Apple has finally embraced key-based 2FA. So should you

Enlarge / An Ars-branded Yubikey.
Steven Klein

reader comments

184 with 125 posters participating

Share this story

Almost three years ago, Google introduced its Advanced Protection Program (APP), a security plan for high-risk users that requires hardware keys for account access and is arguably the industry's most effective way to stop account takeovers in their tracks. But until now there was a major flaw that held APP back: its iPhone and iPad offerings were prohibitively limited for most users. Now that this has changed—more on the change in a bit—I feel comfortable recommending APP much more widely.

What is APP?

By requiring users to produce a physical security key in addition to a password each time they log in with a new device, APP is designed to stop the kinds of account breaches that Russian operatives used to disrupt the 2016 presidential election when they published sensitive emails from high-ranking Democratic officials.

Those attacks presented targets with convincing emails purportedly from Google. They warned, falsely, that the target's account password had been obtained by an outsider and

should immediately be changed. When Hillary Clinton's presidential campaign chairman John Podesta and other Democrats complied, they effectively surrendered their passwords to hackers. Although hackers have many ways to compromise accounts, phishing remains one of the most popular, both because it's easy and because the success rate is so high.

APP makes such attacks all but impossible. The cryptographic secrets stored on the physical keys required by APP can't be phished and—theoretically—can't be extracted even when someone gets physical access to a key or hacks the device it connects to. Unless attackers steal the key—something that's not feasible remotely—they can't log in even if they obtain the target's password.

Think of APP as two-factor authentication (2FA) or multifactor authentication (MFA) on steroids.

Security practitioners almost unanimously consider physical keys a more secure MFA alternative to authenticator apps, which provide an ever-changing password that users enter as a second factor. Temporary passwords are even more of a problem when sent via SMS text messages, which are vulnerable to SIM-swapping attacks and to compromises of cell phone networks. One-time passwords are also problematic because they can be phished and in some cases can be stolen. A 2016 study of 50,000 Google employees over two years found that security keys beat out other forms of 2FA, both for security and reliability. APP combines the security of physical keys with a rigorous method for locking down an account. When first setting up APP, users must enroll two security keys such as those made by Yubico or Titan Security. Once the keys are enrolled, all devices that may be logged in to the account are automatically logged out and can only be logged back in using one of the keys as a second factor.

Users must also use the keys when logging in from any new

devices for the first time. (Google calls this process bootstrapping). Once a device is authenticated, it by default no longer needs the second authentication factor during subsequent logins. Even then, Google may require a second factor again in the event that company employees see logins from suspicious IPs or other signs that the account has been, or is close to being, hijacked. APP, works with all Google apps as well as its Nest series of smart home services, but it restricts the third-party apps to all but a handful. Google says that APP provides additional safeguards but has never offered many details beyond that.

To make bootstrapping less painful, users can enroll their Android—and more recently their iOS device—as an additional physical key that is activated by clicking *yes* on a screen that automatically appears during the bootstrapping process. The appeal of this option is that users generally have their phone in their pockets, making it more convenient than more traditional physical keys.

Here’s how it looks on both iOS and Android:

Enlarge / A built-in security key in an iPhone (left) and a Pixel (right).

The phone-based keys—which comply with the recently introduced WebAuthn standard (more about that later)—work only when Bluetooth is enabled on both the phone and the device that's being bootstrapped. On top of that, the keys only work when both the phone and the bootstrapped device are in close proximity to each other. This requirement fixes a security weakness in earlier push-based 2FA, in which users tapped an OK button on their phones after successfully entering an account password.

Similar to temporary passwords from authenticators and SMS, push-authentication protections can be bypassed when an

attacker’s carefully timed login closely follows the target trying to log in to the attacker’s fake site. Since the targets think they’re logging in, they have no reason not to hit the *yes* button. The Bluetooth requirement adds an additional hurdle—not only must the attacker have the target’s account password and time things perfectly, but the attacker must *also* have physical proximity to the target’s device.

Great for Android, but what about iOS?

As a security maven and a journalist who works with anonymous sources from time to time, I enrolled in APP, both with my personal account and my work one, which uses G Suite. (I had to ask my administrator to allow APP first, but he was able to easily turn it on.) The process for each account took less than five minutes, not counting the time it took to buy two keys. From then on, a physical key was the sole means of providing a second factor of authentication.

