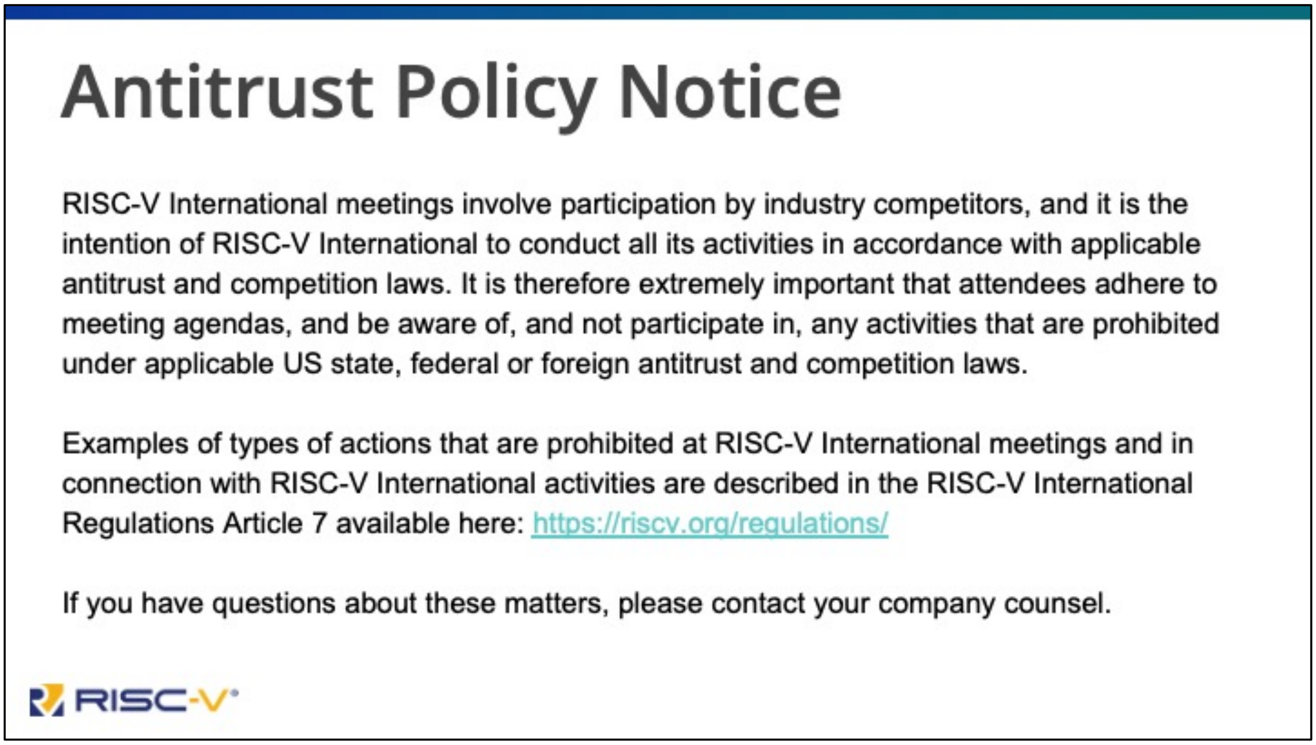
RISC-V®

Security HC

2nd September 2021

Meeting notes from the Security HC call, 2nd September 2021



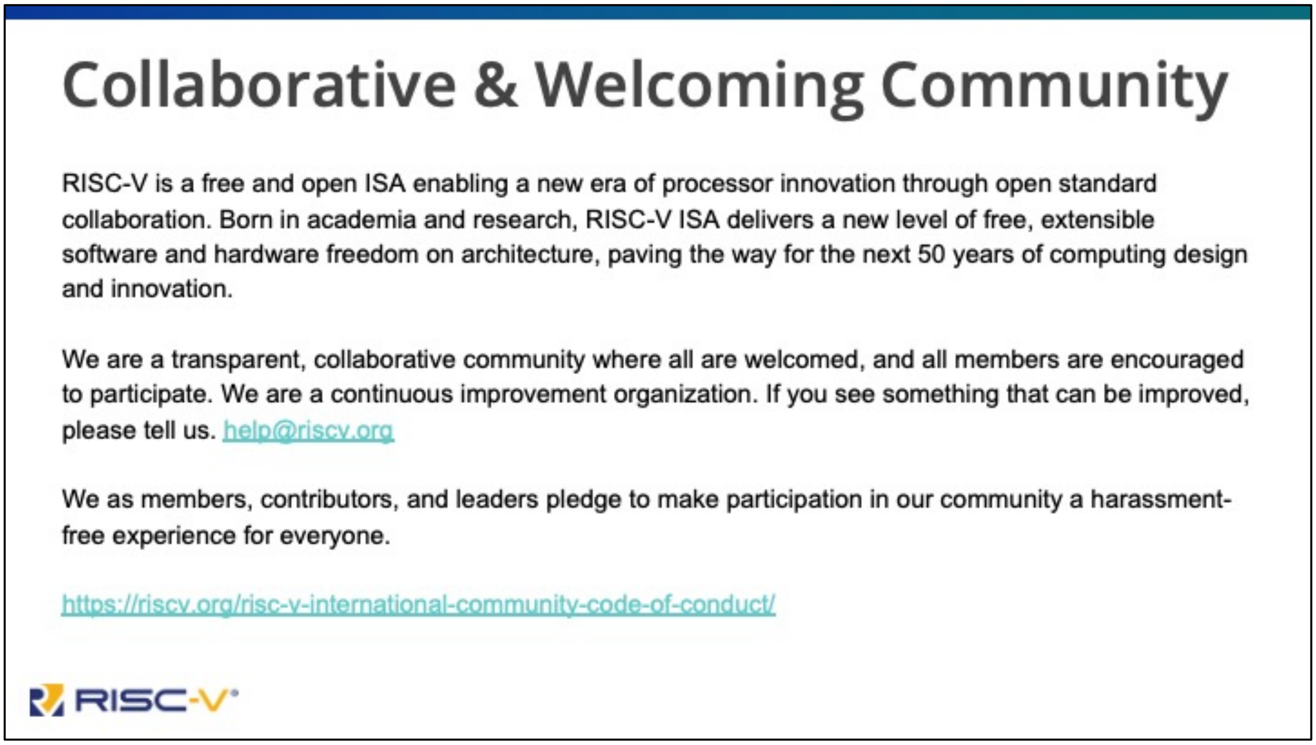
Antitrust Policy Notice

