Open Source Firmware

Daniel Maslowski

Disclaimer: No shaming, no mocking!

Agenda

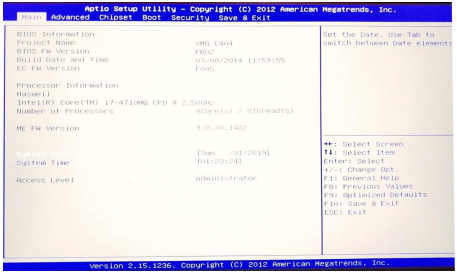
- Introduction
- Motivation
- Inspecting Hardware
- Building Firmware
- User/Developer Experience

Introduction

Firmware is everywhere

Embedded devices

- SoC



Laptops

- BIOS/UEFI (host CPU)
- ME (coprocessor)
- GbE
- EC

What Firmware Does

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

Open Source Firmware Origins

1994

- IEEE 1275-1994
- Open Firmware
- OpenBIOS

1999

- Das U-Boot
- LinuxBIOS, later renamed to coreboot

2004

- TianoCore

Motivation

Vendor Firmware

Vendor firmware may have issues, but isn't fixed for various reasons.

https://lists.freebsd.org/pipermail/freebsd-acpi/2006-February/002571.html

How can I fix these problems of the asl of my computer?

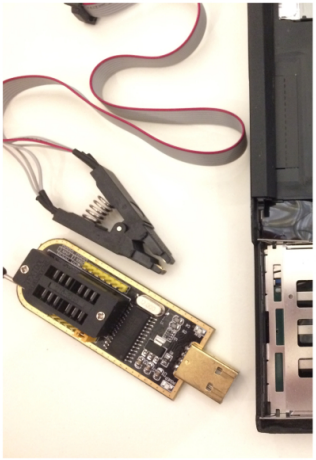
Moore, Robert robert.moore at intel.com
Wed Feb 15 14:39:53 PST 2006

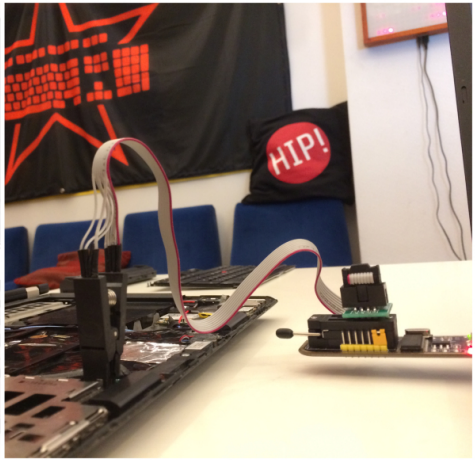
- Previous message: kern/80815: ACPI(pci_link) problem in 5.4-STABLE: TIMEOUT - WRITE_DMA retrying
- Next message: How can I fix these problems of the asl of my computer?
- **Messages sorted by:** [date] [thread] [subject] [author]

```
ze2205au.asl  2243:                         Return (UPRS)
Error    1022 -                 Object does not exist ^  (UPRS)

ze2205au.asl  2253:                         Store (UPRS, Local0)
Error    1022 -                 Object does not exist ^  (UPRS)

ze2205au.asl  4138:             Name (_WDG, Buffer (0x50)
Warning  2033 -    Unknown reserved name ^  (_WDG)

ze2205au.asl  4699:             Method (_WED, 1, NotSerialized)
Warning  2033 -      Unknown reserved name ^  (_WED)


1) Add "External (UPRS)" after the definition block is opened:

DefinitionBlock ("DSDT.aml", "DSDT", 1, "HP    ", "3091    ", 537137673)
{
    External (UPRS)

2) Ignore the warnings. Your BIOS writers did not read the ACPI spec or
became blind sometime in the middle of it, highly probable. :-)
```

Recovery

Updates can brick an existing system, so recovery options should be known.