While APP is no magic bullet against breaches, it does more than any other measure I can think of to prevent account compromises that result from phishing and other types of attacks that exploit compromised passwords. I liked the assurance, and I also liked the usability. Using a Pixel XL that had NFC support, I was able to easily use physical keys on all the devices I owned, even during the early days of APP when key options were more limited. Things became easier still when I could use my phone as a security key.

Until now, however, I’ve held off recommending the general use of APP or even physical keys for 2FA on other sites. My reason: Apple’s long-standing practice of tightly restricting access to the Lightning port, and until recently iPhone and iPad NFC, made using hardware-based keys on these devices prohibitively limited. It was hardly worth recommending an authentication method that was unpalatable or unsuitable to

users of one of the world's most popular and influential platforms.

For most of APP's existence, the only kinds of physical keys that worked with iPhones and iPads were dongles that used BLE, short for Bluetooth Low Energy. I found those dongles fragile, cumbersome, and prone to failures that sometimes required three or more tries before logins would succeed. These keys were the antithesis of the Apple mantra "It just works."

Even worse, I have my doubts about Bluetooth security. A raft of vulnerabilities, both in the Bluetooth specification and in some of its implementations, raises legitimate concerns that they aren't subjected to rigorous security auditing. Google's disclosure last year of a vulnerability that made it possible for nearby hackers to hijack the Titan Bluetooth pairing process didn't make me feel any better. (The flaw has since been fixed.)

This lack of viable key options was out of Google's hands. Apple's tradition of building from the inside out—and its aversion to technologies it views as untested—made the company slow to open its products to hardware-based keys. As a result, Apple resisted calls to allow iPhones and iPads to connect to most devices over NFC or through its Lightning port.

While USB-based keys could be used on Macs (and Windows and Linux devices) that ran Chrome and, later, Firefox and other browsers, Bluetooth remained the sole means to connect keys to iPhones and iPads. Ultimately, Bluetooth keys never seemed to catch on. Key maker Yubico, for instance, still doesn't offer products that use Bluetooth. Comments like these on a Google support forum capture some users' frustration with the lack of viable options. With iOS and iPadOS largely left out, Google and some industry partners did their best to cobble together alternatives.

In June 2019, for example, Google began allowing APP account

holders to use their Android phones as security keys to log in to their iPhones and iPads, but this option didn't do much to convince me that APP was ready for the iPhone and iPad masses. Once I got over the learning curve, the option worked well enough. But even then, the requirement of a second mobile device—running a rival OS, no less—meant it wasn't likely to appeal to a large percentage of iOS and iPadOS users.

In August 2019, Yubico released the Yubikey 5Ci, a key that used proprietary technology to connect to Apple's Lightning port while the world waited for Apple to add native support. Most people hardly took notice because the 5Ci could only be used with the iOS version of the upstart browser Brave and then for a vanishingly small number of services. More mainstream browsers and sites were completely left out. It wasn't until the following month—September 2019—that Safari for macOS added support for physical keys, making it the last major browser to do so.

It was only with December's release of iOS and iPadOS 13.3 that Apple added native support for NFC, USB keys through an authentication standard known as FIDO2. These additions were a major improvement, but they came with their own limitations. Seven months later, only Safari and Brave for iOS and iPadOS can use authentication keys. A variety of sites that offer hardware-based 2FA don't work well or at all with Brave. While the browser works with Yubico keys, keys from Titan aren't supported at all.

To the frustration of browser makers and online service operators, Apple has yet to publish the programming interfaces that third-party browsers need to actually read the keys using the recently added native support. (Brave can read 5Ci keys thanks to a proprietary Yubico interface. To support Yubico NFC keys, Brave uses a combination of Yubico interfaces and a set of Apple APIs that give iOS and iPadOS apps raw access to NFC-enabled devices.) An Apple spokesman confirmed the company has not yet made the support available but said that shouldn't

be interpreted as that it won’t happen in the future.

All of these usability restrictions kept me from widely recommending physical keys at all—again because I didn’t want to endorse one MFA method for iOS and iPadOS and another one for all other platforms.

https://arstechnica.com/?p=1690028