**Moving From Passwords to Authenticators**

Submitted by :

Kavita

M.Sc. 1st year, DUCS

Passwords have been used by humans since ancient times. With the introduction of web and user accounts on the internet, these passwords naturally transitioned to the web.

Passwords are used to authenticate users across applications.

# Drawbacks of using Passwords

Suppose a user has multiple accounts across various applications. Maintaining these passwords itself is a tedious task. Hence, users use the same passwords across applications. Consequently, data breaches and hacks can be easily performed on such data which expose users across platforms and put enterprises at risk.

So, a simpler, stronger, user-friendly authentication method is required which accurately verifies the user’s identity and eliminates the risk of compromised credentials.

# Moving to Authenticators

The FIDO Alliance ( collection of companies supported secure and usable authentication) and W3C together make it possible to move from passwords to more secure modern authentication based on asymmetric cryptography.

W3C published specifications for browsers as a formal W3C recommendation called the *WebAuthn protocol*. FIDO published specifications for everything else as the *Client to Authenticator Protocol (CTAP).*

These two protocols together enable the password-less user experience.

# Working

To use the WebAuthn protocol, a user must have a client and an authenticator. Clients are browsers or mobile applications. An authenticator is a device that performs the cryptographic operations necessary for the WebAuthn protocol. Two core actions to be performed with an authenticator: Registration/Enrollment and Authentication

For example, In FIDO 2.0, a user can navigate to any website on a PC, receive a notification on his registered device (phone), and scan a fingerprint (one of the authenticators) via the phone's fingerprint sensor to log in. This user experience can be tailored to each person's unique preferences and constraints while maintaining a level of security far exceeding that which passwords offer.

# Benefits of WebAuthn Scheme

* **Memory wise-Effortless:** Some users prefer a PIN, while others prefer a biometric as an authenticator. If the user chooses a biometric, he need not remember any secret password.
* **Scalable-for-Users:** Because users can re-use the same phone and same second factor (PIN, fingerprint, etc.) across all relying parties, this is more scalable as compared to the passwords scheme.
* **Nothing-to-Carry:** If the user already carries a phone (as is increasingly the case), they don't need to carry anything else.
* **Infrequent Errors:** Using Biometrics is more reliable than using passwords. False rejects (when the authentication system rejects the correct person) were highest for password website log-ins and password laptop unlock— up to four times as high for websites than fingerprints or physical keys.

# Drawbacks of WebAuthn Scheme

* **Difficult-to-Upgrade:** Each time a user upgrade devices, for each relying party where he has registered an old authenticator, the user will need to log in, delete the old authenticator and register a new one manually. One solution is to use the *Transfer Access Protocol* to upgrade devices.
* **Difficult-to-Recover:** If a user has lost his registered device, then the WebAuthn scheme makes it difficult to recover his account access. The solution is the *Preemptively Synced Keys (PSK) Protocol*, it uses a second device called a “backup device” (but the user needs not to register manually from the backup device).

# Future Work:

# 

The ratio of passwordless authenticator users is increasing day by day. It is the task of companies to encourage a passwordless world to reduce cyber attacks.