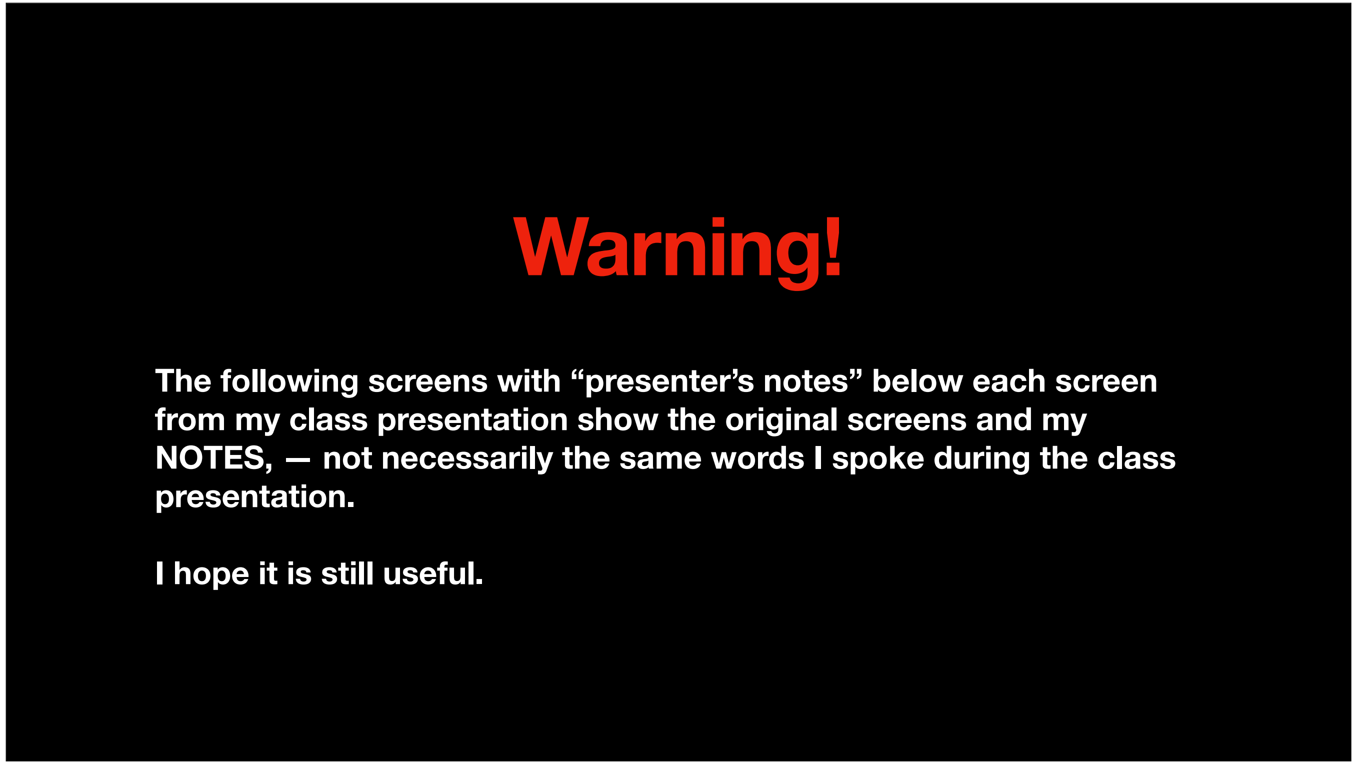
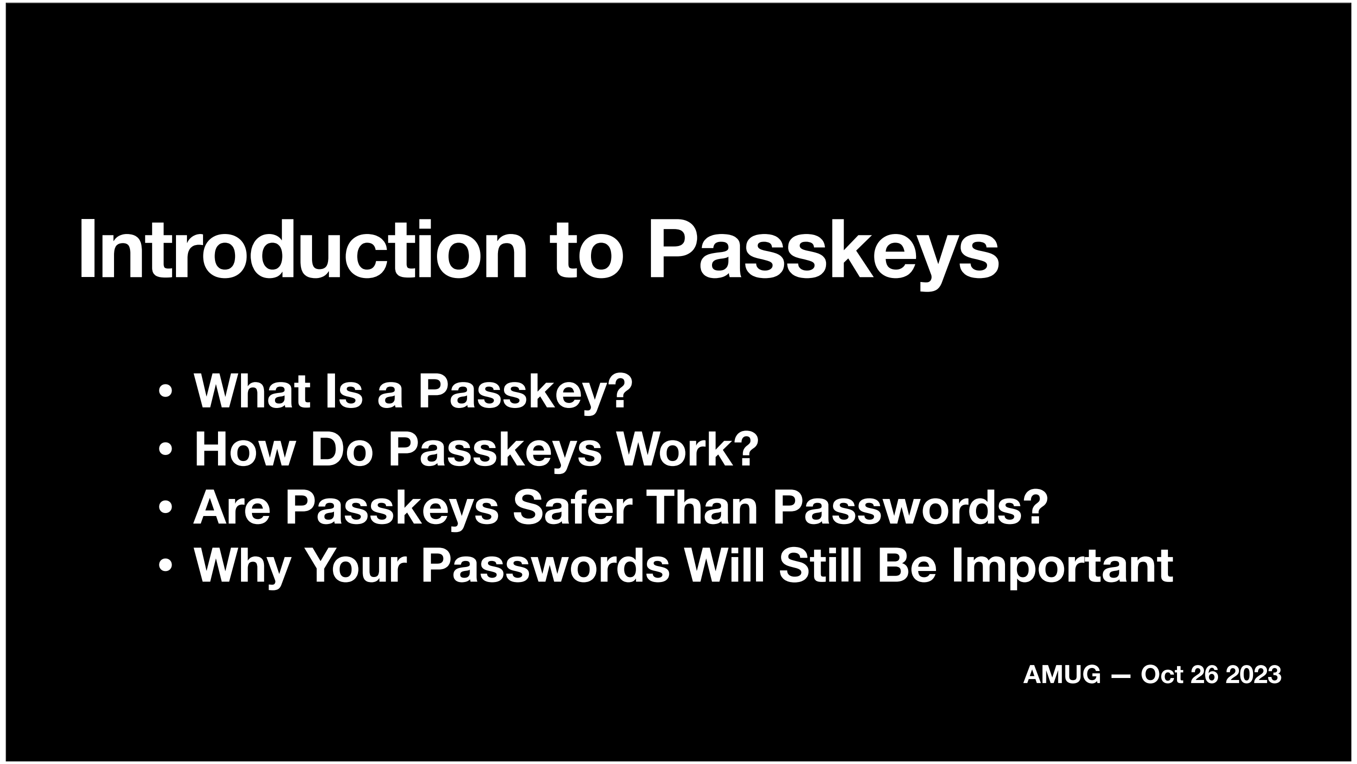


Warning!

The following screens with “presenter’s notes” below each screen from my class presentation show the original screens and my NOTES, — not necessarily the same words I spoke during the class presentation.

