linaro™

Arm Solutions at Lightspeed

OSFC 2024

Ilias Apalodimas

OSFC

- Conference aiming at improving open source firmware support
- Was held in Bochum this year
- Schedule can be found here
- Presentations and videos have not been published yet

Event Summary: The event had a primary focus on x86 and server space, so although some interesting sessions, did not come across any TrustedFirmware.org new member opportunities.

Summary

- A mix of talks including
  - Architecture details and related software – e.g TF-A, openSBI, rustSBI, openSIL etc
  - Software components – e.g TF-A, coreboot, openBMC, Zephyr etc
  - Firmware in Rust
  - Board bringup stories
- A lot of talks were aimed at coreboot and openBMC
- More server orientated than embedded currently
- Focus on security is lacking

Interesting talks

- Practical PCR forgery
  - Talk on TPM vulnerabilities
  - All described attacks were based on faulty hardware designs
- Provable Security in Embedded Systems
  - Verification work in Tock OS
  - Very nice talk discussing Rust and the verification methods it has
  - TockOS uses flux
- Virtualizing Firmware on RISC-V
  - Mentioned RMM, Armv9 as an example
  - Explains the difference approach miralis followed
  - They are trying to sandbox firmware components by virtualizing M-mode to protect the OS from it

Interesting talks

- Open source all the way down
  - How opentitan develops firmware in parallel with the silicon designs
  - Deep dive on their architecture, FPGAs and testing methods
  - Some cost analysis of how expensive this is
- Getting your open source software ready for 0-day SoC bringup
  - Good intro in Arm standards and SystemReady certification
  - Also included armv9 architecture and components – e.g RMM
  - An attempt to convince vendors to work closer with the upstream community
- What CSP Servers Need from Open Source Firmware Solutions
  - Hosts in CSPs are treated more like embedded systems o
  - Once they enter data centers, the servers are not open for expansion of modification
  - Since CSPs are focused on security having smaller and open source firmware reduces their attack surface

Interesting talks

- AMD's Long-Term Strategy for Open Source Firmware
  - An update on AMDs activities on open source firmware
  - openSIL is still a PoC
  - Expected to be production grade in 1-2 years from now
- Open source platform communication with MCTP
  - Mostly low level details of how MCTP works
  - The interesting part is that patches are available in upstream kernel, using standard network sockets
- Operating system provided device-trees
  - Real world problems OSes have by firmware provided DTs
  - Some proposals to resolve this were proposed
  - Contradicts some parts of EBBR/SystemReady-IR