Offene Boot Firmware leicht gemacht

Autoboot

Klemens Nanni
contact@autoboot.org
GPG: B375A7EE

IRC – #autoboot @freenode

Klemens Nanni

- **Nutzer seit Juni '15, kein Entwickler**
  - Student 1. Semester Informatik
- **Arbeitsmaschine ist Testmaschine (X201)**
- **Autoboot aus eigenen Problemen mit Coreboot entstanden**

Übersicht

- **Coreboot**
  - Funktionsweise
  - Payloads
  - Unterstützte Hardware
  - Bugs
- **“Blobs”**
  - Intel ME (AMT)
  - Microcode
  - VGA BIOS

Übersicht

- **Libreboot**
  - 100% frei
  - getestet
  - benutzerfreundlich
  - vorkonfiguriert
  - wenig Hardware unterstützt
- **Autoboot**
  - “Blobs” nur soweit nötig
  - für Einsteiger leicht gemacht
  - unterstützt jedes “Coreboot-Board”
- **Installation / Hardware**

Coreboot: Funktionsweise

1) Bootblock

1) Flash access
2) ROM lookup

2) ROM

1) Memory init
2) Early chipset init

3) RAM

1) Device enumeration
2) Resource assignment
3) ACPI table creation
4) SMM handle

4) Payload

Coreboot: Payloads

- **GRUB2**
  - Linux, *BSD
  - Ext4, LVM, RAID, ZFS, BTRFS, ...
  - (plain) dm-crypt / LUKS
  - cbmemc, coreboot framebuffer kompatibel
- **SeaBIOS**
  - Linux, *BSD, Windows
  - BIOS calls
- **TianoCore (UEFI)**
- **Linux Kernel**

Coreboot: Hardware (Libreboot)

- **230 Boards, u.a:**
  - ThinkPads
    - **X/T60(s|t)**
    - **X200(s), R/T4/500**
    - X201(s|t)
    - X220(s|t), T420s, T520
    - X230, T530
  - AMD Opteron (Server, 2x CPU)
    - **KFSN4-DRE**
    - **KGPE-D16**
  - Google Chromebooks
    - **C201**
    - Pavilion 14
    - S 550
    - C7, Pixel
    - C720, Pixel 2, 14
  - MacBook
    - **1,1**
    - **2,1**
    - Air 4.2

Coreboot: Bugs

- **fehlende ACPI Codes**

  → teilweise kein Hotplug

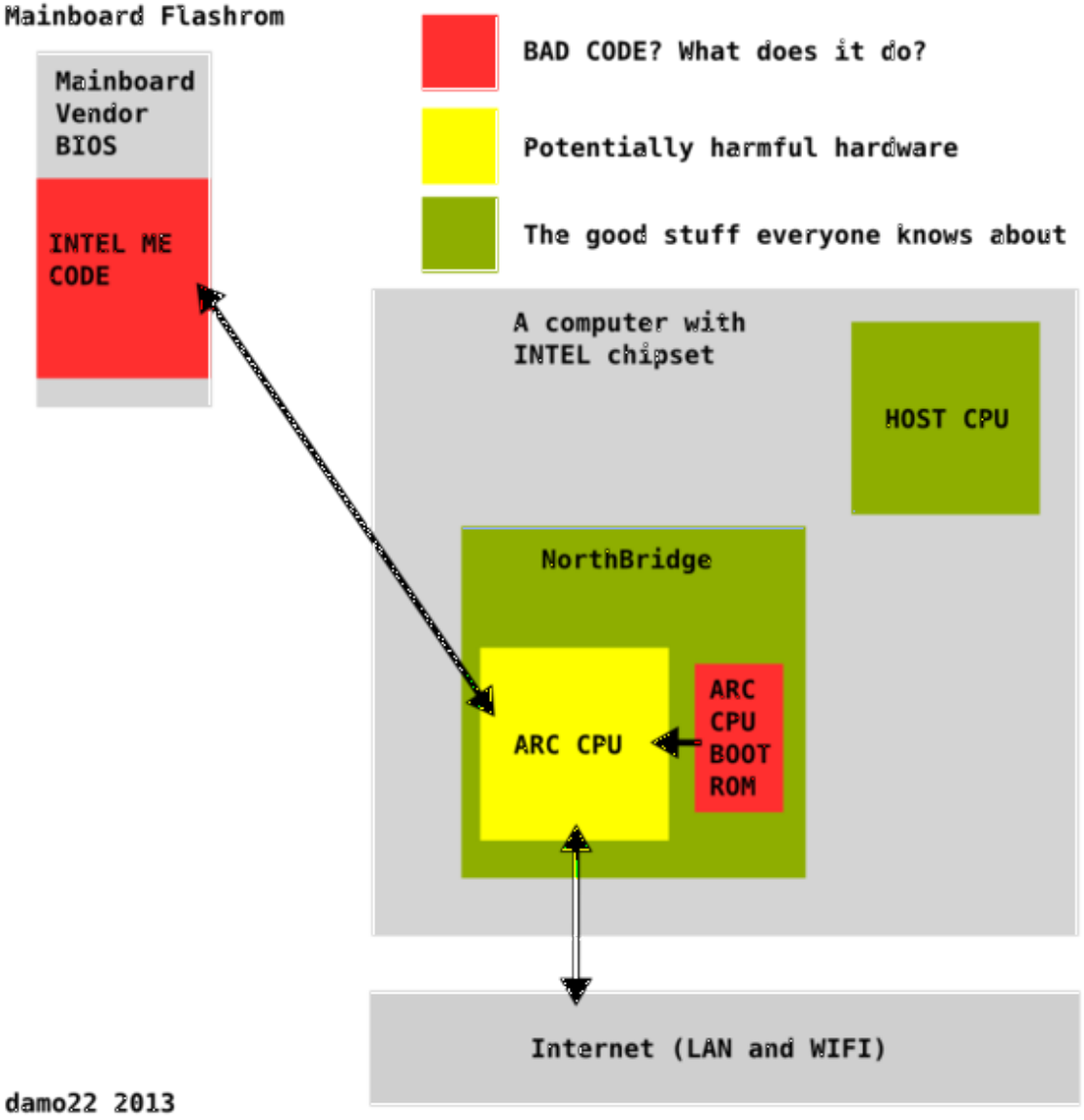
- **Board-spezifisch**
  - X201:
    - “resume from suspend” → Race Condition
    - PCI-E u. USB fehlerhaft (ab 456f495d)
  - T520: diskrete GPU nicht unterstützt
  - X22/30: kein MRC Cache → längere Bootzeit