I hope it is still useful.

Disclaimer on the posted presentation screens and Presenter’s Notes



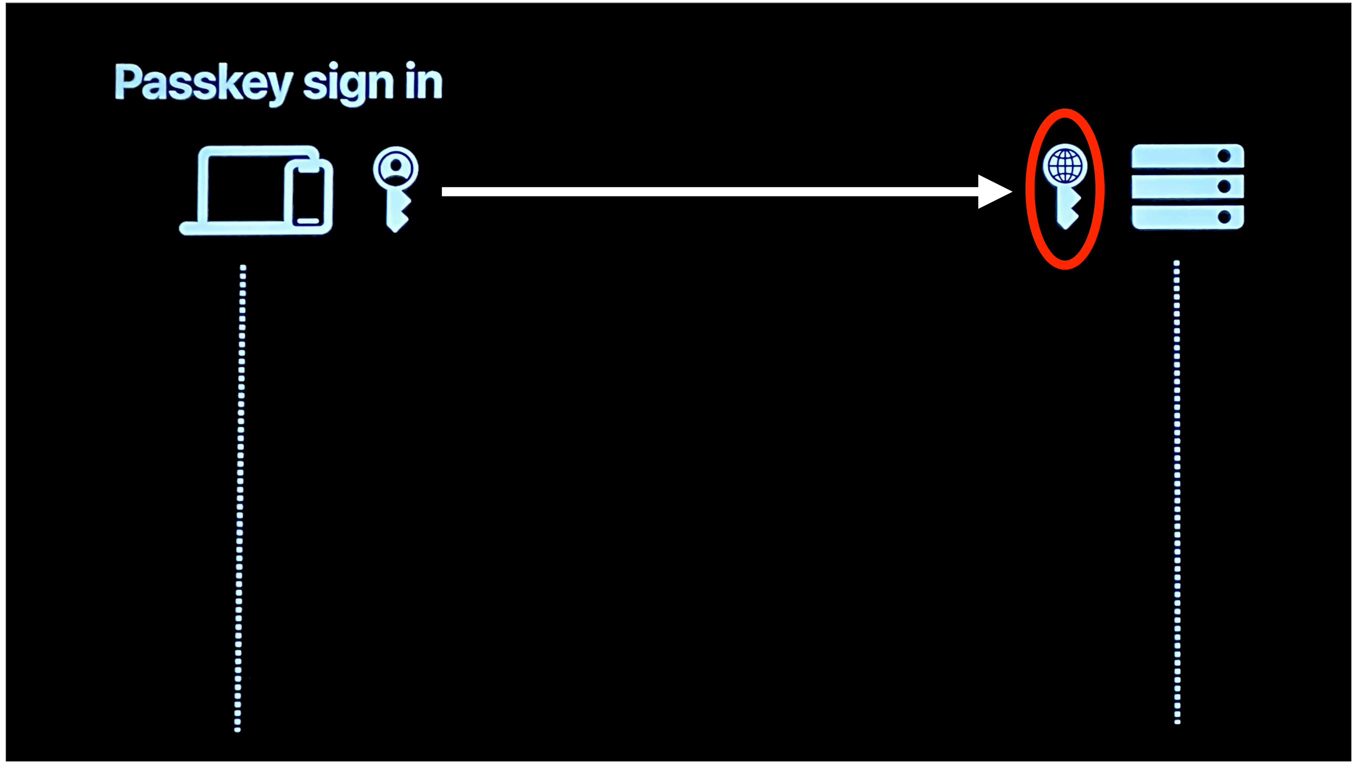
Introduction to Passkeys

- What Is a Passkey?
- How Do Passkeys Work?
- Are Passkeys Safer Than Passwords?
- Why Your Passwords Will Still Be Important

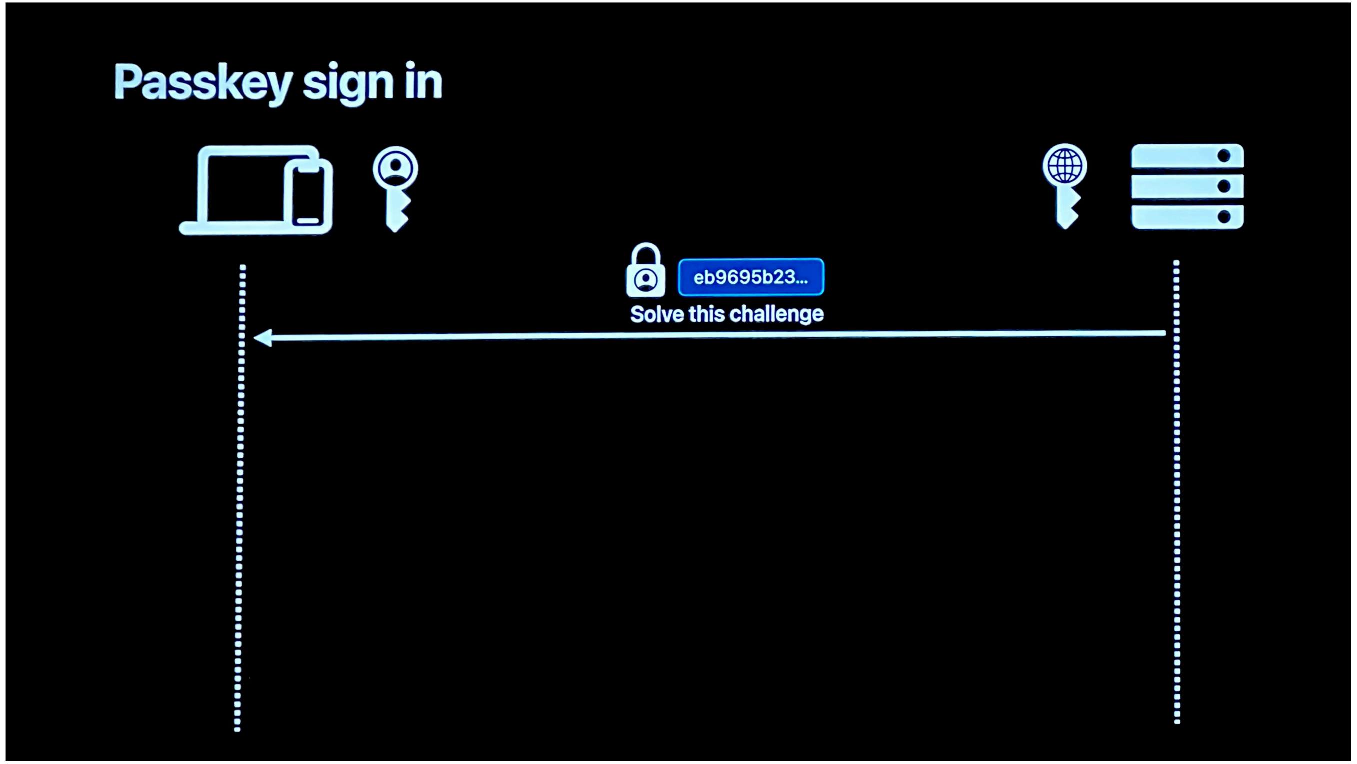
AMUG — Oct 26 2023

In this introduction to Passkeys, I want to cover an explanation of what Passkey Authentication is, how it works, and why this authentication system is safer and less prone to hacking than the existing Password systems we all still use for most of our accounts.

