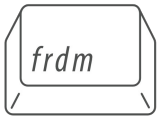

SOFTWARE FREEDOM LAW CENTER
1995 Broadway, 17th Floor
New York, NY 10023
212.580.0800
212.580.0898 fax
www.softwarefreedom.org

July 9, 2012

VIA E-MAIL & EXPRESS MAIL

Mr. David O. Carson
General Counsel
U.S. Copyright Office
P.O. Box 70400
Washington, D.C. 20024

Re: Docket No. RM 2011-7
Exemptions to Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works

Dear Mr. Carson:

I write in response to your letter of June 21, 2012, in which you asked "whether and how Windows 8 would prevent another operating system from being installed on a particular computing device." As required by Microsoft's Windows Certification program, Windows 8 computers will use the "Secure Boot" mechanism of the Unified Extensible Firmware Interface ("UEFI") to prevent unauthenticated operating systems from booting. In this letter, we will describe how the Secure Boot mechanism works and how, in conjunction with Microsoft's certification requirements, it will prevent the installation and development of alternative operating systems, including the majority of free and open source operating systems.

I. How UEFI and Secure Boot Authenticate Software During System Boot

To understand how Microsoft's certification requirements limit operating system choice, it is first necessary to understand how UEFI Secure Boot works. The purpose of the UEFI system generally is to allow firmware embedded in a computer's hardware components to interface with the computer's operating system.[1] It replaces a legacy system called the Basic Input and Output System ("BIOS"). When a computer is first powered on, UEFI performs an initial set of operations known as the boot process,[2] which includes locating and initializing peripheral devices (e.g. a hard disk drive or mouse)

1 For a graphical depiction of the UEFI's placement in the software stack, *see* http://en.wikipedia.org/wiki/File:Efi-simple.svg (as of June 27, 2012).

2 Wikipedia, *Booting*, available at http://en.wikipedia.org/wiki/Booting, (as of June 27, 2012).

and then finding, loading, and starting an operating system.[3]

The UEFI standard defines an optional procedure called “Secure Boot” that is intended to prevent malicious code from being executed during the boot process. Secure Boot uses a security mechanism called public-key encryption to authenticate software being loaded during boot.[4] Public-key encryption employes a pair of cryptographic keys—one public, one private—to validate the authenticity of a digital file. A signature for the file is generated using an algorithm that takes both the file and the private key as input. The resulting signature is unique; it can only correspond to that particular file and can only have been generated by that particular private key. A person or computer in possession of the public key can verify—without having access to the corresponding private key—that the signature was generated by that private key and that the file has not been altered since the signature was generated.

Secure Boot uses this verification process to establish a trust relationship between a device's firmware and its operating system.[5] A limited set of public keys is enrolled into the device's firmware before it is sold.[6] When the system boots, the Secure Boot mechanism checks the signature of the operating system against the keys in its database. If the signature can be validated with a known key, the firmware can be sure that the operating system 1) was signed with a trusted private key and 2) has not been modified since signing.[7] If the signature cannot be validated using the known public key, then the system will not boot.[8]

II. Microsoft's Windows 8 Secure Boot Requirements

Though Secure Boot is an optional feature of the UEFI specification, Microsoft has made it mandatory for many devices through its Windows Hardware Certification Program, a set of technical requirements and tests by which computing device manufacturers can have their products certified as Windows-compatible.[9] According to the current Windows Hardware Certification Requirements, Secure Boot must be enabled on every personal computing device certified for Windows 8,[10] and each of those devices must have Microsoft's signing key pre-installed.[11]

For ARM devices, the requirements go much further: manufacturers must make it impossible for device owners to disable Secure Boot[12] or to enroll new keys in the UEFI key database.[13] This unprecedented

3 *Id.*

4 Unified Extensible Firmware Interface Specification, Version 2.3.1, Errata B, at 1449 (April 10, 2012) (available at http://www.uefi.org/specs) [hereinafter UEFI Specification].

5 *Id.* at 1448.

6 *Id.*

7 Jeremy Kerr et al., *UEFI Secure Boot Impact On Linux*, at 2, October 28, 2011, http://ozlabs.org/docs/uefi-secure-boot-impact-on-linux.pdf (last visited July 4, 2012); Matthew Garrett, *The Security of Secure Boot*, June 7, 2012, http://mjg59.dreamwidth.org/12897.html (last visited July 4, 2012).

