Will FIDO passkey help us to move on from Passwords?

Dario Salice - November 2022

I’m Dario Salice ...

Identity & Security Consultant

- Building a boutique consulting business around Security, Identity, and Product Management.
- 12+ years in Product Management roles including Google & Meta
- Board member of FIDO Alliance for 3 years
- 20+ years in Telecommunication and Information Technology.

dario@jenario.com

Overview / Agenda

- Let’s talk about passwords
- What is (a) passkey?
- How does it work?
- What’s the potential?
- Limitations?

When passwords used to be ok

- Jane and Bob needed physical access to the terminal in a secured office building
- Both of them only had one password to remember
- Simple tools to prevent them from brute-forcing each others passwords were feasible

The problem with passwords (Security & Access)

- They don’t offer sufficient protection
- They make it hard for us to access our data

- both depend on the user’s ability to make good decisions, manage their credentials , and be aware every time they click.

The problem with passwords: Security

- People use guessable passwords
- Passwords can get phished - sometimes in exchange of Amazon Giftcards
- People reuse passwords which puts them at risk if one platform gets breached
- Bad Actors can spell - give them more credit

24% of Americans have used a known weak password like abc123, admin, etc.

2 out of 3 people reuse their passwords across apps & sites.

22% of all data-breaches start with a successful phishing attempt

The problem with passwords: Access

- People struggle to manage all their passwords and tend to forget them
- Password policies increase friction for people to use their work tools
- Most Relying Parties experience significant churn when their users switch devices

75% of US users get frustrated with maintaining their passwords.

78% of people had to reset their password in the last three months.

What's passwordless?

Everyone talks about passwordless … what is it?

Passwordless login (event) - Using an authentication method other than a password - e.g through existing session, pre-registered authentication app, local biometrics.

- There's still a password that the bad actor can abuse

Passwordless accounts are account where there's no password that can be used for authentication.

What is Passkey (aka FIDO Multi-Device credentials)?

It's a digital FIDO Credential, tied to an account, that can be synced across devices

- Cryptographic entity using public and private keys
- Previously known as "Platform authenticators" to perform passwordless "reauthentication"
- Synchronization across devices using cloud keychain (e.g iCloud, Google Sync, etc.)

Passkey is meant to replace password-based authentication

The Passkey experience

What happened ?

Registration :

Foo-App
Hi Jennifer, do you want to use Passkey in the future?

YES

No

Foo-App
Passkey successfully registered. Enjoy using the Foo-App

iCloud KeyChain
Jennifer@foo - Passkey created

The Passkey experience

What happened ?

Passkey Login

New Device

Same iCloud account :

Foo-App
Do you want to use Passkey to log in?

YES

No

Foo-App
Login successful.

Enjoy using the Foo-App

iCloud KeyChain
Jennifer@foo - Passkey created

Where is Passkey supported?

(at this point - November 2022)

- Latest iOS, Safari, Mac OS, iPadOS released in Q3/2022

- Google ecosystem (Android, Chrome, ChromeOS) expected in Q4/22 -Q1/23
- Microsoft ecosystem (Windows, Edge) expected in H1/23

How Passkey will improve Security

A Passkey-based login …

… doesn’t include anything that can be guessed by a bad actor

… Can’t be phished or replicated by a “man-in-the-middle” attacker

… Can’t be re-used when compromising another identity-provider

These factors deterministically impact the attackers ability to perform their preferred ways to compromise accounts.

And reduce the user’s responsibility to make good password choices

How Passkey can reduce churn

Sign-in using Passkey has less friction, because …

… It doesn’t require people to remember passwords

… It doesn’t require dedicated authenticators (Hardware or Software)

… It makes credentials available across multiple devices and across apps (e.g native app and browser)

Cross-Platform login with Passkey?

Since Passkeys only move within their ecosystem (for now), Cross-Platform login flows are being launched.

Foo-App
Login

Username
Password

Use Passkey from other device

Foo-App
Login

Device with access to Foo-App Passkey

Foo-App
Login successful.

Do you want to use Passkey in the future?

YES

KeyChain
Jennifer@foo - No Passkey created

Phases of rolling out Passkey

Phase 1: Opportunistic rollout

Prompt people to register Passkey, where available.

Offer as preferred login option, when possible

Impact:
Increase #of Passkeys and Passkey-based logins → churn reduction

Phase 2: Reduce Trust in password-based logins

Change your risk-based policies or introduce deterministic challenges for password-logins that could be done using Passkey.

Impact:
Make password-compromise harder → compromise reduction

Phase 3: Remove password creation on sign-up (where possible)

Stop asking new users to create a password, where possible.

