

printout

Keystone MacCentral Macintosh Users Group ♦ <http://www.keystonemac.com>

November Meeting

We plan on using a new adapter — that allows better access to the projector — to demo iOS apps from iPhone and iPads. Wendy will talk about making videos. And Dennis will continue his exploration of interesting tidbits that he runs across. ☛

Meet us at

Bethany Village Retirement Center

Education Room

5225 Wilson Lane, Mechanicsburg, PA 17055

Tuesday, November 21st 2017 6:30 p.m.

Attendance is free and open to all interested persons.

Contents

November Meeting	1
A Prairie HomeKit Companion: HomeKit Security Provides	
Peace of Mind by Julio Ojeda-Zapata	3 - 8
11 Things You Should Know about iOS 11 by Josh Centers	8 - 12
macOS 10.13 High Sierra Now Available:	
When Should You Upgrade? by Adam C. Engst	12 - 13
Wi-Fi Security Flaw Not As Bad As It's KRACKed Up To Be	
by Glenn Fleishman	13 - 15
Software Review	16

Keystone MacCentral is a not-for-profit group of Macintosh enthusiasts who generally meet the third Tuesday of every month to exchange information, participate in question-and-answer sessions, view product demonstrations, and obtain resource materials that will help them get the most out of their computer systems. Meetings are free and open to the public. The *Keystone MacCentral printout* is the official newsletter of Keystone MacCentral and an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by any for-profit organization, including Apple Inc. Copyright © 2017, Keystone MacCentral, 310 Somerset Drive, Shiresmanstown, PA 17011.

Nonprofit user groups may reproduce articles from the Printout only if the copyright notice is included, the articles have not been edited, are clearly attributed to the original author and to the Keystone MacCentral Printout, and a copy of the publication is mailed to the editor of this newsletter.

The opinions, statements, positions, and views stated herein are those of the author(s) or publisher and are not intended to be the opinions, statements, positions, or views of Apple, Inc.

Throughout this publication, trademarked names are used. Rather than include a trademark symbol in every occurrence of a trademarked name, we are using the trademarked names only for editorial purposes and to the benefit of the trademark owner with no intent of trademark infringement.

Board of Directors

President

Linda J Cober

Recorder

Wendy Adams

Treasurer

Tim Sullivan

Program Director

Dennis McMahon

Membership Chair

Eric Adams

Correspondence Secretary

Sandra Cober

Newsletter Editor

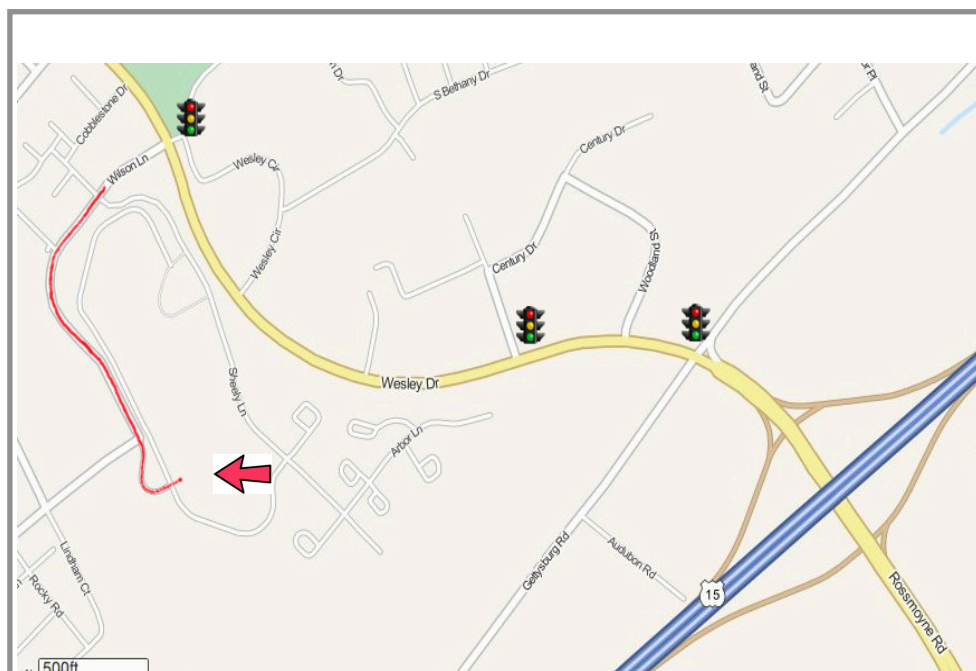
Tim Sullivan

Industry Liaison

Eric Adams

Web Master

Tom Bank II



Keystone MacCentral Essentials

Meeting Place

Bethany Village West
Maplewood Assisted Living (Bld 21)
5225 Wilson Lane
Mechanicsburg, PA 17055

Web Site

<http://www.keystonemac.com>

Mailing Address

310 Somerset Drive
Shiresmanstown, PA 17011

A Prairie HomeKit Companion: HomeKit Security Provides Peace of Mind

I am a bit paranoid by nature, and those tendencies dial up to 11 when I travel. Although I have never experienced a burglary, I'm convinced intruders will clean out the house sooner or later.

So before a recent trip, I took a major precautionary measure to assuage my simmering insecurities. I set up Internet-connected video cameras, motion sensors, and smart outlets so I could control and monitor my home from afar.

This was an opportunity to play with Apple's HomeKit technology, which lets iOS devices manage a variety of home-automation products from other companies. (Be sure to read earlier installments in this "[A Prairie HomeKit Companion](#)" series, a name I love since I live in [Lake Wobegon](#) country, aka Minnesota.)

Unable to achieve all my monitoring goals with the HomeKit devices available to me, though, I searched farther afield for other home-security gear that also works with Apple devices – albeit outside the HomeKit ecosystem.

I ended up with a motley assortment of security gadgets and related apps, but it served my needs nicely once I had everything set up. My gadget collection went a long way to soothing my jitters when I was away, and getting it working was a lot of fun, too.

Of course, I had to make this happen on my own – which is a far cry from hiring a security company to install a comparable system while you relax with a latte.

The latter course is tempting. As a Comcast subscriber, it would be easy to have [Xfinity Home Security](#) added to my cable, Internet, and phone bill. As an AT&T wireless subscriber, it would also be simple to sign up for AT&T's [Digital Life](#) security services. There are numerous other home-security service providers for hire.

But I'm a geek who loves to tinker and a cheapskate who wants to avoid monthly fees. I didn't find the necessary setup tasks to be onerous, so the do-it-yourself approach is worth considering even if you're not a penny-pinching tech dweeb like me.

A variety of companies stand ready to assist. Verizon Wireless, for example, doesn't offer home-security services like those of AT&T, but it does sell a curated line of third-party [security products](#). Verizon loaned me the Belkin and Canary products reviewed here.

Security Goals — HomeKit features rule-composing capabilities and other automation features, but I lacked the time and patience to bother with most of them amid my frantic travel prep. I had a few simple goals:

- I wanted to turn lights on and off manually whenever I liked by picking up my iPhone and tapping on-screen buttons. I hoped this would fool wannabe burglars into thinking my house was occupied.
- I craved the ability to peer into my home's common areas, like the living room and kitchen, mostly to set my mind at ease that nothing was amiss.
- I wanted my iPhone and Apple Watch to alert me if motion was detected in the common areas and other parts of my house.

First Up, HomeKit — I initially hoped my security system could rely only on HomeKit-compatible devices. I largely, if not entirely, achieved that goal.

In my experiments with HomeKit products from a variety of vendors, I had the best luck with [Elgato](#) equipment. This isn't surprising: Elgato's devices have never let me down in any major way.

Elgato has collected its growing assortment of HomeKit devices under the Eve brand. They include environmental sensors, smart outlets, light switches, and motion detectors. [Elgato has announced](#) even more Eve gizmos, like smart door locks, smoke detectors, window-movement sensors, and even irrigation controllers and thermostatic radiator valves.

For my custom security system, I focused on the [Eve Energy](#) smart outlet and [Eve Motion](#) sensor, which cost \$49.95 each. Both have the virtue of being deployable without time-wasting installation. Devices that require drilling and so on for setup are a hard sell for my Luddite wife, who doesn't want an endless succession of shiny doodads eating their way into our walls.

