LUKS-Verschlüsselung in der Praxis

Johannes Schirm

Vortrag auf der Tübix 2017,
30 Minuten

Grund des Vortrags

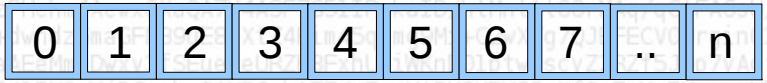
- ➜ Student der Medien- und Kommunikationsinformatik in Reutlingen
- ➜ Bachelorarbeit und Anstellung am Max-Planck-Institut für biologische Kybernetik in Tübingen im Bereich virtueller Realität
- ➜ Seit Anfang 2016 besonders interessiert an freier Software

- ➜ Sehr interessantes Thema: LUKS-Verschlüsselung richtig einsetzen
- ➜ Der Vortrag soll die grundsätzliche Funktionsweise vermitteln
- ➜ Zusätzlich sollen Wege zur Optimierung und Vereinfachung gezeigt werden
- ➜ Kurze Einführung zur Theorie, dann Echtzeitdemonstration!

LUKS

Blockgeräte

- ➜ Können von der Benutzerebene aus mithilfe von virtuellen Gerätedateien unter */dev/* angesprochen werden
- ➜ Festplatten, USB-Sticks und ähnliche Geräte werden automatisch von udev mit dynamischem Namen bereitgestellt
- ➜ Blockspeicher wird in Bytes angesprochen und stellt einen einzigen Datenstrom dar:



Verschlüsselung mit Mapper

Benutzer

/dev/sdb

0	1	2	3	4	5	6	7	..	n

Verschlüsselung mit Mapper

Benutzer

/dev/mapper/geheim

/dev/sdb

dm_crypt

0	1	2	3	4	5	6	7	..	n

?	?	?	?	?	?	?	?	..	?

Sichere Verschlüsselung?

AES ist ein bekanntes Verfahren

Die Möglichkeiten für einen 128-Bit Schlüssel können errechnet werden mit:

- ➜ 10.000.000 Computern
- ➜ CPUs, die jeweils 10.000.000 Schlüssel pro Sekunde testen können
- ➜ Mehrere Tausend Mal die Zeit, die das Universum schon existiert

...zu einfach? Gut, dann eben 256-Bit.

Das Kernelmodul „dm_crypt“

- ➜ Seit Kernel 2.6 verfügbar
- ➜ Teil der Device-Mapper-Infrastruktur
- ➜ Das Modul selbst muss jedoch gesondert geladen werden
- ➜ Es sind alle dem System bekannte Verschlüsselungsverfahren nutzbar (/proc/crypto)
- ➜ „*cryptsetup*“ ist ein Paket zur Steuerung und Verwaltung des Moduls

Linux Unified Key Setup

- ➜ Zusätzlicher Header für rohes dm_crypt
- ➜ Verwaltung von bis zu acht Passwörtern
- ➜ Speicherung der Verfahren in Metadaten

- ➜ Vereinfacht schnellen Zugriff auf Daten
- ➜ Verlust der Abstreitbarkeit wegen Klartextheader
- ➜ Zusätzlicher Platzverbrauch (2 MiB)

Echtzeitdemo!

Die Materialien dazu finden Sie auf:
https://www.johannes-schirm.de/tuebix2017/