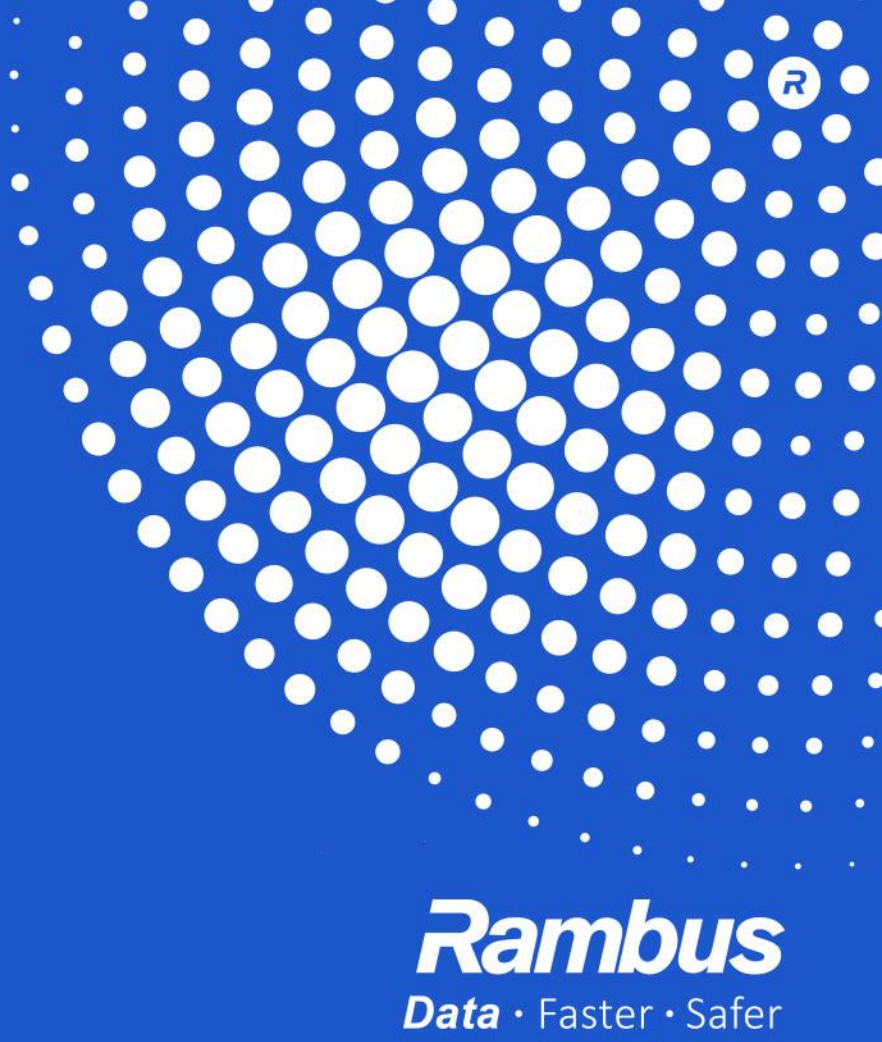
RISC V International Security Committee Meeting

Helena Handschuh, Rambus, Chair

January 20th, 2021



Antitrust Policy Notice

RISC-V International meetings involve participation by industry competitors, and it is the intention of RISC-V International to conduct all its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at RISC-V International meetings and in connection with RISC-V International activities are described in the RISC-V International Regulations Article 7 available here: https://riscv.org/regulations/

If you have questions about these matters, please contact your company counsel.

RISC-V International

RISC-V is a free and open ISA enabling a new era of processor innovation through open standard collaboration. Born in academia and research, RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and innovation.

We are a transparent, collaborative community where all are welcomed, and all members are encouraged to participate.

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

https://riscv.org/risc-v-international-community-code-of-conduct/

Agenda

- Role Call: DonB, Mark, Akira, Alric, David Kruckemyer, Greg Sullivan, Jiawei, JoeX, John Ingalls, Kuniyasu, Li Weiwei, Markku, Nate Voorhies, Rich, Stephano, Steve Cornelius, Andy Glew, Helena.
- Security Committee Charter (reminder)
- Security Response Team – status update
- Security related Task Groups – short update
  - Crypto TG
  - TEE TG
  - CMO TG → create informal fence.t group for security
- Speaker Program – proposed next speaker
- Open discussion topics (all)
- AOB

Security Committee

chair: Helena Handschuh, Rambus
vice-chair: Joe Kiniry, Galois

website: https://lists.riscv.org/g/security (internal)
mailing list: security@lists.riscv.org (public)
committee meeting documents: https://lists.riscv.org/g/security/files/Meeting%20Documents (internal)
Presentations: https://lists.riscv.org/g/security/files/Presentations (internal)
Alternating timezone meetings: Wednesdays 9:00am-10:00am PST and 4:00pm-5:00pm PST
Speaker Program: approx. every other meeting (i.e. once a month approx.)