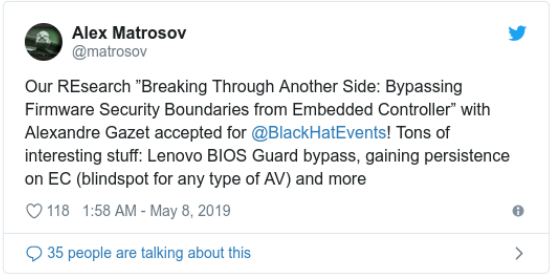


Malware

Malware can be hidden in firmware, so it has to be auditable.

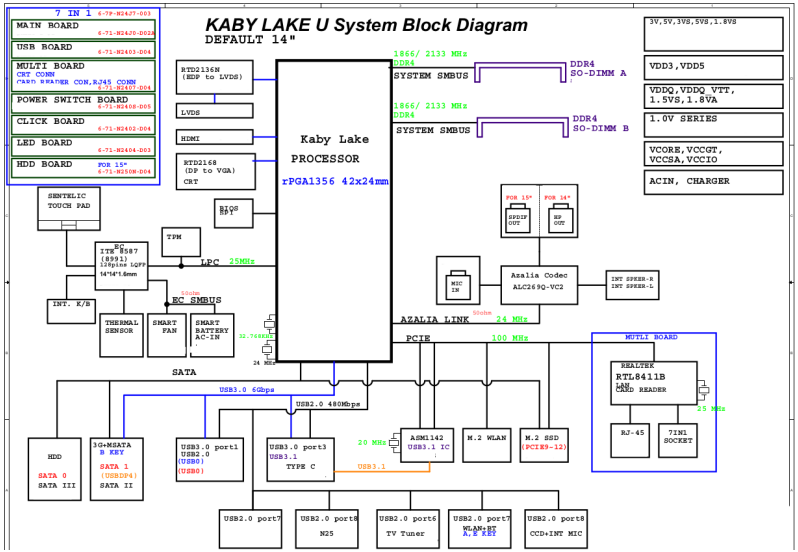
Breaking Through Another Side: Bypassing Firmware Security Boundaries from Embedded Controller

MAY 8, 2019 - HUCKTECH

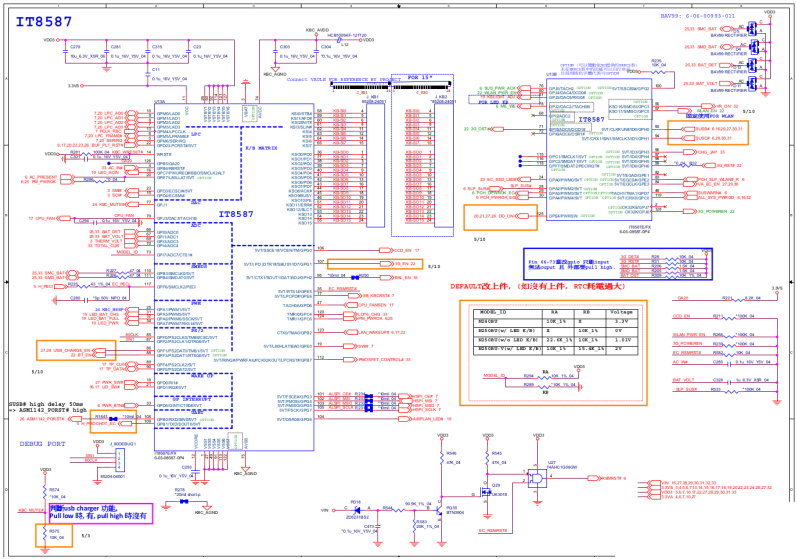


Hardware Inspection

System Block Diagram



Embedded Controller Schematic



Hardware Inspection Software Utilities

- igt-gpu-tools
- i2c-tools
- dmesg
- lspci
- acpidump (part of iasl, `util/acpi/acpidump-all` script in coreboot)
- dmidecode
- lstopo (part of hwloc) to list PCI device topology

from coreboot:

- autoport (-make_logs uses tools below + lspci, acpidump, dmidecode)
- ectool
- inteltool
- superiotool

Building Firmware

Build Process

- toolchain for target architecture (x86, ARM, …)
- firmware source code ;)

```
$ EDK_TOOLS_PATH=`pwd`/../BaseTools ./build.sh
Initializing workspace

...

FV Space Information
SECFV [10%Full] 212992 total, 22192 used, 190800 free
PEIFV [20%Full] 917504 total, 189992 used, 727512 free
DXEFV [36%Full] 11534336 total, 4216648 used, 7317688 free
FVMAIN_COMPACT [35%Full] 3440640 total, 1222080 used, 2218560 free

- Done -
```

Recent Development

Developers Wanted

- TUXEDO Computers is hiring a coreboot developer

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!

