Introducing Open Source Firmware

Daniel Maslowski

Chaosdorf

Warning: Politics involved ⚠

Agenda

- Introduction
- Motivation
- Projects
- Open Source Firmware Conference
- Future Work

Introduction

Firmware is everywhere

Laptops

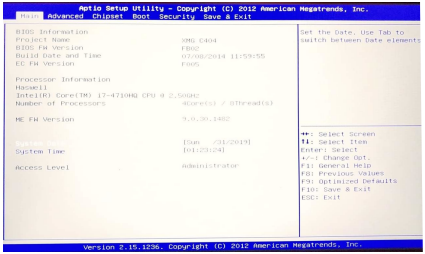
- BIOS/UEFI (host CPU)
- ME/PSP (coprocessor)
- Gigabit Ethernet (GbE)
- Embedded Controller (EC)

Servers

- Baseboard Management Controller (BMC)

Embedded devices

- System-on-Chip



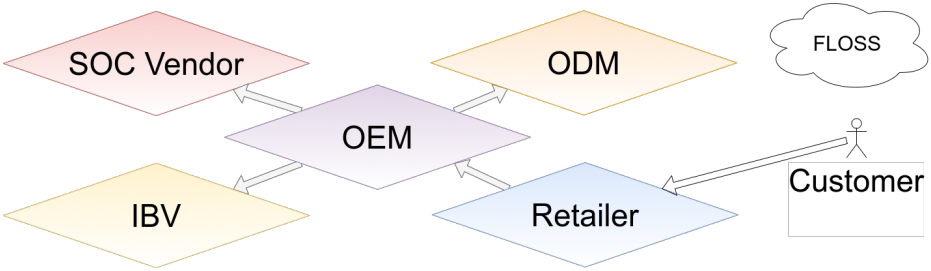
Chaosdorf

What firmware does

- hardware initialization
  - specific to SoC, mainboard, some peripherals
- user interaction
  - UI, settings, boot selection
- OS interfacing
  - updates, feedback, power management

Motivation

Hardware supply chain



Motivations to keep code proprietary

- intellectual property
- security by obscurity
- hiding quality issues

Dexter’s Law

Only proprietary software vendors want proprietary software.

Vendor perspective

> *Intel is working towards releasing as much source code as possible going forward. A binary component is still the best way to encapsulate the complex solution that developers may not necessarily need to bother about as long as the binary component does its job right.*

source: FSP whitepaper

Security

Firmware, Kernel and the Rings on x86

- -3: ME
- -2: SMM / UEFI kernel
- -1: hypervisor
- 0: OS kernel
- 3: userspace

Jessie Frazelle on Open Source Firmware

https://blog.jessfraz.com/post/why-open-source-firmware-is-important-for-security/

Fear

Introduction

- UEFI firmware is now widely deployed and has become a target for hackers and security analysts/researchers
- Poor implementations affect the credibility of the UEFI “brand” and market perception of all implementations
- As with all software implementations, there are going to be faults - (Phoenix is not perfect, even if we want to be)
- Phoenix would like to share some of our best practices in the interest of raising the quality and security of all UEFI implementations

source: Phoenix

Issues

- consumers get very few updates
- some bugs are never fixed and require workarounds

V

viliuzk

Oct 10, 2018

13

0

10

0

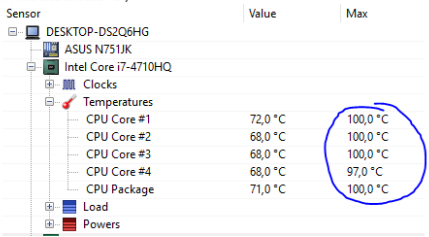
Oct 16, 2018 #1

Hi guys,

I hope you can help me with my problem. Recently bought used laptop, Asus N751JK.
Played CS:GO and started lagging (medium graphics). Checked with hardware monitor, CPU temp goes up to 100°C which as far as I understand is dangerous temp.

Reapplied thermal paste (Grizzly Aeronaut), opened bottom HDD case and put laptop on fan cooler, but it did not help. It still goes up to 100°C. (I attach image).
Room temperature is 21°C .

What else should I try ?

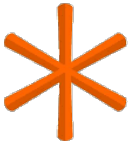


Chaosdorf

Projects

(not only) x86

coreboot



tianocore

LinuxBoot

TianoCore

- reference implementation from Intel + community
- EDK II/UDK (EFI Development Kit II aka UEFI Development Kit)
- used by Independent BIOS Vendors (IBVs)
  - AMI: Aptio
  - Phoenix: SCT (SecureCore Technology™)
  - Insyde: InsydeH2O®
- OVMF (Open Virtual Machine Firmware)
  - made for QEMU
  - debuggable through GDB using a bridge
- potential for secure boot on Linux
  - draft from the Fedora Project
  - ideas from James Bottomley

coreboot

- supports many boards and multiple architectures
- initializes hardware, then hands over to a payload
  - default: SeaBIOS
  - can directly boot a Linux kernel
- on Chromebooks by default and few other consumer devices
- full or almost full support for older Lenovo ThinkPads and HP EliteBooks
- more laptops are being added: Clevo, Razer, Gigabyte
- requires proprietary binaries for current x86 architectures
  - Intel: FSP (Firmware Support Package)
  - AMD: AGESA (AMD Generic Encapsulated Software Architecture)

