Lenovo Desktop Firmware Security Design White Paper

Table of Contents

Introduction

Lenovo Firmware Security Design provides comprehensive security solutions more advanced than traditional firmware design. Well beyond traditional firmware design, Lenovo Firmware Security Design not only protects against BIOS corruption, but also provides protection in four aspects:

- DATA
  Data residing in computer system can't be stolen by the design of I/O access restriction policy and device password, and can be completely disposed by Firmware level secure wipe method for the retired units.
- DEVICE
  Lenovo Firmware Security Design provides individual I/O device control at chipset level and keeps publishing new firmware versions through OTA for industry security hole fixes.
- CONFIGURATION
  Customized BIOS settings and sensitive settings can only be changed with admin authorization methods.
- PLATFORM
  Lenovo Firmware Security Design supports IHV chipset level and OSV OS level security features and provides Lenovo customized security silicon hardware, enhancing security design at platform level.

Following these directions, Lenovo continues to deliver complete secure hardware and endpoint protection for customers needing security and provides the ability to secure deployment & config devices properly to meet customers' use.

Why Firmware Security?

We can say without hesitation that security is becoming more and more important, and device firmware plays a vital role in enhancing the computer's security. Since modern computers are always on the internet, cyber-attacks are happening more often and becoming more precisely targeted. These types of firmware including BIOS, Embedded Controller, Intel Management Engine, and some others are attractive targets for attackers.

The firmware is sent to users and runs in an insecure environment, which is easy to be subjected to reverse analysis by hackers. In addition, during the operation of Embedded Controller Firmware, BIOS etc. Hackers can reverse the static code through the official firmware package or analyze and modify the parameters in the memory of the PC through the firmware during the operation of the PC, which makes the security of the firmware more complicated.

Above all, modern PCs have more requirements on security:

- Modern personal computers are required to be able to store information so that its confidentiality is maintained securely.
- Modern personal computers are required to protect against personal privacy being stolen or spied on through computer's device.
- Modern personal computers are required to protect sensitive options for chipset and operation system through BIOS setup.
- Modern personal computers are required to be able to provide the mechanisms for ensuring that Platform Firmware remain in a state of integrity and are protected from corruption, and mechanisms for restoring Platform Firmware to a state of integrity if any such firmware code is detected to have been corrupted.

Lenovo Firmware Security Leading Design

Lenovo firmware security design aims to provide solutions to meet modern personal computers' requirements. And some of these solutions go well beyond the industry standard.

Lenovo provides **Smart USB Protection** to protect the security of PC input and output through USB ports. **Chassis or bottom cover anti-disassembly protection** gives better protection to system hardware; Lenovo BIOS supports the SHA256, and SMx algorithms, which makes the security more reliable and independent.

Lenovo Firmware Resiliency is an advanced and comprehensive firmware resiliency solution. With this design, the integrity of some platform firmware such as Firmware of Embedded Controller, BIOS, and Intel Management Engine, is verified every time when the PC is booted. When the firmware is attacked, it can be restored from backup in time.

One Key Disposal (OKD) provides IT administrator with an easy way to clear customers' sensitive information when system enters disposal process.

Lenovo firmware provides types of **BIOS event logs** with time stamps, which helps users get to know the BIOS changes immediately at a glance.

Kernel Direct Memory Access (DMA) Protection is a security mechanism designed to prevent external hardware devices from accessing the system's memory without authorization.

The **Factory BIOS Verification Mechanism** can effectively protect the security of machines in the production environment.

These solutions will be introduced in the chapters below.

Smart USB Protection

External USB devices are very significant for the security of computers since many viruses are transmitted to computers and maliciously copy computer sensitive data through a USB disk. Smart USB Protection is designed for USB access control.

Firmware based security

This is a native BIOS feature that does not need to install any other OS-level drivers or applications. It provides the firmware-based security, which gives access control in Windows and during system power-on. Administrator could set a BIOS password on the PC for policy authorization to protect peripheral USB and Type-C access.

Flexible USB port access control

Smart USB Protection is to provide flexible USB port access control to enhance such security. It provides various options through BIOS setup for Computer administrator to set different USB port access policies.

• Disabled: All USB devices could be used normally

• Read Only: Copy from USB disk only

• No Access: USB disk NOT support; only USB Keyboard and Mouse allowed.

