Status of OpenPOWER support in coreboot

FOSDEM 2021

Michał Żygowski

3MDEB

whoami?

Michał Żygowski

Firmware Engineer

- @_miczyg_
- michal.zygowski@3mdeb.com
- linkedin.com/in/miczyg
- facebook.com/miczyg1395

- Braswell SoC, PC Engines and Protectli maintainer in coreboot
- interested in:
  - advanced hardware and firmware features
  - coreboot
  - security solutions

Agenda

- Who is involved?
- Why coreboot?
- Use cases
- Development roadmap
- Current status
- Future plans
- Dasharo
- Dasharo Trustworthy Computing
- How to help/contribute?
- Demo
- Q&A

Why coreboot?

Initialize the necessary hardware as fast as possible and boot to Linux

This is the goal of both OpenPOWER firmware and coreboot. So why not use it? coreboot always was a good replacement or alternative for the platform firmware.

Who uses coreboot?

- Google (Chromebooks) https://chromium.googlesource.com/chromiumos/third_party/coreboot/
- Siemens (industrial devices)
- Tesla Motors https://github.com/teslamotors/coreboot
- Supermicro servers
- Various Lenovo laptops
- PC Engines (network appliance devices)

Why coreboot?

- coreboot is easier and faster:
    - coreboot C vs. OpenPOWER firmware C++
    - boot speed (coreboot should be faster)

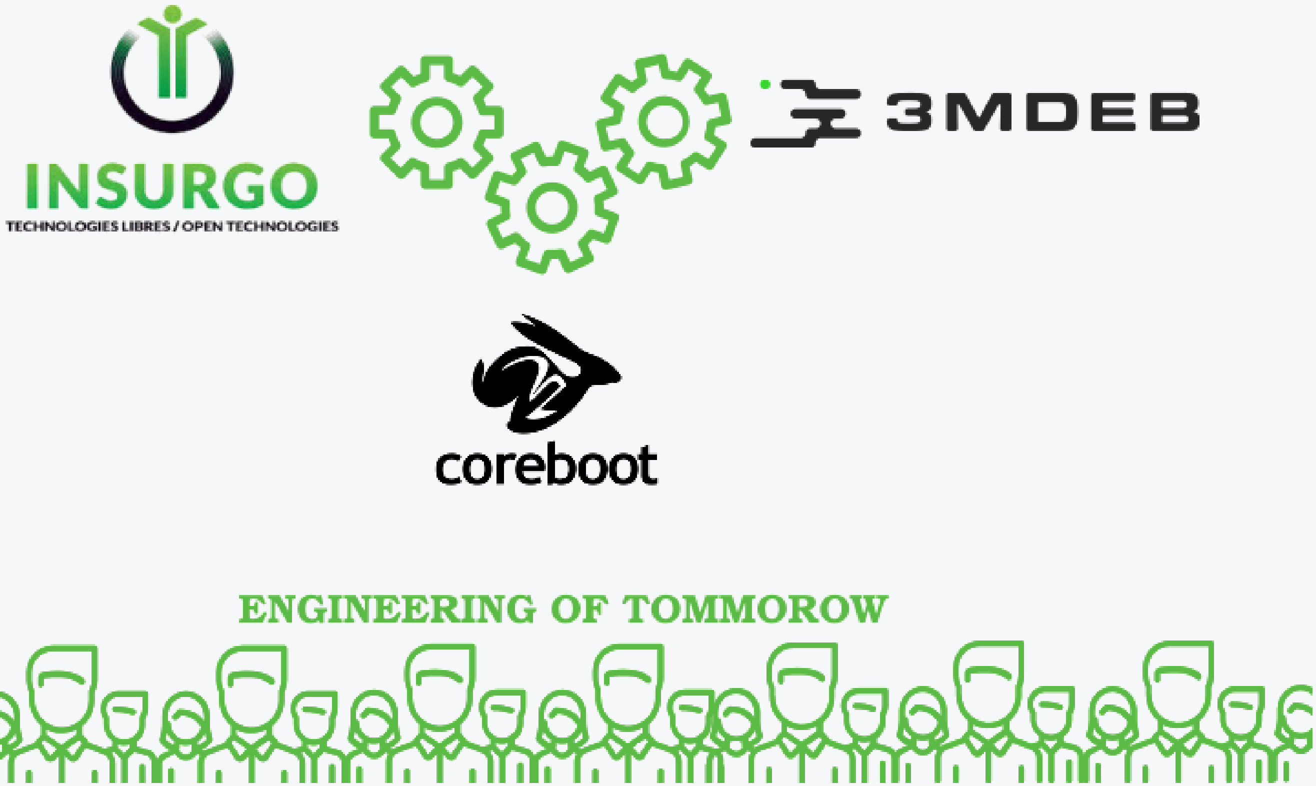
Hostboot is a VM to run FSI routines, and the FSI routines are written one by one by the hardware engineers designing the silicon itself. This leads to overly complex and difficult to understand code, as you can see.

