What Are the Latest Developments for a Strong Passwordless Authentication?

Anastasios Arampatzis, Homo Digitalis

Corporate and personal data are being stored in distributed cloud platforms at a growing rate due to the acceleration of digital transformation across all industries and sectors, increased adoption of cloud-based technologies, and hybrid work norms. Many entities, including apps, organizations, people, devices, etc., have access to this data.

Traditional security measures are no longer sufficient to safeguard our data because traditional brick-and-mortar company borders have shrunk. Identity has become the new castle to guard, yet new security issues are associated with identity protection. To counter this tendency, businesses are investing in enhancing their access controls, switching to a zero-trust cybersecurity approach, and maximizing the effectiveness of multi-factor authentication (MFA).

What is MFA?

A solid access management policy must include MFA as a critical component. MFA is essential in limiting attackers' ability to steal our digital identities and access our systems. MFA demands one or more extra verification elements in addition to a username and password, which lessens the possibility of a successful cyber-attack.

What is MFA fatigue?

There are crucial implementation elements that can affect the security and usability of an MFA deployment, and it is essential to remember that not all MFA solutions offer equal protection against authentication attacks. Due to flaws in the MFA implementation, we have seen numerous attacks over the previous two years when thieves could get around the MFA protection.

In such attacks, also known as push bombing or MFA fatigue, cybercriminals bombard unsuspecting targets with mobile push alerts requesting them to accept attempts to enter their corporate accounts using stolen credentials. The victims often give in to the malicious MFA push requests sent repeatedly, either unintentionally or in an effort to stop receiving what seems like an endless stream of alerts, allowing the attackers to log into their accounts.

What are the latest developments in access control?

To mitigate the MFA attacks, tech giants Google and Microsoft have recently announced two initiatives that push toward a more secure and even passwordless future. Let’s examine what these developments are.

Google takes a step toward a passwordless future.

The tech giant recently launched passkeys, a type of digital credential, as an option to generate and use in place of passwords as a safer, more practical alternative.

What are passkeys?

Passkeys are created using public-key cryptography, also known as asymmetric encryption, which uses a set of private and public keys. The private key, a crucial part of the passkey, is kept on the device, while the public key is held on the side of the app or website. The passkey's value is not accessible to websites. Google

determines whether a website's public key corresponds to the passkey the user uses to log into their account.

Unlike a password, this authentication approach dramatically increases the resilience of accounts because the key cannot be stolen from the website it is stored on, phished, or intercepted in transit. Additionally, the account cannot be attacked due to a weak password or password reuse since there is no password.

Figure 1: Google Passkeys (Source: Google)

As Google noted in their announcement:

"Using passwords puts a lot of responsibility on users. Choosing strong passwords and remembering them across various accounts can be hard. In addition, even the most savvy users are often misled into giving them up during phishing attempts. 2SV (2FA/MFA) helps, but again puts strain on the user with additional, unwanted friction and still doesn't fully protect against phishing attacks and targeted attacks like 'SIM swaps' for SMS verification. Passkeys help address all these issues."

Passkeys utilize the three forms of information that are used frequently in MFA: something you have (such as a smartphone), something you are (such as your biometrics), or something you know (such as a PIN or pattern). Although passkeys qualify as a type of MFA, the FIDO Alliance claims that several regulatory organizations still need to acknowledge this, even though they are actively striving to do so.

It would be best not to create a passkey on the shared computer at your place of business since passkeys should only be established on devices you individually control. Google stated that passkeys for employee sign-ins would be enabled by Workspace account managers "soon." As anyone using the device could access your Google account, you shouldn't create one on shared devices like your family computer. Once a passkey is generated on that device, anyone who can unlock it can sign back into your account using the passkey, even if you have logged out.

Microsoft hardens MFA with number matching.

Microsoft announced they would start enforcing number matching for Microsoft Authenticator MFA alerts to block MFA fatigue attack attempts.

“Beginning May 8, 2023, number matching is enabled for all Authenticator push notifications. As relevant services deploy, users worldwide who are enabled for Authenticator push notifications will begin to see number matching in their approval requests,” reads the company’s announcement.

What is number matching?

Number matching is a setting that forces the user to enter numbers displayed in the platform where they try to authenticate into their authenticator app to approve the request, explains the US Cybersecurity and Infrastructure Security Agency (CISA).

