RISC-V Summit China 2023

Enhance UEFI on RISC-V

- MultiArchUefiPkg - Bringing RISC-V and IHV Ecosystems Together
- StandaloneMmPkg - Bringing UEFI Secure Execution to RISC-V

Yong Li (yong.li@intel.com)

Andrei Warkentin (andrei.warkentin@intel.com)

Aug.23 2023

intel®

Legal Notices and Disclaimers

Statements in this document that refer to future plans or expectations are forward-looking statements. These statements are based on current expectations and involve many risks and uncertainties that could cause actual results to differ materially from those expressed or implied in such statements. For more information on the factors that could cause actual results to differ materially, see our most recent earnings release and SEC filings at www.intc.com.

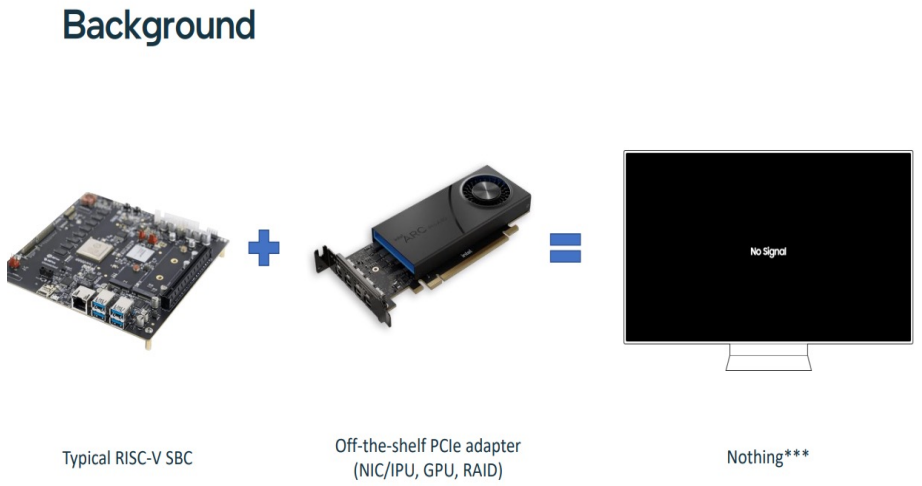
All product plans and roadmaps are subject to change without notice. Any forecasts of goods and services needed for Intel's operations are provided for discussion purposes only. Intel will have no liability to make any purchase in connection with forecasts published in this document. Code names are often used by Intel to identify products, technologies, or services that are in development and usage may change over time. No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

 This document contains information on products and/or processes in development.

MultiArchUefiPkg - Bringing RISC-V and IHV Ecosystems Together

- Today ➔ Non-standard RISC-V platforms, that don't lend to building to horizontal market segments where interoperability is key
- Tomorrow ➔ An interoperable RISC-V ecosystem that allows building servers and PCs

How to make existing PCIe devices work?
Will future PCIe devices ship with RISC-V firmware drivers?



MultiArchUefiPkg – Option ROM Emulation

Status:

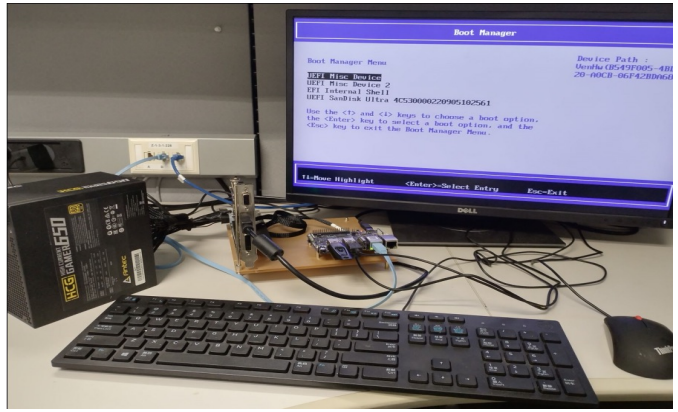
- 64-bit x64 and AArch64 instruction emulation
- Supports 64-bit RISC-V UEFI hosts
- Abstracts Qemu/TCG with Unicorn Engine API
- Verified on RiscVVirt w/ PCIE passthrough
- Verified on VisionFive2 SBC

Homepage and Source Code:

- *https://wiki.riseproject.dev/display/HOME/EDK2_00_01+-+MultiArchUefiPkg*
- *https://github.com/intel/MultiArchUefiPkg*

Next Step:

- Verify on more platforms
- Correctness, perf, code size and etc



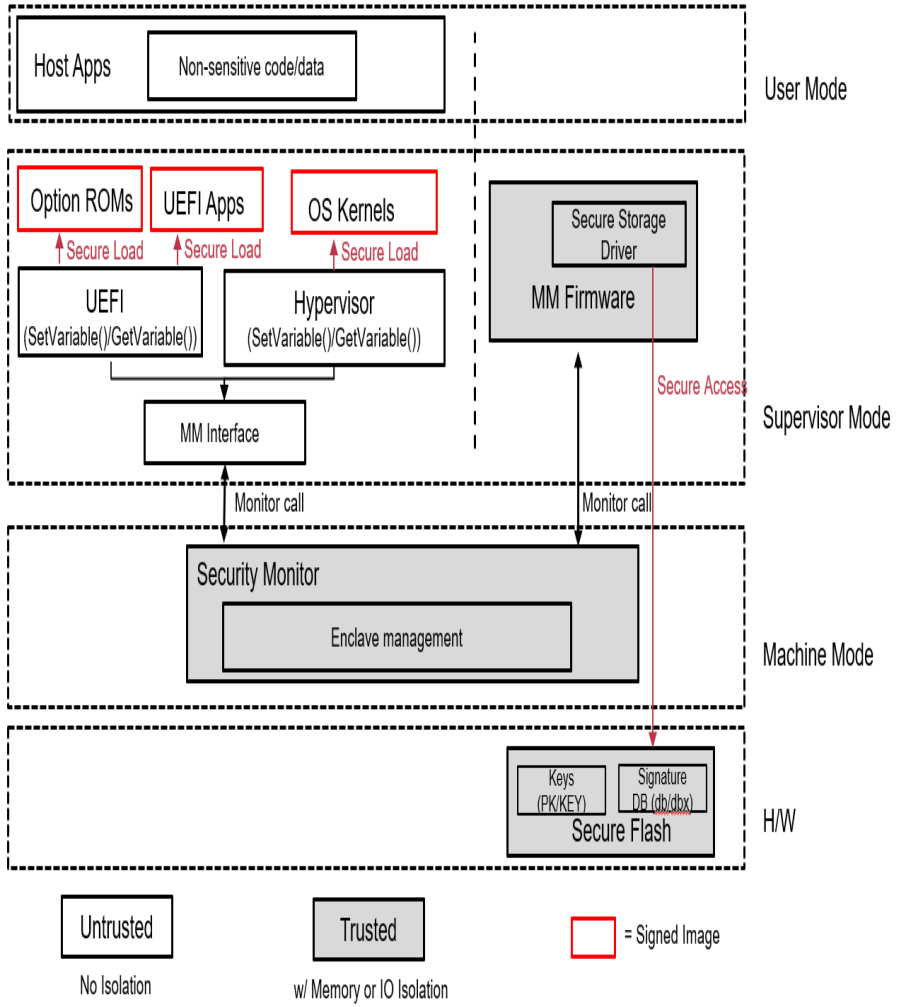

```
7A 0000000A ? - -  -  - Usb Keyboard Driver
7B 00000011 ? - -  -  - Usb Mass Storage Driver
83 13000406 ? - -  -  - Intel(R) GOP Driver [19.0.1030]
FS0:\> drivers
```

StandaloneMmPkg – Bringing UEFI Secure Execution to RISC-V

- UEFI Secure Execution Environment ➔ A software sandbox environment running in the Secure World, under the control of privileged software, to instantiate PI Standalone Management Mode, in order to execute MM (secure) services.
- Typical Use Case ➔ UEFI secure boot service do the authentication and update variables for ensuring that code launched by the UEFI firmware is trusted and that each efi payload loaded is authenticated.

How to ensure the UEFI Secure Execution on RISC-V is secure ?

How will the secure implementation be on RISC-V based servers and PCs ?



