Earlier LVC20 contents...

- **Trusted Firmware Project update**

- **(PSA) Secure Partitions in OP-TEE**
Agenda

• Current TZ architecture and challenges
• Firmware Framework for A-class
• SPM architecture and Hafnium
• Project status
• Upstream activity
• End to end testing
Current TZ architecture (recap)
Current architecture (challenges)

- NWd isolation
- Trusted App. Ecosystem
- Principle of least privilege
- Multiple vendors
Firmware Framework for Armv8-A (FF-A)

- Harmonizes NWd / SWd endpoint communication
- (Secure) Partitions and (Secure) Partition Manager
- Partition manifest (or resources description)
- Standard interfaces (SMC based)
  - Setup and discovery
  - Message passing (register-based / shared memory)
  - Memory sharing
FF-A with virtualization
FF-A with virtualization

Armv8.4-Secure EL2
SPM architecture
Hafnium and Trusted Firmware

- Transitioned from Google to trustedfirmware.org
- Open development, BSD-3
- Co-maintained by Google and Arm
- Become the reference S-EL2 firmware
Project status

- Prototyping
- FF-A setup and discovery
- EL3 SPM Dispatcher

- Secure boot enablement
- Multiple secure partitions
- World switch

- Interrupt management
- Memory sharing
- Power management

- SMMU support
- S-EL0 partitions
- AArch32 SPs

Q1’20
- TF-A v2.3
  SPMD (EL3)

Q2’20
- Hafnium transition
  trustedfirmware.org

Q3’20
- TF-A v2.4
  SPMC / Hafnium (S-EL2)

Q4’20
- Continued iterations and hardening

SPMC upstream activity
TF-A v2.4 contents and upstream activity

- TF-A
  - SPMD component
  - Power management
  - SP secure boot
  - SPM design document
- TF-a-tests
  - Bare-metal Secure Partitions
  - Multiple partitions support
  - Setup and discovery interfaces
  - RX/TX buffers, memory & device regions
  - Direct message interface

- Hafnium
  - Partition manifest parsing
  - Direct message interface
  - World switch
  - Memory sharing (early support)
  - Interrupts (early support)
End to end testing

VM endpoint
- EL0
  - Client app.
  - Kernel
  - OP-TEE driver
  - FF-A driver
  - FF-A

EL1
- OP-TEE driver
- FF-A

EL2
- Hypervisor (optional)

EL3 firmware

SP endpoint
- TA
- TA
- S-EL0
  - Secure service
- S-EL1
  - shim
- S-EL2
  - FF-A
- SPMC (Hafnium)
  - FF-A
- EL3

FF-A driver
- Client app.
- Secure service
- Shim
- FF-A
- FF-A
- FF-A
End to end testing

- Reference open-source EL3 + S-EL2 firmware
- Using standard FF-A interface
- End to end test across SW stacks (FVP - based)

EL0
- Client app.
- Kernel
- OP-TEE driver
- FF-A driver
- FF-A

EL1
- OP-TEE driver
- FF-A

EL2
- Hypervisor (optional)

EL3
- SPMC (Hafnium)
- SPMD

SP endpoint
- TA
- TA
- Secure service
- Shim

VM endpoint
- Client app.
- Kernel
- OP-TEE driver
- FF-A driver
- FF-A

S-EL0
- FF-A

S-EL1
- FF-A

S-EL2
- FF-A

S-EL3
- FF-A

FF-A
- Reference open-source EL3 + S-EL2 firmware
- Using standard FF-A interface
- End to end test across SW stacks (FVP - based)
Resources

- **TF-A Technical Forum**
  - https://www.trustedfirmware.org/meetings/tf-a-technical-forum/
  - *Secure EL2 SPM (Secure Partition Manager) Hafnium-based*
- **TF-A SPMC documentation**
- **Hafnium documentation**
  - https://review.trustedfirmware.org/plugins/gitiles/hafnium/hafnium/+/HEAD/README.md
- **FF-A specification**
- **Gerrit code reviews**
  - https://review.trustedfirmware.org/q/status:open+project:hafnium/hafnium
- **Mailing list**
  - https://lists.trustedfirmware.org/mailman/listinfo/hafnium
What is Hafnium?

- Originally a Google project
- Type-1 “bare-metal” Hypervisor running in the Normal World
- Supports AArch64 NS-EL2
- Instantiates untrusted VMs at NS-EL1
- Isolates VM memory through Stage-2 MMU
- Provides VM-to-VM communication
- Low latency primary VM schedules secondary VMs
- TEE communication infrastructure (e.g. Trusty)
- Fast build system
- Build targets FVP, QEMU, Rpi
- Hafnium test suite
Direct message request/response (FF-A v1.0)

- EL1/0
  - VM1
    - vFF-A
- EL2
  - Hypervisor (Hafnium)
    - pFF-A
- EL3
  - EL3 firmware
    - SPMD
- S-EL1/0
  - SP1
    - vFF-A
- S-EL2
  - SPMC (Hafnium)
    - pFF-A
Direct message request (FF-A v1.0)

Pinned MP vCPU# = PE#

EL1/0

Pinned MP vCPU# = PE#

S-EL1/0

EL2

Hypervisor (Hafnium)

VM1

EL3

EL3 firmware

Pinned MP vCPU# = PE#

S-EL2

SP1

SPMC (Hafnium)

Pinned MP vCPU# = PE#

Pinned MP vCPU# = PE#

vFF-A

SMC

SMC

vFF-A

vFF-A

SMC

SMC

VM1

SMC

SMC

Pinned MP vCPU# = PE#

vCPU# = PE#

vCPU# = PE#

Pinned MP vCPU# = PE#
Direct message response (FF-A v1.0)

- Pinned MP vCPU# = PE#
  - EL1/0
    - ERET vFF-A
    - EL2
      - Hypervisor (Hafnium)
        - pFF-A
      - VM1
    - S-EL1/0
      - SP1
        - SMC vFF-A
  - EL3 firmware
    - SPMD
    - ERET
    - SPMC (Hafnium)
      - pFF-A
      - SMC