DEMYSTIFYING FIDO2:

THE GROWING ALTERNATIVE TO PASSWORDS

FIDO, CAN YOU PLEASE AUTHENTICATE ME? GOOD DOG.

For years, experts have been predicting the demise of the lowly password. This is not because they knew how to do away with them, but only because they said we have no choice. We've heard the complaints endlessly. Passwords are the common vector to account takeovers and identity theft. Lazy people employ passwords that are too easy to guess or uncover. Strong passwords are easy to forget. Legit users regularly forget not only their own passwords, but even the answers to their own security questions. Hilariously enough, a well-known politician's email was broken into by an enterprising soul who clicked on her "forgot password" link and found that the answers to her security questions were all easily Googled.

Substitutes or augmentations for passwords have existed for decades, things such as hard tokens that are costly, as well as difficult to distribute, track, and manage. There are still legit use cases for these, but again, they come with baggage, for both the enterprise as well as the individual user.

Passwords really do have to take a step aside, or at least be supplemented by something that can add an extra layer of security against cyber-criminals. But that something needs to be easy to deploy by organizations and easy to use by their constituents. Biometrics have stepped in, by way of face, voice, and fingerprint, but these are usually limited to a single device, which limits their use in cross-platform, cross-device environments.

For the sake of security, for the sake of single sign-on across those environments, for the sake of unburdening users from those troublesome passwords, we now have FIDO.

FIDO, or Fast ID Online, is one of those acronyms that is perhaps easier to pronounce than it is to understand. Before most people have come to comprehend what it provides, we've already come to FIDO2, the next generation of this passwordless specification for registering and validating user accounts. FIDO2 simplifies the experience for users who don't need to remember and use passwords, and IT staff who subsequently don't need to manage those passwords.

It's not enough to simply say "passwordless," of course. What takes the place of passwords with FIDO, and how much work is required? There are many specifications and protocols that promise a blueprint for account creation and management, but the devil is in the details, which often involve the ease of deployment (or lack thereof). Various security protocols do not get adopted, even when they are required for compliance purposes, simply because they are too hard to put into practice.

But the ease of use of a FIDO2 platform cradles users in a safe, secure, seamless environment, which then promotes adoption. In this way, FIDO is one of the more well-thought-out approaches to user access.

WHAT ARE THE BENEFITS OF FIDO?

Within a FIDO2 flow, a user can make use of a common device for accessing online sites, integrating both desktop and mobile formats. This access starts with first creating credentials, then leveraging them day after day.

If you've ever been to an identity / access (IAM) trade show, you likely saw the kiosks manned by the FIDO Alliance crew, an industry association working to reduce reliance on easily-compromised passwords, mainly through the use of device and biometric. Their mandate is education about how a FIDO-powered platform provides registration, authentication, privacy protection, and even account recovery. But while you're waiting to fly to the next industry event and hear what they have to say, let's illuminate the way the FIDO2 specification enables the entire user lifecycle in a seamless, password-free environment. And let's do it as simply and painlessly as possible.

REGISTRATION

A user begins their lifecycle in a FIDO format by first registering. This involves choosing an Authenticator that is supported by a target online service. In other words, you want to access my features? Here are the authentication methods I accept. Examples of Authenticators are facial ID, fingerprint, or Windows Hello.

The capabilities of these methods are supported by a personal device, along with an optional biometric. The user's own device creates a pair of keys, the private one it retains and a public one that is registered with the desired online service. The key pair is unique to the user's account, the user's device, and the chosen service. The private key, along with any data related to the auth method, are secured on that device.

AUTHENTICATION

Now that the user is registered, they can authenticate day to day. For example, they pull up the online service they've registered for, which challenges for credentials. The user unlocks the Authenticator on their previously-registered device by fingerprint, PIN, voice, or facial, typically the same method used for the original registration.

The device leverages the user's account identifier to select the user's key and responds to the challenge. The device then returns the signed challenge to the service, which validates it against the public key it holds and authenticates the user.

To greatly simplify all that: the device proves possession of the private key by signing the challenge from the site.

