



Sicherheitstage SS/09 Verschlüsselung von Daten mit TrueCrypt

TRUECRYPT

FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION

Birgit Gersbeck-Schierholz, IT-Sicherheit, RRZN



TrueCrypt

- frei verfügbare, quelloffene Verschlüsselungssoftware für Windows und Linux

- On-the-fly-Verschlüsselung/Entschlüsselung: TrueCrypt entschlüsselt nur für den Arbeitsspeicher/RAM, es werden keine unverschlüsselten Daten auf der Festplatte zwischengespeichert.

- erzeugt eine verschlüsselte Systempartition oder verschlüsselte Volumes, dabei erfolgt die Authentisierung über alphanumerische Kennwörter und Schlüsseldateien, Volumes können im laufenden Betrieb beliebig geöffnet und geschlossen werden

- bietet 3 Verschlüsselungsverfahren an: AES, Serpent, Twofish, diese können einzeln und in allen möglichen Kombinationen eingesetzt werden (Performance!)

- Aktuelle Version 6.2a



TrueCrypt

Punkte, die im Folgenden näher erläutert werden sollen:

- TrueCrypt-System-Verschlüsselung
- "Traveler Mode"
- "Hidden Files"
- Schlüsseldateien



TrueCrypt System-Verschlüsselung



Alle Dateien und Registry-Einträge sind permanent verschlüsselt

Pre-boot Authentifizierung wird realisiert über den TrueCrypt Boot Loader

TrueCrypt Rescue Disk für den Fall, dass

- -> Der TrueCrypt-Boot-Loader defekt ist oder mit Malware infiziert ist
- -> Der Master-Key oder andere kritische Daten defekt sind
- -> Windows defekt ist



TrueCrypt System-Verschlüsselung

- Unterstützte Windows Betriebssysteme:
 - Windows XP
 - Windows XP x64
 - Windows Vista
 - Windows Vista x64
 - Windows Server 2003
 - Windows Server 2003 x64

TrueCrypt System-Verschlüsselung

True	Crypt	_ _ X	ſ	
Volumes	System Schlüsseldateien Extras Einstellungen Hilfe	Homepage		Unverschlüsseltes
LW F: G: J: J: J: J: J: J: M: M: M: M: Q: Q:	System Schlusseldatelen Extras Einstellungen Hilfe System-Partition/Laufwerk dauerhaft entschlüsseln System-Partition/Laufwerk dauerhaft entschlüsseln Unterbrochenen Vorgang fortsetzen Verstecktes Betriebssystem erstellen Rettungsdatenträger erstellen Rettungsdatenträger überprüfen Ohne Pre-Boot Authentifikation einbinden Kennwort ändern Algorithmus für Headerschlüsselberechnung ändern Eigenschaften Einstellungen Volume erstellen	Cache sicher löschen		System wiederherstellen
Volum	e	Tel Datai		
		· Datei		

- Absicherung nur mit Passwort, die Funktion "Schlüsseldatei" wird nicht unterstützt
- Nach Passwortwahl werden Header-Key und Master-Key generiert
- Iso-Image f
 ür Rescue-Disk wird erstellt
- Nach Neustart startet der Verschlüsselungsvorgang
- Nach erfolgreicher TrueCrypt-Verschlüsselung meldet sich vor jedem Bootvorgang der TrueCrypt-Boot-Loader und fordert das Passwort



TrueCrypt System-Verschlüsselung



- 30.07.09: Österreichischer IT-Sicherheitsspezialist stellt sein "Bootkit" "Stoned" vor, das diese Systemverschlüsselung aushebelt, indem es sich in den Master Boot Record schreibt, der stets unverschlüsselt ist.
- Für eine Infektion mit "Stoned" ist ein physischer Zugang notwendig (z.B. CD-Laufwerk)
- Die verschlüsselten Daten sind weiterhin verschlüsselt und können weiterhin nur mit dem TrueCrypt-Passwort entschlüsselt werden.







- Der TrueCrypt "Traveler Mode" ermöglicht eine Installation der Verschlüsselungssoftware auf dem USB-Stick. Damit kann kann der verschlüsselte Inhalt an jedem Rechner entschlüsselt werden. Eine TrueCrypt-Installation auf dem Endgerät ist nicht notwendig.
- Problem dabei ist, dass der Benutzer Admin-Rechte braucht, da auf dem Rechner ein Laufwerk gemountet werden muss.
- Um trotzdem diesen sehr eleganten Modus nutzen zu können, wird im Folgenden eine "Hybrid-Konfiguration" vorgeschlagen.



- USB-Stick
 - TrueCrypt Traveler-Mode im unverschlüsselten Bereich
 - Verschlüsselte TrueCrypt-Container, z.B. dienstlich und privat



- Arbeitsplatz-Rechner
 - Benutzer mit eingeschränkten Rechten
 - TrueCrypt-Installation auf dem Rechner
 - Optional:
 - Automatisches Mounten des verschlüsselten TrueCrypt-Volumes
 - Bei Rechnerstart wird das TrueCrypt-Passwort abgefragt

- Dienst-Notebook, Privat-Rechner, ...
 - Benutzer hat Admin-Rechte
 - Keine TrueCrypt-Installation notwendig

$R \mid R \mid Z \mid N \mid$



- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - TrueCrypt-Installation
 - 1. Admin installiert TrueCrypt auf dem Rechner





- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - TrueCrypt-Installation
 - 2. Admin installiert den "Traveler Mode" auf dem USB-Stick

