Growing Threats Demand Dynamic Trust Approach to Hardware Security

A Lattice Semiconductor White Paper.

August 2020

Learn more:

www.latticesemi.com

Contact us online:

www.latticesemi.com/contact
www.latticesemi.com/buy

TABLE OF CONTENTS

The Need for Dynamic Trust

For developers designing electronic products serving nearly every market, securing their product designs against firmware-based attacks is becoming a serious concern. The National Vulnerability Database reported that between 2016 and 2019 the number of firmware vulnerabilities grew over 700 percent[1], and industry analyst Gartner reports by 2022 “70 percent of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability[2].”

These vulnerabilities are not only jeopardizing final products deployed in the field. They can also affect individual components as they move through today’s rapidly changing and increasingly unpredictable global electronics supply chain: from initial component manufacturing and shipment to a contract manufacturer, to system integration and on through the device’s entire operating life in the field. The vulnerabilities can be exploited by bad actors and result in a host of different security issues, including data theft, data corruption, Trojan or malware insertion, equipment hijacking, cloning, and design theft. Successful attacks on platform firmware can render a system inoperable, possibly permanently, or exploit the system for ransom, data theft, and hacking. Because such exploits operate below the operating system level, they can be impossible to detect until the damage is done. Any of these attacks can have a major impact on a company’s revenue and reputation.

Protecting electronic system hardware from unwanted access is not a new problem, and there are solutions in place designed to protect unauthorized users from accessing component firmware. However, these solutions typically use Von Neumann architecture microcontrollers (MCUs), which often don’t have the real-time performance required to manage multiple devices should they be attacked. FPGAs which are inherently parallel in nature enable the monitoring, protecting and recovering of multiple devices simultaneously with nanosecond response times.

Even with today’s best TPM and operating system security solutions, system firmware can be attacked before, during, or after system manufacture. Moreover, compromised firmware can be difficult to detect because system components typically load firmware before the operating system and any software-based security solutions (such as post-boot validation checks) are operational. The corrupted firmware can then cloak itself from static post-boot integrity checks, rendering it invisible to security and malware scans.

Electronic systems must change and adapt to new threats as they evolve, and automatically take appropriate action when compromised firmware is detected. To protect system firmware, security solutions need “dynamic trust”: resiliency against firmware attacks based on a parallel, real-time, reactive solution that offers comprehensive firmware protection throughout a system’s lifecycle, beginning with the time components spend moving through the supply chain, from initial product assembly, end-product shipping, integration, and the product’s entire operational lifetime.

