9.1.1.2.2.1

B 9.2.3.2.1.2 Expresscard/Cardbus

Siehe B 9.1.1.2.2.6

11 Peter Gutmann: Data Remanence in Semiconductor Devices, http://www.cypherpunks.to/~peter/usenix01.pdf

B 9.2.4 Lokales Auslesen im aktiven und nicht gesperrten Zustand

Ein Innentäter habe einen eigenen Benutzerzugang am System des anzugreifenden Geheimnisträgers. Dann ergeben sich *zusätzlich* weitere Angriffsmöglichkeiten für den Innentäter.

Diese basieren auf Ergebnissen des AP4. Da dort keine vollständige Sicherheitsanalyse des Codes durchgeführt wurde, kann der Baum auch nur einen Überblick über die dort bereits bekannt gewordenen Schwächen geben.

B 9.2.4.1 Mit eigenen Benutzerrechten

B 9.2.4.1.1 Falsch gesetzte Dateiberechtigungen

Wenn mehrere Benutzer gleichzeitig an einem System angemeldet sind und jeweils eigene verschlüsselte Volumes eingehängt haben, könnte durch falsch gesetzte Dateiberechtigungen ein Benutzer auf die Daten eines anderen zugreifen

Die gleichzeitige Anmeldung mehrerer Benutzer auf einem Desktopsystem wird unter Windows „Schneller Benutzerwechsel" genannt.

Annahme: A17 Innerhalb des Volumes sind die Zugriffsrechte geeignet beschränkt.

B 9.2.4.1.2 Seitenkanalangriffe

B 9.2.4.1.2.1 Cache-Timing-Angriff

Wenn AES wie in TrueCrypt mit großen Tabellen beschleunigt wird, kann ein Angreifer auf dem selben Rechner über die Laufzeiten bestimmter Cache-Zugriffe Rückschlüsse über dessen Inhalt ziehen, und damit z.B. über Schlüssel. Bei einer Verwendung einer Hardwarebeschleunigung wie AES-NI ist das nicht der Fall.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
5	8	0	4	7	24

Annahme: A26 Zur Abwehr von Cache-Timing-Angriffen auf AES wird eine Hardwarebeschleunigung eingesetzt.

B 9.2.4.2 Mit erweiterten Rechten

Siehe auch: Manipulation des Systems B 9.1

B 9.2.5 Aus der Ferne bei aktivem System

Bei aktiver Festplattenverschlüsselung verhält sich ein eingeschalteter PC nach außen wie ein PC ohne Festplattenverschlüsselung.

Annahme: A16.3 Das Betriebssystem oder Drittsoftware schützt vor Angriffen über das Netz.

B 10 Benutzung von System verhindern (E12)

Siehe B 3

5.5.1 Angriffsbaum CoreService

Dieser Baum wurde aus Gründen der Übersichtlichkeit fortgesetzt aus B 9.1.1.1.2.1
Hier werden nur die auffälligsten Schwächen aus AP4 aufgezählt. Für weitere Details müsste – wie dort empfohlen – eine vollständig Schwachstellenanalyse durchgeführt werden.

B 11 Linux: Ausnutzen von CoreService

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0	<=3	0	<=1	0	<=4

B 11.1 Logische Schwächen

B 11.1.1 Fehlerhafte/Fehlende Rechteüberprüfung

B 11.1.1.1 SetFileOwnerRequest

B 11.1.1.2 ... (genaue Codeanalyse nötig)

B 11.1.2 ...(genaue Codeanalyse nötig)

B 11.2 Ungenügend abgesicherter Aufruf des CoreService

B 11.2.1 sudo

B 11.2.2 Manipulation von Umgebungsvariablen

B 11.2.3 ... ... (genaue Codeanalyse nötig)

B 11.3 Ungenügend abgesicherte Aufrufe von Hilfsprogrammen

B 11.3.1 Manipulation von Umgebungsvariablen

B 11.3.2 Unsichere Optionen

B 11.3.2.1 Mount

B 11.3.2.1.1 nosuid nicht per default

Es ist sehr leicht möglich, einen selbst erstellten ext*-Container oder externen Datenträger mit einer dem root-Benutzer gehörenden ausführbaren Datei mit gesetztem setuid-Flag zu mounten und sofort root-Rechte zu erlangen.

