dm-integrity

Übersicht

- LUKS
- Device mapper vs ZFS
- Bit rot
- Integritysetup
  - RAID
  - Boot

LUKS

Disclaimer

- Crypto!
  - Go watch https://www.youtube.com/watch?v=eMG3qjzOjvI

LUKS

- Diskverschlüsselung unter Linux
  - Sicher
  - Ausgereift
- Length-preserving
  - Wieso ist das wichtig?

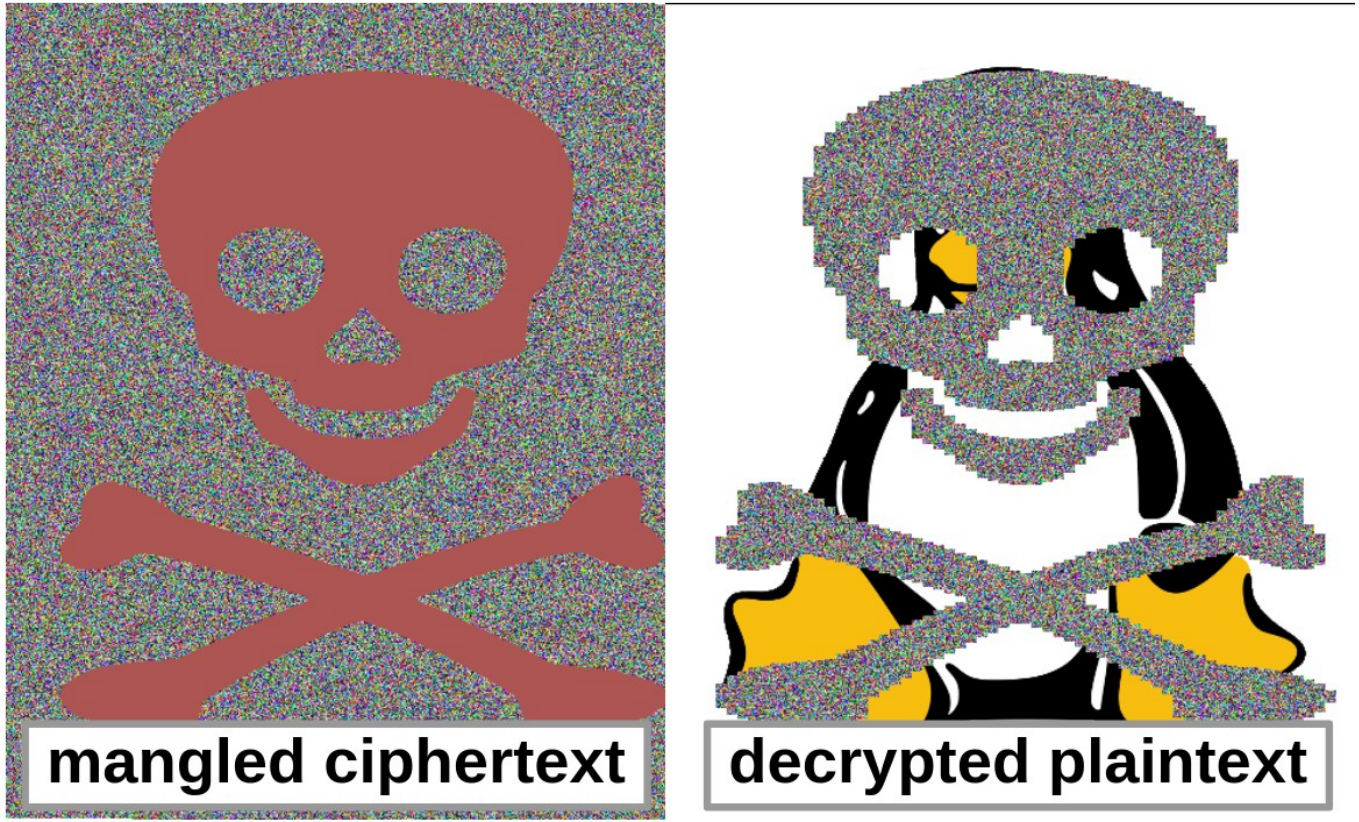
Authenticated encryption

- Inhalte sind “signiert”
  - Verifiziert trusted parties
  - Erkennt Manipulationen
  - Standard für Netzwerktraffic (HTTPS, SSH, …)
    - Wenn auch nicht immer gleich…

LUKS ist nicht authenticated

- Wieso ist das ein Problem?
  - Weniger schlimm als bei Netzwerkverkehr
  - Angriffe sind komplex
  - Trotzdem denkbar

Angriff auf LUKS



“Data integrity protection with cryptsetup toolswith cryptsetup tools” by Milan Brož, FOSDEM 2018

Verteidigung

- Authenticated encryption
  - Jeder block wird signiert
- Problem:
  - Signatur muss gespeichert werden
    - Nicht mehr length-preserving!
- LUKS kann das heute!