Blobs: Intel Management Engine

- **seit Juni '06 (965 Express Chipset) in allen Systemen**
- **eigener Prozessor, eigener Cache**
- **interner Bus**
- **signiert, komprimiert**
- **läuft in S3, komplett “out-of-band”**
- **Direct Memory Access (DMA)**

- **modular**
  - ThreadX (RTOS)
  - Dynamic Application Loader (DAL, Java VM)
    - kann ext. Module von HDD laden
  - Active Management Technology (AMT)
  - Trusted Platform Module (TPM)
  - Boot Guard
  - Protected Audio and Video Path (PAVP)/Intel Insider (DRM)
- **Netzwerkzugriff**
  - eigene MAC

Intel Management Engine



Active Management Technology

Intel® Active Management Technology

Computer: PVR

System Status
Hardware Information
- System
- Processor
- Memory
- Disk

Event Log
Remote Control
Network Settings
User Accounts
Update Firmware

Memory Information

Module 1

Manufacturer	0xCE00000000000000
Serial number	0x030EDD23
Size	512 MB
Speed	667 MHz
Form factor	DIMM
Type	DDR2
Type detail	Synchronous
Asset tag	Unknown
Part number	0x4D33203738543635353343 5A332D43453720

Module 2

Manufacturer	0xCE00000000000000
Serial number	0x50053A79
Size	512 MB
Speed	667 MHz
Form factor	DIMM
Type	DDR2
Type detail	Synchronous
Asset tag	Unknown
Part number	0x4D33203738543634353346473 02D43453620

Blobs: Microcode

- Bei fast allen Systemen optional
- Behebt Fehler der CPU
- Voraussetzung für hardwarebeschleunigte Virtualisierung (Intel Vt-x)
- signiert u. komprimiert
- kann potentiell Schadcode enthalten

Libreboot

- **“deblobbed” Coreboot Distribution**
- **stabil → stets ausgewählte, getestete Commits als Basis für Release**
- **automatisiertes Build-System (Coreboot u. Payload)**
  - Download
  - Build
  - Flash / Update
- **fertig gebaute, signierte ROM Images**

Libreboot

- **GRUB2 als Standardpayload**
  - unterstützt Keyfiles, externe LUKS Header
  - bootet von
    - externen Medien wie USB und CD/DVD
    - nahezu jedem Festplattensetup
- **lädt persönliche Konfiguration**
  - Eigene Menüeintrage unter /boot/grub/grub.cfg wie gewohnt → kein Flashzugriff bei Kernel Update nötig
- **Kein Support für Intel Systeme ab 2008 (Management Engine)**

  → Fokus auf AMD

Autoboot

- **“reblobbed” Libreboot**

  → benutzerfreundliches System mit Unterstützung for jedes Coreboot Board

- **en pair mit Libreboot, möglichst keine Divergenz beim Build System**
- **bietet sicheren Einstieg für Neulinge**
- **Ziele:**
  - freie Boot Firmware für jedermann zugänglich

    → Gewinnung neuer, potentieller Entwickler

Autoboot: Installation

- **Git clone http://git.autoboot.org/autoboot.git**
- **./download coreboot grub**
- ***(./build config corebootmodify x201_8mb)***
- **./build module coreboot**
- **./build module grub**
- **./build roms withgrub x201_8mb**

Hardware

- **schreibgeschützte Chips**

  → erstmalige Installtion durch externen Flasher (BeagleBone, Rasberry Pi, BusPirate, etc.)

- **Updates bequem aus Userspace**
  - ./flash upate <rom image>