But I will also point out that it will be years still before Passkeys have any chance of replacing Passwords for most login systems, and why your Passwords will remain important to secure even after you move from Passwords to Passkeys. Apple began introducing Passkey systems to their App Developers 2½ years ago, and made Passkeys useable on all Apple devices a year later. More than a year later, it’s just starting to catch on.

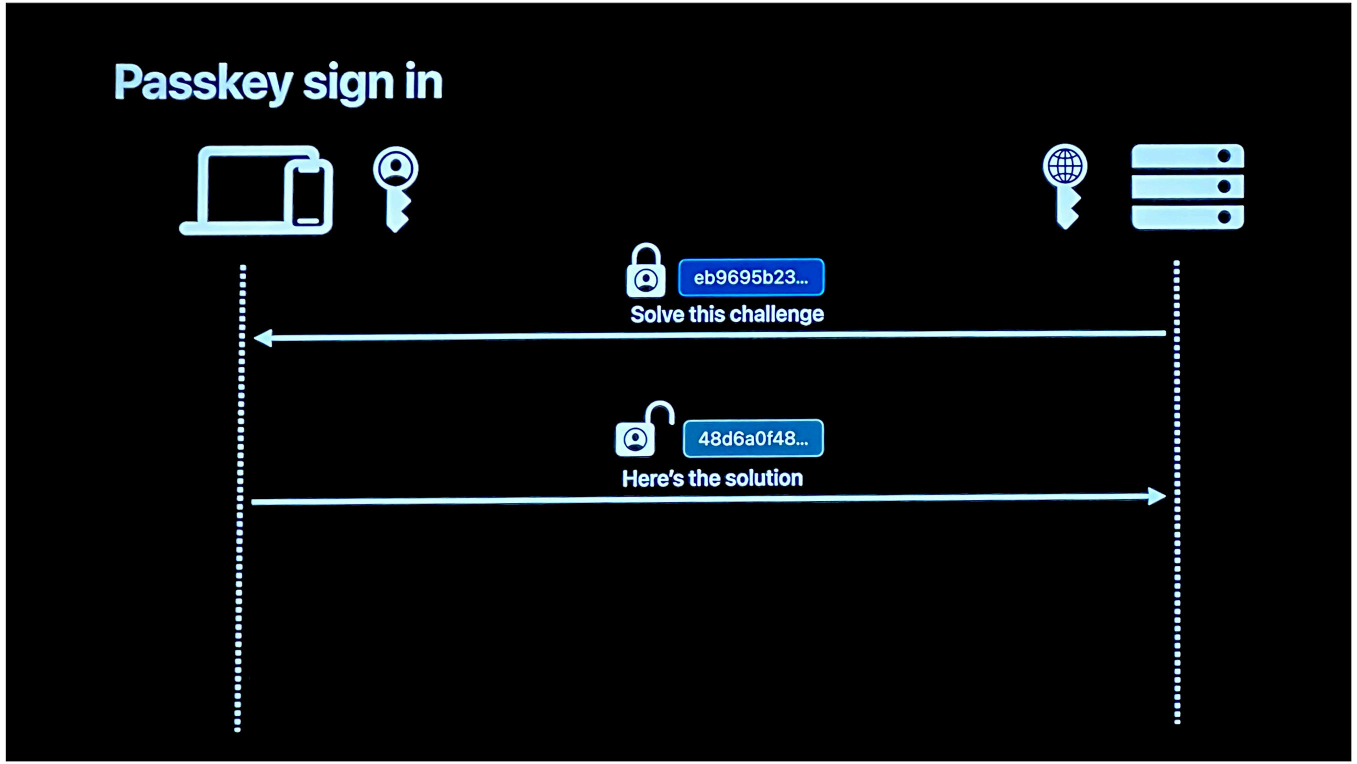


Passkeys work differently than passwords. When you create a Passkey for accounts which support them, your Apple device generates a PAIR of Keys and sends the PUBLIC KEY to the site’s Server, where it is stored as the credential for your account. There is nothing secret about that Public Key — it can’t decode anything — it can just matches up when the device that sent it lands on the login page. The PRIVATE Key never leaves your device, and it does all of the work to authenticate you right on your device.



Passkey sign in

When you later need to login to this account, as the sign-in screen loads, your device triggers the matching Public Key on the server to send back an encrypted challenge - a different one every time it’s used - and your device then uses its stored Private Key to decode that challenge.



Passkey sign in

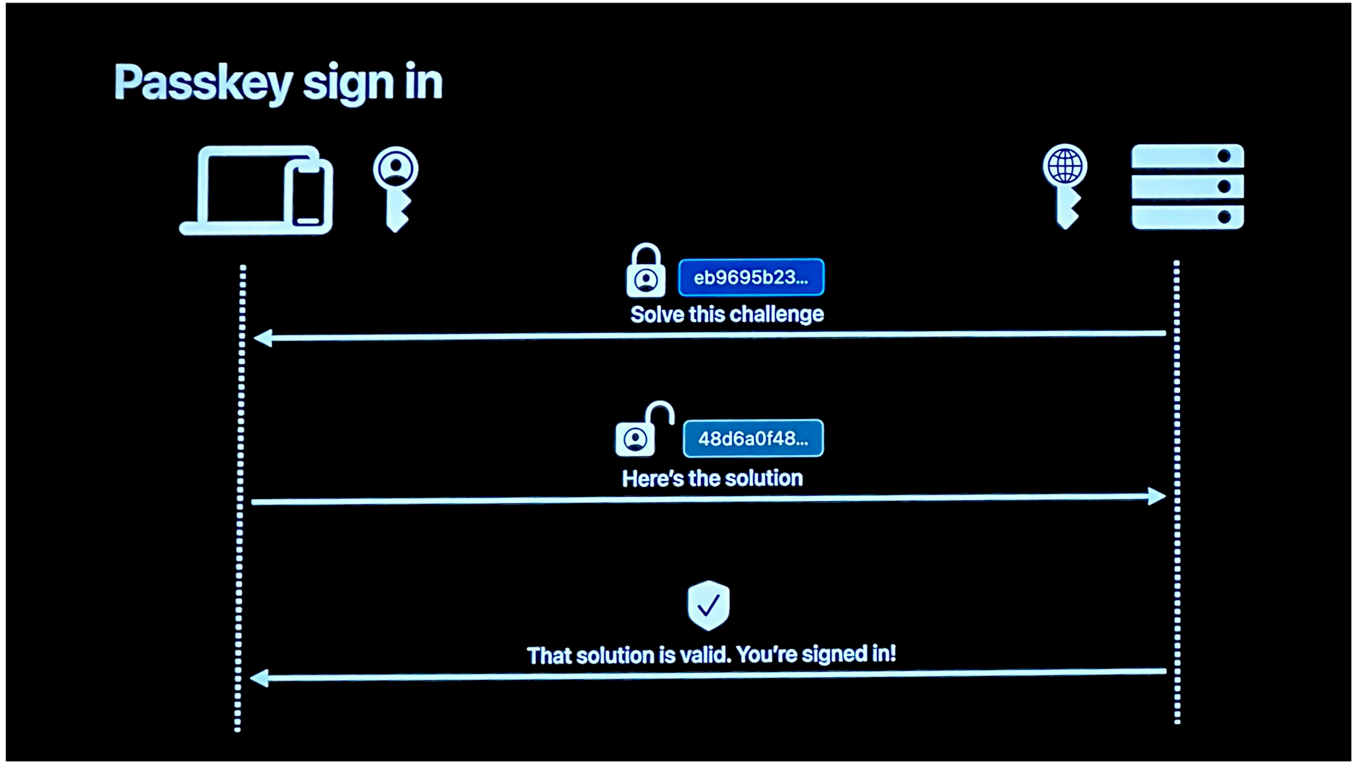
eb9695b23...