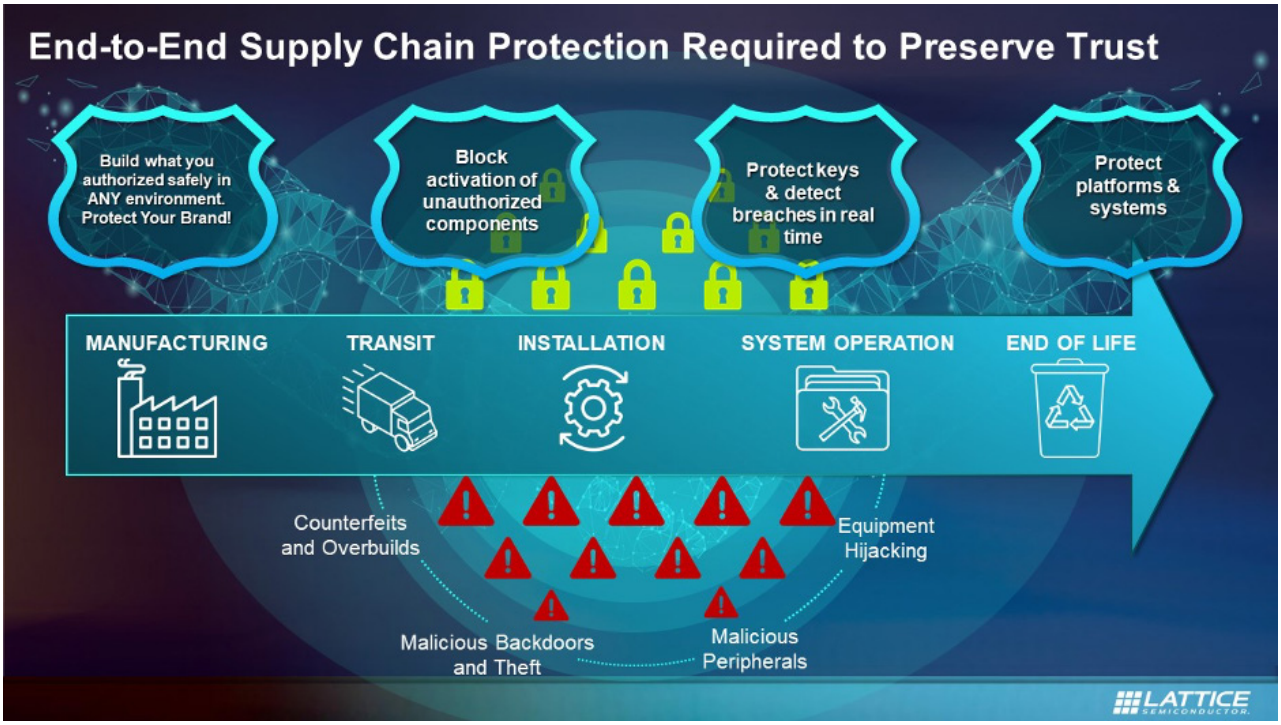

Figure 1: Keeping a component secure as it moves through the supply chain becomes challenging due to a range of potential threats.

New NIST Standard

How can OEMs protect themselves from this constantly escalating threat? Thankfully, the U.S. federal government's National Institute of Standards and Technology (NIST) recognized the threat to firmware and released the NIST Platform Firmware Resiliency (PFR) Guidelines (NIST SP-800-193) to address the importance of properly implementing PFR. The guidelines promote resiliency in the platform by describing security mechanisms for protecting the platform against unauthorized changes, detecting unauthorized changes that occur, and recovering from attacks rapidly and securely.

The guidelines support resiliency of platforms against attacks by following three principles.

- Protection: NIST guidelines for protection include mechanisms for ensuring that platform firmware and critical data remain in a state of integrity and are protected from corruption, including a process for ensuring the authenticity and integrity of firmware updates. The guidelines also require concurrent monitoring of all protected external memories and their interface buses at runtime (with nanosecond response times) and enforcement of strict access controls to all firmware.

- Detection: Mechanisms for detecting when platform firmware code and critical data have been corrupted. This requires autonomous firmware authentication of protected ICs before they boot.

- Recovery: Mechanisms for restoring platform firmware code and critical data to a known good, authenticated state of integrity in the event they are detected to have been corrupted, even against Denial of Service and Replay Attack scenarios, and when forced to recover through an authorized mechanism. This recovery needs to occur automatically and in real time to keep the system online while minimizing the use of hands-on support resources.

To address this rapidly evolving market and developing standards, Lattice Semiconductor has dramatically extended the capabilities of its hardware security products with a new value-added security solutions stack and a new supply chain security service. The Lattice Sentry™ solutions stack minimizes in-system firmware attack vulnerabilities by providing real-time, dynamic protection, detection, and recovery capabilities to all programmable components in a system. The Sentry solutions stack delivers a complete, fully validated, easily customizable NIST 800-193 compliant PFR solution using Lattice's MachXO3D™ secure FPGA. The solutions stack includes a suite of ready-to-use, resilient, production validated IP cores to help protect and monitor SPI and I2C devices and their buses within a system. The stack also includes demo boards and reference designs to test and showcase PFR capabilities. Software tools available with the stack include Lattice's latest IP ecosystem and development environment, Lattice Propel™. Propel helps even non-FPGA users customize their PFR implementations by letting them modify the C code for the stack's RISC-V processor IP, and visually layout the IPs used to create a full system. This system can be imported into the Lattice Diamond Tool to generate a configuration bitstream. The stack includes a full PFR reference design featuring easily modifiable PFR management code, quick switch schematics for SPI/QSPi, a manifest generator, and a processor command emulator.

The Lattice Sentry solutions stack can slash time to market dramatically. Without the pre-validated IP cores and reference design, developing a solution such as this could take months. With Sentry, developers can develop a complete NIST 800-193 compliant solution by modifying the example C code managing the FPGA's real-time operation. The pre-validated IPs can be integrated into the FPGA's configuration bitstream, along with the RISC-V CPU which runs the C code, all using Lattice's Propel software. No FPGA design experience is necessary, although Lattice provides hooks to allow customers interested in developing their own FPGA IP to integrate it with the rest of the Sentry solutions stack.

