

05-17-2020, Beginners/Mac Basics SIG – SilentKnight Demo

Note: This discussion is based on macOS, 10.14.6 (Mojave). Some illustrations may differ when using other versions of macOS or OS X. Most illustrations are from screenshots on my iMac or MacBook Pro.

This Mac Basics presentation will take a different focus. I'll discuss a special Mac system firmware and software update utility known as **SilentKnight**. It's one of many freeware utilities by developer Howard Oakley.

I follow Howard's website (<https://eclecticlight.co>) and recently read an article about some Macs not getting firmware updates when they should. Here's the link: <https://eclecticlight.co/2020/03/30/some-macs-dont-update-their-firmware-when-they-should/>

As his article explains:

"Keeping your Mac's firmware up to date is important. Old versions can have incompatibilities with more recent releases of macOS (or Security Updates), and may contain security vulnerabilities and other bugs. When everything works well, you shouldn't have to worry about any of this. You let Software Update download and install macOS updates, and whenever new firmware is released for your particular model, that gets updated too.

"Occasionally, though, updaters don't install the firmware updates they're expected to. When this happens once, it's no great disaster, and applying the update a second time – perhaps in the 'Combo' updater – often does the trick. It's not as convenient, perhaps, as being able to run a separate firmware installer, but works."

Software Security Updates

The macOS includes a number of security software features of which we're generally aware but that need periodic updating. For example, there's **XProtect** that checks apps and some other files to see if they are malicious. You may know about **Gatekeeper** which checks the authenticity of apps and some other items. Also, there's the **Malware Removal Tool (MRT)** to detect and remove malware.

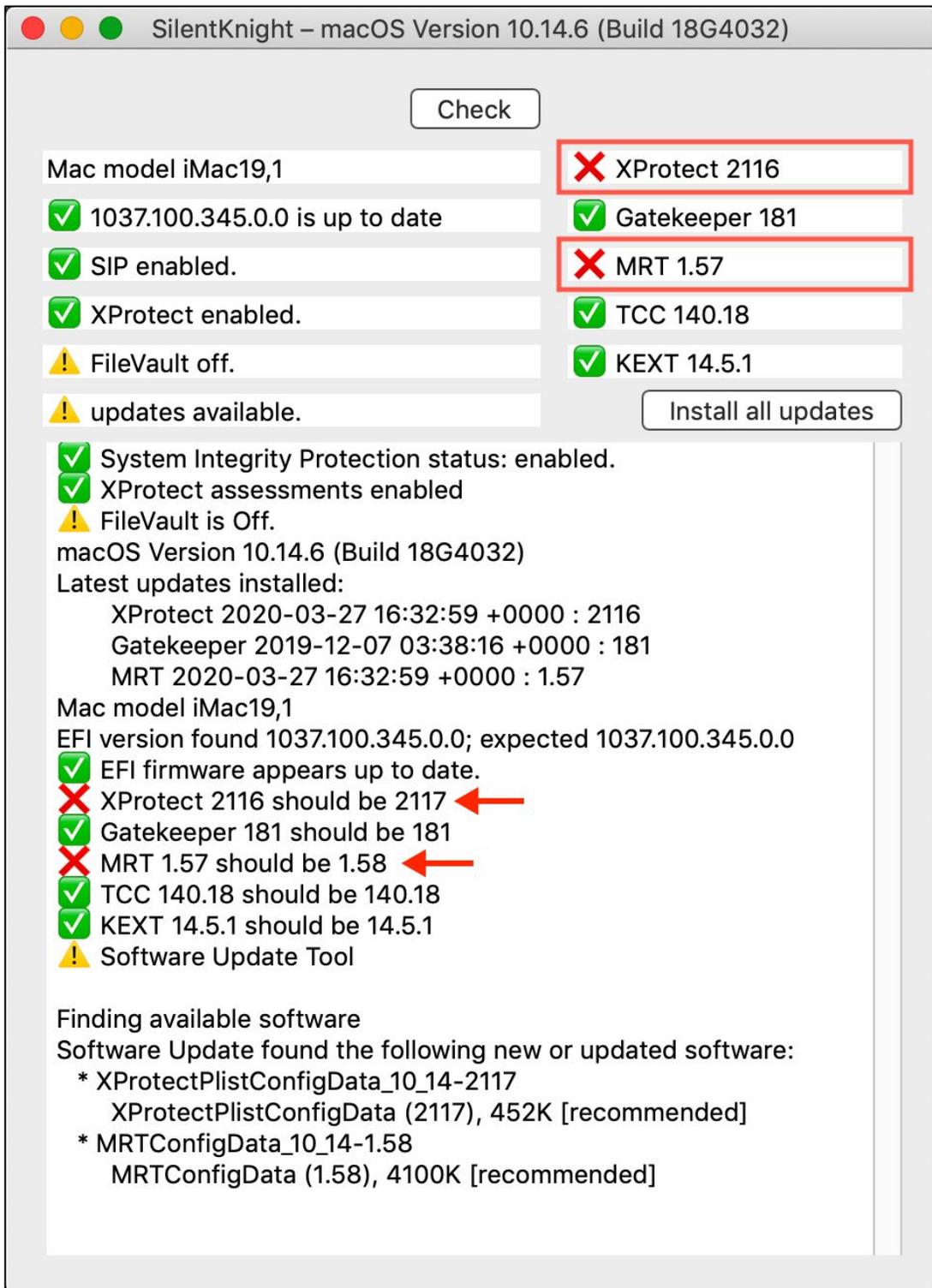
Recent Experience. The article referred to recent macOS updates for firmware and MRT (Malware Removal Tool). I checked for these updates using Apple's **System Information** utility (more on this later) and found that they had not been installed.

