Open Source Firmware status on AMD platforms 2021

FOSDEM 2021 Open Source Firmware, BMC and Bootloader Devroom

Piotr Król and Michał Żygowski

3MDEB

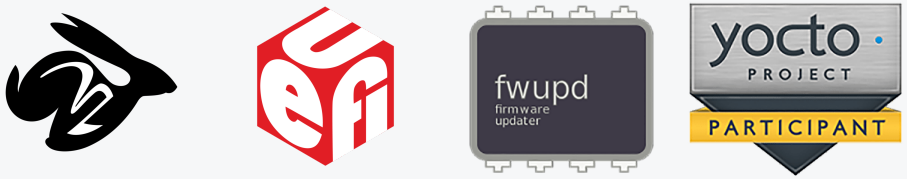
whoami

Piotr Król
3mdeb Founder

- coreboot contributor and maintainer
- Conference speaker and organizer
- Trainer for military, government and industrial organizations
- Former Intel BIOS SW Engineer
- 12yrs in business
- 6yrs in Open Source Firmware
- C-level positions in

3MDEB LPN PLANT VITRO

Who we are ?



- coreboot licensed service providers since 2016
- coreboot project leadership participants
- UEFI Adopters since 2018
- Official consultants for Linux Foundation fwupd/LVFS project
- Yocto Participants and Embedded Linux experts
- Open Source Firmware enthusiasts and evangelists

Agenda

- Definitions
- Status of AMD platforms in coreboot
- AGESA v9
- AMD and coreboot - now
- AMD and OSF
- AMD and coreboot - future
- OSF on non-Chromebook Ryzen boards?
- Platform Maintainership
- References
- Q&A

Refer to FOSDEM2020 Michał Żygowski talk "Status of AMD platforms in coreboot" https://3mdeb.com/events/#fosdem

