Secure Boot: Ensuring Client Firmware Protection

Introduction

Client systems need to consistently available and, if the hardware and software are sound, the primary concern becomes security. The information technology (IT) department can institute various solutions

including a unified threat management (UTM) paradigm, which may include endpoint protection, anti-virus, and more. However, individual systems may still be vulnerable depending on protocols as the weakest part of the system tends to be personnel. A basic but reliable, and more importantly automatic, hardware assessment on system boot-up can act as a strong secondary line of defense. This is the reasoning behind Secure Boot, boot protection built on the Unified Extensible Firmware Interface (UEFI) that is functional with Windows 8+ as well as most Linux operating systems (OS).

What is Secure Boot?

UEFI is the modern firmware and Basic Input/Output System (BIOS) utilized on most client machines. One functional improvement is security, which can include a trusted platform module (TPM) to provide tamper-resistant encryption key storage. Secure Boot also operates on public and private encryption keys with the goal of making sure the client system has not been compromised. The public key, or platform key (PK), is assigned per-platform while the private key is for modifying the key enrollment/exchange key (KEK) database. The idea is to check to see if the public key is on the whitelist database (DB) or malicious blacklist database (DBX), relying on OEM-programmed keys to determine a client system's status.

Secure Boot as such is an interface between the operating system and the UEFI-based BIOS. Its primary purpose is to resist malicious attacks and malware by detecting the presence of threats before they do lasting damage. This process includes the detection of boot loader tampering, suspicious modification of system files, and the presence of unauthorized option ROMs (OpROM), as validated through the use of a digital signature. Proper credentials as defined usually by OEM are required for the system to boot normally. Secure Boot, assuming the proper requirements are met, will go through a protected sequence to ensure the system does not load into a compromised environment.

Requirements

Secure Boot is based on the UEFI v2.3.1 Errata C specification and requires a PK with a valid KEK database, a signature database, and an exposed interface for Section 27 of that specification. Firmware must support encryption with 2048-bit Rivest-Shamir-Adleman (RSA-2048) and 256-bit Secure Hash Algorithm (SHA-256). A boot manager, such as Windows Boot Manager, must be present and active. Any proper Secure Boot implementation must have rollback protection – this is to prevent the use of older firmware that may have later-patched vulnerabilities still present. Lastly, there must be support for the EFI_HASH_PROTOCOL and EFI_RNG_PROTOCOL features for keying to work properly.

Sequence

If all the above requirements are met, Secure Boot proceeds by checking the platform key against the signature databases. If there is an issue, there may be OEM-specific recovery to restore trusted firmware. A problem with the boot manager will revert to a backup copy of the manager or will rely on OEM remediation, while a driver or kernel issue will load a recovery environment like Windows RE. Following these steps, antimalware software will be loaded as a precaution to detect any lingering malware. Lastly, Secure Boot loads the kernel drivers and proceeds with initialized user mode processes for the OS – that is, it boots the system.

Summary

Client machines within a network may still be susceptible to threats and as such some basic firmware protection is necessary. This comes in the form of Secure Boot, which utilizes encryption keys and databases to make sure the system and its environment remain uncompromised. If any issues are detected the system will have a fallback protocol to restore it to working order. This sequence will then boot the system only when the key is validated and malware is excluded. Then the OS is safely booted through the assistance of the UEFI firmware.

Secure Boot provides a safe, consistent, reliable layer of defense to prevent malware at the software and

firmware levels. Proper organization and maintenance of encryption keys ensures that if for some reason a client system becomes compromised, data is salvaged and further damage is prevented. This is especially important in the era of rootkits and other deep malware. Properly-configured UEFI along with hardware and OS support means that many of these threats can be mitigated even on infection within a larger security framework. Recovery, regardless of the method, restores the machine to operating condition along with important data.

Our SSD Solutions

CA6 Series | PCIe™ Gen 4

- Slim form factor— M.2 2280
- Random read/write up to 1000K/1000K IOPS
- Low latency
- LDPC technology

Please contact our Solid State Storage Technology Corp. expert for more information.

*Specifications and features are subject to change without prior notice. Images are samples only, not actual products.

Request Full Specs Sheets

ABOUT US

A subsidiary of KIOXIA Corporation, **Solid State Storage Technology Corporation** is a global leader in the design, development, and manufacturing of digital storage solutions. We offer a comprehensive lineup of high-performance customizable SSDs for the Enterprise, Industrial, and Business Client markets. With various form factors and interfaces, our SSD solutions help businesses simplify their storage infrastructures accelerating variable workloads, improving efficiency, and reducing total cost of ownership.

Learn more at www.ssstc.com