Both Elgato products easily integrated into my HomeKit network via app scanning of numeric codes on the gizmos (see "[A Prairie HomeKit Companion: Setting Up Accessories and Rooms](#)," 16 January 2017).

I installed the Eve Energy devices into electrical outlets throughout my home, with lamps plugged into each one and turned on.

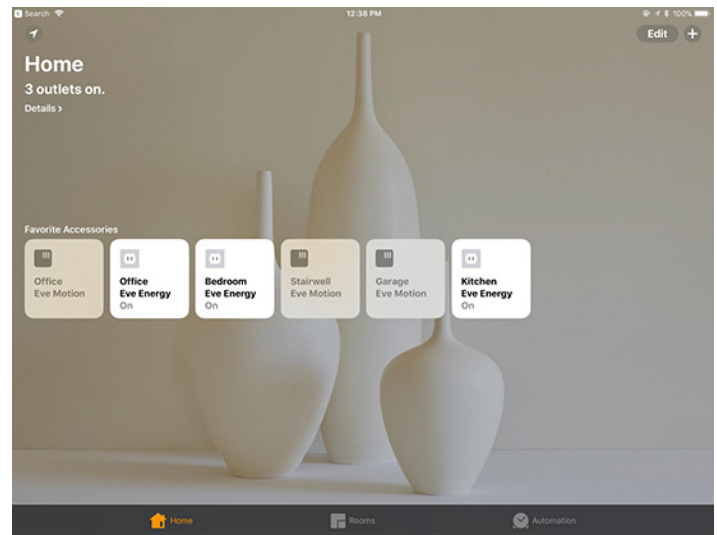


I then deployed the battery-powered Eve Motion sensors in key spots: my garage beside a door that could be a burglar's entry point; at the top of a staircase that intruders would use to infiltrate second-floor rooms; and in my home-office [Fortress of Solitude](#), or, if you are more of a Marvel persuasion, [Sanctum Sanctorum](#).

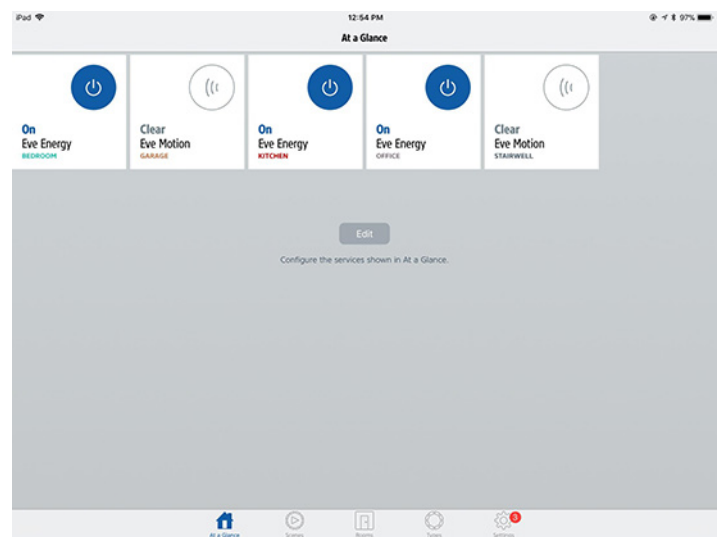


After just a bit of fiddling in Apple's Home app on my iPhone, I was able to set up buttons corresponding to each of the devices as favorite accessories on the main screen (see "[A Prairie HomeKit Companion: Setting Up Accessories and Rooms](#)," 16 January 2017). This had two purposes.

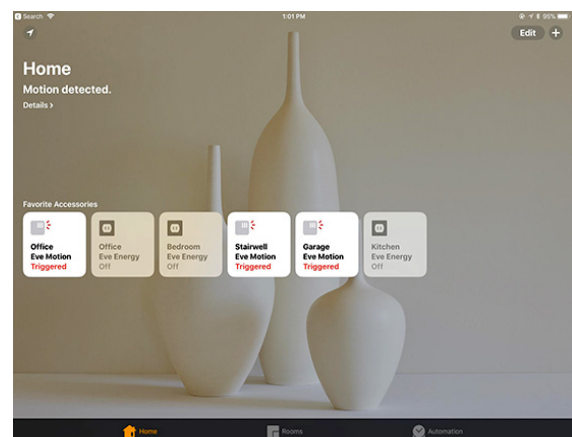
The Eve Energy buttons provided a handy way to turn the lamps on and off in the Home app. This worked at my home via Wi-Fi, since all the gadgetry used the same wireless network, and also from afar, since I had set up my Apple TV as a HomeKit hub for remote access (see "[A Prairie HomeKit Companion: Automating Your Home](#)," 10 February 2017).



I could also accomplish this via Elgato's [Eve app](#) (see "[A Prairie HomeKit Companion: The Elgato Eve Room](#)," 19 June 2017), but I prefer the Home app's cleaner, more elegant presentation.



The Eve Motion buttons in the Home app had a different purpose: alerting me when motion was detected. I was certain to miss such visual cues since I wouldn't constantly be staring at the Home app, of course, so I switched on alerts. That involved flipping a software toggle in the Home app for each sensor, and checking in Settings > Notifications that notifications for the Home app were enabled.



Once I'd done all this, the sensors began to send alerts to my iPhone – and, by extension, my Apple Watch. No burglar triggered them, but I did verify that they worked reliably when a neighbor popped in a couple of times to handle a few chores during my absence.

Elgato's devices performed spotlessly in every way. I emphasize this because it was not the case with some other HomeKit devices – including smart outlets and motion sensors – from other companies. Difficulties I encountered with other devices included set-up snafus as well as show-stopping failures during testing.

I won't name the other vendors since I don't feel I did my due diligence in trying to resolve technical issues amid my rush to prepare for my journey (even though, in some cases, I burned hours trying to figure out what was wrong). At the same time, I wanted confidence in the gear I had tasked with protecting my kingdom, and only Elgato's devices provided that for me.

Another Smart Outlet – For giggles, I threw in another smart outlet that is not — at least right now — compatible with HomeKit but has reasonably good Apple compatibility. Belkin's \$49.99 [Insight Smart Plug](#), part of its Wemo line of home-automation products, works much like Eve Energy.



Setup was straightforward, starting by detecting a Wi-Fi signal from the plug and then completing the process in the iOS [Wemo app](#). From then on, the Insight Smart Plug performed splendidly.

In the Wemo app, an image of the plug had a round power-like button next to it, and tapping it never failed to turn a bedside lamp on or off. This worked at home on Wi-Fi and from afar, with no Apple TV-like hub device required.



The Insight Smart Plug now functions within a couple of home-control ecosystems: [Amazon Echo, with its Alexa assistant](#) and [Google Home, with Google Assistant](#). You also can link it to the [IFTTT](#) – If This, Then That – automation service.

So what about HomeKit? Belkin, which has been flirting with the Apple technology for a couple of years with no follow-through, finally said in May 2017 that it would release a [Wemo Bridge](#) to bring its Wemo devices into the HomeKit fold. It's a somewhat awkward arrangement given that you have to deploy extra hardware to access existing Wemo devices via HomeKit, but it's better than nothing. The Wemo Bridge is due before the end of the year, but Belkin hasn't announced pricing yet.



Adding Security Cameras — Internet-accessible security cameras were another must-have item on my home-security checklist, and here is where I ran into difficulty staying within the HomeKit ecosystem.

There just aren't many HomeKit-compatible video cameras out there. In fact, on Apple's [HomeKit accessory page](#), there's only one — D-Link's \$149.95 [Omna 180 Cam HD](#). I repeatedly tried and failed to get an Omna review unit, so I can't speak to its reliability.

So I had to venture beyond the HomeKit universe for a security camera. There are tons of options, and I narrowed my search to cameras from Canary and Netgear. Apple compatibility is reasonably good in both cases, since both companies provide iOS apps. Canary even extends this to the Apple Watch.

