INTERNATIONAL STANDARD

ISO/IEC 19678

First edition
2015-05-01

Information Technology — BIOS Protection Guidelines

Technologies de l'information — Lignes directrices de protection BIOS

Reference number
ISO/IEC 19678:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Note: ITTF will provide the document number needed below

ISO/IEC 19678 was prepared by the U.S. National Institute of Standards and Technology from NIST SP 800-147, BIOS Protection Guidelines. NIST SP 800-147 was reformatted in accordance with ISO/IEC Directives, Part 2, while maintaining the technical content of the NIST publication (available at http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf). The resulting standard was adopted under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* in parallel with its approval by the national bodies of ISO and IEC.

Introduction

Modern computers rely on fundamental system firmware, commonly known as the system Basic Input/Output System (BIOS), to facilitate the hardware initialization process and transition control to the operating system. The BIOS is typically developed by both original equipment manufacturers (OEMs) and independent BIOS vendors, and is distributed to end-users by motherboard or computer manufacturers. Manufacturers frequently update system firmware to fix bugs, patch vulnerabilities, and support new hardware. This International Standard provides security requirements and guidance for preventing the unauthorized modification of BIOS firmware on PC client systems.

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. A malicious BIOS modification could be part of a sophisticated, targeted attack on an organization—either a permanent denial of service (if the BIOS is corrupted) or a persistent malware presence (if the BIOS is implanted with malware). The move from conventional BIOS implementations to implementations based on the Unified Extensible Firmware Interface (UEFI) may make it easier for malware to target the BIOS in a widespread fashion, as these BIOS implementations are based on a common specification.

This International Standard focuses on current and future x86 and x64 desktop and laptop systems, although the controls and procedures could potentially apply to any system design. Likewise, although the guide is oriented toward enterprise-class platforms, the necessary technologies are expected to migrate to consumer-grade systems over time. The security requirements do not attempt to prevent installation of unauthentic BIOSs through the supply chain, by physical replacement of the BIOS chip, or through secure local update procedures.

The intended audience for this International Standard includes BIOS and platform vendors, and information system security professionals who are responsible for managing the endpoint platforms' security, secure boot processes, and hardware security modules. The material may also be of use when developing enterprise-wide procurement strategies and deployment.

The material in this International Standard is technically oriented, and it is assumed that readers have at least a basic understanding of system and network security. The International Standard provides background information to help such readers understand the topics that are discussed. Readers are encouraged to take advantage of other resources (including those listed in this International Standard) for more detailed information.

Information Technology— BIOS Protection Guidelines

1 Scope

This International Standard provides requirements and guidelines for preventing the unauthorized modification of *Basic Input/Output System (BIOS)* firmware on PC client systems. 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. A malicious BIOS modification could be part of a sophisticated, targeted attack on an organization —either a permanent denial of service (if the BIOS is corrupted) or a persistent malware presence (if the BIOS is implanted with malware).

As used in this publication, the term BIOS refers to conventional BIOS, *Extensible Firmware Interface (EFI)* BIOS, and *Unified Extensible Firmware Interface (UEFI)* BIOS*.* This International Standard applies to system BIOS firmware (e.g., conventional BIOS or UEFI BIOS) stored in the system flash memory of computer systems, including portions that may be formatted as Option ROMs. However, it does not apply to Option ROMs, UEFI drivers, and firmware stored elsewhere in a computer system.

Subclause 7.2 provides platform vendors with requirements for a secure BIOS update process. Additionally, subclause 7.3 provides guidelines for managing the BIOS in an operational environment.

While this International Standard focuses on current and future x86 and x64 client platforms, the controls and procedures are independent of any particular system design.

2 Conformance

The following terms are used in this standard to indicate mandatory requirements, recommended options, or permissible actions.

- The terms “shall” and “shall not” indicate requirements to be followed strictly in order to conform to this standard and from which no deviation is permitted.
- The terms “should” and “should not” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.
- The terms “may” and “need not” indicate a course of action permissible within the limits of this standard.

An implementation is conformant to this standard if it implements the requirements specified in subclause 7.2.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

FIPS 186-4, *Digital Signature Standard.* July 2013.

NIST SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications.* November 2006.

NIST SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. January 2011.

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

4.1
Basic Input/Output System (BIOS)
boot firmware, such as those based on the conventional BIOS, Extensible Firmware Interface (EFI), and the Unified Extensible Firmware Interface (UEFI)

4.2
conventional BIOS
legacy boot firmware used in many x86-compatible computer systems (also known as the legacy BIOS)

4.3
Core Root of Trust for Measurement (CRTM)
the first piece of BIOS code that executes on the main processor during the boot process. On a system with a Trusted Platform Module the CRTM is implicitly trusted to bootstrap the process of building a measurement chain for subsequent attestation of other firmware and software that is executed on the computer system.

4.4
Extensible Firmware Interface (EFI)
a specification for the interface between the operating system and the platform firmware. Version 1.10 of the EFI specifications was the final version of the EFI specifications, and subsequent revisions made by the Unified EFI Forum are part of the UEFI specifications

4.5
firmware
software that is included in read-only memory (ROM)

4.6
option ROM
firmware that is called by the system BIOS, such as BIOS firmware on add-on cards (e.g., video card, hard drive controller, network card) as well as modules which extend the capabilities of the system BIOS

4.7
Protected Mode
an operational mode found in x86-compatible processors with hardware support for memory protection, virtual memory, and multitasking

4.8
Real Mode
a legacy high-privilege operating mode in x86-compatible processors

4.9
System Management Mode (SMM)
a high-privilege operating mode found in x86-compatible processors used for low-level system management functions

4.10
system flash memory
the non-volatile storage location of system BIOS, typically in electronically erasable programmable read-only memory (EEPROM) flash memory on the motherboard. While system flash memory is a technology-specific term, requirements and guidelines in this document referring to the system flash memory are intended to apply to any non-volatile storage medium containing the system BIOS.

