INSO
20122
1st.Edition
2016

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۲۰۱۲۲
چاپ اول
۱۳۹۴

فناوری اطلاعات
راهنماهای حفاظت از سامانه ورودی خروجی پایه (بایوس) (BIOS)

Information Technology—BIOS protection Guidelines

ICS: 35.080

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات - راهنماهای حفاظت از سامانه ورودی خروجی پایه (بایوس) (BIOS)»

رئیس:	**سمت و/یا محل اشتغال:**
جمالی، شهرام (دکتری مهندسی کامپیوتر)	عضو هیئت علمی دانشگاه محقق اردبیلی
دبیر:	
علی پسندی، ندا (کارشناسی ارشد مهندسی کامپیوتر)	کارشناس اداره کل استاندارد استان اردبیل
اعضا: (اسامی به ترتیب حروف الفبا)	
اقبالی، نسرین (دکتری تخصصی آنالیز)	عضو هیئت علمی دانشگاه محقق اردبیلی
بی‌مانند، هدی (کارشناسی ارشد مهندسی کامپیوتر)	کارشناس اداره کل استاندارد استان ایلام
حکمت‌جو، سیروس (کارشناسی مهندسی تولیدات گیاهی)	رئیس اداره امور حقوقی اداره کل استاندارد استان اردبیل
سماپور، توفان (کارشناسی ارشد مهندسی کامپیوتر)	مسئول آموزش‌های الکترونیک جهاد دانشگاهی واحد اردبیل
سیاوشیان، سیاوش (کارشناسی ارشد مهندسی کامپیوتر)	معاون فناوری اطلاعات و ارتباطات سازمان ملی استاندارد ایران
سید هاشمی، سید ناصر (کارشناسی ارشد مهندسی کامپیوتر)	عضو مستقل
شرافت‌خواه آذری، شهین (کارشناسی ارشد مهندسی علوم و صنایع غذایی)	رئیس استاندارد سازی و آموزش و ترویج استاندارد اداره کل استاندارد استان اردبیل
طالبی، مهدی کارشناسی مهندسی صنایع	کارشناس اداره کل استاندارد استان اردبیل

علی پسندی، بیتا (کارشناسی ارشد مهندسی کامپیوتر)	مدرس دانشگاه پیام نور اردبیل
علی محمدی، حامد (کارشناسی ارشد مهندسی کامپیوتر)	کارشناس اداره کل ارتباطات و فناوری اطلاعات استان اردبیل
فدا، امیر (کارشناسی مهندسی برق)	رئیس واحد فناوری اطلاعات و ارتباطات اداره کل استاندارد استان اردبیل
مینائی، مژگان (کارشناسی فناوری اطلاعات و ارتباطات)	کارشناس اداره کل استاندارد استان اردبیل
یحیایی، سمیرا (کارشناسی ارشد مهندسی کامپیوتر)	کارشناس اداره کل استاندارد استان سمنان
یزدان پور، محمد رضا (کارشناسی ارشد مهندسی کامپیوتر)	رئیس گروه فناوری اطلاعات و ارتباطات سازمان ملی استاندارد ایران
یزدانی، نازنین (کارشناسی مهندسی کامپیوتر)	کارشناس سازمان ملی استاندارد ایران

ویراستار:

بستان‌دوست راد، احسان (کارشناسی ارشد مهندسی صنایع)	کارشناس استاندارد

فهرست مندرجات

عنوان **صفحه**

عنوان **صفحه**

پیش‌گفتار

استاندارد «تکنولوژی اطلاعات-رهنماهای حفاظت از BIOS (بایوس)» که پیش‌نویس آن در کمیسیون‌های مربوط تهیه و تدوین شده است، در سیصد و نود و هشتمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۹۴/۱۲/۴ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 19678: 2015, Information Technology—BIOS Protection Guidlines

مقدمه

رایانه‌های امروزی به یک ثابت‌افزار[۱] سیستمی بنیادین به نام BIOS[۲] متکی می‌باشند که فرآیند راه‌اندازی اولیه سخت‌افزار و انتقال کنترل به سیستم عامل را تسهیل می‌کند. BIOS معمولاً توسط تولیدکنندگان اصلی تجهیزات (OEM[۳]s) و یا عرضه‌کنندگان مستقل[۴] BIOS توسعه داده می شود، و به وسیله‌ی سازندگان برداصلی یا کامپیوتر به دست کاربران نهایی می‌رسد. سازندگان به منظور برطرف کردن اشکالات، رفع آسیب پذیری‌ها و پشتیبانی از سخت‌افزار جدید مکرراً ثابت‌افزار سیستم را به روز می‌کنند. این استاندارد ملی برای جلوگیری از تغییر غیر مجاز ثابت‌افزار BIOS بر روی سیستم‌های PC کارخواه[۵] راهنما و الزامات امنیتی را ارائه می‌کند.

تغییرات غیر مجاز ثابت‌افزار BIOS توسط بدافزار[۶]ها به دلیل موقعیت منحصر به فرد و ممتاز BIOS در معماری PC یک تهدید جدی می‌باشد. تغییر مخرب BIOS می‌تواند بخشی از یک حمله پیچیده و هدفمند به یک سازمان باشد - حمله انکار سرویس دائمی[۷] (در صورت خراب شدن BIOS) یا حضور مداوم نرم‌افزار مخرب (در صورت جایگزین شدن BIOS با نرم‌افزار مخرب) نمونه‌های از این حملات هستند. حرکت از پیاده‌سازی‌های BIOS متعارف[۸] به پیاده‌سازی‌های مبتنی بر واسط ثابت‌افزار یکپارچه قابل توسعه[۹] (UEFI) ممکن است زمینه را برای نرم‌افزار مخرب برای حمله به BIOS به صورت گسترده فراهم نماید، زیرا که چنین پیاده‌سازی‌های BIOS بر پایه مشخصات مشترکی هستند.

این استاندارد ملی بر روی سیستم‌های رومیزی و لپ‌تاپ x86 و x64 حال و آینده تمرکز می‌کند، هرچند که کنترل‌ها و رویه‌ها به طور بالقوه در هر طراحی[۱۰] سیستمی می‌توانند به کار گرفته شوند. همچنین اگرچه این راهنما در مورد بسترهای رده سازمانی[۱۱] است، فن‌آوری‌های ضروری برای مهاجرت به سیستم‌های رده مشتری[۱۲] در طول زمان مورد انتظار است. الزامات امنیتی مانع نصب BIOS نامعتبر[۱۳] از طریق زنجیره تامین همانند تعویض فیزیکی تراشه BIOS، یا از طریق رویه‌های به روز رسانی امن محلی نیستند.

1- Firmware

۲- سامانه ورودی/خروجی پایه (Basic Input/Output System)

3- Original Equipment Manufacturer

4- Independent

۵- این واژه را فرهنگستان زبان و ادب فارسی واژه به جای سرویس‌گیرنده (client) پیشنهاد کرده است.

6- Malicious software

7- PDoS attack

8- Conventional

9- Unified Extensible Firmware Interface

10- Design

11- Enterprise class platform

12- Consumet grade system

13- Unauthentic

مخاطبان مورد نظر این استاندارد شامل عرضه‌کنندگان بستر و BIOS، و متخصصان امنیت سیستم‌های اطلاعاتی است که مسئول مدیریت امنیت بسترهای پایانی[۱]، فرآیندهای راه‌انداز[۲]ی امن، پودمان[۳]های امنیتی امنیتی سخت‌افزاری می‌باشند. این استاندارد همچنین ممکن است هنگام تدوین راهبرد[۴]های تدارکاتی گسترده سطح سازمانی و استقرار[۵] آن‌ها نیز استفاده شود.

این استاندارد شامل اصول فنی است، و فرض بر این است که خوانندگان حداقل درک اولیه‌ای از امنیت سیستم و شبکه دارند. این استاندارد ملی اطلاعات پیش زمینه را برای کمک به چنین خوانندگانی ارائه می‌دهد تا موضوعات مورد بحث را دریابند. پیشنهاد می‌شود خوانندگان از دیگر منابع (شامل استانداردهای نام برده شده در این استاندارد) برای اطلاعات تفصیلی بیشتر بهره ببرند.

1- Endpoint
2- Boot
3 -Modمدule
4- Strategy
5- Deployment

فناوری اطلاعات – راهنماهای حفاظت از سامانه ورودی خروجی پایه (بایوس) (BIOS)

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین الزامات و راهنماهای برای جلوگیری از تغییر غیر مجاز[1] ثابت‌افزار BIOS بر روی سیستم‌های PC کارخواه است. تغییرات غیر مجاز ثابت‌افزار BIOS توسط بدافزارها به دلیل موقعیت منحصر به فرد و ممتاز BIOS در معماری PC یک تهدید جدی می‌باشد. تغییر مخرب BIOS می‌تواند بخشی از یک حمله پیچیده و هدفمند به یک سازمان باشد - حمله انکار سرویس دائمی (در صورت خراب شدن BIOS) یا حضور مداوم نرم‌افزار مخرب (در صورت جایگزین شدن BIOS با نرم‌افزار مخرب) نمونه‌های از این حملات هستند.

در این استاندارد ملی، عبارت BIOS به BIOS متعارف، واسط ثابت‌افزار قابل توسعه[2] (EFI) BIOS، و UEFI BIOS اشاره دارد. این استاندارد ملی برای ثابت‌افزار BIOS سیستم (مانند BIOS متعارف یا UEFI BIOS) که در حافظه فلش سیستم کامپیوتری ذخیره شده است، کاربرد دارد. این حافظه شامل بخش‌هایی است که ممکن است به عنوان ROMهای اختیاری[3] قالب بندی شود، به کار می‌رود. با این حال، این استاندارد در مورد ROMهای اختیاری، راه‌اندازهای UEFI، و ثابت‌افزارهای ذخیره شده در سایر قسمت‌های سیستم کامپیوتری کاربرد ندارد.

بند ۷-۲ برای عرضه‌کنندگان بستر الزامات فرآیند به روز رسانی امن BIOS را فراهم می‌آورد. همچنین، بند ۷-۳ راهنماهایی برای مدیریت BIOS در محیط عملیاتی ارائه می‌کند.