- availability, flexibility:
    - coreboot is well recognized brand for open source firmware
    - one firmware for all platforms and architectures
    - it is easier to find developers for coreboot than OpenPOWER firmware

Why coreboot?

- diversity of implementations:
    - some software combinations may be a better fit for a given application
    - the more alternatives are available, the more people will find a solution that satisfies them
- There are some project (e.g. Heads+Qubes OS) which already are well-integrated with coreboot, why to not leverage that?
- At OSFC 2020 we heard that IBM was also interested in coreboot

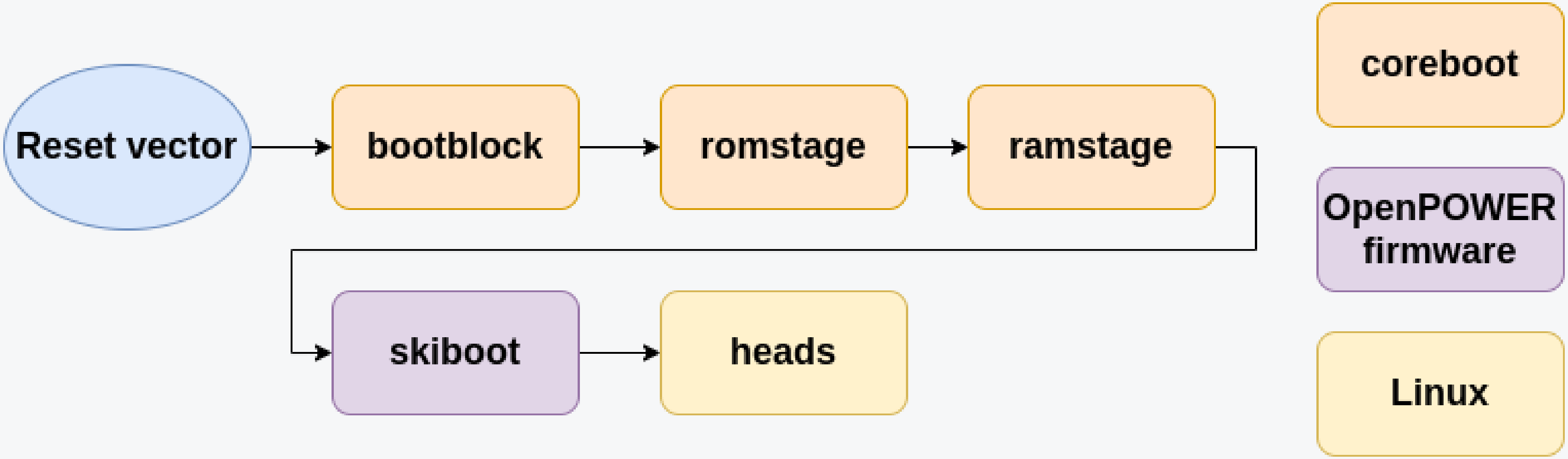
Who is involved?



