AMI and Lattice Semiconductor Announce Joint Platform Firmware Resiliency Security Solution: AMI PlatFire Firmware with Lattice Sentry Solutions Stack

November 19, 2020

FOR RELEASE: November 19, 2020

DULUTH, GEORGIA / HILLSBORO, OREGON AMI®, a global leader in powering, managing, and securing the world's connected digital infrastructure through its BIOS, BMC and security solutions, and Lattice Semiconductor, the low power programmable leader, are pleased to announce a new jointly-developed platform firmware security solution, AMI PlatFire™ Firmware with the Lattice Sentry™ solutions stack. The solution enables developers to quickly and easily implement system-level cyber resiliency that is pre-validated as compliant with NIST Platform Firmware Resiliency (PFR) Guidelines (NIST SP 800-193), making it easy for developers with limited hardware security expertise or limited time-to-market to implement PFR on the latest industry-standard server platforms.

The solution combines technology from two of the leading names in PFR - AMI and Lattice Semiconductor - to bring the industry an integrated, fully-featured, pre-verified and secure Platform Root-of-Trust (PRoT) solution that is flexible, scalable, low cost, and easy to implement. The solution uses the Lattice Sentry stack, featuring a low-power Lattice MachXO3D™ secure control FPGA running pre-verified, PFR-compliant IP, to implement a PRoT on a server's motherboard. The AMI PlatFire firmware then orchestrates the connection between the PRoT and other on-board components, such as SoCs and RoCs, to confirm the firmware they are running is valid.

"We're excited by the growing interest from customers across markets in implementing PFR to protect their systems. Pairing our Sentry solutions stack with AMI's new PlatFire firmware provides a comprehensive, system-level PFR solution that helps developers quickly and easily protect their system firmware, making PFR support possible for a larger potential customer base," said Esam Elashmawi, Chief Strategy and Marketing Officer, Lattice Semiconductor.

Sanjoy Maity, Chief Executive Officer of AMI, added that "Our AMI PlatFire PRoT firmware provides customers an affordable, flexible and comprehensive alternative to existing competitor solutions. By partnering with Lattice Semiconductor to deliver AMI PlatFire on a secure Lattice MachXO3D FPGA with the Lattice Sentry Security stack and a full suite of design and development tools, together we can offer complete system security that is fully compliant with NIST PFR Guidelines and is host CPU vendor agnostic - so customers don't have to feel locked into a particular ecosystem or platform to have a secured system."

Firmware Security Trends are Changing Faster than Ever

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]. The NIST PFR guidelines were written to help developers understand how to protect legitimate firmware, detect unauthorized firmware, and restore compromised firmware to a known good state by establishing a PRoT. PRoT solutions validate platform firmware at boot to ensure it has not been modified illegitimately. Currently, developers with PFR design expertise are in limited supply, and OEMs requiring support for PFR often have strict time-to-market requirements that preclude developing a PFR solution from scratch. Recognizing these trends, AMI and Lattice worked together to deliver a tightly integrated, pre-validated PFR solution. It provides a robust PRoT, for real-time I2C bus and SPI monitoring of both BIOS and BMC SPIs, so from the moment a system boots all transactions over the SPI bus are monitored.

What is AMI PlatFire?

AMI has applied its 35 years of deep expertise in BIOS and BMC firmware development to deliver a robust PFR solution designed to detect, protect and recover firmware from unauthorized modification. As implemented in the AMI-Lattice joint solution, the PlatFire firmware executing on the Lattice MachXO3D with the Lattice Sentry solution stack orchestrates the connection between the solution's PRoT and all other ICs on the motherboard. Moreover, AMI PlatFire firmware is host CPU-agnostic, to give system developers greater flexibility in supporting the CPU requirements of their chosen server platform.

Thanks to its seamless integration with Aptio® UEFI Firmware and MegaRAC® SPX BMC Firmware from AMI, AMI PlatFire delivers a truly turnkey PFR solution - making use of the Lattice MachXO3D IP blocks to support detection and recovery of platform firmware, together with runtime monitoring of SPI flash memory used to store the platform firmware.

What is Lattice Sentry?

The Lattice Sentry solutions stack delivers a robust combination of customizable embedded software, reference designs based on the Lattice MachXO3D secure control FPGA, IP, and development tools to accelerate the implementation of secure systems compliant with PFR guidelines. As the system controller, the MachXO3D is the first component to execute code and attest power sequencing logic at system startup, making it an ideal platform for establishing a PRoT. Thanks to the MachXO3D FPGA's parallel processing architecture and flash memory, the device monitors for and detects attacks in real time - a truly groundbreaking innovation as real time monitoring is currently beyond the processing capabilities of competing PRoT solutions like MCUs.

For more information on the joint AMI PlatFire™ PRoT Firmware on Lattice Sentry solutions stack, please call 1-800-828-9264 to speak with an AMI Security Solutions expert or contact us via https://ami.com/en/contact-us/.

For more information about Lattice Sentry, please visit https://www.latticesemi.com/latticesentry.

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.

About AMI

Founded in 1985 and known worldwide for AMIBIOS®, the mission of AMI is to power, manage and secure connected devices by providing best-in-class UEFI and remote management firmware, software and utilities to top-tier manufacturers of desktop, server, mobile and embedded/IoT systems. In line with its technology focus, AMI is a member of numerous industry associations and standards groups, such as the Unified EFI Forum (UEFI), the NIST National Cybersecurity Excellence Partnership (NCEP) and Trusted Computing Group (TCG). Headquartered in Duluth, Georgia, AMI has locations in the U.S., China, Germany, India, Japan, Korea, Taiwan and Hong Kong to better serve its customers.

For more information on AMI, its products or services, call 1-800-828-9264 or visit ami.com.

Media Contact:
Bob Nelson
Lattice Semiconductor
Phone: 408-826-6339
Bob.Nelson@latticesemi.com

Investor Contact:
Rick Muscha
Lattice Semiconductor
Phone: 408-826-6000
Rick.Muscha@latticesemi.com

1. Source: National Vulnerability Database (2016 and 2019)