TSP

Tyrone Secure Platform

Add-on-Module TCG 1.2 / 2.0 -FIPS

The Tyrone Trusted Platform Module (TCG 2.0) is a hardware-based security device that can be added to a system motherboard to hold computer generated keys for encryption. This outstanding solution ensures that information keys, passwords and digital certificates will be more secure from external software attacks and physical theft, by performing all cryptographic functions on the device. Tyrone TPM (TCG 2.0) is an ideal tool for customers who are looking for an additional layer of security to their Tyrone Servers.

Specifications

Physical Dimensions

26.13mm x 14.64mm x 9.93mm

Security Features

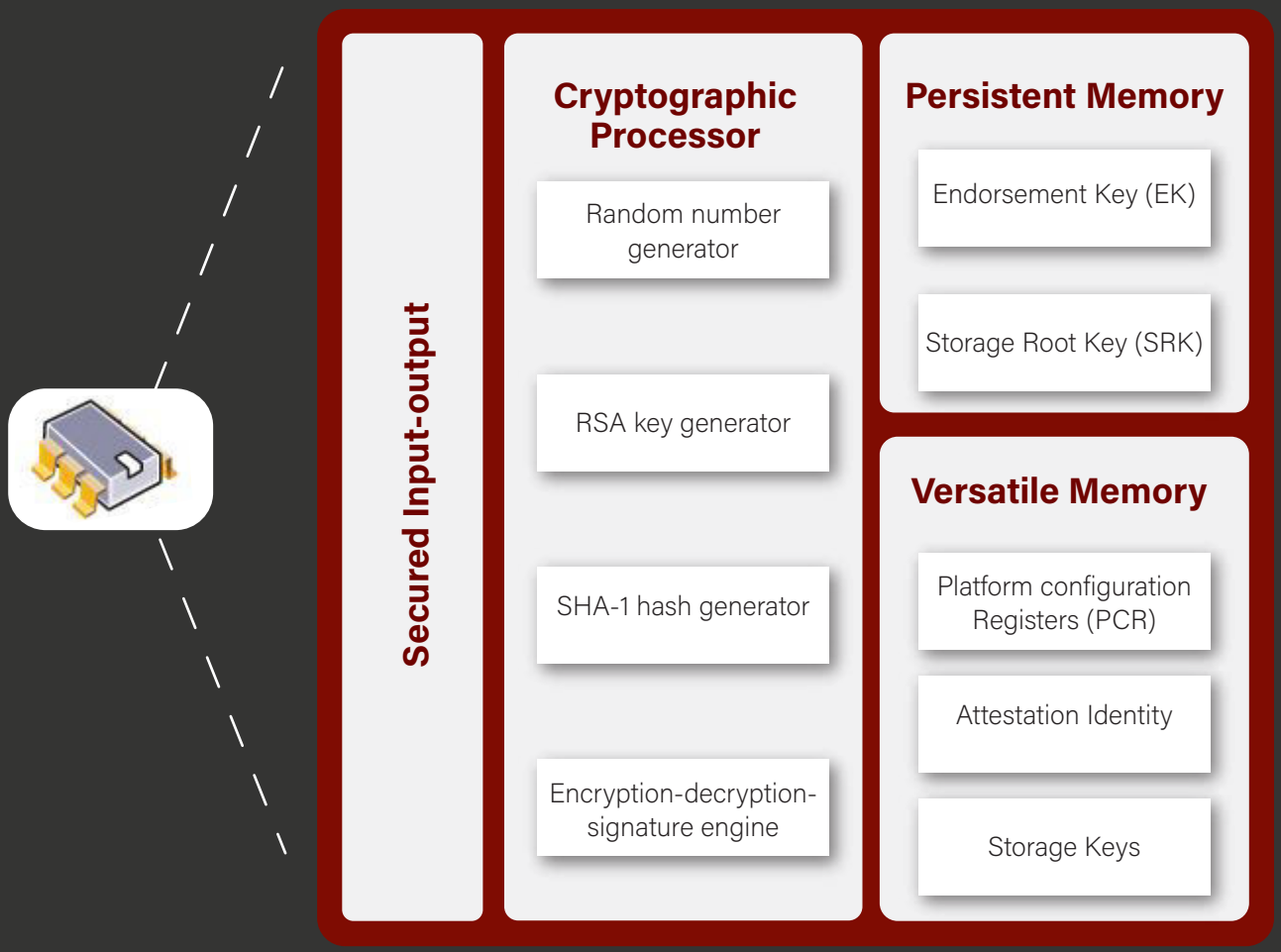
Over/Under voltage Detection
Low frequency sensor
High frequency filter
Reset filter
Memory Encryption/Decryption (MED)

System Lockdown

System Lockdown is a security feature that prevents all system configuration changes including firmware updates.

