Lattice’s New MachX03D FPGA Enhances Security with Hardware Root-of-Trust Capabilities

May 20, 2019

FPGA Family Simplifies Implementation of Comprehensive, Flexible and Robust Hardware Security throughout Product Lifecycle

- Enhances security in computing, communications, industrial control and automotive systems

HILLSBORO, Ore.--(BUSINESS WIRE)--May 20, 2019-- Lattice Semiconductor Corporation (NASDAQ: LSCC), the low power programmable leader, today announced the MachXO3D™ FPGA for securing systems against a variety of threats. Unsecured systems can lead to data and design theft, product cloning and overbuilding, and device tampering or hijacking. With MachXO3D, OEMs can simplify the implementation of robust, comprehensive and flexible hardware-based security for all system components. MachXO3D can protect, detect and recover itself and other components from unauthorized firmware access at every stage of a system’s lifecycle, from the point of manufacturing all the way to the system’s end of life.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20190520005138/en/

Lattice Semiconductor MachXO3D FPGA (Graphic: Business Wire)

Component firmware is an increasingly popular attack vector for cyberattacks. According to a report in “MIT Technology Review,” security vulnerabilities rendered over 3 billion chips in systems of all types open to data theft via the exploitation of their firmware[1]. Unsecured firmware also exposes OEMs to the financial and brand reputation risks associated with device hijacking (for use in DDoS attacks) and device tampering or destruction. Failure to address these risks can negatively impact a company’s reputation and financial performance.

According to Patrick Moorhead, president and founder of Moor Insights & Strategy, “Compromised firmware is particularly insidious as it not only leaves user data vulnerable, but can also make systems permanently inoperable, disrupting the user experience and exposing OEMs to liability. FPGAs provide a compelling hardware platform choice for securing system firmware as they’re able to perform multiple functions in parallel, making them much faster at identifying and responding to unauthorized firmware when detected.”

When used to implement system control functions, MachXO3 FPGA devices are typically the “first-on/last-off” component on circuit boards. By integrating security and system control functions, the MachXO3D becomes the first link in a chain of trust that protects entire systems.

With MachXO3D, Lattice is enhancing the device configuration and programming steps in the manufacturing process. These enhancements, in combination with MachXO3D’s security features, protect systems by securing communication between the MachXO3D and legitimate firmware providers. This protection stays in effect throughout the component’s entire lifecycle, including system manufacture, transit, installation, operation and decommissioning. According to Symantec, there was a 78 percent increase in supply chain-related attacks between 2017 and 2018[2].

“System developers commonly take advantage of FPGA flexibility to enhance system functions after deployment,” said Gordon Hands, Director of

Solutions Marketing, Lattice Semiconductor. “With MachXO3D, we took care to retain that flexibility while adding a secure configuration block to deliver the industry’s first control-oriented FPGA compliant with NIST’s Platform Firmware Resilience specification.”

Key features of the new MachXO3D include:

- Control function FPGA that provides 4K and 9K look-up tables for implementing logic that instantly configures at power up from on device flash memory
- On-device regulator for single 2.5/3.3-volt power supply operation
- Support for up to 2700 Kbits of user Flash memory and up to 430 Kbits sysMEM™ embedded block RAM to provide more flexible design options
- Up to 383 I/Os, configurable to support LVCMOS 3.3 to 1.0, and designed to integrate into a wide variety of system environments with features such as hot-socketing, default pull-down, input hysteresis, and programmable slew rate
- Embedded security block that provides pre-verified hardware support for cryptographic functions such as ECC, AES, SHA, PKC and Unique Secure ID
- Embedded secure configuration engine to ensure only FPGA configurations from a trusted source can be installed
- Dual on-device configuration memories to enable fail-safe reprogramming of component firmware in the event of compromise

Samples are available. For more information about MachXO3D, please visit http://www.latticesemi.com/MachXO3D.

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] Giles, M. (2018, Jan. 5). At Least 3 Billion Computer Chips Have Spectre Security Hole, *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/609891/at-least-3-billion-computer-chips-have-the-spectre-security-hole/

[2]Symantec. (2018, February). *ISTR: Internet Security Threat Report*. Retrieved from https://www.symantec.com/security-center/threat-report?om_ext_cid=biz_vnty_istr-24_multi_v10195

View source version on businesswire.com: https://www.businesswire.com/news/home/20190520005138/en/

Source: Lattice Semiconductor Corporation

MEDIA CONTACTS:
Doug Hunter
Lattice Semiconductor
503-268-8512
Doug.Hunter@latticesemi.com

INVESTOR CONTACT:
David Pasquale
Global IR Partners
914-337-8801
lscc@globalirpartners.com