Gegenmaßnahme: Mountoption nosuid erzwingen.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
0	3	0	1	0	4

B 11.3.2.1.2 Benutzer kann Mount-Optionen selbst angeben.

Potentielle Gefahr: eventuell erzwungene Mountoptionen können rückgängig gemacht werden.

B 11.3.3 Codeschwächen

B 11.3.4 ... (genaue Codeanalyse nötig)

B 11.4 ... (genaue Codeanalyse nötig)

5.6 Angriffsbaum geheime Algorithmen (W6)

Für die Festplattenverschlüsselung ist vorgesehen, in bestimmten Fällen einen eigenen, geheimen Algorithmus einzusetzen.

B 12 Geheimen Algorithmus erlangen (UND) (E13)

Ein Angreifer will den geheimen Algorithmus erhalten.

B 12.1 Binärcode des Algorithmus erlangen

Der Algorithmus kann an genau 3 Orten vorliegen;

B 12.1.1 Innerhalb des System-Volumes

Siehe Angriffsbaum Vertraulichkeit System B 9.2

B 12.1.2 Version im Bootloader

Der Angreifer liest den Bootloader aus.

B 12.1.2.1 Zugriff auf das Bootmedium

Siehe B 9.1.1.3.1.1

B 12.1.3 Im RAM

B 12.1.3.1 Durch allgemeinen Angreifer

Siehe Angriffsbaum B 9.2.3

B 12.1.3.2 Angriff durch Innentäter (zusätzlich)

Siehe Angriffsbaum B 9.2.4

B 12.2 Reverse Engineering

Das Reverse Engineering von Kryptoalgorithmen aus Binärcode ist zwar durch dessen Komplexität nichttrivial, aber aufgrund der beschränkten Größe vergleichsweise wenig zeitaufwändig.

Time	Expertise	Knowledge	W.o.O.	Equipment	Summe
5	6	0	1	0	12

Gegenmaßnahmen: Speichern des Algorithmus auf externem Datenträger (z.B. auf Smartcard); Verschlüsselung des vertraulichen Algorithmus direkt durch Smartcard, oder mit einem anderen, nicht vertraulichen Algorithmus (Denn möglicherweise waren für die Wahl des vertraulichen Algorithmus für die Festplattenverschlüsselung Gründe ausschlaggebend, die für die Verschlüsselung eines kurzen, feststehenden Stücks Binärcode irrelevant sind oder durch zusätzlich Maßnahmen wie MAC/Hash/Signatur irrelevant gemacht werden können. Beispiel: Vergleichbar sicherer offener Algorithmus ist für große Datenmengen zu langsam, proprietärer Algorithmus ist integritätssichernd usw.)

Annahme: A27 Geheim zu haltende Algorithmen müssen entweder vom System getrennt sein oder durch einen öffentlichen Kryptoalgorithmus geschützt werden.

5.7 *Angriffsbaum Software-Lebenszyklus (W7)*

B 13 Software-Lebenszyklus angreifen (W7)

B 13.1 Installation (W7.1)

B 13.1.1 Manipulation der Installationsdateien (E13.1)

B 13.1.1.1 Manipulation durch Autoren

Bewertung: Aufgrund der Anonymität der Autoren besteht ein erhöhtes Risiko.

B 13.1.1.1.1 Manipulation am Binärcode

Der ausgelieferte Binärcode könnte von einem anderen als dem veröffentlichten Quelltext stammen bzw. der Binärcode nach dem Kompilieren verändert worden sein, sodass Hintertüren enthalten sind.

Gegenmaßnahme: Vergleich mit selbst kompiliertem Binärcode, Direkte Benutzung des selbst kompilierten Binärcodes.

Annahme: A32 Es wird ein von einer vertrauenswürdigen Instanz kompilierter oder verifizierter Binärcode verwendet.

B 13.1.1.1.2 Manipulation an Quelltext

Es könnten sich Hintertüren bzw. absichtliche Programmierfehler im Quelltext befinden.

Gegenmaßnahme: Code-Review

Annahme: A31 Der Quelltext wurde vollständig auf Fehler und Hintertüren untersucht.