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



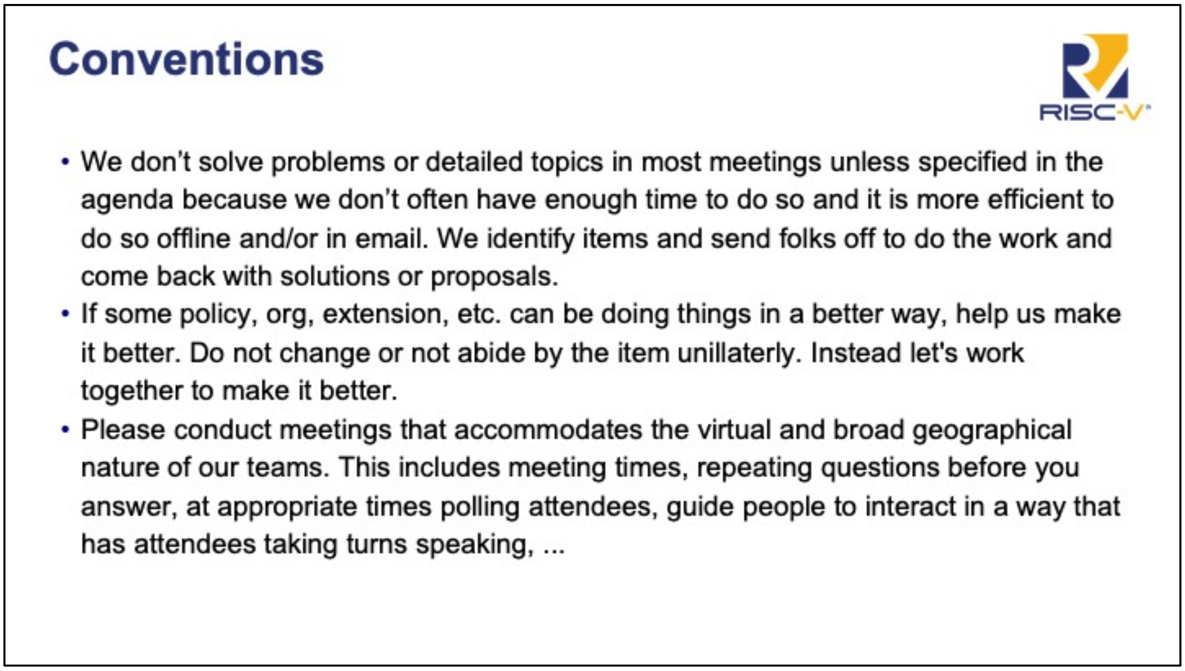
Collaborative & Welcoming Community

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

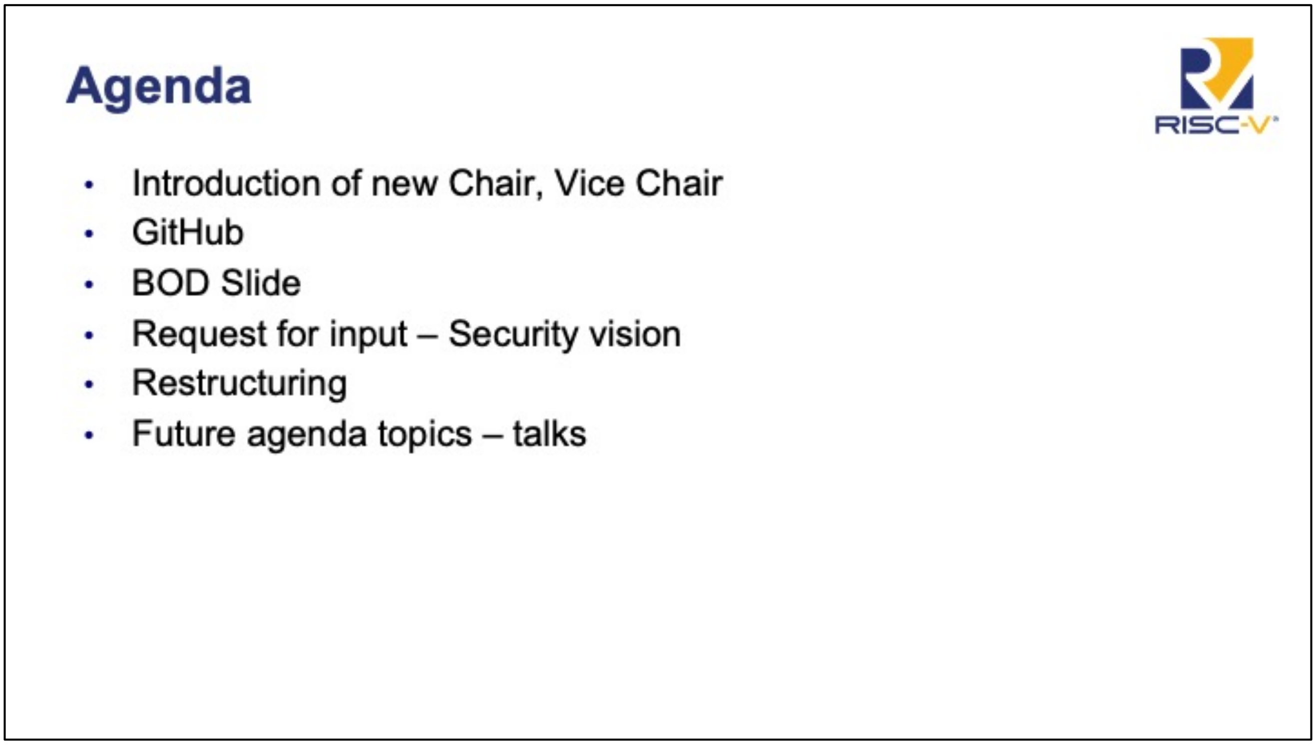
We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

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



Conventions

- 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, ...