StandaloneMmPkg – UEFI Secure Service

Status:

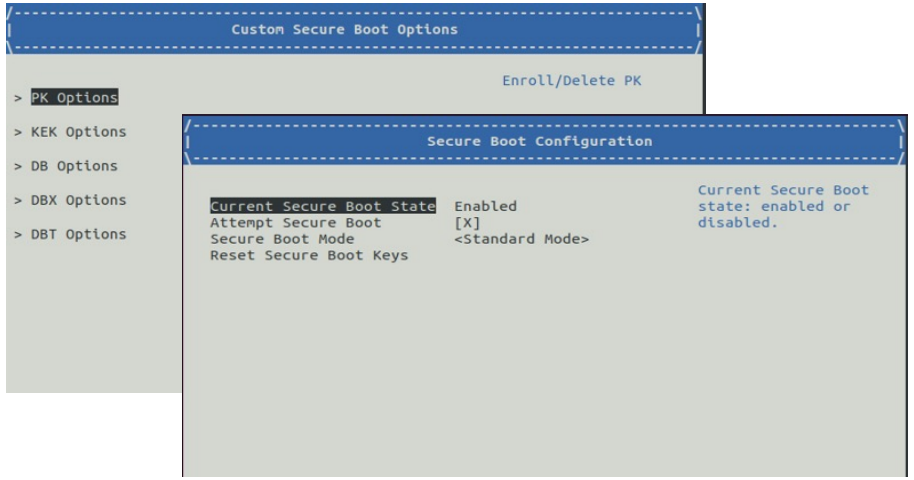
- Supports both PMP/sPMP and CoVE based TEE
- Prototyped with Penglai and Salus on QEMU
- Verified UEFI secure variables service
- Verified UEFI secure boot flow

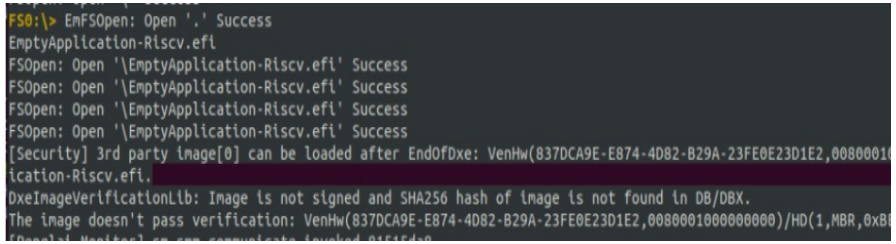
Homepage and Source Code:

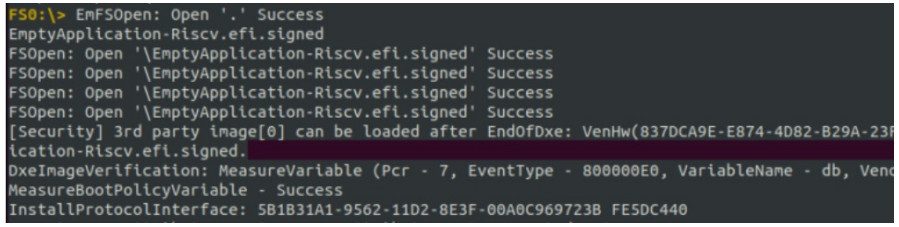
- https://wiki.riseproject.dev/display/HOME/EDK2_00_02+-+StandaloneMmPkg
- https://github.com/tianocore/edk2-staging/tree/RiscV64StandaloneMm

Next Step:

- UEFI PI and BRS-I update
- Code upstream, port to real hardware platform
- Secure firmware upgrade, management services ..







- https://riseproject.dev

RISE is focused on positive and transparent collaborations with upstream projects to deliver commercial-ready software for various use cases

https://www.intel.com/content/www/us/en/developer/articles/community/rising-to-the-challenge-risc-v-software-readiness.html

- RISE Firmware WG
  https://wiki.riseproject.dev/display/HOME/Firmware+WG
- UEFI on RISC-V Firmware Mailing List
  https://groups.google.com/a/riscv.org/g/fw-exchange
- More projects Intel China team is working on

Topic	When
RISC-V Vector Support on Valgrind	August 25 6pm
Best practice to optimize SW with vectorization on RISC-V	Poster
RISC-V firmware solution	August 24 4:30pm
Enhance UEFI on RISC-V	August 24 4:20pm
Enabling compliance test for RISC-V BRS	August 24 3pm
The ACRN/RISC-V project: embedded hypervisor design and status update	August 24 5pm

Welcome to Join RISC-V UEFI Firmware Development and Feedback Needed !


intel