هرچند این استاندارد ملی بر روی بسترهای کارخواه x86 و x64 [۳۲ بیتی و ۶۴ بیتی] حال و آینده تمرکز می‌کند، کنترل‌ها و رویه‌ها مستقل از طراحی خاص سیستم هستند.

۲ مراجع الزامی[4]

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

1- Unauthorized
2- Extensible Firmware Interface
3- Option ROM
4- Normative references

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

2-1 FIPS 186-4, Digital Signature Standard. July 2013.

2-2 NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications. November 2006.

2-3 NIST SP 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms *and Key Lengths*. January 2011.

۳ انطباق

عبارت‌های زیر در این استاندارد برای نشان دادن الزامات اجباری، گزینه‌های پیشنهادی، یا اقدامات مجاز به کار رفته است.

- عبارت «باید» و «باید» نشان می‌دهد که الزامات به منظور انطباق با این استاندارد به شدت دنبال می‌شوند و هیچ انحرافی از آن مجاز نیست.
- عبارت «پیشنهاد می‌شود» و «پیشنهاد نمی‌شود» نشان می‌دهد که در بین چندین چیز ممکن یکی به عنوان مورد مناسب خاص توصیه می‌شود، بدون ذکر کردن یا استثنا کردن بقیه موارد، یا اینکه عملی مشخص ترجیح داده می‌شود ولی الزامی ندارد، یا اینکه (در حالت منفی) یک امکان مشخص یا عملی رد می‌شود اما ممنوع نیست.
- عبارت «شاید» و «نیازی نیست» نشان می‌دهد که عملیاتی با در نظر گرفتن محدودیت‌های این استاندارد مجاز است.

در صورتی که پیاده‌سازی الزامات تعیین شده در زیربند ۷-۲ را اجرا کند با این استاندارد انطباق دارد.

۴ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌روند.

۱-۴

سامانه ورودی/خروجی پایه (BIOS)

ثابت‌افزار راه‌انداز می‌باشد، مانند ثابت‌افزارهایی که مبتنی بر BIOS متعارف، EFI، و UEFI هستند.

۲-۴

BIOS متعارف

ثابت‌افزار راه‌انداز موروثی[1] است که در بسیاری از سیستم‌های کامپیوتری سازگار با x86 استفاده می‌شود. (همچنین به عنوان BIOS موروثی شناخته می‌شود).

۳-۴

ریشه اصلی اعتماد برای سنجش[2] (CRTM)

اولین قطعه کد BIOS که بر روی پردازشگر مرکزی در طول فرآیند راه‌اندازی اجرا می‌شود. بر روی سیستمی با پودمان بستر مورد اعتماد، CRTM به طور ضمنی برای راه‌اندازی مستقل[3] فرآیند ایجاد یک زنجیره سنجش برای گواهی متعاقب سایر ثابت‌افزارها و نرم‌افزارها که توسط ماشین اجرا می‌گردند مورد اعتماد قرار می‌گیرد.

۴-۴

واسط ثابت‌افزار قابل توسعه (EFI)

مشخصاتی برای واسط بین سیستم عامل و ثابت‌افزار بستر است. مشخصات EFI نسخه ۱٫۱۰ آخرین نسخه مشخصات EFI است، و تجدیدنظرهای بعدی که توسط انجمن Unified EFI انجام شد بخشی از مشخصات UEFI هستند.

۵-۴

ثابت‌افزار

نرم‌افزاری که در حافظه فقط خواندنی قرار دارد.

1- Legacy
2- Core Root of Trust for Measurment
3- Bootstrap

۶-۴

ROM اختیاری

ثابت‌افزاری که توسط BIOS سیستم فراخوانی می‌شود، از قبیل ثابت‌افزار BIOS بر روی کارت‌های افزودنی[1] (مثل کارت گرافیک، کنترل‌کننده دیسک سخت، کارت شبکه) یا پودمان‌هایی که قابلیت‌های BIOS سیستم را توسعه می‌دهند.

۷-۴

حالت حفاظت شده[2]

یک حالت عملیاتی که در پردازنده‌های سازگار با x86 جهت حفاظت از حافظه، حافظه مجازی، و چند وظیفه‌ایی با پشتیبانی سخت‌افزاری قرار داده شده است.

۸-۴

حالت حقیقی[3]

یک حالت عملیاتی موروثی با سطح دسترسی بالا[4] در پردازنده‌های سازگار با x86 می‌باشد.

۹-۴

حالت مدیریت سیستم[5] (SMM)

یک حالت عملیاتی با سطح دسترسی بالا که در پردازنده‌های سازگار با x86 قرار دارد و برای توابع سطح پایین مدیریت سیستم به کار می‌رود.

۱۰-۴

حافظه فلش سیستم[6]

مکان ذخیره سازی غیر فرّار BIOS سیستم است، که معمولاً حافظه فلش از نوع حافظه فقط خواندنی قابل برنامه ریزی پاک شدنی با جریان برق (EEPROM) روی برد اصلی است. گرچه الزامات و راهنماهای این

1- Add-on
2- Protected mode
3- Real mode
4- High-privilege
5- System Management Mode
6- System flash memory

استاندارد به حافظه فلش سیستم که یک اصطلاح خاص فناوری است، اشاره دارند اما در هر رسانه‌ی ذخیره-سازی غیر فرّار که محتوی BIOS سیستم است به کار می‌روند.

۱۱-۴

پودمان بستر مورد اعتماد

یک مدار مجتمع مقاوم در برابر دستکاری در برد اصلی برخی کامپیوترها قرار دارد و می‌تواند عملیات رمزنگاری (از جمله تولید کلید) انجام دهد و از حجم محدودی از اطلاعات حساس مثل رمز عبورها و کلیدهای رمزنگاری محافظت کند.

۱۲-۴

واسط ثابت‌افزار یکپارچه قابل توسعه (UEFI)

مشخصاتی برای واسط بین سیستم عامل و ثابت‌افزار بستر است که توسط انجمن UEFI توسعه داده شد.

۵ کوته نوشت

در این استاندارد، نمادها و کوته‌نوشت‌های زیر به کار می‌رود.

ACPI

واسط پیشرفته پیکربندی و توان

BDS

انتخاب افزاره[1] راه‌انداز

BIOS

سامانه ورودی/خروجی پایه

CPU

واحد پردازش مرکزی

CRTM

ریشه مرکزی اعتماد برای سنجش

1- Device

DXE

محیط اجرای گرداننده[1]

EEPROM

حافظه فقط خواندنی قابل برنامه ریزی الکتریکی پاک شدنی

EFI

واسط ثابت‌افزار قابل توسعه

FIPS

استاندارد پردازش اطلاعات فدرال[2]

GPT

جدول بخش‌بندی[3] GUID

GUID

شناسه یکتای سراسری

MBR

رکورد راه‌انداز اصلی

OEM

سازندگان اصلی تجهیزات

OS

سیستم عامل

PEI

راه‌اندازی پیش EFI

POST

فرآیند خود آزمونی به محض روشن شدن سیستم

PXE

محیط اجرا پیش از راه‌اندازی

ROM

1- Driver

۲- استانداردهای مربوط به امنیت کامپیوتری دولت آمریکا که الزامات پودمان‌های رمزنگاری را تعیین می‌کند.

3- Partition

حافظه فقط خواندنی

RT

زمان اجرا

RTU

ریشه اعتماد برای به روز رسانی

SMI

وقفه مدیریت سیستم

SMM

حالت مدیریت سیستم

TPM

پودمان بستر مورد اعتماد

UEFI

واسط ثابت‌افزار یکپارچه قابل توسعه

۶ پیشینه

۶-۱ BIOS سیستم

BIOS سیستم اولین بخش نرم‌افزاری است که زمانی که کامپیوتر روشن می‌شود در واحد پردازشگر مرکزی (CPU) اصلی[1] اجرا می‌شود. درحالیکه BIOS سیستم در ابتدا مسئول فراهم کردن دسترسی سیستم‌عامل به سخت‌افزار بود، نقش اصلی آن در ماشین‌های مدرن راه‌اندازی اولیه و آزمایش مؤلفه‌های سخت‌افزاری و بارگذاری سیستم‌عامل است. علاوه بر این، BIOS توابع مهم مدیریت سیستم، اعم از مدیریت توان و گرمایی را بارگذاری و مقداردهی اولیه می‌کند. همچنین BIOS سیستم ممکن است وصله‌های ریزبرنامه CPU را در طول فرآیند راه‌اندازی بارگذاری کند.

چندین نوع متفاوت از ثابت‌افزار BIOS وجود دارد. برخی کامپیوترها از BIOS متعارف ۱۶ بیتی استفاده می‌کنند، در حالی که خیلی از سیستم‌های جدیدتر از ثابت‌افزار راه‌انداز مبتنی بر مشخصات UEFI (مرجع شماره ۲۳ را ببینید) استفاده می‌کنند. در این استاندارد به تمامی انواع ثابت‌افزار راه‌انداز با عنوان ثابت‌افزار BIOS، BIOS سیستم، یا فقط BIOS اشاره می‌شود. در صورت نیاز، ثابت‌افزار BIOS متداول از ثابت‌افزار UEFI با نامیدن آنها به ترتیب تحت عناوین BIOS متداول و UEFI BIOS متمایز خواهند شد.

1- Main Central Processing Unit

BIOS معمولاً توسط OEMها و یا عرضه‌کنندگان مستقل BIOS توسعه داده می‌شود، و همراه با سخت‌افزار به دست کاربران نهایی می‌رسد. سازندگان به منظور برطرف کردن اشکالات، رفع آسیب پذیری‌ها و پشتیبانی از سخت‌افزار جدید مکرراً ثابت‌افزار سیستم را به روز می‌کنند. BIOS سیستم معمولاً در حافظه EEPROM یا سایر شکل‌های حافظه فلش ذخیره می‌شود، و توسط کاربران نهایی قابل تغییر است. معمولاً ثابت‌افزار BIOS سیستم با استفاده از برنامه یا ابزاری که دانش خاص از مؤلفه‌های ذخیره‌سازی غیر فرّاری که BIOS در آن ذخیره شده است دارد، به روز رسانی می‌گردد.