3mdeb loves coreboot

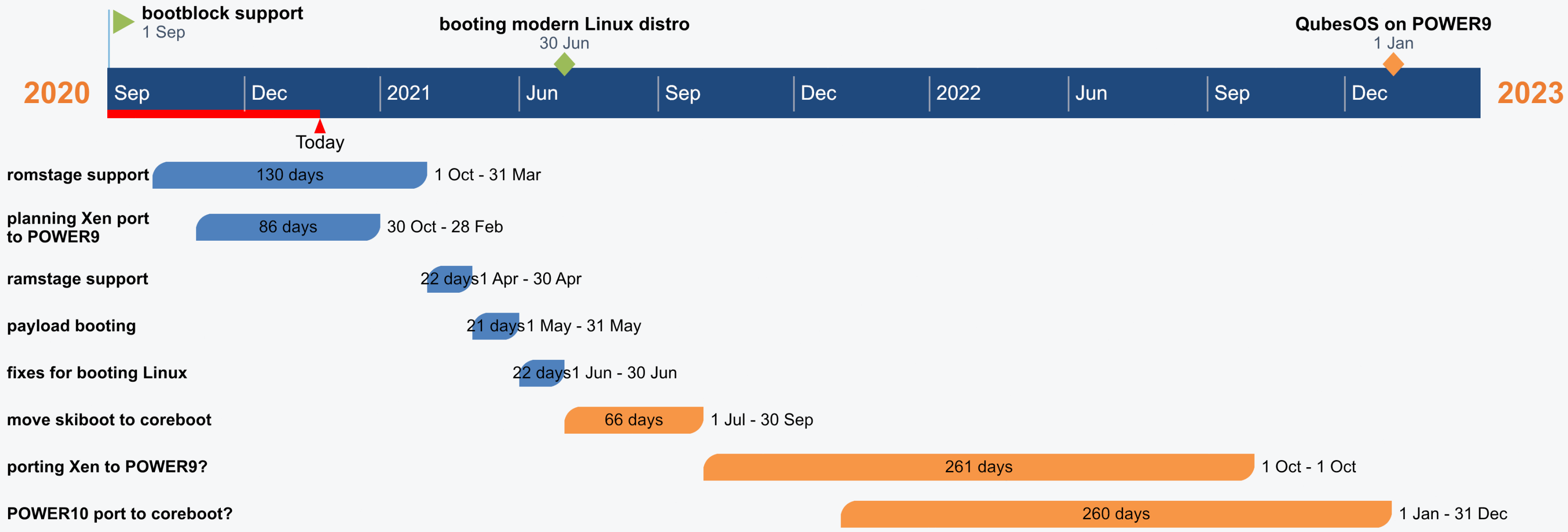
- strong presence in boot firmware for network appliance and firewall devices
- SRTM and DRTM firmware development
- TPM2.0 enabling
- IOMMU and other advanced hardware features enabling
- low level validation integration (BITS, CHIPSEC)
- Open Source Firmware training and workshops
- GRUB and QubesOS minisummit organizers
- active in Open Source Firmware community for 5+ years

