

Say goodbye to BIOS — and hello to UEFI!



By Woody Leonhard

If you've ever struggled with your PC's BIOS — or been knee-capped by a rootkit that assailed the BIOS — you undoubtedly wondered why this archaic part of every PC wasn't scrapped long ago.

Well, be of good cheer: Windows 8 will finally pull the PC industry out of the BIOS generation and into a far more capable — and controversial — alternative, the Unified Extensible Firmware Interface.

To best understand where we're headed, it's helpful to look at where we've been. An integral part of every PC, the Basic Input/Output System spans the entire history of the personal computer — more than 30 years. The very first IBM PC had a BIOS. And despite extraordinary advances in hardware and software, the BIOS we still puzzle over today is not much different from the one in that original PC.

Essentially a miniature OS, the BIOS has a simple but critical function — when a PC powers up, the BIOS checks that all hardware is in order (the POST or "power-on self-test" sequence); fires up the full operating system on the machine, such as Windows (using OS loader code); and then hands all control of the computer over to the OS.

Although older operating systems (such as DOS) relied on the BIOS to perform input and output functions, modern OSes (including Windows) have their own device drivers and completely bypass the BIOS after they're up and running.

These days, it's rare that a PC user is forced to invoke the BIOS's cryptic and somewhat enigmatic user interface. Usually, it's in response to some near-catastrophic system failure.

The Unified Extensible Firmware Interface (UEFI) is essentially the next generation of BIOS. It's a system that potentially offers new and more advanced control of the boot-up process. If your PC is less than two or three years old, chances are good that it already has UEFI ([more info](#)) capabilities. Chances are **very** good that you didn't know that, because the hardware manufacturers have been carefully keeping the old BIOS interface as your default boot system. But that will change with Windows 8.

generation and into a far more capable — and controversial — alternative, the Unified Extensible Firmware Interface.

To best understand where we're headed, it's helpful to look at where we've been. An integral part of every PC, the Basic Input/Output System spans the entire history of the personal computer — more than 30 years. The very first IBM PC had a BIOS. And despite extraordinary advances in hardware and software, the BIOS we still puzzle over today is not much different from the one in that original PC.

Essentially a miniature OS, the BIOS has a simple but critical function — when a PC powers up, the BIOS checks that all hardware is in order (the POST or "power-on self-test" sequence); fires up the full operating system on the machine, such as Windows (using OS loader code); and then hands all control of the computer over to the OS.

Although older operating systems (such as DOS) relied on the BIOS to perform input and output functions, modern OSes (including Windows) have their own device drivers and completely bypass the BIOS after they're up and running.

These days, it's rare that a PC user is forced to invoke the BIOS's cryptic and somewhat enigmatic user interface. Usually, it's in response to some near-catastrophic system failure.

The Unified Extensible Firmware Interface (UEFI) is essentially the next generation of BIOS. It's a system that potentially offers new and more advanced control of the boot-up process. If your PC is less than two

or three years old, chances are good that it already has UEFI ([more info](#)) capabilities. Chances are **very** good that you didn't know that, because the hardware manufacturers have been carefully keeping the old BIOS interface as your default boot system. But that will change with Windows 8.

How UEFI is different from/better than BIOS

The standard BIOS has all sorts of problems, not least of which is its susceptibility to malware. For example, there are rootkits that hook themselves into the BIOS OS-loader code, permitting them to run underneath Windows. They're difficult to remove and will re infect Windows over and over.

And because the BIOS sits on a chip on the motherboard, it's more difficult to update than an operating system or an application. So most PC users never update their BIOS, leaving the PC possibly incompatible with newer operating systems. (The early PC BIOS was hard-coded on a chip, so upgrading required replacing the entire chip or PROM.)

The UEFI is a more sophisticated system that runs before your primary OS kicks in. Unlike the BIOS, UEFI can access **all** PC hardware, including the mouse and network connections. It can take advantage of modern video cards and monitors. It can even access the Internet.

And as you can see in Figure 1, UEFI offers a modern, easy-to-decipher user interface. It could make dual-booting simpler, more visual, and controllable by mouse or touch. If you've ever played your BIOS, you discover that UEFI is in a whole new dimension.



Figure 1. The Asus.com website offers this view of a UEFI-interface screen — clearly, an improvement over the typical BIOS UI we're faced with today.

Unlike the BIOS, the UEFI can exist on a disk, just like any other program — or in nonvolatile memory on the motherboard or even on a network share.

At this point, it's important to note that systems can run either the BIOS or the UEFI — or both. When they're both used, the BIOS goes first to run POST, then the UEFI takes over and hooks into any calls that may be made to the BIOS. (Windows typically doesn't make calls directly to the BIOS, but other

operating systems might — and the UEFI will handle them, not the BIOS.)

The UEFI can also run without the BIOS — it can take care of all OS loading/interface functions previously handled by the BIOS. The only thing the UEFI can't do is perform the POST or run the initial setup (configuring the CPU, memory, and other hardware). PCs that have the UEFI but no BIOS have separate programs for POST and setup that run automatically when the PC is powered on.