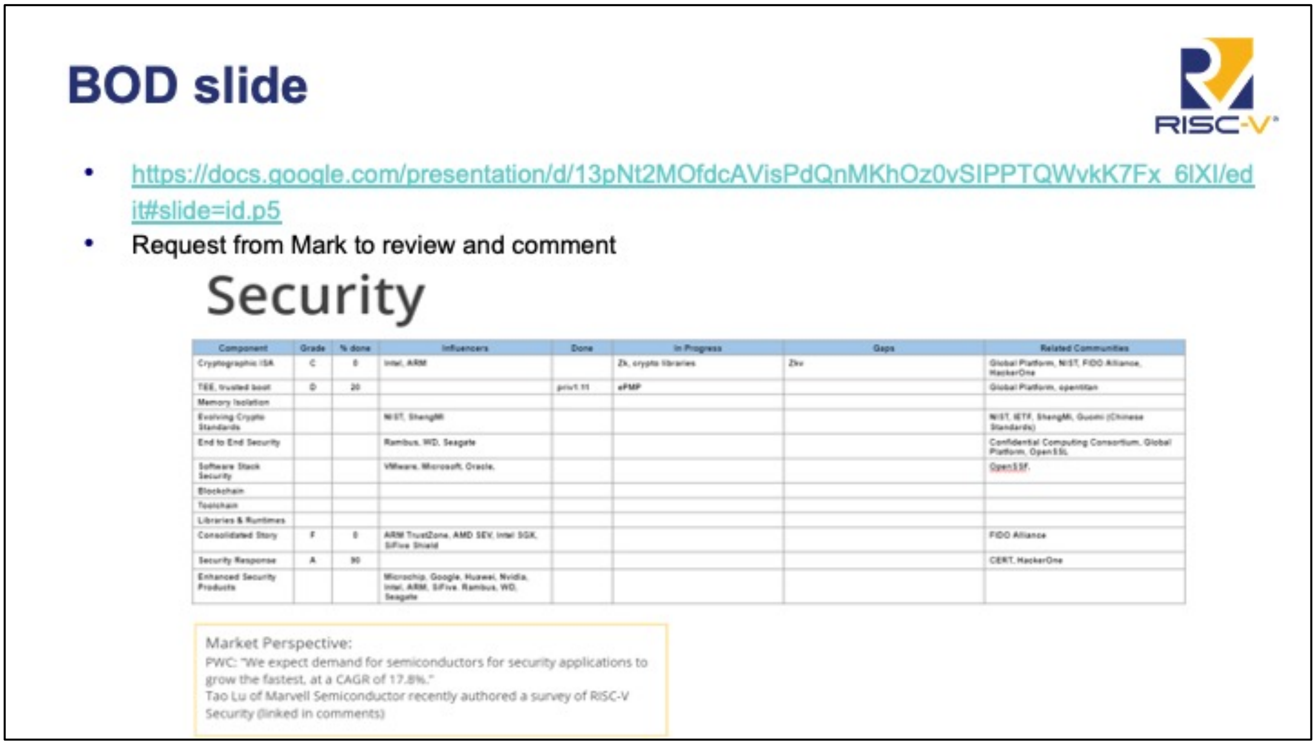
Agenda

- Introduction of new Chair, Vice Chair
- GitHub
- BOD Slide
- Request for input – Security vision
- Restructuring
- Future agenda topics – talks

- Introductions from Andrew and Manuel as new chair and vice chair.
  - Thanks to Helena for her excellent work previously

- Mark led the congratulations to the Scalar Crypto extension team on their imminent public review

- Manuel introduced the Github repo for the security HC.
  - This years notes have been ported across to github, older notes are available on the legacy systems
  - https://github.com/riscv-admin/security



BOD slide

- https://docs.google.com/presentation/d/13pNt2MOfdcAVisPdQnMKhOz0vSIPPTQWvkK7Fx_6lXI/edit#slide=id.p5
- Request from Mark to review and comment