8 *Id.*

9 *See, e.g.*, Windows Certification Policies and Processes, May 10, 2012, available at http://msdn.microsoft.com/en-us/library/windows/hardware/hh852370.aspx (last visited July 4, 2012); Windows Hardware Certification Program, available at http://msdn.microsoft.com/en-us/library/windows/hardware/gg463010.aspx (last visited July 4, 2012).

10 Microsoft, Windows Hardware Certification Requirements, at 119, available at http://msdn.microsoft.com/en-us/library/windows/hardware/hh748200 (last visited July 2, 2012) [hereinafter Windows Hardware Certification Requirements]. Servers are the only devices excluded from this requirement. *Id.*

11 *Id.* at 122.

12 *Id.*

13 *Id.*; s*ee also* James Bottomley and Jonathan Corbet, *Making UEFI Secure Boot Work With Open Platforms*, The Linux

restriction applies to all Windows phones and tablets, including Microsoft's recently announced Surface tablet.[14] It also applies to a significant number of notebook and "hybrid" notebook-tablet computers; according to current estimates, 3% of all notebook computers are ARM-based,[15] a figure that is expected to grow to 23% by 2015.[16]

As we discussed in our initial comments, most personal computer vendors seek certification, because Microsoft controls nearly 90% of the PC operating system market.[17] Consequently, the majority of new personal computers and other Windows devices will recognize Microsoft's key. Few hardware manufacturers are likely to install other vendors' keys, because such a large majority of consumers use Windows. And for ARM devices, certification may be not only strongly recommended, but required: Microsoft plans to make its ARM version of Windows available only to hardware vendors for pre-installation on devices,[18] which would allow it to require certification as a condition of the license.

III. The Impact of Microsoft's Requirements on Free Software Operating Systems

The combination of Microsoft's Secure Boot-related certification requirements with Windows' market dominance has several practical consequences. First, owners of Windows-certified non-ARM devices (i.e. most personal computers) who wish to install an operating system that is not signed with Microsoft's key will be required to either disable Secure Boot or enroll a key corresponding to that operating system in the UEFI database. Second, owners of Windows-certified ARM devices will be unable to install any operating system that is not signed with Microsoft's key. Third, operating system developers will be unable to produce new or adapted operating systems for Windows-certified ARM devices.

In an effort to quiet the concerns of other operating system producers about the supremacy of its key, Microsoft has established a program (in partnership with Verisign) to allow third parties to have their operating systems signed by Microsoft. After paying a $99 enrollment fee, participants can use the system to sign their own software.[19] However, the details of this program are not public and many questions remain, the most crucial being whether the key Microsoft is offering to third parties is the

---

Foundation, October 2011, available at http://www.linuxfoundation.org/publications/making-uefi-secure-boot-work-with-open-platforms (last visited July 2, 2012) (discussing how allowing end-users to enroll their own keys would ensure UEFI secure boot compatibility with linux-based operating systems).

14 David Goldman, *Microsoft unveils Surface tablet to rival iPad*, money.cnn.com, June 19, 2012, http://money.cnn.com/2012/06/18/technology/microsoft-windows-tablet/index.htm (last visited July 4, 2012).

15 Marius Oiaga, *With Windows 8, x86 CPUs Will Lose Ground to ARM*, Softpedia.com, Jul. 20, 2011, http://news.softpedia.com/news/With-Windows-8-x86-CPUs-Will-Lose-Ground-to-ARM-212497.shtml (last visited July 2, 2012).

16 *Id.*

17 Software Freedom Law Center, Comment in the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, at 9. *See also* Microsoft—Windows Logo'd Products List, https://sysdev.microsoft.com/en-US/Hardware/LPL/ProductList.aspx?m=7&g=s&cid=800&aqid=&fl=86win7 (last visited July 5, 2012) (listing thousands of products certified for compatibility with Windows 7, including dozens of PCs produced by each of the top 5 computing manufacturers—HP, Lenovo, Dell, Acer, and ASUS); s*ee also* Press Release, Gartner, Gartner Says Worldwide PC Shipments Grew 1.9 Percent in First Quarter of 2012, Apr. 11, 2012, available at http://www.gartner.com/it/page.jsp?id=1981717 (listing top PC vendors by units shipped).