TrueCrypt			
Volumes System Schlüsseldateien E	xtras Einstellungen Hilfe	Homepage	
LW Volume	Benchmark-Test Testvektoren	isselungsalg. Typ	TrueCrypt Traveler Disk Installation
G:	Traveler Disk Installation		Dateieinstellungen Erstelle die Traveler Disk Datein in (Traveler Disk Stammverzeichneis):
 ⇒ J: ⇒ K: 	Schlüsseldatei erstellen. TrueCrypt-Volume erstellen		G:\Durchsuchen
≪>L: ≪>M:	Laufwerksbuchstaben aktualisieren		Assistent für die Erstellung von TrueCrypt-Volumes mitkopieren
≪N: ≪O: ≪O:	Volume-Header sichern Volume-Header wiederherstellen		Autostart-Konfiguration (autorun.inf) Beim Anschließen einer Traveler Disk:
● R: ● S: ● T:	Volume-Verlauf löschen Kennwort-Cache sicher löschen		Nichts machen TrueCrypt starten
		· 🖃	C <u>T</u> rueCrypt-Volume autom. einbinden (wie unten angegeben)
Volume erstellen	Eigenschaften,	Cache sicher löschen	Einstellungen beim Einbinden
Volume		Datei	Laufwerksbuchstabe; erster verfügbare
Verlauf nicht speicher	VolOperationen	Datenträger	Explorer-Fenster für eingebundenes Volume öffnen Als schreibgeschütztes Laufwerk einbinden
Einbinden Alle Dater	ntr. einbinden Alle trennen	Beenden	Kennwort im Cache halten
			Erstellen Schließen



- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - TrueCrypt-Installation
 - 3. Admin oder der Benutzer selbst legt ein oder mehrere Volumes auf dem USB-Stick an

True(Trypt							_	
<u>V</u> olumes	S <u>y</u> stem	Schlüsseldateien	E <u>x</u> tras	Einstellun <u>g</u> en	<u>H</u> ilfe			Home	page
LW	Volume				Größe	Verschlüsselu	nasala	Typ	
	volume				Grobe	verschlasseld	igadigi	178	
- М:									
See 1.									
0:									
Q									
Sec.									
С. т.									
Sin Contraction (1997) € 1997									
₩V:									
×:									
→ Ti → 7:									-
1 - 2.									
	/olume ers	stellen		Eigenschafte	n	0	ache sich	er löscher	
	_		_						
Volum	e								
						_	Dat	ei .	
							Date	- 1	
		Verlauf nicht speid	hern	Vo	IOperatio	nen	Datentr	äger	
	_								_
	Finhinden		atentr ei	obinden	Alle tree	nen l	Re	andan	
	Linonden	Alle Da	itterna i ei		Aje del	inen	<u>D</u> e	enden	



- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - Arbeiten mit dem verschlüsselten USB-Stick Variante 1



11 Leibniz 102 Universität 1004 Hannover

$R \mid R \mid Z \mid N \mid$

TrueCrypt "Traveler Mode"

- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - Arbeiten mit dem verschlüsselten USB-Stick

Variante 2





$R \mid R \mid Z \mid N \mid$



- Arbeitsplatz-Rechner (Benutzer mit eingeschränkten Rechten)
 - Arbeiten mit dem verschlüsselten USB-Stick Variante 2





TrueCrypt "Traveler Mode"

- Dienst-Notebook, Privat-Rechner (Benutzer hat jeweils Administratorrechte)
 - Arbeiten mit dem verschlüsselten USB-Stick
 - Start- und Stoppdateien auf dem USB-Stick
 - 1. Mounten.bat

Datei	Bearbeit	en Suchen	Ansicht	Format	Sprachen	Einstellungen	Makr
0 5	86	66 4	b	9 C	8 bg	3 3	⊡ ≡
📄 ma	ounten.bat	1					
	1 Tru	eCrypt.ex	e /lz /	'q /a /d	c n /m r	m /v GEHEI	М
	2 act	ion=Mount	TrueCr	ypt Vol	lume		

2. Ende.bat



TrueCrypt – "Hidden Volume"

"Plausible Deniability"

- "glaubwürdiges Abstreiten der Kenntnis eines Sachverhaltes"
- hört sich geheimnisvoll an, ist aber nur in bestimmten Fällen sinnvoll



R R Z N



TrueCrypt – "Hidden Volume"

Hidden Volume erstellen



OK

X



Leibniz <u>Un</u>iversität

Hannover

102



TrueCrypt – "Hidden Volume"

Hidden Volume, graphische Darstellung





TrueCrypt – Arbeiten mit Schlüsseldateien (Key Files)

- Zusätzlich zum Passwort kann eine oder mehrere Schlüsseldateien verwendet werden, um das verschlüsselten TrueCrypt–Volumes abzusichern.
- Es handelt sich um einen zusätzlichen Schutz vor Keyloggern oder Brute Force Angriffen auf das Passwort.
- Ermöglicht multi-user shared access
- Es werden zwei Verfahren zur Bereitstellung von Schlüsseldateien angeboten:
 - Mittels TrueCrypt–Zufallsgenerator (max. Länge 512 bit)
 - Eine existierende Datei oder ein kompletter Pfad







TrueCrypt

Wiederherstellung/Entschlüsseln der Daten bei PW/Schlüsselverlust

Nicht möglich!!!



Literatur:

- http://www.truecrypt.org/
- <u>http://board.gulli.com/thread/674868-anleitung-tutorial-und-howto-truecrypt-verschlsselung/</u>