Netgear sent me a couple of its [Arlo Pro](#) security cameras, which worked out nicely. The compact cameras are cordless, working off rechargeable batteries. They are weatherproof and can be used indoors or outdoors; I opted for indoor use so I wouldn't have to spend time installing them on the side of my house while simultaneously annoying my wife.



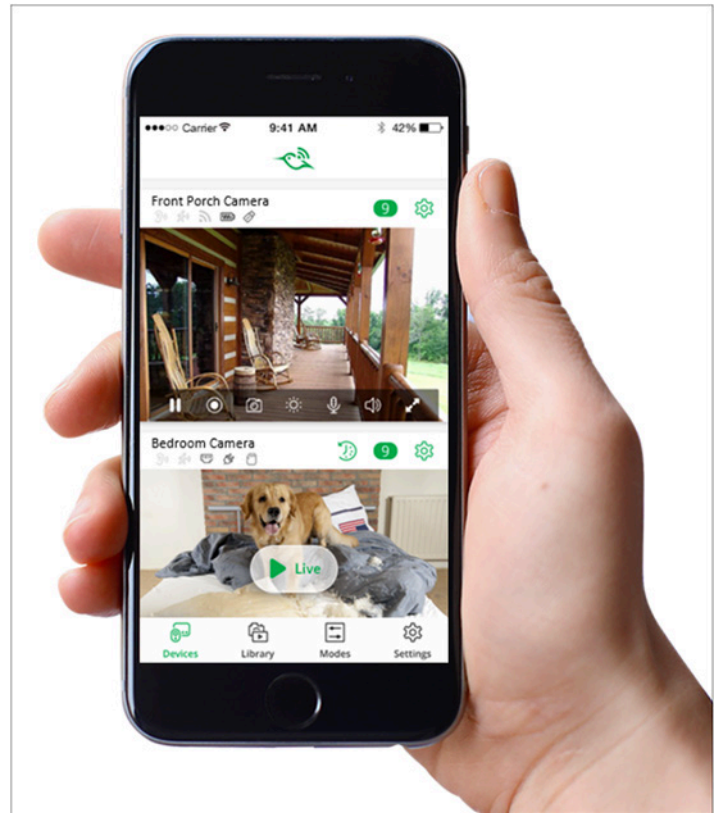
My setup was the height of simplicity — I placed one on each of my home's stairwells, with one camera pointed at the back door and another aimed at the front door. I hoped that anyone who came in would trip the cameras' motion sensors — nothing gets past these things — and trigger the recording of a video snippet to document the incident.

You can set the duration of videos between 10 seconds and 5 minutes once motion sensing is triggered, or you can set the camera to record only as long as motion is being sensed. Netgear offers free cloud storage for recent recordings (going back a week), unlike other camera vendors that charge fees for online archiving.

The camera also has a siren that can be activated to spook burglars. I had to be careful when testing this feature; at 100+ decibels, it's so loud that it can damage hearing.

The [Arlo app](#) is nicely designed, with a live-feed page (tap to see live video), a library showing motion events in reverse chronological order, and a "mode" section to manually arm or disarm the cameras, put them on a

schedule, or set up geofencing so behavior changes depending on the whereabouts of authorized users. I did not bother with most of these features; I just wanted to be alerted via my Apple Watch about motion events with corresponding mini-recordings — and I was.



The Arlo cameras have a few annoying characteristics. Much like the forthcoming Wemo Bridge, they require the use of a large hub-like device that connects physically to your broadband router. Such an approach isn't a big deal but further clutters the already crowded space around my router.



(Note that Netgear sells the Arlo cameras as kits, with two or more of the cameras along with the hub. I tested a \$419.99 kit with two cameras along with the hub.)

More irksome is the Arlo camera's inability to charge, via its Micro-USB port, with anything but the power adapter Netgear provides. I cursed at one point when I could not find that charger and tried a bunch of others; all were summarily rejected. Not cool, Netgear.

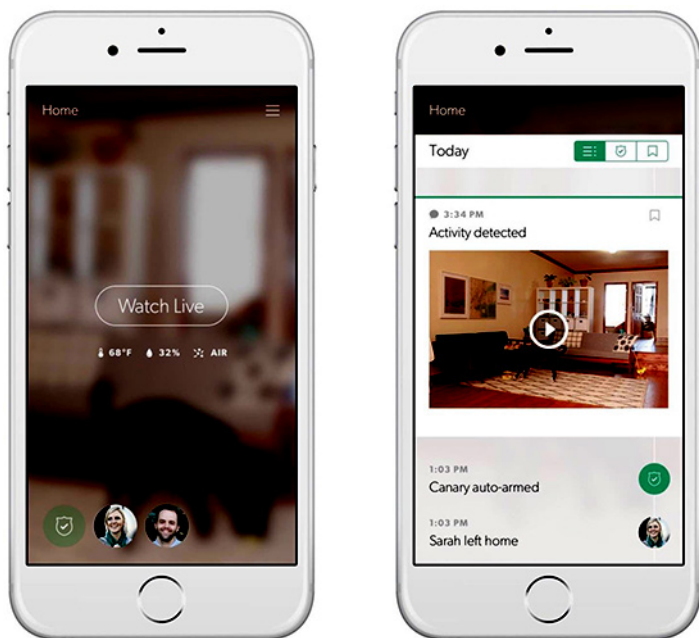
The company has been rumored to be working on HomeKit support but had nothing to announce as I wrote this.

Canary has a different approach to home-video security. Its flagship product, the \$149 [Canary](#), is a stylish, self-contained cylinder that sits on a bookshelf or other flat surface to provide a wide-angle view of your home's interior (the Arlo Pro's view is a bit tighter).



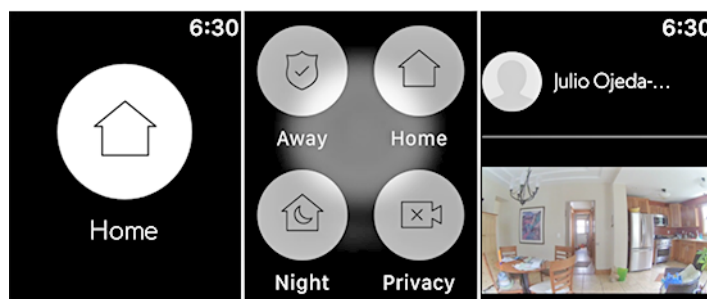
Like the Arlo, the Canary detects motion and records corresponding bits of video. By default, these clips last only 10 seconds and go back only a day, but for \$10 a month, you can access full-length videos going back 30 days. The Canary also has a 90+ decibel siren. Unlike the Arlo, it monitors air quality, humidity, and temperature, so if there is flooding or a fire, it can alert you.

The [Canary's iOS app](#) is a beauty. The camera's viewpoint is stylishly blurred with an overlaid Watch Live button to bring the view into focus. If you have more than one camera, you can swipe right or left to go from unit to unit. Buttons along the bottom let you set modes (Away, Home, and Night) to alter its behavior based on whereabouts or sleeping status of authorized users. You can easily add more authorized users.



The Canary's Apple Watch app has one primary purpose, mode switching, which includes a privacy mode if you want to suspend surveillance for a time. The Apple Watch

app is attractive, with a single big white button showing the current mode (force-press for a four-button grid to switch modes). You can also scroll down to see recent motion events, shown as thumbnails.



Canary also has a pretty good Apple TV app, but that obviously was of no use to me while I was traveling.

Of course, using both the Arlo and Canary for indoor monitoring was redundant. If I were to do this all over, I would put the Arlos outside, one in the front of my house, and one over the back patio, while relying on the Canary for indoor monitoring.

Canary also has an Arlo equivalent, the \$179 [Canary Flex](#), which can be deployed outdoors as well as indoors. I had a Flex unit to test, as well, and I placed it in the living room, with the primary Canary unit in my kitchen. In hindsight, I should have used the Flex outside along with the Arlos for comprehensive outdoor surveillance.



As for HomeKit integration, [Canary has confirmed it is coming](#) but won't be supported with existing products. The company has announced a Canary Plus – essentially a successor to its current Canary product – that will support HomeKit. However, Canary says that once you have at least one Canary Plus deployed, any older Canary devices on the same network will be HomeKit-ready by extension.

