Password Versus Passwordless Authentication:

What Is Better for Organizations?

Mark Malinowski

Department of Cybersecurity, Excelsior University

Author Note

This paper was originally prepared as the capstone project for CYS 596: Capstone Project in Cybersecurity at Excelsior University and submitted on December 6, 2023. It has been edited for style and APA formatting for inclusion in a writing portfolio; the argument and structure are those of the original paper, and a few sources were corrected, updated, or replaced.

Abstract

Over the past 30 years, exponential technological advancements have made the world more accessible, enabling everyone to remain connected at all times and giving almost everyone small computers in the form of cell phones at their fingertips to do virtually any task. With the technological boom came a need to secure personal accounts with a password; however, with emerging technology, a new wave of security has emerged in the form of passwordless authentication using biometrics and other multifactor authentication methods. This paper examines passwords and passwordless authentication by comparing both authentication methods in terms of security, ease of use, implementation cost, and user adoption, and it provides an informed opinion on which is better for individuals and organizations. The paper concludes that, despite implementation costs and upfront work, the security and ease-of-use advantages of passwordless solutions outweigh the continued use of passwords.

Keywords: authentication, biometrics, multifactor authentication, passwordless authentication, passwords

Password Versus Passwordless Authentication: What Is Better for Organizations?

Forgotten and mistyped passwords are a common problem for users who have too many passwords to remember. The average person has approximately 100 passwords, and that number increased by 25% between 2019 and 2020 (Rowe, 2023). Passwords date back to the Roman army, which used phrases called "watchwords" to verify that soldiers trying to gain access to camp were Roman (Dashlane, 2023). Passwords can be effective. However, they are no longer the only way to authenticate one's identity. Passwords have become another option rather than a requirement. Now, there is a new method to authenticate users: passwordless authentication. Some companies even offer the ability for users to rid themselves of passwords altogether. Microsoft now offers the ability to move away from passwords and use two-factor authentication (2FA) or multifactor authentication (MFA) for account access (Taylor, 2023). Passwordless authentication uses concepts like MFA to verify one's identity. Nevertheless, whether it is a better solution than passwords is subjective and specific to the user or organization. For organizations, the decision depends on weighing security risk, implementation cost, and user adoption. This paper deepens the understanding of passwordless technology, compares passwordless authentication and passwords, discusses convenience, and provides real-world cases for using passwordless authentication to inform that decision.

Overview of Passwordless Technology

In this paper, *passwordless* refers to any authentication method that does not involve a password to gain access to an account or service. Passwordless technology is a modernized way to address new and emerging security threats. As society and technology continue to move rapidly toward a more digital ecosystem, security must outpace technology to ensure confidentiality, integrity, and availability for all users and organizations. Furthermore,

passwordless authentication is a mechanism to drive the effort of security pacing. Lastly, passwordless technology is not a new solution.

There has been a strong enough use case in the past to drive the need to shift from passwords to 2FA and MFA. The case was so strong that the United States Department of Defense (DoD) moved away from passwords as a means of authentication due to the inherent security weaknesses that passwords present. Daily, military members log in to work systems through a 2FA method and sometimes MFA for more sensitive systems. For example, the military identification card doubles as a network access card and is called a Common Access Card (CAC), which is used to log in to unclassified systems. The CAC has DoD encryption, signature, and Personal Identity Verification (PIV) security certificates. Additionally, the CAC requires the user to possess the CAC and know a six- to eight-digit personal identification number (PIN) to gain access (U.S. Department of Defense, n.d.). The private sector has begun implementing passwordless authentication, similar to the DoD's efforts.

Passwordless Authentication Methods

There are many commercially available passwordless solutions for the average user. Some of the methods for authentication without a password are using an authenticator app that delivers a one-time PIN through Google Authenticator or Microsoft's solution; there are many other authenticator solutions, but those two are the more prevalent solutions on the market presently. The authenticator application is stored on the user's mobile phone. To log in, the user must possess the phone, unlock the phone through a PIN, Face ID, or Touch ID, and open the authentication application using another PIN or biometric ID like a fingerprint. Furthermore, many different vendors and websites use passwordless technology like those solutions. Aside from authentication applications, biometric passwordless technology is widely used.

Fingerprint Authentication

Fingerprint authentication is another form of biometric authentication that is still widely available to the public. Fingerprint authentication for mobile authentication has existed for over a decade and was wildly popular five years ago (Thales Group, 2023). However, with the invention of mechanisms like Face ID and iris recognition, fingerprint ID is slowly fading away, which is not a loss from a security standpoint. According to researchers at the New York University (NYU) Tandon School of Engineering and Michigan State University, fingerprint identification technology is not without issues. When setting up fingerprints on the phone, a user may be asked to supply partial prints, and the phone can then be unlocked mistakenly by others or deliberately by nefarious actors; the issue is that the fingerprint reader only reads a small section of the print versus its entirety, making it less secure (NYU Tandon School of Engineering, 2017).