- Security Standing Committee Charter:
  - Promote RISC-V as an ideal vehicle for the security community
  - Liaise with other internal RISC V committees and with external security committees
  - Create an information repository on new attack trends, threats and countermeasures
  - Identify top 10 open challenges in security for the RISC-V community to address
  - Propose security committees (Marketing or Technical) to tackle specific security topics
  - Recruit security talent to the RISC-V ecosystem (e.g., into committees)
  - Develop consensus around best security practices for IoT devices and embedded systems

New: Security Response Team

- Don Bailey appointed acting Chair of the new group
- Don and Helena had some introductory discussions with :
  - Alex Rice (Hacker1 crowdsourcing);
  - Cacey Alice (Bugcrowd);

- Proposed initial Charter for the new group:
- The RISC-V Security Response Team (SRT) shall be tasked with the reception, evaluation, and coordinated remediation of security flaws within the RISC-V specification. To achieve these goals, SRT shall define both policy and methodology for working with external researchers, RISC-V members, and RISC-V implementers, that clearly and easily defines each facet of the security response process. The overall goal is to ensure the integrity of the RISC-V architecture by creating an open channel for acceptance and processing of security flaws. SRT shall, where possible, work with third party organizations capable of and experienced in the vulnerability disclosure process.

- Candidates: Alistair Francis (WD); Philip Paeps (FreeBSD).
- Security Committee discussed the candidates and decided to nominate and appoint Don Bailey as Chair and Alistair Francis as Vice-Chair. Proposal is to make the group a SIG.
- Move to notify tech-lsm and tech-chairs as the next step; collected all items.
- Helena to point the two groups to the new Charter and Chair/Vice-Chair resumes.

Task Groups relating to Security – TEE TG

Joe Xie, Nvidia and Nick Kossifidis, Forth

Tuesday every other week at 8:00am pacific time

All links to specs on TEE wiki page (PMP, TBI)

ePMP

New internal poll for last minute spec update. Done with the spec.

Public review

Still waiting for CSR assignment approval. Should hopefully happen soon.

Other proposals

- TBI/PM proposal (Joined effort, with J-group)
  - -Pointer masking proposal discussed in J group. Plan to ratify in Q2. Spec is close to done. Compiler has been updated.
- sPMP and IOPMP
  - -Current plan is to get sPMP through internal TEE poll in Q1.
  - -IOPMP planning to go through internal TEE poll in Q2. Andes and SiFive have proposals. Nvidia and Microchip also have an internal implementation. Looking to unify all these into IOPMP proposal.

Task Groups relating to Security – Crypto Extensions TG

Crypto Task Group

Chairs: Richard Newell, Microchip and Derek Atkins, Veridify

Note: Full version of this update in the RISCV Member's Day folder

Scalar Cryptographic Extension:

- CSR for accessing a hardware entropy source for generating random numbers (NIST and BSI compatible)
- New dedicated instructions for AES/SHA (NIST) and SM3/SM4
- Shared with Bitmanip extension:
  - Rotations / Permutations
  - Carryless Multiply
- Email went out today calling it "stable" unless any objections; "freeze" still needs some work.
- Support on SPIKE already there. Support group being created. Could help us with additional simulation.

Vector Cryptographic extension:

- Stable for quite a while, but depends on vector being stable/frozen; hope to be part of RVA22 (planned December 2021)
- Built on top of base vector extensions; Low-latency limited-rounds instructions for AES, SHA2
- Full-rounds instructions for AES, SHA2
- Vector Bit-manip (rotate/permute/vector carryless multiply)
- SAIL models depend on vector ones, so vector crypto will move forward when vector is ready; need help from support group.

Open discussion items

- Cache timing side-channels
  - Came to realization that security and regular cache management requirements/goals may be too different from each other and not easy to put under the same hood
  - Proposal is to spin up a “fence.t” informal subgroup that can fast-track the instruction when ready
    - i.e. cache flush operations when switching security domains etc. AISA etc.(Gernot’s proposal)
    - Academic paper available and video from the Summit. Slides available from Andy. Rich to send pointers.
  - Andy proposing to give the Security Committee an overview of current cache management proposal at next SSC meeting.
- Security Reviews:
  - In discussing the newly created Security Response Team SIG it was suggested that we might also need another HSC/SIG that would deal with spec reviews produced by other TGs within RISCV, in addition to a Security Incident Response Team that will deal with externally submitted security vulnerability disclosures.
  - To be discussed at next SSC meeting.
  - Current Security TGs build their extensions with security as a primary goal, but other specifications would benefit from security reviews as well, i.e. Debug etc.
- GlobalPlatform TEE APIs
  - Kuniyasu (AIST) published a new paper about performance evaluation and comparison of the GP TEE APIs on Intel SGX and RISCV Keystone
  - Posted into RISCV internal website in Security Folder under Publications

AOB

Thank you!