Solve this challenge

48d6a0f48...

Here’s the solution

Your device sends back a one-time response to that one-time challenge, proving that yours is the device that created the account.



Passkey sign in

eb9695b23...

Solve this challenge

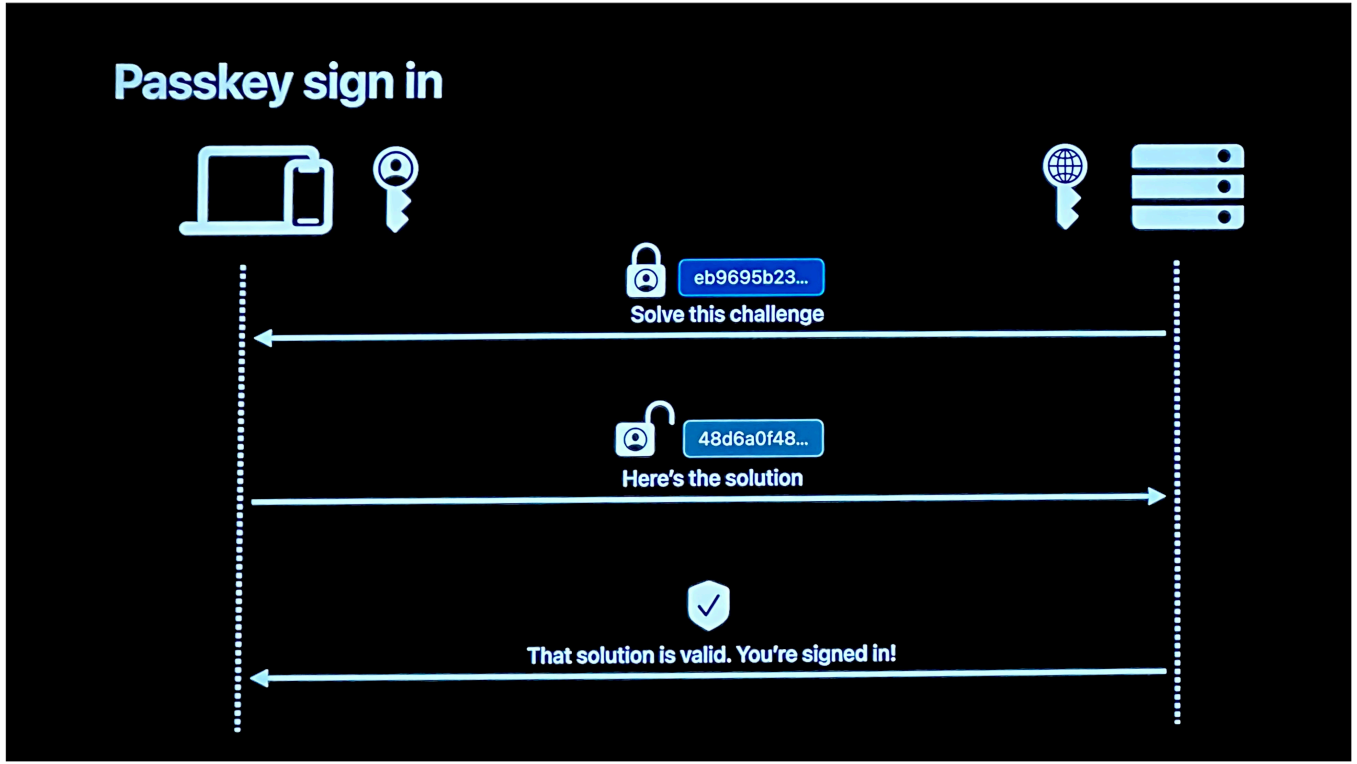
48d6a0f48...

Here's the solution

That solution is valid. You're signed in!

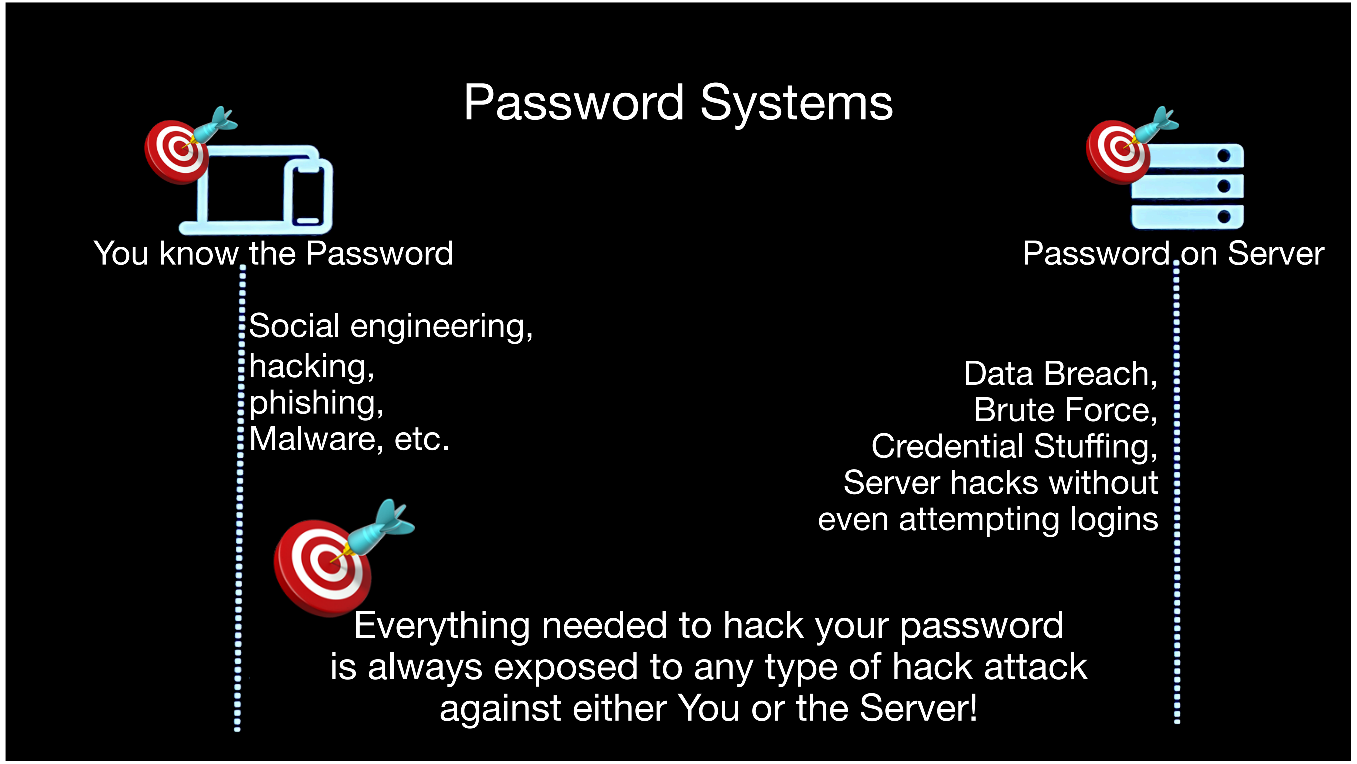
The server reads the resulting code against the request, and - without having to store either of them on the server - it simply notes that you have proved the account is yours and lets you in.