Embedded Controller Based Firmware Resiliency

This design provides ThinkShield Embedded Controller based solution for supporting resiliency features of platform firmware in the Pre-OS environment.

With the Firmware Resiliency Design, the Platform Firmware can reach the goals:

• Protection: Mechanisms for ensuring that Platform Firmware remain in a state of integrity and are protected from corruption, such as the process for ensuring the authenticity and integrity of firmware updates.

• Detection: Mechanisms for detecting when Platform Firmware have been corrupted.

• Recovery: Mechanisms for restoring Platform Firmware to a state of integrity if any such firmware code is detected to be corrupted, or when forced to recover through an authorized mechanism.

Architecture Overview

The realization of Firmware Resiliency is based on:

• ThinkShield Embedded Controller

It plays the role of the root-of-trust, and by the EC firmware's communication with BIOS to perform the integrity check and backup/recovery of platform firmware.

• Dual SPI Flash

Two SPI flashes are designed to be connected to the platform. One is Primary SPI (System Flash), which is similar to regular Intel PCH attached SPI flash; the other one is Secondary SPI (Flash Backup), which is mainly used to backup platform firmware.

• The Chain-of-Trust design

This design could ensure the platform firmware's integrity during system boot.

• The communication among platform firmware

The communication puts forward the components' verification result within platform firmware to trigger recovery if needed.

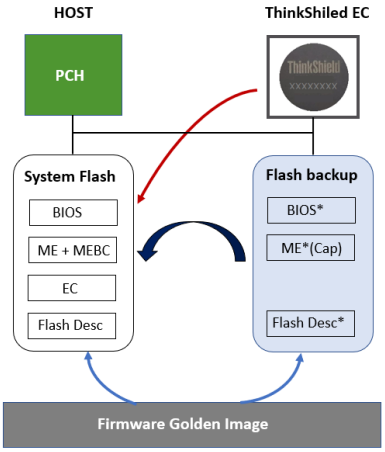

Figure 1 Architecture Overview

Pre-OS Boot authentication

Secure boot is a security standard that is developed for the PC industry to prevent attacks to the pre-boot firmware environment. Secure boot of Lenovo Think products that requires platform firmware to be authenticated before it is executed. Each firmware image must be signed using a known, trusted Digital Signature Algorithm (DSA). The firmware image that authenticates the platform firmware signature must either be an immutable root-of-trust or firmware that has been deemed trusted by the root-of-trust. Once a component is trusted, it can authenticate the next level firmware in the system. The ThinkShield Embedded Controller (EC) is supposed to play the role of performing as such immutable root-of-trust to supporting resiliency features of some platform firmware, such as Embedded Controller Firmware (EC_FW), BIOS, Intel Management Engine Flash Descriptor, etc.

EC Boot ROM firmware, used as the root-of-trust or trust anchor in the system, is an immutable trusted code implemented in a mask ROM. The Boot ROM secure bootloader acts as a first-stage bootloader (FSBL), which loads and authenticates the EC_FW stored in SPI Flash. The EC Boot ROM should use digital signature for authenticating the EC_FW stored on SPI flash.

Further, the EC_FW should be designed to authenticate application firmware (AP_FW), including BIOS, Intel Management Engine Flash Descriptor that stored in SPI flash. The EC_FW uses digital signature algorithms (DSA) for authenticating AP Firmware images. The EC_FW holds the host processor in reset until it validates the firmware integrity of the AP_FW images and validates that the OEM has signed them. Once the EC_FW validates the AP_FW's integrity and authenticity, it releases the reset to the host processor. The AP_FW is custom application-specific firmware that ultimately configures and boots the system. The AP_FW is trusted because it is authenticated by the EC_FW, which was authenticated by the Boot ROM secure bootloader. This process of authenticating each image before it is executed is known as a Chain-of-Trust.

Figure 2 Chain-of-Trust in Secure Boot

EC Firmware Resiliency

EC Boot ROM embedded in the EC chip, with immutable trusted code implemented in a mask ROM. The Boot ROM initializes the device and executes a Boot Loader that securely boots the system by loading EC Firmware. EC Firmware was digitally signed that used to be verified by Boot ROM during boot.

EC Firmware update is to continuously support the current Secure Capsule Update by Windows UEFI Firmware Update (WUFU) Tool.

