رابط متحد توسعه‌پذیر سیستم‌عامل

از ویکی‌پدیا، دانشنامهٔ آزاد

رابط متحد توسعه‌پذیر سیستم‌عامل (به انگلیسی: Unified Extensible Firmware Interface) یا به اختصار **UEFI**، یک ویژگی نرم‌افزاری رابط بین سیستم‌عامل و پلاتفرم سخت افزار می‌باشد. این ویژگی جایگزین رابط سخت‌افزار بایوس است. در حال حاضر در تمام کامپیوترهای شخصی سازگار با آی‌بی‌ام ارائه شده‌است. در بررسی‌ها، ویژگی UEFI، تمامی خدمات بایوس را پشتیبانی می‌کند. به وسیله این ویژگی می‌توان عیب یابی و تعمیرات (یا تنظیمات امنیتی) را بدون نیاز به هیچگونه سیستم‌عاملی انجام داد. EFI اصلی توسط اینتل توسعه داده می‌شد. برخی از این شیوه‌ها و قالب داده‌ها، انعکاسی از ویژگی‌های ویندوز می‌باشد.
در سال ۲۰۰۵ UEFI جایگزین EFI 1.10 (نسخه نهایی EFI) شد. در حال حاضر ویژگی UEFI توسط انجمن Unified EFI مدیریت می‌شود.

لوگوی UEFI

محتویات

تاریخچه

ایدهٔ اصلی برای EFI به هنگام توسعهٔ اولین سیستم ایتانیوم (به انگلیسی: Itanium) اینتل ـ اچ‌پی در اواسط دههٔ ۱۹۹۰ به وجود آمد. محدودیت‌های بایوس رایانه‌های شخصی (حالت پردازندهٔ ۱۶ ـ بیتی، ۱ مگابایت فضای قابل آدرس‌دهی، وابستگی‌های سخت‌افزاری پی‌سی ای‌اتی(به انگلیسی: PC AT) و...) برای سرورهای بزرگ‌تری که ایتانیوم به سمت آن‌ها حرکت می‌کرد، غیر قابل قبول بود.[۱] تلاش برای حل این مشکلات در ابتدا با نام *آغازگر بوت اینتل*، در سال ۱۹۹۸ شروع شد، و بعدها به EFI تغییر نام داد. در ژوئیه سال ۲۰۰۵ اینتل توسعهٔ ویژگی EFI را در ورژن ۱٫۱۰ آن متوقف کرد، و آن را به *انجمن یکپارچهٔ EFI* سپرد. این انجمن گسترش ویژگی را با عنوان *UEFI* (*Unified Extensible Firmware Interface*) آغاز کرد. مالک ویژگی ورژن اصلی EFI همچنان اینتل است که برای کالاهای تحت EFI مجوز فراهم می‌کند، اما مالکیت ویژگی UEFI به انجمن بر می‌گردد. ورژن UEFI ۲٫۱ در ۷ ژانویه ۲۰۰۷ منتشر شد. در این نسخه رمزنگاری، اهراز هویت تحت شبکه و معماری رابط کاربری (زیرسازه‌های رابط‌های انسانی در uefi) پیاده شدند. نسخه فعلی آن، ۲٫۳٫۱ در تاریخ آوریل ۲۰۱۱ مورد تائید قرار گرفت.[۲]

محتوا

رابط تعریف شده توسط مشخصه EFI شامل جداول داده‌ایِ اطلاعات پلت‌فرم، سرویس‌های بوت و سرویس‌های زمان‌اجرا می‌باشد که برای بارگذارنده سیستم‌عامل و همچنین خود سیستم‌عامل قابل دسترس می‌باشد. فرم‌ویر UEFI مزایای چندی را نسبت به بایوس قدیمی سیستم‌ها داراست.[۳]

- قابلیت راه‌اندازی از دیسک‌های بزرگ (بیش‌از ۲٫۲ ترابایت) با کمک GPT.
- زمان راه‌اندازی سریعتر
- معماری مستقل از پردازنده
- درایورهای مستقل از پردازنده
- محیطی انعطاف‌پذیر قبل از اجرای سیستم‌عامل، شامل قابلیت اتصال به شبکه
- طراحی ماژولار