Application Supports

Microsoft Tools
Mozilla Firefox™
Mozilla Thunderbird™
Netscape Communicator
Google Chromebook
Google Chromebox
Microsoft Encrypted File System
RSA Secure ID
Check Point r▪ SecuRemote/SecureClient
Check Point™ VPN-1/FireWall-1 NG
Entrust™ Desktop Manager Solutions
Adobe™ Acrobat 6.0 Professional
GemSafe for TPM / Smart Card



Key Features

TCG 2.0 compliant trusted platform module (TPM)
Compliant embedded software
EEPROM for TCG firmware enhancements and for user data and keys
Hardware accelerator for SHA-1 and SHA-256
Random Number Generator (RNG)
Meeting Intel TXT, Microsoft Windows and Google Chromebook certification criteria Protection against Dictionary Attack
SPI interface
Intel Trusted Execution Technology Support
AMO Secure Virtual Machine Architecture Support
Protection and Secrecy of the cryptographic system both for reading out and manipulation of the material.
Pre-Generation of RSA Keys
Power saving sleep mode
3.3 V power supply
Built-in support by Linux Kernel
Operating temperature range: -20"C to +B0"C
Root-of-Trust

Compliance

RoHS, CC EAL4+ certified TPM Chipset (SLB9672), FIPS 140-2

WHITEPAPER - TYRONE SERVERS SDI200/SDA200 SERIES – SECURITY FEATURES

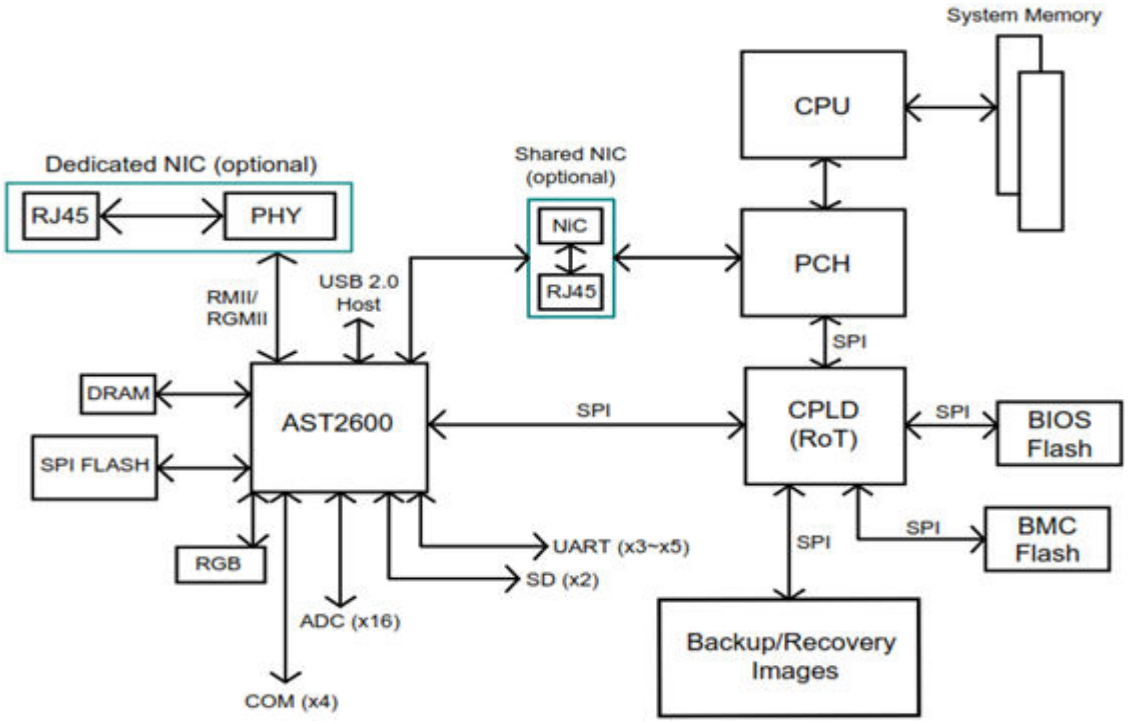
Tyrone Servers supports a variety of system security options designed to prevent unauthorized system access or tampering of server settings.

