Security HC meeting

Jan 06, 2022

Only RISC-V Members May Attend

- Non-members are asked to please leave except for Joint Working Groups (JWG).
- Members share IP protection by virtue of their common membership agreement. Non-members being present jeopardizes that protection. Joint working groups (JWG) agree that any IP discussed or worked on is fully open source and unencumbered as per the policy.
- It is easy to become a member. Check out riscv.org/membership
- If you need work done between non-members or or other orgs and RISC-V, please use a joint working group (JWG).
    - used to allow non-members in SIGs but the SIGs purpose has changed.
- Please put your name and company (in parens after your name) as your zoom name. If you are an individual member just use the word “individual” instead of company name.
- Non-member guests may present to the group but should only stay for the presentation. Guests should leave for any follow on discussions.

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.

Collaborative & Welcoming Community

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 are a continuous improvement organization. If you see something that can be improved, please tell us. help@riscv.org

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

https://riscv.org/community/community-code-of-conduct/

Conventions

- Unless it is a scheduled agenda topic, we don’t solve problems or detailed topics in most meetings unless specified in the agenda because we don’t often have enough time to do so and it is more efficient to do so offline and/or in email. We identify items and send folks off to do the work and come back with solutions or proposals.
- If some policy, org, extension, etc. can be doing things in a better way, help us make it better. Do not change or not abide by the item unillaterly. Instead let's work together to make it better.
- Please conduct meetings that accommodates the virtual and broad geographical nature of our teams. This includes meeting times, repeating questions before you answer, at appropriate times polling attendees, guide people to interact in a way that has attendees taking turns speaking, …
- Where appropriate and possible, meeting minutes will be added as speaker notes within the slides for the Agenda

Risc-V Security

Agenda

- Revised IOPMP TG charter
- Sec HC materials for BoD and LF; will use latest Security Direction materials: https://github.com/riscv-admin/security/blob/main/topics/RiscV%20security%20direction%20Jan%202021_v3a.pptx
- Proposal for Russian Crypto TG
- Status/updates for TEE TG, Blockchain SIG, Trusted Computing SIG, CFI SIG, uArch SIG

IOPMP TG

- Acting Chair – Paul Ku
  - VC ?
  - Process to request TG creation

IOPMP Charter proposal

Security of a platform is an ever-present issue, and a fundamental requirement of security is memory isolation. CPUs are not the only agents able to access memory, however. Other bus masters in a platform, e.g., DMA or GPU, can as well. While a RISC-V hart has a PMP/ePMP, SMPU, or MMU to control its accesses, a mechanism is also needed to control accesses from those bus masters.

The protection mechanisms inside a hart, e.g., PMP/ePMP, SMPU, or MMU, create memory isolations according to hart's mode. These mechanisms check every access issued from the hart. However, the other bus masters do not usually have any similar checking mechanism. Thus, these bus masters can access anywhere. Besides, A bus master could access crossing the regions belonging to multiple harts' modes or could access only a subset of the region belonging to a hart's mode. That is, we think the memory view of a bus master should be orthogonal to that of a hart. The IOPMP will associate a bus master to the corresponding regions in its own way. Thus, the Memory Domain was introduced as the memory view of a bus master. Besides, the IOPMP is also designed for a system not equipping MMU, such as MCU or IoT with limited memory. Consequently, the current RISC-V memory protection mechanism cannot fully cover the IOPMP's targets.

A software solution has been proposed and implemented for RISC-V that requires each memory transfer request to be checked by higher-privileged software before being performed. However, it suffers from longer latency and is challenging to extend to complex bus masters, e.g., GPU or DSP, which can take a program as an input. This TG will define the IOPMP that will check transactions on the fly and stop those with any violations.

