

RISC V International Security Committee Meeting

Helena Handschuh, Rambus, Chair

March 17th, 2021



Rambus
Data • Faster • Safer

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: Don, Allen, Andrea, Axel, Ben, Michael, Christoph, Colin, Gary, Karl, Leo, Markku, Morten, Patty, Paul, Philipp, Steve, Tariq, Thomas, Alistair, Rich, Helena.
- [RISCV Forums: Security](#) – event on April 14th (7-10am PST); program to be published soon.
- Elections : TG chairs/vice-chairs have been elected, upcoming HC/IC elections
- Security related Task Groups – updates
 - Security response team (SIG)
 - Crypto TG
 - TEE TG
 - Blockchain SIG – formal vote
 - CMO TG → create informal fence.t group for security
- Speaker Program – [Andy Glew presented fence.t proposal](#)
 - Continue discussions today
 - Next Speaker: trying to invite Todd Austin, Morpheus
- Open discussion topics (all)
- AOB

Security Committee (created in July 2018)

chair: Helena Handschuh, Rambus

vice-chair: Joe Kiniry, Galois

website: <https://lists.riscv.org/g/security> (internal; moving to Github soon).

mailing list: security@lists.riscv.org (public)

committee meeting minutes: <https://lists.riscv.org/g/security/files/Meeting%20Notes> (internal)

Presentations: <https://lists.riscv.org/g/security/files/Speaker%20Program> (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

TG Chair/Vice-Chair Election results (March 15th)

The following chairs will be seated as of April 1, 2021, with the next election scheduled for Q1 2022. Congratulations to all new chairs, as well as those returning for another year of service.

Bit Manipulation	Ken Dockser	Qualcomm	Claire Wolfe	YoSysHQ
Vector Extension	Krste Asanovic	SiFive	Roger Espasa	Semidynamics
J Extension	Martin Maas	Google	Gap	
P Extension	Chuanhua Chang	Andes	Wei Wu	ISCAS
Zfinx	Tariq Kurd	Huawei	Gap	
Cryptographic Extensions	Richard Newell	Microchip	Derek Atkins	Individual
Virtual Memory	Dan Lustig	NVIDIA	Andrea Mondelli	Huawei
FastER Interrupts	Dan Smathers	Seagate	Kevin Chen	Andes
Trusted Execution Environment (TEE)	Nick Kossifidis	FORTH	Paul Ku	Andes
Configuration Structure	Tim Newsome	SiFive	Abner Chang	Individual
Debug	Tim Newsome	SiFive	Paul Donohue	Ventana
E-Trace	Gajinder Panesar	Mentor/Siemens	John Rayfield	Individual
Nexus	Robert Chyla	IAR Systems	Bruce Abledinger	SiFive

Security Response Team (SIG) - update

- Don Bailey appointed as Chair and Alistair Francis appointed as Vice-Chair.
 - Next step: need final charter.
- 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.
- Don and Helena had a second call with HackerOne to discuss the platform they offer for encouraging hackers and security experts to take a look at our work products, i.e. ISA specifications and extensions; the platform allows to submit security vulnerability disclosures and to discuss possible solutions, and file CVEs

Task Groups relating to Security – Crypto Extensions TG

Crypto Task Group

Chairs: Richard Newell, Microchip and Derek Atkins, IC

Meetings every Thursday 10:00am pacific (please check your timezone wrt daylight saving)

Status page on the Wiki. Scalar in opcode and consistency review; few/no waivers needed.

https://docs.google.com/document/d/1QF_T7oJxv4eqg0x1-MysMnIGpqQHT_j6cDmktg4UbE4/edit
CSR proposal https://docs.google.com/document/d/10Do1nh-v25TJWTRaVjLC19P0_TwJsnioAq2iVjyDocQ/edit#heading=h.jb45dbgegyfc

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
- *Technical Lab Partners* now helping out: IIT Madras and PLTC; helping finish the missing items to get us to ratification
- Discussion ongoing about data-independent timing; timing should not leak the secret data; how to indicate/mandate/query this?

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.

Task Groups relating to Security – TEE TG

Joe Xie, Nvidia and Nick Kossifidis, Forth

Tuesday weekly meetings 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.