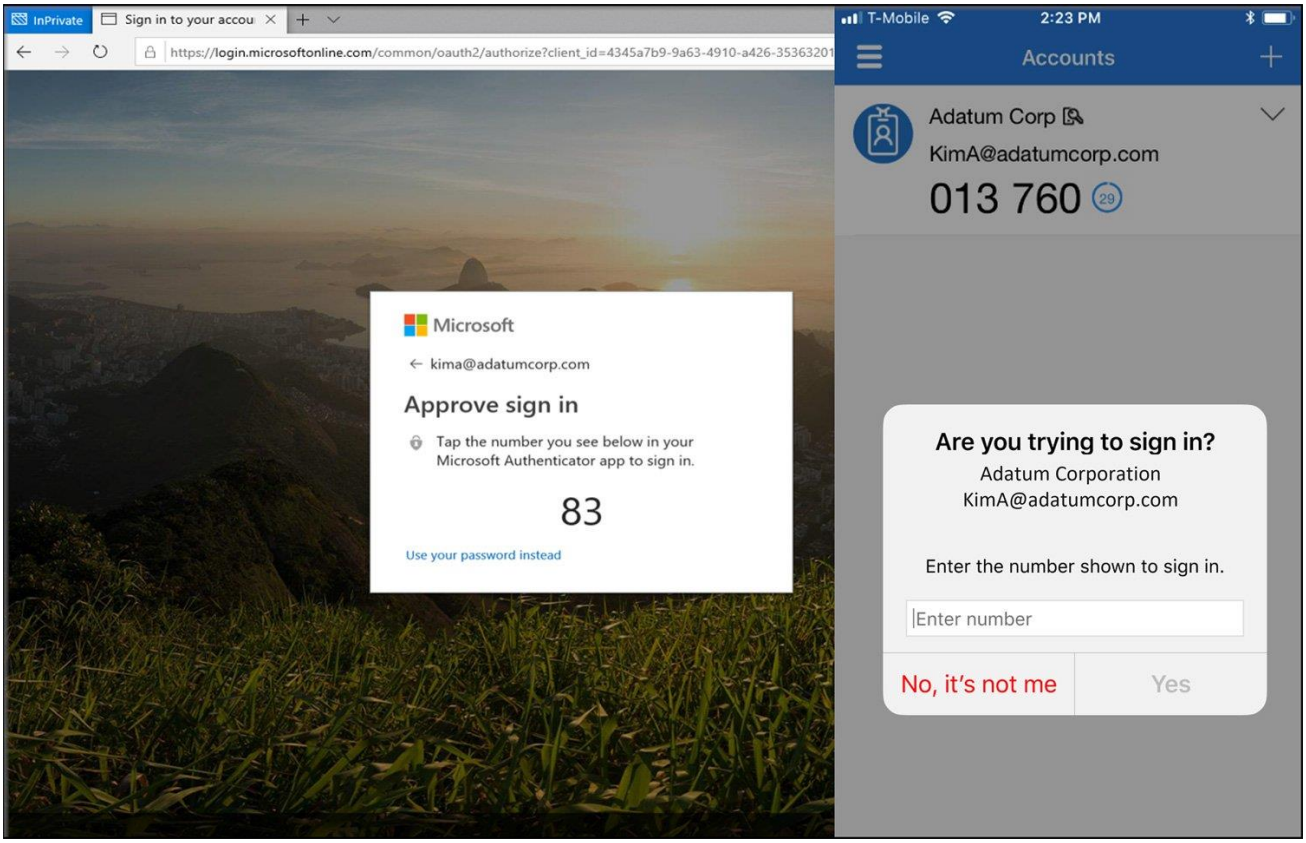

Figure 2: Number Matching. Source: Microsoft

The number-matching requirement reduces MFA fatigue by needing access to the login screen to authorize requests. When users use Microsoft Authenticator to respond to an MFA push message, they will see a number. To complete the approval, they must enter that number into the app. Users cannot approve requests without the numbers being entered on the login screen.

"Number matching is a key security upgrade to traditional second-factor notifications in Microsoft Authenticator. We will remove the admin controls and enforce the number match experience tenant-wide for all Microsoft Authenticator push notifications users starting May 8, 2023," Microsoft says.

If you want to learn more about multi-factor authentication and how your organization can successfully and effectively deploy MFA, download our latest paper, “Selecting A Multi-Factor Authentication Solution: How to Address the Human and Technology Concerns.”