یک سیستم کامپیوتری می‌تواند در چندین مکان مختلف BIOS داشته باشد. BIOS علاوه بر برد اصلی می‌تواند در کنترل‌کننده‌های دیسک خوان[1]، کارت‌های گرافیک، کارت شبکه و سایر کارت‌های افزودنی قرار داده شود. این ثابت‌افزار اضافی عموماً به شکل ROMهای اختیاری (شامل BIOS متعارف و/یا گرداننده‌های UEFI) است. در طول فرآیند راه‌اندازی، ROMهای اختیاری به وسیله ثابت‌افزار سیستم بارگذاری و اجرا می‌گردند. سایر افزاره‌های سیستم، مثل دیسک‌های سخت و درایوهای نوری، ممکن است میکروکنترلر[2] و سایر انواع ثابت‌افزارهای خودشان را داشته باشند.

همان طور که در بند ۱ اشاره شد، الزامات و راهنماهای این استاندارد ملی در مورد ثابت‌افزار BIOS که در حافظه فلش سیستم ذخیره شده است، به کار می‌روند، که شامل ROMهای اختیاری و راه‌اندازهای UEFI است که در ثابت‌افزار BIOS سیستم ذخیره شده‌اند و با سازوکار یکسان به روز رسانی می‌شوند. این الزامات در مورد ROMهای اختیاری، درایوهای UEFI، و ثابت‌افزارهای ذخیره شده در سایر قسمت‌های سیستم کامپیوتری کاربرد ندارد.

۲-۶ نقش BIOS سیستم در فرآیند راه‌اندازی

نقش اولیه BIOS راه‌اندازی مؤلفه‌های سخت‌افزاری مهم و بارگذاری سیستم عامل می‌باشد. این فرآیند به راه‌اندازی[3] معروف است. فرآیند راه‌اندازی از BIOS سیستم به طور معمول شامل مراحل زیر می‌باشد:

۱. اجرای ریشه مرکزی اعتماد: BIOS سیستم ممکن است شامل یک بلوک کوچک مرکزی از ثابت‌افزاری باشد که قبل از همه اجرا می‌شود و قادر به بازبینی یکپارچه‌گی سایر مؤلفه‌های ثابت‌افزار است. این بلوک معمولاً بلوک راه‌انداز BIOS نامیده می‌شود. برای برنامه‌های محاسباتی مورد اعتماد، بلوک مذکور همچنین ممکن است شامل CRTM باشد.

1- hard drive
2- Microcontroller
3- Booting

۲. راه‌اندازی اولیه و آزمون سخت‌افزار سطح پایین: در ابتدای فرآیند راه‌اندازی، BIOS قطعات سخت-افزاری کلیدی، شامل برد اصلی، تراشه، حافظه و CPU سیستم کامپیوتری را آزمایش و راه‌اندازی اولیه می‌کند.
۳. بارگذاری و اجرای سایر پودمان‌های ثابت‌افزار: BIOS سیستم قطعه‌های بیشتری از ثابت‌افزار را اجرا می‌کند که هم قابلیت‌های BIOS سیستم را توسعه می‌دهد و هم سایر مؤلفه‌های سخت‌افزاری لازم برای راه‌اندازی سیستم را مقداردهی می‌کند. این پودمان‌های اضافی ممکن است در همان حافظه فلشی که BIOS سیستم در آن است ذخیره شوند، یا اینکه ممکن است در دستگاه‌های سخت‌افزاری که آنها را مقداردهی می‌کنند (برای مثال کارت گرافیکی، کارت شبکه محلی) ذخیره شوند.
۴. انتخاب افزاره راه‌انداز: پس از اینکه سخت‌افزار سیستم پیکربندی شد، BIOS سیستم به دنبال افزاره راه‌انداز می‌گردد (برای مثال دیسک سخت، دیسک نوری، درایو USB) و بارکننده راه‌انداز ذخیره شده در آن افزاره را اجرا می‌کند.
۵. بارگذاری سیستم عامل: در حالی که BIOS سیستم هنوز کنترل کامپیوتر را دارد، بارکننده راه‌انداز شروع به بارگذاری و راه‌اندازی هسته سیستم عامل می‌کند. وقتی که هسته سیستم عامل به کار افتاد، کنترل اصلی سیستم کامپیوتری از BIOS سیستم به سیستم عامل انتقال می‌یابد.

علاوه بر موارد ذکر شده، BIOS سیستم گرداننده SMI (به نام کد SMM نیز شناخته می‌شود) را بارگذاری می‌کند، و جداول ACPI و برنامه را مقداردهی اولیه می‌کند. این‌ها توابع مهم مدیریت سیستم مثل مدیریت توان و دما را برای اجرای سیستم کامپیوتری فراهم می‌کنند.

این بند فرآیند راه‌اندازی در سیستم‌های مبتنی بر BIOS متعارف و سیستم‌های مبتنی بر UEFI را توصیف می‌کند. هر چند که BIOS متعارف در خیلی از کامپیوترهای امروزی رومیزی و لپ‌تاپ به کار گرفته شده است، صنعت به سمت UEFI BIOS حرکت می‌کند.

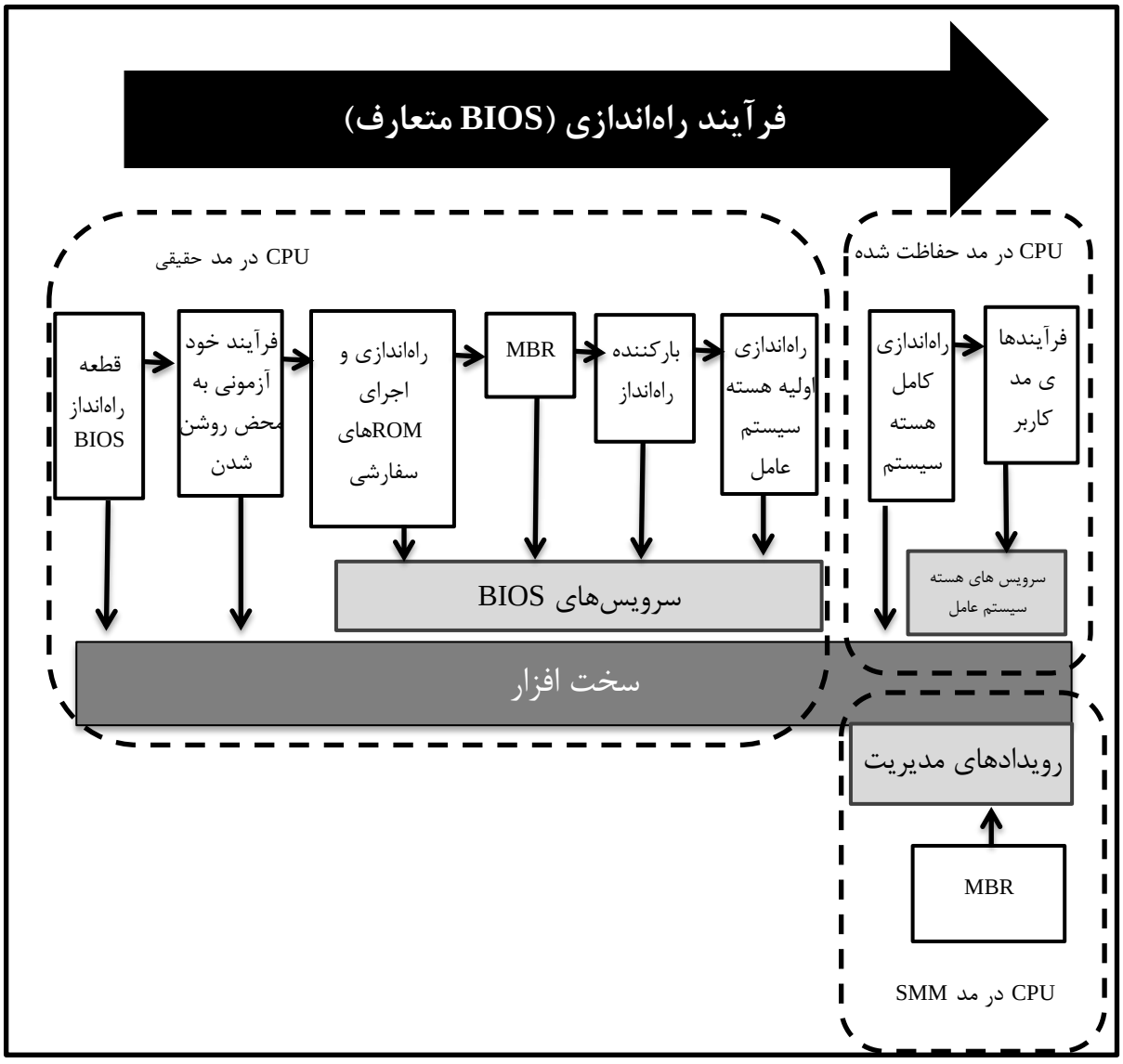
۶-۲-۱ فرآیند راه‌اندازی BIOS متعارف

شکل ۱ فرآیند راه‌اندازی BIOS متعارف در سیستم‌های سازگار با x86 را نشان می‌دهد. BIOS متعارف اغلب در حالت حقیقی ۱۶ بیتی اجرا می‌شود، هرچند برخی پیاده‌سازی‌های اخیر در حالت محافظت شده اجرا می‌شوند. برخی ثابت‌افزارهای مبتنی بر BIOS متعارف بلوک کوچکی از ثابت‌افزار BIOS را دارند – معروف به بلوک راه‌انداز BIOS – که به طور منطقی جدا از بقیه BIOS است. بر روی این سیستم‌های کامپیوتری قطعه راه‌انداز اولین ثابت‌افزاری است که در طول فرآیند راه‌اندازی اجرا می‌شود. قطعه راه‌انداز مسئول بررسی یکپارچگی سایر دستورالعمل‌های BIOS است، و در صورتی که ثابت‌افزار BIOS اصلی سیستم آسیب ببیند، ممکن است سازوکارهایی برای بازیابی[1] مهیا کند. در اکثرمعماری‌های محاسباتی مورد

1- Recovery

اطمینان، بلوک راه‌انداز BIOS به عنوان CRTM سیستم کامپیوتری سرویس می‌دهد، زیرا این ثابت‌افزار به طور ضمنی برای راه‌اندازی فرآیند ایجاد یک زنجیره سنجش برای گواهی سایر ثابت‌افزارها و نرم‌افزارها که متعاقباً توسط ماشین اجرا می‌گردند مورد اعتماد است (مرجع شماره ۲۰ را ببینید).