I downloaded SilentKnight, and when I ran it (**Check** button), the report confirmed that my iMac hadn't been updated. I then used SilentKnight's **Install all updates** button to download and install all updates—and after several minutes, nothing happened (downloads took too much time and timed out)! It turned out that my VPN was the culprit. When I turned it off, the updates were downloaded, and all firmware and software updates were successfully installed. Interestingly, subsequent updates with my VPN turned on ran without any problems. So, your mileage may vary.

SilentKnight

SilentKnight 1.0 was first issued in July 2019 as a comprehensive replacement for an earlier version of a utility to check EFI firmware, security settings, and security updates automatically. It's now up to version 1.6.

Here's what it looked like after I ran it on my iMac back on April 4, 2020:



SilentKnight Report

05-17-2020, Beginners/Mac Basics SIG – SilentKnight Demo

SilentKnight’s support documentation explains the symbols used in a report:

“Those considered to be up to date are prefaced by the  symbol to indicate a ‘pass.’ Those considered to merit further checking or action on your part are prefaced by . Those which appear to be out of date or worth attending to are prefaced by . Items updated in the last 24 hours are shown with a  by them.”

As you can see, there were two software updates (**XProtect** and **MRT**) that hadn’t been installed. This was verified by running the **System Information** utility.

System Information Utility. This is located in the **Utilities** folder. It can also be accessed by selecting **About This Mac** under the Apple menu and then clicking on the **System Report...** button in the resulting window:



“About This Mac” Window

After running the System Information utility and selecting **Installations** under the **Software** section, here’s a screenshot of the System Information report (Software section, Installations) for MRTConfigData:

| | | | |
|------------------------|---|-----------|-------------------|
| Microsoft Word for Mac | | 3rd Party | 3/14/20, 10:01 PM |
| MRTConfigData | 1.49 | Apple | 12/6/19, 9:38 PM |
| MRTConfigData | 1.50 | Apple | 12/6/19, 9:39 PM |
| MRTConfigData | 1.51 | Apple | 12/22/19, 9:52 PM |
| MRTConfigData | 1.52 | Apple | 1/8/20, 3:04 AM |
| MRTConfigData | 1.53 | Apple | 1/22/20, 3:49 PM |
| MRTConfigData | 1.54 | Apple | 2/5/20, 11:42 PM |
| MRTConfigData | 1.55 | Apple | 2/21/20, 3:05 PM |
| MRTConfigData |  1.57 | Apple | 3/27/20, 11:32 AM |
| Numbers | 6.0 | Apple | 12/22/19, 8:51 PM |

System Information Utility Report Software Section (Installations, MRTConfigData)

05-17-2020, Beginners/Mac Basics SIG – SilentKnight Demo

As you can see, the latest version of MRTConfigData that has been installed is 1.57. However, SilentKnight reported that it should be version 1.58.

Reference Information: SilentKnight's support information explains the following about XProtect and MRT:

XProtect. "XProtect is responsible for checking apps and some other files for tell-tale signatures indicating that they are malicious. It should always be enabled: if it's reported in its box at the left to be disabled, contact Apple support as a matter of urgency, as your Mac may have already been attacked by malware. Apple infrequently updates its signature and malware definitions using a pushed security update.