B 13.1.1.2 Manipulation bei Auslieferung

B 13.1.1.2.1 Manipulation auf Homepage

B 13.1.1.2.2 Manipulation bei Übertragung

Gegenmaßnahme: Die Signatur überprüfen.

Annahme: A30 Alle zu installierenden Dateien werden zuvor per Signatur auf ihre Integrität geprüft.

B 13.2 Update (W7.2)

B 13.2.1 Updatedateien manipulieren (E13.2)

Ein Update wird durchgeführt, indem die Installationsdatei heruntergeladen wird und über die alte Version installiert wird. Die Bedrohungen sind daher die gleichen wie in B 13.1 .

B 13.3 Reparaturen (W7.3)

B 13.3.1 Rückstände auslesen (E13.3)

TrueCrypt bietet zur Reparatur eines System-Volumes an, dieses zu entschlüsseln, um es mit einem herkömmlichen Dienstprogramm behandeln zu können. Dabei können Rückstände nach B 1.1.1.1.2 entstehen.

Gegenmaßnahme: Verwendung eines Rettungssystems mit eingebauter Festplattenverschlüsselungssoftware.

Annahme: A3 Auf dem Datenträger wurden zuvor und werden nie sensible Daten im Klartext gespeichert.

B 13.4 Deinstallation (W7.4)

Die Festplattenverschlüsselung soll nicht mehr verwendet werden. Dazu sollen die sensiblen Daten gelöscht, die Verschlüsselung entfernt und die Festplattenverschlüsselungssoftware deinstalliert werden.

B 13.4.1 Rückstände von vertraulichen Daten entschlüsselt zurücklassen (E13.4)

B 13.4.1.1 Swap

Unter Linux wird der verschlüsselte Swap auf einer separaten Partition bei jedem Booten mit einem neuen, zufälligen, nur für diese Sitzung gültigen Schlüssel eingehängt, d.h. es besteht kein Risiko.

Unter Windows wird der Swap als Datei auf dem entsprechend verschlüsselten Systemvolume angelegt. Es muss nun dafür gesorgt werden, dass dieser nicht entschlüsselt wird, indem er z.B. kurzzeitig deaktiviert und gelöscht wird, und im unverschlüsselten System neu angelegt wird.

Annahme: A29.1 Bei der Deinstallation wird der Swap sicher gelöscht.

B 13.4.1.2 Temporäre Dateien / Systemrückstände

Es muss garantiert sein, dass Teile von sensiblen Daten oder Informationen über sensible Daten, die in der Zwischenzeit noch nicht aus der Geheimhaltung entlassen wurden, nirgendwo auf dem Volume gespeichert sind. Wenn dies aufgrund der Komplexität der entsprechenden Software nicht möglich ist (eher die Regel als die Ausnahme), ist das ganze Volume sicher zu löschen.

Annahme: A29 Bei der Deinstallation dürfen keine Informationen bezüglich der verarbeiteten sensiblen Daten mehr im System enthalten sein.

B 13.4.1.3 Freie Blöcke

Beim Löschen, Ändern oder Verschieben von Dateien innerhalb eines verschlüsselten Volumes bleiben Rückstände. Bei einer vollständigen Entschlüsselung werden diese Rückstände mit entschlüsselt.

Annahme: A29.2 Es müssen alle freien Bereiche innerhalb des verschlüsselten Volumes vor der Deinstallation sicher gelöscht sein.

Anmerkung: In der Regel ist es am effizientesten, das System sicher zu löschen und neu zu installieren.

6 Zusammenfassung

6.1 Problematische Annahmen

In der momentanen Version von TrueCrypt sind einige zur Abwehr von Angriffen getroffene Annahmen noch nicht oder nicht sicher erfüllt oder anderweitig problematisch:

- **A6 A6.1 A6.2 A6.3 (Umschlüsseln)**

  Das Umschlüsseln ist noch nicht implementiert. Momentan kann der gleiche Effekt erreicht werden, indem ein neues verschlüsseltes Volume gleicher Größe angelegt wird und das alte Volume auf Dateisystemebene (etwa per dd) blockweise kopiert wird. Einen ähnlichen Effekt kann man erreichen, indem man die Daten dateiweise in ein neues Volume (ausreichender, aber ansonsten beliebiger Größe) kopiert.