Thunderbolt

- System76 makes open source Thunderbolt controller firmware
  - USB4 based on Thunderbolt

OPEN FIRMWARE

System76 has been granted a Thunderbolt license, meaning that we can now integrate Thunderbolt compatibility into our open firmware. This is a huge development in the open firmware project, as we can now achieve full functionality of Thunderbolt in our machines once the firmware is implemented.

Privacy

- Qubes OS certified Insurgo Privacy Beast X230

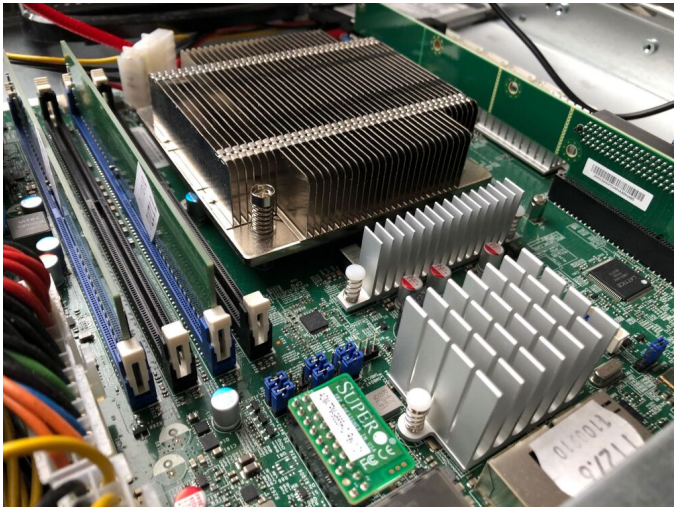
coreboot

- coreboot 4.10 has been released

Release	Date	Source	Source GPG	Blobs	Blobs GPG	Release Notes
coreboot 4.0	8. Feb 2010	⬇	⬇			
coreboot 4.1	13. July 2015	⬇	⬇	⬇	⬇	⬇
coreboot 4.2	30. October 2015	⬇	⬇	⬇	⬇	⬇
coreboot 4.3	29. January 2016	⬇	⬇	⬇	⬇	⬇
coreboot 4.4	01. May 2016	⬇	⬇	⬇	⬇	⬇
coreboot 4.5	18. October 2016	⬇	⬇	⬇	⬇	⬇
coreboot 4.6	30. April 2017	⬇	⬇	⬇	⬇	⬇
coreboot 4.7	14. January 2018	⬇	⬇	⬇	⬇	⬇
coreboot 4.8.1	16. May 2018	⬇	⬇	⬇	⬇	⬇
coreboot 4.9	20. December 2018	⬇	⬇	⬇	⬇	⬇
coreboot 4.10	22. July 2019	⬇	⬇	⬇	⬇	⬇

Servers

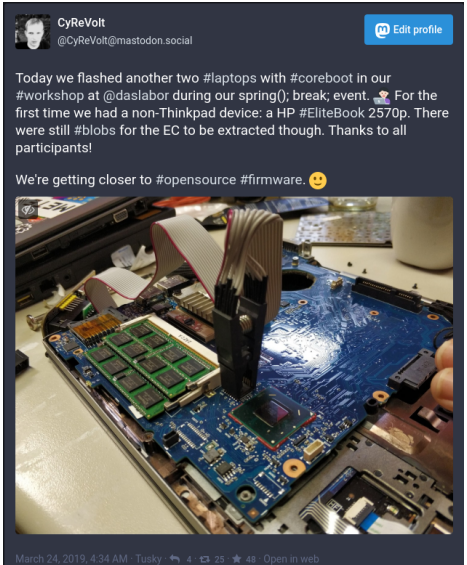
- 9elements Cyber Security ported coreboot to modern server board