The Upshot – My grand home-security experiment was a success in granting me the peace of mind that had eluded me on past trips, when I fretted about potential home break-ins.

In fact, I so enjoyed deploying and using the security devices that I almost wanted a burglary attempt to have transpired so I could have responded from a distance. It would certainly have made for a dramatic article.

To fantasize for a second: How would I have responded to a break-in? For starters, I would have been gleeful in activating the ridiculously loud sirens on the Canary and the Arlo cameras, which would have likely sufficed to scare away intruders. As an alternative, I could have given them a severe talking-to via speakers built into the cameras. In addition, the Canary camera has built-in options to summon police, paramedics, and firefighter crews, so sending the cops to my house would have been a cinch.

Realistically, the entire experience probably would have been pretty scary, though, and we likely would have worried about it afterward, so I guess I'm glad it didn't happen.

My only big regret during this home-security experiment was not being able to stay within HomeKit, as I had intended.

Were I to do a version of this article a year from now, though, it would likely read differently. Suppliers of home-automation products seem to be edging slowly but surely toward HomeKit.

Indeed, as I was putting the finishing touches on this article, Logitech [announced](#) HomeKit support via a firmware update for the [Circle 2](#), its compact, corded security camera for use indoors and outdoors. Logitech sent me one to try out, and I am putting it through its paces now.



At the same time, Apple is reportedly making it easier for device makers to [add HomeKit compatibility](#) (see "[A Prairie HomeKit Companion: What's Coming in iOS 11](#)," 7 July 2017). This is all terrific news as Apple goes up against the likes of Amazon and Google in the home-automation space. 📺

by Josh Centers

11 Things You Should Know about iOS 11

iOS 11 is now available, either via iTunes or Settings > General > Software Update. I've spent the last few months documenting it for "[Take Control of iOS 11](#)" — which we've updated to version 1.1 to coincide with the official iOS 11 launch.

If you've been following TidBITS, you've probably seen articles we've been writing about iOS 11, such as "[A Prairie HomeKit Companion: What's Coming in iOS 11](#)" (7 July 2017), "[ARKit: Augmented Reality for More Than Gaming](#)" (28 July 2017), and "[iOS 11 to Bring Do Not Disturb While Driving](#)" (21 August 2017).

Those articles hopefully whetted your appetite for iOS 11, but before you pull the trigger, here are 11 things you need to know.

#1: Your Favorite Apps May Not Work -- Don't say you haven't been warned! Adam Engst suggested this might happen in "[Apple to Deprecate 32-bit iOS Apps](#)," (15 May 2017) and Marc Zeedar told you it would in "[The Problem With Abandoned Apps](#)," (17 July 2017): apps that have not been updated to run in 64-bit mode remain on your device, but you'll receive an error message if you try to launch them.

If you're running iOS 10.3.1 or later, check Settings > General > About > Applications to see a list of which apps on your device, if any, will not run under iOS 11. If you have some important ones on that list, see if there's an

update available, likely as a new app. If not, hold off on iOS 11 until you figure out a solution.

But you don't have to worry about the [TidBITS News](#) app! Thanks to Matt Neuburg, it should keep working for years to come (see "[TidBITS News Shows How an Old 32-bit iOS App Becomes 64-bit](#)," 16 May 2017).

#2: Some Features Are Missing -- Three major features that Apple promised for iOS 11 at WWDC are missing: Messages in iCloud, person-to-person Apple Pay, and AirPlay 2 (see "[iOS 11 Gets Smarter in Small Ways](#)," 5 June 2017).

The idea behind Messages in iCloud is that it will store your messages and attachments in iCloud (where is it storing them now?), making sync more reliable. The feature was present in earlier betas, but Apple removed it midway through the cycle for unspecified reasons. In internal beta-tester documents, Apple has vowed to bring it back later, but the company has said nothing to the general public.

Personally, I was skeptical of the feature, since it counted against your iCloud storage quota and attachments to conversation can get big. No other messaging service charges its customers for such basic functionality, and maybe someone at Apple realized that this was going too far.

Apple has also delayed person-to-person Apple Pay payments. The concept is that you can use an iMessage app to send money directly to another person via Apple Pay.

Received money will be stored on a virtual Apple Pay Cash Card. It's uncertain what the holdup is, but needless to say, financial products are complicated, so it's not entirely surprising.

Apple confirmed the delay in a [press release](#):

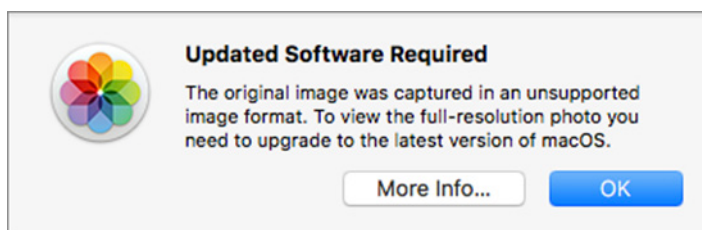
Coming this fall with an update to iOS 11 and watchOS 4, Apple Pay users will be able to send and receive money from friends and family quickly, easily and securely

Also, AirPlay 2 seems to be missing. Apple says AirPlay 2 will let you manage receivers with the Home app, output audio to multiple receivers, and work more reliably overall. However, based on my own testing, [as well as AppleInsider's](#), it doesn't seem to be implemented yet. Strangely, Apple mentions AirPlay 2 in the developer release notes for tvOS 11. Perhaps it's implemented in tvOS, but not iOS? I suspect we'll learn more whenever Apple launches the HomePod smart speaker.

We're as frustrated by the delay of these features as you are, and I'll update "[Take Control of iOS 11](#)" as soon as they're available.

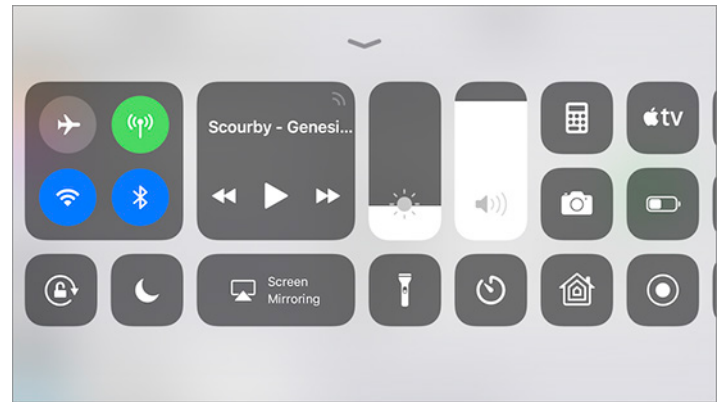
#3: Be Wary of New Video and Photo Formats -- By default, iOS 11 will capture videos and photos in the new HEVC and HEIF formats — assuming your device [has an A10 Fusion chip or better](#). That means the iPhone 7 and later, and the 2017 iPad Pro models. As Glenn Fleishman explained in "[HEVC and HEIF Will Make Video and Photos More Efficient](#)" (30 June 2017), these formats provide a host of advantages, most notably reduced file sizes, but they have one big disadvantage: a general lack of compatibility throughout the industry!

Windows computers can't read these formats yet. Nor can Apple products running operating systems before iOS 11 and macOS 10.13 High Sierra. Images I've captured in HEIF on iOS 11 can't be viewed at full resolution when synced to my 10.12 Sierra-based Mac via iCloud Photo Library.



Apart from iCloud Photo Library, this shouldn't be a major issue because exporting from Photos in iOS 11 and High Sierra generates files in standard formats. And if it is a problem, you can still capture images and videos in the JPEG and H.264 formats in iOS 11 by going to Settings > Camera > Formats and selecting Most Compatible.

#4: Control Center Is Crazy -- One of the biggest shocks after installing iOS 11 will probably be the new Control Center. It's totally bonkers! It's so different that I dedicate an entire chapter of "[Take Control of iOS 11](#)" to it. I don't have the space to repeat it all here, but here are some quick tips and notes:



Control Center has been reduced from two or three pages in iOS 10 to a single page in iOS 11. That should reduce some confusion.