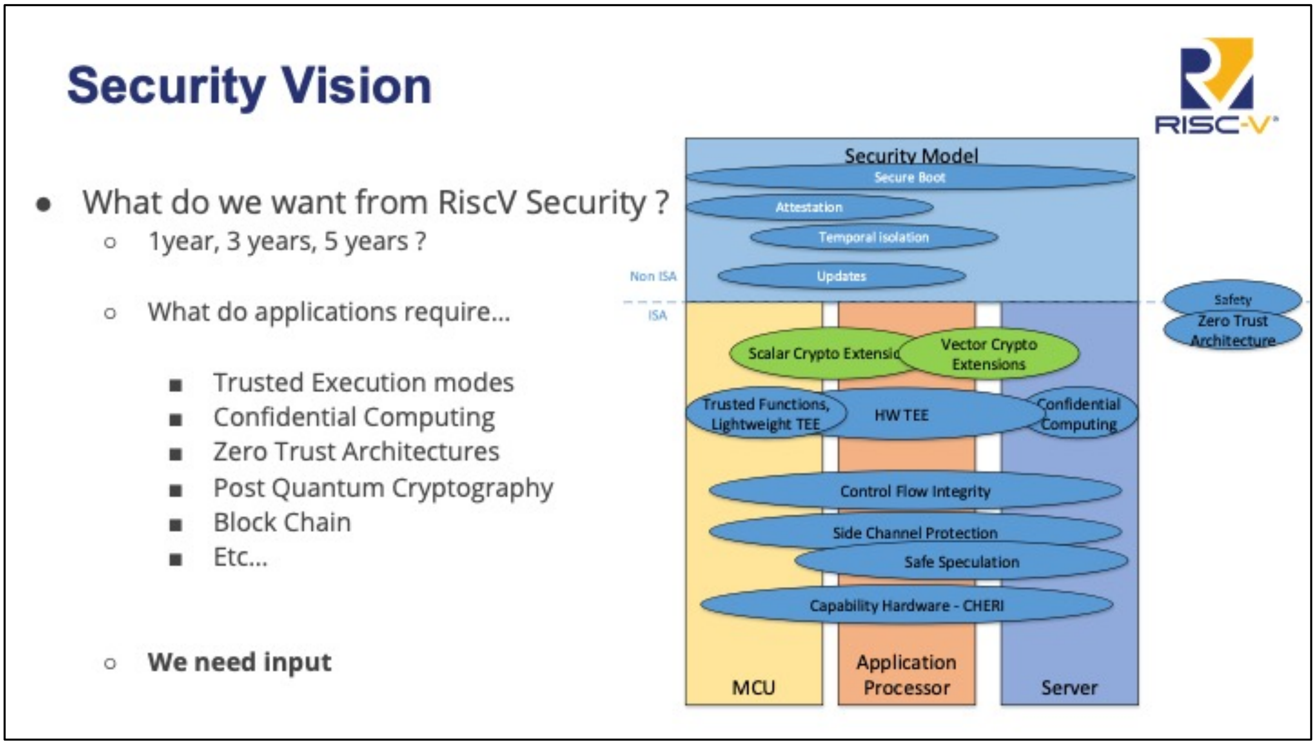
Security

Component	Grade	% done	Influencers	Done	In Progress	Gaps	Related Communities
Cryptographic ISA	C	0	Intel, ARM		Zk, crypto libraries	Zkv	Global Platform, NIST, FIDO Alliance, HackerOne
TEE, trusted boot	D	20		priv1.11	ePMP		Global Platform, opentitan
Memory Isolation							
Evolving Crypto Standards			NIST, ShengMi				NIST, IETF, ShengMi, Guomi (Chinese Standards)
End to End Security			Rambus, WD, Seagate				Confidential Computing Consortium, Global Platform, OpenSSL
Software Stack Security			VMware, Microsoft, Oracle,				OpenSSF,
Blockchain							
Toolchain							
Libraries & Runtimes							
Consolidated Story	F	0	ARM TrustZone, AMD SEV, Intel SGX, SiFive Shield				FIDO Alliance
Security Response	A	90					CERT, HackerOne
Enhanced Security Products			Microchip, Google, Huawei, Nvidia, Intel, ARM, SiFive, Rambus, WD, Seagate				

Market Perspective:
PWC: "We expect demand for semiconductors for security applications to grow the fastest, at a CAGR of 17.8%."
Tao Lu of Marvell Semiconductor recently authored a survey of RISC-V Security (linked in comments)

- New ‘Report Card’ format for reporting to the board.
- Request from mark that folks spend a few minutes to directly edit and update this slide – we may need to amend the content lines

- https://docs.google.com/presentation/d/13pNt2MOfdcAVisPdQnMKhOz0vSIPPTQWvkK7Fx_6lXI/edit?usp=sharing



Security Vision

- What do we want from RiscV Security ?
  - 1year, 3 years, 5 years ?
  - What do applications require...
    - Trusted Execution modes
    - Confidential Computing
    - Zero Trust Architectures
    - Post Quantum Cryptography
    - Block Chain
    - Etc...
  - **We need input**

