Lattice Sentry Solutions Stack 2.0 Enhances Cyber Resiliency with New Expanded Capabilities

March 1, 2021

- Leading-edge Cryptography for Next-generation Server Platforms
- Faster Boot Times Help Ensure Safe System Operation
- Real-time Monitoring of Mainboard Components Against Unauthorized Firmware Access

HILLSBORO, Ore.--(BUSINESS WIRE)--Mar. 1, 2021-- As the next step in its ongoing mission to deliver secure, cyber-resilient system control solutions, Lattice Semiconductor Corporation (NASDAQ: LSCC), the low power programmable leader, today announced the latest version of its solutions stack for secure system control, Lattice Sentry™ 2.0. The solutions stack enables next-generation hardware Root-of-Trust (HRoT) solutions compliant with NIST Platform Firmware Resiliency (PFR) Guidelines (NIST SP-800-193) and supporting 384-bit encryption. This new version of Lattice Sentry addresses the rapidly evolving security requirements of current and emerging server platforms by providing developers an efficient and secure way to quickly implement enhanced system and cryptographic applications. The stack supports firmware security for the communications, computing, industrial, automotive, and smart consumer markets.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20210301005143/en/

The Lattice Sentry solutions stack helps developers create cyber resilient system control applications compliant with NIST guidelines for platform firmware security (NIST SP-800-193). It consists of a complete reference platform, fully validated IP building blocks, easy-to-use FPGA design tools, reference designs, and a network of custom design services. (Photo: Business Wire)

The Cloud Security Industry Summit (CSIS) is a group of cloud service providers working towards industry alignment on best-of-breed security solutions. In a whitepaper jointly authored with the Open Compute Project (OCP), CSIS said, "Firmware represents a significant threat vector for computer systems, appliances, and associated infrastructure. If the first code that executes on a device when it powers on were to become compromised, then the entire system can and should no longer be trusted as secure. Firmware can be compromised through malicious attacks or unintentionally."[1]

"Staying on top of evolving cybersecurity threats is a constant struggle for most organizations. To help them keep pace, Lattice is committed to the ongoing improvement of the security, performance, and ease-of-use capabilities of our Sentry stack," said Eric Sivertson, Vice President of Security Business, Lattice Semiconductor. "Lattice is a long-time leader in server control solutions, and Lattice control PLDs are the first-on/last-off component in many servers currently in service. With the Sentry stack, developers can easily add support for strong firmware security to system control applications based on Lattice secure control PLDs, creating an ideal platform to establish a HRoT to validate the legitimacy of all firmware instances in a system."

Key features for Sentry 2.0 include:

- Heightened security – The Sentry solutions stack supports the Lattice Mach™-NX secure control FPGA and a secure enclave IP block that enable 384-bit cryptography (ECC-256/384 and HMAC-SHA-384) to better secure Sentry-protected firmware against unauthorized access. Support for 384-bit crypto is a requirement for many next-generation server platforms.
- 4x faster pre-boot authentication – Sentry 2.0 supports faster ECDSA (40 ms), SHA (up to 70 Mbps), and QSPI

performance (64 MHz). These features enable Sentry 2.0 to deliver faster boot times that help minimize system down time and reduce exposure to attempted attacks on firmware during the boot process.
- Ability to monitor up to five firmware images in real-time – To further extend the PFR-compliant HRoT enabled by Lattice Sentry, the stack is capable of real-time monitoring of up to five mainboard components in a system at boot and during ongoing operation. Competing MCU-based security solutions, as an example, lack the processing performance to properly monitor that many components in real-time.

For more information about the Lattice products mentioned above, please visit:

- www.latticesemi.com/LatticeSentry
- www.latticesemi.com/Mach-NX

About Lattice Semiconductor

Lattice Semiconductor (NASDAQ: LSCC) is the low power programmable leader. We solve customer problems across the network, from the Edge to the Cloud, in the growing communications, computing, industrial, automotive, and consumer markets. Our technology, long-standing relationships, and commitment to world-class support let our customers quickly and easily unleash their innovation to create a smart, secure, and connected world.

For more information about Lattice, please visit www.latticesemi.com. You can also follow us via LinkedIn, Twitter, Facebook, YouTube, WeChat, Weibo, or Youku.

[1] https://www.opencompute.org/documents/csis-firmware-security-best-practices-position-paper-version-1-0-pdf

View source version on businesswire.com: https://www.businesswire.com/news/home/20210301005143/en/

MEDIA CONTACT:
Bob Nelson
Lattice Semiconductor
408-826-6339
Bob.Nelson@latticesemi.com

INVESTOR CONTACT:
Rick Muscha
Lattice Semiconductor
408-826-6000
Rick.Muscha@latticesemi.com

Source: Lattice Semiconductor