The Boot ROM also provided the capabilities to detect the integrity of EC Firmware and recovery.

Flash Descriptor Resiliency

The Flash Descriptor is a data structure that is programmed on the SPI flash part on Intel PCH based platforms. The Descriptor data structure describes the layout of the flash and defines configuration parameters for the PCH.

The Flash Descriptor is signed using a private key and authenticated using a public key. OEM generates the private key that is kept a secret, and the corresponding public key is stored in the EC OTP Memory.

The Runtime EC_FW is capable of loading the Flash Descriptor from system flash, then performing authentication on the loaded Flash Descriptor using ECDSA signature protocol, and is required to recover the Flash Descriptor in case the Flash Descriptor fails the ECDSA authentication.

BIOS Resiliency

As some dynamic data and user-configurable BIOS settings can't be signed to one fixed signature, we usually use different way to identify the integrity of BIOS static code and dynamic data. Here describes the executable BIOS static code resiliency.

The static BIOS code was divided into two portions for the resiliency implementation, Boot Block and Main BIOS. EC_FW is required to verify the integrity of the Boot Block region before Host CPU accessing BIOS region. And the validation of main BIOS is supported by Intel Boot Guard. However, both Boot Block and Main BIOS will also be treated as the whole BIOS backup image stored in the backup flash for recovery purposes, so EC_FW is also required to verify the integrity of the entire BIOS backup image after performing BIOS Backup Update. Therefore, Boot Block, main BIOS and the whole BIOS backup image will be digitally signed for the verification.

Every time system is about to power on, EC is required to authenticate the BIOS Boot Block region, which is stored in System Flash. If the authentication fails, EC performs a

BIOS recovery process. If EC verifies Boot Block, Boot Block verifies the integrity of the remainder of the Main BIOS during POST. If it fails, BIOS notifies EC to perform recovery.

ME Firmware Resiliency

The root of Trust of ME Firmware is ROM inside the PCH silicon HW, which ROM is unchangeable. The ROM is responsible for many things, including loading the first piece of ME code from SPI flash and authenticating against keys in the ROM.

ME Firmware Data Resiliency design is described in Intel® CSME Data Resiliency of Intel® Converged Security and Management Engine Specification.

ME Firmware Code Resiliency design owned by Intel forms the protection and detection principles point of view. For recovery, Lenovo BIOS implementation for ME resiliency follows Intel Chasm Falls design. The main difference in Lenovo ME resiliency design is to store ME capsule data used for recovery process in Backup Flash instead of ESP (EFI System Partition) located in system storage (e.g. SSD). Intel Chasm Falls design is to update ME capsule data in ESP when ME Firmware is updated successfully by Windows Update. Lenovo design is to update ME capsule data in Backup Flash when ME Firmware is updated successfully by Windows Update.

Strong Password Policy

Lenovo Strong Password Policy is to provide an enhanced password policy for customization.

[Strong Password]
When enabled, the password length must be at least 8 characters. Setting or updating the BIOS password (SVP, POP, SMP) and Hard Disk Password (HDP) requires at least one uppercase letter, one lowercase letter and one numeric character.

[Special Char]
If enabled, the BIOS will verify that the password (SVP, POP, SMP, HDP) contains at least one special character. If not, the BIOS will reject the password setting or update operation.

[Set Minimum Length]
Options: Disabled / 8 Characters / 9 Characters / 10 Characters / 11 Characters / 12 Characters
If a minimum password length is set, the length of the password (SVP, POP, SMP, HDP) must be equal to or longer than the set value. Otherwise, the password length can be 1 to 128 characters.

[Password Encryption Algorithm]
Options: SHA-256 Hash/SM3 Hash/SHA-512 Hash.

Select the encryption algorithm for BIOS Password (SVP, POP, SMP) and Hard Disk password (HDP).

Strong password will help customers strengthen password security, as complex passwords are more difficult for hackers to guess or crack. This reduces the risk of data breaches due to weak passwords and reduce password sharing risk: it can be easier for users to remember a basic password made up of only numbers or words than a complex one with various alphanumeric and special characters.

Enhanced Tamper Protection

Lenovo enhanced tamper protection allows leverage built-in tamper switch to delete customer secrets when bottom cover is removed. Including immediate shutdown to erase keys stored in RAM, TPM clear to erase keys, Log tamper switch events.