Use cases

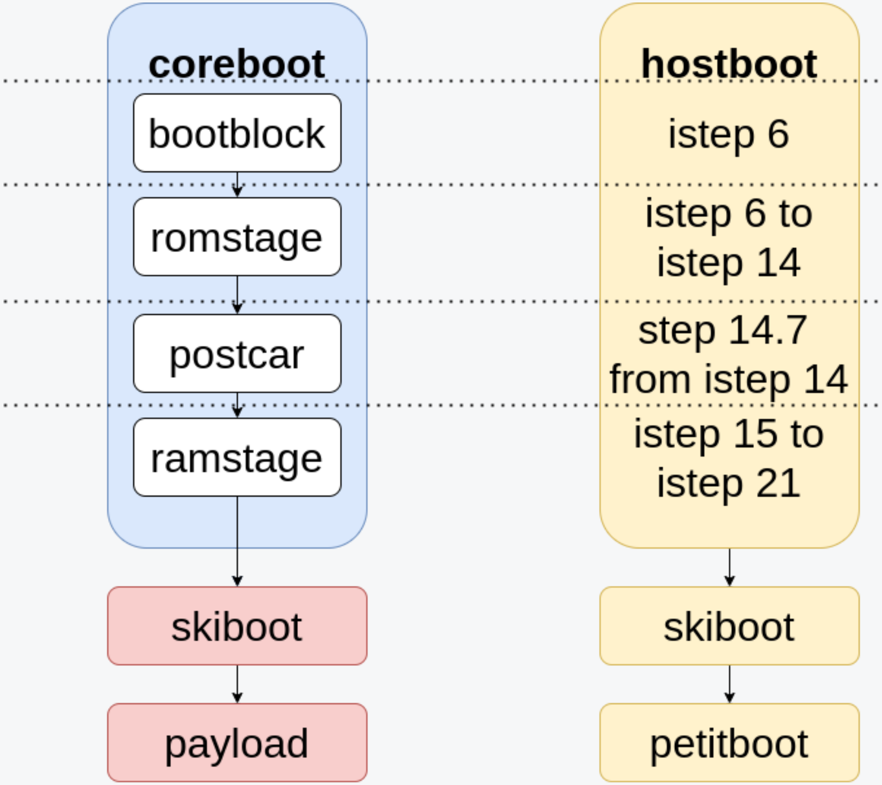


- coreboot + skiboot + heads
  - simple replacement of hostboot with coreboot
  - faster boot time
  - heads security model

Development roadmap



Development roadmap



https://github.com/open-power/docs/blob/master/hostboot/P9_Boot_Flow_OpenPOWER.pdf

Current status

romstage

- Working on the access to the SCOM registers
  - Access to the direct SCOM registers - **DONE**
  - Access to the indirect SCOM registers - **IN PROGRESS**
- Rewriting the DDR4 initialization code:
  - **800k SLOC!**
  - Finished analysis (after 3 months!)
  - Writing the code - **IN PROGRESS**

other

- Replicating the firmware status reporting to BMC:
  - To avoid watchdog resets
  - Let BMC follow the boot process of coreboot
- Launching consecutive stages **DONE**

Future plans

- **port skiboot** related hardware initialization **to coreboot**
- **Xen** port to **POWER9**:
- **POWER10 support ~2022** (even after release would be probably hard to get and expensive)
- **support** firmware update via **fwupd/LVFS** for OpenPOWER based machines
  - 3mdeb got a grant from NlNet for porting fwupd to BSD systems: https://nlnet.nl/project/fwdup-BSD/
- offer **specialized solutions** for OpenPOWER **with Dasharo** boot firmware technology
- **boost knowledge** about coreboot and OpenPOWER with **training** to **widen the group of specialists** and **attract world with POWER** architecture

Xen port to POWER9

- Topic is driven on the xen-devel
    - https://lists.xenproject.org/archives/html/xen-devel/2020-11/msg01152.html
- Many parties interested: IBM, CITRIX, Vates, VanTosh, QubesOS, 3mdeb
- Getting closer to the dream of QubesOS on OpenPOWER
- Other references: https://github.com/QubesOS/qubes-issues/issues/4318
- Last meeting was a deep technical dive but no next steps defined

Dasharo

Dasharo is a set of productized services, Open Core, and SaaS products which help to provide scalable, modular, easy to combine Open Source BIOS, UEFI, and Firmware solutions. It offers the components that are needed to develop and maintain a high quality, and modular firmware, for the stability and security of your platform.

