SECURE RF
Securing the Internet of Things

News Release

SecureRF's Digital Signature Algorithm WalnutDSA™ Featured in Secure Boot Application at the 7th RISC-V Workshop

Richard Newell of Microsemi Will Present an Accelerated Secure Boot Application Implemented Using Cryptographic Extensions Proposed by the RISC-V Security Working Group

Shelton, CT, November 27, 2017 – SecureRF Corporation's quantum-resistant Walnut Digital Signature Algorithm™ (WalnutDSA™) will be featured in a talk titled "Using Proposed Vector and Crypto Extensions for Fast and Secure Boot" at the 7th RISC-V Workshop on November 29, 2017 in Milpitas, California. The presentation, created by Microsemi's Senior Product Architect Richard Newell and SecureRF's development team, will focus on an accelerated secure boot application based on WalnutDSA that was implemented using new cryptographic extensions proposed by the RISC-V Security Working Group.

Modern IoT devices are easily hacked because they lack adequate layers of security. One way to limit the vulnerabilities inherent in the IoT is to enable a device to validate its firmware to ensure that the device's functions have not been modified. A proven validation approach is to implement a secure boot solution that enables a manufacturer to create a digital signature on its firmware that can be validated before bootup. Newell will explain how to leverage proposed RISC-V crypto, vector, and matrix math extensions to enable a significant speedup of WalnutDSA, the core technology behind SecureRF's secure boot solution.

The proposed extensions that will be added to the RISC-V instruction set are designed to handle cryptographic operations efficiently. They will enable certain algorithms, such as WalnutDSA, to run much faster than if they were implemented in the RISC-V standard instruction set alone. The increased efficiency is obtained by allowing math operations to occur in parallel, by providing wide storage registers, by reducing the number of instruction and data fetches, and by allowing operations to occur in different number systems, such as the power of 2 finite field that many SecureRF methods utilize.

"The RISC-V instruction set architecture is growing in acceptance, and the need for security on the platform is paramount," said Derek Atkins, Chief Technology Officer at SecureRF. "As more manufacturers turn to RISC-V for their products, they can rely on SecureRF's quantum-resistant, public-key solutions to provide authentication and data protection for their designs."

SecureRF's WalnutDSA and Ironwood Key Agreement Protocol™, which won ARM's 2017 Innovation Award: Best Contribution to IoT Security, are well-suited for processors based on the RISC-V instruction set. Based on Group Theoretic Cryptography methods, SecureRF's tools are at least 60 times faster than ECC and consume up to 140 times less energy. Moreover, the company's solutions will protect IoT devices even when quantum computers become available and render legacy methods such as ECC and RSA obsolete. To get your free IoT Embedded Security Software Development Kit, call 1-203-227-3151 or email info@securerf.com.

The 7th RISC-V Workshop will be held from November 28-30, 2017, at Western Digital in Milpitas, CA. Newell's presentation is scheduled for 2:18 PM PT on November 29. SecureRF representatives will be in attendance to field questions from attendees.

# # #

About SecureRF

SecureRF Corporation (securerf.com) develops and licenses quantum-resistant, public-key security tools for low-resource processors powering the Internet of Things (IoT). The company's authentication and data protection solutions are highly efficient when compared to techniques like ECC and RSA. SecureRF delivers ultra-low-energy, fast, and small footprint solutions ideally suited for 32-bit, 16-bit, and even 8-bit devices like the ARM Cortex M0/M3 and RISC-V processors. SecureRF security solutions are used to address wireless sensors, NFC, Bluetooth, and RFID tags as well as embedded platforms including FPGAs, microcontrollers, and ASICs. Software Development Kits, RTL, and tools are available for a wide range of environments.

# # #

Company Contact:
C. J. Abate
Marketing@SecureRF.com
+1 203-227-3151