arm

SMC Fuzzing Improvements

Slava Andrianov

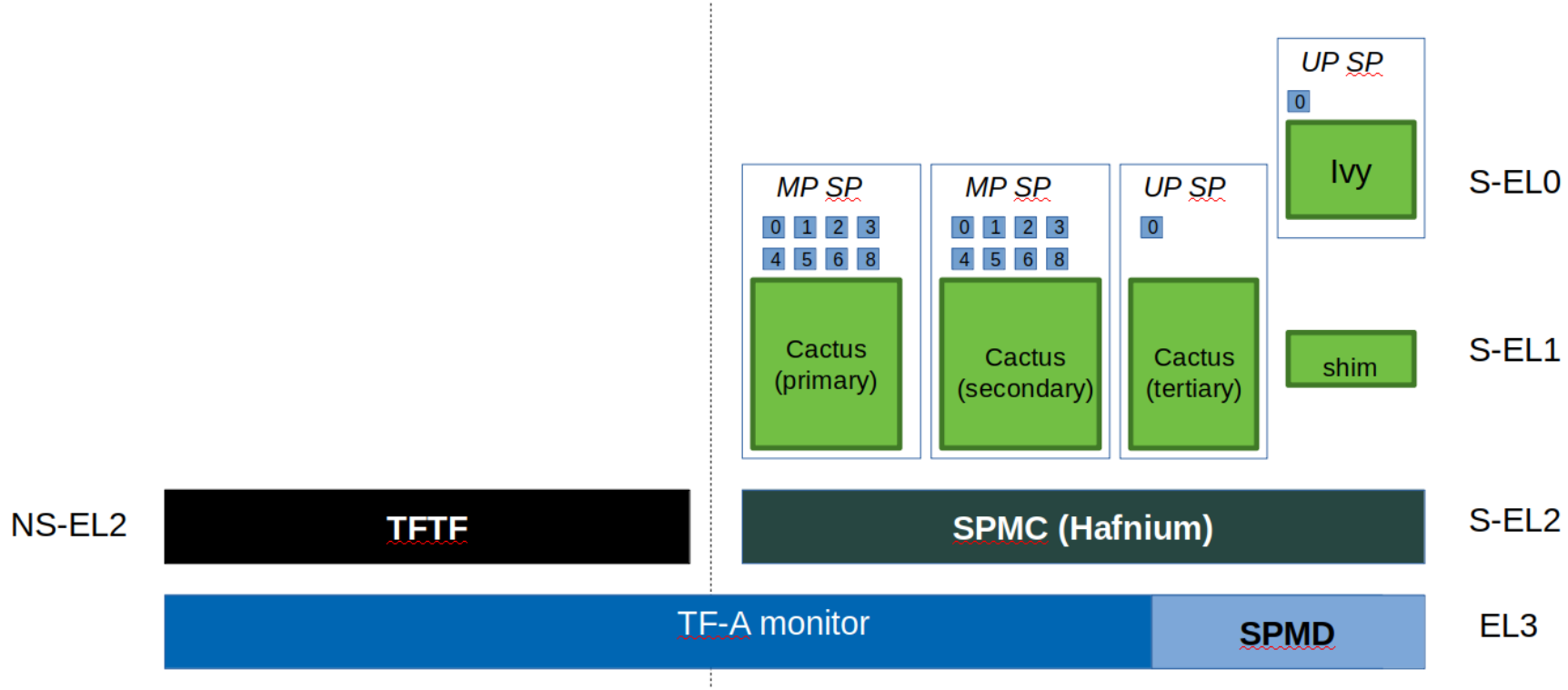
30th October 2025

Agenda

- Motivating Secure World Fuzzing
- SMC Fuzzer Improvements
- Configuring Secure World Fuzzing
- Future Work

Motivating Secure World Fuzzing

- The Firmware Framework for A profile (FF-A) specification defines how communication should happen across partition boundaries, especially in the case of communication between the secure and non secure worlds
- The secure world can have access to sensitive information and/or perform privileged actions
- Secure world partitions have multiple different states, each of which have differing restrictions on the partition's FF-A behavior