Because the Private Key that your device generated when setting up the Passkey never leaves your device and its codes are used only one-time to match a one-time challenge each time, there is nothing kept on the Server that could let a hacker access to your account.



Passkey sign in

This creates a system where - if the server is hacked and everything on it is stolen by a hacker - there is no information which can be used to get into your account! All the server has is the Public Key to generate challenges, with no clues about what the next correct answer should look like.
Phishing won't work as you don't use a password to get into the legitimate site, and phishing can't generate a valid challenge request to respond to. Brute Force attacks will fail because there are no Server Challenges to be matched with a response. 2-Factor Authentication is not needed because your device already proved it created the account passkey by answering the one-time challenge.



Password Systems

You know the Password

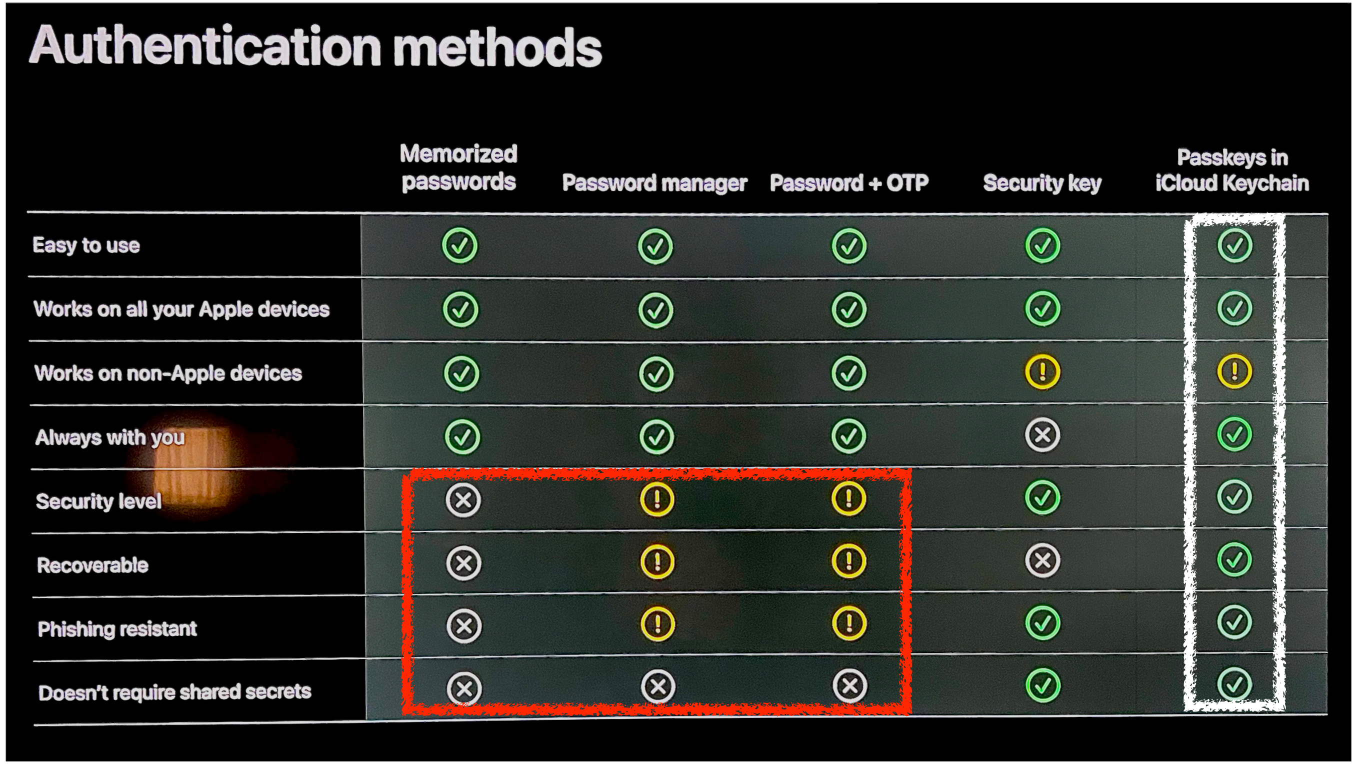
Social engineering,
hacking,
phishing,
Malware, etc.

Password on Server

Data Breach,
Brute Force,
Credential Stuffing,
Server hacks without
even attempting logins

Everything needed to hack your password
is always exposed to any type of hack attack
against either You or the Server!

