Linux
-
Verschlüsselte Dateisysteme mit dm-crypt

Übersicht

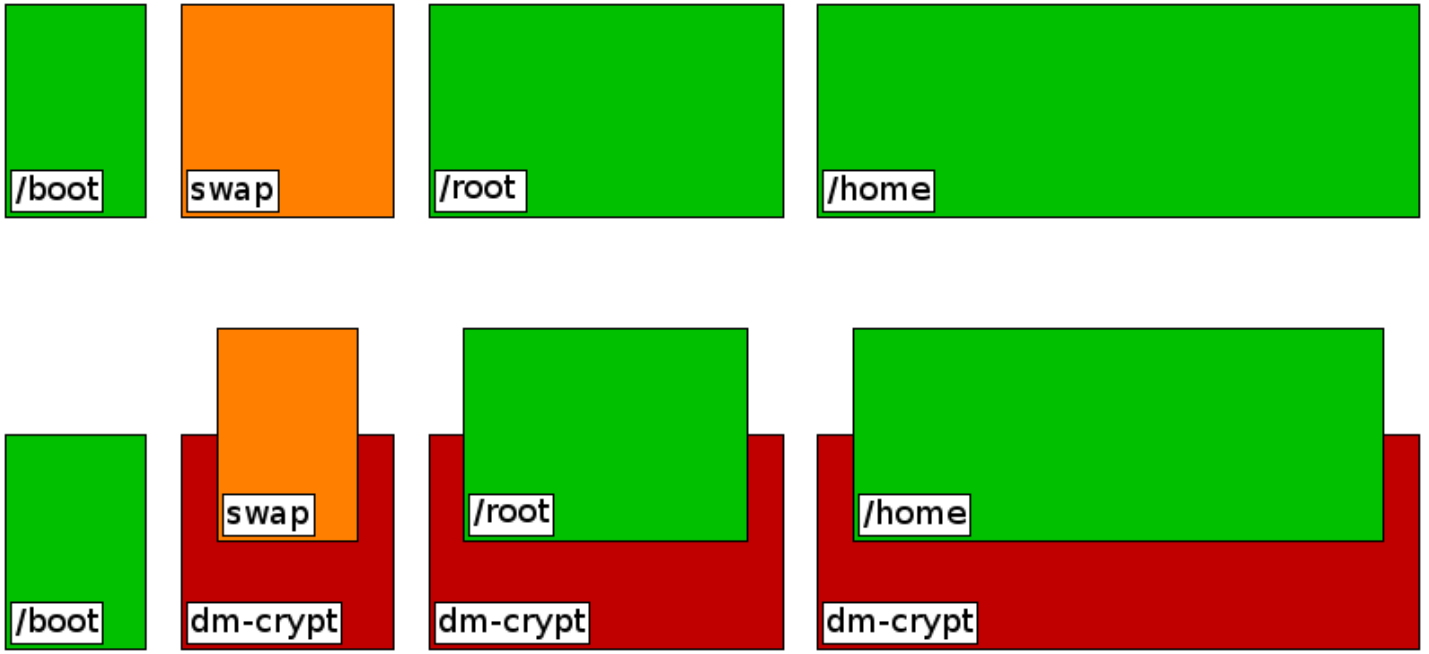
- Was verschlüsseln?
- dm-crypt
  - Kernelsupport
  - Tools im Userspace
- Besonderheiten im Bootprozess
- Kombination mit lvm
- Praxisübung

Was verschlüsseln?

