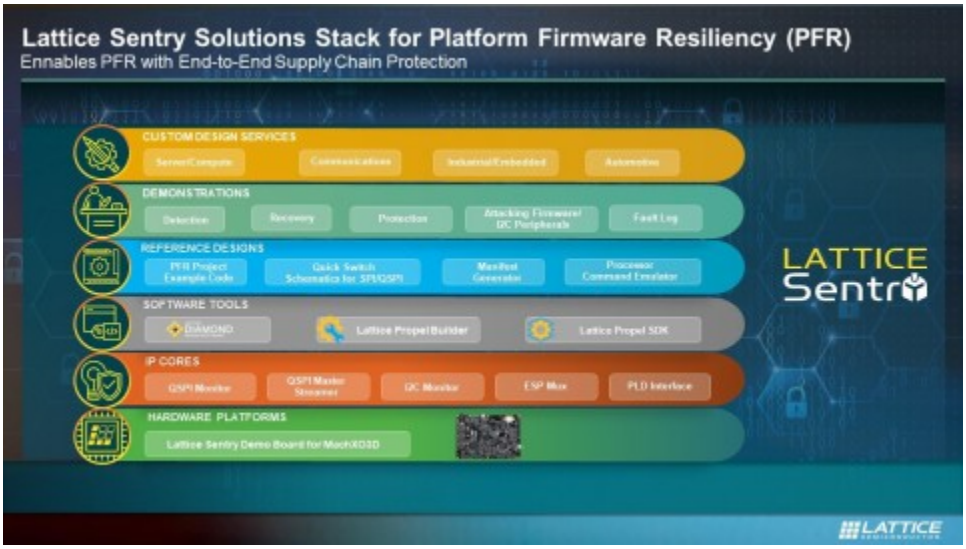
Lattice Sentry Solutions Stack and SupplyGuard Service Deliver End-to-End Supply Chain Protection with Dynamic Trust

August 12, 2020

- *Sentry Stack Software Solution Delivers NIST-compliant, Real-time, Dynamic PFR Software Solution that Reduces Time-to-Market from Months to Weeks*
- *SupplyGuard Service Preserves Trust throughout Unprotected Supply Chains by Protecting Against Counterfeiting, Overbuilding, and Trojan Insertion*

HILLSBORO, Ore.--(BUSINESS WIRE)--Aug. 12, 2020-- Lattice Semiconductor Corporation (NASDAQ: LSCC), the low power programmable leader, today launched the Lattice Sentry™ solutions stack and the Lattice SupplyGuard™ supply chain protection service. The Sentry stack is a robust combination of customizable embedded software, reference designs, IP, and development tools to accelerate the implementation of secure systems compliant with NIST Platform Firmware Resiliency (PFR) Guidelines (NIST SP-800-193). The Lattice SupplyGuard service extends the system protection provided by the Sentry stack throughout today's challenging and rapidly changing supply chain by delivering factory-locked devices to protect them from attacks like cloning and malware insertion, and enables secure device ownership transfer. These hardware security solutions are increasingly important to a range of applications, including communications, datacenter, industrial, automotive, aerospace, and client computing.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20200812005214/en/



The Lattice Sentry Solutions Stack (Graphic: Business Wire)

According to Patrick Moorhead, president and founder of Moor Insights & Strategy, "5G, Edge computing, and IoT are accelerating the pace at which devices are becoming connected, and security concerns are on the rise among high-tech OEMs serving every market. Developers need to know their hardware platforms are secured against cyberattack and IP theft. They need security solutions that support comprehensive protection throughout a product's entire operating life in the field, which means the solution must be able to dynamically adapt to an evolving threat landscape."

"Lattice continues to execute to our solutions stack roadmap and strategy to provide our customers with easy to use, system-level solutions for key focus applications. The Lattice Sentry solutions stack makes it easy for customers to implement a hardware Root-of-Trust (RoT)-based PFR solution compliant with the NIST SP-800-193 guidelines," said Deepak Boppana, Sr. Director, Segments and Solutions Marketing, Lattice. "With Sentry's validated IPs, pre-verified reference designs, and hardware demos, developers can quickly customize the PFR solution by modifying the C code provided with the RISC-V and Propel design environment to cut time-to-market from ten months to just six weeks."

The security paradigm is changing, and firmware is an increasingly popular attack vector. The National Vulnerability Database reported that between 2016 and 2019 the number of firmware vulnerabilities grew over 700 percent[1]. Protecting systems against unauthorized firmware access requires dynamic, persistent, real-time hardware platform security for all connected devices. This includes securing component firmware from unauthorized access and enabling the system to automatically protect, detect, and recover from an attack in an instant. TPM and MCU-based hardware security solutions use serial processing and cannot deliver the real-time performance that parallel processing solutions like Lattice FPGAs can.

"To provide them with peace of mind in a constantly changing and increasingly risky supply chain environment, Lattice developed our SupplyGuard service to help our customers securely provision their devices while lowering their overall costs," said Eric Sivertson, Vice President of Security Business, Lattice. "With Sentry and SupplyGuard, Lattice delivers comprehensive, truly parallel, nanosecond reactive, next-generation security to enable dynamic trust for our customers and the users of their products."

Key features of the Lattice Sentry solutions stack include:

- Hardware security capabilities – the Sentry solutions stack provides a pre-verified, NIST-compliant PFR implementation that enforces strict, real-time access controls to all system firmware during and after system boot. If corrupt firmware is detected, Sentry can automatically rollback to a previously known good state version of the firmware so secure system operation continues without interruption.
- Compliance with latest NIST SP-800-193 standard and CAVP certifications – the stack enables implementation of a hardware RoT through its support for the cryptographically-sound Lattice MachXO3D™ family of FPGAs.
- Ease of use – developers can drag-and-drop Sentry's validated IPs and modify the included RISC-V C reference code in the Lattice Propel design environment without any prior FPGA experience.
- Rapid time-to-market – the Sentry stack provides pre-verified and tested application demos, reference designs, and development boards that can slash development times for PFR applications from ten months to just six weeks.
- Flexible, platform-agnostic security solution – Sentry offers comprehensive, real-time PFR support for firmware and programmable peripherals. It can act as a RoT in a system and/or complement any existing BMC/MCU/TPM-based architecture for full NIST SP-800-193 compliance.

Key features of the Lattice SupplyGuard supply chain protection service include:

- Robust security throughout device lifecycle – SupplyGuard is a subscribed service that offers OEMs and ODMs peace of mind by tracking locked Lattice FPGAs through their entire lifecycle, from the point of manufacture, through transport through the global supply chain, system integration and assembly, initial configuration, and deployment. SupplyGuard helps protect OEMs by:
  - Ensuring only authorized manufacturers can build an OEM's design, regardless of their location.
  - Providing OEMs with a secure key infrastructure to prevent the activation of their IP on unauthorized components to stop product cloning and overbuilding.
  - Securing devices against the download and installation of Trojans, malware, or other unauthorized software to protect platforms and systems against equipment hijacking or other cyberattacks.
- Flexible, low-cost implementation – SupplyGuard is highly customizable to meet the specific security and supply chain needs of OEMs in every industry Lattice serves. The service lowers the operating costs associated with implementing a secure manufacturing ecosystem.

For more information, please visit www.latticesemi.com/LatticeSentry and www.latticesemi.com/LatticeSupplyGuard

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 lets 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] Source: National Vulnerability Database (2016 and 2019)

View source version on businesswire.com: https://www.businesswire.com/news/home/20200812005214/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 Corporation