Let’s see a demo! 💻

LinuxBoot

Let Linux do it

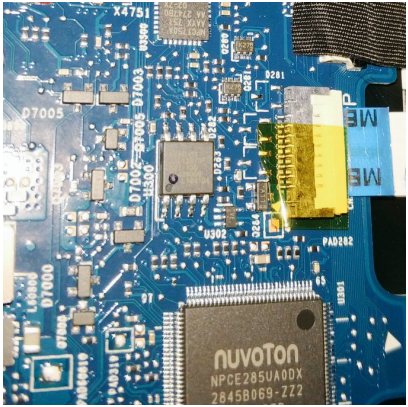
- Linux kernel provides device drivers and networking
- initramfs with utilities, bootloader, whatever you wish
- approach rather than implementation
- can run on top of
  - coreboot: as payload
  - U-Boot
  - vendor UEFI firmware: remove DXEs, build Linux with EFI support

Implementations

- u-root
  - written in Go
  - utilities like busybox
  - offers bootloaders
- Heads
  - authenticated / measured boot

Embedded Controller

- Chromium OS EC
- System76 EC



Baseboard Management Controller

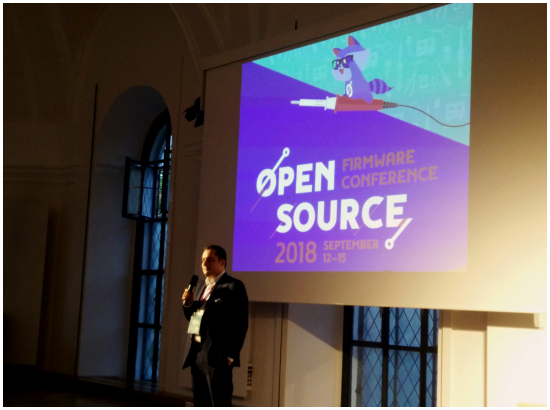
- EDK2 Redfish POC
- OpenBMC
- u-bmc

Project	OpenBMC	u-bmc
Languages	C++, Python	Go
Tooling	Yocto, OpenEmbedded	u-root
Kernel	OpenBMC Linux fork	OpenBMC Linux fork
Init	systemd	
IPC	D-Bus	
RPC	IPMI, REST	gRPC
Metrics		OpenMetrics

Open Source Firmware Conference

Chaosdorf

OSFC 2018 in Erlangen, Germany



- almost 200 participants
- 2 days of talks
  - 2 tracks (main + security)
- 2 days of workshops + hackathon

Chaosdorf

OSFC 2019 in Silicon Valley, California

- more than 250 participants
- 2 days of talks
  - 3 tracks (general, security, BMC)
- 2 days of lightning talks + hackathon

Chaosdorf

Future Work

Developers wanted

- TUXEDO Computers is hiring coreboot developers

TUXEDO COMPUTERS

Software Developers for Coreboot BIOS (m/f/d)

We're hiring:

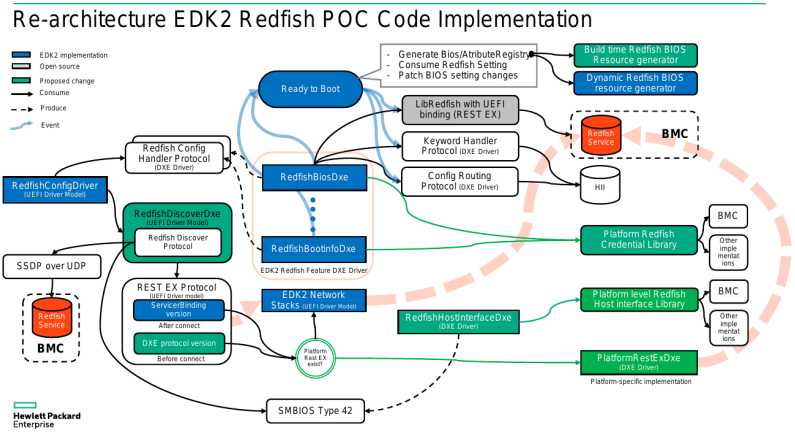
To increase our team in Königsbrunn (Germany) we are looking for **Software Developers for Coreboot BIOS (m/f/d)** in a permanent position. **German language skills required - level B2 or higher!**

Are you a software developer with heart and soul?
C is for you not only a letter and kernel you find not only in avocados totally exciting?
If you also know how to solve a ticket for the dbus and have both feet firmly on the socket, you've come to the right place!

oreboot

- introduced at OSFC 2019
- downstream fork of coreboot
- implemented in Rust
- policy: no proprietary blobs, *absolutely*
- first targets
  - RISC-V (HiFive Unleashed)
  - QEMU (ARM)

Redfish POC rearchitecture



Chaosdorf

UEFI Forum public webinar

How to create a secure development lifecycle for firmware*

- Wednesday, October 23 at 9:00 am PT
- Moderator: Brian Richardson (TBD)
- Panelists:
  - Dick Wilkins, Phoenix
  - Tim Lewis, Insyde Software
  - Eric Johnson, AMI

https://uefi.org/node/4004

Chaosdorf

Questions? 

Thanks!