3MDEB

- Before 3mdeb was created in 2015 <u>**OST1**</u> provided best in class, available for free, structured training content about platform security.
- coreboot, OST1, Invisible Things Lab research and Matthew Garret lectures about UEFI, influenced me to create 3mdeb in 2015.
- Who would expect that after years we would have chance to contribute back to OpenSecurityTraining2.

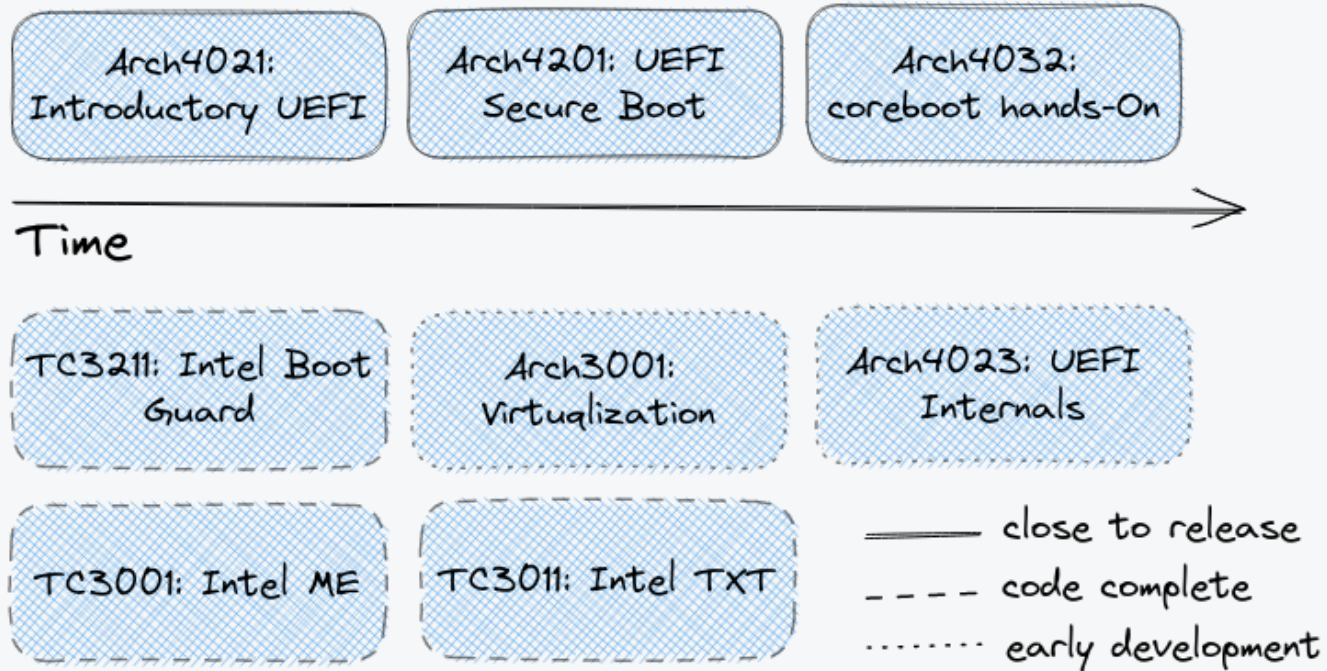| Type	Who loads	Loaded from	Who execute	Example
I-A	Host	System FW	Host	BIOS, FSP, uCode
I-B	Host	Peripheral Dev	Host	OpROM, PXE
II-A	Non-Host	Non-Host FW	Non-Host	BMC, EC, CSME
II-B	Peripheral	Peripheral Dev	Peripheral Dev	NIC, NVMe, GPU

- "A new Golden Age for Computer Architecture: Domain-Specific Hardware/Software Co-Design, Enhanced Security, Open Instruction Sets and Agile Chip Development", John Hennessy and David Patterson 2017 ACM A.M. Turing Award Lecture - link
- "It's Time for Operating Systems to Rediscover Hardware", Timothy Roscoe, USENIX ATC '21/OSDI '21 Joint Keynote Address - link
- Lot of standardization bodies work on cleaning up the mess.

