# Angriffsszenarien auf TrueCrypt

Clemens Bernhard Röllgen

Global IP Telecommunications
roellgen@globaliptel.com

## Zusammenfassung

In diesem Fachbeitrag werden Angriffsmöglichkeiten auf die populäre Festplattenverschlüsselungssoftware "TrueCrypt" beschrieben. Die Angriffe sind vom Autor bereits im Jahr 2008 veröffentlicht worden und sind das Ergebnis der intensiven Analyse von Quellcode und des Hinterfragens der Motivation der Entwickler von TrueCrypt. Angesichts neuer Erkenntnisse über das Ausmaß der Spionage-aktivitäten verschiedener Geheimdienste stellen sich überdies entscheidende Fragen: Wer sind die Entwickler? Warum behaupten die Entwickler urplötzlich, die Software sei unsicher? Warum wird die Entwicklung aufgegeben?

# 1 Einleitung

TrueCrypt ist laut der bei Layered Technologies, Plano, Texas gehosteten Website "TrueCrypt.org" etwa 30 Millionen Mal heruntergeladen und vermutlich ebenso häufig installiert worden. Die Software ist mit absoluter Sicherheit klarer Marktführer. Der Preis mit € 0,00 ist natürlich unschlagbar. Er wirft jedoch durchaus Fragen über die Finanzierung des Projekts auf.

Festplattenverschlüsselung ist ein zentrales Marktsegment auf dem Gebiet der IT Sicherheit – schließlich liegen bei jedem Anwender sensible Daten auf seinen Rechnern, die eigentlich vor dem Zugriff von Wettbewerbern oder Hackern geschützt sein sollen. Technisch wird dies mit On-The-Fly Verschlüsselung gelöst. TrueCrypt verfügt über alle üblicherweise nachgefragten Leistungsmerkmale: Containerverschlüsselung und Verschlüsselung kompletter Datenträger über eine Erweiterung des BIOS.

Eine marktbeherrschende Software zieht grundsätzlich das Interesse von Hackern jeglicher Ausprägung an. Bei sensiblen Firmendaten ist die Anziehungskraft ganz besonders magisch. Der Marktführer sollte daher ein ausgeprägtes Interesse an sehr hoher Datensicherheit haben. Es ist jedoch eine ganze Reihe von Attacken auf TrueCrypt bekannt und es ist sogar Software kommerziell erhältlich, mit der das Sicherheitsmodell komplett ausgehebelt wird! Das Entwicklerteam unternimmt jedoch seit dem Jahr 2008 keinerlei Anstrengungen, die Sicherheitslücken zu schließen. Immerhin wird laut Reuters nach dem mysteriösen Ende von TrueCrypt [Menn14] seitens eines angeblichen Entwicklers von nicht behobenen Sicherheitslücken berichtet. Auf der Entwicklerseite unter http://TrueCrypt.sourceforge.net/ [True14] wird am 12.06.2014 mit den Worten *„WARNING: Using TrueCrypt is not secure"* vor TrueCrypt gewarnt.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 127-135.

# 2 Das Team

Hinter TrueCrypt steht die TrueCrypt Foundation/TrueCrypt Developers Association, LC, 2360 Corporate Circle Ste 400, Henderson, 89074-7722, Nevada, USA. Es ist ein Managing Member/President/Secretary/Treasurer/Director benannt: Ondrej Tesarik [Neva14]. Die IP Adresse von TrueCrypt.org (72.233.34.82) ist auf die Stadt Plano, 75093 Texas, USA lokalisierbar. Die Organisation dürfte somit innerhalb des rechtlichen Rahmens der Gesetze der USA operieren. Am 16.12.2009 wurde als Besitzer der Marke „TRUECRPYT“ David Tesarik in der TAUSSIGOVA 1170/5, 18200 PRAHA, CZ eingetragen [Uspt09].

Die Recherche nach den Köpfen hinter TrueCrypt fördert lediglich drei Pseudonyme zutage: „David“, "ennead" und "syncon". Mittlerweile sind selbst diese Pseudonyme von der Website verschwunden. TrueCrypt-foundation.org ist mindestens bis zum 22.12.2021 auf die NAVAS Station 80S 120w, Marie Byrd Land 80S 120W, AQ (Antarktis) registriert [Whoi14]. Die wahre Adresse war vermutlich ein Mehrfamilienhaus in der Vratimovska 484, 19000 Praha, CZ, Tel.: +420.921624125 [PCre04].