بلوک راه‌انداز قسمتی از BIOS متعارف را اجرا می‌کند که اکثر مؤلفه‌های سخت‌افزاری را راه‌اندازی اولیه می‌کند (برنامه POST). در طول POST، سخت‌افزار کلیدی سطح پایین در سیستم کامپیوتری شامل تراشه، CPU و حافظه راه‌اندازی اولیه می‌شود. BIOS کارت گرافیک را راه‌اندازی می‌کند، که خود کارت گرافیک ممکن است BIOS خودش را برای راه‌اندازی پردازنده و حافظه گرافیکی بارگذاری و اجرا کند.



شکل ۱ فرآیند راه‌اندازی BIOS متعارف

سپس، BIOS سیستم به دنبال سایر دستگاه‌های جانبی و میکروکنترلرها می‌گردد، و ROM اختیاری روی این مؤلفه‌ها را اجرا می‌کند که برای راه‌اندازی اولیه آنها لازم است. ROMهای اختیاری در اوایل فرآیند راه-اندازی اجرا می‌شوند و می‌توانند ویژگی‌های گوناگونی را به فرآیند راه‌اندازی اضافه کنند. برای مثال یک ROM اختیاری بر روی واسط شبکه می‌تواند محیط اجرای PXE را بارگذاری کند، که به کامپیوتر اجازه می‌دهد از طریق شبکه راه‌اندازی شود.

سپس BIOS سیستم، کامپیوتر را برای یافتن افزاره‌های ذخیره‌سازی که به عنوان افزاره‌های راه‌انداز شناسایی شده‌اند، پویش[1] می‌کند. در یک مورد نوعی، BIOS تلاش می‌کند تا از طریق اولین افزاره راه‌انداز که رکورد راه‌انداز اصلی معتبری بر روی آن یافته راه‌اندازی شود. MBR به بارکننده راه‌انداز ذخیره شده بر روی دیسک اشاره می‌کند، که به نوبه خود فرآیند بارگذاری سیستم عامل را شروع می‌کند.

در طول فرآیند راه‌اندازی، BIOS گرداننده‌های SMI را بارگذاری کرده و جداول ACPI و دستورالعمل‌ها را مقداردهی می‌کند. گرداننده‌های SMI در حالت ویژه‌ای با سطح دسترسی بالا در CPU اجرا می‌شوند که یک حالت ۳۲ بیتی معروف به مدیریت سیستم است و می‌تواند بسیاری از سازوکارهای امنیتی سخت‌افزاری حالت محافظت شده از قبیل قطعه‌بندی حافظه و محافظت از صفحه‌ها کنار بگذارد.

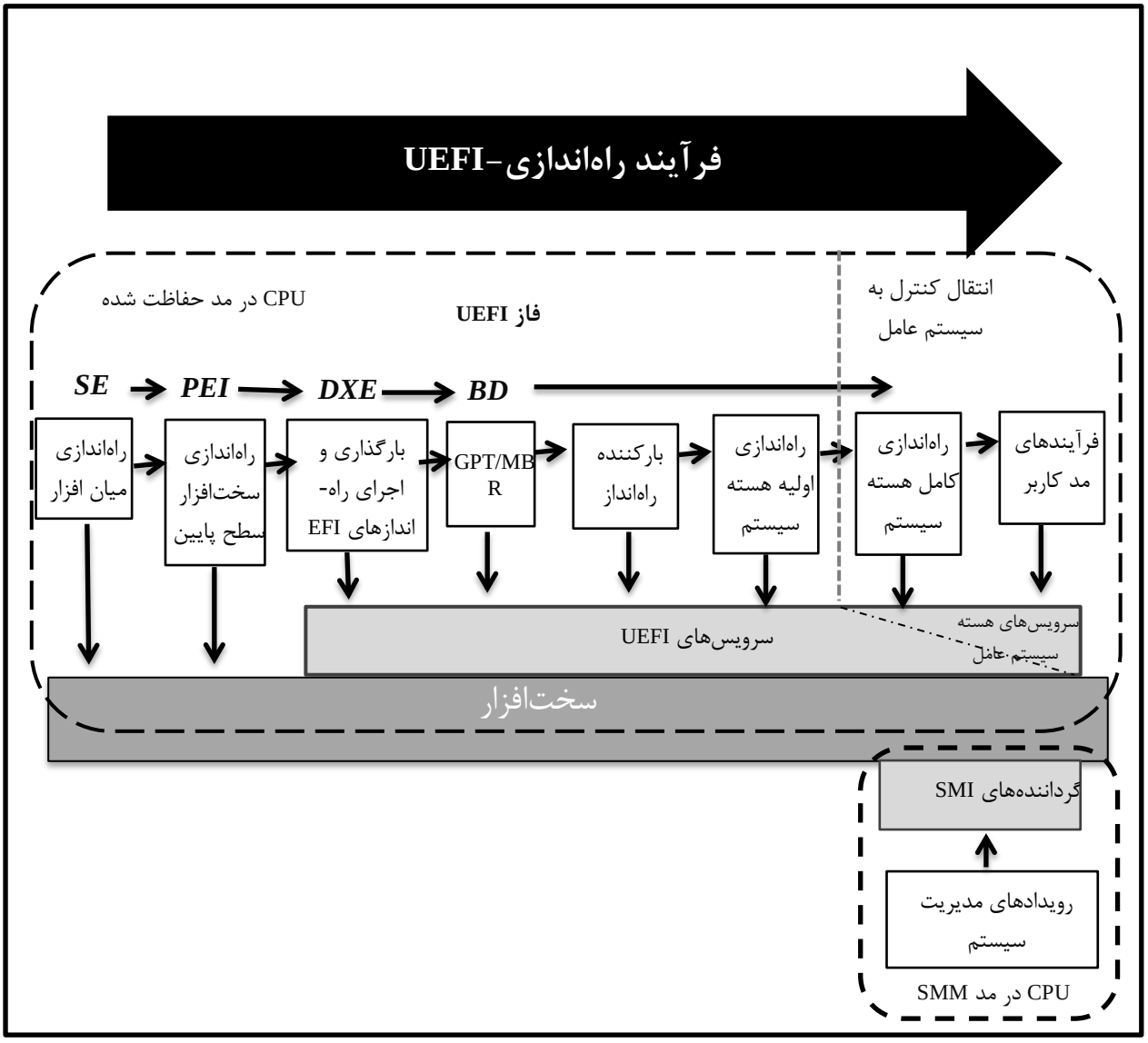
۶-۲-۲ فرآیند راه‌اندازی UEFI

در سطح بالا، فرآیند راه‌اندازی UEFI، نشان داده شده در شکل ۲، روندی مشابه فرآیند راه‌اندازی BIOS متعارف دارد. یک تفاوت این است که دستورالعمل‌های UEFI در حالت محافظت شده ۳۲ یا ۶۴ بیتی CPU اجرا می‌شوند، نه در حالت حقیقی ۱۶ بیتی که اغلب در BIOS متعارف مطرح است. اکثر بسترهای مبتی بر UEFI با بلوک مرکزی کوچکی از دستورالعمل‌ها شروع می‌شوند که مسئولیت اصلی تصدیق[2] دستورالعمل-های بعدی را دارند، که در سیستم کامپیوتری اجرا می‌شوند. این روند خیلی شبیه نقش بلوک راه‌انداز در BIOS متعارف است. این قسمت از فرآیند راه‌اندازی به نام فاز امنیتی (SEC) معروف است، و به عنوان ریشه مرکزی اعتماد در سیستم کامپیوتری سرویس‌دهی می‌کند.

فار بعدی فرآیند راه‌اندازی UEFI، فاز PEI می‌باشد. هدف فاز PEI راه‌اندازی مؤلفه‌های کلیدی سیستم از قبیل پردازنده، تراشه و برد اصلی است. در برخی موارد، در یک سیستم UEFI دستورالعمل‌های فاز امنیتی و فاز PEI ریشه مرکزی اعتماد را در یک سیستم UEFI تشکیل می‌دهند. هدف فاز PEI آماده کردن سیستم برای فاز DXE می‌باشد. اکثر راه‌اندازی‌های اولیه سیستم در فاز DXE انجام می‌شوند. ثابت‌افزاری که در این فاز اجرا می‌شود مسئول جستجو و اجرای راه‌اندازهایی است که پشتیبانی افزاره یا ویژگی‌های اضافی در طول فرآیند راه‌اندازی را مهیا می‌کند. در طول این فاز، UEFI BIOS ممکن است ROMهای اختیاری متعارف را

1- Scan
2- Authenticating

اجرا کند که هدف یکسانی دارند. در فرآیند راه‌اندازی UEFI، فازهای PEI و DXE زمینه بارگذاری سیستم عامل را فراهم می‌آورند. کارهای نهایی لازم برای بارگذاری سیستم عامل در فاز BDS انجام می‌شوند. این فاز افزاره‌های کنسول را برای عملیات ساده ورودی/خروجی در سیستم راه‌اندازی اولیه می‌کند. افزاره‌های کنسول شامل واسط‌های متنی یا گرافیکی محلی و همچنین واسط‌های راه‌دور مثل Telnet یا نمایش راه‌دور روی HTTP است. فاز BDS همچنین سایر راه‌اندازهای لازم برای مدیریت کنسول یا افزاره‌های راه‌انداز را بارگذاری می‌کند. در نهایت، ثابت‌افزار بارکننده راه‌انداز را از اولین MBR یا افزاره راه‌انداز قالب‌بندی شده GPT بارگذاری می‌کند، و سپس سیستم عامل را بارگذاری می‌نماید.



شکل ۲ فرآیند راه‌اندازی UEFI

در طول فرآیند راه‌اندازی UEFI BIOS گرداننده وقفه SMI را بارگذاری می‌کند و جداول ACPI و دستورالعمل‌ها را مقداردهی اولیه می‌کند.

فاز زمان اجرا[1] در فرآیند راه‌اندازی UEFI زمانی شروع می‌شود که سیستم‌عامل آماده گرفتن کنترل از UEFI BIOS است. در طول این فاز، خدمات[2] زمان اجرای UEFI در دسترس سیستم عامل هستند.