"To determine the current version of XProtect data files installed, SilentKnight obtains the version number of /System/Library/CoreServices/XProtect.bundle (in 10.15, /Library/Apple/System/Library/CoreServices/XProtect.bundle).

"When updated, the new data takes immediate effect. You don't need to restart your Mac."

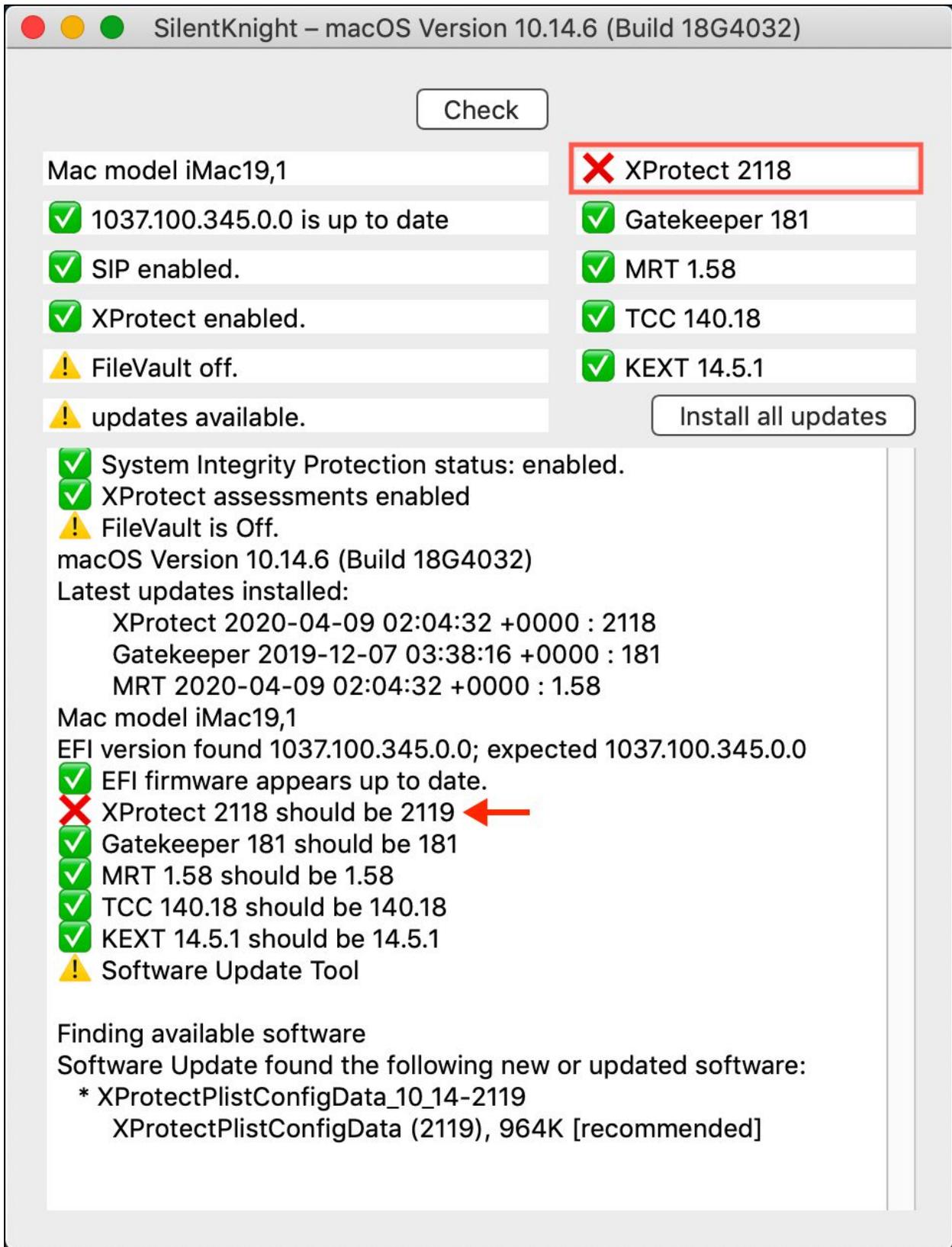
MRT. "If the system detects that malware is present, it calls on the Malware Removal Tool MRT to do the job. Although this hasn't been updated very often over the last year or so, it remains a central part of macOS system security, and Apple does still maintain it.

"The app's data are contained within the app at System/Library/CoreServices/MRT.app (in 10.15 Library/Apple/System/Library/CoreServices/MRT.app), and the version given here is that of that app.

