Increase Security with TPM, Secure Boot, and Trusted Boot

By Vibhoosh Gupta

Published: 2024-08-27 · Archived: 2026-04-05 17:56:14 UTC

Increase Security with TPM, Secure Boot, and Trusted Boot

 Control systems must be secure by design and should have a hardware root of trust as the foundation of all the security constructs in the control system. Emerson PLC/PAC controllers come with Trusted Platform Module (TPM) technology that enables hardware root of trust. All PLC/PAC boot firmware is signed by Emerson with the private key stored in the TPM to ensure only Emerson-signed firmware will run on the hardware. Patches supplied by Emerson are also signed for verification purposes prior to loading. Here’s why TPM is important.

Trusted Platform Module

The Trusted Platform Module (TPM) is a separate hardware module with a dedicated microcontroller providing cryptographic key generation and key storage capability. Since each TPM chip has a unique and secret RSA key pair burned in, it can perform platform authentication. Software can use the TPM to authenticate other hardware devices. The TPM can be used for both encryption and decryption operations and is an excellent source of entropy for random number generation. The random number generator makes it virtually impossible for any other system to guess the generated sequence. This capability, when combined with the server public key, creates an encrypted link between two ends. The TPM generates a non-repeatable number that makes it difficult for outside influences to decipher the data being transmitted. The TPM can be implemented on any computer platform and is required by the United States Department of Defense (TPM version 1.2 or higher) for many of their devices, including phones and computers. TPM forms a “hardware root of trust” when used in conjunction with BIOS. Root of Trust (RoT) is a set of functions in the trusted computing module that is always trusted by the computer's operating system (OS). The RoT serves as a separate computer engine, controlling the trusted computing platform cryptographic processor on the device in which it is embedded. TPM allows secure storage and reporting of security metrics that can be used to randomly validate the system’s configurations to ensure changes haven’t occurred. Remote Attestation, an authentication process, can be facilitated when the TPM creates a nearly unforgeable hash key that is a signature of the hardware and software configuration. This could allow third-party systems to verify that the software has not been changed.

Secure Boot

With Secure Boot, the control system firmware checks that the system boot loader is signed with a cryptographic key authorized by Emerson and stored in a database contained in the firmware. It is used by UEFI (Unified Extensible Firmware Interface) in conjunction with BIOS for controlled boot to prevent the execution of unsigned programs.

Trusted Boot

Trusted Boot takes over where Secure Boot leaves off. Trusted Boot verifies the digital signature of the OS. In turn, the OS verifies the components it will use in the startup process, such as startup files and boot drivers. If a file has been modified, the boot loader detects the change, then refuses to load the corrupt component. Trusted

Boot will only use trusted software, often implemented by using signed and certified software from the manufacturer, resulting in proper configuration and patch management.

This discussion is one of a series of blogs discussing security in industrial PLC/PAC control systems. If you'd like to see others, click here.

Are you currently relying on hardware root of trust?

- unified architecture framework
- Edge controller
- Industry 4.0
- Edge Computing
- IIoT
- OPC UA
- Industrial Computing
- Industrial Processes
- PLC
- PAC
- IoT