The Baseboard Management Controller (BMC) provides remote access to multiple users at different locations for networking. It also allows a system administrator to monitor system health and manage computer events remotely.

BMC operates independently from the operating system. With the AST2600 controller and the BMC firmware built in, the motherboard allows the users to access, monitor, diagnose, and manage a remote server via Console Redirection. It also provides remote access to multiple users from different locations for system maintenance and management.

The various security features were implemented for the BMC firmware stack built on the ASPEED AST 2600 controller. System security options supported include –

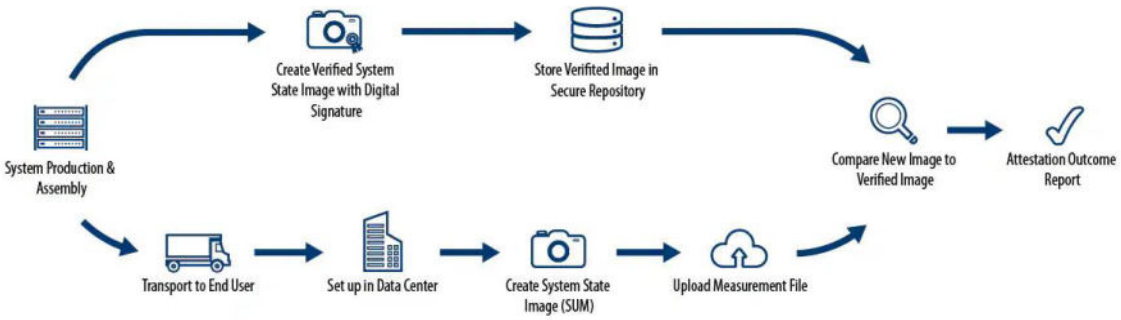
1. Platform inventory Check
2. Chassis Intrusion Detection
3. Password protection, Front panel lockout & Dynamic USB Port enable/disable
4. Platform Firmware Resilience (PFR)
5. Unified Extensible Firmware Interface (UEFI) Secure Boot Technology with Secure Start
6. Cryptographically Signed Firmware updates
7. System Lockdown Mode
8. Trusted Platform Module (TPM 2.0)
9. Intel® Trusted Execution Technology (Intel® TXT) for Intel Platforms



AST2600 Block Diagram

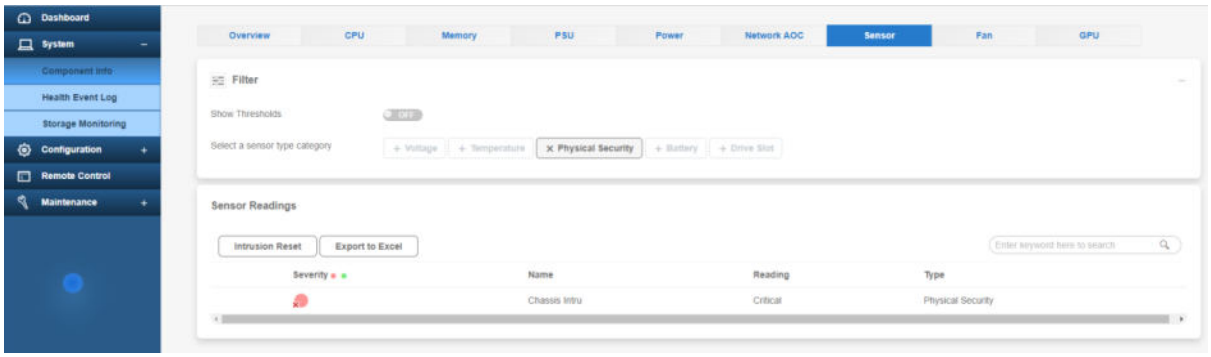
1. Platform inventory Check

To ensure smooth Day One operation, it is highly recommended that your systems are verified using Tyrone's system attestation process. System attestation enables you to authenticate the state of your Tyrone system, components, and firmware, and ensure that they match the state of when they left factory premises. Attestation will detect any changes in the composition of your hardware and firmware through cryptographic signing, thereby guaranteeing the state of your server, while identifying and reporting any unauthorized changes.