You can now customize Control Center to a certain extent in Settings > Control Center > Customize Controls. Most notably, you can add a variety of Apple-provided controls — it doesn't seem that independent developers can provide Control Center buttons. And although you can remove a few default controls, others are fixed: the networking platter, the media platter, Orientation Lock, Do Not Disturb, Screen Mirroring, Brightness, and Volume.

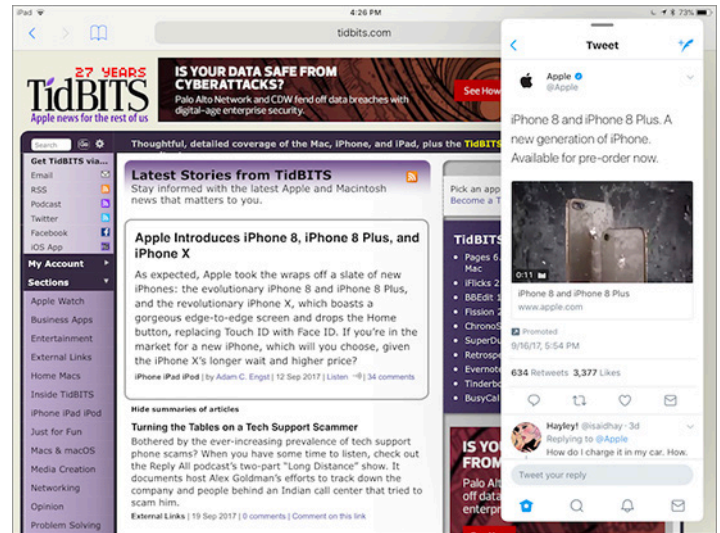
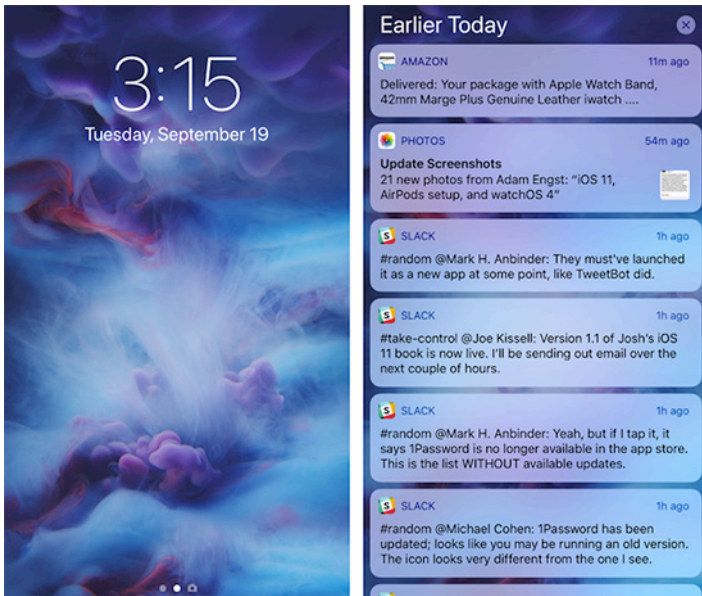
Modify which Controls appear and in what order in Settings > Control Center > Customize Controls.

I find three of the new controls are particularly useful: Low Power Mode, Screen Recording, and Apple TV Remote. Yes, there is now an Apple TV Remote in Control Center, with no app installation required. It may be my single favorite iOS 11 feature.

There are two ways to manipulate Control Center controls: tap and press. Tapping usually activates the control, while pressing reveals more options. You can experiment with each one or just read my descriptions in "[Take Control of iOS 11](#)."

#5: So Long, Notification Center -- In a move that seems obvious in hindsight, Apple has removed Notification Center in iOS 11, integrating its functionality into the Lock screen.

Here's how you get to notifications now. When your device is locked, the Lock screen shows only new notifications. To reveal past notifications, you can either swipe up on the Lock screen or swipe down from above the top of the screen, just as if you were pulling down Notification Center.



When your device is unlocked, swipe down from above the top of the screen to reveal the Lock screen and all of your notifications. This doesn't actually lock your device — either press Home or swipe up from below the bottom of the screen to return to where you were.

#6: iPad Multitasking -- Apple focused on the iPad experience in iOS 11, giving it more unique interface features and redesigning its multitasking system.

The star of the new multitasking approach is the redesigned Dock, which looks and works more like the Mac Dock. It can hold up to 15 apps and has a section to the right which displays recent and frequently used apps. That's also where Handoff apps now appear on the iPad.

You can invoke Slide Over or Split View in several ways, but it comes down to dragging one app from the Dock or Home screen onto another active app. So you can:

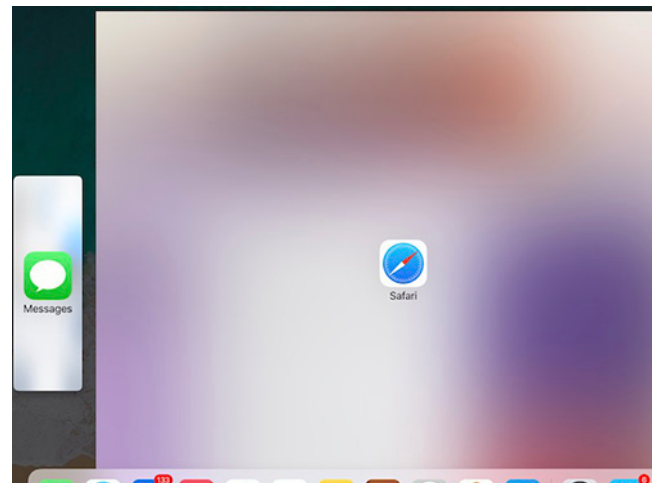
- While in an app, swipe up from under the bottom of the screen to display the Dock. Drag an app icon from the Dock onto the open app.

- From the Home screen, start dragging any app icon, and then, with another finger (perhaps on your other hand), tap another app's icon on the Home screen or in the Dock to open it, then drop the first app.

- Perform the same actions starting on the search screen, or by switching apps with the Command-Tab app switcher if you have a keyboard attached.

If you drop the dragged app on the main window while it's showing its vertical lozenge, it opens in Slide Over, which overlays the main app on the right side of the screen. Convert a Slide Over app to Split View by dragging up on the bar at the top of its window.

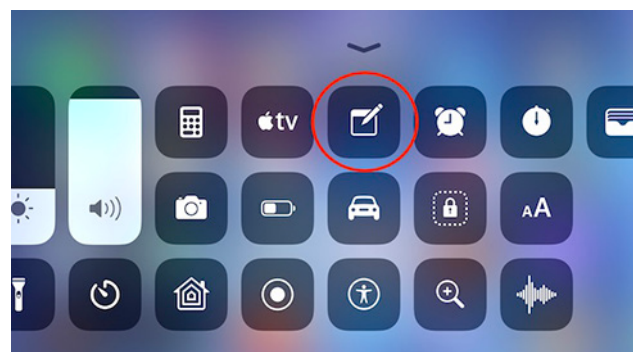
However, if you keep dragging that lozenge to either the left or right edge of the screen, the view changes to indicate that dropping it will open in Split View. It's great that you can now position the new app on either side.



There's so much going on with the iPad in iOS 11 that I dedicated a full chapter of "Take Control of iOS 11" to it.

#7: Instant Notes -- If you have an iPad Pro running iOS 11, you can tap the Lock screen with an Apple Pencil to create a new note in the Notes app (the screen must be awake, and I've found a second tap is sometimes necessary).

However, you don't need an iPad Pro and Apple Pencil to make an Instant Note. If you add the Notes button to Control Center on any iOS device, you can tap that button to create an Instant Note when your device is locked!



You can adjust Instant Notes' behavior in Settings > Notes > Access Notes from Lock Screen. The default is Always Create New Note, but you can also set it to resume the last note you worked on, which would be handy if you're taking notes in a meeting or class.