RECOVERY

Even having control of the authenticating device is no guarantee against account takeover if there are other means of accessing or compromising that account. The use of multiple Authenticators allows a user to authenticate through backup means in the event of takeover. Users also have the option to register a FIDO Security Key as a backup Authenticator for all their accounts.

Just as an online service has registration requirements, it will likely have requirements for identity proofing if a user needs reclaim their account. Through a backup Authenticator, a user may have an avenue to access an identity proofing scheme and undo the takeover, such as resetting a password or PIN.

When a device is lost or must be replaced, FIDO allows for the use of passkeys (described below) to still access their credentials and therefore their access to critical systems.

SECURITY, PRIVACY, CONTROL, EASE OF IMPLEMENTATION

FIDO2 remain safely on the user's device, are not stored in the cloud, and are unique across systems. Because of this, phishing is eliminated, as are replay/eavesdropping attacks. In this way, FIDO greatly reduces the surface area in which cyber-thieves can operate against a user, who alone can access their device, their Authenticator, and their personal biometrics.

User privacy is also protected, since Fido keys are unique for each registered site, and therefore users cannot be tracked across multiple sites.

Based on open standards, FIDO2 can be easily enabled across all major browsers and platforms, by use of a simple Javascript call, making for ease of deployment. Likewise, ease of use trickles down to the user, who access their credentials via fingerprint, voice, or face, or by leveraging FIDO security keys. This gives users a wide choice of devices. FIDO2 has overcome its early issues with compatibility, and now plays nicely with all major web browsers, as well as Windows 10 and Android. Neither Mac nor iOS support FIDO2, but Safari does. Physical security keys are available that work with various FIDO2-certified devices and authentication services.

FIDO (PASSKEYS) AS UNIVERSAL BRIDGE

For decades, there have been single sign-on (SSO) schemes and vendors. And the same problem exists in the present day as then: they don't always speak to each other. While SAML and other protocols have made some tokens and passports portable, that is not always the case, especially in the case of critical or sensitive sites and services.

Based on FIDO standards, passkeys are a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices. Unlike passwords, passkeys are always strong and phishing-resistant.

Passkeys simplify account registration for apps and websites, are easy to use, work across most of a user's devices, and even work on other devices within physical proximity.

FIDO-based authentication can be accomplished across devices and sites using passkeys, an authentication method that eliminate the need for phishing-prone usernames and passwords. Passkeys enable users to leverage their FIDO credentials without the need to register (or re-register) each and every device. Device-specific passkeys can also be bound to a FIDO security key, although unbound passkeys are useful when a user has lost or must replace their physical device. Users can leverage the same PIN or biometric used in unlocking their devices for approving their login, again without the usual name/password combination.

This portability allows users to leverage the flexibility and security of FIDO across sites and devices, making it the perfect bridge in corporate environments where authentication methods are not compatible between systems.

SO WHAT'S THE CATCH?

FIDO2 obviously requires an extra step in setting up your multi-factor authentication. But a few extra seconds of prep on Day Zero, in order to secure and enable an easy form of authentication from Day 1 to Day n, are a logical trade-off. Protection from phishing, man-in-the-middle attacks, credential stuffing, and other standard forms of cyber-theft is a powerful, collateral effect of implementing FIDO2. More and more sites, every single day, are becoming FIDO-enabled, and organizations with large numbers of corporate apps leverage FIDO2 for the protection from their own users' mistakes (such as clicking on those malevolent links) as well as ease of use for their employees and customers.

OUR PASSWORDLESS FUTURE IS NOW

As previously stated, there are many so-called "standards," most of them acronyms that end with "ML," that are bounced around by those same experts, yet those standards are not widely implemented, because no viable consortium has sponsored them, or because of their unrealistic approach to actual deployment. These weaknesses render them largely ineffective and impractical. But FIDO2 has widespread adoption, as evidenced by the many vendors who build to the specification, and the major platforms that now support it.

FIDO2 presents a clear path to operational success, with obvious benefits to both the enterprise and the enterprise user. If passwords are not completely dead, they are possibly on their way to obsolescence, and most definitely to a diminished role, particularly in corporate ecosystems. Simplified infrastructures, streamlined user experience, and increased security and privacy are all powerful advantages to FIDO2.