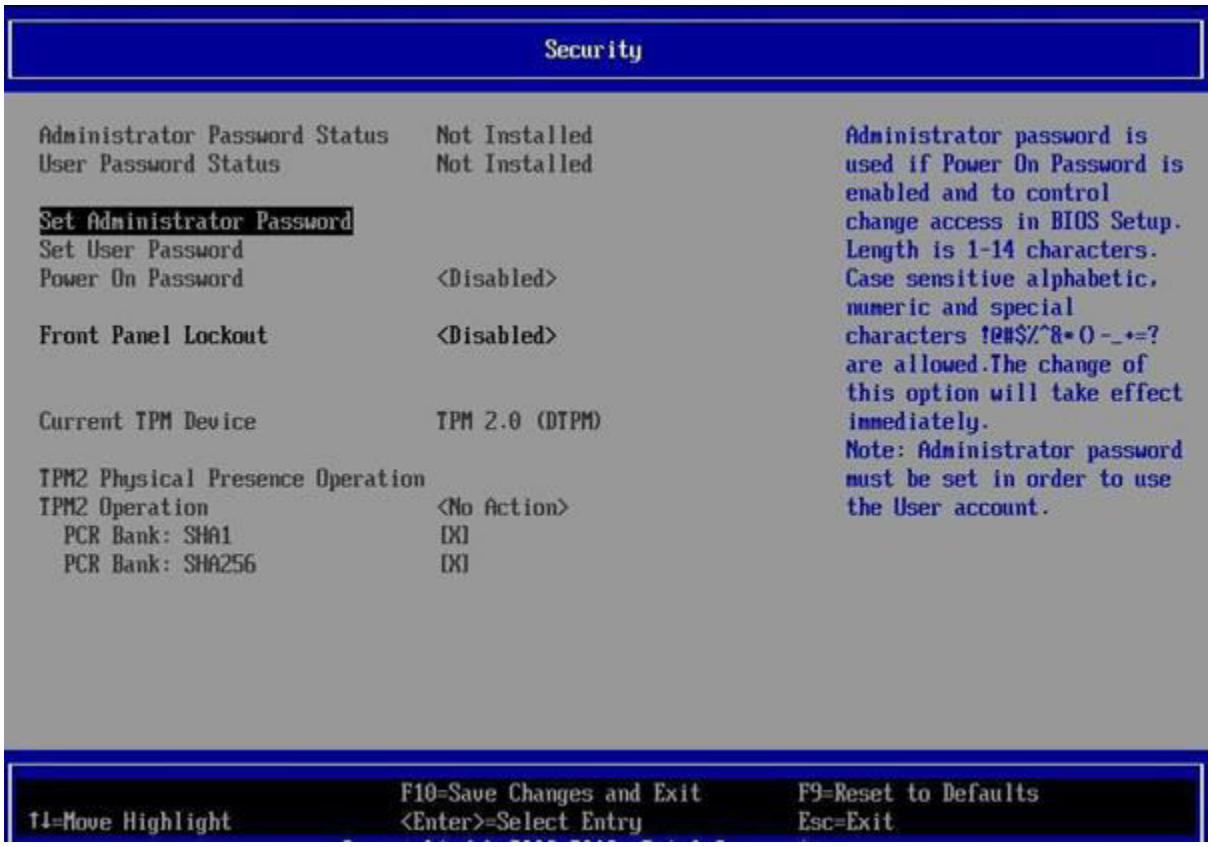
2. Chassis Intrusion Detection

Chassis intrusion detection, also known as physical intrusion detection or tamper detection, is a security feature that specifically focuses on detecting unauthorized access or tampering with the physical components of electronic devices. It is designed to monitor and protect the integrity of a device's chassis, which houses its critical internal components



3. Password Protection, Front panel lockout & Dynamic USB Port enable/disable

The BIOS Setup utility includes a Security tab where options to configure passwords, front panel lockout, and TPM settings, can be found. Dynamic enable/disable of ports (USB etc.) is supported in Tyrone Servers



i. Password Setup

The BIOS uses passwords to prevent unauthorized access to the server board. Passwords can restrict entry to the BIOS Setup utility, restrict use of the Boot Device popup menu during POST, suppress automatic USB device re-ordering, and prevent unauthorized system power-on. It is strongly recommended that an administrator password be set. A system with no administrator password set allows anyone who has access to the server board to change BIOS settings.