Security Model

Secure Boot

Attestation

Temporal isolation

Updates

Non ISA

ISA

Safety

Zero Trust Architecture

Scalar Crypto Extensio

Vector Crypto Extensions

Trusted Functions, Lightweight TEE

HW TEE

Confidential Computing

Control Flow Integrity

Side Channel Protection

Safe Speculation

Capability Hardware - CHERI

MCU

Application Processor

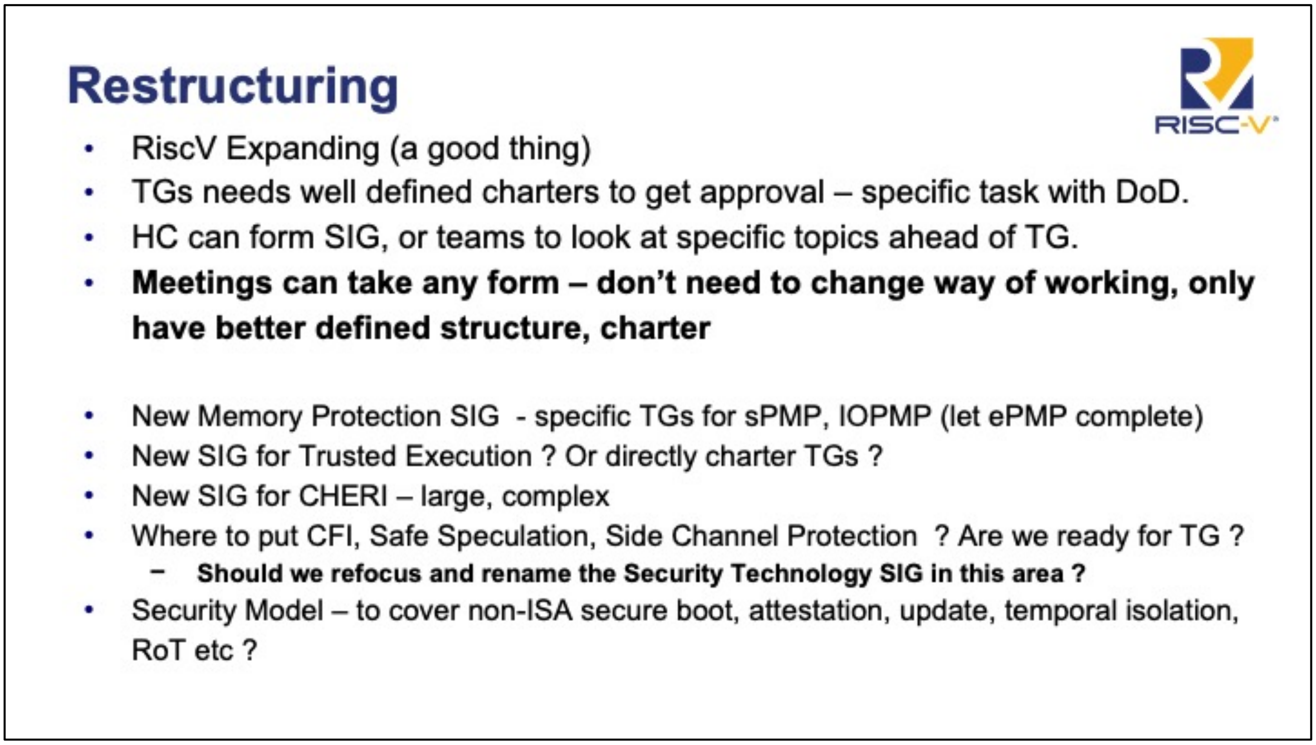
Server

- Andy requested that we all discuss and put forward ideas for the Risc-V security vision – from perspective of applications and feature requirements that we are missing, so we can organise to fill the gaps.

Bruno MUSSARD :- Would make sense to split solutions and security functions.
For instance: trusted boot is a SF while TEE is a way to address it.
You need a baseline for the security functions you want to target. SESIP framework can be a good starting point.

Richard - Fence.t fits pretty well in your "Safe Speculation/Side Channel Protection" bubble(s)

Concluded that folks should post their ideas and requirements via email. Andy and Manuel will create a more complete 1st picture for folks to comment. Target is comments received before next Friday, 10th September.



