**1. What is signing? What is a certificate, where does it come from and how does it work with a device driver?**

Signing is used to verify the security and integrity of code, and to “verify the identity of the vendor”. A certificate is a set of data that identifies a publisher. It is issued by a “Certification Authority” who has been proofed as being reliable and having integrity, and can be trusted to correctly issue certificates. The “signature” consists of two keys. The private and public keys. The private is embedded in the Driver, most commonly in the package’s catalog file, while the public key is used to verify the signature.

Source:

<http://msdn.microsoft.com/en-us/library/windows/hardware/ff543743%28v=vs.85%29.aspx>

-By the Guy(s) who wrote MSDN

**2a. How does linux handle device driver security?**

For a software provider who wants reliable continued support by Linux, the source code is scrutinized through a public peer review before it is accepted into the mainline Kernel. Out-of-mainline open source

drivers require constant development and upgrades, similar to Windows. Also, a hardware provider can have free driver development provided by a Linux Kernel Maintainer, which also adds security. But, I haven't seen anything that doesn't say that someone can make a malicious driver and install it, or sell

hardware with malicious drivers. It would be difficult as Kernel APIs change often, but is possible.

Source:

<http://www.linuxfoundation.org/collaborate/workgroups/technical-advisory-board-tab/linuxdevicedrivermodel>

-By Dan Kohn, #2 person at Linux Foundation. <http://www.dankohn.com/bio.html>

**2b. How does Mac handle device driver security?**

Mach-the protected Memory aspect

Apple has standard libraries for things like mice or keyboards. If these things don’t work, or a custom piece of hardware needs a custom driver, Apple provides an “I/O Kit” designed to create drives with a restricted subset of C++, limiting what can be done with the drivers. By providing this restricted set of capabilities, creating malicious driver code is extremely difficult. As added protection, a feature called “Mach” protects memory, immediately preventing software from accessing memory they are not permitted to use.

Source:

<https://developer.apple.com/library/ios/documentation/miscellaneous/conceptual/iphoneostechoverview/coreoslayer/coreoslayer.html>

<https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/OSX_Technology_Overview/SystemTechnology/SystemTechnology.html#//apple_ref/doc/uid/TP40001067-CH207-TPXREF172>

-By Apple Inc.