An administrator password must be set in order to set the user password.

The maximum length of a password is 14 characters. The minimum length is one character. The password can be made up of a combination of alphanumeric (a-z, A-Z, 0–9) characters and any of the following special characters:

! @ # $ % ^ & * ( ) - _ + = ? Passwords are case sensitive.
The administrator and user passwords must be different from each other. An error message is displayed, and a different password must be entered if there is an attempt to enter the same password for both. The use of strong passwords is encouraged, but not required. To

meet the criteria for a strong password, the password entered must be at least eight characters in length. It must include at least one each of alphabetic, numeric, and special characters. If a weak password is entered, a warning message is displayed, and the weak password is accepted. Once set, a password can be cleared by changing it to a null string. This action requires the administrator password and must be done through BIOS Setup. Clearing the administrator password also clears the user password. Passwords can also be cleared by using the password clear jumper on the server board. For more information on the password clear jumper, see Section 13.2.

Resetting the BIOS configuration settings to default values (by any method) has no effect on the administrator and user passwords.

As a security measure, if a user or administrator enters an incorrect password three times in a row during the boot sequence, the system is placed into a halt state. A system reset is required to exit out of the halt state. This feature makes it more difficult to guess or break a password.

In addition, on the next successful reboot, the Error Manager displays a Major Error code 0048. A SEL event is also logged to alert the authorized user or administrator that a password access failure has occurred.

ii. System Administrator Password Rights

When the correct administrator password is entered, the user may perform the following actions:

- Access the BIOS Setup utility.
- Configure all BIOS Setup options in the BIOS Setup utility.
- Clear both the administrator and user passwords.
- Access the Boot Menu during POST.

If the Power On Password function is enabled in BIOS Setup, the BIOS halts early in POST to request a password (administrator or user) before continuing POST.

iii. Authorized System User Password Rights and Restrictions

When the correct user password is entered, the user can perform the following actions:

- Access the BIOS Setup utility.
- View, but not change, any BIOS Setup options in the BIOS Setup utility.
- Modify system time and date in the BIOS Setup utility.

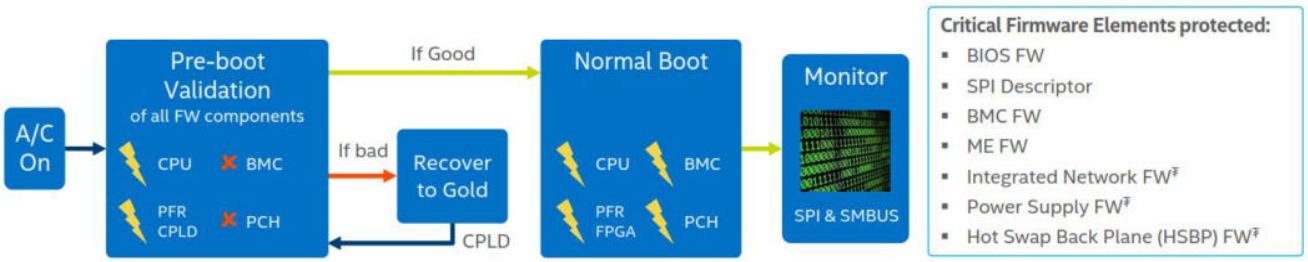
If the Power On Password function is enabled in BIOS Setup, the BIOS halts early in POST to request a password (administrator or user) before continuing POST.

Configuring an administrator password imposes restrictions on booting the system and configures most setup fields to read-only if the administrator password is not provided. The boot popup menu requires the administrator password to function, and the USB reordering is suppressed as long as the administrator password is enabled. Users are restricted from booting in anything other than the boot order defined in setup by an administrator.

