print | close

# What's the Difference Between Firmware, Then and Now?

*Electronic Design*

(Unpublished) Michael Krau

Fri, 2016-10-21 12:24

The Unified Extensible Firmware Interface (UEFI) Forum is a community effort supported by industry-leading technology organizations and individuals to enable the evolution of firmware platform technologies. The Forum champions firmware innovation through industry collaboration and the advocacy of a standardized interface that simplifies and secures platform initialization and firmware bootstrap operations. UEFI specifications promote business and technological efficiency; improve performance and security; facilitate interoperability between devices, platforms and systems; and enable next-generation technologies.

**Firmware Then**

In 1979, IBM introduced its personal computer (PC), which included the first BIOS (Basic Input/Output System) instruction set in the firmware. The team designing the PC at IBM was told that expectations for sales were modest, on the order of a few hundred thousand machines to the product's end of life. In fact, though, they sold more like 750,000 and created a new standard that has been replicated by an entire industry for the past 35 years (plus).

Related

11 Myths About UEFI

The Migration from Legacy BIOS to UEFI Firmware

Bye Bye BIOS. Hello UEFI

Since the design team didn't have extremely high expectations for the PC, there wasn't really a lot of consideration given to long-term evolution in the initial design of BIOS. As a result, through the years, the technology was extended in ways not originally envisioned. Over time, the BIOS started to become increasingly complex and serpentine in order to shoehorn new functionality in places it was never intended to fit.

This created the opportunity for manufacturers to develop clones of the IBM PC, and they began reverse-engineering the machines to create new dialects of BIOS. At one point, Intel identified over 20 separate versions of BIOS that required its support. Consequently, myriad versions were out there, all of which were complex and different enough that inserting support for new technology was a major job across the industry. Essentially, it was like doing one complicated engineering retrofit 20 times over, adding no new real value each time. As an ecosystem, this simply wasn't economically sustainable.

Part of the problem was that IBM recognized it had a winner technology after the fact. When IBM went back to redesign the PC, it committed to the PS2 and the Micro Channel Architecture (MCA). Moreover, its licensing of

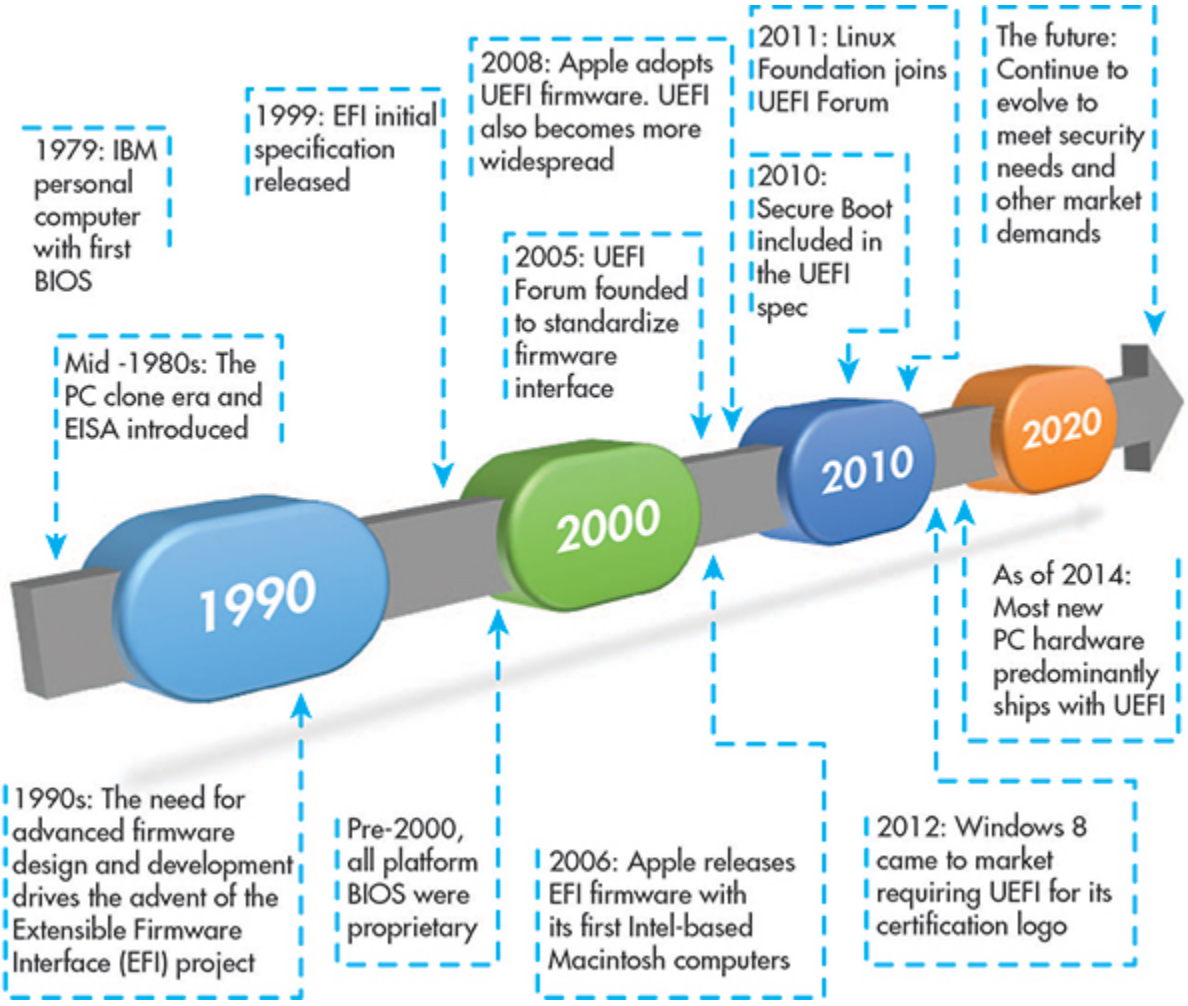
A was extremely limiting; many vendors had been building PC-compatible designs years before MCA/PS2. wever, to license MCA/PS2 the licensee would have to pay a "back royalty" to IBM for every PC design they ever sold.

