0x1: Open Source Firmware community triage

3mdeb vBeer Event

3mdeb Team

3MDEB

Topics

- How hard would be to have coreboot on modern device?
- OSF vision vs reality
- Are True Open Source™ even possible in today's reality?
- Secure Boot as source of evil debunked
- Differences between various coreboot-based projects: Heads, Skulls, libreboot, retroboot, oreboot etc.
- How we can bring back KGPE-D16 back to upstream coreboot

Dasharo firmware menu walk-through

https://asciinema.org/a/374013?cols=50

Next vBeer

Ideas for future

- Alexey Vazhnov: coreboot documentation maintanership + user documentation contribution issues
- Trammell:
  - spispy + RTE
  - ulx3s ecp5 (bigger one) can replace Orange Pi
  - X11 boot time comparison
- Rich:
  - grading

Wire channel

- Event Wire channel: `3mdeb-vBeer`
- Please ping: `pietrushnic` on Wire to get access

Dasharo Certification Program

- Registers should have no magic values in it
  - if there is register value there should be reference to public document
- Fixed configuration that are known to work
  - hardware
  - software stack
- Reference tools and documentation that will prove feature works
- https://bestpractices.coreinfrastructure.org/en/criteria/0
- https://bestpractices.coreinfrastructure.org/en
- https://github.com/opencomputeproject/Security/blob/master/SecureFirmwareDev

Q&A

class: center, middle, outro