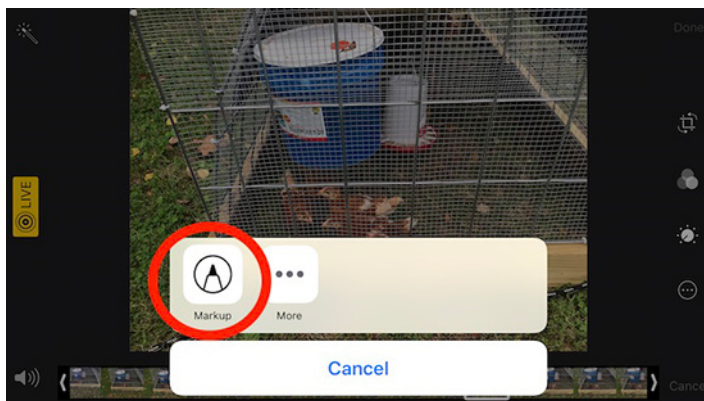
#8: Explaining Instant Markup -- Every year, Apple introduces some vague set of features under a single marketing term, which I have to figure out how to explain. Instant Markup is this year's entry.

The iOS 11 release notes imply that Instant Markup means that if you tap an Apple Pencil to an iPad Pro, you can mark up whatever is on screen. That's not true, and again, you don't need an Apple Pencil.

Instead, Instant Markup features are sprinkled throughout iOS 11. Here are a few examples:

Take a screenshot by pressing Sleep/Wake and Home. A thumbnail appears in the lower-left corner of the screen. Tap it to draw on it with markup tools.

Open a photo in Photos, tap Edit, tap the ellipsis button, and then tap Markup to draw on a photo.



In Safari, tap the Share button, then Create PDF, and then the marker icon in the upper-right corner to mark up the page as a PDF.

In iBooks, tap the marker icon while viewing a PDF to mark it up.

Don't get me wrong — it's great that this functionality is available throughout iOS now. It's just that Apple's marketing is a bit misleading, and how you access it is inconsistent.

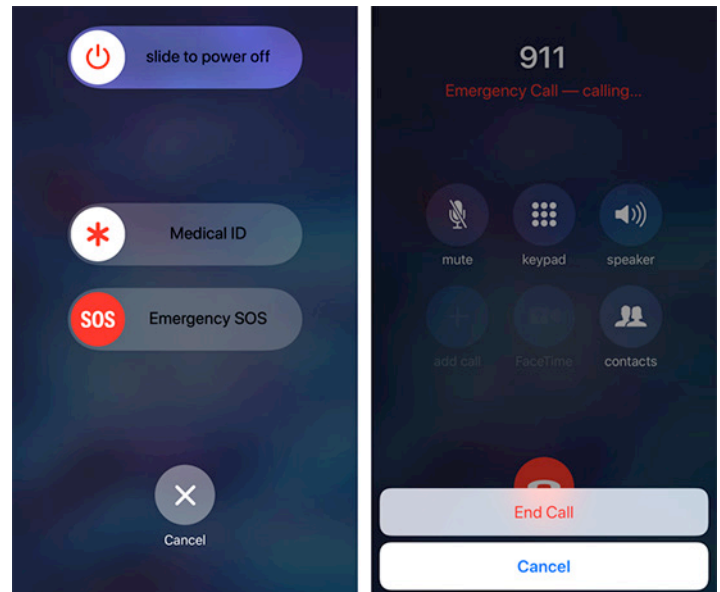
#9: Emergency SOS -- This new iPhone-only feature is important, but be careful with it. Press the Sleep/Wake button five times in rapid succession. You should see three sliders: Slide to Power Off, Medical ID, and Emergency SOS. Don't touch the Emergency SOS slider until you've finished reading this section!

First, just by accessing that screen, you have deactivated Touch ID (and presumably Face ID on the upcoming iPhone X). In many jurisdictions, the law says you can be compelled to unlock a device with a fingerprint but not a passcode. Keep that in mind, but remember that law

enforcement and border guards can make your life miserable if you refuse to provide a passcode (see [“Getting Your Devices and Data Over the U.S. Border,”](#) 14 April 2017).

As you expect, the Slide to Power Off slider shuts your iPhone off, and the Medical ID slider displays your Medical ID, which you can configure in the Health app, in the Medical ID view.

What does that scary red Emergency SOS slider do? First, it calls emergency services — 911 in the United States. After the call is completed or cancelled, it sends a text message to your emergency contacts and shares your location with them.



Here's the message it sends on my iPhone 7 Plus. There doesn't appear to be any way of modifying it:

Emergency SOS Josh Centers has made an emergency call. You are receiving this message because Josh has listed you as an emergency contact.

You set up your emergency contacts in Settings > Emergency SOS.

After it notifies your emergency contacts, it displays your Medical ID, presumably to help any emergency responders.

Remember: five quick presses of the Sleep/Wake button could save your bacon. It's worth trying it to make sure you know what's involved, but don't slide that Emergency SOS button unless it's a real emergency. We hope the feature doesn't cause too many errant calls.

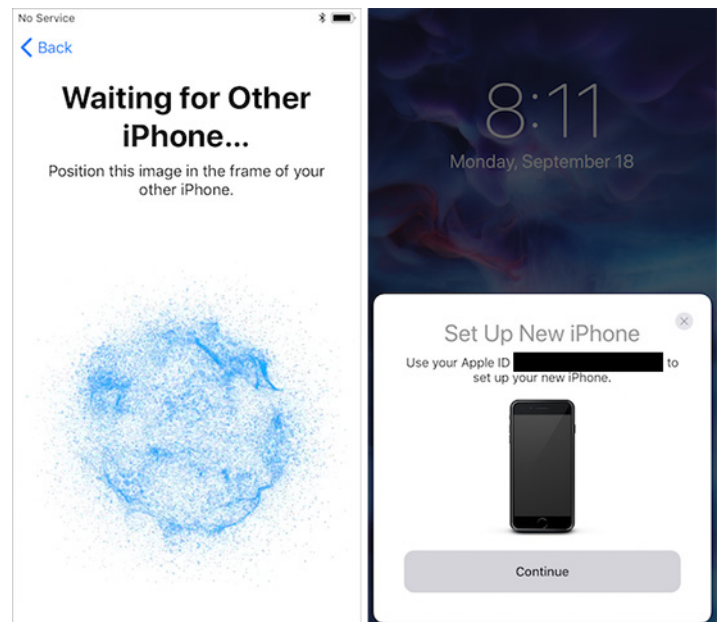
#10: Offload Apps -- Apple has long been stingy with storage space on iOS devices, and it has always been difficult to manage storage in iOS. iOS 11 improves the situation, thanks to a new storage management screen, which you can find in Settings > General > iPhone (or iPad) Storage. It offers suggestions for various things you can do or enable to save space.

But I want to point out a specific new setting, which can also be found in Settings > iTunes & App Stores: Offload Unused Apps. This setting automatically uninstalls unused apps, but retains their data. If you later reinstall the app from the App Store, it's as though you never deleted it!

The only reason not to enable this setting is if you have way more storage space than you'll ever use. For the rest of us, it can free up space with no risk of data loss.

#11: Quick Start -- It's new iPhone season, and while setup isn't a great hardship, it is the most time-consuming part of getting a new iPhone. For years, you've been able to set up an Apple TV automatically by placing an iOS device near it. Now you can finally set up iOS 11 devices the same way!

So, if you have a new iPhone 8 on the way, for instance, I highly recommend upgrading your existing iPhone to iOS 11 before it arrives. Then, when you set up your new iPhone, you'll save yourself from entering Apple ID credentials, Wi-Fi passwords, and the like. Just follow the onscreen prompts at setup or check out the What's New chapter of "Take Control of iOS 11" for instructions.

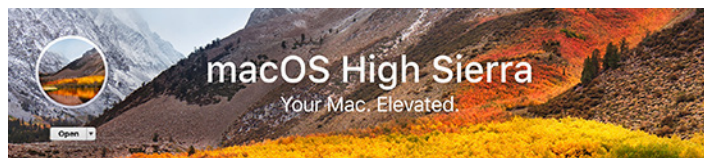


I hope you found these tips and highlights helpful, and check out "[Take Control of iOS 11](#)" for even more iOS advice! 🍷

by Adam C. Engst

macOS 10.13 High Sierra Now Available: When Should You Upgrade?