- Was sollte verschlüsselt werden?
  - Daten
  - root-Dateisystem?
  - Swap?
  - boot-Dateisystem?

dm-crypt

- „Schicht“ zwischen FS und Partition



Kernelsupport

```
.config - Linux Kernel v2.6.25-rc8 Configuration
                          Device Drivers
  Arrow keys navigate the menu.  <Enter> selects submenus --->.
  Highlighted letters are hotkeys.  Pressing <Y> includes, <N> excludes,
  <M> modularizes features.  Press <Esc><Esc> to exit, <?> for Help, </>
  for Search.  Legend: [*] built-in  [ ] excluded  <M> module  < >
      -(-)
      < > ATA/ATAPI/MFM/RLL support  --->
          SCSI device support  --->
      <*> Serial ATA (prod) and Parallel ATA (experimental) drivers  --
      [*] Multiple devices driver support (RAID and LVM)  --->
      [ ] Fusion MPT device support  --->
          IEEE 1394 (FireWire) support  --->
      < > I2O device support  --->
      [ ] Macintosh device drivers  --->
      [*] Network device support  --->
      < > ISDN support  --->
      .(+)
                <Select>    < Exit >    < Help >
```

Kernelsupport

```
.config - Linux Kernel v2.6.25-rc8 Configuration
 Multiple devices driver support (RAID and LVM)
 Arrow keys navigate the menu.  <Enter> selects submenus --->.
 Highlighted letters are hotkeys.  Pressing <Y> includes, <N> excludes,
 <M> modularizes features.  Press <Esc><Esc> to exit, <?> for Help, </>
 for Search.  Legend: [*] built-in  [ ] excluded  <M> module  < >

    --- Multiple devices driver support (RAID and LVM)
    < >   RAID support
    <*>   Device mapper support
    [ ]     Device mapper debugging support
    <*>     Crypt target support
    < >     Snapshot target
    < >     Mirror target
    < >     Zero target
    < >     Multipath target
    < >     I/O delaying target (EXPERIMENTAL)
    .(+)

                <Select>    < Exit >    < Help >
```

Tools im Userspace

- cryptsetup-luks
  - Zum Initialisieren der Verschlüsselung
  - Mappen und Freigeben der Devices

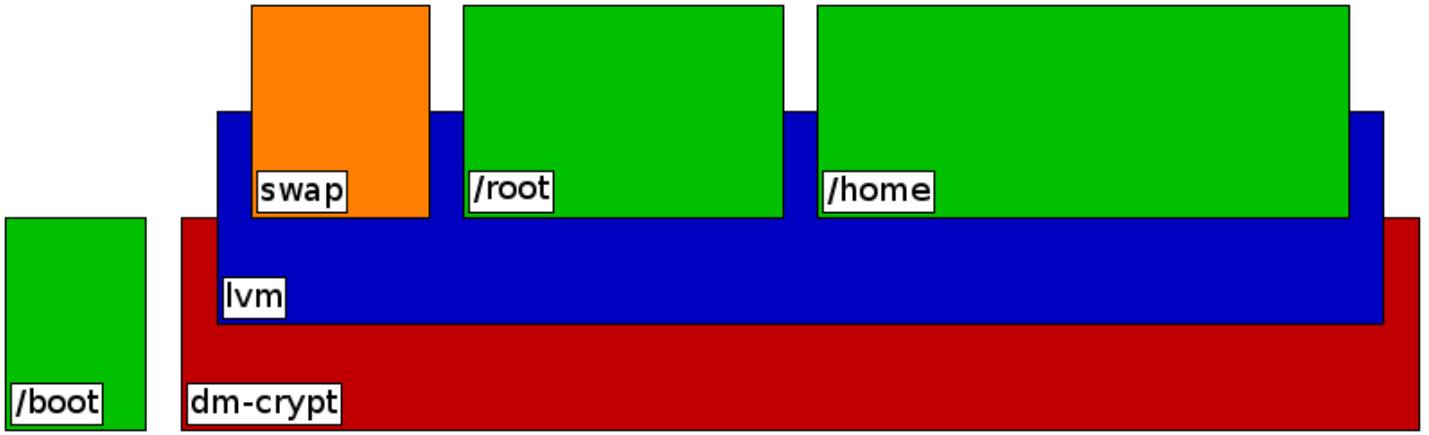
Besonderheiten im Bootprozess

- Initial Ramdisk (initrd)

Die Partition muss entschlüsselt werden bevor das root-Dateisystem gemountet und das System gestartet werden kann.

LVM

- Kombination mit LVM
  - Nur eine verschlüsselte Partition



Praxisübung

- Umstellung eines bestehenden Gentoo-Systems