As we all know, the BIOS initialization process — including POST — seems to take a long time. The UEFI, on the other hand, can run quickly.

Moreover, a BIOS is easily reverse-engineered and typically has no internal security protection, making it a sitting duck for malware. A UEFI can run malware-dodging techniques such as policing operating systems prior to loading them — which might make rootkit writers' lives considerably more difficult. For example, the UEFI could refuse to run OSes that lack proper digital security signatures.

And that's where the UEFI controversy begins.

Windows 8 will implement UEFI in new ways

Back in September, Microsoft wrote voluminously about the UEFI in Windows 8. The first [post](#), "Reengineering the Windows boot experience," talks about the basic ways Windows 8 will use the UEFI. (If your PC doesn't support a UEFI, Win8 should still work fine.)

The article shows how current text-based, boot-time options, such as system repair store and image recovery, can be made more usable with a new graphical interface. The story goes on to describe how system startup could go, in seconds, from power-on to Windows Desktop without so much as flickering the screen. It also shows how dual-boot will work with a graphical face-lift.

The changes appear to be largely cosmetic, but they're long overdue and a welcome improvement to the constrained, DOS-era recovery environments under which Windows operates.

The second [article](#), "Protecting the pre-OS environment with UEFI," shows how the UEFI secure boot — using Public Key Infrastructure (PKI) digital certificates — validates programs, peripherals, and OS loaders before they can run. The system can go out to the Internet and check whether the UEFI is about to run an OS that has had its certificate yanked.

If it sounds a lot like Secure Sockets Layer protection — no stranger to controversy, as I detailed in my Sept. 15, 2011, [Top Story](#) — there certainly are similarities.

Microsoft states it will let the hardware manufacturers struggle with the difficult question of who controls the digital-signature keys. "Microsoft supports OEMs having the flexibility to decide who manages security certificates and how to allow customers to import and manage those certificates, and manage secure boot. We believe it is important to support this flexibility to the OEMs and to allow our customers to decide how they want to manage their systems."

Still, Microsoft is ensuring that anyone buying a certified Windows 8 PC can rely on a certain level of protection from rogue OS loaders. "For Windows customers, Microsoft is using the Windows Certification program to ensure that systems shipping with Windows 8 have secure boot enabled by default, that firmware not allow programmatic control of secure boot (to prevent malware from disabling security policies in firmware), and that OEMs prevent unauthorized attempts at updating firmware that could compromise system integrity."

The controversial side of dual boot

When those details first hit, the Linux community flew up in arms. Dual booting between Windows 8 and Linux might require a digital signature from a recognized certificate authority. That authority might be

Microsoft, through its Windows Certification program, and Linux folks would have to pay the piper.

That controversy went on for a while but eventually died down (though it never disappeared) when it became clear that putting together the signature is relatively easy and not very expensive.

Then another conflagration started last week. To understand why, you have to understand that UEFI secure boot has two bail-out options. First, most PCs let you turn off UEFI secure boot entirely. You have to be sitting at the computer and do it manually, but it's easy enough. In one of the Microsoft postings mentioned previously, the company acknowledged that hardware manufacturers could "allow customers to ... manage secure boot."

Second, there's a provision for something called "custom secure boot mode" in which you, as a customer, can sit at your computer and type in a signature for any OS loader you darned well like. This manually created whitelist overrides the Windows 8 or third-party check, letting the UEFI run OS loaders unhindered.

You must also understand that Windows 8 will run on two entirely different hardware platforms — Intel/AMD platforms spanning the range from (ponderous!) tablets to full-size desktops, and the svelte, tablet-friendly ARM platforms. If you use Win8, one of your first decisions will be which platform you choose.

The Linux world was taken aback when researcher Glyn Moody and the Software Freedom Law Center announced last week in a [blog](#) that Microsoft is making specific demands from hardware manufacturers who intend to sell Windows 8 bundled with their ARM machines — that is, those lightweight Windows 8 tablets. The Microsoft restrictions prevent hardware manufacturers from disabling secure boot and also prevent hardware manufacturers from implementing "custom secure boot" whitelists — but again, only on ARM hardware.

In other words, if at some point in the future you buy an ARM-based tablet with Windows 8 preinstalled, you won't be able to dual-boot with Linux or any operating system other than the ones that pass the security check. Presumably that could mean Windows 8 or some later version of Windows that Microsoft might ordain in the future.

Aside from the fact that the restrictions fly in the face of what Microsoft specifically said in September, it's hard for me to get too worked up about them. If you buy a Win8 (ARM) tablet, you won't be able to root it ([Wikipedia definition](#)), and you may not be able to upgrade it. You'll just have to take that into account when you think about buying one — assuming Microsoft is up-front about the limitation and mentions it to consumers.

Intel-based Windows 8 machines — even tablets (including tablets that run only the Metro interface) — aren't hobbled by those ARM restrictions. At least at this point, Intel/AMD machines are, in fact, required to allow multibooting (with signed operating systems) and even to replace Windows 8 with an OS of your choice. It remains to be seen whether Microsoft's going to change its mind about that distinction.