Aptio® V Security Features

UEFI BIOS FIRMWARE SECURITY DEEP DIVE

REVISION 1.11.1 – APRIL 15, 2021

Aptio® V Security Features Deep Dive

04/15/2021

Revision History

2015-07-01	1.00	Initial Release
2018-10-24	1.01	Minor Changes
2019-04-09	1.02	Minor Changes
2020-10-05	1.10	Security Feature Additions
2021-04-09	1.11	Updated document template, updated screen captures
2021-04-15	1.11.1	Updated type of document to Deep Dive

Disclaimer

Although efforts have been made to assure the accuracy of the information contained here, AMI expressly disclaims liability for any error in this information, and for damages, whether direct, indirect, special, exemplary, consequential or otherwise, that may result from such error, including but not limited to the loss of profits resulting from the use or misuse of the User Guide or information contained therein (even if AMI has been advised of the possibility of such damages). Any questions or comments regarding this User Guide or its contents should be addressed to AMI at the address shown on the inside of the front cover.

AMI provides this publication "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a specific purpose.

Some states do not allow disclaimer of express or implied warranties or the limitation or exclusion of liability for indirect, special, exemplary, incidental or consequential damages in certain transactions; therefore, this statement may not apply to you. Also, you may have other rights that vary from jurisdiction to jurisdiction.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. AMI may make improvements and/or revisions in the product(s) and/or the program(s) described in this publication at any time.

Requests for technical information about AMI products should be made to your AMI authorized reseller or marketing representative.

Table of Contents

(Intentionally Blank)

Chapter 1 Introduction

AMI makes security an utmost priority. AMI takes preventative measures including implementing many of the industry standards including NIST SP 800-147 (Secure Flash), NIST SP 800-155 and UEFI Secure Boot. AMI has a fully custom TPM 1.2 and TPM 2.0 eModule as well as a Signing Server for managing keys and signing Aptio firmware. AMI also provides full support for Intel® Boot Guard and Intel® BIOS Guard.

AMI belongs to many security groups including UEFI Security Sub-team, UEFI Security Response Team, Trusted Computing Group (TCG) and we also have direct dealings with MITRE, LegbaCore, and Intel Offensive Security Research. Being part of these groups lets AMI keep up with the latest in security measures and helps make sure that AMI Aptio is as secure as possible. AMI takes a proactive step on security threats and takes immediate action to make sure all AMI Aptio products are not vulnerable to the threats. AMI also follows secure development methodologies and performs penetration testing on Aptio. For additional information please contact your AMI representative.

AMI has noticed features missing from some of the security specifications that certain customers have needed. AMI worked tirelessly with these customers to give them the security features that meet their needs. Contact an AMI sales representative for more information.

(Intentionally Blank)

Chapter 2 AMI Industry Security Engagements

NIST and NCCoE

In 2019, AMI joined the National Cybersecurity Excellence Partnership (NCEP) at the National Cybersecurity Center of Excellence (NCCoE). The NCEP is a public-private partnership that offers U.S. companies the opportunity to form a long-term relationship with the NCCoE, whose mission is to collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs. AMI will work with the NCCoE to ensure AMI products provide solutions that satisfy NIST requirements and guidelines.

AMI contributed to a joint effort Internal Report by Intel, NIST, and AMI – "Foundational Container Platform Security Prototype."

AMI participated in a new NIST project with various key industry players surrounding 5G Cybersecurity. This will lead to the creation of a NIST Special Publication SP 1800-XXX.

AMI is working with renowned security leaders to help ensure AMI customers have secure products with trusted case studies for end users.

Cloud Security Industry Summit (CSIS)

AMI has participated in the CSIS Working Groups hosted by Intel, together with key industry players for cloud computing. AMI has contributed to the creation of the CSIS whitepaper "Case for Trustworthy BMC."

AMI has also developed some SP-X Security enhancements related to CSIS work, which will be useful to all customers regardless of market segment.