18 Gregg Keizer, *FAQ: All about Windows RT, the OS behind a Microsoft tablet*, ComputerWorld.com, June 18, 2012, http://www.computerworld.com/s/article/9228202/FAQ_All_about_Windows_RT_the_OS_behind_a_Microsoft_tablet (last visited July 6, 2012).

19 Windows Dev Center – Hardware, available at https://sysdev.microsoft.com/en-US/Hardware/signup/.

same key it requires to be enrolled in certified hardware. There is no evidence that it will be; if it's any other key, the program may prove useless to third parties.

Even if it is the same key, the program will at best benefit traditional operating system vendors, leaving the majority of free and open source operating system users and developers without useful options. To date, only two free software operating system producers have announced plans to enroll in the Microsoft/Verisign program, each of them backed by large commercial vendors.[20] Most free software operating systems are produced by decentralized communities of volunteer programmers.[21] These communities don't operate like Microsoft, releasing a new operating system version ever several years. In addition to regular, stable releases, most of these projects make new versions of their operating systems available for download on a weekly or even daily basis.[22] This enables users who want access to the newest features to help the projects locate and remove bugs before a longer-term release is made. It would be extremely difficult for free software projects to maintain these rapid release cycles if they were required to submit each new version to the Microsoft/Verisign process for signing.

For some widely used free software operating systems, the program may not offer even a partial solution. The Gentoo Linux project, for example, does not distribute complete operating systems that can be signed. Rather, a Gentoo user compiles an operating system from source code according to a custom-defined configuration.[23] Thus, it may be impossible for individual users to install an operating system like Gentoo Linux on an ARM-based Windows device without enrolling in the Microsoft/Verisign program themselves.

For the same reason, operating system developers will be particularly harmed by Microsoft's policies. Developing or adapting an operating system for a device requires constantly making changes to the operating system and recompiling it from source code to binary code. For a device on which Secure Boot couldn't be disabled, a developer would have to submit each iteration (possibly several each day) for signing via the Microsoft/Verisign process before testing it on the device. This is unworkable for the hardiest of developers. Worse, it categorically excludes developers who can't afford the $99 registration fee or do not have access to a credit card; since many free and open source software developers are too young to qualify for a credit card or live in countries where they are not readily available, this is a significant barrier. For all of these reasons, after-market operating system development is only feasible on devices on which Secure Boot can be disabled or circumvented.

At best, Microsoft's Windows 8 certification requirements will put other operating system producers at a further disadvantage in the operating system market, by imposing an extra step—the Verisign signing

---

20 Lawrence Latif, *Canonical will use Intel's efilinux in Ubuntu for UEFI secure boot*, The Inquirer, June 25, 2012, http://www.theinquirer.net/inquirer/news/2186842/canonical-intels-efilinux-ubuntu-uefi-secure-boot (last visited July 2, 2012); *see also* Matthew Garrett, *Implementing UEFI Secure Boot in Fedora*, May 30, 2012, http://mjg59.dreamwidth.org/12368.html (discussing how Fedora will be signed by a Microsoft key in order to be functional in the UEFI secure boot environment).

21 Only three of the ten most popular free software operating systems have a corporate sponsor. *See* DistroWatch.com, *Top Ten Distributions*, http://distrowatch.com/dwres.php?resource=major (last visited July 5, 2012).

22 Debian, Weekly build, http://cdimage.debian.org/cdimage/weekly-builds/ (last visited July 5, 2012) (providing download links for weekly testing distributions of the Debian operating system); Arch Linux, Downloads, http://www.archlinux.org/download/ (last visited July 5, 2012) (providing download links for daily “snapshot” distributions of the Arch Linux operating system).

23 Gentoo, Gentoo Linux x86 Quick Install Guide, http://www.gentoo.org/doc/en/gentoo-x86-quickinstall.xml) (last visited July 5, 2012).

process—on competitors wishing to enter the market. At worst, the requirements will keep competing operating systems off of ARM-based Windows devices entirely, by ensuring that only Microsoft operating systems can be installed on them, no matter what competing producers or device owners do.

I hope this addresses your question adequately; please feel free to contact me if you have any further questions.

Very truly yours,

Aaron Williamson
Senior Staff Counsel
Software Freedom Law Center

CC: Jesse Feder, Business Software Alliance
Steven Metalitz, Mitchell, Silberberg & Knupp LLP
Brett Wynkoop & Jay Sulzberger, New Yorkers for Fair Use