Status of AMD platforms in coreboot

FOSDEM 2020 Hardware enablement devroom

Michał Żygowski

3MDEB
Michał Żygowski
Firmware Engineer

Social media:

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

- PC Engines platforms maintainer in coreboot
- Braswell SoC maintainer in coreboot
- one of 36 official coreboot developers
- interested in:
  - advanced hardware and firmware features
  - security solutions
- Introduction
- Definitions
- AMD and coreboot - history
  - AGESA v3 (and earlier), CIM-x
  - AGESA v5 open-source
  - AGESA v5 binaryPI
- AMD and coreboot - future
  - AGESA v9
  - Platform maintainership
- References
- Q&A
- **AGESA** - AMD **Generic Encapsulated Software Architecture**
  AMD processor initialization source code

- **CIM-x** - AMD southbridge initialization code

- **FCH** - Fusion **Controller Hub**
  new generation of AMD southbridges/chipsets

- **PSP** - Platform **Security Processor**
  AMD's equivalent of Intel ME, a coprocessor on the chipset performing similar operations to the ME (security, crypto, CPU bringup, etc.)

For the processor codenames and architecture names please refer to [wikipedia](https://en.wikipedia.org/wiki/List_of_AMD_microprocessors).
AGESAv3 (and earlier), CIM-x, around 2008:

- Family 10 support, Geode processors
- Processor, memory, Hyper Transport initialization
- Southbridge initialization (8111/8131, M690, SB600/SB700)
- 3 chip solutions
- already dropped from master branch due to maintainability problems

Products:

- **PC Engines ALIX boards** (Geode LX) - maintaining was too troublesome (no MTRRs, no clean CAR setup, many FIXME in the code etc.)
AGESAv5 open-source (2011-2013):

- CIM-x only for family 14h
- CIM-x merged into AGESA for newer families
- since family 15h discrete FCHs (many variants)
- open-source up to family 15h (Trinity) and 16h (Kabini)

Products:

- Lenovo G505s (family 15h)
- PC Engines apu1 (family 14h)
- ASRock E350M1 (family 14h), IMB-A180 (family 16h)
- Asus AM1I-A (family 16h), F2A85-M (family 15h)
AGESAv5 binaryPI (~2014):

- closed source, binary releases of AGESA
- first appearances of PSP and integrated FCHs
- supported by family 15h processors models 30h-3Fh, 60h-6Fh and 70h-7Fh, family 16h processors models 30h-3Fh
- currently unmaintained by AMD
- broken suspend/resume, issues with CAR teardown

Products:

- **PC Engines apu2** (family 16h)
- Chromebooks
  (family 15h models 70h-7Fh - StoneyRidge)
AGESAv9 (2019-now):

- another closed source implementation
- support for family 17h (Ryzen)
- apparently it is designed only for Chromebooks
- work-in-progress, due to AMD's groundbreaking change to their processors architecture it takes a lot of time and effort to make it land into the main tree in usable form
- 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](https://www.youtube.com/watch?v=eyRsk8GU3OE)

Products:

- **Chromebooks**
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 the 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)
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 blob-free, fully libre hardware (no PSP, microcode etc.)
Hope:

- 3mdeb applied for funding to bring back the Asus KGPE-D16 board back to master branch
- 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))

Future:

- 3mdeb will keep improving the AMD support in coreboot via PC Engines company and their apu products
- possibly bring back other native ports beside Asus KGPE-D16
- family 17h support (Ryzen/Zen) is rather unlikely for other products than Chromebooks in coreboot
• Marc Jones at coreboot summit 2008: AMD coreboot Development
• Marshall Dawson at Denver coreboot conference 2017: AMD and coreboot - History and future
• Own experience
Q&A