FIRST.org and TianoCore

AMI has participated in FIRST.org activities, including the PSIRT Working Group, 3rd Party Components Working Group, and PSIRT Tooling Working Group. AMI is also a 2021 FIRST.org Conference Program Committee member and will assist in planning the conference.

AMI participates in the TianoCore Security Working Group and has volunteered to manage CVE Numbering Authority responsibilities (issuing CVEs) for TianoCore.

Colorado State University

AMI has engaged with security researchers and established a security lab at Colorado State University Fort Collins. These research activities included 3rd party code analysis

and penetration testing of AMI IP, as well as researching ways to improve SAST results for firmware.

Together with CSU, AMI is member of the National Science Foundation (NSF) Center for Cybersecurity Analytics and Automation (CCAA), a multi-University National Science Foundation Industry/University Cooperative Research (I/UCRC) center.

Chapter 3 Security Features

Trusted Platform Module (TPM)

Trusted Platform Module (TPM) is an international standard that uses a dedicated microcontroller that can be used to authenticate a platform. The TPM specification is written by the Trusted Computing Group (TCG). TPM offers ways to securely generate cryptographic keys with a limitation on their use. There are many use cases for TPM including platform integrity, disc encryption and password protection. There are currently two main versions of TPM: TPM 1.2 and TPM 2.0. TPM 2.0 provides better security algorithms and more flexibility in the algorithms used.

AMI provides a TPM 2.0 eModule that provides support for both TPM 2.0 and TPM 1.2 as well as a separate TPM 1.2 only eModule. AMI's solution also provides Intel and AMD firmware TPM support. For further information on Trusted Platform Modules, please refer to the Trusted Computing Group's website.

TPM Based Password

The TPM Password Support eModule allows a platform to use TPM2.0 discrete devices for the management of the AMI TSE Setup password. This allows hardware-enabled security to protect Administrator and User passwords in the firmware environment.

TCG Storage Security

TCG OPAL is a storage security subsystem class and provides protocols for its security feature interface. The TCG OPAL specification includes mechanisms for managing access control to user data stored on the Storage Device, including controlling media encryption, key management, and read/write lock state.

AMI has developed the TcgStorageSecurity eModule in Aptio5.x to provide full support for the TCG OPAL standard in order to manage security features of native OPAL drives, including self-encrypting drives (SEDs).

NIST SP 800-147 (Secure Flash)

NIST 800-147 provides guidelines for a secure BIOS update mechanism. A secure BIOS update must include:

- A process for verifying the authenticity and integrity of BIOS updates.
- A mechanism for ensuring that the BIOS is protected from modification from the signing of the BIOS ROM image to the actual BIOS update.

AMI has a fully custom Secure Flash solution with images that are signed in conformance with digital signature algorithms specified within NIST SP 800-147 guidelines. AMI's

solution employs standard crypto protocols with a 2048bit RSA key and SHA256 hash. For more information on Secure Flash see the NIST BIOS Protection Guidelines.

NIST SP 800-155 (BIOS Integrity Measurement Guidelines)

The purpose of NIST 800-155 is to ensure the integrity of the BIOS at boot time. This is done by generating a 'Golden Measurement' value at build time and placing it into a signed file in the Platform Configuration Registers. When the computer boots the BIOS code will calculate the integrity value of the current BIOS and compares this value with the 'Golden Measurement' calculated at build time. If the values do not match then an event can occur, which could be notifying the user or prevent the system from booting. This event is customizable by the customer.

AMI has developed a full solution that meets the requirements of NIST SP 800-155 and has integrated it into the standard TCG eModule. For more information on NIST SP 800-155 see the NIST BIOS Integrity Measurement Guidelines.

NIST SP 800-193 (Platform Firmware Resiliency Guidelines)

Intel® Platform Firmware Resilience (Intel® PFR)

Intel® Platform Firmware Resilience (Intel® PFR) protects critical firmware during boot and runtime attacks. In the case malware is detected, Intel PFR will perform a recovery to a gold image.

AMI's Aptio V provides full support for Intel PFR.