۳-۶ به روزرسانی BIOS سیستم

یک سیستم و نرم‌افزار و ثابت‌افزار مدیریتی پشتیبان آن، سازوکارهای مجاز مختلفی برای به روزرسانی قانونی BIOS سیستم فراهم می‌کنند. این سازوکارها شامل موارد زیر است.

۱. به روزرسانی‌های شروع شده توسط کاربر: سازندگان سیستم و برد اصلی معمولاً ابزارهایی با قابلیت به روزرسانی BIOS سیستم به کاربر عرضه می‌نمایند. سابقاً، کاربران نهایی برای انجام این به روزرسانی‌ها سیستم را از طریق رسانه خارجی راه‌اندازی می‌کردند، ولی امروزه اکثر سازندگان ابزارهایی فراهم کرده‌اند که می‌توانند BIOS سیستم را از طریق سیستم عامل عادی کاربر به روزرسانی کنند. بسته به سازوکارهای امنیتی پیاده‌سازی شده در سیستم، این ابزارها ممکن است به طور مستقیم BIOS سیستم را به روز رسانی کنند یا اینکه ممکن است یک به روزرسانی را برای دفعه بعدی که سیستم راه‌اندازی می‌شود برنامه‌ریزی کنند.

۲. به روزرسانی‌های مدیریت شده: سیستم کامپیوتری ممکن است عامل‌های مبتنی بر سخت‌افزار و نرم‌افزار داشته باشد که به مدیر سیستم اجازه می‌دهند از راه دور و بدون دخالت کاربر BIOS سیستم را به روز کند.

۳. عقب‌گرد: پیاده‌سازی‌هایی از BIOS سیستم که قبل از اعمال به روزرسانی‌ها، آنها را اعتبارسنجی می‌کنند، می‌توانند شماره نسخه را هم در طول فرآیند به روزرسانی بررسی کند. در این موارد، BIOS سیستم ممکن است فرآیند به روزرسانی مخصوصی برای برگرداندن ثابت‌افزار نصب شده به نسخه قبلی داشته باشد. برای مثال فرآیند عقب‌گرد ممکن است نیازمند حضور فیزیکی کاربر باشد. این سازوکار در برابر مهاجمانی می‌ایستد که ثابت‌افزار قدیمی را با آسیب‌پذیری‌های شناخته شده نصب می‌کنند[3].

۴. بازیابی دستی: برای بازیابی یک BIOS خراب یا آلوده، بسیاری از سیستم‌های کامپیوتری سازوکار-هایی فراهم می‌کنند تا به کاربر اجازه دهد با حضور فیزیکی در طول فرآیند راه‌اندازی، BIOS فعلی سیستم را با یک نسخه و پیکربندی شناخته شده مناسب جایگزین کند.

1- Run time
2- Services
3- Flash

۵. بازیابی خودکار: برخی از سیستم‌های کامپیوتری قادر به تشخیص خراب شدن BIOS سیستم و بازیابی آن از تصویر[1] ثابت‌افزار پشتیبان ذخیره شده در یک مکان ذخیره‌سازی جداگانه از BIOS اصلی سیستم هستند (برای مثال یک تراشه دوم حافظه فلش، یک پارتیشن مخفی روی دیسک خوان).

۴-۶ اهمیت یکپارچگی BIOS

BIOS سیستم یک مؤلفه امنیتی بحرانی در یک سیستم کامپیوتری می‌باشد، زیرا که اولین برنامه‌ای است که به وسیله CPU اصلی اجرا می‌شود. مادامیکه که BIOS سیستم، احتمالاً با استفاده از TPM، می‌تواند یکپارچگی ثابت‌افزار و نرم‌افزاری را که بعد در فرآیند راه‌اندازی اجرا می‌شود را بازبینی[2] کند، معمولاً تمام یا بخشی از BIOS سیستم به طور ضمنی مورد اعتماد قرار می‌گیرد.

BIOS سیستم به طور بالقوه هدف جالبی برای حمله می‌باشد. کدهای مخرب در حال اجرا در سطح BIOS می‌توانند کنترل بخش‌های زیادی از سیستم کامپیوتری را بدست گیرند. این کدها می‌توانند برای مصالحه با هر مؤلفه‌ای که بعدها در فرآیند راه‌اندازی بار گذاری می‌شود و شامل کد SMM، بارکننده راه‌انداز، فوق‌ناظر[3]، و سیستم عامل می‌باشد، استفاده گردند. BIOS در حافظه غیر فرّار نگهداری می‌شود که اطلاعات بر روی آن بین دوره‌های قطع و وصل برق باقی می‌ماند. بدافزارهای نوشته شده در BIOS می‌توانند برای دوباره آلوده کردن ماشین حتی بعد از نصب سیستم عامل جدید یا تعویض دیسک سخت استفاده شوند. از آنجا که BIOS سیستم در ابتدای فرآیند راه‌اندازی با سطح دسترسی بالا[4] بر روی ماشین اجرا می‌شود، بدافزارهای اجرا شده در سطح BIOS ممکن است به سختی قابل تشخیص باشند. زیرا BIOS در ابتدا بارگذاری می‌شود، و هیچ فرصتی برای محصولات ضد بدافزار جهت پویش BIOS به صورت معتبر[5] وجود ندارد.

استفاده از BIOS ممکن است در نسخه خاصی از BIOS سیستم یا مؤلفه‌های سخت‌افزاری مشخص (برای مثال یک تراشه خاص برد اصلی)، خاص سیستم[6] باشد. در مقابل، اکثر بدافزارها اجرای نرم‌افزار را در سطح یا بالای هسته سیستم عامل هدف قرار می‌دهند، که برای توسعه آسان‌تر است و می‌تواند دسته بزرگتری از ماشین‌ها را مورد حمله قرار دهد. بدافزارهای سطح BIOS به احتمال زیاد در حملات هدفدار بر روی سیستم‌های کامپیوتری پر ارزش به کار گرفته شوند. حرکت به BIOS مبتنی بر UEFI ممکن است حمله

1- Image
2- Verify
۳- یا هایپرویزور که یک واسط نرم افزاری است و بین سخت‌افزار و سیستم عامل‌های مهمان وظیفه مدیریت و مانیتورینگ منابع را دارد، و به آن VMMیا ویرچوال ماشین مانیتور هم گفته می شود.
4- High privilege
5- Authoritatively
6- System-specific

گسترده بدافزار به BIOS را آسان‌تر کند، زیرا این نوع پیاده‌سازی‌های BIOS بـر پایـه مشخصـات مشـترکی می‌باشند.

به دلایل فوق‌الذکر، نمونه‌های شناخته شده اندکی از بدافزارهای سطح BIOS وجود دارد. در حال حاضر تنها بدافزار شناخته شده برای عموم که BIOS سیستم را مورد هدف قرار داده و تعداد قابل توجهی از کامپیوترها را آلوده کرده است ویروس CIH معروف به ویروس Chernobyl (مرجع شماره ۱۹ را ببینید) مـی‌باشـد، کـه اولین بار در سال ۱۹۹۸ شناسایی شد. جزئی[۱] از این ویروس سـعی مـی‌کنـد BIOS سیسـتم‌هـایی را کـه از تراشه خاصی در آن زمان استفاده می‌کردند، بازنویسی کند. این بدافزار به آسیب‌پذیری‌های مختلفـی کـه در ماشین‌های امروزی رفع شده است، اتکا می‌کرد.

محققان امنیتی سایر حملات بالقوه در BIOS متعارف و ثابت‌افزار EFI/UEFI را شرح داده‌اند. حملات اثبات مفهوم[۲] نشان داده‌اند که اجازه درج کدهای آلوده در پیاده‌سازی‌هـای BIOS متعـارف را مـی‌دهنـد کـه بـه-روزرسانی‌های بدون امضا را ممکن می‌کند (مرجع شماره ۱۳ را ببینید). محققان دیگـری بـه آسـیب‌پـذیری سرریز شدن میان‌گیر[۳] در EFI BIOS در بسترهای نرم‌افزاری امـروزی پـی بـرده‌انـد. گرچـه EFI BIOS در ابتدای فرآیند راه‌اندازی از نوشته شدن ثابت‌افزار محافظت مـی‌کنـد و فقـط بـه روزرسـانی‌هـای امضـا شـده ثابت‌افزار را انجام می‌دهد، سرریز میان‌گیر به محققان فرصت داد که فرآیند به روزرسانی امن را با اجرای یک بخش امضاء نشده در بسته به روزرسانی ثابت‌افزار کنار بزنند، قبل از اینکه محافظت از نوشتن به کار گرفتـه شود (مرجع شماره ۲۳ را ببینید).

چنین آسیب‌پذیری‌هایی می‌تواند به مهاجمان امکان ساخت بدافزار مخفی را بدهـد کـه بـا سـطح دسترسـی خیلی بالا در سیستم عمل می‌کنـد. BIOS سیسـتم قبـل از سـپردن کنتـرل کـامپیوتر بـه سیسـتم عامـل، گرداننده‌های SMI را بارگذاری می‌کند. کدهای مخرب نوشته شده در BIOS می‌توانند گرداننده‌های SMI را برای ساخت بدافزاری که در SMM اجرا مـی‌شـود، تغییـر دهـد (مرجـع شـماره ۳ را ببینیـد). ایـن مسـئله دسترسی نامحدود بدافزار به حافظه فیزیکی و دستگاه‌های جانبی متصل به ماشین میزبان را موجب می‌شود، و شناسایی نرم‌افزار در حال اجرا بر روی سیستم عامل را بسیار سخت می‌کند.

۶-۵ تهدیدهای متوجه BIOS سیستم

بند قبل اهمیت حفظ یکپارچگی BIOS سیستم را بیان کرد. این بند برخی از روش‌های مختلـف حملـه بـه یکپارچگی BIOS سیستم را توصیف می‌کنـد، و حملاتـی را مشـخص مـی‌کنـد کـه در حـوزه کنتـرل‌هـا و فرآیندهای امنیتی تبیین شده در بند ۷ می‌باشند.

۱- (Payload) بخشی از نرم‌افزار مخرب که عملیات خرابکارانه انجام می‌دهد.

