Dasharo OSF vPub Winter 2022

(aka 3mdeb vPub vol. 4)

vPub Event

3mdeb Team

General rules

Our mission is to fill the space left by lack of direct human-to-human backstage discussion, networking and after-parties.

We are primarily dedicated to open source firmware, open source hardware and open instruction set architecture.

Thank you for spending time with us! First of all have fun!

General rules

- For details (including clickable links) please visit: https://vpub.dasharo.com
- Chat is on `#dasharo-osf-vpub:matrix.org`
  - You can join video and audio from there
  - Presenters have to use `https://meet.jit.si/dasharo-osf-vpub`
  - Please note `#dasharo-osf-vpub` is just one of the channels in Dasharo Matrix Space, feel free to join others `#dasharo:matrix.org`
- Please note we using Jitsi free tier. We kindly ask to use video only when necessary (to say hello, for toast) or when the number of active participants gets small.
- Be kind to each other.
- Adult beverages allowed.
- Mute by default.
- No audio or video recording
- "Last *haker* standing party"
- Feel free to introduce yourself and tell us why you joined.
- Feel free to queue the topics, questions, problems, by sending private message to moderator (`pietrushnic`).

History

- This is fourth event
  - not counting unofficial ones organized as part of virtual conferences
- Last event was called "Dasharo OSF vPub Fall 2021" and had place on 16th Nov 2021
- We were visited by 40 unique users
- Event last for 7.5h (8PM UTC - 3:30AM UTC)
- Slides can be found in Dasharo OSF vPub Archive: https://vpub.dasharo.com/archive/vpub-0x3/

What's new

- We experimenting with adding some structure
- On top of each hour we will start 10 minutes presentation/demo followed by Q&A session
  - precise schedule on the vPub website: https://vpub.dasharo.com
- Topics that we will discuss today:
  - Racklet by Dennis Marttinen
  - Technology Commons Trust by Michiel Leenaars
  - LibreSoC debugging by Like Kennerth Casson Leighton
  - oreboot by Daniel Maslowski
  - FSF RYF by Richard Stallman
  - GSoC 2022 by Felix Singer and tonux
- Please note we looking for project/topics and products suggestions for next vPub
  - On-going call for participation is on the bottom of vPub website
- After above talks if we would have enough energy we can switch to some open discussion topics we prepared for today

Crowdfunding

- open source firmware/hardware and open ISA needs better funding models,
- cryptocurrency crowdfunding,
- KYC is probably biggest issues among all,
- TecraCoing seemed to be interesting in that space: https://tecracoin.io/
  - unfortunately despite claims about using non-KYC Uniswap in terms of service I fund full validation of identity and tax jurisdiction,
- from privacy and liberty stand point crypto-crowdfunding would be great model for not-so-cheap firmware/hardware and ISA development,

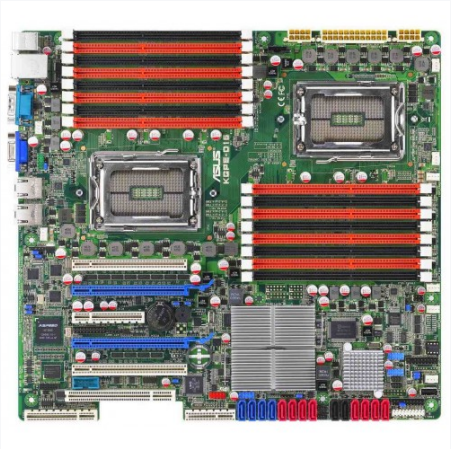
Intel ACM

- Public review of the open letter draft to open the Intel ACMs code,
- Read-only version available here: https://pad.riseup.net/p/qmlVCDtO74uKOMbDaHUg

fwupd/LVFS

- Open source firmware distribution through fwupd/LVFS,
- 28 Jan 2022 Richard organized LVFS Community Meeting,
- Notes available here: https://github.com/fwupd/fwupd/wiki/LVFS-Community-Meeting-2022-01-28#notes
- Meanwhile couple other questions popped up on Twitter:
  - Richard started discussion about simplified and scalable way of building firmware here.
  - pflash support for POWER9 firmware here

Dasharo compatible hardware



- **Asus KGPE-D16**
  - Project sponsored by Immunefi with the purpose of building trustworthy platform for blockchain developers.
  - Last release: v0.3.0 16 Dec 2021
  - Documentation: https://docs.dasharo.com/variants/asus_kgpe_d16/releases/
  - How to buy: (shop offline) https://store.vikings.net/libre-friendly-hardware/d16-ryf-certfied

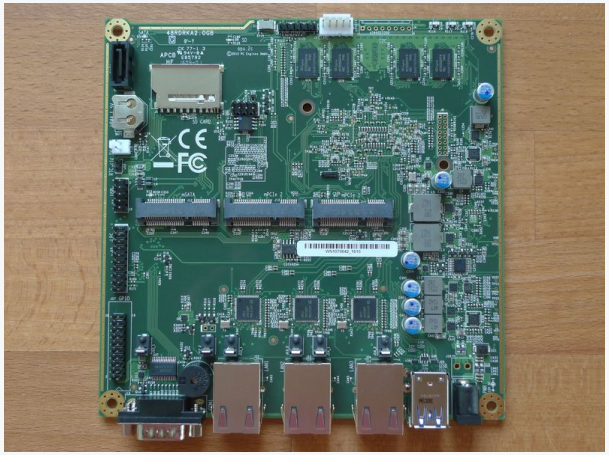
Dasharo compatible hardware

- **Raptor Computing System Talos II**
  - Project sponsored by Insurgo with the purpose of building trustworthy platform for general purpose use.
  - Last release: v0.4.1 10 Jan 2022
  - Documentation: https://docs.dasharo.com/variants/talos_2/releases/
  - How to buy: write to https://insurgo.ca/#contact

Dasharo compatible hardware

- **Dell OptiPlex 7010/9010**
  - Project sponsored by 3mdeb with the purpose of creating daily driver for SME.
  - Last release: v0.1.0 18 Jan 2021
  - Documentation: https://docs.dasharo.com/variants/dell_optiplex/overview/
  - How to buy: 3mdeb eBay https://www.ebay.pl/usr/3_mdeb

Dasharo compatible hardware



- **PC Engines apu2**
  - Project sponsored by PC Engines with the purpose of providing high quality firewall hardware.
  - Last release: v4.15.0.3 16 Feb 2022
  - Documentation: https://pcengines.github.io
  - How to buy: https://www.pcengines.ch/order.htm
  - This firmware is not branded Dasharo, but based on it bake custom PC Engines firmware and provide it under Dasharo branding.

Dasharo compatible hardware

- **NovaCustom NV40 Series**
  - Project sponsored by NovaCustom with the purpose of providing open source firmware laptop.
  - Last release: v1.0.0 19 Jan 2022
  - Documentation: https://docs.dasharo.com/variants/clevo_nv41/releases
  - How to buy: https://configurelaptop.eu/nv40-series/

- Website: https://ost2.fyi/
- OpenSecurityTraining2 reward system plans and ideas,
  - Idea of Slack with access to trainers for students who finished at least one course was approved and is under implementation,
- Other ideas discussed at FOSDEM'22 after-party: NFT

Root of Trust

- Recent advancements in Root of Trust technologies (MS Pluton announcements, TrenchBoot project status)

Next vPub plans and ideas

- Dasharo OSF vPub Spring 2022
- We plan physical Dasharo OSF Pub in Q2'22
    - Location: Gdańsk
    - Similar format but with human-to-human interaction

Q&A