Why do we need an open source approach?

• Sharing specifications with peers can advance development faster
• Compliance is critical to build up an ecosystem
• Interoperability
• No security by obscurity
• Open formal models allow to test for security issues
• Formalizing the security test tools and development tools
• Make tools available to entire community
• Reason on security models and functionality
Ways the RISCV Foundation can help...

Let’s start with a clean slate: RISCV open specifications

- Secure Processor Ingredients...
  - RISCV base Instruction Set Architecture (ratified)
  - Privilege specification defining privilege modes (Machine, Supervisor, Hypervisor, User)
  - Security Extensions:
    - Crypto extensions (Richard Newell, Microchip) and a Trusted Execution Environment TG (Joe Xie, Nvidia)

- HW ecosystem: 69 cores available here: https://riscv.org/risc-v-cores/
- Software ecosystem:
  - Simulators, Object toolchain, Debugging, C compilers and libraries
  - Boot loaders and monitors, OS and OS kernels
  - Compilers and runtimes for other languages, IDEs
  - …….. Security (!)
RISCV Foundation Task Groups relating to Security

**Crypto extensions Task Group**
(Richard Newell, Microchip
Derek Atkins, SecureRF)

- Approach based on vector extensions
- AES instructions (1 round, full round)
  - 128, 192, 256; done
- SHA-2 instructions (16 rounds, full round)
  - SHA-256 and SHA-512; almost done
- Need to convert AES and SHA-2 into specs now
- Looking into accelerating Public Key Crypto algorithms
  - Long integer arithmetic
  - Post Quantum specific extensions? NIST announced a round 3 to begin in ~June 2020 (for 18 months); standard in 2024
- Future directions:
  - More light-weight approach: could recommend subset of vector extensions only
  - XCrypto (Bristol): scalar instructions, rotates, etc. to have SW run faster

**TEE Task Group**
(Joe Xie, Nvidia
Nick Kossifidis, Forth)

- HW:
  - PMP Physical Memory Protection based on Privilege spec 1.12; poll ongoing.
  - IO PMP proposal 0.1; good feedback so far.
  - Next: Control Flow Integrity (CFI) ext.
- SW:
  - Secure Monitor architecture
  - Secure boot architecture
RISCV Foundation and GlobalPlatform

- MoU signed about two months ago;
- Makes formal liaisons possible and feedback from each other on early spec drafts
- Announced at GP Fall meetings in Madrid last month
- Most likely intersect: lightweight TEE APIs for IoT

- Common interest in:
  - TEE specifications; how to simplify for IoT versus Mobile world
  - Security certification – seeking input/feedback from RISCV Community on SESIP scheme
  - TEE protection profile already exists; GP working on a Secure MCU protection profile next
“Lando” : a formal specification language for HW design with 4 sublanguages:
- A system spec language
- Architecture language
- Product line engineering language
- Security property specification language

A domain model for specifying security properties.
- Ex: formalization of the NIST CWEs related to buffer/memory errors

BESSPIN: a tool suite for formal reasoning
- GRIFT: subsystem of tool suite already contributed to RISCV Formal TG

Platform specs and security-enriched ISA:
- Secure voting machine platform spec includes security properties/guarantees (DefCon)
- 6 other platform specs based on RISCV SoCs
Top 10 Challenges in Security for RISC-V Community

- Micro-architectural security implementation flaws
  - Regular side-channel attacks (TA, SPA, DPA)
  - Cache timing side-channel attacks
  - Speculative execution issues (Spectre, Meltdown, Foreshadow,...)

- Security Certification and Assurance
  - Open-source versus confidential/proprietary specs?
  - How to address security certification when implementation security is “out of scope”

- Post-Quantum Crypto acceleration
  - Accelerate lattice based, code based, super-singular isogeny based primitives?

- Security Vulnerabilities Disclosure program?
  - Should we have one? How to set it up?
Conclusion

- Open source approach is great
- Many new opportunities
- Thriving RISC-V ecosystem

- How to address security in the RISC-V world is a complex question
  - Most serious security issues result from micro-arch flaws
  - Many good ideas and initiatives already
  - Still many open problems to work on

Call to action!
Thank you