2- Proof-of-concept

3- Buffer-overflow

اولین تهدید متوجه یکپارچگی BIOS سیستم زمانی است که سیستم در زنجیره تامین انتقال می‌یابد. تکنیک‌های امنیتی زنجیره تامین خارج از حوزه کنترل‌های امنیتی مشخص شده در این استاندارد ملی هستند. با این حال، برخی از رویه‌های مشخص شده در زیر بند ۷-۳ می‌توانند برای شناسایی و اصلاح سیستم‌هایی که BIOS سیستم تایید نشده دارند، استفاده شوند.

با فرض اینکه BIOS مورد نظر تولیدکننده روی سیستم نصب شده است، در طول حیات سیستم چندین تهدید متوجه یکپارچگی BIOS سیستم می‌باشد:

- یکی از شدیدترین تهدیدها، نصب BIOS آلوده توسط کاربر می‌باشد. شیوه اصلی به روزرسانی BIOS سیستم توسط کاربر، اغلب استفاده از برنامه‌های سودمند به روزرسانی BIOS می‌باشد. الزامات و راهنماهای لحاظ شده در این استاندارد ملی کاربران را در صورتی که دسترسی فیزیکی به سیستم کامپیوتری دارند، از نصب تصویرهای تایید نشده BIOS منع نمی‌کند. مانند تهدیدهای زنجیره تامین، رویه‌های امنیتی ممکن است قادر به تشخیص و اصلاح BIOS تایید نشده سیستم باشند، آغاز یک رویه بازیابی برای برگرداندن یک BIOS تایید شده نمونه‌ای از این مورد می‌باشد.
- بدافزارها می‌توانند از کنترل‌های ضعیف امنیتی BIOS حداکثر استفاده را کنند یا از آسیب‌پذیری‌های خود BIOS جهت نصب دوباره یا تغییر BIOS سیستم بهره‌برداری کنند. بعید است که نرم‌افزارهای مخرب همه منظوره این قابلیت را داشته باشند، ولی یک حمله هدفمند به یک سازمان می‌تواند به سمت BIOS استاندارد سازمان هدایت شود. BIOS مخرب می‌تواند از طریق شبکه یا با استفاده از رسانه بر روی سیستم قرار گیرد. الزامات و راهنماهای ارائه شده در این استاندارد ملی برای جلوگیری از چنین حملاتی طراحی شده‌اند.
- ابزارهای مدیریت سیستم مبتنی بر شبکه می‌توانند برای راه‌اندازی یک حمله سازمانی گسترده به BIOS سیستم‌ها استفاده شوند. برای مثال، سرور[۱] نگهداری شده توسط سازمان برای به روز رسانی BIOSهای به کاررفته در سیستم‌های سازمان را در نظر بگیرید؛ یک سرور از دست رفته[۲] می‌تواند یک BIOS آلوده را در تمام سیستم‌های کامپیوتری سازمان منتشر کند. این یک حمله با تاثیر بالاست، ولی نیاز به یک کارمند داخلی یا مصالحه در فرآیند به روزرسانی سازمان دارد. الزامات و راهنماهای ارائه شده در این استاندارد ملی برای جلوگیری از چنین حملاتی طراحی شده‌اند.
- هر یک از سازوکارهای پیشین می‌توانند برای عقب‌گرد به یک BIOS سیستم معتبر[۳] ولی آسیب‌پذیر استفاده شوند. این حمله، یک حمله نفوذی خاص است، زیرا BIOS «بد» معتبر می‌باشد (توسط سازنده توزیع شده است). کنترل‌های امنیتی مشخص شده در بند زیر در درجه اول روی بازبینی

۱- فرهنگستان زبان و ادب فارسی، استفاده از واژه کارساز را به جای سرور پیشنهاد کرده است.

۲- سروری که تحت کنترل بدافزار می‌باشد (compromised server)

3- Authentic

منبع و یکپارچگی BIOS سیستم متمرکز شده‌اند. این استاندارد ملی شامل توصیه‌ای برای حفاظت از عقب‌گرد می‌باشد.

کنترل‌های توصیف شده در بند زیر در درجه اول به جلوگیری از تغییر غیر مجاز BIOS سیستم به وسیله نرم‌افزار به طور بالقوه مخرب در حال اجرا بر روی سیستم‌های کامپیوتری متمرکز شده‌اند. در الزامات زیربخش ۷-۲ به نصب یک BIOS سیستم تایید نشده در زنجیره تامین، توسط افراد با دسترسی فیزیکی، یا از طریق عقب‌گرد به BIOS سیستم معتبر ولی آسیب‌پذیر پرداخته نشده است، ولی می‌تواند با استفاده از فرآیندهای مشخص شده در زیر بخش ۷-۳ مورد توجه قرار گیرد.

۷ کاهش تهدید

۷-۱ کلیات

BIOS مؤلفه‌ای حیاتی برای یک سیستم امن می‌باشد. به عنوان اولین برنامه‌ای که در طول فرآیند راه‌اندازی اجرا می‌شود، BIOS سیستم به طور ضمنی مورد اعتماد مؤلفه‌های سخت‌افزاری و نرم‌افزاری سیستم قرار می‌گیرد. بند پیشین نقش BIOS سیستم را در فرآیند راه‌اندازی شرح داد، BIOS سیستم برای مهاجمان طعمه جذابی است، و تهدیدهای بالقوه ناشی از تغییرات غیرمجاز BIOS می‌باشد. این بند الزامات امنیتی را برای پیاده‌سازی BIOS معرفی و روش‌هایی را برای مدیریت BIOSها در یک محیط سازمانی توصیه می‌کند. زیر بند ۷-۲ الزاماتی برای فرآیند به روزرسانی امن BIOS ارائه می‌کند. مخاطبان مورد نظر این استاندارد، فروشندگان بستر است که پیاده‌سازی BIOS را طراحی، اجرا، یا انتخاب می‌کنند. مادامیکه که محصولات بلافاصله در دسترس نباشند، سازمان‌ها می‌توانند از این الزامات در فرآیندهای تدارکاتی خود استفاده کنند، و طرح‌هایی را برای استفاده از این ویژگی‌های امنیتی در زمانی که آنها در دسترس باشند، ایجاد کنند. سازمان‌ها برای توسعه این طرح‌ها می‌توانند از روش‌های پیشنهادی مدیریت BIOS در زیر بند ۷-۳ استفاده نمایند. توصیه‌ها به منظور جلوگیری از تغییرات غیرمجاز BIOS می‌باشند.

۷-۲ الزامات امنیتی پیاده‌سازی BIOS سیستم

این زیربند الزاماتی برای حفظ یکپارچگی BIOS پس از امن کردن سازوکارهای به کار رفته برای به روزرسانی BIOS فراهم می‌کند. به طور خاص، این زیربند الزامات پیاده‌سازی‌های BIOS سیستم را برای یک سازوکار به روزرسانی امن معین می‌کند. یک سازوکار به روزرسانی امن BIOS شامل موارد زیر می‌باشد:

۱. فرآیندی برای بازبینی اعتبار[1] و یکپارچگی به روزرسانی‌های BIOS، و
۲. سازوکاری برای اطمینان از اینکه BIOS از تغییرات خارج از فرآیند به روزرسانی امن مصون می‌ماند.

1- Verifying the authenticity

اصالت‌سنجی[1] بازبینی می‌کند که تصویر به روزرسانی BIOS توسط کد منبع مجاز تولید شده است و بدون تغییر است. تمام به روزرسانی‌های BIOS یا باید از طریق سازوکار به روزرسانی تایید اعتبار شده BIOS به نحوی که در زیربند ۷-۲-۱ توصیف شد، یا با استفاده از یک سازوکار انتخابی به روزرسانی امن محلی مطابق با الزامات زیربند ۷-۲-۲ انجام شوند.

الزامات سازوکار به روزرسانی امن BIOS تمام خطرات مربوط به BIOS سیستم را رفع نمی‌کند. برخی تهدیدها برای تغییر غیرمجاز BIOS سیستم باقی مانده است. برای مثال، این الزامات از تغییر BIOS سیستم توسط افرادی با دسترسی فیزیکی به سیستم ممانعت نمی‌کند، و یا نبود آسیب‌پذیری در پیاده‌سازی‌های BIOS سیستم را تضمین نمی‌کند. این الزامات در مورد BIOS سیستم باید توام با رویه‌ها و خط مشی‌های امنیتی موجود در سازمان‌ها به کار روند.

۷-۲-۱ اصالت‌سنجی به روزرسانی BIOS

سازوکار به روزرسانی تایید اعتبار شده BIOS از امضای دیجیتال برای اطمینان از صحت تصویر به روزرسانی BIOS استفاده می‌کند. برای به روزرسانی BIOS توسط سازوکار به روزرسانی تایید اعتبار شده BIOS، باید ریشه اعتماد برای به روزرسانی (RTU) وجود داشته باشد که یک الگوریتم تایید امضا و یک انباره کلید که شامل کلید عمومی مورد نیاز برای بازبینی امضای تصویر به روزرسانی BIOS است را دربر دارد. انباره کلید و الگوریتم تایید امضا باید به طور محافظت شده در سیستم کامپیوتری ذخیره شوند، و فقط از طریق سازوکار به روزرسانی تایید اعتبار شده یا سازوکار به روزرسانی امن محلی ذکر شده در زیربند ۷-۲-۲ قابل تغییر باشند.

انباره کلید در RTU باید شامل یک کلید عمومی باشد، که برای بازبینی امضای تصویر به روزرسانی BIOS به کار می‌رود، و یا در صورتی که یک کپی از کلید عمومی توسط تصویر به روزرسانی BIOS مهیا باشد، باید شامل یک درهم‌سازی پنهانی از کلید عمومی باشد. در حالت دوم، سازوکار به روزرسانی باید قبل از استفاده از کلید ارائه شده برای بازبینی امضا مربوط به تصویر به روزرسانی، کلید عمومی ارائه شده در تصویر به روزرسانی BIOS را درهم‌سازی کند، و اطمینان حاصل کند که آن با یک درهم‌سازی در انباره کلید تطبیق دارد.

تصویر BIOS باید علامت تطابق با NIST SP 800-89 داشته باشد، که با استفاده از الگوریتم‌های تایید شده امضای دیجیتالی که در NIST FIPS 186-3 مشخص شده‌اند، حداقل توان امنیتی ۱۱۲ بیتی مطابق با NIST SP 800-1331A را فراهم می‌کند.