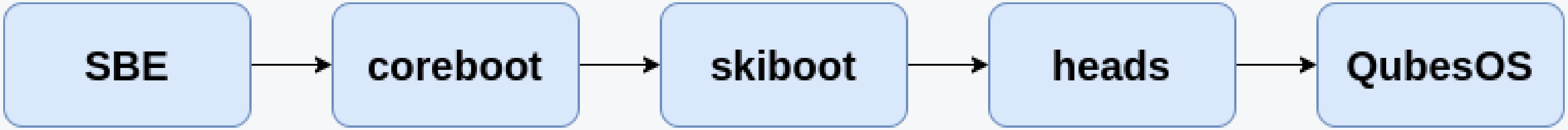
Dasharo Trustworthy Computing

Dasharo firmware for OpenPOWER Talos II based on coreboot.

System features:

- Dasharo Deployment and Provisioning Server (DAPS) Support
- Dasharo Security: safeboot support
- Dasharo Security: Firmware re-ownership support
- Dasharo Compatibility: QubesOS Support
- Dasharo Compatibility: Firmware recovery
- Dasharo Security: D-RTM with TrenchBoot
- Dasharo Security: Remote attestation with Dasharo Attestation Server
- Dasharo Maintenance: Regular signed firmware updates
- Dasharo Compatibility: Regression Test Results and QA reports
- Dasharo Security: S-CRTM with hardware technologies

Dasharo Trustworthy Computing

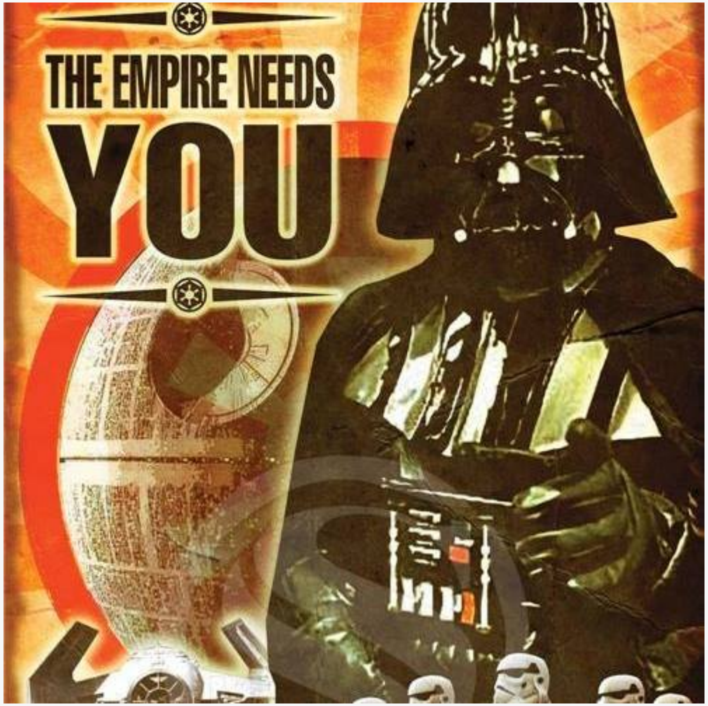


How to help/contribute

- Whole development is open-source:
  - https://github.com/3mdeb/coreboot/tree/talos_2_support
  - https://github.com/3mdeb/op-docker
  - https://github.com/3mdeb/talos-op-build/tree/coreboot_support
  - https://github.com/3mdeb/pnor/tree/coreboot_support
  - https://github.com/3mdeb/openpower-coreboot-docs (docs and information for a newcomer)
- If you have hardware then joins us with development
- If you are experienced in OpenPOWER POWER9 architecture, but cannot develop, your knowledge is also welcome: we have many issues and questions with regards to the hostboot code
- Every two weeks we are having the interesting OpenPOWER discussion. You are welcome to visit us on 18th February at 4PM CET. Topics:
  - great benefits a coreboot is going to provide to POWER-based PCs
  - our progress and some interesting challenges we are facing
  - unique features of Dasharo coreboot-based firmware

Call to action

Do it now!



Talos II booting coreboot’s bootblock

https://asciinema.org/a/JQ1MaBSzGN1L1JcbgTX3G3kt6

Q&A