سازگار با پردازنده

بایوس محدود به مُد پردازنده ۱۶ بیتی و ۱ مگابایت فضای قابل آدرس‌دهی است که این امر به دلیل طراحی آن برای کامپیوتر ۵۱۵۰ شرکت IBM بوده که از پردازنده ۱۶ بیتی ۸۰۸۰ اینتل استفاده می‌کرده‌است.[۴][۵] در مقایسه، مُد پردازنده در UEFI می‌تواند ۳۲ بیتی (برای معماری x86-32 و ARM) و یا ۶۴ بیتی (برای معماری x86-64 و ایتانیوم) باشد. [۶] UEFI ۶۴

بیتی از long mode که به برنامه‌ها در محیط اجرائیِ پیش از بوت، اجازه دسترسی به تمامی حافظه با استفاده از آرس دهی ۶۴ بیتی می‌دهد پشتیبانی می‌کند. [۷] UEFI عملاً نیاز دارد تا فرم‌ویر و سیستم‌عامل از نظر اندازه بیت محاسباتی هم اندازه باشند. به عنوان مثال طراحی ۶۴ بیتی UEFI تنها می‌تواند یک سیستم‌عامل ۶۴ بیتی را راه‌اندازی کند.

سازگار با دستگاه‌های حافظه

در EFI علاوه بر شمای استاندارد پارتیشن دیسک، که از رکورد بوت‌اصلی (به انگلیسی: Master Boot Record) استفاده می‌کند، شمای پارتیشن‌بندی جدیدی نیز استفاده می‌کند. جدول پارتیشن GUID (به اختصار *GPT*) فاقد از هرگونه محدودیت‌های موجود در معماری رکوردبوت اصلی داس می‌باشد. به طور مشخص، این رکورد محدود به تعداد و اندازه پارتیشن‌های دیسک (تا ۴ پارتیشن بر روی هر دیسک و تا ۲/۲ ترابایت برای هر دیسک) می‌باشد در حالی که GPT قادر به شناسایی دیسک یا پارتیشنی به اندازه ۹/۴ زِتابایت (به انگلیسی: ZiB) می‌باشد. همچنین مشخصه EFI به فایل سیستم خاصی محدود نمی‌شود. [۸]

سرویس‌ها

EFI دو نوع سرویس را معرفی کرده‌است. سرویس‌های راه‌انداز و سریس‌های زمان اجرا. سرویس‌های بوت تنها زمانی که فرم‌ویر مالکیت پلت‌فرم را در اختیار دارد قابل دسترس می‌باشند (قبل از فراخوانی ExitBootServices). سرویس‌های بوت شامل کنسول‌های متنی و گرافیکی بر روی دستگاه‌ها و باس‌های مختلف و دستگاه‌های متنی/داده‌ای می‌شود. درحالی که سرویس‌های زمان اجرا تا زمانی که سیستم‌عامل در حال اجراست نیز قابل دسترسی هستند. سرویس‌های زمان اجرا شامل سرویس‌هایی چون تاریخ، زمان و دسترسی به NVRAM می‌شوند.

سرویس‌های متغیری

متغیرهای UEFI روشی برای ذخیره داده‌ها را به شکلی غیرفرار مهیا می‌کند که مابین فرم‌ور پلتفرم و سیستم‌عامل و یا ابزار خود UEFI به اشتراک گذاشته می‌شود. فضای‌نام متغیر توسط GUIDها شناسائی می‌شوند. این متغیرها شامل جفت داده‌های کلید و مقدار می‌باشند.

سرویس‌های زمانی

UEFI سرویس‌های زمانی مستقل از دستگاه را شامل می‌شود. سرویس‌های زمانی‌ای شامل پشتیبانی از منطقه زمانی و فیلدهای صرفه‌جویی در مصرف روشنایی روز که به ساعت بلادرنگ سخت‌افزاری اجازه می‌دهد تا به زمان محلی و یا به وقت جهانی تنظیم شود. در ماشین‌هایی که از ساعت بلادرنگ PC-AT استفاده می‌کنند، هنوز ساعت نیاز به تنظیم شدن به زمان محلی برای سازگاری با ویندوزهای مبتنی بر بایوس دارند.

پروتکل‌ها

EFI پروتکل‌ها را به‌عنوان مجموعه‌ای از رابط‌های نرم‌افزاری برای ارتباطات مابین دو ماژول باینری معرفی کرده‌است. تمامی درایورهای EFI سرویس خود را از طریق این پروتکل‌ها به دیگران ارائه می‌دهند.