4.11
Trusted Platform Module (TPM)
a tamper-resistant integrated circuit built into some computer motherboards that can perform cryptographic operations (including key generation) and protect small amounts of sensitive information, such as passwords and cryptographic keys

4.12
Unified Extensible Firmware Interface (UEFI)
a specification for the interface between the operating system and the platform firmware developed by the UEFI Forum

5 Symbols (and abbreviated terms)

ACPI
Advanced Configuration and Power Interface

BDS
Boot Device Selection

BIOS
Basic Input/Output System

CPU
Central Processing Unit

CRTM
Core Root of Trust for Measurement

DXE
Driver Execution Environment

EEPROM
Electrically Erasable Programmable Read-Only Memory

EFI
Extensible Firmware Interface

FIPS
Federal Information Processing Standard

GPT
GUID Partition Table

GUID
Globally Unique Identifier

MBR
Master Boot Record

OEM
Original Equipment Manufacturer

OS
Operating System

PEI
Pre-EFI Initialization

POST
Power-on self-test

PXE
Preboot Execution Environment

ROM
Read-only Memory

RT
Runtime

RTU
Root of Trust for Update

SMI
System Management Interrupt

SMM
System Management Mode

TPM
Trusted Platform Module

UEFI
Unified Extensible Firmware Interface

6 Background

6.1 System BIOS

The system BIOS is the first piece of software executed on the main central processing unit (CPU) when a computer is powered on. While the system BIOS was originally responsible for providing operating systems access to hardware, its primary role on modern machines is to initialize and test hardware components and load the operating system. In addition, the BIOS loads and initializes important system management functions, such as power and thermal management. The system BIOS may also load CPU microcode patches during the boot process.

There are several different types of BIOS firmware. Some computers use a 16-bit conventional BIOS, while many newer systems use boot firmware based on the UEFI specifications [23]. In this International Standard we refer to all types of boot firmware as BIOS firmware, the system BIOS, or simply BIOS. When necessary, we differentiate conventional BIOS firmware from UEFI firmware by calling them the conventional BIOS and UEFI BIOS, respectively.

System BIOS is typically developed by both original equipment manufacturers (OEMs) and independent BIOS vendors, and is distributed to end users with computer hardware. Manufacturers frequently update system firmware to fix bugs, patch vulnerabilities, and support new hardware. The system BIOS is typically stored on electrically erasable programmable read-only memory (EEPROM) or other forms of flash memory, and is modifiable by end users. Typically, system BIOS firmware is updated using a utility or tool that has special knowledge of the non-volatile storage components in which the BIOS is stored.

A given computer system can have BIOS in several different locations. In addition to the motherboard, BIOS can be found on hard drive controllers, video cards, network cards and other add-in cards. This additional firmware generally takes the form of *Option ROMs* (containing conventional BIOS and/or UEFI drivers). These are loaded and executed by the system firmware during the boot process. Other system devices, such as hard drives and optical drives, may have their own microcontrollers and other types of firmware.

As noted in clause 1, the requirements and guidelines in this International Standard apply to BIOS firmware stored in the system flash. This includes Option ROMs and UEFI drivers that are stored with the system BIOS firmware and are updated by the same mechanism. It does not apply to Option ROMs, UEFI drivers, and firmware stored elsewhere in a computer system.

6.2 Role of system BIOS in the boot process

The primary function of the system BIOS is to initialize important hardware components and to load the operating system. This process is known as *booting*. The boot process of the system BIOS typically executes in the following stages:

1. Execute Core Root of Trust: The system BIOS may include a small core block of firmware that executes first and is capable of verifying the integrity of other firmware components. This has traditionally been called the *BIOS Boot Block*. For trusted computing applications, it may also contain the Core Root of Trust for Measurement (CRTM).

2. Initialize and Test Low-Level Hardware: Very early in the boot process the system BIOS initializes and tests key pieces of hardware on the computer system, including the motherboard, chipset, memory and CPU.

3. Load and Execute Additional Firmware Modules: The system BIOS executes additional pieces of firmware that either extend the capabilities of the system BIOS or initialize other hardware components necessary for booting the system. These additional modules may be stored within the same flash memory as the system BIOS or they may be stored in the hardware devices they initialize (e.g., video card, local area network card).

4. Select Boot Device: After system hardware has been configured, the system BIOS searches for a boot device (e.g., hard drive, optical drive, USB drive) and executes the boot loader stored on that device.

5. Load Operating System: While the system BIOS is still in control of the computer, the boot loader begins to load and initialize the operating system kernel. Once the kernel is functional, primary control of the computer system transfers from the system BIOS to the operating system.

In addition, the system BIOS loads system management interrupt (SMI) handlers (also known as System Management Mode (SMM) code) and initializes Advanced Configuration and Power Interface (ACPI) tables and code. These provide important system management functions for the running computer system, such as power and thermal management.

This clause describes the boot process in conventional BIOS-based systems and the boot process in UEFI-based systems. While conventional BIOS is used in many desktop and laptop computers deployed today, the industry has begun transitioning to UEFI BIOS.

6.2.1 Conventional BIOS boot process

Figure 1 shows a typical boot process for x86-compatible systems running a conventional BIOS. The conventional BIOS often executes in 16-bit real mode, although some more recent implementations execute