1- Authentication

سازوکار به روزرسانی باید اطمینان حاصل کند که تصویر به روزرسانی BIOS به صورت دیجیتال امضا شده است، و آن امضای دیجیتال می‌تواند قبل از به روزرسانی BIOS با استفاده از یک کلید در RTU بازبینی شود. سازوکارهای بازیابی همچنین باید از سازوکار به روزرسانی تایید اعتبار شده استفاده کنند، مگر اینکه فرآیند بازیابی الزامات یک به روزرسانی امن محلی را تامین کند. پیشنهاد می‌شود سازوکار تایید اعتبار شده از عقب‌گردهای غیر مجاز BIOS به نسخه معتبر پیشین با ضعف امنیتی شناخته شده، جلوگیری نماید. این محدودیت سازوکار عقب‌گرد ممکن است برای مثال با بازبینی اینکه شماره نسخه تصویر BIOS بزرگتر از شماره نسخه تصویر BIOS فعلی نصب شده است، انجام گردد.

برخی سازمان‌ها ممکن است مایل به اعمال کنترل بیشتر بر به روزرسانی‌های BIOS در محیط‌های بسیار امن‌تر باشند. طراحی سازوکار به روزرسانی تایید اعتبار شده ممکن است اجازه کنترل سازمانی بر روی فرآیند به روزرسانی را بدهد، که در این حالت اجازه به روزرسانی‌های BIOS یا عقب‌گردهای BIOS به نسخه‌های پیشین فقط در صورتی داده می‌شود که به روزرسانی یا عقب‌گرد توسط سازمان مجاز شمرده شده باشند. برای مثال تصویرهای BIOS خاص می‌توانند توسط سازمان با امضای ثانوی[1] آن‌ها بوسیله یک کلید کنترل شده از سوی سازمان اجازه داده شود، که در طول فرآیند به روزرسانی بازبینی خواهد شد.

۷-۲-۲ به روزرسانی امن محلی

پیاده‌سازی‌های BIOS ممکن است به صورت اختیاری شامل یک سازوکار به روزرسانی امن محلی باشد که BIOS سیستم را بدون استفاده از سازوکار به روزرسانی تایید اعتبار شده به روز رسانی می‌کند. اگر سازوکار به روزرسانی امن محلی پیاده‌سازی شود، فقط باید برای بارگذاری اولین تصویر BIOS یا بازیابی یک BIOS معیوب استفاده شود که نمی‌تواند با استفاده از سازوکار به روزرسانی تایید اعتبار شده توصیف شده در زیربند ۷-۲-۱ اصلاح شود. یک سازوکار به روزرسانی امن محلی باید صحت و یکپارچگی تصویر به روزرسانی BIOS را با الزام به حضور فیزیکی تضمین کند. حفاظت‌های بیشتری ممکن است در سازوکار به روزرسانی امن محلی از طریق الزام به ورود رمز مسئول سیستم یا باز کردن یک قفل سخت‌افزاری (به عنوان مثال یک وصل‌کننده[2] برد اصلی) پیش از صدور مجوز به روزرسانی BIOS سیستم انجام شود.

۷-۲-۳ حفاظت از یکپارچگی[3]

برای جلوگیری از تغییرات ناخواسته یا مخرب BIOS سیستم، خارج از فرآیند به روزرسانی BIOS، RTU و BIOS سیستم (به استثنای داده‌های پیکربندی مورد استفاده BIOS سیستم که در حافظه غیر فرّار ذخیره شده‌اند) باید از تغییرات ناخواسته یا مخرب با استفاده از سازوکاری محافظت گردند، که خارج از به روزرسانی

1- Countersigning
2- Jumper
3- Integrity protection

تایید اعتبار شده BIOS نمی‌تواند بازنویسی شود. سازوکار حفاظت خود باید از تغییرات غیرمجاز محافظت شود.

سازوکار به روزرسانی تایید اعتبار شده BOIS باید به وسیله سازوکاری که حداقل به اندازه سازوکار حفاظتی RTU و BIOS سیستم قوی است، از تغییرات ناخواسته یا مخرب محافظت شود.

سازوکار حفاظت باید نواحی مربوط به BIOS در حافظه فلش سیستم را قبل از اجرای ثابت‌افزار یا نرم‌افزاری که می‌تواند بدون استفاده از سازوکار به روزرسانی تایید اعتبار شده یا یک سازوکار به روزرسانی امن محلی تغییرات ایجاد کند، محافظت کند. پیشنهاد می‌شود حفاظت‌ها توسط سازوکارهای سخت‌افزاری که جز با سازوکار مجاز قابل تغییر نیستند اجرا شوند.

۷-۲-۴ غیرقابل گذر بودن[1]

سازوکار به روزرسانی تایید اعتبار شده BIOS باید یک سازوکار انحصاری برای تغییر BIOS سیستم در نبود مداخله فیزیکی از طریق سازوکار به روزرسانی امن محلی باشد. طراحی سیستم و مؤلفه‌های همراه سیستم و ثابت‌افزار باید تضمین کند که جز از طریق سازوکار به روز رسانی امن محلی هیچ راهی برای پردازنده یا سایر مؤلفه‌های سیستم وجود ندارد تا بتوانند سازوکار به روزرسانی تایید اعتبار شده را کنار بگذارند. هر سازوکاری که قادر به کنار زدن سازوکار به روزرسانی تایید اعتبار شده باشد، آسیب‌پذیری ایجاد می‌کند که به نرم-افزارهای مخرب اجازه می‌دهد BIOS سیستم را تغییر دهند یا فلش سیستم را با تصویر BIOS از یک منبع نامعتبر بازنویسی کنند.

یک بستر نوین شامل ویژگی‌های طراحی مانند سایه‌سازی BIOS در RAM[2] است که به مؤلفه‌های سیستم امکان دسترسی مستقیم به BIOS را به منظور بهبود عملکرد یا برای عملیات حالت مدیریت سیستم می-دهد. مؤلفه‌های سیستم ممکن است دسترسی خواندن به حافظه فلش BIOS داشته باشند، ولی نباید قادر به تغییر BIOS به طور مستقیم باشند، مگر از طریق سازوکار به روزرسانی تایید اعتبار شده یا به وسیله سازوکاری مجاز که نیاز به مداخله فیزیکی دارد. به عنوان مثال ویژگی کنترل گذرگاه[3] که پردازنده اصلی را کنار می‌گذارد (مانند دسترسی مستقیم حافظه[4] به فلش سیستم) نباید قادر به تغییر ثابت‌افزار به طور مستقیم باشد. همچنین میکروکنترلرهای سیستم نباید قادر به تغییر ثابت‌افزار به طور مستقیم باشند، مگر اینکه مؤلفه‌های سخت‌افزاری و ثابت‌افزاری میکروکنترلر با سازوکار معادل در RTU محافظت شوند. الزامات

1- Non-bypassability

۲- کپی کردن BIOS در RAM (shadowing the BIOS in RAM)

3- Bus mastering

4- Direct Memory Access (DMA)

غیر قابل گذشت بودن به داده‌های پیکربندی مورد استفاده BIOS که در حافظه غیر فرّار ذخیره شده‌اند، اعمال نمی‌شود.

۷-۳ روش‌های توصیه شده برای مدیریت BIOS

این زیربند ملاحظاتی برای مدیریت BIOS در محیط عملیاتی سازمانی جهت بهبود سیاست‌ها، فرآیندها، و روش‌های عملیاتی موجود مطرح می‌کند. این زیربند بر روی فعالیت‌های کلیدی با محوریت تامین، استقرار، مدیریت، و امحا BIOS به عنوان بخشی از تمام چرخه حیات بستر نرم‌افزاری تمرکز می‌کند. همچنین فعالیت‌های اجرا شده درفاز بازیابی برای رسیدگی به شرایط استثنایی هستند.

۷-۳-۱ فاز تدارک[1]

پی‌ریزی سازوکاری برای سازمان برای شناسایی، فهرست‌بندی، و رهگیری سیستم‌های کامپیوتری متفاوت سازمانی در تمام چرخه حیات خود امری ضروری است. شناسایی و نظارت بر ویژگی‌های تصویر BIOS از قبیل نام سازنده، شماره نسخه، یا برچسب زمانی به سازمان اجازه می‌دهد تا به روزرسانی، عقب‌گرد، و بازیابی را انجام دهد. پیشنهاد می‌شود سازمان یک «تصویر اصلی طلایی»[2] برای هر BIOS تایید شده در حافظه‌های آفلاین امن نگهداری کند که شامل نسخه‌های جایگزین باشد.

اگر بستر نرم‌افزاری یک ریشه اعتماد برای به روزرسانی (RTU) قابل پیکربندی داشته باشد، لازم است که سازمان یک کپی از انباره کلید و الگوریتم تایید امضا را نگهداری کند. اگر RTU در BIOS سیستم یکپارچه-سازی شده باشد، آنگاه این الزام با نگهداری تصویر BIOS طلایی برآورده می‌شود. اگر RTU در BIOS سیستم یکپارچه‌سازی نشده باشد، پیشنهاد می‌شود امنیت فراهم شده برای RTU حداقل به اندازه امنیت فراهم شده برای تصویر BIOS طلایی قوی باشد.

اغلب سازمان‌ها به سازنده به عنوان منبع BIOS تایید اعتبار شده اتکاء می‌کنند. در این صورت سازمان هیچ کلید خصوصی را نگهداری نمی‌کند، و RTU فقط شامل کلیدهای عمومی است که توسط سازنده تدارک دیده شده است. حال اگر سازمان بخواهد با امضای ثانوی برخی یا همه به روزرسانی‌های تایید شده BIOS مشارکت فعال در فرآیند تایید اعتبار BIOS داشته باشد، RTU شاید شامل یک یا بیش از یک کلید عمومی مربوط به سازمان باشد. در این صورت، سازمان باید کلید متناظر خصوصی را به شکل امن نگهداری کند به طوریکه به روزرسانی بعدی BIOS بتواند امضا شود. پیشنهاد می‌شود کلیدهای خصوصی تحت کنترل چندگانه نگهداری شوند تا از حملات داخلی محافظت شوند. برای کلیدهای سازمانی، کلیدهای عمومی متناظر نیز باید به طور امن نگهداری شوند (برای اطمینان از اصالت‌سنجی منبع).