LUKS + dm-integrity

- LUKS berechnet Signatur
- Dm-integrity speichert die Signatur
  - Und auch die Daten
- Beim lesen prüft dm-integrity die Daten
- Cryptsetup regelt das alles!

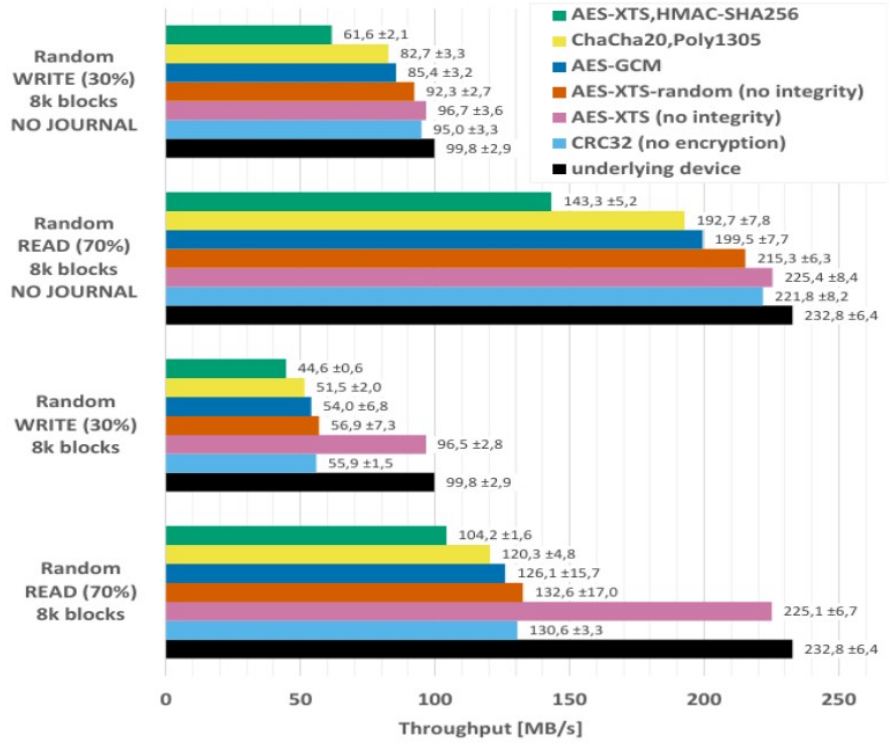
==> Demo

Probleme

- Nicht stabil!
- Langsam!
  - Berechnen
  - Journal

Benchmarks

- SSD, 30% writes / 70% reads (very inefficient case)



"Data integrity protection with cryptsetup toolswith cryptsetup tools" by Milan Brož, FOSDEM 2018

ZFS

ZFS

- 2005 vorgestellt
  - Von SUN Microsystems für Solaris
- Verändert die Storage-Branche
  - Keine RAID-Controller mehr
  - Flexibel
  - Viele Funktionen

ZFS on Linux

- Inkompatible Lizenz
- Technische Inkompatibilitäten
- Btrfs als native Alternative
  - Schwierige Entwicklung
    - Wenig Entwickler
    - Dateisystem sind schwierig
    - Alles neu
    - Die Branche verändert sich

Linux device mapper

- Teil des Linux Kernels
- Mappt Funktion auf Block devices
- Exponiert neues Block device
  - → stackable

Storage unter Linux

- Dm-raid
- LUKS / cryptsetup
- LVM

stratis

- Red-Hat Projekt
- Feature-parity mit ZFS
- Komplett Device mapper basiert

Zurück zum Thema

- Welche Rolle spielt dm-integrity?
  - Stand-alone

Bit rot

Bit rot

- Data degredation / data decay
- Passiert auf allen Speichermedien von selbst
- Wird vom Speichermedium nicht bemerkt
- Tratizionelle Dateisysteme schüzen nicht davor!

Dm-integrity stand-alone

- Crc32
- Meldet Fehler an darüber liegendes Layer
- Schützt so vor Bit rot

integritysetup

Einsatz ohne RAID

- Im PC / auf dem Laptop
- Vielleicht doch mit LUKS?
- Backups!

RAID

- dm-integrity unterhalb vom RAID!
- Was wenn LUKS?

Boot

- Nicht alle initrds können integrity
  - Dracut macht massiv Probleme
- Hier hilft die Integration mit LUKS

LVM

- Vielleicht doch lieber LVM?
- Oder gar Stratis?

Ende / Fragen?