Dasharo OSF vPub Fall 2021

(aka 3mdeb vPub vol. 3)

vPub Event

3mdeb Team

General rules

We believe building and growing community around OSF, OSHW and Open ISA is especially important in recent times, so thank you for spending time with us! First of all have fun!

- For details please visit: https://vpub.dasharo.com
- We prefer discussion on Matrix: `#dasharo-osf-vpub:matrix.org`
  - in future we hope to use similar setup as FOSDEM (Matrix+Jitsi)
- 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.
- 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)

General rules

- No audio or video recording
- "Last human standing party"
- For details please visit: https://vpub.dasharo.com
- We prefer discussion on Matrix: `#dasharo-osf-vpub:matrix.org`
    - in future we hope to use similar setup as FOSDEM (Matrix+Jitsi)
- Feel free to subscribe to Dasharo vPub Newsletter so you can stay

History

- This is third (fourth?) event
  - we organized one informal vPub after Qubes OS mini-summit 2021
- Last event was called vPub 0x2 and had place on 7th May 2021
- There were ~50 attendees in peak
- Event last for 12h (3PM UTC - 3AM UTC)
- Blog post: https://blog.3mdeb.com/2021/2021-07-01-osf_vpub_02/

Linux Secure Launch - TrenchBoot Summit questions

- Am I correct in understanding that the Secure Upgrade tentative mechanism described at LPC is not the same as the Secure Upgrade from the FOSDEM talk? Also, is the latter already implemented in Trenchboot? 1
- Has anybody looked into making systemd-boot capable of being a DCE Preamble for DL (instead of grub)? There was a recent post of Lennart Poettering about secure boot but I don't think he addressed D-RTM. 2

Will Intel Alder Lake beat the AMD and how open its firmware can be?

- topics was rather not picked up

FOSDEM 2022: virtual

- what topic you would like to see in OSF devroom (if we will get it)
- Thierry: redistribution of blobs
- IOMMU: PCIScreamer and similar stuff
  - unmapping DMA buffer is expensive - this is hardcore OS innovation to change that
  - walk-through and how to make it work
- Reproducible toolchain
- TrenchBoot update
- AMD status
- vPub we will

Laptop testing

- Chamelium: https://www.chromium.org/chromium-os/testing/chamelium
- Martin: works on opening tools (hw+sw) of Google testing team to make it simpler and cheaper
- Marek (Quber OS Team): PiKVM: https://pikvm.org/

vGPU

- Arthur: SRIOV, it maight be good to have OSF for GPUs
- https://libre-soc.org/
- NVIDIA grading usage of hardware based on subscription
- https://libvf.io

Root of Trust and its futures

KGPE-D16 status

TrenchBoot Summit

Libre/Open smartphone

- Our experience from using PinePhone
  - GrapheneOS is better daily driver replacement
- What do you think about new PinePhone Pro?
  - https://linmob.net/thoughts-on-the-pinephone-pro/
- https://sxmo.org/
- TrustZone
  - https://www.blackhat.com/docs/us-14/materials/us-14-Rosenberg-Reflections-on-Trusting-TrustZone.pdf
- Blackberry and Nokia case study

Promise of OSF on POWER9

- Videos from OpenPOWER summit 2021 already available: https://youtu.be/fyyqyJjQmbc

Future of OCP

- AMI joined OCP, suddenly no OSF talks were approved for OCP Summit
- now we have very interesting new repos at: https://github.com/opencomputeproject
- OSF (Open System Firmware) vs OSF (Open Source Firmware)

Dasharo OSF vPub Winter 2022

Q&A