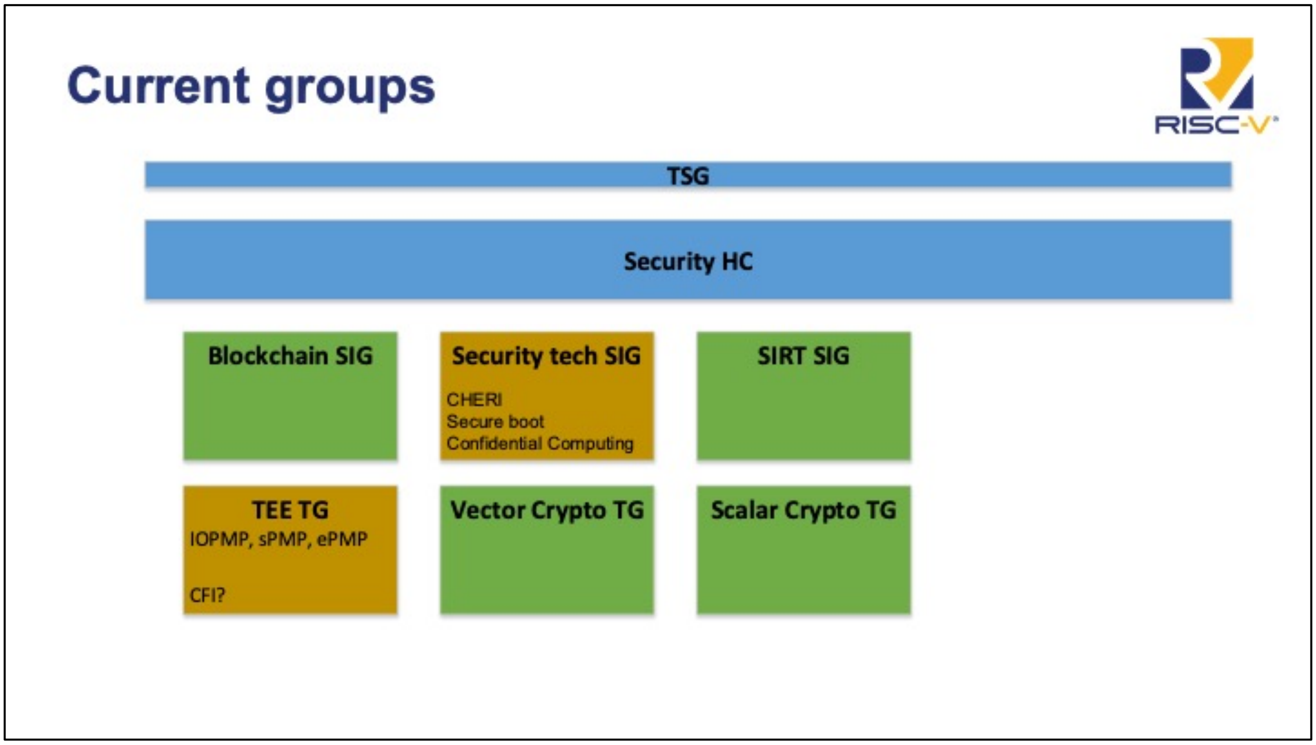
Restructuring

- RiscV Expanding (a good thing)
- TGs needs well defined charters to get approval – specific task with DoD.
- HC can form SIG, or teams to look at specific topics ahead of TG.
- **Meetings can take any form – don't need to change way of working, only have better defined structure, charter**

- New Memory Protection SIG - specific TGs for sPMP, IOPMP (let ePMP complete)
- New SIG for Trusted Execution ? Or directly charter TGs ?
- New SIG for CHERI – large, complex
- Where to put CFI, Safe Speculation, Side Channel Protection ? Are we ready for TG ?
  - **Should we refocus and rename the Security Technology SIG in this area ?**
- Security Model – to cover non-ISA secure boot, attestation, update, temporal isolation, RoT etc ?

- Mark and Andy Introduced the need to restructure as we get more requirements and grow.
- Reiterated the fact that meetings don't need to reflect the precise TG structure, i.e. multiple topics in one meeting is expected, or even no meetings as some groups perform entirely by mail.

- Proposal (needs Nicks feedback) is to create Memory Protection SIG to replace the TEE TG (led by Nick). Allow the ePMP to complete and charter precisely the other PMP activities.