ICANN 3.7.7.2 [Ican01] sieht jedoch die Löschung von Registrierungen vor, wenn dabei absichtlich falsche Angaben gemacht werden: „*3.7.7.2 A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration*“.

Laut eines Redakteurs von Heise Security schien die Spur zeitweise zum Geheimdienst Israels zu führen. „*Man habe das Gefühl dass es sich bei dem Team hinter TrueCrypt um ein Phantom handelt.*“ Laut heise.de [Holl14] soll ein gewisser TrueCrypt-Entwickler namens „David“ e-Mails verfasst haben, aus denen hervorgeht: „*Demnach gebe es bei dem Entwicklerteam "kein Interesse" mehr an dem Projekt: "Nichts hält ewig." Der gegenwärtige Audit jedenfalls sei nicht der Auslöser gewesen, den habe man begrüßt. .. Aus den kurzen Äußerungen zu dem E-Mail-Austausch geht noch hervor, dass die TrueCrypt-Entwickler angeblich keinen Kontakt zu irgendeiner Regierungsbehörde hatten. Einzige Ausnahme sei eine Anfrage wegen eines "Support-Vertrags" gewesen. .. Außerdem habe sich der Entwickler noch zu einer möglichen Weiterentwicklung von TrueCrypt unter anderer Lizenz geäußert. Demnach stehe er "persönlich" einem Fork kritisch gegenüber und hielte das für gefährlich, da nur das Team den Code wirklich kennen würden. Der sei aber als Referenz weiterhin verfügbar. Außerdem habe er sich überzeugt gezeigt, dass Bitlocker "gut genug" sei. Dass dieses Microsoft-Programm nur für Windows verfügbar sei, sei kein Problem, sei dieses Betriebssystem doch auch "das eigentliche Ziel des Projekts" gewesen*.“

# 3 Die Qualität des Quellcodes

Der Quellcode von TrueCrypt basiert auf dem Projekt E4M von Paul Le Roux. Der Copyrightvermerk von Paul Le Roux ist immer noch in den aktuellen Sourcen von TrueCrypt auffindbar. E4M basiert auf einem Beispiel für einen NT4 Treiber einer RAM Disk (Microsoft DDK).

Der Code ist professionell geschrieben und frei von Merkmalen, die Rückschlüsse auf die Persönlichkeit eines Programmierers zulassen. Aus der Erfahrung mit einem ähnlichen Projekt (OTFE Containerverschlüsselung) muss ein Team, welches eine Software mit der Komplexität

von TrueCrypt entwickeln soll, aus mindestens 10 Entwicklern bestehen. Die Verschlüsselung über das BIOS bindet dabei den Großteil der Entwicklermannschaft. Externe Hilfe von Verschlüsselungsexperten und von Prozessorherstellern wird überdies benötigt. AES ist in TrueCrypt fünffach implementiert: tabellenorientiert, „klein“, in x86 Assembler, x64 Assembler und hardwarebeschleunigt.

Die Lösung wirkt klinisch sauber. Sie lässt überdies keinen Zweifel aufkommen, dass irgendeine Funktionalität technisch auf andere Art besser programmiert werden könnte. Das Sicherheitsmodell geht davon aus, dass Angriffe während der Laufzeit von TrueCrypt kaum zu erwarten sind. Das TrueCrypt Projekt hat sich überwiegend darauf konzentriert, nicht zur Laufzeit eingebundene Containerdateien abzusichern. Angriffe erfolgen jedoch heute meist während der Laufzeit über unterschiedlichste Seitenkanäle.

# 4 Angriffsszenarien

Angriffe auf in Betrieb befindliche Computer sind seit vielen Jahren wahrscheinlicher als die klassische Konfiszierung von Hardware. Unter Berücksichtigung dieses Aspekts ist TrueCrypt sowohl am Control Panel (Grafische Benutzerschnittstelle), als auch am Verschlüsselungstreiber angreifbar.