The IOPMP Task Group will deliver an IOPMP architectural specific as a reference for the developers of a new project or an extension of a legacy project. Platforms are diversified and have different latency, performance, area, capacity, and portability requirements. The architectural definition will cover platforms with a range of scales, bus masters, and bus protocols will enable the integration of legacy platforms into the RISC-V ecosystem. Consequently, the Task Group will define several options, standard models, and extensions to accommodate different requirements. Due to a certain number of options and models, we need to take portability into consideration. Besides the configuration structure under discussion, we will also provide a procedure of standard model discovery.

In the TEE Task group, we have already discussed and will incorporate:
(1) how to associate a bus master with a set of rules,
(2) how to protect the rules and related settings,
(3) the atomicity and consistency issue when programming an IOPMP, and
(4) the standard procedure for model discovery.
The IOPMP will complete this existing foundation by incorporating the above in a specification and further defining
- register definitions,
- reactions to an access violation (including the AIA supporting),
- additional usage cases, and
- analysis of IOPMP attacks.

Besides the specification, we will provide a simulator. If the resource is available, we will also provide test cases and the reference code for a security monitor manipulating the IOPMPs.

We are aware of some related items not included in this version. If we receive the requests and agree, we may cover the following items in the future version:
- the error handling of speculative accesses,
- the mitigation of deny-of-service and side-channel attacks,
- supporting NoC,
- the interactions with the caches and the cache manipulation operations,
- programming the source ID, or
- supporting multiple VMs in a hart with different permissions.

Material for BOD, LF

- https://github.com/riscv-admin/security/blob/main/topics/RiscV%20security%20direction%20Jan%202021_v3a.pptx

Russian Crypto

- Separate TG proposal, Alexander Kozlov offered to be acting chair
- Process to request TG formation

Proposed GOST-TG Charter

RISC-V International is committed to helping members succeed in specialized and regional markets where the flexibility of the RISC-V ISA offers a unique advantage in relation to cryptographic algorithm support and performance.

The focus of the GOST-R Crypto Extension TG (GOST-TG) is to investigate, evaluate, and specify ISA extensions for the implementation of Russian defined-symmetric cryptography. The main algorithms in scope are defined in GOST R 34.12-2015 ("Kuznyechik" and "Magma" block ciphers) and GOST R 34.11-2012 ("Streebog" cryptographic hash function). The goal of the extension is to both improve performance and also to reduce the risk of security vulnerabilities such as timing attacks in RISC-V cryptographic stacks. Quantitative analysis (e.g. modes of operation) is primarily based on use cases in IETF, ETSI, and 3GPP/5G security protocols and required platform security features. The TG may propose both stand-alone extensions and ones that work in conjunction with other extensions (such as vector, scalar cryptography, and bit manipulation).

NOTE. The initial algorithm selection rationale is from GOST / TLS 1.2 (https://www.ietf.org/id/draft-smyshlyaev-tls12-gost-suites-18.html) and GOST / TLS 1.3 (https://www.ietf.org/id/draft-smyshlyaev-tls13-gost-suites-05.html) which themselves correspond to ratified standard protocol specifications R 1323565.1.020-2020 and R 1323565.1.030-2020.

--- end charter proposal ---

Motivational summary for GOST-TG (which is slightly narrower):

- Gap to be filled: A market for processors and coprocessors supporting G
OST-R cryptography exists in Russia, and RISC-V members are well-positioned to meet this demand. There are regulations in place that mandate the use of these algorithms in some use cases. RISC-V already supports equivalent Chinese national ciphers and hashes SM4 and SM3 (as does ARM).

- Deliverables: An optional ISA extension for specific Russian national ciphers. The deliverables match CETG Definition-of-Done: Technical rationale, ISA definitions, specification document, architectural compatibility tests, SAIL, opcode allocation, compiler support, etc. The scope is limited to symmetric cryptography ("Kuznyechik", "Magma", and "Streebog") on both RV32 and RV64.

Other Status Updates

- TEE TG – Nick
- Blockchain SIG - Patty
- Trusted Computing SIG - Suresh
- CFI SIG - George
- uArch SIG - Ronan

- Securty Model – Suresh / Don ?

Open Action Items

Running list of open AI’s