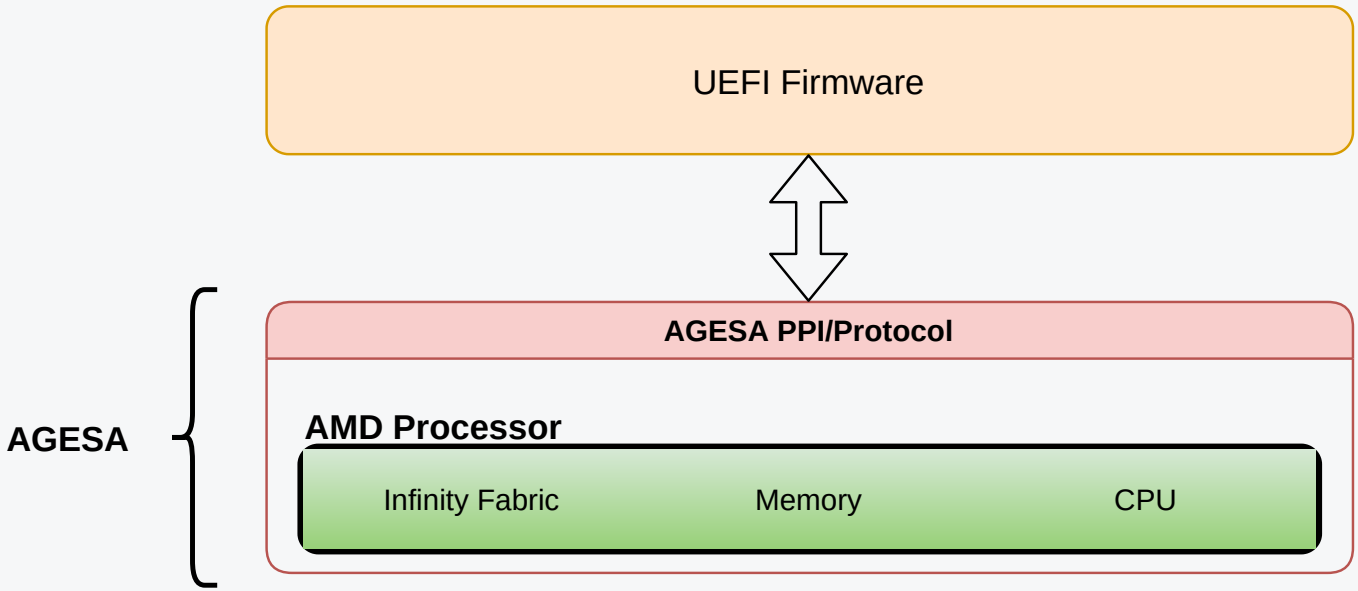
Definitions

- AGESA - **A**MD **G**eneric **E**ncapsulated **S**oftware **A**rchitecture AMD processor initialization source code
  - we can easily call it FSP for AMD
  - requires NDA and sometimes "special relations"
  - it is not monolithic, it consist of platform initialization, silicon initialization, drivers and external interfaces definition
  - despite being complaint with UEFI reference implementation (edk2) it does not support open source toolchains (GCC or LLVM)
  - from AMD OSF group: AGESA goes through modifications to support GCC
- AMD Security Processor - (commonly referred to as PSP - **P**latform **S**ecurity **P**rocessor AMD's equivalent of Intel ME), a coprocessor on the chipset performing similar operations to the ME (security, crypto, CPU bringup, etc.)
  - 36c3 presentation: https://youtu.be/bKH5nGLgi08

For the processor codenames and architecture names please refer to wikipedia

In AMD own words

AGESA roughly consist of Processor Core Subsystem, PEIM and DXE drivers which produce AGESA PPI and AGESA Protocol



A little bit of clarification

- another closed source implementation
- v9 is successor of v5
- v9 support for family 17h (Ryzen, EPYC) and later
- **uses UEFI interface and integrates to EDK2 only!**
- v9 design could not meet Chromebooks firmware design needs
    - UEFI/PI interfaces (e.g. PPI) at that point were not abstracted to work with coreboot
    - problem was solved by Intel FSP (Firmware Support Package)
    - since 2014 FSP was well-established and integrated with various OSF projects (coreboot, U-Boot)
- v9 had to get FSP support
    - the correct™ thing to do was adding support for TianoCore edk2 IntelFsp2Pkg

AGESA v9 FSP adaptation

- support for family 17h (Ryzen) **and later**
- Despite Google being leading partner for Picasso FSP (AGESA with FSP interface) it is compatible with all AMD Picasso-based systems
- After FSP adaptation AGESA v9 **conforms to FSP 2.0 specification**
- since new AMD systems got DRAM initialized made by AMD Security Processor there is no need for Cache-As-Ram (CAR), what effectively eliminates FSP-T stage (Temp RAM initialization phase)
- Improved v9 also contain few additional HOB (Hands-Off Blocks) to transmit some information between proprietary and outside world
- for more details see Kerry Brown's talk from OSFC 2019:
  `Adaptation of AMD Reference Firmware to coreboot© Using FSP 2.0`
  https://www.youtube.com/watch?v=eyRsk8GU3OE
    - please note: AMD decided no to use hybrid romstage, but use traditional coreboot flow with bootblock and romstage
- Products: Google Zork Chromebook

AMD and coreboot - now

From the release notes (v4.12 and v4.13)

- in v4.13 new resource allocator (v4) were introduced to improve efficiency of device memory allocation
- As result v4.14 either will gain v4 support for Family 14h-16h either platform would be dropped from upstream releases
    - we working on having correct support for PC Engines firewalls

AMD and coreboot - now

From the source code and reviews

- Despite there are no `@amd.com` patches going upstream, team contributing to coreboot is officially hired by AMD
- diffstat: `322 files changed, 2306 insertions(+), 13518 deletions(-)`
  - mostly skeleton code for new platforms added and dead code for old platforms droped
- Under review
  - initial patches for AMD Cezanne support (AMD Ryzen 5000)
  - initial patches for AMD Majolica support (FP6 APU, AMD Ryzen 5000U ?)