4. Platform Firmware Resilience

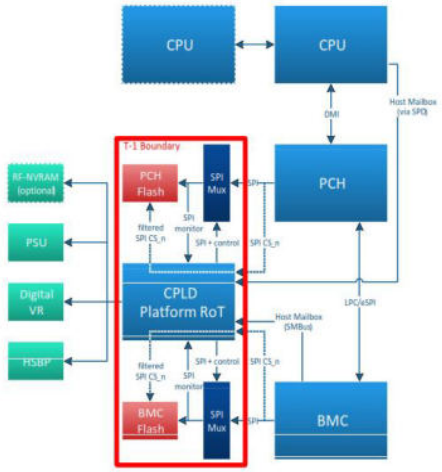
Platform Firmware Resilience (PFR) is an FPGA-based solution, that helps protect the various platform firmware components. It provides Silicon Root-of-Trust integrated in Platform for Pre-Boot and Run time Security of BIOS, BMC etc.

PFR monitors and filters malicious traffic on the system buses. It also verifies the integrity of platform firmware images before any firmware code is executed. And most significantly, it can even restore corrupted firmware automatically from a protected known-good recovery image. Data center owners now have additional options to help protect against permanent denial of service firmware attacks with Platform Firmware Resilience.



PFR functional diagram

Features :



- CPLD acts a standalone Platform RoT
- Leverages Boot Guard for defense in depth
- Isolated pre-boot mode (T-1) for authentication and recovery of all platform FW
- CPLD PRoT is RoT for Update for the platform FW
- Protects SPI and SMBus devices against corruption (PDoS, damage of components)

CPLD features

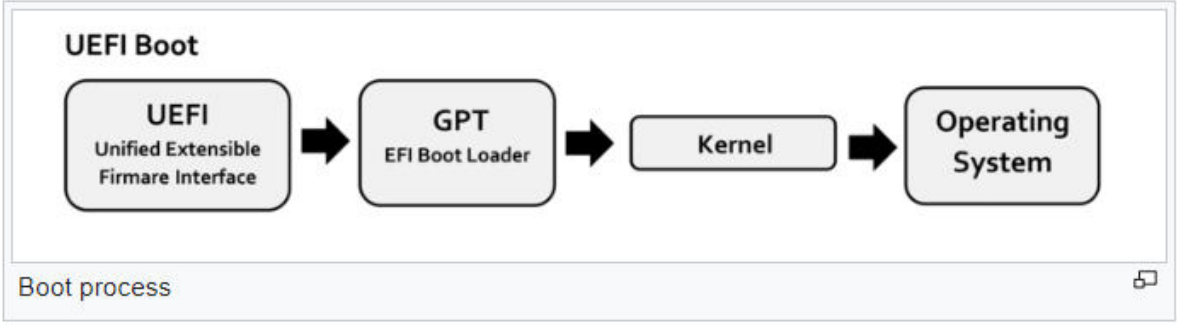
5. Unified Extensible Firmware Interface (UEFI) Secure Boot Technology

The Unified Extensible Firmware Interface (UEFI) is a firmware that runs when the computer is booted. It initializes the hardware and loads the operating system into the memory

Unlike BIOS, UEFI doesn't look for the MBR in the first sector of the Boot Device. It maintains a list of valid boot volumes called EFI Service Partitions. During the POST procedure, the UEFI firmware scans all of the bootable storage devices that are connected to the system for a valid GUID Partition Table (GPT), which is an improvement over MBR. Unlike the MBR, GPT doesn't contain a Boot-Loader. The firmware itself scans the GPT to find an EFI Service Partition to boot from, and directly loads the OS from the right partition.

UEFI provides the feature of Secure Boot. It allows only authentic drivers and services to load at boot time, to make sure that no malware can be loaded at computer startup. It also requires drivers and the Kernel to have a digital signature, which makes it an effective tool in countering piracy and boot-sector malware.

UEFI secure boot technology defines how a platform's firmware can authenticate a digitally signed UEFI image, such as an operating system loader or a UEFI driver stored in an option ROM. This provides the capability to ensure that those UEFI images are only loaded in an owner authorized fashion and provides a common means to ensure platform security and integrity over systems running UEFI-based firmware.



Boot process

6. Cryptographically Signed Firmware updates

We had added the capability to cryptographically sign the software to ensure the authenticity of the software download better. Signs the BMC software automatically for all products. Upon installation of new BIOS or BMC Firmware, the software signature is checked to ensure the contents of the software have not been modified.

Due to issues of backward compatibility, we are making the upgrade to these new features optional for existing systems. Once the functionality is enabled, customers cannot go back to previous, unsigned software versions, which is problematic for customers who have locked-down their systems to a specific firmware version.

