TEKTAGON™ XFR

Extreme Firmware Resiliency

Serious Firmware Protection

Firmware presents a large and ever-expanding attack surface

Securing the firmware layer is often overlooked, but it is a single point of failure in devices and is one of the stealthiest ways for an attacker to gain control of a system. An attacker with access to device firmware can potentially bypass authentication and encryption mechanisms, modify the core functionality of a device, and plant persistent malware.

Because of this, our security experts have developed Tektagon™ XFR, a Platform Root of Trust solution designed to detect, protect and recover firmware from unauthorized modification and help you thrive in the face of uncertainty.

Tektagon™ XFR, designed with Lattice Semiconductor, brings the industry an integrated Platform Root of Trust solution that is cost-effective, scalable, compatible, and easy to implement.

The solution uses the Lattice Sentry stack, featuring low-power Lattice secure control FPGAs running pre-verified, PFR-compliant IP, to implement Platform Root of Trust on a server's motherboard. Tektagon™ XFR firmware then orchestrates the connection between the Platform Root of Trust and other on-board components, such as SoCs and RoCs, to validate firmware and if necessary, recover it in the event of firmware compromise.

This solution enables quick implementation of system-level NIST-compliant firmware resiliency, making it easy to implement PFR on the latest industry-standard server platforms.

Key Features:

Establishes a chain of trust and protects hardware from malicious attacks with the AMI Platform Root of Trust Architecture on dedicated silicon

- Based on Lattice FPGA to provide independent HRoT with maximum flexibility
- NIST® compliant (SP 800-193) with robust Platform Firmware Resiliency (PFR)
- Compatible with Intel®, AMD®, Arm®, RISC-V® and other host silicon vendors
- Configurable modular code
- Secure firmware update of recovery image
- SPDM Support
- Out-of-box compatibility with AMI firmware products:
    - Aptio® V UEFI Firmware
    - Aptio® OpenEdition™ Firmware
    - MegaRAC® SP-X BMC Firmware
    - MegaRAC OpenEdition™ BMC Firmware

True Platform Root of Trust

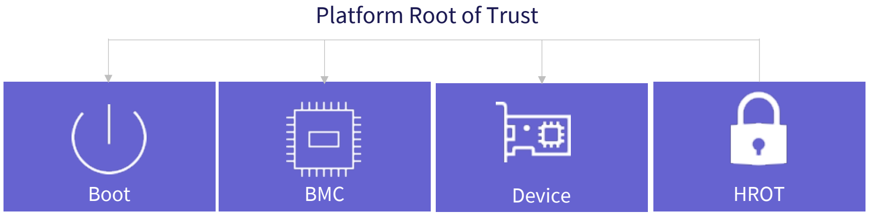
According to the NIST SP 800-193 Platform Firmware Resiliency (PFR) guidelines, there are three basic requirements for resilient firmware: the firmware must be protected from tampering, corrupted firmware can be detected, and firmware must be able to be recovered. As a secure hardware solution that meets all of these requirements for firmware security, Tektagon XFR stands out as a true Platform Root of Trust solution.

Customizable Recovery

Tektagon XFR can force recovery on boot failure, preventing booting from tampered firmware. The recovery image can be stored in a dedicated SPI flash or the same SPI flash protected by SPI flash descriptors. Tektagon XFR provides a secure way to update and validate the recovery image.

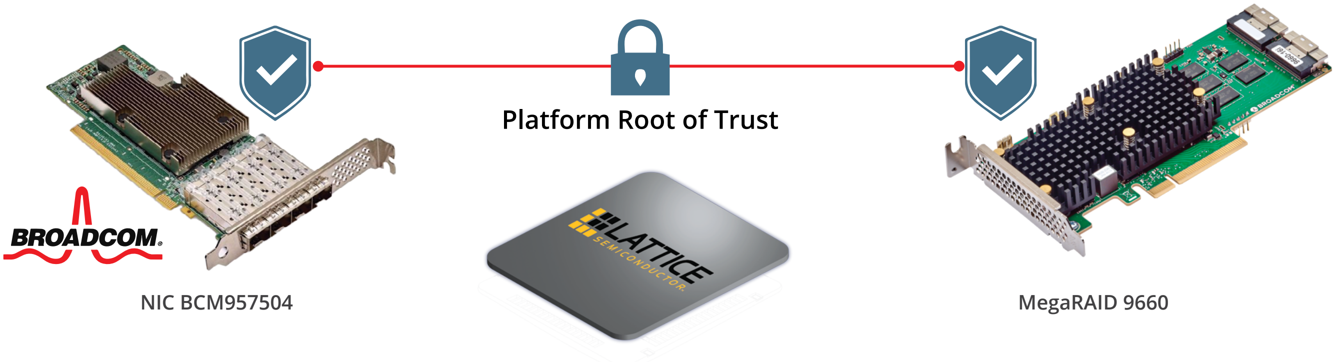
Aptio® UEFI and MegaRAC® BMC

Tektagon XFR can be used as a standalone solution or together with AMI Aptio eModules and MegaRAC SP-X technology packs to further enhance system firmware security.



Supports SPDM Firmware

Adds Root of Trust measurements for firmware running on the platform to authenticate server critical devices such as RAID, NIC and Power Supplies.



Te Tektagon™ XFR

For more information, please visit:

Run Secure with Tektagon™ XFR at www.ami.com/ami-hrot/