Angriffe auf die grafische Benutzerschnittstelle durch:

- Trojaner, welche Tastaturereignisse aufzeichnen
- Software, die allokierten Speicher aufzeichnet
- Sicherheitskopien verschlüsselter Container
- Schwache Verschlüsselung

Angriffe auf den Verschlüsselungstreiber:

- Software, die allokierten Speicher aufzeichnet
- Puffern von Schlüsseln
- Fehlende Flexibilität beim Startsektor versteckter Container
- Schwache Verschlüsselung
- Transport der Daten des Mount Requests im Klartext

## 4.1 Trojaner, welche Tastaturereignisse aufzeichnen

Derartige Trojaner sind seit langem bekannt. Gegenmaßnahmen schließen die Verwendung speziell gesicherter, externer Tastaturen ein, welche jedoch kaum von den Anwendern einer kostenlos verfügbaren Software gekauft würden.

Eine technisch realisierbare und kostenneutrale Lösung ist eine virtuelle Anti-Trojaner-Tastatur nach Abbildung 1 [Röll08a].

Die virtuelle Tastatur nach Abbildung. 1 ist von einer OTFE Verschlüsselungssoftware, die sich im Wettbewerb mit TrueCrypt befindet, bekannt. Es ist nicht bekannt, inwieweit z.B. die Capturemodule der Firma Digitask eine derartige virtuelle Tastatur angreifen können. Es ist jedoch zu erwarten, dass ein professionell geschriebener Trojaner Tastaturereignisse aufzeichnen kann.

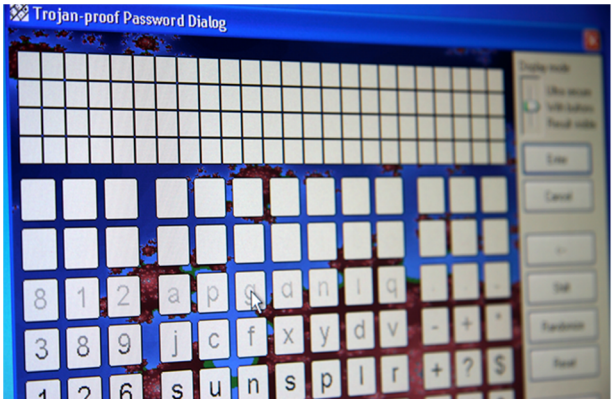


**Abb. 1:** Virtuelle Tastatur zur Eingabe von Kennwörtern

Eine virtuelle Tastatur nach Abbildung. 1 nutzt die Fähigkeit eines Threads, die Prioritätsklasse dynamisch verändern zu können. Sobald die virtuellen Tasten auf dem Bildschirm sichtbar sind, ist die Threadpriorität auf den maximal möglichen Wert eingestellt und es werden auf allen Prozessorkernen rechenintensive Operationen ausgeführt. Sobald die virtuellen Tasten jedoch nicht mehr sichtbar sind, wird die Threadpriorität stark abgesenkt, wodurch das Betriebssystem in die Lage versetzt wird, wartende Threads mit hoher oder normaler Priorität zur Ausführung zu bringen. Eine derartige virtuelle Tastatur verhält sich aus dem Blickwinkel des Betriebssystems kooperativ und es ist zu erwarten, dass bösartige Capturemodule grundsätzlich während der Dunkelphasen vom Betriebssystem zur Ausführung gebracht werden.

## 4.2 Software, die allokierten Speicher aufzeichnet

Diese Form der Attacke wird von mehreren Firmen für unter 1000 USD angeboten. Im RAM des Computers wird entweder das Control Panel oder der Verschlüsselungstreiber von TrueCrypt, BitLocker oder PGP lokalisiert und Bereiche mit hoher Entropie analysiert. Dort ist die Wahrscheinlichkeit am größten, die Rundenschlüssel der Verschlüsselungsalgorithmen oder sogar zwischengespeicherte Schlüssel zu finden.