UEFI Secure Boot

UEFI Secure Boot guarantees that Option ROMs, bootloaders, drivers, and applications outside of the BIOS firmware are authorized to run. Secure Boot has two databases of keys, one that is keys that are allowed, and one is keys that are not allowed. When the computer is booting the signature of the additional code will be compared to the keys in the two databases. Then depending on the build configuration of the BIOS; the computer could halt the boot process or warn the user of invalid signatures.

AMI Aptio V provides full support for UEFI Secure Boot requirements and provides additional features including the ability to manually specify that a boot loader is valid from within default setup menus. This way Secure Boot can still be enabled but will allow code that a user trusts to be executed. This feature can be enabled/disabled by the OEM/ODM. For more information on Secure Boot see UEFI Secure boot in Modern Computer Security Solutions.

AMD Platform Secure Boot (AMD PSB)

PSB is intended to assert, by a root of trust anchored in the H/W, the integrity and authenticity of a portion of System ROM image before it can execute.

AMI's AptioV provides full support for AMD PSB.

AMD Secure Encrypted Virtualization (SEV)

AMD Secure Encrypted Virtualization (SEV) Uses one key per virtual machine to isolate guests and the hypervisor from one another. The keys are managed by the AMD Secure Processor. SEV requires enablement in the guest operating system and hypervisor. The guest changes allow the VM to indicate which pages in memory should be encrypted. The hypervisor changes use hardware virtualization instructions and communication with the AMD Secure processor to manage the appropriate keys in the memory controller.

AMI's Aptio V provides full support for AMD SEV.

AMD Transparent Secure Memory Encryption (TSME)

While SME provides a lot of flexibility for managing main memory encryption, it does require support in the OS/HV. For systems that desire only the physical protection of SME but run legacy OS or HV software, they may use a mode called Transparent SME (TSME). In TSME, all memory is encrypted regardless of the value of the C-bit on any particular page. This mode provides a simple method to enable encryption without requiring software modifications.

AMI's Aptio V provides full support for AMD TSME.

AMD PSP Firmware Anti-Rollback

AMD PSP's firmware Anti-Rollback is a feature to prevent firmware to be rollbacked to old versions.

AMI's Aptio V provides full support for AMD PSP firmware Anti-Rollback.

Intel® Boot Guard

Intel Boot Guard is a hardware-based boot integrity protection that prevents unauthorized software and malware takeover of boot blocks critical to a system's function, thus providing added level of platform security based on hardware. Please refer to Intel documentation for further information on this feature.

AMI's Aptio V provides full support for Intel Boot Guard.

Intel® BIOS Guard

Intel BIOS Guard is an augmentation of existing chipset-based BIOS Flash protection capabilities targeted to address the increasing malware threat to BIOS flash storage. It protects the BIOS flash from modification without platform manufacturer authorization, helps defend the platform against direct low-level attacks of the BIOS Flash. Please refer to Intel documentation for further information on this feature.

AMI's Aptio V fully supports Intel BIOS Guard.

Intel® Trusted Execution Technology (Intel® TXT)

Intel® Trusted Execution Technology is a set of hardware extensions to Intel® processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution. Intel Trusted Execution Technology provides hardware-based mechanisms that help protect against software-based attacks and protects the confidentiality and integrity of data stored or created on the client PC.

AMI's Aptio V provides full support for Intel TXT.

Intel® Software Guard Extensions (Intel® SGX)

Intel Software Guard Extensions (Intel SGX) offers hardware-based memory encryption that isolates specific application code and data in memory. Intel SGX allows user-level code to allocate private regions of memory, called enclaves, which are designed to be protected from processes running at higher privilege levels. Intel SGX helps protect against many known and active threats. It adds another layer of defense by helping reduce the attack surface of the system

AMI's Aptio V provides full support for Intel SGX.

Intel® Virtualization Technology (Intel® VT)

Intel® Virtualization Technology abstracts hardware that allows multiple workloads to share a common set of resources. On shared virtualized hardware, a variety of workloads can co-locate while maintaining full isolation from each other, freely migrate across infrastructures, and scale as needed.