User/Developer Experience

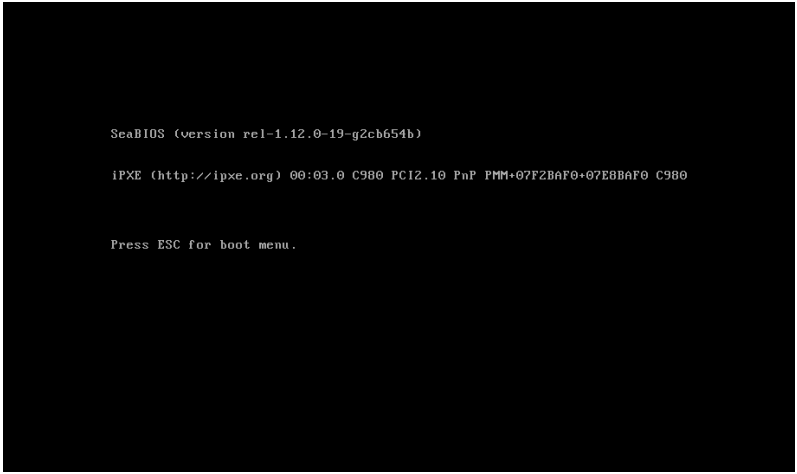
Prebuilt Binaries

- easy peasy: download, flash and run



Emulation in QEMU

- easy peasy: download, build and run



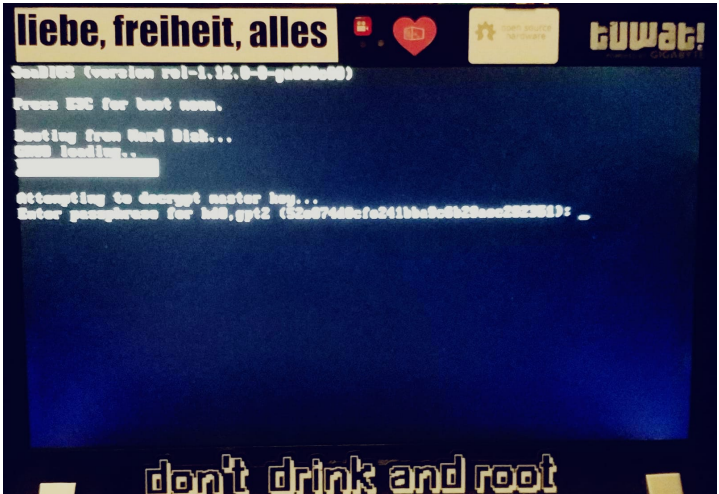
Supported Devices

- easy peasy: download, build, flash and run

```
Name                           Offset     Type           Size   Comp
cbfs master header             0x0        cbfs header      32 none
fallback/romstage              0x80       stage         62708 none
cpu_microcode_blob.bin         0xf600     microcode    122880 none
fallback/ramstage              0x2d680    stage         76715 none
vgaroms/seavgabios.bin         0x40280    raw           28160 none
config                         0x47100    raw             183 none
revision                       0x47200    raw             579 none
cmos_layout.bin                0x47480    cmos_layout    1804 none
fallback/dsdt.aml              0x47c00    raw           14078 none
fallback/payload               0x4b380    simple elf    68150 none
payload_config                 0x5be00    raw            1682 none
payload_revision               0x5c500    raw             273 none
etc/ps2-keyboard-spinup        0x5c680    raw               8 none
(empty)                        0x5c6c0    null        1716952 none
bootblock                      0x1ff9c0   bootblock       976 none
    HOSTCC     cbfstool/ifwitool.o
    HOSTCC     cbfstool/ifwitool (link)

Built lenovo/t400 (ThinkPad T400)
```

Porting

- a lot of time, knowledge and effort required
- can be frustrating because of “intellectual property”
- luck and fortune help, and of course the coreboot IRC channel :)



Announcement

Open Source Firmware Conference 2019

- San Francisco
- https://osfc.io
- tracks: general, security, BMC

Thanks! :)