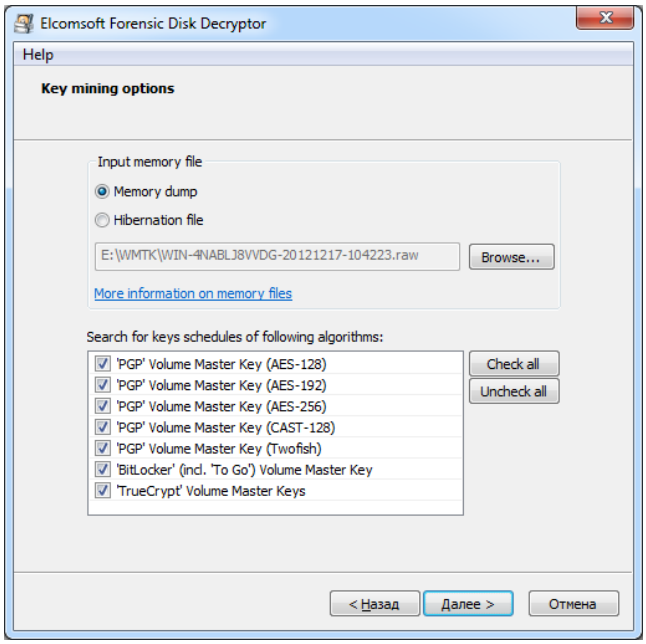


**Abb. 2:** Kommerzielle Software zum Auslesen von Schlüsseln [Elco12]

Das „Passware Kit Forensic 13.1" [Pass13] ist sogar zu folgenden Aktionen in der Lage:

> *„Recovers encryption keys for hard disks protected with BitLocker in minutes, including BitLocker ToGo*
>
> *Decrypts TrueCrypt, FileVault2, and PGP volumes in minutes"*

Die Acquisition der Rohdaten erfolgt hierbei über die Betriebssystemfunktionen *ZwMapViewOfSection(), MmMapIOSpace()* und die nicht dokumentierte Funktion *MmMapMemoryDumpMdl()*, welche zur ausschließlichen Verwendung durch den Kernel Debugger vorgesehen ist [StMc13] Alle drei Funktionen können bei neueren Windows Versionen nur noch aus dem Kernel heraus durch einen Treiber aufgerufen werden.

## 4.3 Sicherheitskopien verschlüsselter Container

Üblicherweise unterstützt OTFE Software den Anwender nicht beim Anlegen von Sicherheitskopien. So existiert nach einiger Zeit höchstwahrscheinlich mindestens eine ältere Kopie eines Containers mit modifiziertem Inhalt. OTFE Software führt naturgemäß bei der sektorweisen Verschlüsselung von Containern mit identischen Kennwörtern die exakt gleichen Operationen durch. TrueCrypt verwendet sogenannte „Disk Keys". In der Containerdatei befindet sich ein Schlüssel, welcher vom Verschlüsselungstreiber gelesen und mit dem Schlüssel, den der Anwender eingibt, exklusiv-oder verknüpft wird. Die Methodik ist keineswegs unsicher. Der Vorteil darin liegt in der Möglichkeit, Benutzerkennwörter leicht ändern zu können, ohne dazu einen kompletten Container neu verschlüsseln zu müssen. Ändert der Anwender das Passwort, so ändert sich lediglich der „Disk Key".

Ist bei einer OTFE Software beispielsweise der Inhalt von Sektor 12345 in der aktuellen Version und im Backup identisch, so liegt mit 100% Sicherheit der gleiche Klartext vor. Es ist daher möglich, nach Unterschieden zu fahnden und diese grafisch darzustellen.