- **A6.1 (Mitzählen der verschlüsselten Datenmenge)**

  Ein Mitzählen ist noch nicht implementiert. Der Zähler muss sicher gespeichert sein, z.B. im TPM oder in einem integritätsgesicherten Bereich. Dabei muss auch beachtet werden, dass ein vollständiges Rücksetzen des gesamten Volumes den Zähler nicht rücksetzen darf oder zumindest als Manipulation erkannt wird, sodass Gegenmaßnahmen ergriffen werden können, z.B. eine verfrühte Umschlüsselung.

- **A8 (Logische Integritätssicherung)**

  Da TrueCrypt in der momentanen Version keine eingebaute Integritätssicherung bietet, und auch standardmäßig keine Integritätssicherung von den betrachteten Betriebssystemen bereitgestellt wird, kann den entsprechenden Angriffen nicht durch die Festplattenverschlüsselung begegnet werden, sondern erfordert organisatorische Maßnahmen wie den Einsatz von Siegeln.

  Bei verschlüsselten Systemen kann bei perfekter Erfüllung der entsprechenden Annahmen nach Feststellung physikalischer Integrität auch von logischer Integrität ausgegangen werden. Verschlüsselte Datenträger jedoch müssten nach jeder Benutzung erneut versiegelt werden.

- **A16 (Das Betriebssystem ist sicher.)**

  Diese Forderung kann bei den üblichen Betriebssystemen nicht hundertprozentig erfüllt werden. Es müssen hier die üblichen Sicherheitsvorkehrungen getroffen werden, um sich dieser Forderung wenigstens anzunähern, d.h. regelmäßige Sicherheitsupdates, Virenscanner, Firewalls usw.

- **A18 (Es werden nur die Funktionen benutzt, die keine Administratorrechte seitens des Benutzers erfordern.)**

  Diese Forderung ist unter Windows erfüllbar, allerdings können Benutzer dann nicht die volle Funktionalität nutzen, z.B. verschlüsselte Datenträger erstellen, Passwörter ändern usw.

  Unter Linux ist die Benutzung ganz ohne erhöhte Rechte nicht sinnvoll möglich. Mit – eingeschränkt über sudo – erhöhten Rechten ist zwar von der Konstruktion her theoretisch eine fast uneingeschränkte Nutzbarkeit möglich, dies führt jedoch aufgrund der massiven Lücken immer zu vollen Administratorrechten und verletzt daher diese Voraussetzung.

- **A19 (Ein benutzter Passwort-Cache ist nach Benutzern getrennt.)**

  In der Windows-Version ist der Passwort-Cache nicht nach Benutzern getrennt. Er muss daher modifiziert oder deaktiviert werden.

- **A21.3 (Es wird ein Rechner verwendet, bei dem das Rücksetzen der BIOS-Einstellungen nicht trivial möglich ist.)**

  Dies ist nicht bei jedem Rechner möglich. Eventuell können durch ein TPM die entsprechenden Angriffe dann trotzdem abgewehrt werden.

- **A25 (Verkleben des Arbeitsspeichers)**

  Dies ist problematisch, da bei wirksamer Ausführung eine Reparatur oder eine Aufrüstung dauerhaft unmöglich wird und durch unzureichende Kühlung eine Verkürzung der Lebensdauer möglich ist.

- **A26 (Zur Abwehr von Cache-Timing-Angriffen auf AES wird eine Hardwarebeschleunigung eingesetzt.)**

  Beschleunigungseinheiten sind erst bei neueren Prozessoren verfügbar.

- **A27 (Schutz proprietärer Algorithmen)**

Da noch keine proprietären Algorithmen verwendet werden, ist dieser Punkt momentan belanglos, muss aber bei der Implementierung dieser Algorithmen von vorn herein berücksichtigt werden.

6.2 *Verbleibende Angriffe*

Trotz der getroffenen Annahmen können folgende Angriffe nicht vollständig abgewehrt werden:

- **B 9.2.2.2.1.1.3 (Cold-Boot)**

  Die Absicherung durch Siegel sichert nur gegen *unbemerktes* Öffnen. Hat der Angreifer hier keine Einschränkungen, wird es nahezu unmöglich, sich gegen Angriffe mit angemessenem Aufwand zur Wehr zu setzen.