1- Provisioning
2- Golden master image

به علاوه، یک خط مشی پیکربندی مشترک برای هر بستر باید ایجاد شود تا مطابق سیاست‌های سازمان باشد. پیشنهاد می‌شود که خط مشی تضمین کند که ویژگی‌های حفاظت از یکپارچگی و غیر قابل گذر بودن فعال[1] هستند (در صورتی که این ویژگی‌ها قابل پیکربندی باشند)، و سیاست‌های سازمان در مورد رمز عبور و ترتیب راه‌اندازی افزاره اجرا می‌شوند. درنهایت، پیشنهاد می‌شود که اطلاعات تصویر BIOS و خط مشی تنظیمات مربوطه برای هر بستر در طرح مدیریت پیکربندی مستندسازی شود.

۷-۳-۲ فاز استقرار بستر[2]

پیشنهاد می‌شود برای تهیه BIOS تایید اعتبار شده از تصویر اصلی طلایی[3] برای بستر از فرآیند به روزرسانی امن محلی استفاده شود، RTU متناظر نصب شود، و پارامترهای پیکربندی مربوط به BIOS قبل از اینکه سیستم‌های کامپیوتری به کار گرفته شوند، معین گردند. این کار به سازمان کمک می‌کند تا در همان وضعیت شروع مشخص‌اش استوار باقی بماند. پیشنهاد می‌شود که سازمان برای تایید اینکه سیاست‌ها، ،فرآیندها و رویه‌های مربوط به BIOS سازمان به درستی دنبال می‌شوند به طور دوره‌ای ارزیابی‌هایی را انجام دهد.

به ویژه رویه‌ها باید تضمین کنند که BIOS مناسب نصب شده است، RTU شامل تمام کلیدهای لازم می‌باشد، و ویژگی‌های حفاظت از یکپارچگی و غیر قابل برگشت بودن در صورت قابل پیکربندی بودن فعال هستند.

۷-۳-۳ فاز نگهداری و عملیاتی[4]

این فاز شامل فعالیت‌های نگهداری و عملیاتی است که برای حفظ امنیت و قابلیت اطمینان[5] BIOS در محیط‌های عملیاتی دارای اهمیت است. پیشنهاد می‌شود به روزرسانی‌های BIOS با استفاده از فرآیند مدیریت تغییر انجام شود و نسخه جدید تایید اعتبار شده با توجه تصویر قبلی BIOS که جایگزین شده است، در طرح پیکربندی مستندسازی گردد.

پیشنهاد می‌شود که تصویر BIOS و خط مشی پیکربندی به طور مرتب تحت نظارت باشد. اگر انحراف تایید نشده‌ایی از این خط مشی پایه آشکار شود، پیشنهاد می‌شود به رویداد رسیدگی کرده، و آن را به عنوان بخشی از فعالیت‌های واکنش به رخداد مستندسازی و اصلاح نمود. پیشنهاد می‌شود طرح واکنش به رخداد فرآیند و مجموعه ابزارهای مجازی را که می‌توانند برای ثبت رویداد به منظور کمک به تعیین علت ریشه

1- enable
2- Platform deployment
3- Golden master image
4- Operation and maintenance
5- Reliability

استفاده شوند، مستند سازی کند. پیشنهاد می‌شود ه سازوکار به روز رسانی امن محلی برای بازیابی از تصویر مورد توافق BIOS استفاده شود.

اگر تصویر جدید BIOS برای توسعه قابلیت‌های سیستم، بهبود قابلیت اطمینان سیستم، یا اصلاح آسیب پذیری‌های نرم‌افزاری نیاز باشد، پیشنهاد می‌شود که به روز رسانی‌های BIOS از طریق فرآیند به روز رسانی تایید اعتبار شده انجام شود. در صورتی که سازمان مشارکت فعال در فرآیند به روز رسانی داشته باشد، فرآیند کنترل چند بخشی باید برای بدست آوردن کلید خصوصی از حافظه امن و تولید امضای دیجیتال اجرا شود. همچنین پیشنهاد می‌شود که بسته نصب BIOS امضا شود، و امضای دیجیتال قبل از اجرا مورد بازبینی قرار گیرد. وقتی که به روز رسانی با موفقیت اجرا شد، برای تایید اینکه سیستم کامپیوتری همچنان مطابق با سیاست‌های تعریف شده سازمان است، پیشنهاد می‌شود که خط مشی پیکربندی[1] اعتبار سنجی گردد.

۷-۳-۴ فاز بازیابی

در برخی شرایط، به روز رسانی مورد نیاز BIOS نمی‌تواند با استفاده از فرآیند به روز رسانی تایید اعتبار شده انجام شود. به عنوان مثال، یک BIOS یا RTU معیوب شاید قادر به اجرا یا فراخوانی رویه‌های احراز هویت نباشد. در این گونه موارد، BIOS و/یا RTU مناسب ممکن است با استفاده از فرآیند به روز رسانی امن محلی نصب شوند. در سایر مواقع به روز رسانی BIOS ممکن است عواقب ناخواسته‌ای داشته باشد، که سازمان را مجبور به عقب‌گرد به نسخه پیشین کند. ممکن است مراحل بیشتری برای به روز رسانی تایید اعتبار شده به منظور صدور مجوز عقب‌گرد لازم باشد (اگر نسخه‌بندی یا برچسب زمانی در طول فرآیند اصالت‌سنجی مقایسه شوند)، یا ممکن است فرآیند به روز رسانی امن محلی برای برقراری پایه پیکربندی امن لازم باشد. همانند فاز نگهداری و عملیاتی ضروری است که پیکربندی BIOS را با سیاست‌های تعریف شده سازمان بعد از عقب‌گرد یا نصب دوباره اعتبارسنجی کنیم.

۷-۳-۵ فاز امحا

قبل از اینکه سیستم کامپیوتری امحا و از سازمان خارج شود، پیشنهاد می‌شود که سازمان هر گونه داده حساس BIOS را حذف یا نابود کند. بهتر است پایه پیکربندی دوباره به تنظیمات پیش‌فرض کارخانه‌ای برگردد، به ویژه اینکه پیشنهاد می‌شود تنظیمات حساس مثل رمز عبورها از سیستم حذف شوند، و کلیدها نیز از انباره کلید حذف گردند. اگر BIOS سیستم شامل هر گونه تغییرات سفارشی خاص سازمان باشد، پیشنهاد می‌شود تصویر BIOS تدارک دیده شده توسط عرضه‌کننده نصب شود. این فاز از چرخه حیات بستر نرم‌افزاری شانس نشت اطلاعات را کاهش می‌دهد.

1- Configuration baseline

کتاب‌نامه

[1] G. Duarte. "How Computers Boot Up." 5 June 2008.http://www.duartes.org/gustavo/blog/post/how-computers-boot-up

[2] EFI 1.10 Specification. Intel. 1 November 2003. http://www.intel.com/technology/efi/

[3] Shawn Embleton, Sherri Sparks, and Cliff C. Zou. "SMM Rootkits: A New Breed of OS Independent Malware," Proceedings of 4th International Conference on Security and Privacy in Communication Networks (SecureComm), Istanbul, Turkey, September 22-25, 2008 .

[4] FIPS 180-3, Secure Hash Standard. October 2008.

[5] FIPS 186-4, Digital Signature Standard. July 2013.

[6] Loïc Duflot, Olivier Grumelard, Olivier Levillain and Benjamin Morin. "ACPI and SMI handlers: some limits to trusted computing." Journal in Computer Virology. Volume 6, Number 4, 353-374.

[7] D. Grawrock. Dynamics of a Trusted Platform: A Building Block Approach. Hillsboro, OR: Intel Press, 2009.

[8] J. Heasman. "Firmware Rootkits: A Threat to the Enterprise." Black Hat DC. Washington, DC. 28 February 2007. http://www.nccgroup.com/Libraries/Document_Downloads/02_07_Firmware_Rootkits_The_Threat_to_the_Enterprise_Black_Hat_Washington_2007_sflb.sflb.ashx

[9] J. Heasman. "Hacking the Extensible Firmware Interface." Black Hat USA. Las Vegas, NV. 2 August 2007. https://www.blackhat.com/presentations/bh-usa-07/Heasman/Presentation/bh-usa-07-heasman.pdf

[10] Intel Platform Innovation Framework for EFI- Architecture Specification v0.9. Intel. September ۲۰۰۳. http://www.intel.com/technology/framework/

[11] A. Kumar, G. Purushottam, and Y. Saint-Hilaire. Active Platform Management Demystified .Hillsboro, OR: Intel Press, 2009.

[12] Salihun, Darmawan. BIOS Disassembly Ninjutsu Uncovered. Wayne, PA: A-LIST, 2007.

[13] A. Sacco, A. Ortéga. "Persistant BIOS Infection." Phrack. Issue 66. 6 November 2009 http://www.phrack.com/issues.html?issue=66&id=7

[14] NIST SP 800-57, Recommendation for Key Management – Part 1: General. March 2007.

[15] NIST SP 800-61rev1, Computer Security Incident Handling Guide. March 2008.

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

[17] Draft NIST SP 800-128, Guide for Security Configuration Management of Information Systems . March 2010.

[18] NIST SP 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algoriths and Key Lengths. January 2011.

[19] W95.CIH Technical Details. Symantec. 25 April 2002. http://www.symantec.com/security_response/writeup.jsp?docid=2000-122010-2655-99

[20] PC Client Work Group Specific Implementation Specification for Conventional Bios Specification, Version 1.2. Trusted Computing Group. July 2005. http://www.trustedcomputinggroup.org/resources/pc_client_work_group_specific_implementation_specification_for_conventional_bios_specification_version_12

[21] UEFI Specification Version 2.3. Unified EFI Forum. May 2009. http://www.uefi.org/specs/

[22] F. Wecherowski. “A Real SMM Rootkit: Reversing and Hooking BIOS SMI Handlers.” Phrack. Issue 66. 6 November 2009. http://www.phrack.com/issues.html?issue=66&id=11

[23] R. Wojtczuk and A. Tereshkin. “Attacking Intel BIOS.” Black Hat USA. Las Vegas, NV. 30 July 2009. http://www.blackhat.com/presentations/bh-usa09/WOJTCZUK/BHUSA09-Wojtczuk-AtkIntelBios-SLIDES.pdf