Te Tektagon OpenEdition™

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 OpenEdition™

Tektagon OpenEdition™ is an 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 its open-source architecture, Tektagon OpenEdition™ augments transparency, resulting in high-quality code and improves implementation by providing greater customizability, extensibility and support for the open-source community – resulting in faster time-to-market. Tektagon OpenEdition™ is available for the open-source community through Open Compute Project® repository.

Features:

- Utilizes ASPEED® AST1060 silicon
- Open-source solution
- Intel® PFR 2.0 compatible
- Immutable Trust Code Boot ROM
- Image Verification
- Image Recovery
- Configurable Module Project
- Platform Manifest Support
- Field updatable HRoT FW
- SPI filtering during runtime
- I^{2}C/SMBus filtering
- Secure firmware update
- Key management
- Attestation Support
- NIST® (SP 800-193) compliant
- Suitable for entry server platforms
- Optional premium features and support packages

Why has AMI developed an open-source Root-of-trust solution?

AMI is driving the industry forward. Open-source firmware is a growing community in software development. Some of the largest companies in the world use open-source. Vast majority of enterprise IT leaders believe enterprise open-source provides flexibility to customize solutions to meet company's needs. AMI is embracing open-source through the Open Compute Project® and leveraging decades of firmware expertise to contribute innovative features back to the community and committed to contributing to the open-source community to encourage transparency, ownership, and security in the firmware ecosystem.

HIGHLIGHTS

- Open-source Solution – Improves implementation and augments transparency, resulting in high-quality firmware code due to open-source community.
- Detects, recovers, protects firmware – Provides rock-solid firmware security by preventing unauthorized tampering with platform firmware.
- Compatibility - Compatibility with AMI products such as Aptio, MegaRAC and 3rd party firmware.
- Customizability - Enables customizations for easier integration with peripheral platform interfaces.
- Extensibility - Empowers for the addition of new capabilities and functionality to platform security.
- Time-to-market - Simplifies design with optional support package for integration with other firmware to reduce cycle time.

Intel® is a registered trademark of Intel Corporation or its subsidiaries. AMD® is a registered trademark of AMD. ASPEED® is a registered trademark of ASPEED Technology Inc. Arm® is a registered trademark of Arm Limited or its affiliates. RISC-V® is a registered trademark of RISC-V International. NIST® is a registered trademark of National Institute of Standards and Technology. Open Compute Project® is a registered trademark of the Open Compute Project® in the U.S. and other countries.

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