galois

RISC-V: An Open Platform for Security R&D

Joe Kiniry, Galois

with contributions from Helena Handschuh (Rambus), Joe Xie (NVIDIA), Richard Newell (Microchip/ Microsemi), Dan Zimmerman (Galois)

on behalf of the RISC-V Foundation's Security Standing Committee and its Task Groups

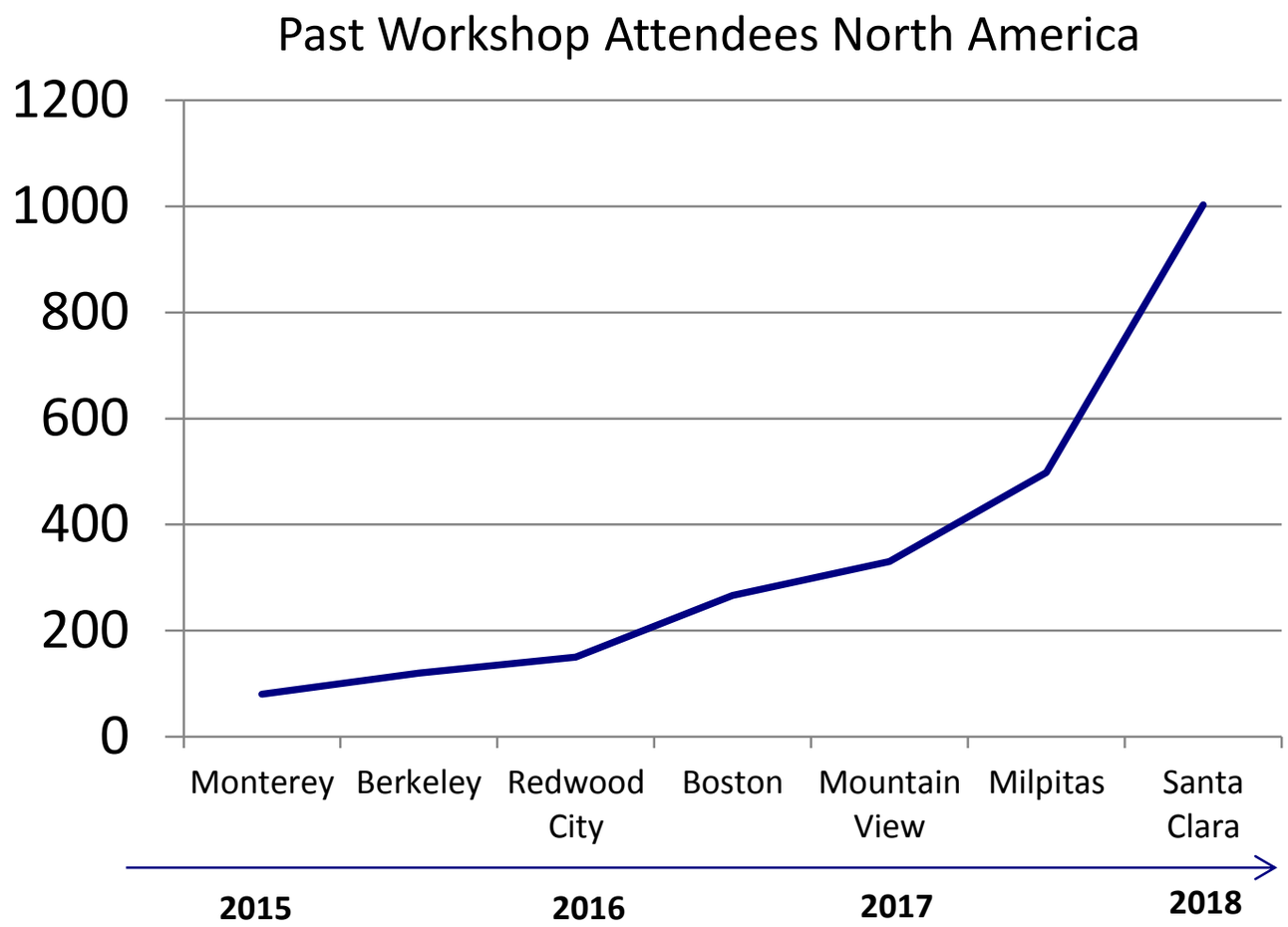
What is RISC-V?

- RISC-V (pronounced *risk-five*) is the fifth major RISC design effort at UC Berkeley
- high-quality, license-free, royalty-free RISC ISA
- used to design everything from tiny microcontrollers to multicore servers with domain specific accelerators
- development started in Summer 2010
- early workshops were a couple of handfuls of graduate students and faculty from Berkeley & MIT
- the latest RISC-V Summit had >1,000 attendees and hundreds of companies were represented

- **a platform for doing open secure hardware R&D and product development for very low cost**

RISC-V Community Evolution

- latest RISC-V Summit
  - December 2018
  - ~2X attendance growth
  - ~250 abstracts
  - 59 sessions
  - 29 exhibitors
- in 2019, production shipments of RISC-V cores will be in the range of 10–100M



The RISC-V Foundation

- ISA governed by a non-profit foundation—the RISC-V Foundation—since Summer 2015
  - over 200 members
- RWC attendees should be excited about individual membership
  - you can join and have an impact for $99/yr

Why is RISC-V Interesting?

- **simple**
  - far smaller than other commercial ISAs
- **clean-slate design**
  - clear separation between user and privileged ISA
  - avoids μarchitecture or technology-dependent features
- **modular**
  - small standard base ISA
  - multiple standard extensions
- **designed for extensibility/specialization**
  - variable-length instruction encoding
  - vast opcode space available for instruction-set extensions
- **stable**
  - base and standard extensions are frozen
  - additions via optional extensions, not new versions

RISC-V + Security

- top-level Security Standing Committee to provide leadership, guidance, and strategy
  - Chair: Helena Handschuh (Rambus)
    Vice Chair: Joe Kiniry (Galois)
- two active Task Groups
  - cryptographic extensions
    - Chair: Richard Newell (Microchip/Microsemi)
      Vice Chair: Dan Zimmerman (Galois)
    - broad set of crypto algorithms via instructions
    - leverages work from vector extension
  - trusted execution environment
    - Chair: Joe Xie (NVIDIA)
    - different shaped enclaves for different kinds of SoCs (microcontroller — server-class CPUs)

Security-Related R&D

- several mechanized formal specifications of the ISA and (possibly secure) cores
  - MIT, SRI, Cambridge, Galois, Symbiotic EDA
- several cryptographic extension implementations
  - from ad hoc to formally synthesized, from not tested at all to formally verified, from leaky to side channel-free
- secure boot implementations and enclaves
  - from ports of large historic nightmares to formally verified implementations
- SSITH teams are creating dozens of different secure SoCs that include dozens of security features

Why Should RWC Participants Care?

- clean ISA and extension framework
  - extending an existing CPU with new ideas in security is straightforward and has minimal cost
  - we aim to get security right in a principled way
- many companies are developing RISC-V cores or ASICs and need security expertise
- low barrier to learning about hardware design, development, and verification
  - open source ISA, CPUs, formal ISA specs, design & formal verification tools, and more
- low-hanging fruit in R&D and business opportunities

For More Information

- the main RISC-V Foundation website
  - https://riscv.org/
- RISC-V Twitter
  - https://twitter.com/risc_v
  - @risc_v
- RISC-V LinkedIn Page
  - https://www.linkedin.com/company/risc-v-foundation
- RISC-V mailing lists / groups
  - https://riscv.org/mailing-lists/