درایورهای دستگاه

علاوه بر راه‌اندازهای دستگاه‌های استانداردی که مبتنی بر معماری خاصی هستند، efi محیطی را برای درایورهای مستقل از پردازنده مهیا می‌کند که کدبایتِ efi و یا به‌اختصار EBC نامیده می‌شود. با این مفهوم، EBC شبیه به open-hardware، فرم‌ویر مستقل از سخت‌افزار استفاده شده در کامپیوترهای مکینتاش مبتنی بر Power-PC شرکت Apple و کامپیوترهای اسپارک شرکت Sun Microsystems می‌باشد.

ویژگی‌های بخش گرافیک

مشخصه efi پروتکل UGA (مبدل گرافیک جهانی) را به عنوان روشی برای پشتیبانی از گرافیک مستقل از سخت‌افزار معرفی کرده‌است. حال uefi شامل UGA نمی‌شود بلکه آن را با پروتکل GOP (پروتکل خروجی گرافیکی) با هدف حذف وابستگی‌های سخت‌افزاری vga جایگزین کرده‌است. این دو پروتکل مشابه یکدیگر می‌باشند.
در uefi نسخه ۲٫۱ زیرساخت رابط انسانی (HII) معرفی شده تا ورودی کاربری را مدیریت، رشته‌ها، قلم‌ها و فرم‌ها را (به مفهوم HTML) محلی‌سازی کند. این ویژگی، OEMها و یا IBVها را قادر به طراحی رابط‌های گرافیکی برای انجام عملیات پیکره‌بندی قبل از راه‌اندازی سیستم‌عامل می‌سازد. UEFI خود شامل رابط کاربری نمی‌شود. بیشتر پیاده سازی‌های اولیه UEFI بر پایه کنسول بودند اما از ابتدای سال ۲۰۰۷ چندین پیاده سازی با رابط کاربری گرافیکی صورت گرفته‌است.

راه‌اندازی

UEFI مدیر راه‌انداز (به انگلیسی: Boot Manager) خود را داراست. این مدیر راه‌انداز، موتور رویه‌ای فرم‌ویر است که مسئول بارگذاری بارگذارنده سیستم‌عامل (به انگلیسی: OS loader) و تمام درایورهای مورد نیاز می‌باشد. پیکره‌بندی راه‌انداز، توسط مجموعه‌ای از متغیرهای سراسری NVRAM شامل متغیرهای راه‌انداز که مسیر بارگذارنده‌های سیستم‌عامل‌ها را مشخص می‌کنند شامل می‌شود.
بارگذارنده‌های سیستم‌عامل دسته‌ای از ابزارهای UEFI می‌باشند. به عنوان مثال، این بارگذارنده‌ها بر روی سیستم‌فایلی به صورت یک سند مجزا ذخیره شده‌اند که می‌توانند برای فرم‌ویر قابل‌دسترس باشند. سیستم‌فایل های پشتیبانی شده در UEFI شامل FAT12 (فلاپی دیسک‌ها)، FAT16 و FAT32 در دیسک‌های سخت و ISO9660 و UDF در دیسک‌های فشرده (CD/DVD) می‌باشد. جدول‌های پارتیشن پشتیبانی شده نیز شامل MBR و GPT می‌باشند. بارگذارنده‌های راه‌انداز (به انگلیسی: Boot Loaders) نیز می‌توانند به صورت خودکار توسط فرم‌ویر شناسایی شوند تا در نهایت منجر به راه‌اندازی شدن از دستگاه‌های قابل‌حملی همچون حافظه‌های USB شوند. این ویژگی متکی بر استانداردسازی مسیر فایل راه‌انداز سیستم‌عامل‌ها می‌باشد که

وابسته به معماری پلت‌فرم خواهد بود.
همچنین عموماً فرم‌ویرهای UEFI شامل رابط کاربری‌ای برای مدیریت راه‌انداز خود هستند تا به کاربران خود اجازه انتخاب و راه‌اندازی سیستم‌عامل‌شان را از میان گزینه‌های قابل انتخاب بدهند.

پوسته EFI

EFI پوسته‌ای را معرفی کرده که می‌تواند برای اجرای دیگر ابزارهای EFI مورد استفاده قرار بگیرد.

