coreboot

lynxis

10. November 2015

Was ist ein Bootloader?

- Erstes Programm
- Initialisiert Hardware
- läd das OS

Was ist das BIOS?

- Basic Input Output System
- Initialisiert die Hardware damit das OS geladen werden kann
- z.B. Festplattenerkennung, PCI, Grafik, Tastatur, ..
- eine Library von Funktionen

Was ist das coreboot?

- ein Bootloader
- initialisiert die Hardware
- simpler Code
- geschrieben in C, wenig ASM
- unterstützt ARM ARM64 x86 AMD64 MIPSel RISC-V

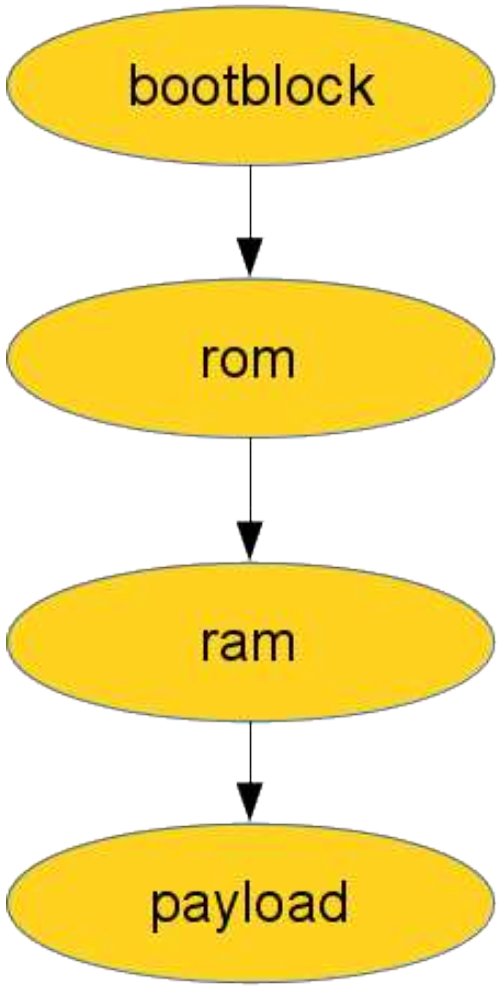
Wieso coreboot?

- open source
- erweiterbar
- reproduzierbar
- schnell
- sicher

corebooted devices

- mehr als 200 devices
- Thinkpads
- Chromebooks
- industrie boards APU
- Satelliten
- Cluster

Aufbau von coreboot



Setup rom acces

Setup ram

Device drivers

Payloads

- SeaBIOS
- GRUB2
- FILO
- OpenBIOS
- ELF binary z.B. Linux + initramfs

The dark side

- x86 SMM/SMI System Management Mode
- Intel Boot Guard
- Intel ME
- ARM Trust Zone
- AMD Platform Security Processor

Wie fange ich an?

- Unterstütztem Board
- z.B. Thinkpad
- ein Flasher z.B. Raspi oder BBB
- full backup
- autoboot oder libreboot