Facial Recognition

Facial recognition has an overwhelming presence in the mobile phone industry and some of the defense industries. Apple popularized facial recognition on mobile phones with Face ID. It is incredibly convenient and works efficiently. Cell phone users look at the screen, and it unlocks their phone. Additionally, places like airports use facial recognition for authentication (Sumra, 2019). CLEAR, a private company with lanes at Transportation Security Administration (TSA) security checkpoints, uses facial recognition that moves travelers through security quickly without needing to pull out a physical identification card (CLEAR, n.d.). Despite all the convenience of facial identification, it has its drawbacks.

While facial identification is convenient, users must decide whether they trust that companies adequately store their biometric data (Sumra, 2019). This concern was evident in the

Office of Personnel Management (OPM) data breach. Unknown attackers successfully exfiltrated biometric data for millions of government workers (Committee on Oversight and Government Reform, 2016). Since attackers successfully exfiltrated biometric data from the U.S. government, it raises the question of whether biometric data are safe on a mobile device. Apple states that Face ID data do not leave the device and are never backed up to iCloud (Apple, 2026). It is unsettling to think of biometric data hacking because a user cannot simply reset their biometric features like they can a password.

YubiKey by Yubico

The YubiKey is a hardware key used to authenticate enterprise and individual user accounts (Gillis, 2023). YubiKey allows users to authenticate using near-field communication (NFC) and fingerprint ID or PIN and acts as a physical item a user possesses to log in.

One-Time PINs

One-time PINs (OTPs) are incredibly useful when correctly implemented for 2FA or MFA. Currently, many financial institutions like Wells Fargo use an OTP in tandem with other means of authentication (Wells Fargo, n.d.). To use an OTP, a user logs in and receives a text message or email with a four- to eight-digit PIN. Upon receipt, the user must input the same PIN to access the system. Usually, the PIN is only effective for a limited time; if the user surpasses the allotted time, they must request a new OTP.

Voice Biometrics

Voice printing is another form of biometric authentication used by financial institutions and other organizations. The customer or requestor can typically do this independently and over the phone. The speech print software takes samples of the person’s voice and analyzes the unique

patterns specific to the person. A person's voice patterns are incredibly unique, much like a fingerprint (Shoup et al., 2016).

Benefits of Passwordless Technology

Passwordless technology seems like an obvious choice to some. There are many benefits for users and organizations that want to bolster security and enhance the usability of work systems. Some of the benefits of passwordless technology include security and ease of use. The following sections discuss how these benefits improve the user experience from a security and ease-of-use perspective.

Passwordless Technology Benefit: Security

The security built into passwordless technology is strong and proven. For example, using YubiKeys is an excellent way for organizations and users to improve their security and protect their organizations. YubiKeys have built-in 2FA capabilities. A YubiKey is something the user must physically possess, combined with a fingerprint and/or a one-time PIN. Furthermore, YubiKeys eliminate the need for passwords.

Passwordless Technology Benefit: Ease of Use

Passwordless technology makes it easier to access systems and is usually faster than using a password. For example, with Apple's passkey service, the user points their camera at a QR code, executes biometric authentication with Face ID, and then accesses the account or system. Besides passkeys, physical keys are easy and fast. Additionally, the YubiKey, a physical key, is quite simple. After the user associates the YubiKey with their account credentials, the user must physically have the key, insert or tap it, and use their fingerprint to gain access and accomplish 2FA measures. Finding a system that is easier and more secure than that would be difficult. Lastly, reading emails is more accessible because users are less concerned about

phishing attempts. Protective measures like YubiKeys make it nearly impossible to steal a password since it is a physical device that requires possession, biometrics, and a PIN or authenticator application (Yubico, 2023).

Social Aspect of Using Passwordless Solutions

Focusing only on their technological aspects when discussing passwordless solutions and technology is easy, but there is more to consider between passwordless versus password authentication. Another aspect people, employees, and employers must recognize is the social aspect of going passwordless, which stems from generational differences. Furthermore, Millennials are a generation that grew up in the connected world and used technology most, if not all, of their lives. Considering that, it would be reasonable to believe they are well-versed in cyber and password hygiene, but the data say otherwise. According to a 2023 ManageEngine survey, Millennials are more likely than other generations to reuse passwords across accounts, connect work devices to public Wi-Fi, and open links from unknown senders (Donegan, 2023).