الحاقات

الحاقیات (به انگلیسی: Extensions) را می‌توان به واقع از هر حافظه غیرفراری که به کامپیوتر متصل شده‌است بارگذاری کرد. برای مثال، سازنده تجهیزات اصلی (به انگلیسی: OEM) می‌تواند سیستم‌هایی را با پارتیشن EFI بر روی دیسک سخت کامپیوتر خود تولید و روانه بازار کند که کارائی‌های اضافه‌تری را نسبت عملکرد استاندارد EFI موجود بر روی بردمادر در اختیار کاربر قرار می‌دهد.

پیاده‌سازی و به‌کارگیری

اینتل

پیاده سازی اینتل از EFI *چارچوب نوین پلت‌فرم اینتل* (به انگلیسی: Intel Platform Innovation Framework) با کدنام *تیانو* (به انگلیسی: Tiano) نامیده می‌شود.

سیستم‌های عامل

سیستم‌عاملی که بتواند از فرم‌ویر EFI/UEFI راه‌اندازی شود اصطلاحاً سیستم‌عامل آگاه از EFI/UEFI (به انگلیسی: EFI-(U) aware OS) نامیده می‌شود. واژه **راه‌اندازی شدن از EFI/UEFI** بدین معناست که سیستم مستقیماً و با استفاده از «بارگذارنده سیستم‌عامل» EFI/UEFI ذخیره شده بر روی دستگاه حافظه، راه‌اندازی شود. مکان پیش‌فرض این بارگذارنده برابر است با EFI/BOOT/boot[arch].EFI/ برخی از بنگاه‌های فروش سیستم‌عامل ممکن است بارگذارنده سیستم‌عامل (به انگلیسی: OS Loader) خود را داشته باشند و یا همچنین مسیر پیش‌فرض راه‌انداز را تغییر دهند.

- لینوکس، از اوایل سال ۲۰۰۰ قادر بوده تا از EFI در زمان راه‌اندازی با استفاده از «بارگذارنده راه‌انداز EFI» ابزار elilo و یا نسخه جدیدتر EFI ابزار GRUB استفاده کند. همچنین لینوکس به همراه ابزار گراب می‌تواند از جدول پارتیشن GUID بدون نیاز به UEFI راه‌اندازی شود.

نقدها

بسیاری از فعالان حقوق دیجیتالی به UEFI اعتراض کرده‌اند. رونالد جی. مینیچ (به انگلیسی: Ronald G. Minnich)، یکی از نویسندگان *coreboot*، و کُری داکترو (به انگلیسی: Cory Doctorow)، فعال حقوق دیجیتالی، EFI را به عنوان تلاشی برای حفظ «مالکیت خصوصی» توسط حذف امکان کنترل کامل رایانه، توسط مالکش نقد کرده‌اند.[۹]
همچنین مشکلات قدیمی بایاس را در نیاز به وجود دو راه‌انداز متفاوت، یکی برای فرم‌ویر و دیگری برای سیستم‌عامل را بر روی بیشتر سخت‌افزارها رفع نمی‌کند.
در UEFI پشته شبکه، برخلاف بسیاری از BIOSها به صورت کامل از ابتدا پیاده‌سازی شده‌است و بهمین دلیل هدف بالقوه‌ای برای سوءاستفاده‌های امنیتی راه‌دور می‌باشد

راه‌انداز امن

توسعه‌دهنده شرکت Red Hat به نام متیو گرت (به انگلیسی: Matthew Garrett) در مقاله‌اش با عنوان «راه‌اندازی امن در»UEFI (به انگلیسی: UEFI secure booting) نگرانی خود را چنین مطرح کرده که ویژگی «راه‌انداز امن» ممکن‌است ضربه‌ای برای لینوکس باشد (ماشین‌هایی که به همراه لوگوی ویندوز ۸ و با قابلیت فعال‌شده بوت‌امن همراه با فقط کلیدهای شرکت OEM و مایکروسافت فروخته می‌شوند قادر به راه‌اندازی کپی‌ای از سیستم‌عامل لینوکس نخواهند بود). در جوابیه، شرکت مایکروسافت بیان کرد که مشتریان قادر خواهند بود تا ویژگی راه‌انداز امن را از طریق رابط UEFI غیرفعال کنند ولی نگرانی‌ها همچنان باقی‌است چراکه برخی OEMها ممکن‌است این قابلیت را از کامپیوترهای خود حذف کنند. بعدها گزارش شد که مایکروسافت ظاهراً پیاده‌سازی قابلیت غیرفعال سازی بوت‌امن را بر روی سیستم‌هایی با معماری ARM را ممنوع کرده‌است.
جاشوا گی (به انگلیسی: Joshua Gay) از بنیاد نرم‌افزار آزاد نیز نگرانی خود مبنی بر پیاده‌سازی «راه‌انداز امن» در UEFI را مطرح و بنیاد نرم‌افزار آزاد بیانیه عمومی‌ای را برای امضاکردن معرفی کرد که چنین می‌گوید:

