Passkeys

What is a passkey?

- A replacement for traditional passwords

What's wrong with passwords?

- People don't always use different passwords for different accounts
- People don't always use strong passwords
- Hard to remember lots of strong passwords unless you use a password manager
- Possibility of passwords being 'stolen' from servers

How are passwords stolen?

- The actual passwords aren't stored on servers
- Hashes are stored instead
- A hash is the result of applying a mathematical function to the password
- Hashes can't be converted back into passwords, BUT...

How are passwords stolen?

- ... modern computing power means you can pre-calculate the hash for all possible passwords of a certain length and complexity in a reasonable time. Then if an intruder manages to steal the hash file, they can look up the password that corresponds to a given hash

- Dictionary-based attacks use and combine lists of words, including previously-hacked passwords and allowing for substitutions such as $ for S

- Phishing

- NB: This is a simplified description

So how do passkeys work?

- They are based on Public Key Cryptography (PKC)

How does PKC work?

- PKC is used in SSL/TLS and hence in HTTPS, so you already trust it
- Uses a private key (which only you know) and a public key (which you can tell anyone and everyone)
- These two keys are mathematically related, but it is (practically) impossible to determine one from the other.

So how does PKC work?

- I want to send you the message "HELLO"
- I encrypt this using your public key, giving (say) "d2785cfb7cb8c3c"
- You receive the message and decrypt using your private key, giving "HELLO"

So how do passkeys work?

- To create a passcode, you generate a pair of **public** and **private** keys, and send the public key to the server

- When you try to log in, the server generates a 'secret' (a random value, eg "ac7c91aac42105e") and encrypts this using your **public** key, giving (say) "12bef082c7bec37"

- Your device receives the message and decrypts it using your **private** key, giving "ac7c91aac42105e". It them re-encrypts that value using your **private** key, giving (say) "b7549a96457a9bd" and sends that back to the server

- The server decrypts that using your **public** key, giving the original secret

So why are passkeys better?

- They are built on standards that have been subject to extensive expert scrutiny
- Your password is not stored on the server, so it can't be stolen
- Your public key is stored on the server, but it is of no value to an attacker
- Your device manages passkeys, so you don't need a separate password manager (though some password managers do support passkeys)
- Your private key is stored securely on your device, eg in iCloud Keychain, or on a hardware key. NB: passkeys can be syncable or locked to a single device
- If you're using (eg) a friend's computer and you need to log in to a service using a passkey, there is a mechanism using QR codes to allow you to authorise the login from your iPhone or other device that has your passkey (using Bluetooth for added security)

But, but, but...