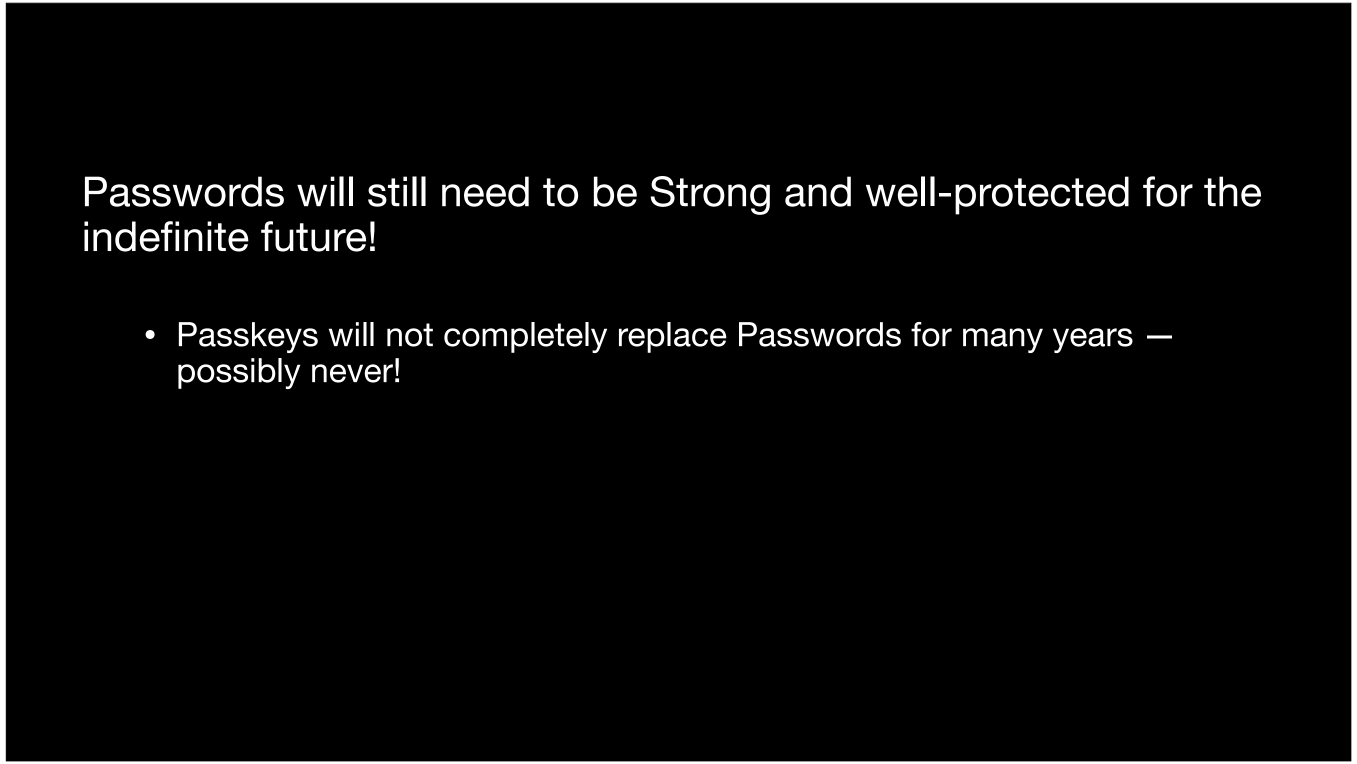
Compare this to a system with Passwords, where the password or some encrypted Hash of it is actually stored right on the account server.
First, that makes the server is a prime target for hacking as the password or its hash can be stolen and either used directly or reverse engineered to learn the password.
You can be phished for credentials several ways. Once a hacker has obtained your Password, your account is wide open.
2FA alleviates this risk significantly, but also requires you to use Text Message codes or Emails to confirm your login, and even those are susceptible to interception once your password has been exposed to a hacker.



Authentication methods

	Memorized passwords	Password manager	Password + OTP	Security key	Passkeys in iCloud Keychain
Easy to use	✓	✓	✓	✓	✓
Works on all your Apple devices	✓	✓	✓	✓	✓
Works on non-Apple devices	✓	✓	✓	⚠	⚠
Always with you	✓	✓	✓	⊗	✓
Security level	⊗	⚠	⚠	✓	✓
Recoverable	⊗	⚠	⚠	⊗	✓
Phishing resistant	⊗	⚠	⚠	✓	✓
Doesn't require shared secrets	⊗	⊗	⊗	✓	✓

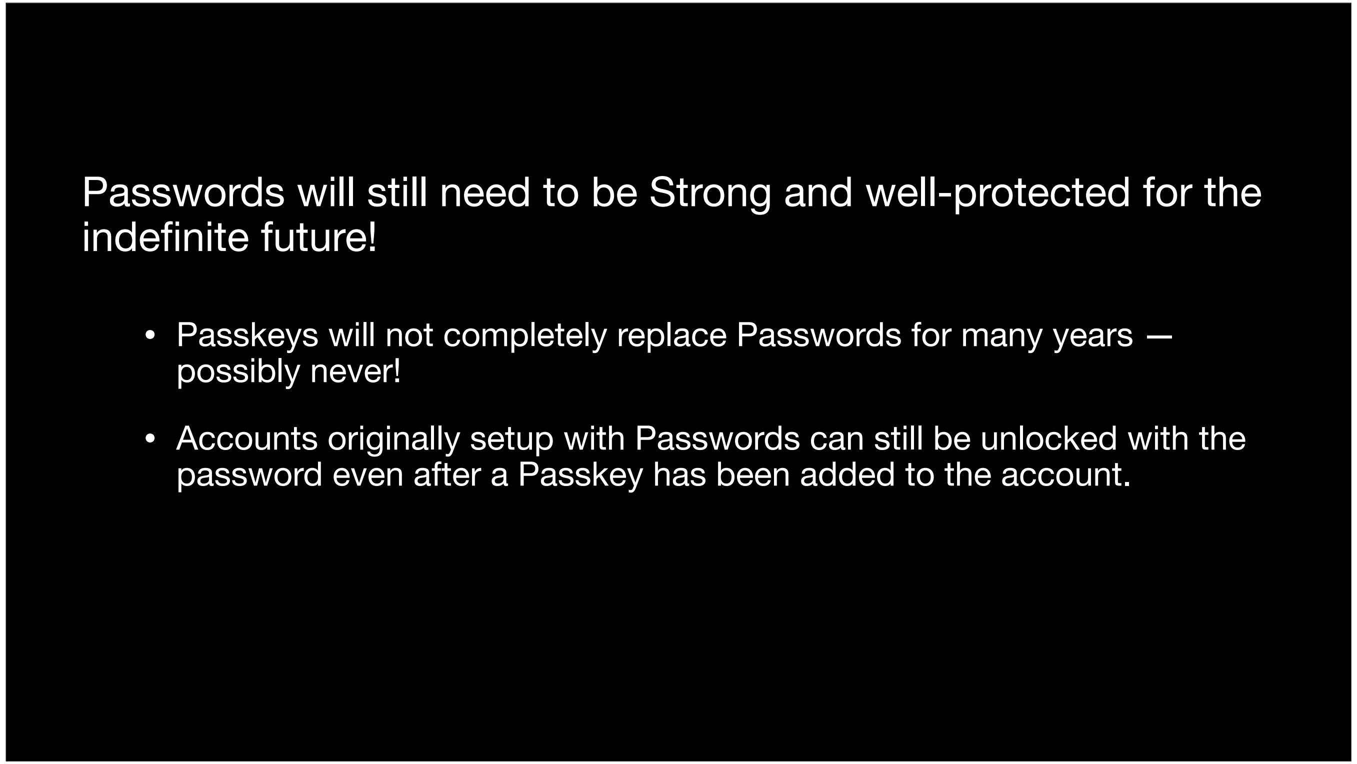
Here's a slide adapted from one of Apple's own developer sessions comparing the various methods of authenticating login credentials and how they compare for safety. Notice that simple password systems - both with and without a password manager - offer poor security. Adding 2FA with a One Time Pin doesn't change the types of attacks that can be used, though it does make such attacks harder to complete. Hardware Security Keys you must have with you improve security significantly but are inconvenient and risk loss or damage, and aren't recoverable. The current weakness of Passkeys is that some non-Apple devices don't work well with them yet - though that's already getting better in the last year.