AMD and coreboot - now

From coreboot leadership meeting

- There is a chance that AMD servers will also get OSF support

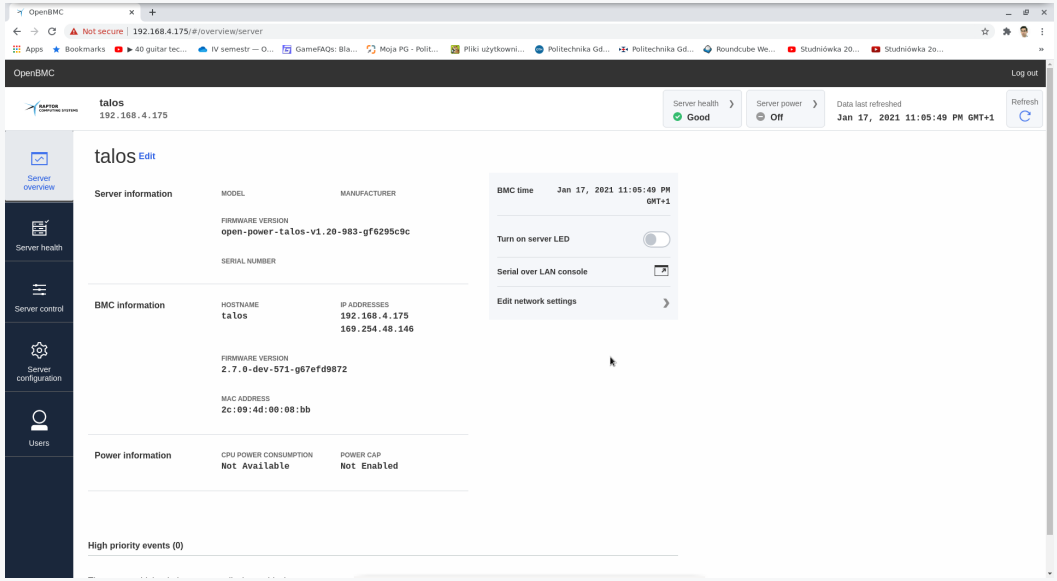
So when community may get something usable?

- in short: we have no idea
- WIP, due to groundbreaking change to architecture it takes a lot of time and effort to make it land into the main tree in usable form
- After finalizing Picasso integration further SoC should get way better timeline, then initial one
- On the other side AMD tries to recruit firmware developers for coreboot work
    - congratulations to our OSF friends who joined AMD, we already see things moving faster
- **NEW: the mainboards are mostly ready for Picasso processors in coreboot**
    - but no ETA yet, not saying about new stuff

Pure open source on AMD EPYC 7002 "Rome"

- Implementing the support from scratch on one of the newest AMD server processor
- Effort by Ronald Minnich (Google)
- Implemented in Rust (oreboot)
- Presented on OSFC2020: https://vimeo.com/showcase/7884533/video/488147337
- It is important to understand limitations
  - not everyone can get/borrow AMD EPYC CRB
  - there are some hw platforms on market, but are those without vendor lock-in?
  - also expensive for OSF vendor without justified business
  - code initializes minimal set of low-speed interfaces to boot Linux
  - to fully utilize platform using OSF there is way more work, which probably would be hard to do without correct™ coordination