One Key Disposal

OKD (One Key Disposal) is a BIOS firmware product that provides IT administrators with an easy way to wipe out all sensitive customer information when the machine needs to be recycled or scrapped.

As a firmware-level solution, it was built into the firmware that has full access to the entire Hard Disk, BIOS settings, EC Firmware, and some others, so it could completely and securely erase the entire Hard Disk, and reset the BIOS settings and EC data to factory default. This is what built-in Windows/Linux OS features can't do.
Moreover, OKD erases such types of data that are independent of the operating system and can be invoked locally via BIOS setup, which will save customer time and improve efficiency.

BIOS Event Log

BIOS Activity Logging defines the BIOS Setup configuration and boot tracking metrics and measurements required to provide insight into the health of a device.

Subcomponent Code Measurement

Subcomponents BIOS, EC, CSME, and Descriptor Region code are to be measured. This Log entry will record the result of comparing the subcomponents code measurements against the expected measurement, and it shows Chain-of-Trust mechanism worked correctly for each subcomponent.

System Pre-boot Authentication Event

Each entry for pre-boot authentication is an event that will be logged. One of the following entries should be logged to record what credentials was provided to gain pre-boot authentication.

- no password provided
- SVP provided

- SMP provided
- POP provided

BIOS Password Change Event

This capability logs any event that changes any of the BIOS passwords. It records changes to any BIOS passwords (SVP, SMP, POP, HDP), and there are 3 types of changes – create password, change password, remove password.
Noted here, it is NOT to record any of the passwords, only the event of change.

Subcomponent Self-Healing Event

This event is to record when a Subcomponent Self-healing event has occurred. It requires event details & recovered firmware version. It is desired to record which part of the firmware validation caused the self-healing event.

BIOS Setup Configuration Change Event

This requirement logs events that occur when the BIOS Setup is entered or setup items are changed via WMI or other setup configuration tools.

Device Change Event

This entry logs events when devices (like CPU, storage, network devices, etc.) are added, removed, or replaced.

System Boot Event

This event records which boot device was utilized to boot the system.

System Tamper Event

This is to record any recognized tamper event as soon as it is discovered. If there is a BIOS Setup option that enables/disables tamper events, this also impacts this logging.

Kernel DMA Protection

DMA allows external devices to bypass the CPU and directly access system memory. While this mechanism significantly improves data transfer efficiency, it also introduces potential security risks — malicious devices can exploit the DMA function to read and write memory directly, thereby stealing sensitive information such as user passwords and encryption keys, or implanting malicious code and performing other malicious operations.

Kernel DMA Protection refers to a series of security measures implemented at the BIOS level. Its core purpose is to block unauthorized devices from conducting malicious DMA operations, thus safeguarding the security of system memory.

Lenovo provides user security protection by enabling the Kernel DMA Protection feature, with specific functions as follows:

Preventing Unauthorized Memory Access

DMA Protection precisely controls DMA operations through technologies such as IOMMU (Input/Output Memory Management Unit), ensuring that only authorized devices can access memory and thereby protecting sensitive data in the system memory.

Protecting System Boot Security

During the system boot process, DMA Protection can effectively guard against DMA attacks in the pre-boot phase. Specifically, before executing Exit Boot Services, the system firmware implements DMA isolation for the I/O buffers of all DMA-capable devices and disables the Bus Master Enable Bit of unauthorized devices. These measures ensure that the memory is already in a protected state before the operating system starts, preventing attackers from using DMA to conduct malicious operations during the boot phase.

Factory BIOS Verification Mechanism

During the production process at Lenovo factories, a strict BIOS verification mechanism is implemented to ensure that the BIOS is not tampered with during production. The details are as follows:

Verification of BIOS Image Based on Lenovo's Database

After a BIOS is developed and passes verification, it will be synchronized to the factory server via LDDS (Lenovo Data Distribution System). At the same time, the BIOS image is recorded in the database. When the factory completes the production of a machine, a tool will be used to check whether the BIOS is correct by comparing it with the database. If the comparison passes, the machine proceeds normally; if not, production is immediately stopped to investigate security issues.