"When updated, MRT may be run automatically to check for any malware which needs to be removed. As MRT is normally only run after starting up, you may prefer to restart after updating, to ensure that the new version scans your Mac promptly. It's also possible to run MRT manually, but that doesn't appear as reliable as restarting."

Clicking on SilentKnight's **Install all updates** button did indeed install the required updates. Unfortunately, I didn't take a screenshot of SilentKnight after updating to show the result.

April 16th Update. Not to worry, a recent notice on the Eclectic Light website noted that XProtect had been updated on April 16th to version 2119. SilentKnight found that XProtect on my iMac was at version 2118 when it should have been 2119. (See the image on the next page.)

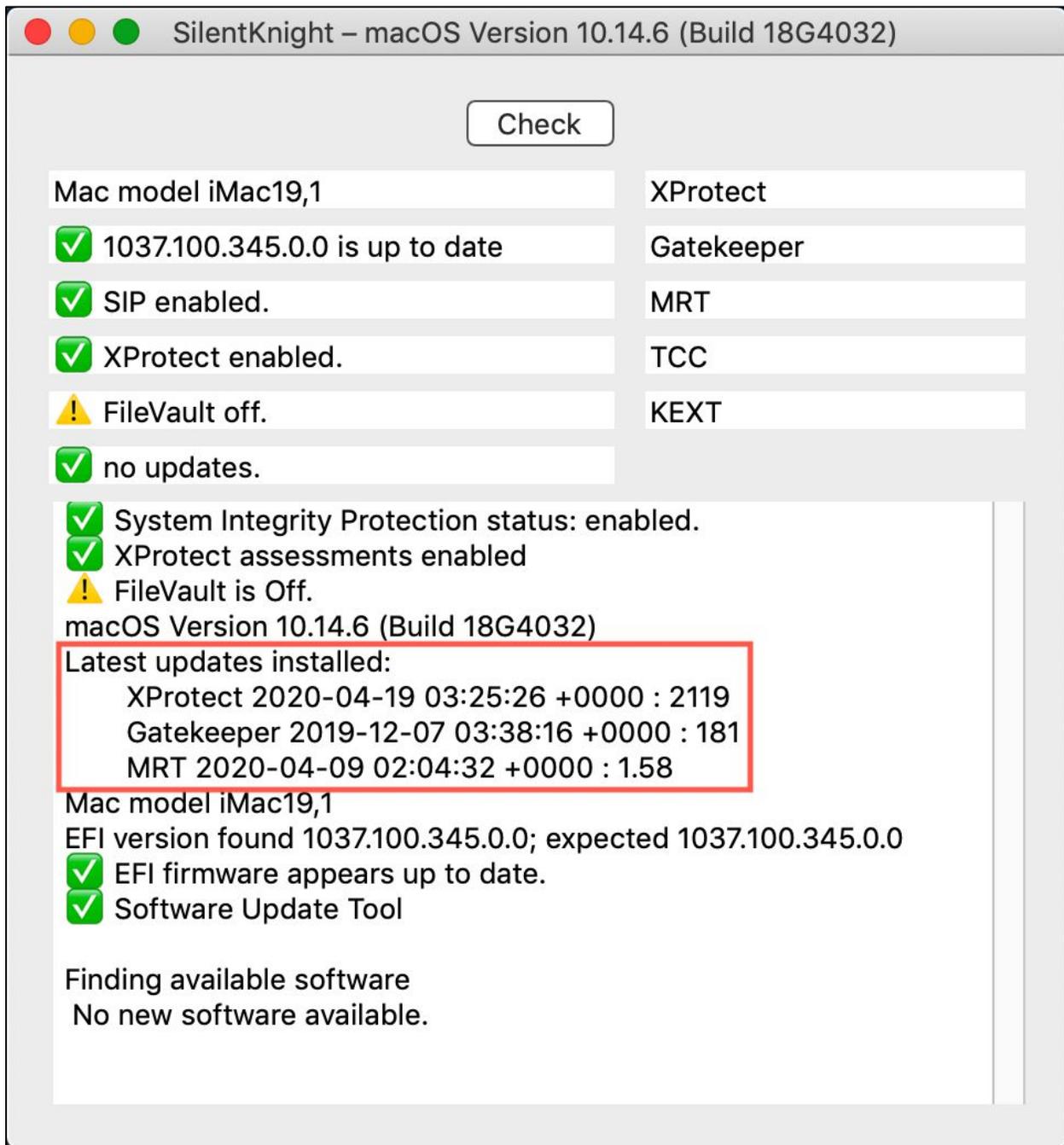


SilentKnight Report

Running SilentKnight installed the required update. The SilentKnight window expanded to show the downloaded information. (See the image on the next page.)

