**Passwords as an Identity Validator**

Students Name

Course, Department

Instructions

Instructor

Date

**Passwords as an Identity Validator**

**Introduction**

Identity verification is one of the key issues in digital security because unauthorized users cannot access systems and confidential information. The most widely used authentication method in history is passwords; they are easy to implement and simple. However, the rising proportion of cyberattacks has shown that using passwords to secure user accounts and organizational information has gradually become inadequate. Reused or weak credentials are vulnerable; even advanced attackers can bypass complicated password requirements. Due to the growing digital threats, there is now a necessity to reconsider the shortcomings of password authentication, discuss mitigation measures, and consider the advantages of passwordless authentication that are reported to provide improved security and user experiences.

**Password Weaknesses and Threats**

Using passwords as a validator of identity is inherently flawed since it is based on human memory and predictable ways of coding. The number of people using weak or recycled passwords on multiple accounts has remained high, exposing them to credential stuffing and brute force. Cybercriminals commonly use phishing operations to dupe users into sharing their credentials, and automated attacks involve trying large volumes of stolen passwords against various services (Aslam, 2020). After gaining access to one account, the attackers can usually access several platforms because of password reuse.

High-profile breaches demonstrate these vulnerabilities. Events like the mass leak of credentials on e-commerce sites and financial institutions show that even organizations with robust infrastructures are vulnerable in cases where passwords are the principal security measures. As a case in point, the 2023 23andMe breach affected 6.9 million users by reusing passwords and credential stuffing, evidence of the vulnerability of password protection and the necessity to switch to more robust authentication modalities (The Guardian, 2025)..

**Mitigation Strategies**

Password authentication is imperfect, but it can be fortified in several ways. Multi-factor authentication (MFA) is a popular approach in which a user must provide additional evidence of identity besides their password, in the form of a one-time password, biometric information, or a hardware token. MFA minimizes the possibility of intrusion even when the credentials are stolen. Aslam (2020) highlights that MFA can effectively protect against phishing, brute force, and credential stuffing attacks as it uses a variety of checkpoints. The usability issue remains an obstacle, particularly in the case of SMS-based codes or complicated app-based systems, but MFA achieves quantifiable increases in e-commerce and enterprise security.

Password managers are other mitigation strategies that decrease the use of poor passwords because they create and save strong and unique passwords per account. Nevertheless, these tools are dangerous because a hacked manager can simultaneously reveal several accounts. User education also reduces risk because phishing awareness and good password creation practices can minimize susceptibility. Nevertheless, such solutions merely place band-aids over the cracks in an imperfect system instead of fixing the main issue, which is using text-based secrets that never change.

**Alternative Authentication Solutions**

The security community has moved to passwordless authentication to address the structural weaknesses of passwords. This category includes biometrics (fingerprints, facial recognition, iris scans), cryptographic keys, behavioral analytics, and token-based systems. Passwordless authentication does not require memorized credentials but instead uses something you are or something you have, which is more difficult to steal or guess (Yusop et al., 2025).

A potential standard is FIDO2, which was created by the FIDO Alliance and is supported by large technology companies. FIDO2 integrates cryptographic authentication and keys that are either hardware-based or software-based. Rather than sending a password, a user authenticates with a secure private key on their device, and the matching public key is sent to the service provider. This design eliminates phishing, credential reuse, and massive database theft, since there is no shared secret to steal (Yusop et al., 2025).

The advantages of FIDO2 and other similar approaches are tremendous. They improve the security and usability, eliminate password fatigue, cause less friction, and provide faster and more reliable access. They are also friendly with mobile devices, laptops, and browsers, i.e., they can be implemented in any industry, such as the financial sector, healthcare industry, and government services.

Nevertheless, there are still adoption issues. FIDO2 necessitates service providers to upgrade their infrastructure, and users must have compatible devices or tokens. Accessibility issues, loss of devices, and recovery systems are still a concern. Despite these challenges, research indicates that passwordless authentication is the way of the future, with greater standardization and the increasing realization that passwords are no longer sufficient to protect contemporary digital environments (Yusop et al., 2025).

**Conclusion**

Passwords have long been the most widely employed digital authentication method, but do not address current cybersecurity threats. They are a weak form of identity authentication as they rely on human memory, are susceptible to phishing, and can be attacked by automation. Short-term solutions such as MFA, password managers, and training help reduce the degree of risk, but are not enough to eliminate the inevitable danger of text-based authentication. More recent passwordless protocols, and FIDO2 in particular, are more powerful alternatives based on cryptography and device-based authentication. Despite issues in adoption and ease of use, the shift toward passwordless systems indicates a paradigm shift in identity management. The future of authentication is in strategies that focus on security and user experience, as safety measures against the emerging threats are designed to be even more robust.

**References**

Aslam, M. (2020). The Impact of Multi-Factor Authentication (MFA) on Strengthening Cybersecurity in Ecommerce Applications. <https://www.researchgate.net/profile/Muhammad-Aslam-270/publication/384322471_The_Impact_of_Multi-Factor_Authentication_MFA_on_Strengthening_Cybersecurity_in_Ecommerce_Applications/links/66f3efb6b753fa724d47bfa5/The-Impact-of-Multi-Factor-Authentication-MFA-on-Strengthening-Cybersecurity-in-Ecommerce-Applications.pdf>

The Guardian, (2025). Hackers got nearly 7 million people’s data from 23andMe. The firm blamed users in ‘very dumb’ move. <https://www.theguardian.com/technology/2024/feb/15/23andme-hack-data-genetic-data-selling-response>

Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. (2025). Advancing passwordless authentication: A systematic review of methods, challenges, and future directions for secure user identity. IEEE Access. <https://ieeexplore.ieee.org/iel8/6287639/6514899/10839395.pdf>