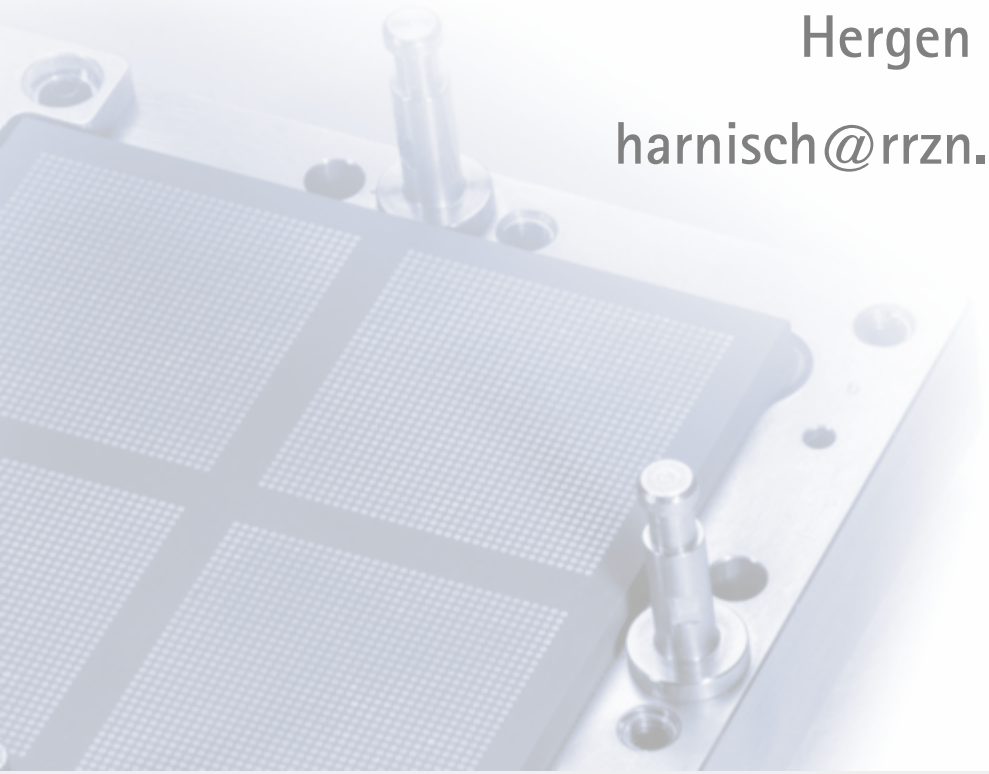
Bitlocker & TrueCrypt



Hergen Harnisch

harnisch@rrzn.uni-hannover.de

1 Gemeinsamkeiten

2 Bitlocker

3 TrueCrypt

R|R|Z|N

Motivation

Ziel Sicherung von vertraulichen, schützenswerten Daten gegen unbefugten Zugriff.

Geräte Lohnenswert und sinnvoll für mobile IT-Geräte:

- Notebooks
- USB-Sticks
- eigentlich auch PDAs, Mobiltelefone etc.

Verschlüsselung einzelner Dateien und Verzeichnisse (z.B. per EFS) nicht ausreichend, da temporäre oder Swap-Dateien Daten enthalten.

R|R|Z|N

Schlüssel oder Passwort

Sicherheit hängt entscheidend von Passwort oder Schlüsselverwaltung ab, Verschlüsselung selbst kaum angreifbar.

schwach	Schlüssel auf Platte, nur mit Passwort
vernünftig	Schlüssel mit Passphrase auf USB-Key
optimal	TPM mit PIN (nicht für mobile Datenträger), Smartcard

Recovery nicht vergessen!

Gefährdung	Verlust des Schlüssels, evt. Defekt TPM, Plattenumbau sinnlos
Maßnahme	Recovery-Passwort bzw. Kopie USB-Key hinterlegen, Backup

andere Produkte haben z.T. Key-Recovery per Challenge-Response für Telefon-Helpdesk (z.B. Ultimaco Safeguard Device Encrpytion)

Nachteile

- Imaging: Images sind kaum komprimierbar (hohe Entropie)
- System-Reparatur: Boot-CDs müssen Partitionsverschlüsselung kennen, z.B. auch Viren-Scan-CDs
- Fehler in Metadaten kann ganzes Volume zerstören
- Performance-Verlust heutzutage eher zweitrangig
  (demnächst auch bei Intel-CPUs AES in Hardware)
- zusätzliches Pre-Boot-Environment (Entschlüsselung vor OS-Boot)
- zusätzliche Schlüsselhardware / PIN- oder Passwort-Eingabe

Bitlocker

- Bestandteil von Windows-Vista/-7 Enterprise & -Ultimate, Windows-2008
- Integration in Active-Directory möglich, Gruppenrichtlinien-Support
- partitionsweise Verschlüsselung
- benötigt zusätzliche „Service"-Partiton für Windows-PE
- unterstützt TPM $\geq$ 1.2 als Key-Store, Recovery-Passwort auch mit TPM; kein Smartcard-Support, aber Key als Datei auf USB-Stick
- kein Challenge-Response-Key-Recovery
- unterstützt eigentlich nur das System-Volume;
  andere Volumes oder USB-Sticks und ausgelagerten Key-Dateien aber über Kommandozeilentool `manage-bde.wsf` möglich

TrueCrypt

- Sowohl ganze Partitionen als auch virtuelle Volumes in Dateien
- verfügbar für Windows $\geq$ 2000, Linux, MacOS-X
  unter Windows auch als Portable-App; Einbindung in Linux per FUSE
- dadurch Recovery-/Virenscan-Boot-CDs mit TrueCrypt-Support möglich
- für mobile Datenträger an verschiedenen Rechner einsetzbar
- keine TPM- oder SmartCard-Unterstützung in Pre-Boot,
  aber für Nicht-OS-Volumes über PKCS-11-Schnittstelle
- keine speziellen Recovery-Keys oder -Passwörter
- Abstreitbarkeit der Verschlüsselung

Links

- Bitlocker-Leitfaden (Kooperation Frauenhofer-Instituts & BSI):
  http://testlab.sit.fraunhofer.de/content/output/project_results/bitlocker/BitLocker-Leitfaden.pdf
  Stand Herbst 2007, enthält auch kurzen Vergleich mit EFS, TrueCrypt