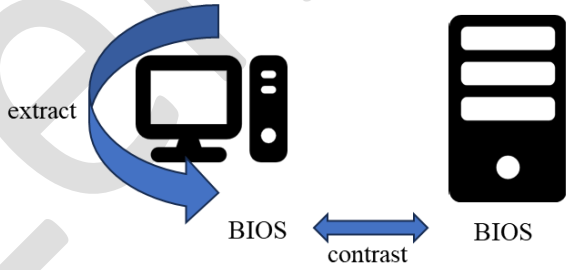

Figure 3 BIOS Comparison

BIOS Signature Verification

All official BIOS versions released by Lenovo have undergone multi-layer digital signature processing. During the BIOS flashing process, a signature verification will be performed against the pre-installed BIOS in the chip. Only BIOS ROMs that pass the verification are allowed to undergo the flashing operation.

Analyze and Repair BIOS

When the computer's BIOS malfunctions, engineers will first capture the relevant BIOS data and extract its operation log information. Subsequently, they will conduct an in-depth analysis of the faulty BIOS files and logs to identify the root cause of the problem.

Finally, engineers will complete the BIOS repair for users and completely resolve the related faults.

Figure 4 BIOS Issue Analysis and Recovery Process

Lenovo Overall Firmware Security Design Summary

In addition to the leading firmware security features, Lenovo Firmware security design provides comprehensive security solution. Here is the summary:

Security Features	Description
BIOS Password	BIOS password is used for pre-boot authentication, and to prevent unauthorized changes to BIOS settings. Lenovo BIOS password design provides three types of passwords: SVP, SMP, and POP to meet the application requirements of multiple scenarios. SVP: Supervisor Password SMP: System Management Password POP: Power On Password
Hard Disk Password	Hard disk password (HDP) is used to protect hard disk against unauthorized access, and to securely erase the hard disk while system is in disposal process.
Individual I/O control	To disable/enable the device access from firmware level, the device will be disappeared in Windows device manager while disabled. This is used in security-sensitive environment, such as preventing data capture from cameras, USB ports.
Secure Roll Back Prevention	Prevent roll back to older BIOS versions through BIOS update program.
Windows UEFI Firmware Update	Enable/Disable the capability to update BIOS through Windows firmware update or LVFS.
secure wipe	A BIOS firmware product that securely erases system integrated Hard Disks. It erases all data and partitions independent of the operating system and can be invoked locally via F12 hotkey through boot menu.
Certificate-based BIOS Authentication	Certificate-based BIOS Authentication allows IT Administrators to manage BIOS settings using a more secure, modern alternative to the BIOS supervisor password.

	It's an enhanced security feature and allows for secure and scalable manageability. It also avoid "bricked" machines with forgotten BIOS Password.
Configuration Change Detection	The newly added/removed/replaced of the system devices including memory module/hard disk, will pop up the user notification during system power on.
BIOS setting protection	Strong cryptographic methods to store BIOS security settings and user credentials in the security data region to prevent settings from being lost.
Odometer	Odometer is system log information to indicate current usage and the system's condition. It includes some metrics that are defined by each component to indicate its current status or history. Each metric is logged by each component, including system board by themselves. It is useful to know how to maintain them. In addition, their objective measurement can be used in following cases. Users may prevent expected failure by checking the odometer data. Each Metrics is automatically logged in system or the subcomponent by its functionality. BIOS read it in POST phase and store them into SMBIOS structure for application usage.

Conclusion

Firmware security is becoming more and more important and realized by more and more people. Lenovo firmware design already provided and continues to provide more leading features that focus on the secure requirements of modern personal computers to give customers a better experience.

- Secure and Comprehensive

  Lenovo firmware security design provides a comprehensive solution to realize data protection, device protection, configuration protection, and platform protection. Moreover, it provides leading designs to make the firmware design more secure.

- Efficiency
  - Lenovo firmware security design provided the ability for commercial IT administrators to prevent their computers' sensitive data from stolen, and have a secure way to dispose unused machine. To use the design, they just need to launch the service from BIOS setup or deploy in OS with both OS and BIOS Administrator privileges, which gives customers more efficiency and reduces the cost needed.

- Easy to use

  Lenovo firmware security design provides multiple features that are easily integrated in BIOS and launched by a hotkey, and simply just need a setup option to set a corresponding policy. Some of them even need no human interactive but can do the protection and recovery automatically.