Tektagon CommunityEdition™

Platform Firmware Resiliency

Zero Trust Security Starts with Firmware

In today's IT landscape, there are more data, more devices, more architectures, and thus more vulnerabilities. The threat landscape continues to evolve with cybercriminals getting more and more sophisticated, realizing firmware vulnerability can be the underbelly of the compute infrastructure and once they can take control of a machine, it can serve as a gateway into organizations' sensitive data. Because of this, organizations' Zero Trust strategy must start with platform firmware security. In order to secure platform firmware, root of trust must be trustworthy and requires every firmware to be validated and trusted.

Tektagon CommunityEdition™

AMI Tektagon CommunityEdition leverages the open-source Platform Root of Trust (PRoT) solution with foundation firmware security features that detect platform firmware corruption, recover the firmware and protect firmware integrity. With support from the open- source community, Tektagon Community Edition augments transparency, resulting in high-quality code and improves implementation by providing greater customizability, and extensibility– resulting in a flexibly implementation for a wide range of platforms. Tektagon CommunityEdition is provided through the Open Compute Project (OCP) Repository.

Features:

- Utilizes ASPEED® AST1060 silicon
- Leverages the open-source community
- Intel® PFR 2.0 compatible
- Immutable Trust Code Boot ROM
- Image Verification
- Image Recovery
- SPI filtering during runtime
- SMBus filtering
- Configurable Modular Project
- Secure firmware update
- Attestation Support
- NIST® (SP 800-193) compliant

Tektagon CommunityEdition Core Features	
ASPEED Controller Flexibility	Able perform secure and authenticated boot of platform and root of trust functions
Cerberus PFR and Intel PFR 2.0 Detection, Protection and Recovery	HRoT Image. SPI filtering during runtime. Auto-recovers on verification failure.
Hardware Abstraction	Host Communication through I2C
HRoT Firmware	PRoT firmware with boot and rollback protection. Immutable Trust Code (Boot ROM). Configuration with Firmware DevOps Project.
Platform Manifest Support	Cerberus PFR. Intel PFR 2.0. 3k Signed PFM Block. Support for Intel PFR 2.0 SPI filtering.
Public/Private Key Management	OTP key storage with revocation and authentication support. Revocation and re-provisioning injection through physical presence.
Hardware Security Accelerators	Supports SHA-256, SHA-384, ECDSA-256, ECDSA-384
Advanced Operation and Management	Key decommissioning and Recommissioning. Event logging.

Tektagon CommunityEdition Specifications	
Host CPU Platform Types	Intel®, AMD, Arm®
HRoT Controller Support	ASPEED® AST1060
Motherboard Device Support	BMC, BIOS Module, DC-SCM, HSM, OTP (Auth Keys)
Controller OS	Zephyr®, Bare Metal
Boot Firmware Compatibility	Aptio V, MegaRAC, Open BMC
I/O Support	SPI, I2C, SMBus, GPIO
Tools Support	Platform Manifest Creation from BIOS/BMC part, Linux® I2C
Compliance	NIST® SP 800-193, RSA

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