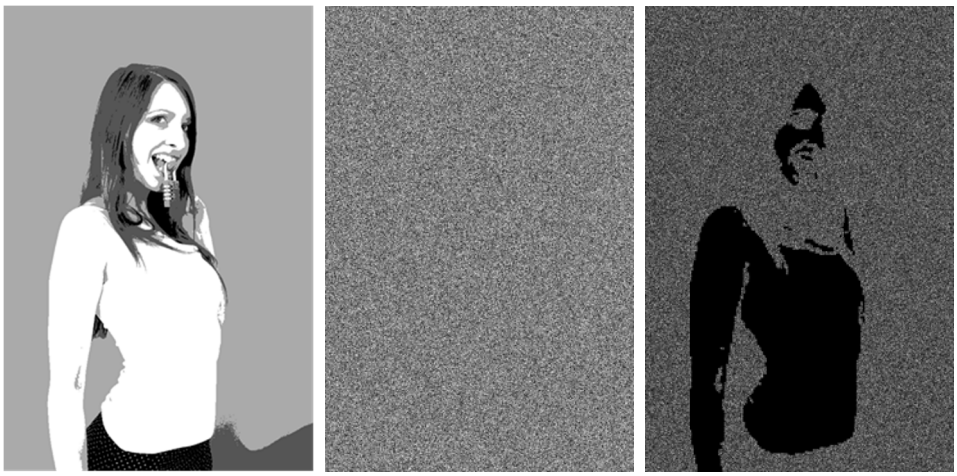

**Abb. 3:** Grafische Darstellung der Unterschiede

Abbildung 3 zeigt das Bild als Klartext (links), mit AES und Blockzähler verschlüsselt (Mitte), die Differenz des Chiffrats (Mitte) vom Chiffrat eines komplett weißen Bildes, welches ebenfalls mit AES und Blockzähler unter Verwendung des gleichen Schlüssels verschlüsselt wurde

Die Attacke [Röll08b] ermöglicht versteckte Container zu enttarnen. Es sind überdies Rückschlüsse auf die Größe des versteckten Containers und in manchen Fällen sogar auf dessen

Inhalt möglich. Es ist weder Kenntnis des Schlüssels, des verwendeten Verschlüsselungsverfahrens, noch des Betriebsmodus (ECB, CM, GCM, LRW, XEX, XTS oder CBC) nötig.

Abhilfe ist lediglich durch das Kopieren einer kompletten Containerdatei möglich, indem die Verschlüsselungssoftware für die Kopie einen neuen „Disk Key“ verwendet.

## 4.4 Schwache Verschlüsselung

Die Rundenschlüssel des AES Verschlüsselungsverfahrens umfassen zwischen 32 und 64 Byte – je nach Länge der gewählten Schlüssellänge. Für die Entschlüsselung ist ein ebenso großes Array erforderlich.

Erfolgt der Angriff auf ein Verschlüsselungsverfahren mittels eingeschleuster Schadsoftware, so sind herkömmliche Paradigmen auf den Prüfstand zu stellen. Die Rundenschlüssel von AES verändern sich während der Laufzeit nicht. Für einen erfolgreichen Angriff auf AES reicht die Kenntnis der Rundenschlüssel für Ver- und Entschlüsselung völlig aus. Diese Aussage trifft auf die meisten bekannten symmetrischen Verfahren gleichermaßen zu.

Abbildung 4 zeigt ein für AES typisches Speicherabbild. Aus Abbildung 2 ergeben sich die realen Auswirkungen dieser Schwäche des Designs.