Current groups

TSG

Security HC

Blockchain SIG

Security tech SIG
CHERI
Secure boot
Confidential Computing

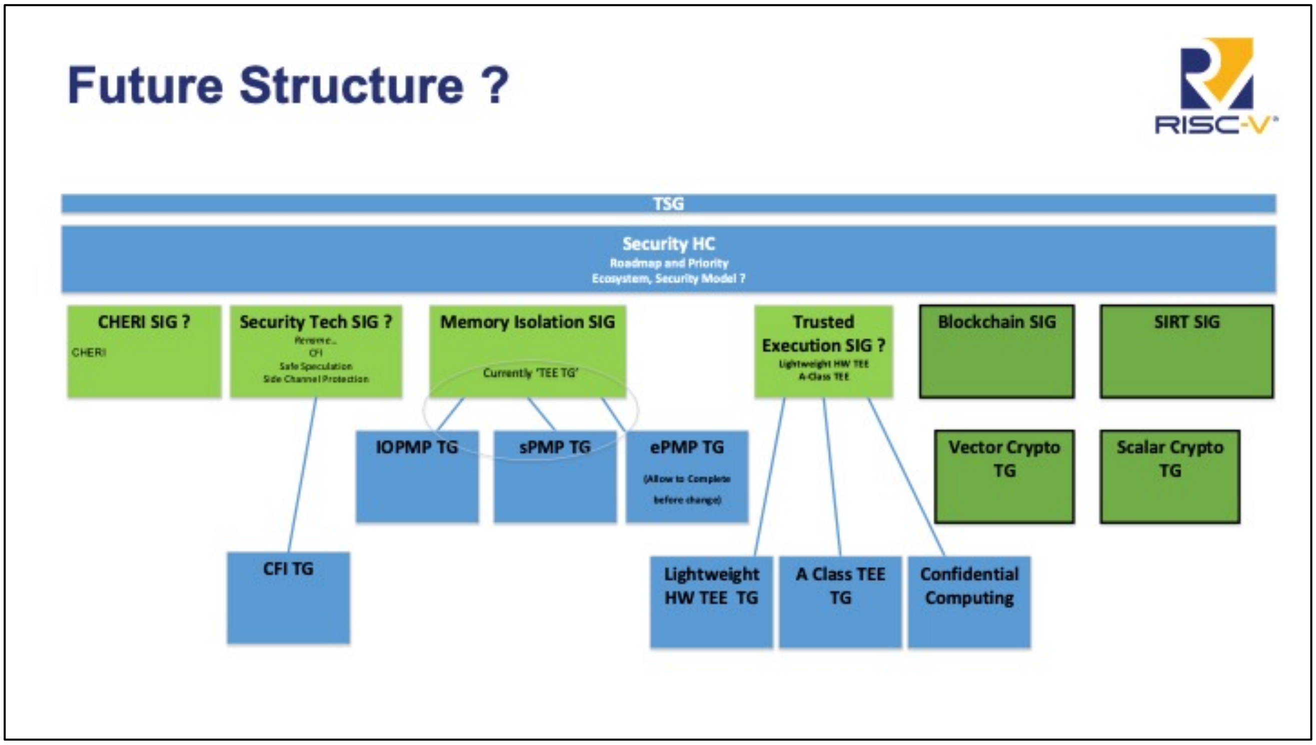
SIRT SIG

TEE TG
IOPMP, sPMP, ePMP
CFI?

Vector Crypto TG

Scalar Crypto TG

- Richard - For completeness you also need to show the PSIRT SIG
- Bruno MUSSARD - Yes. PSIRT is now mandatory to any IC vendor. so, it is part of basic services around secure products.



Future Structure ?

RISC-V

TSG

Security HC
Roadmap and Priority
Ecosystem, Security Model ?

CHERI SIG ?
CHERI

Security Tech SIG ?
Rename...
CFI
Safe Speculation
Side Channel Protection

Memory Isolation SIG
Currently 'TEE TG'

Trusted Execution SIG ?
Lightweight HW TEE
A-Class TEE

Blockchain SIG

SIRT SIG

IOPMP TG

sPMP TG

ePMP TG
(Allow to Complete before change)

Vector Crypto TG

Scalar Crypto TG

CFI TG

Lightweight HW TEE TG

A Class TEE TG

Confidential Computing

Any showed 'straw man' proposal for a new structure. Agreed that we should continue to discuss, Andy will request offline discussion for those interested.

Main comments were around CHERI SIG, as CHERI is only one possible solution to a set of problems, and this SIG could be taken to imply it was already selected.
Andy countered this wasn't the intention, but that it is sufficiently complex that it requires investigation to understand if it could be a solution
Ken Dockser - Perhaps we can create a new group type: Exploratory Group.
CHERI could fit under this.
Agreed to discuss this separately - and the renaming of the security tech SIG to cover CFI etc.

Richard Newell - Perhaps we should also at least be tracking ecosystem activity, e.g., Keystone, CHERI, seL4 which are operating pretty independently of RVI

Don A Bailey Yeah and also people will want to see the entire picture of a deployed device. Not just to server but from silicon to cloud to endpoint.

Thank You