There is a LowRISCV implementation and a Seagate implementation; see if we can use their implementations as PoCs.

Public review

Still waiting for CSR assignment approval. Currently top of the list in O&C review. Should hopefully happen soon.

Other proposals

- Lightweight TEE discussion; sort of privilege level on m-mode; early stage; idea is to cover scenarios where we do not have s-mode; how to run third party service isolated on m mode?
- fast context switch between PMP settings; also early stage discussions
- 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.
 - Need to discuss how sPMP will work with hypervisor extension
 - IOPMP planning to go through internal TEE poll in Q2. Andes and SiFive (Worldguard) have proposals. Nvidia and Microchip also have an internal implementation. Looking to unify all these into IOPMP proposal. Draft on Wiki.

Need a security rep at the profiles meeting/group/email list; waiting for Krste to publish first draft to review.

Profiles (annual cadence) reassembling extensions that are already ratified. K extension will be in focus.

Platform (2 year cadence) trying to include K extension to some extent as well. Recommend K optional for RVM22.

Timelines may not match up to include both Bitmanip and K extension. Specs need to be ratified by Nov 15th.

Blockchain SIG creation

- Preliminary Charter:

The Blockchain SIG is proposed to develop a strategy and provide oversight for blockchain technology and solutions in RISC-V architecture and software ecosystem. The goals are to ensure there are no gaps in the ISA or software and it meets or exceeds industry expectation in performance and security (e.g. privacy-preserving, cryptographic algorithms, Trusted Execution, data ownership, integrity, provenance, etc.)

In addition, the Blockchain SIG will work with the Implementation HC to make sure someone in the community develops a RISC-V based Proof of Concept (PoC) to ensure the whole stack from HW to SW meets the goals. As with all groups, the SIG will engage and interact with other appropriate committees and groups.

- Appointed Chair and Vice-Chair of Blockchain SIG:

- Patty Tu, Wxblockchain
- Gary Xu, aitos.io

- Call for candidates went out on the tech announce list 3 weeks ago.
- Patty Tu and Gary Xu are candidates for their respective roles; no further resumes were received. Patty and Gary introduced themselves to the Security Committee Members.
- Security HC discussed and appointed Patty and Gary as Chair and Vice-Chair of the Blockchain SIG. Congratulations!
- Current preliminary Charter will be finalized now that SIG is formally created.

Speaker Program – Andy Glew, SiFive

- Fence.t proposal, i.e. Cache Management for Security purposes
- **Slides posted here:**
- <https://github.com/AndyGlew/comp-arch.net/blob/master/FENCE.T%20%2B%20security%20flushes%20-%20Ri5%20Security%20Committee%20-%202021-02-17.pptx>
- <https://github.com/AndyGlew/comp-arch.net/blob/master/FENCE.T%20%2B%20security%20flushes%20-%20Ri5%20Security%20Committee%20-%202021-02-17.pdf>
- Earlier proposal from ETH Zurich (Rich will provide link)
- Recording of the presentation posted in security group folder here:
<https://lists.riscv.org/g/security/files/Speaker%20Program>
- Proposal is to create a small group to have more focused technical discussions.
- Will revert results after some discussion to this group to see if a concrete proposal can be fast-tracked.

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 sent pointers.
 - Andy gave the Security Committee an overview of current cache management proposal. Discussions ongoing.
- 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 RISC-V, in addition to a Security Incident Response Team that will deal with externally submitted security vulnerability disclosures.
 - Need a security rep at the profiles group meetings/email discussions
 - 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 RISC-V Keystone
 - Posted into RISC-V 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 RISC-V 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 RISC-V ISA
- Tim Fritzmann, Georg Sigl, RISQ-V extensions for PQC
- Andy Glew, SiFive on fence.t proposal
- Planning to Invite: David Oswald, Platypus
- Reached out to Todd Austin, Morpheus

• Next:

- Earlier suggestions
 - 🔗 Yunsu Fei, Georgia Tech; RISC-V Boom with side-channel protections?
 - 🔗 Power management attacks: VOLTpwn? <https://arxiv.org/pdf/1912.04870v1.pdf>
- CHES 2020: FENL paper?

Communication from GlobalPlatform 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.