Abhilfe ist nur durch die Wahl eines speziell gegen derartige Angriffe gehärteten Verschlüsselungsverfahrens möglich. Ein solches Verschlüsselungsverfahren verändert sinnvollerweise das Speicherabbild fortwährend. Die sichere Abwehr von Angriffen auf Rundenschlüssel ist technisch anspruchsvoll, jedoch nicht unmöglich. Es wurde seitens der Entwickler von TrueCrypt, Bitlocker und PGP bislang keine Anstrengung in dieser Richtung unternommen.

```
0x0000000005F8C4F0  10 c8 f8 05 00 00 00 00 a8 71 12 40 01 00 00 00 00 00 00 00 00 00 00 00 13 f1 04 77
0x0000000005F8C50C  00 00 00 00 ee 14 d4 37 00 00 00 00 de 92 19 40 01 00 00 00 50 1a 0d 06 00 00 00 00
0x0000000005F8C528  40 18 0d 06 00 00 00 00 01 00 00 00 00 00 00 00 43 6c 12 40 01 00 00 00 0a 00 00 00
0x0000000005F8C544  cc cc cc cc 54 c7 f8 05 00 00 00 00 80 00 00 00 80 00 00 00 cc cc cc cc cc cc cc cc
0x0000000005F8C560  10 c8 f8 05 00 00 00 00 73 37 00 40 01 00 00 00 b0 c5 f8 05 00 00 00 00 00 80 37 40
0x0000000005F8C57C  01 00 00 00 80 00 00 00 cc cc cc cc cc cc cc cc cc cc cc cc 01 00 00 00 00 00 00 00
0x0000000005F8C598  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc 0a 00 00 00
0x0000000005F8C5B4  03 02 01 00 07 06 05 04 0b 0a 09 08 0f 0e 0d 0c fd 74 aa d6 fa 72 af d2 f1 78 a6 da
0x0000000005F8C5D0  fe 76 ab d6 0b cf 92 b6 f1 bd 3d 64 00 c5 9b be fe b3 30 68 4e 74 ff b6 bf c9 c2 d2
0x0000000005F8C5EC  bf 0c 59 6c 41 bf 69 04 bc f7 f7 47 03 3e 35 95 bc 32 6c f9 fd 8d 05 fd e8 a3 aa 3c
0x0000000005F8C608  eb 9d 9f a9 57 af f3 50 aa 22 f6 ad 7d 0f 39 5e 96 92 a6 f7 c1 3d 55 a7 6b 1f a3 0a
0x0000000005F8C624  1a 70 f9 14 8c e2 5f e3 4d df 0a 44 26 c0 a9 4e 35 87 43 47 b9 65 1c a4 f4 ba 16 e0
0x0000000005F8C640  d2 7a bf ae d1 32 99 54 68 57 85 f0 9c ed 93 10 4e 97 2c be 7f 1d 11 13 17 4a 94 e3
0x0000000005F8C65C  8b a7 07 f3 c5 30 2b 4d cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
0x0000000005F8C678  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
0x0000000005F8C694  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
0x0000000005F8C6B0  cc cc cc cc 7f 1d 11 13 17 4a 94 e3 8b a7 07 f3 c5 30 2b 4d be 29 aa 13 f6 af 8f 9c
0x0000000005F8C6CC  80 f5 70 f7 03 bf f7 00 63 a4 62 13 48 86 25 8f 76 5a ff 6b 83 4a 87 f7 74 fc 82 8d
0x0000000005F8C6E8  2b 22 47 9c 3e dc da e4 f5 10 78 9c 8d 09 e3 72 5f de c5 11 15 fe 9d 78 cb cc a2 78
0x0000000005F8C704  27 10 c4 2e d2 d7 26 63 4a 20 58 69 de 32 3f 00 04 f5 a2 a8 f5 c7 e2 4d 98 f7 7e 0a
0x0000000005F8C720  94 12 67 69 91 e3 c6 c7 f1 32 40 e5 6d 30 9c 47 0c e5 19 63 99 02 db a0 60 d1 86 22
0x0000000005F8C73C  9c 02 dc a2 61 d5 85 24 f0 df 56 8c f9 d3 5d 82 fc d3 5a 80 fd d7 59 86 03 02 01 00
0x0000000005F8C758  07 06 05 04 0b 0a 09 08 0f 0e 0d 0c cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
0x0000000005F8C774  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
0x0000000005F8C790  cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc
```

**Abb. 4:** 256 Bit AES Rundenschlüssel (encrypt + decrypt) im Speicher der OTFE Software

## 4.5 Puffern von Schlüsseln

TrueCrypt verfügt über dieses komfortable, jedoch gefährliche Feature. Attacken nach Abbildung 2 sind mindestens seit 2008 bekannt, jedoch sind die Entwickler von TrueCrypt nicht gewillt, Abhilfe zu schaffen. Angreifern ist es jedoch meist egal, ob sie AES Rundenschlüssel

oder noch nicht expandierte Schlüssel auslesen müssen. Aufwand und Vorgehensweise (Analyse des RAM) sind nahezu identisch.

## 4.6 Statik des Startsektors versteckter Container

Der 512 Byte Header versteckter Container liegt 1536 Byte unterhalb des Endes des äußeren Containers. Angreifer können mit hoher Sicherheit davon ausgehen, dass wirklich geheime Daten in versteckten Containern residieren. Die Statik des Mechanismus ist unbegreiflich, denn es ist ein Leichtes, den Startsektor völlig variabel zu gestalten und dadurch diesen zum Attackieren eines versteckten Containers dringend erforderlichen Sektor effektiv zu verstecken. In diesem Fall wäre ein Angreifer dazu gezwungen, eine zeitraubende Attacke auf mindestens 90% der Sektoren einer Festplatte anzuwenden. TrueCrypt verhält sich aus der Sicht eines Angreifers äußerst kooperativ.

## 4.7 Transport der Daten des Mount Requests im Klartext

Seit Edward Snowden im Jahr 2013 an die Öffentlichkeit gegangen ist und viel über die Arbeitsweise von Geheimdiensten bekannt wurde, ist klar geworden, dass sich Unternehmen unter Androhung staatlicher Sanktionen erstaunlich kooperativ verhalten.