  Der Angriff kann daher unter den gegebenen Annahmen nicht ausreichend abgewehrt werden, sodass es empfehlenswert ist, die Zugangsmöglichkeiten für Angreifer im laufenden Betrieb bzw. wenige Minuten nach Ausschalten durch eine neue Annahme (A24 „***) einzuschränken. Dies ersetzt auch die problematische Annahme A25 (Speicher verkleben). Das Angreifermodell verändert sich dann dahingehend, dass der Angreifer keinen Zugriff auf ein System mit einer aktiven Festplattenverschlüsselung mehr haben darf.

  Diese Annahme ist aber im Mehrbenutzersystem nur eingeschränkt gegen Außentäter und gar nicht gegen Innentäter durchsetzbar.

- **B 4.2.3 (Schlüssel rechtmäßig erhalten)**

  Ein Innentäter, der ein voll verschlüsseltes System (mit-)benutzt, muss notwendigerweise über die notwendigen Authentifizierungsmerkmale für das System-Volume verfügen und kann somit auch Lese-/Schreibzugriff auf das System-Volume erhalten.

  Dies ist prinzipbedingt. Dieser Angriff kann nur erschwert werden, indem man verhindert, dass der Innentäter sich mit diesen Authentifizierungsmerkmalen (unbemerkt) Zugriff am System vorbei verschafft, z.B. durch ein TPM. Dieses speichert einen Teil des Schlüssels und gibt ihn nur heraus, wenn das System als nicht manipuliert erkannt wird. Das verhindert, dass der Innentäter problemlos z.B. die Festplatte ausbauen und an einem anderen PC auslesen und manipulieren kann. Während des aktiven Systems muss aber hier das System den Schlüssel vor dem Innentäter schützen.

Folgenden Angriffen auf die Benutzertrennung kann momentan – bevor die in AP4 erwähnte Analyse und Behebung aller Design- und Codeschwächen durchgeführt wurde – nur durch vollständigen Verzicht auf das Einsatzszenario „Mehrbenutzersystem" und somit dem Wegfall eines Innentäters begegnet werden.

- **B 9.1.1.1.2.1 (Benutzertrennung Linux)**

  Unter Linux versucht TrueCrypt zwar durch das Design, eine Benutzung durch nicht-privilegierte Benutzerzugänge zu ermöglichen, im momentanen Zustand

wird dies durch Versagen der Benutzertrennung erkauft. Es lassen sich beide Mechanismen zum Zugriff auf mit erhöhten Rechten laufende Programmteile missbrauchen.

  - **B 9.1.1.1.2.1.1 (CoreService angreifen)**
  - **B 9.1.1.1.2.1.2 (Fuse-Schnittstelle angreifen)**

- **B 11.3.3 (Codeschwächen Linux)**
- **B 9.1.1.1.2.2.2 (Codeschwächen Windows)**

Anhang A Bewertungsmaßstab

Die Bewertung geschieht in Anlehnung an „Common Methodology for Information Technology Security Evaluation (CEM v3.1)" R3[12], Anhang B.4, genauere Erläuterungen siehe dort.

Die Punktwerte werden nach folgender Tabelle vergeben:

Faktor	Wert
Gesamtzeit (Time)	
<= ein Tag	0
<= eine Woche	1
<= zwei Wochen	2
<= ein Monat	4
<= zwei Monate	7
<= drei Monate	10
<= vier Monate	13
<= fünf Monate	15
<= sechs Monate	17
> sechs Monate	19
Expertise	
Laie	0
Geübter Benutzer (proficient)	3
Experte	6
Mehrfache Experten	8
Knowledge	
Öffentlich (public)	0
Eingeschränkt (restricted)	3
Sensitiv (sensitive)	7
Kritisch (critical)	11
Window of Opportunity	
Unnötig / unbegrenzter Zugriff	0
Einfach	1
Mittel	4
Schwer	10
Nicht möglich	**
Ausrüstung (Equipment)	
Standard	0
Spezialisiert (specialised)	4
Maßgeschneidert (bespoke)	7
Mehrfach maßgeschneidert (multiple bespoke)	9

12 http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf