OP-TEE Roadmap

Ilias Apalodimas

linaro™

Arm Solutions at Lightspeed

Current activities

- Secure Data path support
  - Patches under review
  - Expecting v3 soon with more changes
- fTPM support
  - Microsoft removed the public TA
  - We are working on pulling it as a separate TA people can use
  - Some patent discussion is ongoing
- OP-TEE in kernel supplicant
  - Patches merged upstream
  - You can read more about it here
- OP-TEE dynamic configuration
  - Support runtime configuration of
    - Number of cores and thread
    - Amount of secure memory
    - Allocation of translation tables

Planned avtivity

- Enhance on FF-A 1.2 support in OP-TEE and Xen
- Enhance testing and coverage. Try to run OP-TEE xtests in hardware and QEMU-SBSA
- Optimize Secure Partition partition support
  - Remove the need for an active thread to enter an S-EL0 SP
- Add support for Logical Secure Partitions
  - An alternative to Pseudo TAs

Thank You!

Visit linaro.org

linaro™

Arm Solutions at Lightspeed