Die Datei Apidrv.h des Quellcodes von TrueCrypt enthält die IO Control Codes, über die der Verschlüsselungstreiber vom Control Panel aus erreichbar ist. Ein ausgesprochen effizienter Angriff ist auf den IO Control Code zum Einbinden eines verschlüsselten Containers möglich:

```
#define MOUNT  466944    /* Mount a volume or partition */
```

Die Betriebssystemfunktion DeviceIoControl() ist die einzige Funktion, mittels derer Anwendersoftware mit Treibern kommunizieren kann. TrueCrypt übergibt dieser Funktion im Klartext den Dateipfad des verschlüsselten Containers, das Passwort und eine kleine Anzahl Kontrolldaten (z.B. ein Read-only Flag). Das Betriebssystem bekommt über eine einzige Funktion Klartextdaten zum Einbinden verschlüsselter Container, die eineindeutig über eine 32 Bit Zahl - den IO Control Code 466944 – identifizierbar ist. Für den Hersteller des Betriebssystems ist es ein Leichtes, die Daten instantan zu identifizieren und die Daten in einem Pufferspeicher langfristig zu speichern. Es ergibt sich mit der Zeit ein lückenloses Bild sämtlicher Versuche, mit TrueCrypt verschlüsselte Container einzubinden. Die Qualität der gewonnenen Informationen ist enorm hoch und die Datenmenge beschränkt sich auf das absolute Minimum: Datum, Uhrzeit, Dateipfad des Volumes und Passwort.

In Anbetracht des Ausmaßes der Überwachung seitens der NSA ist die Wahrscheinlichkeit, dass die beschriebene Attacke real praktiziert wird, im zweistelligen Prozentbereich anzusiedeln. Eine derartige Attacke [Röll08c] lässt sich technisch nicht leicht unterbinden. Das Betriebssystem kann grundsätzlich nach bestimmten IO Control Codes filtern und den Datenverkehr mit Verschlüsselungstreibern aufzeichnen. Es ist jedoch durchaus möglich, Dateipfad und Passwort vor dem Betriebssystem zu verbergen.

Die technische Lösung [Röll08c] umfasst einen Verschlüsselungstreiber, der mit der Steuerungsanwendersoftware zunächst einen Diffie-Hellman Schlüsseltausch durchführt. Misst ein derart konzipierter Treiber die Rechenzeit, lassen sich sogar Man-in-the-middle-Attacken zuverlässig detektieren. Eine Lösung, die der dargestellten Attacke standhält, existiert bereits seit dem Jahre 2008. Sie ist seitdem nicht in der Liste „unterstützter Formate“ kommerzieller Forensiksoftware enthalten.

# 5 Ergebnis

Das mit weitem Abstand weltweit populärste Verschlüsselungstool für Datenträger wurde von einer Gruppe professioneller Entwickler in völliger Anonymität gepflegt und ist somit von zweifelhafter Provenienz. Es existiert eine Reihe von Attacken auf TrueCrypt [4, 5, 6, 7, 8]. Die Effizienz und Popularität der Attacke auf das Speicherabbild des Verschlüsselungstreibers und des Control Panels ist derart hoch, dass es mindestens zwei Anbieter kommerzieller Tools gibt. Das Produkt TrueCrypt entspricht eher nicht den Anforderungen an die Datensicherheit im Zeitalter permanent miteinander vernetzter Universalrechner. Auf der Homepage von Passware [Pass13] bekommt man den Eindruck, dass das „Knacken“ von TrueCrypt-Containern (Volumes) nicht sonderlich schwer ist:


TESTIMONIALS

Today I was able to open a True-Crypt Volume in a very important case. All the relevant information for the case has been in there. Other products have failed before. Thank you Passware!
**Matthias Berg,**
**Hessisches Landeskriminalamt,**
**Detective Inspector.**

**Abb. 5:** Empfehlungsschreiben eines zufriedenen Anwenders der Software „Passware“ [Pass13]

Vage Vermutungen über die Herkunft, weitgehend fehlende öffentliche Kritik seitens einschlägig bekannter Experten und jahrelanges Versäumnis zum Härten der Software gegen leicht zu führende Attacken wie beispielsweise gegen Logger für Tastaturereignisse und der überdies fabelhafte Preis, dafür jedoch die Existenz kommerzieller Software zum Knacken von TrueCrypt Containern, weisen in der Summe auf einen klassischen „Honeypot“ hin.