Not only did this licensing plan fail, but it created such ire in the industry, the "Gang of Nine" (Compaq, AST Research Inc., Epson America Inc., Hewlett-Packard, NEC Corp., Ing C. Olivetti & Co., Tandy Corp., Wyse Technology, and Zenith Data Systems[1]) started the Extended Industry Standard Architecture (EISA) as a counter to IBM's use of its proprietary MCA/PS2. EISA also created the only specification for the PC architecture, under the Title ISA (Industry Standard Architecture), which EISA then extended.

The MCA/EISA split only acted to push the BIOS quagmire out further. With PCs, PS/2s, and EISA-type systems all coexisting, BIOS implementations fractured even further. While all three architectures share much of the same BIOS functionality, the underlying architectures forced more separation of BIOS implementations.

The fundamental design of the original BIOS didn't change, but was always changing in small pieces, which created troublesome issues around PC compatibility. In the 1990s Intel started looking at new ways to boot into the 64-bit architecture with its 64-bit Itanium processor. The original BIOS could not extend to this new architecture, so Intel answered this challenge by developing the Extensible Firmware Interface (EFI) project, with the initial specification released in 1999. The Itanium class device was such a special case that the EFI boot mechanism was considered a strange "one-off." The legacy BIOS was still around and doing well; therefore, the need to shift was not evident.

Eventually, the market pushed for an open industry standard, leading to industry-wide cooperation to protect the interests of the entire ecosystem in the firmware space. In 2005, the UEFI Forum was founded to standardize and extend the firmware to the 64-bit architecture as well as create a common approach for firmware development.




Legacy BIOS had many limitations that were becoming evident with the more advanced technology. UEFI's extensibility allowed systems to take advantage of new technology improvements, which would have proven problematic under the old legacy BIOS solution. The first UEFI specification, which improved the underlying architecture of the BIOS/Pre-OS environment, was designed to promote cross-functionality, as well as support broad adoption across multiple operating systems, including Windows and Linux-based operating systems.

From here, the UEFI specification took off. In 2006, Apple adopted the UEFI standard along with other OEMs that offered 64-bit architecture. In 2010, the UEFI specification addressed security issues with the introduction of Secure Boot. Secure Boot prevented the operating systems from booting unless signed by a key loaded into UEFI. The introduction of Secure Boot is pivotal because it gave Microsoft a level of security that helped build products that customers would trust and want to buy. Therefore, in 2012, Microsoft introduced Windows 8 that required UEFI for its certification logo.[2] By 2014, most new PC hardware was shipping predominately with UEFI.

**Firmware Now**

UEFI is prevalent in the market today; in fact, UEFI is in 80% to 90% of the PC and server markets.[3] Much of what the UEFI Forum has focused on from the beginning is to simplify and remove duplication between firmware and the operating system, allowing them to work together in harmony.

The UEFI specification took off because the original legacy BIOS was beginning to unravel (technically), and new systems were needed to support new and emerging technologies.

oss multiple interfaces, firmware today supports a more secure system, faster boot times, more innovation, a faster time-to-market. In contrast to prior coding structures, UEFI specifications allow for extensibility, modularity, and easy prototyping during development. The specifications are robust and can potentially complement—or even advance—other distributions, such as Linux-based distributions.

The UEFI Forum is focused on creating solutions to changing market demands and challenges that arise. For example, due to increased security features on hardware and software being developed on a daily basis, hackers have become more sophisticated—the vulnerability of the firmware and pre-boot space in a PC is still is a prime target.

As a potential solution to this problem, the UEFI Forum called for firmware, which would describe "hardware linkage and dependencies" and "should not allow execution of code of unknown/untrusted origin." There was little protection enabled through legacy firmware, simply because it was not a top-tiered target. Now, firmware is a key component to the protection of the PC and its valuable stored information.

**Conclusion**

UEFI specifications reflect the past 30-plus years of PC evolution. They describe an abstract interface set for transferring control to an operating system or building modular firmware from one or more silicon and firmware suppliers.

The UEFI Forum, with approximately 300 member companies, continues to evolve platform specifications to meet new technology needs and challenges. The Forum works to ensure critical variables are protected, providing more flexibility to designers and helping the industry adopt new secure implementations that enhance platform security.

To learn more about the UEFI Forum community, please visit: www.uefi.org. More information on joining can be found here: www.uefi.org/membership.

**References:**

1. Bane, M. (1998, November 20), "9 Clonemakers Unite to Take On the Industry Giant," Chicago Tribune. Retrieved June 27, 2016, from http://articles.chicagotribune.com/1988-11-20/business/8802180783_1_extended-industry-standard-architecture-ibm-compaq-computer-corp.

2. Hoot, Scott "Three Pivotal Features Differentiating Bootloading Options," *Electronic Design*, Jan. 5, 2015.

3. UEFI Forum.



**Source URL:** http://electronicdesign.com/dev-tools/what-s-difference-between-firmware-then-and-now