Te TEKTAGON™ BFR

Platform Root of Trust for Device Firmware Embedded Controller Implementation

Costly Data Breaches Reaching Unprotected System Firmware

According to the 2022 “Cost of a Data Breach” report by IBM and Ponemon, between 2021 and 2022 the average cost of a data breach in the corporate world rose 2.6% - from $4.24 million to $4.35 million. Until now, securing against these attacks required data centers and endpoints to run monitoring software to protect against malware entry through applications. However, vulnerabilities are now increasingly exploited below the software and OS layers, infecting motherboard and peripheral device firmware. The October 2020 Futurum Research report confirmed this threat, revealing that 56% of companies experienced an external cyberattack attributed to a vulnerability in hardware or silicon-level security.

Emerging Standardization and AMI Tektagon™ BFR Platform Root of Trust (PRoT)

To address the exposure of platform firmware vulnerabilities to rising cyberattacks on hardware, the National Institute of Standards and Technology (NIST®) created the SP 800-193 Platform Firmware Resiliency Guidelines. These guidelines outline specific requirements for securing platform firmware through detection, recovery and protection to achieve **Platform Root of Trust** (PRoT).

Features:

- **Resilient:**
  Fully NIST® SP 800-193 compliant Platform Root of Trust solution with comprehensive image verification, runtime protection and recovery
- **Total Cost of Ownership:**
  Embedded controller hardware re-usability and ready-to-go factory validation minimize development and BOM costs
- **Seamless Integration:**
  Provides drop-in compatibility AMI MegaRAC® and Aptio® BMC/BIOS firmware, improving time to market
- **Deployment Ready:**
  Cross-platform set of common APIs, configuration and security tools for ease of implementation

The Tektagon BFR PRoT firmware solution from AMI runs on fully NIST 800-193 compliant microcontroller from Microchip® Technology Inc. Working seamlessly with device and system boot firmware, Tektagon BFR delivers full Platform Firmware Resiliency (PFR) that meets all three detection, recovery and protection requirements.

Complete Security Against Firmware Attacks Requires a Truly Resilient Platform

The full cost of a data breach includes not only the cost of data exposure, but also the resources required to get systems back online and costs associated with system downtime. Consequently, systems must secure all areas of the platform to be truly resilient - by preventing the proliferation of intrusions and maintaining system uptime.

The NIST 800-193 guidelines measure compliance in three ways, based on the level of platform security. Protected platforms comply with Root of Trust and the protection of mutable code requirements, while recoverable platforms comply with Root of Trust, detection and recovery from corruption requirements. Truly resilient platforms meet each of these requirements, complying with all Root of Trust, protection, detection and recovery requirements set forth by NIST.

Tektagon BFR makes platforms resilient by meeting all Root of Trust, protection, detection and recovery requirements consistent with the guidelines outlined by NIST. Meeting these requirements provides the greatest level of security against a firmware attack, minimizing data exposure, system downtime and costly recovery measures.

Immutable Hardware-Enabled Protection

Tektagon BFR firmware runs on a secure embedded controller chip that enforces the booting of authorized platform firmware only. An immutable boot loader establishes the root of trust, allowing for validation of the platform firmware with the cryptographic signature of the image. The root of trust permanently fuses the public key used into the hardware, which cannot be altered but can be revoked through a secure process. Tektagon BFR detects platform firmware attacks and prevents a compromised system from booting with corrupted firmware.

Advantage of Uninterrupted Runtime Security

In addition to detection and recovery at boot time, Tektagon BFR also delivers a key advantage during runtime to help meet detection and recovery requirements: by filtering to the SPI bus and providing auto-recovery of the PRoT firmware image during runtime, this uninterrupted filtering and recovery helps maintain performance and platform uptime.

Tektagon BFR Key Features	
Embedded Controller Design	RTOS-protected PRoT for dual use. HRoT chip can be integrated with embedded controller (EC).
Image Verification and Validation	PRoT Image. Complete firmware protection including Aptio® V and MegaRAC® SP-X boot blocks. Includes Secure Bootloader Authentication. SPI filtering during runtime.
Image Recovery	Auto-recovers on verification failure or forced recovery. Auto-update of recovery image with multi-stage auto-recovery. Supports Top Swap BIOS recovery. TOCTOU for BIOS/BMC when using CEC1736.
Cross-functional Firmware Attestation with Hardware Abstraction	Uses SPDM layer. Includes Attestation Firmware Manifest (AFM) Support and Manifest based Policy on attestation failure. Support in-band and out-of-band devices. PRoT measurement of TPM.
PRoT Firmware	Field updateable PRoT firmware with boot and rollback protection. Seamless firmware updates. Configuration with Firmware DevOps Project. Immutable Trust Code (Boot ROM). Supports embedded controller solution without need for dedicated microcontroller.
Platform Manifest Support with Signing	Includes Firmware Volume Manifest (FVM). Updates without updating PRoT firmware. PowerState verification policy.
Public/Private Key Management	OTP key storage with revocation and authentication support. PKCS signature verification of Host/BMC firmware. Revocation and re-provisioning injection through physical presence.
Hardware Security Accelerators	Supports AES-256, SHA-256, SHA-384, ECDSA
Advanced Operation and Management	Auto build, auto test, auto validate. Decommissioning and Recommissioning. Event logging.

Tektagon BFR 2.0 Specifications	
Host CPU Platform Types	Intel®, AMD, Arm®
Other Platforms	ASPEED, RISC-V®
Embedded Controller Support	Microchip® MEC152x & MEC170x
Dedicated PRoT Support	Microchip® CEC17x2 & CEC173x
Motherboard Device Support	BMC (with the CEC173x), BIOS Module, DC-SCM, HSM, TPM, OTP (Auth Keys)
EC Encryption	AES-256
Controller OS	FreeRTOS, Zephyr®, Bare Metal
Boot Firmware Compatibility	Aptio V, MegaRAC, Open BMC
I/O Support	SPI, I2C, SMBus, GPIO, eSPI
Tools Support	Image Verification, Platform Manifest Creation, Factory Validation, DICE, Linux® I2C, AMI CLEFS™, BMC Security Techpack
Compliance	NIST® SP 800-193, DMTF-SPDM, ECDSA-384, RSA, WDT Recovery

For more information please visit the request form at ami.com/contact