05-17-2020, Beginners/Mac Basics SIG – SilentKnight Demo

Running SilentKnight again confirmed that the update had been installed and that all firmware and software was up to date:



SilentKnight Report – Files Were Updated

May 14th Update. I ran SilentKnight again on May 14th to check on the status of my system data files and security updates and noticed that there were additional updates to XProtect (version 2121) and MRT (1.60). After updating, everything looked good. (See the image on the next page.)

05-17-2020, Beginners/Mac Basics SIG – SilentKnight Demo

Mac model iMac19,1

1037.100.345.0.0 is up to date

SIP enabled.

XProtect enabled.

FileVault off.

no updates.

XProtect 2121

Gatekeeper 181

MRT 1.60

TCC 140.18

KEXT 14.5.1

Mac model iMac19,1
EFI version found 1037.100.345.0.0; expected 1037.100.345.0.0

- EFI firmware appears up to date.
- XProtect 2121 should be 2121
- Gatekeeper 181 should be 181
- MRT 1.60 should be 1.60
- TCC 140.18 should be 140.18
- KEXT 14.5.1 should be 14.5.1
- System Integrity Protection status: enabled.
- XProtect assessments enabled
- FileVault is Off.

macOS Version 10.14.6 (Build 18G4032)

Latest updates installed:

- XProtect 2020-05-14 23:37:42 +0000 : 2121
- Gatekeeper 2019-12-07 03:38:16 +0000 : 181
- MRT 2020-05-14 23:37:42 +0000 : 1.60
- Software Update Tool

SilentKnight Report – Everything Looks Good

Why the Need for Updates?

Online updates obviously only occur when your Mac is online, but I use mine every day. It turned out that my settings in the **Software Update** system preference were likely the reason why various updates weren't being installed:



Software Update System Preference

You'll notice that I haven't installed macOS Catalina yet. However, I also haven't checked the box for **Automatically keep my Mac up to date** because I wanted to decide when to have updates installed.

Clicking on the **Advanced...** button reveals additional options for automatically keeping Mac software up to date:



Software Update System Preference – Advanced Options

The Advanced options allow the user to tailor how various components of the macOS are kept up to date.

Note: It's not possible to check any of the options without first previously selecting **Automatically keep my Mac up to date** checkbox.

As you can see, I hadn't checked any of them, especially the last one (**Install system data files and security updates**). Had this been checked, the system data files and security updates would have been installed. [Thanks, Jim Macak, for discussing this with me.]

I've now allowed future updates to be installed:



Software Update System Preference – Advanced Options (Updated)

As you can see from the graphic above, I'm now allowing all future updates to be installed with one exception: macOS updates. I'm presently using macOS 10.14.6 (Mojave) because I'm still not satisfied with the reliability of macOS 10.15.x (Catalina). Version 10.15.4 was current as of this presentation. We'll see what 10.15.5 brings.

Future Use of SilentKnight. I still plan to follow Howard's website and use his SilentKnight utility to periodically verify that all required system data files and security updates have been installed. It never hurts to double check on this.

Summary

Although infrequent, it's possible that your Mac might fall behind on System Security Software Updates. Your Mac needs to be online for these to be installed, and this happens "behind the scene." If your Mac hasn't been online in a while, a needed update may not get installed.

Perhaps you may have a System Preference setting that interferes with updates getting installed. Sometimes, there's just no clear reason why they don't get installed.

Developer Howard Oakley has a free software update utility at his website (<https://eclecticlight.co>) known as **SilentKnight** that nicely solves this problem. When run, it checks to make sure that you Mac has all the latest system security software updates. Its report shows which ones are out of date and then provides a means to update them.

Next Presentation

For the next presentation, we'll take a look another macOS feature.

Have a favorite Mac Tip or utility? Please feel free to pass it along, and I'll see if I can work it into a future presentation.

If you have any suggestions for presentation topics, including macOS utilities, please contact me at slp4668@gmail.com.

-Steve Parker

Credits:

<https://eclecticlight.co/2020/03/30/some-macs-dont-update-their-firmware-when-they-should/>

<https://eclecticlight.co/2019/10/30/how-can-security-data-get-so-out-of-date/>