The research established that Millennials are less likely to be cyber-savvy, but hope exists. Despite their lack of cyber hygiene, Millennials are more apt and willing to use passwordless technology solutions and abandon passwords (Markey, 2023). They are open to biometrics, 2FA, and other means. Conversely, older generations are less likely to want to use biometrics and prefer traditional authentication experiences (Markey, 2023). Finally, Generation Z, the generation younger than Millennials, values convenience and seamless login experiences, which are both demonstrated advantages of passwordless authentication solutions (Markey, 2023).

Password Versus Passwordless Comparison

Comparing passwords and passwordless authentication is no easy task. Each authentication mechanism has its distinct benefits (Bonneau et al., 2012). Considering how a user or organization would implement, use, and maintain passwords is significant and warrants further discussion.

Password and Passwordless Implementation

Password-based solutions are relatively easy and cheap to implement because they have been around for a long time. Since passwords have been around for some time, they are easily accepted by many individuals who make up multiple generations of users. Additionally, passwords are easy to implement if the organization or administrators set strict password complexity requirements and integrate a robust cybersecurity training program that discusses user best practices for maintaining passwords. This training should include the importance of not sharing passwords, not writing passwords down, and making them difficult for others to guess by making them lengthy and complex with numbers, letters, symbols, and different-cased letters. Conversely, passwordless technology is not as simple to implement.

While passwordless technology has advantages, it is more expensive than passwords in some respects and involves learning something new (Bonneau et al., 2012). Another drawback of passwordless technology that must be considered is the human instinct to avoid change or the unknown. Some measures like YubiKey or Apple passkeys are relatively new. Since they are new, there is a chance that some people will become resistant to using passwordless solutions. It is well known that it is not easy to “teach a dog a new trick,” especially when that new trick involves a sensitive topic like authentication and abandoning a password. Furthermore, YubiKey is a popular solution for employers to secure their employees’ account access. However,

employees are humans who are susceptible to making mistakes. One mistake that is easy to make is losing a physical device like a YubiKey. The cost of a YubiKey ranges from about $29 to $98, depending on the model and the company's and its employees' needs (Yubico, n.d.). Resetting a password only costs a system administrator's time, but a YubiKey costs time and money to set up.

Password Vulnerabilities

Passwords have merit, and it is easy to justify their use. However, they are still a less secure means of preventing access to sensitive information or computer systems. There are a few reasons why they can be less secure. Passwords involve a human element, must be changed regularly, and require a complexity that someone can recall quickly, and they must not be reused on multiple devices or accounts.

Since humans have different degrees of technical acumen, making an effective password can be incredibly challenging. This challenge becomes relevant when directing users to make and maintain their passwords. According to Boston University (2023), a strong password is a passphrase of 16 characters or more that uses a mix of uppercase, lowercase, symbols, and numbers. As previously mentioned, the average person has approximately 100 passwords, so adding another into the equation invites a user to reuse a password from another account or write down their password and store it in an unsecured manner, thus defeating the purpose of having a password. Furthermore, a weak password that is improperly developed or stored, as mentioned above, compounds the weakness. According to IT Governance, weak and stolen credentials are among the most common causes of data breaches (Irwin, 2022). Lastly, attackers can perform a variety of remote attacks on passwords that compromise account security (University of Texas at Austin Information Security Office, 2023). These attacks make it incredibly challenging for a

user and detract from user and organizational objectives. Some remote password attacks include brute-force attacks, where the attacker tries to guess a user password, and phishing attacks, where attackers try to obtain login information through malicious emails. Other attacks include man-in-the-middle attacks, where an attacker obtains login information when a user inputs their credentials while connected to an unsecured network, and keyloggers that track and send every keystroke to the attacker; keyloggers are usually attributed to poor computer security practices like installing malicious software (OneLogin, 2023).

Password-Based Versus Passwordless Authentication User Experience

Password-based authentication is something that most users are accustomed to, and for most, it is nothing new. The user and system administration team make a username and password to allow access to systems and services. Based on system and group policies, the account's password must be changed regularly to maintain password security. Additionally, as discussed previously, the user must remember their password to prevent password resets. Password resets are common practice, but memorizing passwords for dozens of accounts using a password manager can become frustrating. Furthermore, having to change dozens of passwords and recall those updated passwords can become aggravating for users.

Passwordless authentication is a bit easier to use because it relies on something the user has, like a CAC, a key, a passkey, or a combination of all those things. The user then combines those items with something they know, like a PIN or an auto-generated time-based PIN, to achieve 2FA and stronger security (Grassi et al., 2017). Overall, the experience is much easier. The only challenge that comes into play is the user's ability to maintain their physical devices or memorize a PIN. Users lose their physical keys often, so one way to thwart that is to register multiple keys and use a PIN that is easy to remember.