7. System Lockdown Mode

Tyrone BMC solution can support the System Lockdown feature, and it offers IT administrators a secure way to prevent unintentional system configuration changes. All system configuration changes, including firmware updates, are restricted when system lockdown is enabled. As a result, the ordinary user only receives notifications when the IT administrator makes a system configuration change.

8. Trustet Platform Module (TPM)

Trusted Platform Module with TCG 2.0, stores information such as keys; password and digital certificates and provides additional security against external software attacks and from physical theft to systems.

TPM implements Root-of-Trust, which initiates during system boot process to establish trust level, gathering measurements about the running environment, OS, for trusted reporting. Security of the whole system is based on the protection and secrecy of the cryptographic system, especially against reading out or manipulation of the key material.

TPM provides a computing system the ability to run applications more securely, run a more secured remote access environment, as well as perform electronic transactions and digital communications more safely and security.

Key Features –

Strong authentication – Hardware module TPM and Software TXT to provide two-factor authentication

TPM leverages Intel's Trusted Execution Technology (Intel® TXT) to strengthen platforms from the emerging threats of hypervisor attacks, BIOS, or other firmware attacks, malicious root kit installations, or other software based attacks. It increases protection by enabling isolation in the boot process.

TPM with Intel® TXT, gives IT and security organizations critical enhancements to help ensure more secure platforms.

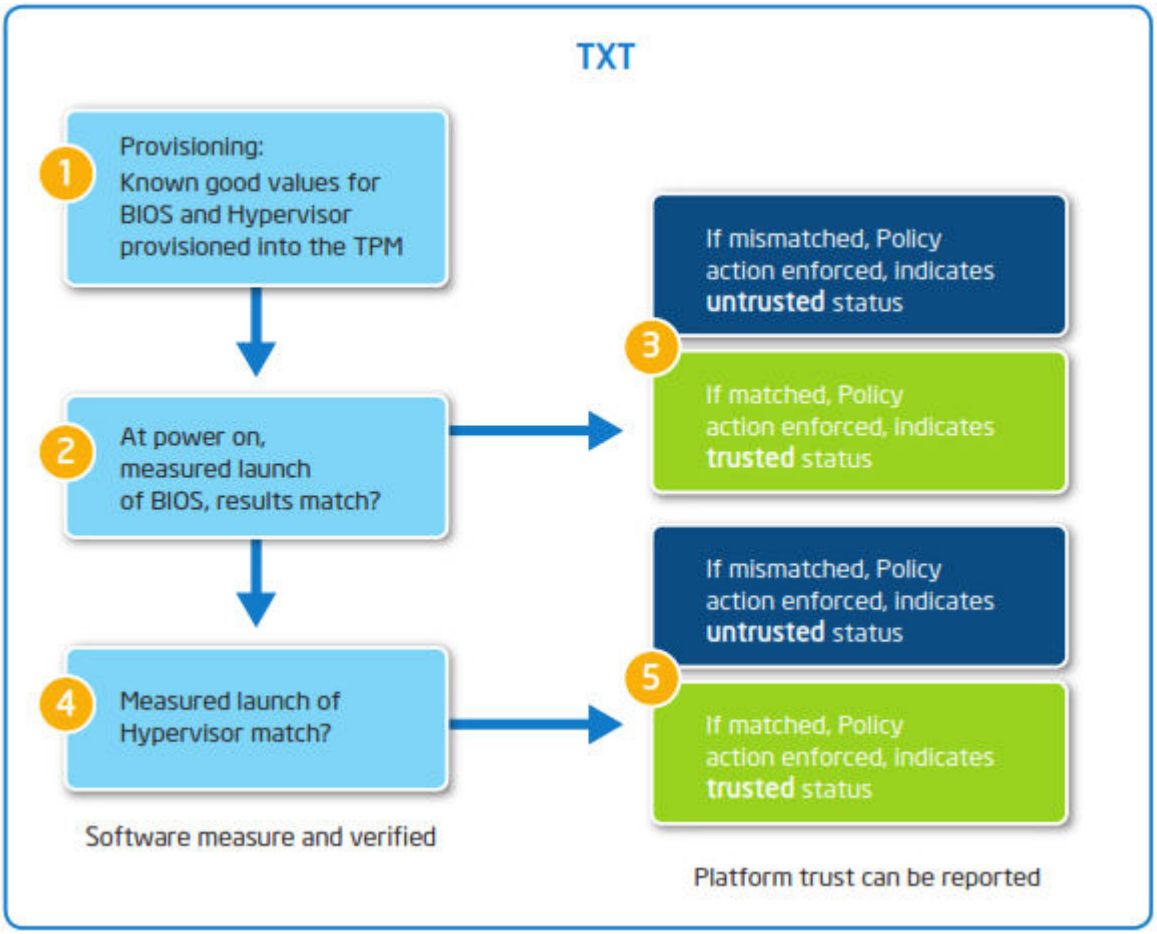
Enhanced Security for Virtual Environment - It extends the Virtual Machine Extensions (VMX) environment of Intel® Virtualization Technology (Intel® VT), permitting a verifiably secure installation, launch, and use of a hypervisor or operating system (OS).