Passwords will still need to be Strong and well-protected for the indefinite future!

- Passkeys will not completely replace Passwords for many years — possibly never!

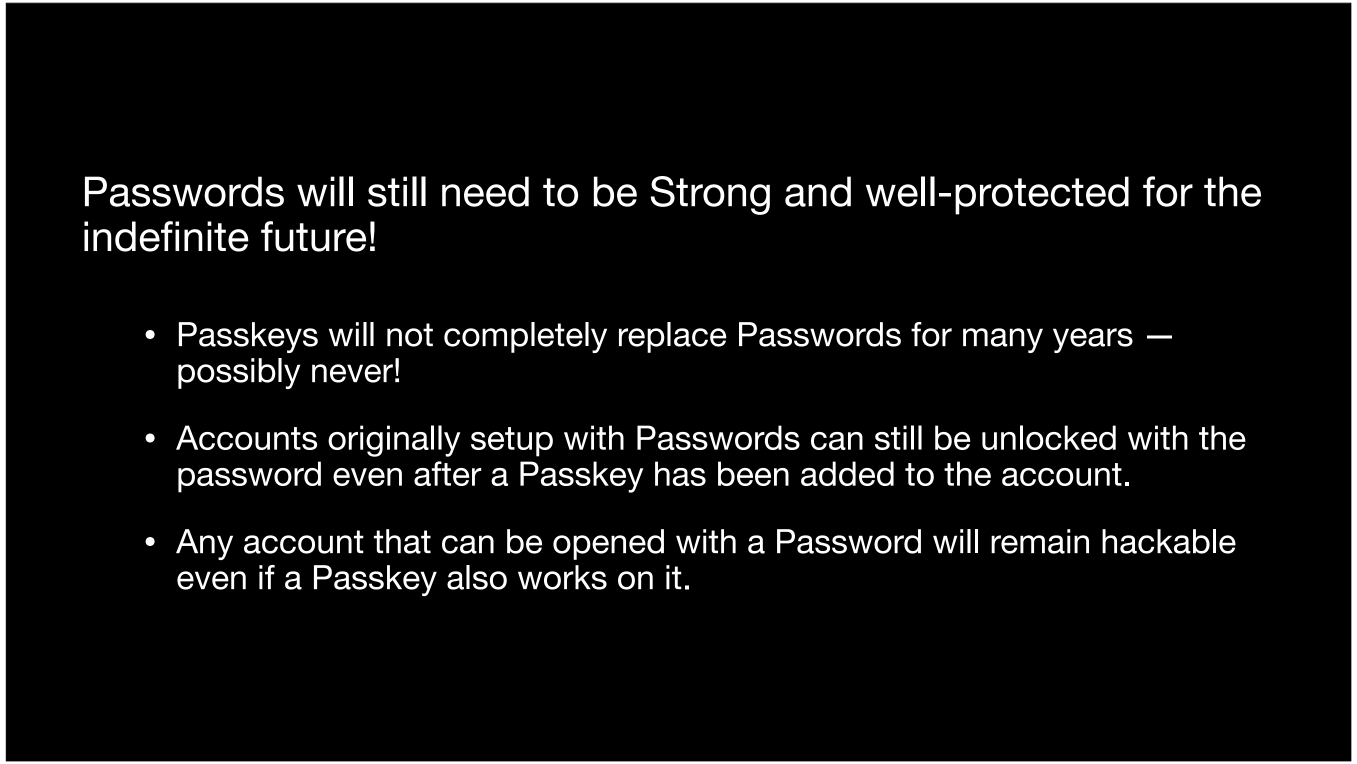
The FIDO Alliance behind Passkeys has been working on this for 10 years. They decided almost 3 years ago to begin the public roll-out for beta testing by developers. Apple began implementation in iOS 14, and made it fully-functional during iOS 15. Other FIDO members took longer but have gradually been offering Passkeys, and it’s now available to users of Apple, Google, Microsoft, Adobe, PayPal, Amazon, and others. The problem is that websites have been slow to recode login systems to work with Passkeys, so it still is not available in most places. At the current rate, another 5 years seems optimistic.



Passwords will still need to be Strong and well-protected for the indefinite future!

- Passkeys will not completely replace Passwords for many years — possibly never!
- Accounts originally setup with Passwords can still be unlocked with the password even after a Passkey has been added to the account.

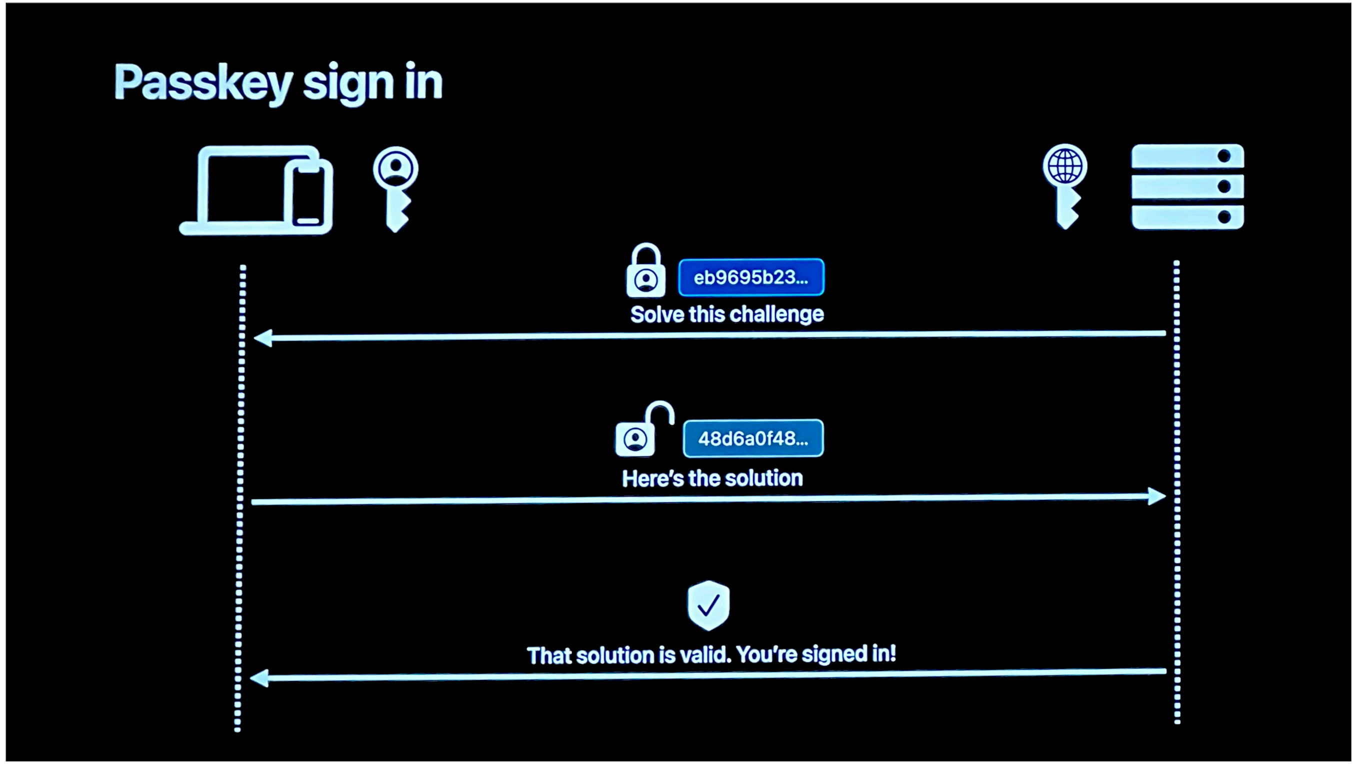
Meanwhile, nearly every account which can work with Passkeys was originally setup to work with passwords, and those passwords don’t simply quit working when you add a passkey to your account. That means that your password remains another way to get into your account even if you don’t use it ourself, so it remains just as susceptible to hacking attacks as ever until some day in the far far distant future when password systems are formally abandoned.