Impact:
Reduce # of accounts with a password → reduction of attack surface

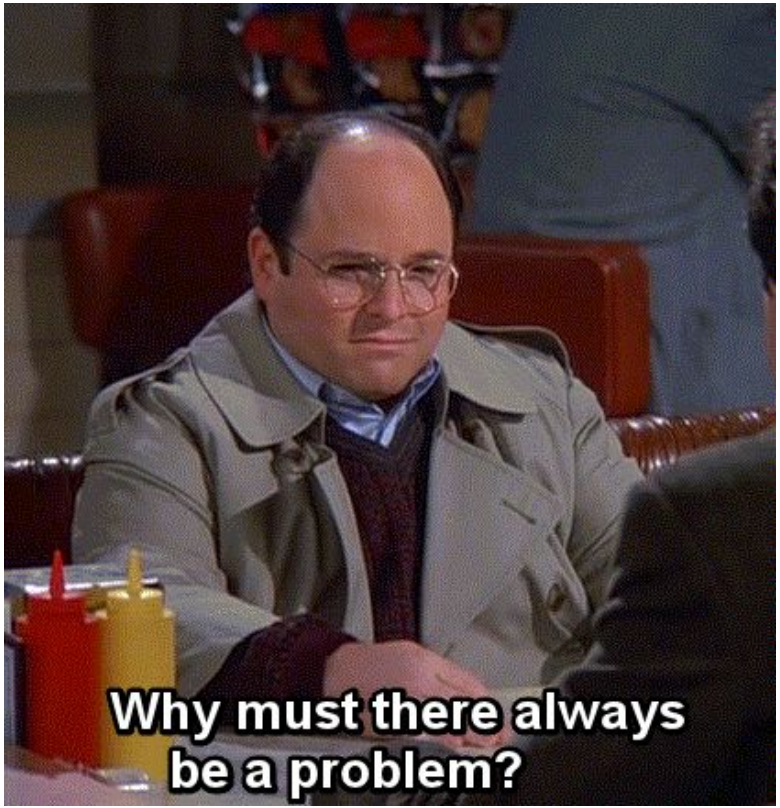
...

Phase n: 100% of accounts are passwordless

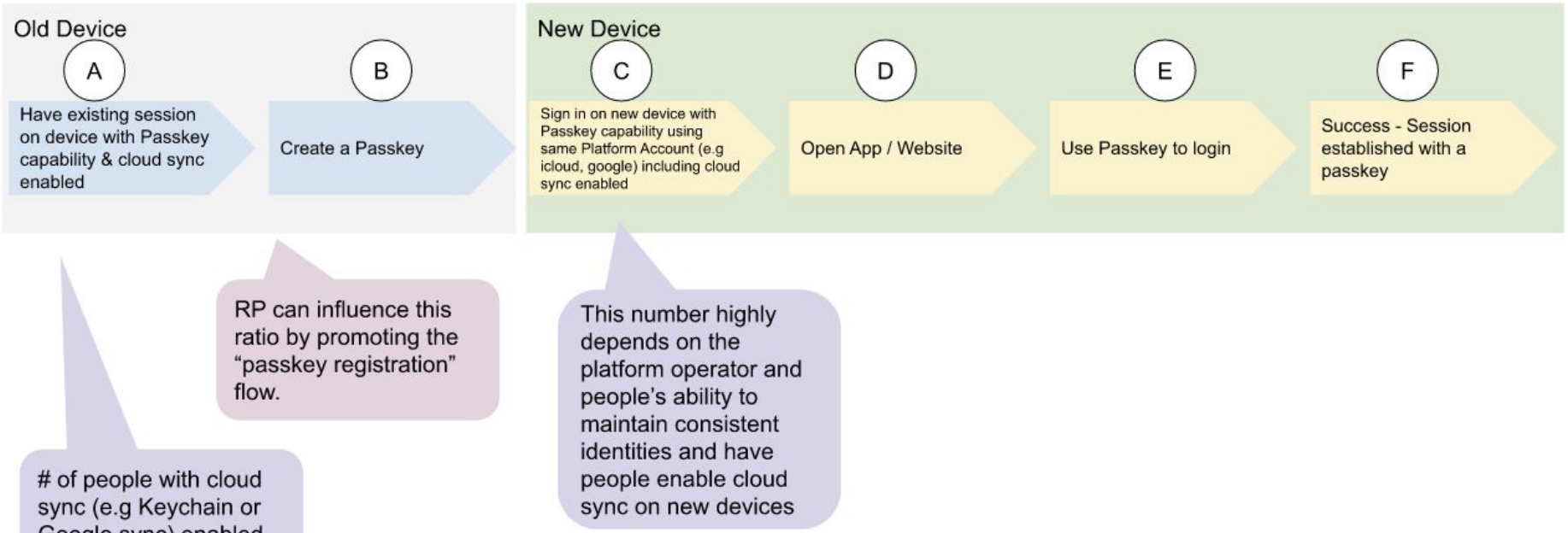
Deprecate passwords on all accounts and user-flows

Impact:
Reduce access-cost and attack-vectors

But ...



There's a but or two



There’s a but or two

- Passkey support is still limited
- Depends on continued use of platform accounts
- Adds scrutiny on platform accounts
- Some regulated use cases depend on Device-based credentials
- The issues of recovery are not solved
- Bad actors will transition to new attack vectors.

Questions & Discussion ...