AMI's Aptio V provides full support for Intel VT.

Intel® Multi-Key Total Memory Encryption (Intel® MKTME)

Total Memory Encryption (TME) – provides the capability to encrypt the entirety of the physical memory of a system. Multi-Key Total Memory Encryption (MKTME) builds on TME and adds support for multiple encryption keys. Software manages the use of keys and can use each of the available keys for encrypting any page of the memory.

AMI's Aptio V provides full support for Intel MKTME.

Intel® Nifty Rock

Intel® Nifty Rock provides SMM code minimal access to IO, Memory, MSR and Save State Area. This will help in reducing the vulnerability in SMM handlers.

AMI's Aptio V provides full support for Intel Nifty Rock.

Arm Trusted Board Boot (TBB)

The Trusted Board Boot (TBB) feature prevents malicious firmware from running on the platform by authenticating all firmware images up to, and including, the normal world bootloader. It does this by establishing a Chain of Trust using Public-Key-Cryptography Standards (PKCS).

AMI's Aptio V provides full support for Arm TBB.

Device Firmware Configuration Interface (DFCI)

With Windows Autopilot Deployment and Intune, you can manage Unified Extensible Firmware Interface (UEFI) settings after they are enrolled by using the Device Firmware Configuration Interface (DFCI). DFCI enables Windows to pass management commands from Intune to UEFI for Autopilot deployed devices. This capability allows you to limit end user's control over BIOS settings. For example, you can lock down the boot options to prevent users from booting up another OS, such as one that does not have the same security features.

AMI's Aptio V has included the UEFI components required to fully support DFCI.

Device Guard

Device Guard is a combination of enterprise-related hardware and software security features in Windows 10 that, when configured together, will lock a device down allowing only trusted applications defined in code integrity policies to be executed.

AMI's Aptio V provides full support for Device Guard.

AMI CLEFS

Having signing keys on each engineer's machine can be a security risk. These keys are most likely not protected in any manner and are more easily compromised. A Hardware Security Module (HSM) is the best solution for key management, but they are very expensive, so AMI has partnered with Thales to offer a solution to enable signing for multiple industry standard technologies

with cloud HSM integration. AMI CLEFS also allows for post-build signing and integration with on-site HSMs.

See AMI CLEFS on ami.com/clefs for more details.

AmiTrustedFv

AMI's AmiTrustedFv eModule extends code root of trust from PEI (verified by hardware root of trust (HRoT)) to DXE. Complements Intel Boot Guard or AMD PSB.

HDD Security

AMI's Aptio V HddSecurity eModule provides support to manage security features in HDDs and NVMe drives based on the SAT3 security protocol. This security implementation checks drives for security support, allows enabling/disabling of HDD security in setup, and provides password prompts for locked drives.

Media Sanitization

Sanitization is viewed as an integral part of security policy and keeps data under organizational control. Organizations and governments should establish security policies focusing on lifecycle management, risk management, and asset management. Media sanitization ensures that data is only available on controlled systems and is wiped when the system is decommissioned and scrapped or transitioned to other departments.

AMI's Aptio V MediaSanitization eModule is an implementation of the DOD 5220-22-M and NIST SP800-88 specifications and supports clearing and purging of data on storage devices.

System Password

AMI has developed a system password feature that allows continuation of BIOS POST only after a user has entered the correct password. It can also be configured to check for a password only upon entering Setup.

IOMMU

An MMU is used by the CPU to translate a virtual address to a physical address. The virtual address of the MMU is in the CPU's view. The IOMMU, in contrast, is used by device to translate another virtual address called IOVA (IO virtual address) to physical address.

AMI has integrated full support for IOMMU in Aptio V.

Custom Security Solutions

AMI is has worked with customers in the past to create custom solutions that meet their needs. Please contact AMI if you are interested in developing further security solutions.

(Intentionally Blank)