Passwords will still need to be Strong and well-protected for the indefinite future!

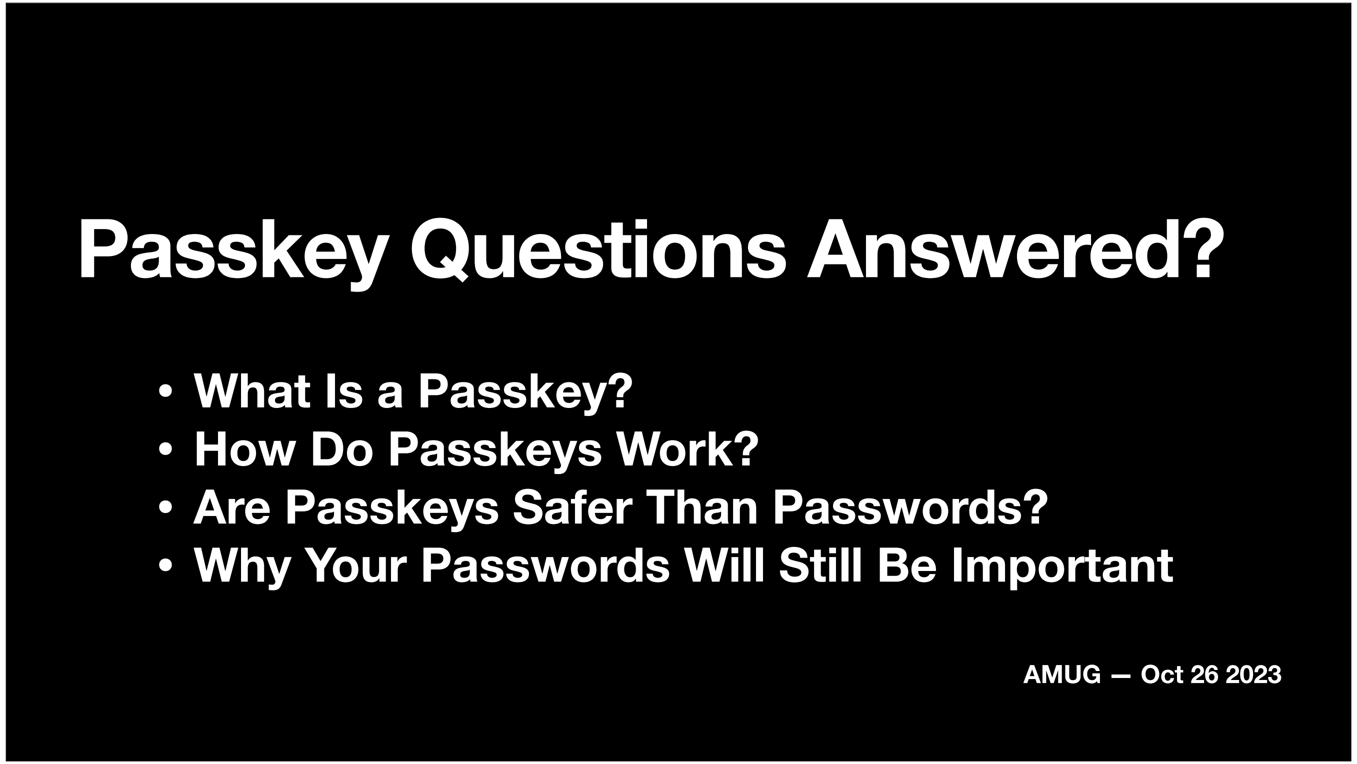
- Passkeys will not completely replace Passwords for many years — possibly never!
- Accounts originally setup with Passwords can still be unlocked with the password even after a Passkey has been added to the account.
- Any account that can be opened with a Password will remain hackable even if a Passkey also works on it.

Phishing will continue, Spam will continue, and your existing accounts with passwords will still need to be protected.
The main advantage of a Passkey is that you won’t have to actually enter your password anywhere that it might be exposed in the meantime, so you will know that any attempt to get you enter the password is probably a hack or phishing attack.



Passkey sign in

So just to review — Passkeys don’t store any login data on the account server - no password - so hacking the Server won’t reveal a way to login.
Both the Private and Public Keys are created by your device, with only the Public Key being sent to the Server when creating the account, and that key alone is incapable of triggering or decoding a login challenge. So even if it were stolen, it couldn’t be used to break into your account.
Passkeys can be stored in your iCloud Keychain and most other modern Password Managers, and used across all of your Apple devices, and even on some non-Apple systems. All we’re waiting for is that Systems Administrators implement Passkeys for the account systems we already use.



Passkey Questions Answered?

- What Is a Passkey?
- How Do Passkeys Work?
- Are Passkeys Safer Than Passwords?
- Why Your Passwords Will Still Be Important

AMUG — Oct 26 2023

I think we’ve answered the questions I intended — What is a passkey, how it works, whey they are safer than passwords, and why Passkeys — though far superior to passwords — are not going to be the Password-Killer that we’ve all heard talked about. At least not for many years to come.

Still, it’s time to improve our security where we can, so Passkeys are the best offer going - though the places offering them are still few and far between. I have roughly 120 digital account systems, and so far, only about 6 of them support Passkeys. It should keep getting better, but at least I can use them where possible and reduce the risk of those accounts being hacked.