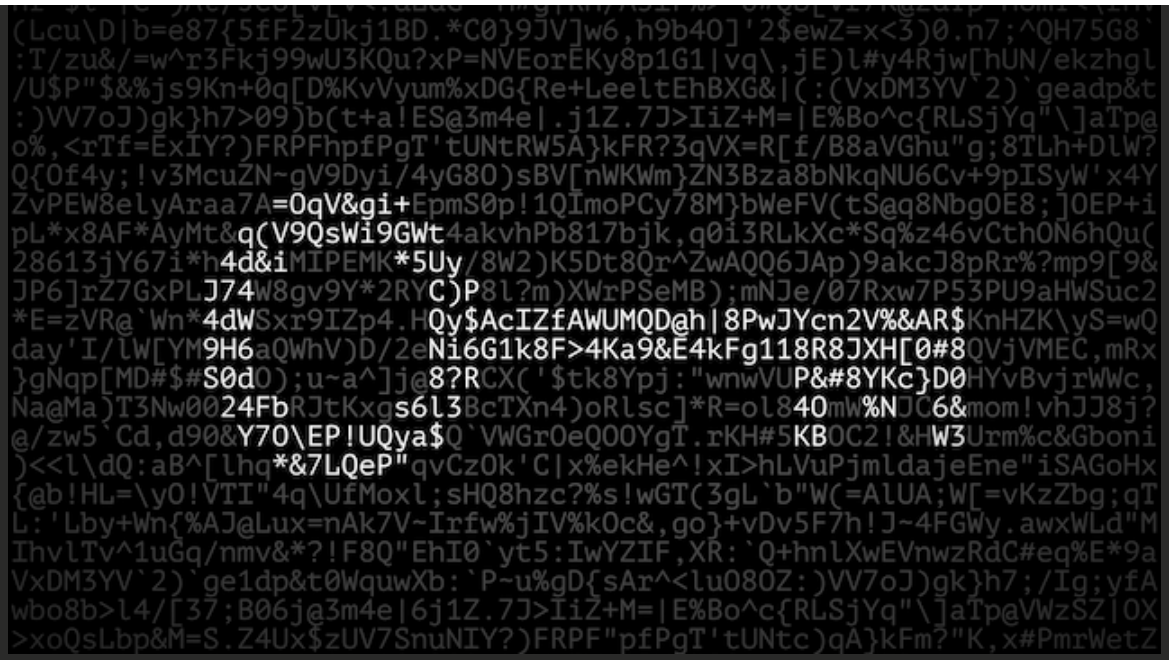
The Pros and Cons of Passkeys

May 21, 2023

When I first read about passkeys, I got super excited. Finally it seemed that we might truly have a “password killer” technology. Passkeys promised to be easier to use and more secure than passwords. It’s a rare thing in security when you can improve convenience and security simultaneously. However, as this cool new technology actually begins to roll out, we see that there are still devils in the details. Let’s look at the current pros and cons of passkeys.



How Passwords Work

Before we can discuss passkeys, we need to quickly review how passwords work. To access an online account, you need to prove that you are the owner of that account – you need to *authenticate* yourself with the website. In most cases today, we do this with user names and passwords. The user name identifies the account. The password is a *shared secret*, something you chose when you set up the account. If you know the secret, you must be the right person.

The websites don't save the user passwords as plain text – that wouldn't be safe. They're transformed using a special cryptographic technique called hashing. A hash is sometimes called a "trap door" function: easy to go one way, very hard to go the other. That is, it's easy to compute the hash from the password, but effectively impossible to figure out the password based on the hash value. So when you type in your password to login, the password is first hashed locally and the hashed value is sent to the server. If this hash matches the hashed password they have stored for your account, then the password you entered must be the right one.

Ideally, this means that even if someone hacks into the website's server and steals all the passwords for all user accounts, then it does them no good because they can't reverse the hashing process. In reality, if you used an easy-to-guess password, the bad guys have already pre-calculated all the hashed versions of common (bad) passwords. If they find a matching hashed password, then they immediately know the actual password used to create that hash.

Other Authentication Methods

Proving your identity usually involves one of the following three methods:

- Something you know (like a password or PIN)
- Something you have (like a physical key or a smart device)
- Something you are (biometrics, like fingerprint or face scan)

To be extra secure, websites can require more than one of these methods, or *multi-factor authentication* (MFA). A popular option today is using one-time PIN codes sent via SMS or generated by an app as a second option, what we refer to as *two-factory authentication* (2FA).

It's important to realize here that 2FA is actually a transitive authentication. Before you can access a 2FA app to get the one-time PIN code, you first have to unlock your phone. That is, you first have to prove to the phone that you are the owner of the phone. This is usually done with a finger or face scan (something you are), which then allows you to use the 2FA app on the phone (something you have).