Apple has now released macOS 10.13 High Sierra via the Mac App Store for Macs running at least OS X 10.8 Mountain Lion, going back to the MacBook and iMac from late 2009 and the MacBook Air, MacBook Pro, Mac mini, and Mac Pro from 2010. (These are the same hardware requirements as for 10.12 Sierra.) As we noted at the very start of our WWDC coverage in "[Tripping to macOS 10.13 High Sierra](#)" (5 June 2017), High Sierra is one of Apple's smaller upgrades in the recent "tick, tock" of operating systems, including Leopard/Snow Leopard, Lion/Mountain Lion, Yosemite/El Capitan, and now Sierra/High Sierra.



However, as much as High Sierra has relatively few user-facing changes and new features, Apple is using the release to make some huge updates under the hood. High Sierra automatically converts Macs with SSDs to the new APFS file system (see "[What Apple's Forthcoming APFS File System Means to You](#)," 24 June 2016) and uses the new HEVC and HEIF formats for videos and photos (see "[HEVC and HEIF Will Make Video and Photos More Efficient](#)," 30

June 2017). These infrastructural changes should modernize the Mac's underpinnings, improve performance, reduce storage needs, and pave the way for future improvements.

The significance of those changes raises the question: when should you upgrade your Mac to High Sierra? With iOS, and even more so with watchOS and tvOS, we generally trust Apple enough to upgrade quickly, in large part because the company exercises such control over those operating systems that they can't vary much. Plus, frankly, problems with an Apple Watch or Apple TV aren't likely to impact your life much.

On a Mac, though, there are innumerable opportunities to stray from the straight and narrow, and many users do. If developers follow Apple's rules, and if Apple did its due diligence during beta testing, there should be no problem with upgrading to High Sierra. But there's no way to know if the hardware and software on your Mac meet Apple's specs, or if Apple was able to test your particular configuration. That doesn't mean anyone failed to do their jobs right; it's just a fact. Add that to the fact that many of us rely heavily on our Macs to get our jobs done, and the upgrade question becomes all the more important.

Happily, if you follow Joe Kissell's advice in "[Take Control of Upgrading to High Sierra](#)" and make a bootable duplicate right before upgrading, you have nothing to lose except perhaps time. That's because, in the worst case scenario, you can always reformat your Mac's boot drive and restore from your bootable duplicate. Joe has released the 1.1 version of his book now, and it includes instructions for downgrading if necessary.

That said, there's no harm in waiting, and High Sierra doesn't have so many features as to make the upgrade immediately compelling (for an in-depth guide to what's new, and much more, see Scholle McFarland's "[Take Control of High Sierra](#)"). If you fall into one of three main groups of users, we recommend holding off on High Sierra for at least a few weeks, or until 10.13.1 comes out with the usual bevy of bug fixes:

If you can't spare the time to deal with unanticipated problems. That's true if you're upgrading your own Mac or if you're upgrading the Macs of users who you support (see "Important High Sierra Changes for IT Admins," 11 September 2017).

If you're uncomfortable with the tasks involved with downgrading despite Joe's advice.

If some piece of software you rely on is incompatible with High Sierra. Developers are releasing updates, but older versions of apps may experience problems.

Users of one particular class of software should delay upgrades: those who rely on disk utilities that haven't yet been upgraded to be compatible with APFS. You really don't want to let an old disk utility touch an APFS-formatted drive. That could also be true of backup software. Although the developers of [Carbon Copy Cloner](#) and [Mac Backup Guru](#) have said that they're ready for APFS, the developers behind [SuperDuper](#) have expressed more worry due to minimal documentation from Apple (nonetheless, SuperDuper 3.0B1 is available for testing).

If you do upgrade to High Sierra, make sure to maintain a Time Machine backup, since Apple has undoubtedly used its internal knowledge about APFS to update Time Machine as necessary. Up-to-date backups protect you from a multitude of evils.

Now, despite these words of caution, if you'll excuse me, I need to finish going through Joe's checklists so I can upgrade my main iMac. 🍷

by Glenn Fleishman

Wi-Fi Security Flaw Not As Bad As It's KRACKed Up To Be

Don't panic about the new Wi-Fi security problem that you've likely seen trumpeted on news sites. Yes, the KRACK exploits reveal a fundamental flaw in the process by which a Wi-Fi device — like a Mac, iPhone, Windows computer, point-of-sale terminal, or smart fridge — connects securely to a Wi-Fi access point. You shouldn't underestimate how significant that is (it's huge), but also don't overestimate how likely it is to affect you (very unlikely).

The KRACK exploits involve how Wi-Fi Protected Access version 2, known as WPA2, lets a client device negotiate encryption keys and cryptographic elements with a base station, while keeping those elements secret from any parties trying to intercept communications, masquerade as the client, or decipher data later.

Every operating system and every device that can initiate a Wi-Fi network connection and that supports WPA2 encryption is vulnerable to at least one of the lines of attack revealed, and the researcher who discovered them has already found more attacks that he hasn't yet released. Wi-Fi access points aren't directly affected.

However, just because every device in the world could have its traffic sniffed doesn't mean that every device will. Remember that Wi-Fi is local area networking: attackers must be within range of their targets.

The KRACK vulnerabilities can be easily patched in hardware that can be updated. Apple told me that all four of its operating systems already have patches in place in the current beta releases, which will roll out in the near future for macOS, iOS, watchOS, and tvOS. Other operating systems and older Apple hardware will not be so lucky. Fortunately, many experts see ways for base stations to be updated too, but with the same proviso: many base stations lack an automatic update process, meaning they'll remain unable to prevent unpatched clients from becoming targets.

A Quick Look at KRACK -- On 16 October 2017, security researcher Mathy Vanhoef presented proofs-of-concept of several different kinds of attacks in a paper he wrote months ago and only [now released in advance of an upcoming presentation](#). He dubbed the series of attacks "KRACKs" (Key Reinstallation AttaCKs), as all major vulnerabilities now need clever names. He disclosed the vulnerabilities carefully, and [US-CERT](#) ultimately took over [disseminating the information](#) so many companies would

have patches ready or nearly so by the disclosure date. (Details were accidentally disclosed earlier than intended, [as Ars Technica explained](#).)

The various WPA2 negotiations rely on what's called a "four-way handshake" and take into account a client failing to receive the key (or failing to acknowledge receipt) during the stage in which the key is delivered. This might be due to interference or an operating system glitch or another anomaly — remember that WPA2 was developed in 2004, when everything, especially wireless devices, was slower and less reliable.

As a result, the Wi-Fi access point can retransmit the key when it believes the client hasn't received it, and the client device then installs it and resets a counter that's used to create a stream of encrypted information that only it and certain other parties like the access point can decipher.

That's where the flaw lies: an attacker can record and replay the transmission of the key, and the client dutifully resets the counter. With that information in hand, a malicious party knowing the contents of certain data packets or guessing they contain plain text (even in an email or Web page) can then decrypt other packets without obtaining the encryption key. An attacker can't join the Wi-Fi network, but can still extract information from it!

Not every operating system suffers from this problem for every kind of negotiation. Windows and iOS, for instance, weren't vulnerable to several types of attack, but were to others. As long as one sort of handshake can have a KRACK used against it, data in transit is vulnerable. Forged data could also be inserted into a network, which could allow ransomware and other malware to be delivered to vulnerable devices.

More terrifying than the flaw itself is the fact that it has existed since WPA2 appeared in 2004, and that it was found by a single person — a graduate student, not a team of veteran security researchers at an anti-intrusion software company — following a slender thread of an idea of something to test after writing a paper on a related topic. (Vanhoeft credits his research supervisor on the paper for his guidance.)

So far, there's no evidence of KRACKs being used in the wild. However, the ease with which Vanhoeft found it means that it's likely that government intelligence agencies have already found and have exploited the flaw in targeted surveillance, because it's exactly the kind of thing that they would be looking for.