Speaker Program

- Gernot Heiser from Data61 on Timing Attacks:
  - Propose creating a Flush instruction and partitioning as mitigation
- Dayeol Lee from Berkeley on the Keystone project (TEE TG):
- Jose Renau from Esperanto on Timing Attack Mitigation Ideas
  - Propose using TimeDomain IDs and other ideas for mitigations
- Jon Geater from Thales provided insights into Trustzone and TEEs (TEE TG)
- Daniel Genkin: Foreshadow
- Stefan Mangard from IAIK Graz : side-channel attacks, control flow integrity, secure memory access
- NXP: SESIP light-weight certification scheme for IoT
- Nicole Fern from Tortuga Logic presented on their security verification tool
- Ted Speers: Vision for the Future in Security for RISCV Foundation
- Gil Bernabeu, Introduction to GlobalPlatform
- Ben Marshall, Xcrypto extensions (not based on vector extensions)
- Greg Sullivan, Dover Microsystems on CoreGuard
- Martin Maas, Google on J extension
- Robert Watson, Cambridge on CHERI
- Dominic Rizzo, lowRISC on OpenTitan
- Gernot Heiser, Timing Fences
- Patrick Schaumont, WPI, Domain-oriented masking for RISCV ISA
- Tim Fritzmann, Georg Sigl, RISQ-V extensions for PQC
- Planning to Invite: David Oswald, Platypus

- **Next:**
  - Earlier suggestions
    - Yunsi Fei, Georgia Tech; RISCV Boom with side-channel protections?
    - Power management attacks:V0LTpwn? https://arxiv.org/pdf/1912.04870v1.pdf
  - CHES 2020: FENL paper?

Backup: communication from GP director

1 – TEE lightweight configuration

The TEE committee has confirmed interest to create a simplified TEE configuration and would like to listen to RISC-V requirements .
FYI, GlobalPlatform publishes Configuration specifications - implementation guide of a reduced set of features from specification to address specific market.
This publication effort can be expedite quickly (<100 days) . We'd like to set up a conf call with the TEE group in order to understand RISC-V scope and start the publication process.
Could you help us to invite the right RISC-V expert?

2 – SESIP evaluation methodology

GlobalPlatform has started a public review of a new security evaluation methodology for IoT Platform.
Details are available at : https://globalplatform.org/specifications/for-public-review/
The Public review ends on January 10th
Could you please transfer the public review details to your group so we can have RISC-V comments ?

We'd like to make a presentation to your group as this evaluation methodology answers today's IoT market requirements to manage security evaluation in an optimized process. We'll be excited to make a presentation about SESIP in a future RISC-V meeting.

3 – Protection profile.

GlobalPlatform has published a TEE protection profile that can be used for TEE security evaluation.
The protection profile is available at : https://www.commoncriteriaportal.org/files/ppfiles/anssi-profil_PP-2014_01.pdf

We are planning to create a Secure micro controller Protection profile and we'll be also interested to present an overview of this document in May/June time frame.

Taxonomy and Formal reasoning (Galois, DARPA SSITH program)

note: not formally part of RISCV Foundation, to be contributed when/if DARPA greenlights

- Galois has built the infrastructure, target platforms, and put secure RISC-V SoC into AWS's F1 EC2 platform for DARPA's first ever bug bounty program. See https://fett.darpa.mil/
- Galois taped out their third ASIC and are working on their fourth (a high-assurance multi-core RISC-V with crypto, image, and AI accelerators) and have a new version of their EDA tool suite for security analysis underway.
- BESSPIN tool suite: currently supports CPUs and SoCs built with Chisel, Bluespec, SystemVerilog, and Verilog, simulation and emulation with Verilator, Bluespec, high-end FPGA dev boards, commercial simulators, and AWS F1, three different OSs (FreeRTOS, Linux, and FreeBSD), and several compiler toolchains (gcc, clang, and several research forks of clang/llvm).
- Galois does not expect to be able to share more of BESSPIN tool suite publicly for now
- Results of FETT program perhaps publishable fall of next year, or later if second FETT program