Survey of Notable Security-Enhancing Activities in the RISC-V Universe

G. Richard Newell[1], Joe Xie[2], Helena Handschuh[3]

(1) Microchip Technology (FPGA Business Unit),
and Chair of the RISC-V Cryptographic Extensions task group

(2) Nvidia, and Chair of the RISC-V Trusted Execution Environment task group

(3) Rambus (Cryptography Research Business Unit), and Chair
of the RISC-V Security Standing Committee

Abstract

The RISC-V open source Instruction Set Architecture (ISA) has quickly become the premier vehicle for CPU security research and many new commercial CPU implementations. The non-profit RISC-V Foundation, with over 235 member organizations representing industry and academia worldwide, has made security a top priority, elevating the Security Standing Committee as the only single-topic committee to report directly to the Foundation's Board of Directors. There are two security-focused technical task groups dedicated to developing ISA extensions, for Trusted Execution Environments and Cryptography, respectively, with influence in task groups working on Formal Specifications, Debug, the Privilege Specification, and other RISC-V task groups having a security impact. The RISC-V ISA has been selected by the DARPA SSITH program for all performers to use for its cyber security designs, and will be one of just two ISAs chosen by the DARPA AISS program for its security research. Together, these two DARPA programs are investing approximately $100M (US) in RISC-V HW-based security. The free and open RISC-V ISA has quickly become the de facto vehicle for CPU security research in academia. This talk will provide a necessarily brief survey of notable RISC-V security activities that are heralding in a new age in CPU security.