It also provides greater application, data, or virtual machine (VM) isolation; and improved security or compliance audit capabilities. Not only can it help reduce support and remediation costs, it can also provide a foundation for more advanced solutions as security needs change to support increasingly virtualized or "multi-tenant" shared data center resources.

9. Intel® Trusted Execution Technology (Intel® TXT) for Intel Platforms

Trusted Execution Technology is a versatile 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. It enables an environment where applications can run within their own space, protected from all other software on the system.

TXT works by creating a Measured Launch Environment (MLE) that enables an accurate comparison of all the critical elements of the launch environment against a known good source. TXT creates a cryptographically unique identifier for each approved launch- enabled component and then provides hardware-based enforcement mechanisms to block the launch of code that does not match approved code.



TXT protects a virtual server environment data center

TXT provides :

- Verified Launch. A hardware-based chain of trust that enables launch of the MLE into a “known good” state. Changes to the MLE can be detected through cryptographic (hash-based or signed) measurements.

- Launch Control policy (LCp). A policy engine for the creation and implementation of enforceable lists of “known good” or approved, executable code.
- Secret protection. Hardware-assisted methods that remove residual data at an improper MLE shutdown, protecting data from memory-snooping software and reset attacks.

- Attestation. The ability to provide platform measurement credentials to local or remote users or systems to complete the trust verification process and support compliance and audit activities.

Security Methodology

1. **NIST SP 800-193**

Platform Firmware Resiliency Guidelines

Date Published: May 2018

Author(s)
Andrew Regenscheid (NIST)

Abstract
This document provides technical guidelines and recommendations supporting resiliency of platform firmware and data against potentially destructive attacks. The platform is a collection of fundamental hardware and firmware components needed to boot and operate a system. A successful attack on platform firmware could render a system inoperable, perhaps permanently, or requiring reprogramming by the original manufacturer, resulting in significant disruptions to users. The technical guidelines in this document promote resiliency in the platform by describing security mechanisms for protecting the platform against unauthorized changes, detecting unauthorized changes that occur, and recovering from attacks rapidly and securely. Implementers, including Original Equipment Manufacturers (OEMs) and component/device suppliers, can use these guidelines to build stronger security mechanisms into platforms. System administrators, security professionals, and users can use this document to guide procurement strategies and priorities for future systems.
https://csrc.nist.gov/pubs/sp/800/193/final

2. NIST SP 800-147B

BIOS Protection Guidelines for Servers

Date Published: August 2014

Author(s)
Andrew Regenscheid (NIST)

Abstract
Modern computers rely on fundamental system firmware, commonly known as the Basic Input/Output System (BIOS), to facilitate the hardware initialization process and transition control to the hypervisor or operating system. Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS's unique and privileged position within the PC architecture. The guidelines in this document include requirements on servers to mitigate the execution of malicious or corrupt BIOS code. They apply to BIOS firmware stored in the BIOS flash, including the BIOS code, the cryptographic keys that are part of the Root of Trust for Update, and static BIOS data. This guide is intended to provide server platform vendors with recommendations and guidelines for a secure BIOS update process.

https://csrc.nist.gov/pubs/sp/800/147/b/final

Tyrone

facebook.com/tyronesystems
twitter.com/tyronesystems
linkedin.com/company/tyrone-systems

Let's Talk

Press Inquiries
Email: info@tyronesystems.com

Support Inquiries
Email: tyronecare@tyronesystems.com

Partner Inquiries
Email: info@tyronesystems.com