How Passkeys Work

Passkeys are sort of a combination of all of those techniques, with some interesting improvements. First of all, passkeys don't use a shared secret. Instead, a *pair* of matched keys is created – a public key and private key. The public key is given to the

Amazon Android Apple Backups Best & Worst Gifts Best Of Book news data breach Data Privacy Week De-Google democracy Equifax Facebook fingerprinting Firefox Fun stuff Giveaway Google Guest Post How-To identity theft IMHO IoT Mobile Phone network New Years Resolutions Password managers Passwords patrons Podcast privacy Proton QR code Reviews scam Security Site news social media SPECIAL surveillance

website to save while the private key is stored in a special, highly secure vault on your device. To authenticate with the website, you need to prove that you are in possession of the private key that matches the public key the website has for you.

How does that work? It's complicated. But basically, when you go to log in to the website, the website generates a special challenge using your public key – a challenge whose response can only be created by someone with the corresponding private key. It's like asking you a question that only you can answer – and also being able to ask you an infinite number of such questions.

This technique has many advantages – here are a few. First, the entire process is managed for you. The keys are generated and they're guaranteed to be unique and super strong. You also never have to remember them or type them in. Second, passkeys are tied to the website and won't work on fake sites – therefore, they can't be phished. Third, this split-key technique neatly solves the shared secret problem. The public key has no value for an attacker, so there's no point in hacking the server to get it.

Here's the Catch

As is often the case, trying to implement the ivory tower idea in a real world environment exposes limitations and shaky assumptions. For passkeys, the problem is that most people have multiple devices. If my private keys are embedded in a super-secure vault on my smartphone, how do I login to a website from my laptop?

Here's the official solution. From your web browser on your laptop, you tell the website that you want to authenticate using a different device. At this point, the website pops up a QR code which you can then scan with the camera app on your smartphone.

Using the information in the QR code and some sort of connection with the phone (Bluetooth, NFC or USB), the smartphone responds to the challenge on behalf of your web browser through a cloud server that was negotiated as part of this process. If everything works right, it's not that difficult from the user's perspective – though under the covers, there's a lot going on.

But wouldn't it would be nicer if you could just log in from your laptop, too? Most password managers will seamlessly and securely synchronize your passwords between all your devices. Why can't we do that with passkeys, too? But the real problem is more fundamental than that. If all my keys are locked in a vault on a single device, what happens when I lose access to that device? In other words, how do I recover access to my accounts?

Account Recovery

We already have this problem today. How do you regain access to your account if you forget your password? You click the "Forgot my password" link. This triggers one of several options – like answering "security questions" or resetting your password using a link sent to the email account associated with your account. I'm guessing that most sites will fall back to username and password as a backup for passkey logins... but that undermines one of the main reasons for using passkeys in the first place. Some sites also give you the option to generate a recovery code, though I'm not sure if that's any more secure than a traditional password. (If you're really interested, this paper has an exhaustive analysis of account recovery methods. This site has other related research.)

Another possible solution is to associate multiple key pairs with each online account. That is, you might generate Key Pair 1 for amazon.com on your smartphone and then Key Pair 2 for amazon.com on your laptop. Either set of keys will get you into your account. However, if you lose or sell your smartphone, you'll need to cancel every key pair that was on that phone and create new key pairs for the new smartphone. That's honestly not practical.

To me, even though it exposes your private keys, I still think the only viable solution to this problem is to allow private keys to be securely synchronized from one device to another. This could be done in a strictly local, peer-to-peer way, not involving any cloud service. But for passkeys to be successful, they must be convenient to use. I think ultimately they need to be capable of synchronizing securely and continuously between multiple devices, like we do today with passwords via cloud-based password managers. You should have the option *not* to do this, but it should be possible – maybe even the default.

My Advice on Passkeys: Wait a Bit

Apple, Google and Microsoft have all rolled out initial support for passkeys. Because they don't want to field support calls from users who have lost their devices, they have created secure mechanisms for backing up and synchronizing your passkeys between your devices. While I have no doubt that they have put a ton of thought into this, right now these mechanisms are proprietary. If you have an iPhone and a Windows PC, they are not going to sync. (You can, however, use the QR code method I described above.)

My advice at this point is to just wait a bit before jumping on the passkeys bandwagon. They have the potential to replace passwords and 2FA, but we need to figure out a workable cross-platform solution to the account recovery and multi-device problems. Existing password managers like 1Password and Bitwarden are already working on this. When those become available, they'll need some time to shake out any problems, so I wouldn't rely on them solely. That is, keep using strong passwords and 2FA for your online accounts, at least as a backup. Maybe some day we'll have a single, open spec for this. But until then, we at least need a solution that works across Windows, macOS, iOS, Android and Linux.

I should also point out that right now very few sites and services even support passkeys. There's a cool site that maintains a searchable list of sites that have passkey support: passkeys.directory. If you want to try out passkeys, check out this demo site.

And stay tuned to my blog, newsletter and/or podcast – I'll keep you updated on all of this.

← Previous Post

Next Post →

Related Posts

Security news update (Feb 8)

By Carey Parker / February 8, 2015

Security roundup (3/1/2015)

By Carey Parker / March 1, 2015

Truly Secure Mobile Communication (for Free!)

By Carey Parker / March 9, 2015

Security roundup (4/5/15)

By Carey Parker / April 5, 2015