AMD and OSF: OpenBMC

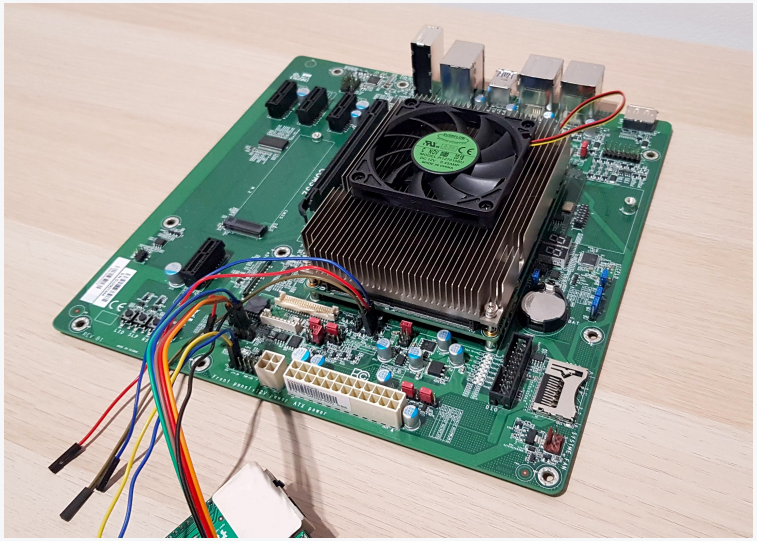


- OpenBMC support for AMD EPYC processors
- Special meta-amd implemented for AMD specific management interfaces
- Support for AMD EPYC EthanolX customer reference server platform
  - including Phosphor WebUI (AngularJS+nodejs)
- Presented at OSFC2020 by Supreeth Venkatesh: https://vimeo.com/showcase/7884533/video/488132697

AMD and coreboot - future

- ~~many platforms are being dropped due to coreboot release requirements~~
- ~~some developers engaged to implement missing functionalities and requirements (mainly me and Kyösti Mälkki)~~
- ~~community aligns with the work and push updated board support~~
- much clean-up and fixes to do, most of the code landed in the repository as copy-paste (MP tables, IRQ tables, ACPI code is also poor)
- thanks to the companies like PC Engines (who support open source development through 3mdeb), the platforms keep living in the coreboot project
- for now old AMD-based platforms can move on, but it is unknown when they will face a wall that cannot be jumped over (closed source blobs making it even harder)

OSF on non-Chromebook Ryzen boards?



- 3mdeb integrated AGESA v9 for R1000/V1000 Ryzen processors into UEFI reference implementation edk2
  - we planning releasing all our source code in 2021 under Dasharo Safety-Critical brand
- Reference platform: DFI GH960-BS-R1505G & COM332-B COMe module

OSF on non-Chromebook Ryzen boards?

Problems we faced

- Written only for MS VS2019 compiler, MS ABI!
- Code tested only with MS Visual Studio Express 2010!
- Lots of bugs in edk2 code for CPU startup for example
- Function definition mismatches between AGESA v9 and UEFI specification/edk2
- We have no knowledge about way for contributing back to AGESA v9 code base

Platform maintainership

Native ports:

- Asus KCMA-D8 (dropped from tree)
- Asus KGPE-D16 (dropped from tree)
- Supermicro H8SCM (dropped from tree)

Situation:

- unmaintained and left behind by their port authors
- many bugs unresolved and many new arose in the meantime
- dropped form master branch due to not fulfilling the coreboot release requirements
- one of the last and newest available blob-free, fully libre hardware (no PSP, microcode etc.)

KGPE-D16 last hope?

- ~~3mdeb applied for funding to bring back the Asus KGPE-D16 board back to master branch~~ **REJECTED**
- AMD's processors can be better in certain aspects than Intel's (fully open-source D-RTM implementation with **Trenchboot** developed by 3mdeb with cooperation of Daniel P. Smith (Apertus Solutions), Andrew Cooper (Xen Project))
  - Adding more and more features to AMD DRTM in TrenchBoot
  - Support for DRTM event log
  - Support for Linux and Xen measured launch
- Insurgo Technologies Libres / Open Technologies together with 3mdeb wanted to revive the KGPE-D16 support in coreboot, however the availability of the platform is so low, that the effort has been halted.
- **Kudos to Thierry for going above and beyond to support that platform**
- **There is still little chance that FSF will engage, since they use that platform, if anyone care and have means of reaching them please let us know**

Announcement

3mdeb works on effort which will coordinate monthly paid hackathon for those who want to learn coreboot and help bring KGPE-D16 back to upstream coreboot.

If you are interested please contact me using email, OSFW Slack, social media or any other means of communication:

piotr.krol@3mdeb.com

References

- Marc Jones at coreboot summit 2008:
  AMD coreboot Development
- Marshall Dawson at Denver coreboot conference 2017:
  AMD and coreboot - History and future
- 3mdeb experience (especially Michał Żygowski and Krystian Hebel)

Q&A