> ما (امضاکنندگان این بیانیه) از تمامی سازندگان کامپیوتری که ویژگی «راه‌انداز امن» خوانده شده در UEFI را پیاده‌سازی می‌کنند می‌خواهیم تا این کار را به روشی انجام دهند تا به سیستم‌عامل‌های آزاد اجازه نصب شدن را بدهند. برای احترام به آزادی کاربر و حفاظت صحیح از امنیت کاربر، سازندگان بایستی یا این اجازه رابه مالک کامپیوتر بدهند تا محدودیت راه‌اندازی مذکور را غیرفعال و یا روش مطمئنی را برای نصب و اجرای سیستم‌عامل آزاد به انتخاب مالک در اختیارش قرار داده شود. ما تاکید می‌کنیم که نه چنین کامپیوترهایی را می‌خریم و نه کامپیوترهایی را که کاربران را از این آزادی مهم سلب می‌کنند توصیه می‌کنیم و فعالانه از مردم در جوامع‌مان می‌خواهیم تا از چنین سیستم‌های زندان‌مانندی پرهیز کنند.

در دسامبر ۲۰۱۱، شرکت مایکروسافت سندی را مرتبط با گواهینامه سخت‌افزاری محصولات OEM خود منتشر کرد، «شرایط لازم برای گواهینامه سخت‌افزاری ویندوز» تائید می‌کند آنها در تلاش برای سلب امکان نصب سیستم‌عامل معادل بر روی دستگاه‌های ARM هستند که ویندوز ۸ در آنها اجرا شده‌است. این سند اصرار دارد که مایکروسافت نیاز دارد تا دستگاه‌های x86 و x86-64 ویژگی امنیتی UEFI را به صورت پیش‌فرض فعال داشته باشند. آنها امکانی را که بوت امن شخصی‌سازی‌شده بتواند کاربر را قادر به اضافه‌کردن امضا کند را در این سند مجاز شمرده‌اند. هرچند که تلاش برای اجرای راه‌انداز امن شخصی‌سازی‌شده و یا انتخاب حالت غیرفعال شده راه‌اندازامن بر روی دستگاه‌های ARM با شرایط دریافت این گاهینامه ناسازگار اعلام شده‌است.

منابع

- مشارکت‌کنندگان ویکی‌پدیا، «Unified Extensible Firmware Interface» (http://en.wikipedia.org/w/index.php?title=Unified_Extensible_Firmware_Interface&oldid=490836814)، ویکی‌پدیای انگلیسی، دانشنامهٔ آزاد (بازیابی در ۱۹ می۲۰۱۲).

۱. "Emulex UEFI Implementation Delivers Industry-leading Features for IBM Systems". Emulex. Retrieved 14 September 2010.
۲. Intel Technology Journal (http://www.intel.com/technology/itj/2011/v15i1/index.htm)
۳. UEFI and Windows (http://www.microsoft.com/whdc/system/platform/firmware/UEFI_Windows.mspx)
۴. http://www.emulex.com/artifacts/757d23e7-8acb-41a7-872a-afb733ab0688/elx_tb_all_uefi_ibm.pdf
۵. LBA explained - Solving the 3TB Problem? | bit-tech.net (http://www.bit-tech.net/hardware/storage/2010/06/01/are-we-ready-for-3tb-hard-disks/2)
۶. http://www.emulex.com/artifacts/757d23e7-8acb-41a7-872a-afb733ab0688/elx_tb_all_uefi_ibm.pdf
۷. http://download.microsoft.com/download/5/e/6/5e66b27b-988b-4f50-af3a-c2ff1e62180f/cor-t605_wh08.pptx
۸. http://www.uefi.org/learning_center/UEFI_MBR_Limits_v2.pdf
۹. «Interview: Ronald G Minnich». Fosdem، 6 February 2007. بازبینی‌شده در 14 September 2010.