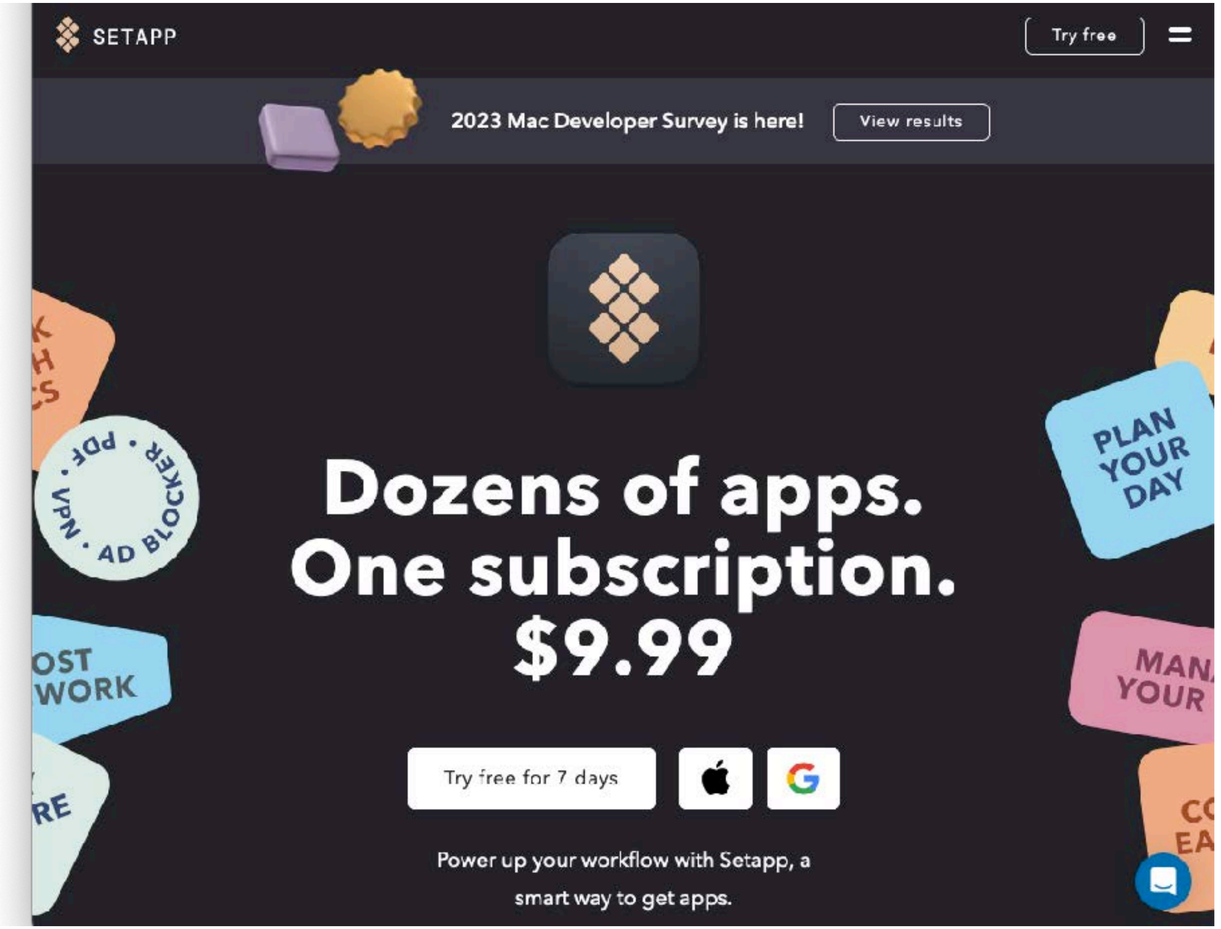
(hat tip to Ars Technica's Dan Goodin)

- **"I don't trust Google/Apple/whoever!"** Use whichever passkey software provider you do trust, and don't use passkey syncing. But if that's your objection, you probably shouldn't be using password syncing either

- **"How can passkey syncing be safe?"** The data representing your passkey is end-to-end encrypted, protecting it while in transit

- "**What if I lose my device(s)?"** In the short term, log in with your password and create a new passkey. In the longer term, you'll probably have to use the recovery code that was generated when you created the account

- "**What if someone uses my device?"** Depends on the scenario: either use biometrics to unlock your device (sneak thieves or 'friends'), or a complex passcode (muggers)


SETAPP
Try free
2023 Mac Developer Survey is here!
View results
Dozens of apps.
One subscription.
$9.99
Try free for 7 days
Power up your workflow with Setapp, a
smart way to get apps.
PDF · VPN · AD BLOCKER
PLAN YOUR DAY

SetApp

What is SetApp

- A subscription service that allows you to use more than 200 applications, mostly from smaller developers

Advantages

- Fairly affordable: $US9.99 a month for Mac, $US12.49 for Mac and iOS, $US14.99 for up to four Macs plus iOS
- Free trial
- Wide range of applications

The apps

- Too many to list here, but some of the better known inclusions are:

  Bartender, CleanMyMac X, iStat menus, Default Folder X, BusyCal, App Tamer, Disk Drill, RapidWeaver, Nitro PDF Pro, Get Backup Pro, and Capto

- An AUSOM member who is a Setapp subscriber pointed out how convenient it is to be able to see which of the apps in the catalogue are relevant to the task you're trying to perform, as opposed to having to learn what each app is capable of doing

All

Optimize

Work

Create

Develop

All apps

Top rated | New

Mac Apps | iOS Apps | Web Apps

DevUtils

Offline development toolkit

100% · Mac

PixelSnap

Measure anything on the screen

100% · Mac

Image2icon

Turn images into icons

100% · Mac

SnapMotion

Capture snaps from your videos

100% · Mac, iOS

Hype

Create animated HTML5 content

100% · Mac

Buildwatch

Track your build time in Xcode

100% · Mac

Goldie App

Measure golden ratio in designs

100% · Mac

Transloader

Start downloads on Mac remotely

100% · Mac

Mental Walk

Reflect on your life

100% · Mac

Launcher with Multiple Widgets

Customize your home

Bartender

Personalize your menu bar

CleanShot X

Take better screenshots and GIFs

Disadvantages

- As with all subscription services, you lose access to the apps when you stop paying