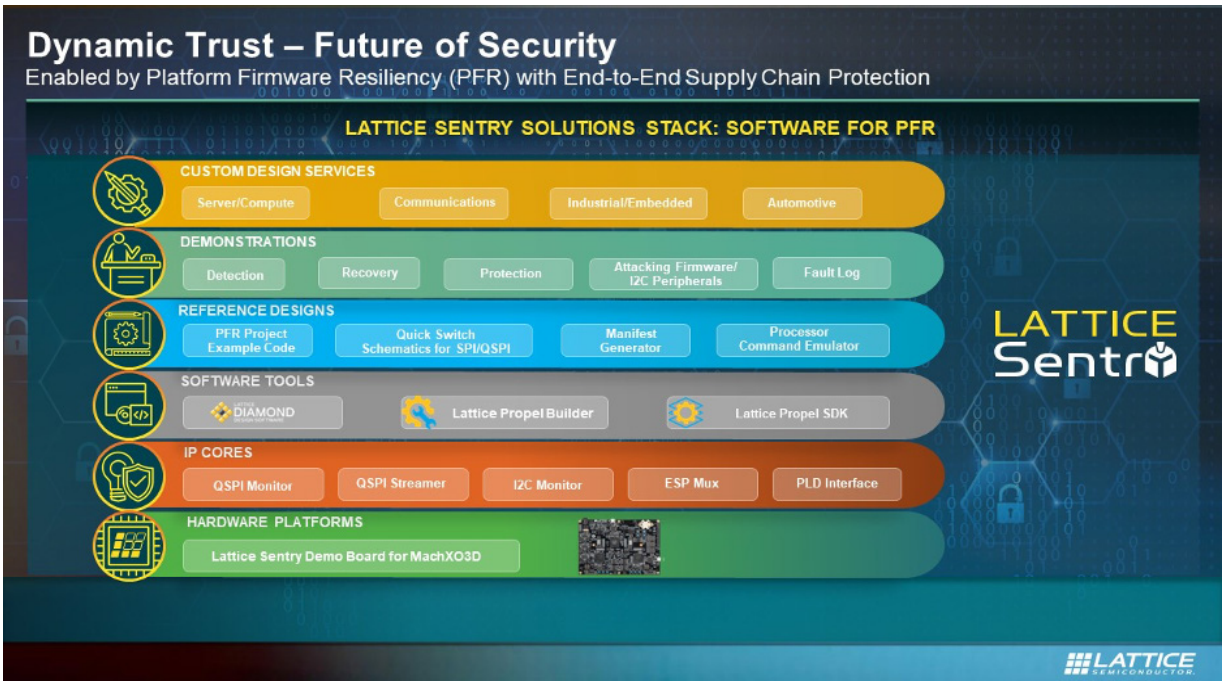

Figure 2: The Lattice Sentry Solutions Stack

In addition to Sentry, Lattice offers SupplyGuard™, an end-to-end supply chain security service. SupplyGuard is a trailblazing subscription service that secures customer IP throughout the supply chain by delivering factory-locked Lattice FPGAs resistant to tampering, Trojan insertion, overbuilding, counterfeiting, and IP theft as they move through the supply chain. This service helps customers ensure that the configuration bitstream and external firmware authentication keys stored on the FPGA are copy- and tamper-resilient. Using SupplyGuard, developers can protect their products across the entire supply chain. SupplyGuard offers protection through secure key provisioning and device ownership transfer performed in a secure, proprietary fashion, setting it apart from currently available provisioning solutions.

The SupplyGuard process begins with Lattice's assignment of a customer-specific part number to the customer's FPGA. Each customer-specific FPGA is programmed at Lattice's factory with customized, cryptographic credentials that allow only the customer to program the FPGA with a configuration bitstream and authentication keys. The service maintains trust and protection as FPGAs move through a supply chain using common carriers and when systems are assembled in third-party factories. The chips depart the Lattice factory completely locked, and only the customer has the required credentials to unlock the FPGA. Lattice generates these unlock credentials using FIPS 140-2 certified High Security Modules (HSMs) and provides them to the customer, who then uses their own HSM to decrypt the credentials; no human in the chain has access to these credentials. The customer's HSM now has the credentials needed to encrypt and sign the customer's customized configuration bitstream and authentication keys. Further, the customer's IP and cryptographic keys are never exposed to Lattice or the supply chain in any form.