Es erscheint angesichts des Erfolges von TrueCrypt als bemerkenswert, dass das Entwicklerteam "kein Interesse" mehr an dem Projekt hat und dass urplötzlich nach mehr als 10 Jahren Weiterentwicklung auf der Entwicklerseite [True14] der Schriftzug „*WARNING: Using TrueCrypt is not secure*“ zu lesen ist.

War die Software jemals sicher? Worin liegt der Grund für diese Warnung? Die Eindringlichkeit, in der die Warnung formuliert ist, sowie das Fehlen einer schlüssigen Begründung, werfen eine Menge Fragen auf. Millionen Menschen haben TrueCrypt vertraut. Ist die Art und Weise der Kommunikation mit den Anwendern angemessen? Für wen ist sie hingegen typisch?

Auf die dringendsten Fragen gibt es bis heute keine Antwort und es steht zu vermuten, dass sich dies nicht ändern wird.

Es bleibt abzuwarten, ob die Entwicklung durch ein anderes Team weitergeführt werden darf. Die Software ließe sich durchaus härten.

## Literatur

[Neva14] Nevada Secretary of State, Nevada: Business search, Suchergebnisse für NV Business IDs NV20091535312 und NV20091452250, http://nvsos.gov/sosentitysearch/CorpSearch.aspx (08.02.2014).

[Whoi14] Whois Suchanfrage bei Network Solutions: http://who.is/whois/TrueCrypt-foundation.org und http://www.whois.com/whois/TrueCrypt.org (08.02.2014).

[PCre04] Forumeintrag bei PCreview.co.uk: http://www.pcreview.co.uk/forums/TrueCrypt-1-0-released-t1967957.html (2004).

[Röll08a] C.B. Röllgen: The Trojan-Horse-Proof Virtual Keyboard http://pmc-ciphers.com/eng/content/TurboCrypt/Secure-password-entry.html (2008).

[Elco12] Elcomsoft: Elcomsoft Forensic Disk Decryptor, http://www.elcomsoft.de/efdd.html (2012).

[Pass13] Passware: Passware Kit Forensic 13.1, http://www.lostpassword.com/kit-forensic.htm (2013).

[Röll08b] C.B. Röllgen: Visualisation of potential weakness of existing cipher engine implementations in commercial on-the-fly disk encryption software, http://www.pmc-ciphers.com/eng/content/TurboCrypt/Backup-Attack.html (2008).

[Röll08c] C. B. Röllgen: Attack on mount control code of commercial on-the-fly disk encryption software and efficient countermeasure, http://pmc-ciphers.com/eng/content/TurboCrypt/Mount-Control-Code-Attack.html (2008).

[Menn14] Joseph Menn (Reuters): Exclusive: Security enthusiasts may revive encryption tool after mystery shutdown, http://www.reuters.com/article/2014/05/29/us-internet-security-encryption-idUSKBN0E925M20140529 (29.05.2014).

[True14] TrueCrypt.sourceforge.net: http://TrueCrypt.sourceforge.net/ (12.06.2014).

[Holl14] Martin Holland (heise.de): Ende von TrueCrypt: Entwickler hat angeblich Interesse verloren, http://www.heise.de/newsticker/meldung/Ende-von-TrueCrypt-Entwickler-hat-angeblich-Interesse-verloren-2211228.html (30.05.2014).

[Uspt09] TRUECRYPT trademark entry, United States Patent and Trademark Office: http://tsdr.uspto.gov/documentviewer?caseId=sn78860644&docId=COA20091217102238#docIndex=7&page=1 (2009).

[Ican01] ICANN: Registrar Accreditation Agreement, REGISTRAR OBLIGATIONS: https://www.icann.org/resources/unthemed-pages/raa-2001-05-17-en#3 (2001).

[StMc13] Johannes Stüttgen, Michael Cohen: Anti-forensic resilient memory acquisition, http://www.dfrws.org/2013/proceedings/DFRWS2013-13.pdf (2013).