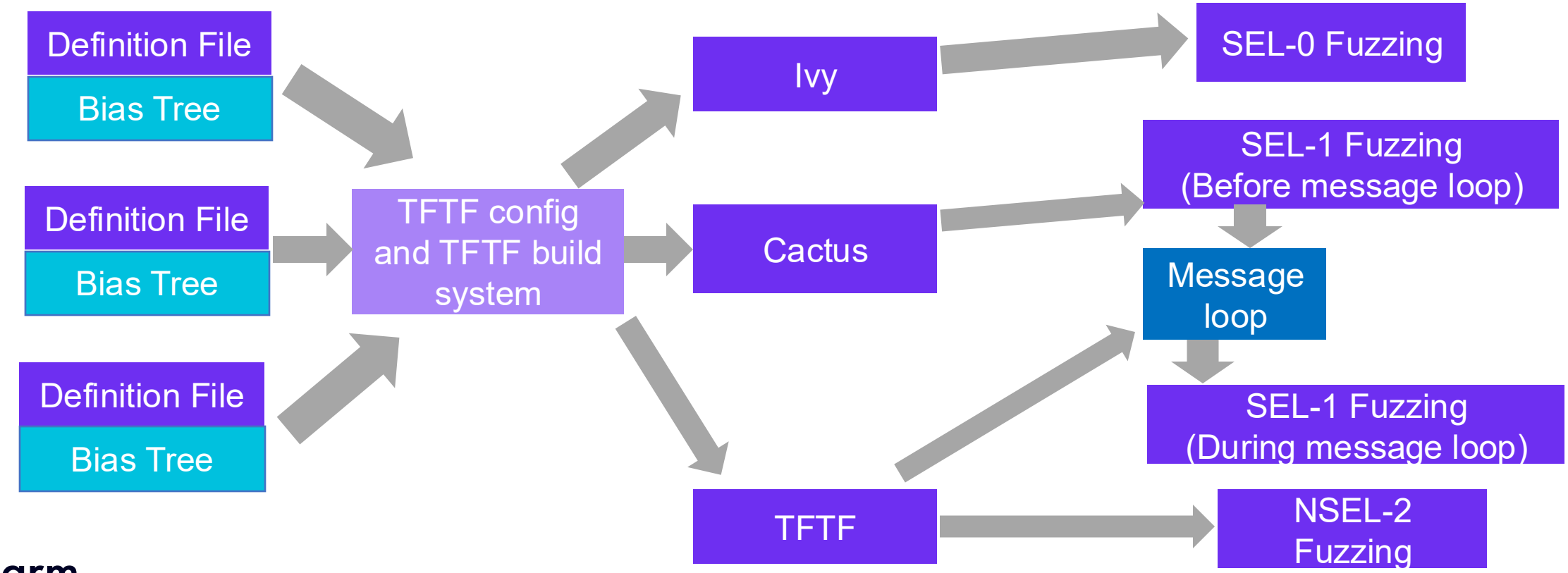


Improvements

- The SMC fuzzer can be run at SEL-1 (Cactus partition) and SEL-0 (Ivy partition) in addition to the previous NSEL-2 (tftf)
- SEL-1 fuzzing can be run before and during the message loop
  - The cactus VM with ID 1 will run its fuzzing before it enters the the cactus message loop
  - Through the cactus message loop, the non secure world can issue a cactus command to request that a secure partition run more fuzzing
- Each EL can now specialize its fuzzing through per exception level definition files and bias trees
- Can use variable coverage to get an overview of the different inputs that have been used in the fuzzing, ensuring the sufficient coverage of the possible inputs into the SMC calls.

Configuring Secure World Fuzzing

- Fuzzing configuration is primarily handled through the TFTF configuration file
- Key parameters
  - Definition file – describes the arguments of the SMC calls and the fields that make up each argument
  - Device tree source file – describes the bias tree that should be used to determine an ordering for the SMC calls
  - Test group – new tests can be added to send a message from NSEL2 to start SEL1 fuzzing



Future Work

- Per partition fuzz configuration
- Greater configurability of fuzzing for the different secure world partition runtime models
- Cactus commands to specify type of fuzzing to run in the secure world

References

- Patches
  - https://review.trustedfirmware.org/c/TF-A/tf-a-tests/+/43898
  - https://review.trustedfirmware.org/c/ci/tf-a-ci-scripts/+/44649
- TFTF SPM Tests Configuration Documentation
  - https://trustedfirmware-a-tests.readthedocs.io/en/latest/getting_started/build.html#cactus-and-ivy
- FFA specification
  - https://developer.arm.com/Architectures/Firmware%20Framework%20for%20A-Profile
- Previous presentations on FFA fuzzing
  - https://www.trustedfirmware.org/docs/TF_A_SMC-Fuzzing_100725.pdf
  - https://www.trustedfirmware.org/docs/Fuzzing-Tech-Forum-11Jul24.pdf

arm

Merci
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Thank You
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు
Köszönöm