Although all this sounds bad, Vanhoeft's disclosure of the KRACKs is actually good news: a researcher dedicated to a responsible disclosure ensured that companies had time to patch before cracking tools were updated. Plus, if bad actors have been exploiting these vulnerabilities, their windows of opportunity will be closing, as I explain next.

Everything That Can Be Patched Will Be -- Apple already has patches in its update stream to fix the various

KRACKs in all its operating systems (see "[Apple Has Already Patched the WPA2 KRACK Weakness in OS Betas](#)," 16 October 2017). (Apple said nothing about AirPort base stations, but we can always hope.) On 10 October 2017, Microsoft [shipped updates](#) to Windows 7 and later and Server 2012 and later. Google has more vaguely promised Android updates in the coming weeks, [according to the Verge](#), but individual Android hardware vendors will have their own schedules. Other operating system and hardware makers have updates shipping now or will release them soon. The Wi-Fi Alliance, which certifies gear that bears the Wi-Fi label, will also [update its testing](#). These responses will rapidly close the largest and most lucrative vectors of attack, those against people with recent hardware, especially mobile devices.

The biggest problem, as with many security attacks, come from three related areas: Google's Android OS, Linux, and Internet of Things (IoT) devices, which are often powered by a form of Linux. In this case, it's also because there's a serious flaw in a commonly used software module that handles the WPA2 negotiation. That flaw is bad: the encryption key in hardware running this module resets to all zeroes when an attacker attempts to replay the captured encryption key — that's right: all zeroes! Because the attacker now knows that key, they can immediately decrypt all data sent by the client. With other operating systems, an intruder has to work harder and capture a lot of data and run more KRACK attacks before deciphering some of the communication. This glaring bug isn't old — it was introduced in a relatively recent update that's incorporated into Android 6.0 and other newer hardware, and affects about 50 percent of all Android devices in use.

Android has long suffered from an update abandonment problem, with Google and its partners quickly dropping support for older releases. A lot of older Android hardware can't be upgraded to even the next major release of the system — or to any incremental improvement. This abandonment problem affects hundreds of millions of older Android devices that can never receive security updates. Review [MasterKey](#), [Stagefright](#), and [Broadpwn](#) for three examples. (Apple typically supports Macs for at least 7 years and sometimes releases very late-in-cycle security updates for even older Macs. With iOS, it's closer to 5 years.)

Even worse are Internet of Things devices that use embedded operating systems with which you never interact directly, many of which can't be updated at all. Even when products can be updated, dodgy manufacturers and cut-rate prices often result in the abandonment of support for a particular model months after it appears. Updates are often difficult to install and manufacturers don't notify customers (or have any way to do so), making it unlikely that an average user will learn of a security fix or, discovering it, be able to install it. KRACK will become another tool in an attacker's kit for recruiting devices like DVRs and nursery webcams into botnet armies.

Conversations with a few security experts made it clear that while the Wi-Fi access point side of the equation isn't at fault for these negotiation flaws, even consumer-focused access points could be updated to block, resist, or report KRACKs. (There's one exception: corporate-scale access points that support "fast handoff" act a little bit like a client in that mode, and routers with that feature have to be patched, too.)

At the enterprise level, vendors are already on top of the problem. In addition, corporate-scale intrusion-detection systems have long monitored for the unauthorized or fake access points that KRACKs require. Cisco, for instance, has provided a short primer to customers to make sure they have enabled the right options to detect KRACK-style intruders.

Public Wi-Fi networks are unlikely to be affected by the KRACK attacks. Most rely on a portal page to control access to an unsecured network, rather than WPA2. If they do employ WPA2 for access, it's typically to restrict usage to customers, as it doesn't provide real security from other users on the same network. In either case, you should always treat public hotspots as untrustworthy.

What You Can Do -- You can and should take steps to protect yourself against KRACKs. Here's how:

Install KRACK-related updates as soon as they are available for any Wi-Fi-enabled device you have.

Check your Wi-Fi base stations' configuration settings and make sure you aren't using the mixed WPA/WPA2 Personal mode in an Apple base station or TKIP encryption or TKIP/AES on other makers' hardware. You'll typically find these settings under Wireless or Wireless Security. These modes are more easily broken in general and offer more risk with KRACKs, too. Instead, make sure to use only WPA2 Personal (or WPA2 Enterprise where available) and AES-CCMP, sometimes listed just as AES. (You can't set WPA2 security on a phone or computer, only at the router.)



Check your email client and make sure that you're using an encrypted connection to your mail host and that any advanced option to allow backing down to an unencrypted connection is disabled.

For macOS Web browsers other than Safari, install HTTPS Everywhere from EFF. (Apple doesn't allow https redirection at the right stage to prevent an insecure connection at the start of a Web session.)

Use a VPN when working on any untrusted network, which could include your home network if updates haven't been released for all your hardware devices. While a VPN doesn't prevent KRACKs, it does ensure that the data encrypted by the VPN client and server is protected from someone intercepting traffic.

KRACKs won't disappear. Because hundreds of millions of unpatched devices will remain on the Internet, these attacks will surely be added to research-oriented hacking software and black-hat cracking tools, and will be used by governments and criminal organizations to target individuals who use an old Android phone or an outdated webcam.

But the odds are against KRACKs having a significant impact on overall Internet security. 🐼



Software Review

macOS High Sierra 10.13.1 update

Oct 31, 2017– 2.11 GB

The macOS High Sierra 10.13.1 update improves the security, stability, and reliability of your Mac.

This update:

- Adds support for 70 new emoji including food types, animals, mythical creatures, clothing options, more expressive smiley faces, gender-neutral characters and more
- Fixes a bug where Bluetooth may be unavailable during Apple Pay transactions
- Improves the reliability of Microsoft Exchange message sync in Mail
- Fixes an issue where Spotlight may not accept keyboard input

Security Update 2017-001 macOS Sierra

Oct 31, 2017– 768.3 MB

System Requirements

- macOS Sierra 10.12.6

Security Update 2017-001 is recommended for all users and improves the security of macOS.

Security Update 2017-004 OS X 10.11.6 El Capitan

Oct 31, 2017– 853.6 MB

System Requirements

- OS X 11.1.6

Security Update 2017-004 is recommended for all users and improves the security of OS X.

iTunes 12.7.1

Oct 31, 2017

System Requirements

- OS X version 10.10.5 or later

The new iTunes focuses on music, movies, TV shows, podcasts, and audiobooks.

Java for OS X 2017-001

Oct 26, 2017– 63.98 MB

Java for macOS 2017-001 installs the legacy Java 6 runtime for macOS 10.13 High Sierra, macOS 10.12 Sierra, macOS 10.11 El Capitan, macOS 10.10 Yosemite, macOS 10.9 Mavericks, macOS 10.8 Mountain Lion, and macOS 10.7 Lion.

This package is exclusively intended for support of legacy software and installs the same deprecated version of Java 6 included in the 2015-001, 2014-001, and 2013-005 releases.


HP Printer Drivers 5.1 for OS X

This download includes the latest HP printing and scanning software for OS X.

macOS 10.13 Supplemental

Oct 5, 2017– 923.4 MB

This supplemental update includes improvements to the stability, reliability and security of your Mac, and is recommended for all macOS High Sierra users. This update:

- Improves installer robustness
- Fixes a cursor graphic bug when using Adobe InDesign
- Resolves an issue where email messages couldn't be deleted from Yahoo accounts in Mail 

Share Keystone MacCentral with other MACaholics

Name _____

Address _____

City _____ State ____ Zip _____

Home Phone _____ Day Phone _____

E-mail Address _____

Date _____ Is this ☐ Renewal or ☐ New?

How did you hear about us? _____

Dues for one person are ☐ \$20/yr. Family or Corporate dues are ☐ \$30/yr.

To join Keystone MacCentral, mail this form with your membership dues (payable to Keystone MacCentral) to:

**Keystone MacCentral
Membership Chair
310 Somerset Drive
Shiresmanstown, PA 17011**

Keystone MacCentral meetings are held at 6:30 p.m. on the 3rd Tuesday of the month at Bethany Village Retirement Center, 5225 Wilson Lane, Mechanicsburg, PA 17055