Once locked with SupplyGuard, a customer's FPGA becomes a mini fortress as it moves through the supply chain: locked and inaccessible until ready to be programmed with the customer's configuration bitstream. The customer's encrypted, signed bitstream is the only one that can be loaded onto these custom-locked FPGA's. At the same time, the customer's bitstream cannot be loaded onto another FPGA, which protects the customer's IP and their authentication keys against cloning and overbuilding. The process of programming the customer's bitstream passes cryptographic control of the chip from the Lattice factory-locked state to the customer-locked state. This ownership transfer occurs in a protected, encrypted state within the Lattice FPGA and is performed on a standard manufacturing line, using standard bulk factory programming equipment. The configuration bitstream remains secure and encrypted at all times, and protected ownership transfer occurs without any special security procedures, personnel, or equipment (e.g., HSM) in the manufacturing environment. This eliminates added time and cost associated with other factory key provisioning solutions.

Figure 3: The Lattice SupplyGuard service protects Lattice FPGAs from unauthorized access as they move through the global supply chain.

Lattice FPGAs Enable Secure System Control

Sentry and SupplyGuard's new security capabilities leverage Lattice's revolutionary MachXO3D family of FPGAs for secure system control. MachXO3D is the industry's first small footprint, low-power FPGA for system control applications designed to help protect firmware across a wide array of computing, communications, industrial, and automotive applications. Pin-compatible with Lattice's popular MachXO family, the MachXO3D allows designers to take advantage of a proven architecture present in over half of all communications systems and servers. MachXO3D secures its own configuration bitstream and enables system security using its independently NIST certified cryptographic functions, including ECDSA, ECIES, AES, SHA, HMAC, TRNG, and Public/Private key generation. Each device features on-chip flash memory (to support a secure, authenticated dual-boot configuration), public key storage for external firmware authentication, and a unique ID. Should the original firmware become corrupted for any reason, the MachXO3D will automatically roll back to the authenticated version and continue system operation without interruption. Using the Sentry solutions stack, the MachXO3D can continually perform this authentication checking and firmware recovery for the external firmware it protects.

Figure 4: The block diagram illustrates how a Lattice Sentry-based PFR application can protect all firmware instances in a system in real time.

The MachXO3D FPGA's cryptographic functions are compliant with the NIST SP 800-90B specification for True Random Number Generation (TRNG) and the Cryptographic Algorithm Validation Program (CAVP). MachXO3D's CAVP functions were independently certified to be compliant with Federal Information Processing Standards (FIPS), the U.S. federal government's standard for cryptographic software.

Lattice Sentry and SupplyGuard Make Dynamic Trust Possible

Lattice's Sentry Solutions Stack and SupplyGuard work together to offer everything designers need to build highly resilient, end-to-end, dynamic trust solutions. SupplyGuard protection delivers the initial links in this chain by protecting the integrity of both the MachXO3D FPGA and the developer's bitstream, as well as the developer's security credentials that protect the rest of the platform's firmware. The FPGA's ability to transfer secure ownership during factory programming seamlessly transfers protection to the developer's signed, encrypted configuration bitstream, which can implement the Sentry PFR capability to protect the platform's firmware before the system boots, throughout its operation, and during every future bootup and operating moment of the system's life. The system remains functioning as intended, while responding to any malicious actions in nanoseconds. Systems built with Sentry and SupplyGuard support can supplement any existing BMC/MCU/TPM-based architecture so developers can keep using existing hardware security solutions to remain adaptable to customer-specific security and supply chain needs.

Conclusion

Today's hardware security landscape is changing rapidly. Hackers are exploiting system firmware vulnerabilities easily within today's supply chain to steal data and designs, hijack products, and create clones to sell on the gray market. How can developers respond? By implementing new value-added hardware security products and services compliant with the NIST 800-193 standard and pursuing an end-to-end dynamic trust approach to hardware security. The new Lattice Sentry solutions stack and SupplyGuard supply chain security service helps them do that quickly and easily.

References

[1] Source: National Vulnerability Database (2016 and 2019)
[2] Source: Gartner, July 2019

Learn more:

www.latticesemi.com

Contact us online:

www.latticesemi.com/contact
www.latticesemi.com/buy