Conclusion

Despite the implementation costs and upfront work, there are many advantages to using and implementing a passwordless solution for personal use or at an organization. The advantages of passwordless solutions include bolstered security via 2FA and MFA, ease of use, and how quickly passwordless authentication executes. Whether people or organizations stay with passwords for now or implement passwordless solutions, there will come a time when passwords are obsolete. For organizations weighing security risk, implementation cost, and user adoption, the emerging technologies and the desire to bolster security outweigh the antiquated usage of passwords and give way to a passwordless society.

References

Apple. (2026, September 18). *About Face ID advanced technology*. Apple Support. https://support.apple.com/en-us/102381

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy* (pp. 553–567). IEEE. https://doi.org/10.1109/SP.2012.44

Boston University. (2023). *How to choose a strong password*. TechWeb. https://www.bu.edu/tech/support/information-security/security-for-everyone/how-to-choose-a-strong-password/

CLEAR. (n.d.). *CLEAR+: Airport fast pass & airport quick pass*. Retrieved October 14, 2026, from https://www.clearme.com/how-it-works

Committee on Oversight and Government Reform, U.S. House of Representatives. (2016). *The OPM data breach: How the government jeopardized our national security for more than a generation* [Majority staff report]. https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

Dashlane. (2023, April 7). *A brief history of passwords*. https://www.dashlane.com/a-brief-history-of-passwords

Donegan, J. (2023, August 3). *Survey: Millennials revealed to be biggest cybersecurity offenders*. ManageEngine Insights. https://www.manageengine.com/insights/it-security/survey-millennials-revealed-to-be-biggest-cybersecurity-offenders

Gillis, A. S. (2023, March 15). *What is a YubiKey?* TechTarget. https://www.techtarget.com/searchsecurity/definition/YubiKey

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Irwin, L. (2022, April 28). *The 5 most common causes of data breaches*. IT Governance. https://web.archive.org/web/20231130204519/https://www.itgovernance.eu/blog/en/the-most-common-causes-of-data-breaches-and-how-you-can-spot-them

Markey, J. (2023, March 13). *Unreleased findings from the Entrust Cybersecurity Institute's "Future of Identity" report*. Security Boulevard. https://securityboulevard.com/2023/03/unreleased-findings-from-the-entrust-cybersecurity-institutes-future-of-identity-report-2/

NYU Tandon School of Engineering. (2017, April 10). *So you think you can secure your mobile phone with a fingerprint?* [Press release]. https://engineering.nyu.edu/news/so-you-think-you-can-secure-your-mobile-phone-fingerprint

OneLogin. (2023). *6 types of password attacks & how to stop them*. https://www.onelogin.com/learn/6-types-password-attacks

Rowe, A. (2023, March 21). *Study reveals average person has 100 passwords*. Tech.co. https://web.archive.org/web/2023/https://tech.co/password-managers/how-many-passwords-average-person

Shoup, A., Talkar, T., Chen, J., & Jain, A. (2016). *An overview and analysis of voice authentication methods* [Unpublished manuscript]. Massachusetts Institute of Technology. https://courses.csail.mit.edu/6.857/2016/files/31.pdf

Sumra, E. (2019, December 18). *Unlocking facial recognition: The design and implications of facial recognition and how privacy may or may not be compromised by using it* [Final project, CCTP-820: Leading by Design]. Georgetown University. https://web.archive.org/web/20200922220351/https://blogs.commons.georgetown.edu/cctp-820-fall2019/2019/12/18/unlocking-facial-recognition-the-design-and-implications-of-facial-recognition-and-how-privacy-may-or-may-not-be-compromised-by-using-it/

Taylor, D. (2023). *What's the password? Account sharing in the context of passwordless authentication* [Undergraduate honors thesis, Brigham Young University]. BYU ScholarsArchive. https://scholarsarchive.byu.edu/studentpub_uht/321

Thales Group. (2023, March). *The history of biometric authentication*. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-biometric-authentication

University of Texas at Austin Information Security Office. (2023). *Passwordless authentication*. https://security.utexas.edu/policies/passwordless-authentication

U.S. Department of Defense. (n.d.). *Getting your CAC*. Common Access Card. Retrieved October 14, 2026, from https://www.cac.mil/Common-Access-Card/Getting-Your-CAC/

Wells Fargo. (n.d.). *Advanced Access*. Retrieved October 14, 2026, from https://www.wellsfargo.com/privacy-security/advanced-access/

Yubico. (n.d.). *Yubico store*. Retrieved October 14, 2026, from https://www.yubico.com/store/

Yubico. (2023, November 16). *Passwordless account login with YubiKey*. https://www.yubico.com/solutions/passwordless/