3MDEB
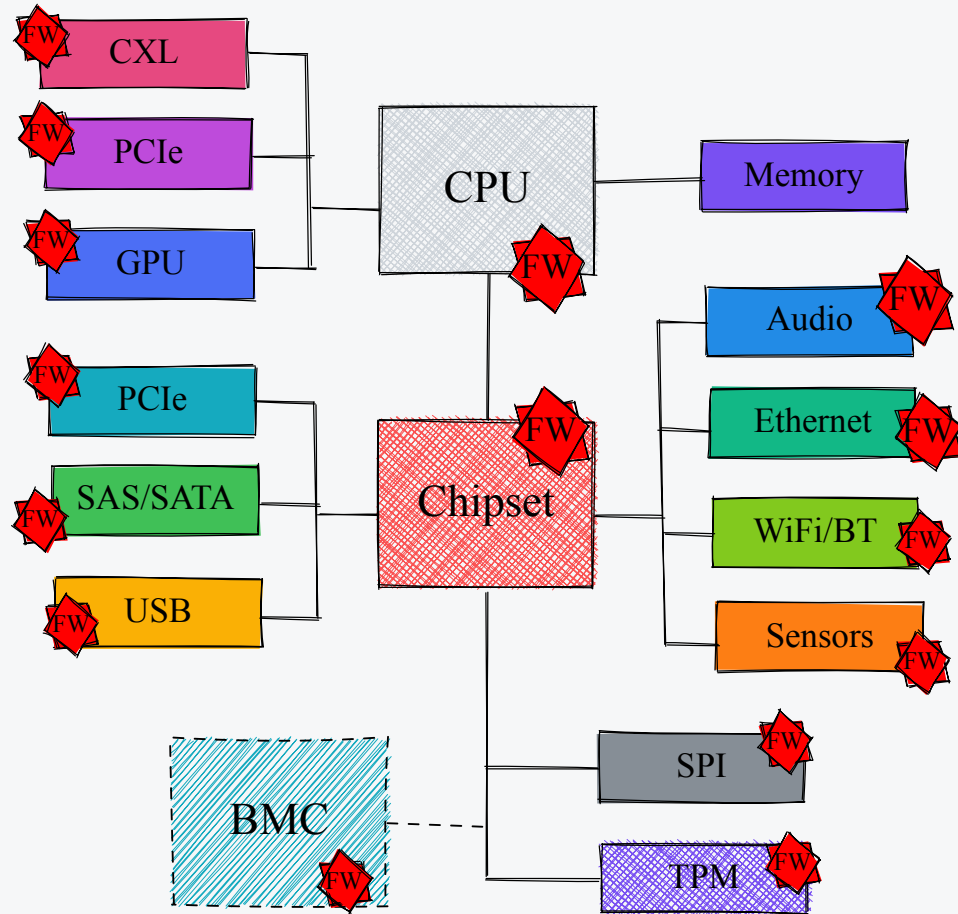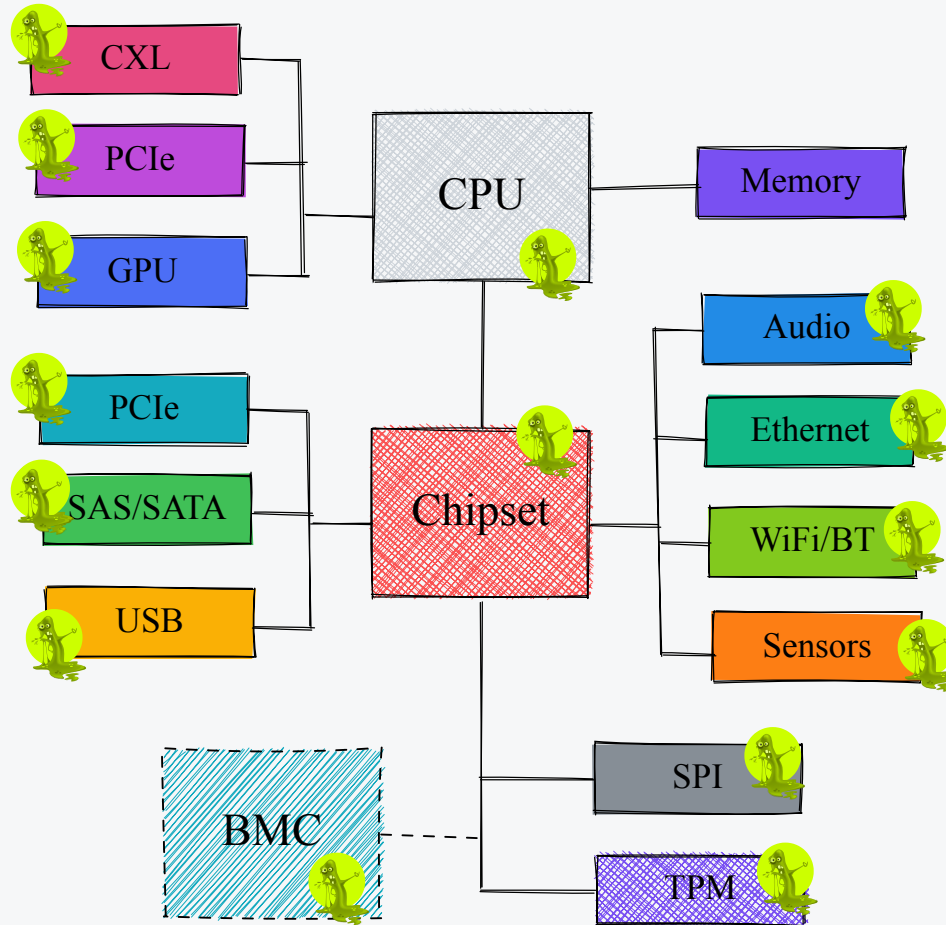
- Computing solutions that we can trust are either old or expensive.
- Without open source firmware it will be hard to create trustworthy solutions, needed for daily use on all levels of computing.
- Without new software engineers interested in open source, low level security and privacy, we cannot build strong enough ecosystem.
- OST2 give us chance to share knowledge more efficiently using privacy respecting and trustworthy solution.
  - We can explain things easily to new beginners
  - Better awareness should lead to better adoption
  - More experts in community harder problems we can solve
- What areas are most useful for open source firmware community?
  - firmware frameworks (coreboot, UEFI, name-you-favourite-one)
  - advanced hardware security
  - trusted computing (TPM)
  - reverse engineering

- Contribute existing training materials.
- Align commercial training roadmap to maximize Creative Commons content creation.
- Reuse existing material for commercial training, mind the attribution.
- Focus on value-added in person and remote live training to generate margin that can sponsor OST2 contribution.
- Leverage conference content delivered in the past.
- Move new employees training to OST2.
- Convert internal analysis, research and reports into training materials.
- Engage your team.

3MDEB

Arch4021: Introductory UEFI

Arch4201: UEFI Secure Boot

Arch4032: coreboot hands-On

Time →

TC3211: Intel Boot Guard

Arch3001: Virtualization

Arch4023: UEFI Internals

TC3001: Intel ME

TC3011: Intel TXT

—— close to release
- - - - code complete
········· early development

- We would like to focus on training materials in 2022
- If you want to speed up things please consider sponsorship or recommend us as trainers in your organization.
- Feel free to send us your wishlists and feedback