Challenges and Opportunities in Password Management: A Review of Current Solutions

Sri Lanka Journal of Social Sciences and Humanities
Volume 3 Issue 2, August 2023:9-20
ISSN: 2773 692X (Online), 2773 6911 (Print)

Published by the Faculty of Social Sciences and Languages, Sabaragamuwa University of Sri Lanka
Website: https://www.sab.ac.lk/sljssh
DOI: https://doi.org/10.4038/sljssh.v3i2.96

Fernando, W.P.K.[1,*] Dissanayake, D.A.N.P.[1], Dushmantha, S.G.V.D.[1], Liyanage, D.L.C.P.[1], and Karunatilake, C[1].

[1] Department of Information and Communication Technology, Faculty of Technology, University of Sri Jayewardenepura, Gangodawila Nugegoda.

Received: 10 February 2023, **Revised:** 25 May 2023, **Accepted:** 16 June 2023.
How to Cite this Article: Fernando, W.P.K., Dissanayake, D.A.N.P., Dushmantha, S.G.V.D., Liyanage, D.L.C.P., & Karunatilake, C. (2023). Challenges and opportunities in password management: A review of current solutions. *Sri Lanka Journal of Social Sciences and Humanities, 3*(2), 9-20.

Abstract

For over six decades, passwords have served as the primary authentication mechanism for almost all modern computer systems. However, password management is a challenging task for most computer users, and that has led users to many malpractices that open the door for most information security breaches over time. Despite many efforts, no alternative solution has ever succeeded in replacing passwords as the primary authentication mechanism. As a result, users are now heavily relying on password managers to alleviate the burden of manual password management. This paper addresses the topic of password management about different types of password managers and their inherent limitations. By evaluating the existing password management approaches and identifying potential improvements, this paper aims to signify an important research gap that exists in the study area; the need for fully automating the process of manual password management.

Keywords: Authentication, Passwords, Password managers, Security, Usability

INTRODUCTION

Despite that several studies have repeatedly proven and been criticized for performing extremely poorly when it comes to security, passwords are still being used as the primary, as well as the oldest authentication mechanism in modern information systems since coming into existence over sixty-one years ago (Taneski, Heričko & Brumen, 2014). The growing number of web services and applications have made it impossible for end-users to memorize passwords and perform manual password rotation due to their high-complexity requirements. Managing a collection of passwords is often considered a difficult task. This has led to users with a low technical background resorting to reusing the same passwords for multiple services or making small changes to the existing password to be used for different services while the ones with good technical backgrounds started to use password wallet solutions for managing their passwords and sensitive information (Sebastian, 2021).

A considerable number of information security breaches happening worldwide are caused by improper handling of passwords. This is due to most users not being informed enough to follow proper security particles and they lack good tools to manage passwords securely and conveniently. According to Sebastian (2021), thirty percent of the information security incidents that occurred in recent years were caused by factors related to passwords and improper password management. 45.7% of users keep the same password or the same password set for multiple web services while 62.9% of users change their password only when prompted to do so. According to Kuka & Bahiti (2018), 14.72% of users never change the password that was initially created. These malpractices often result in financial losses, leakage of personal data, and unauthorized access to private systems.

Even though many technologies came into existence as a result of attempts to find alternatives for passwords, such as patterns, biometrics, and facial recognition, none of them managed to completely replace passwords since they are not capable of providing the same level of trade-off between security and usability that passwords can provide along with the economic and technical benefits. As a result of their weaknesses and other circumstantial factors, there have been mechanisms introduced such as 2FA and MFA to mitigate some of the common problems caused by passwords. Although, the core principle of being used as the primary way of authentication remains true for passwords despite the existence of such mechanisms.

Since passwords cannot be fully replaced, software and hardware managers were introduced allowing users to manage their passwords securely. However, due to the nature of their features such as the utilization of cloud technology, lack of usability, and weak security standards, existing solutions fail to provide a proper solution to this problem (Chaudhary et al., 2019). Most of the existing password management solutions either rely on cloud

[*] **Corresponding author:** Tel.: +94 (76) 621 4960; Email: prageethfndo@gmail.com
https://orcid.org/0000-0001-7567-6863

infrastructure which is often viewed as a target for bad actors or lack usability and features to be useful for an average user. Also, there is a considerable number of users who do not trust cloud services enough to store their passwords, which can be considered valuable assets. This often leads to them either not managing passwords properly or using inconvenient methods like writing down passwords physically or storing them on an insecure local digital file. Despite the many studies and attempts to solve this problem, none of them have managed to come up with a solution that is secure, usable, and completely offline. A solution where the end-user does not have to worry about managing passwords through some complicated process, but rather "just configure it once and then forget about it".

This review paper comprehensively examines the literature on the password problem, explores alternatives, discusses password managers, and delves into hardware-based solutions. It aims to assess the possibility of automating the password management process. Analyzing various sources, the paper highlights vulnerabilities of traditional systems and the need for better solutions. It explores alternative authentication methods like biometrics and two-factor authentication, evaluating the effectiveness of password managers, both software-based and hardware-based. Finally, it discusses the potential for automating password management, considering emerging technologies for improved security and user experience.

LITERATURE REVIEW

Password Problem

Taneski, Heričko & Brumen (2014) discussed that user authentication on modern computer systems can be done under three methods such as "what user knows" (e.g.: - textual password, graphical password), "what user has" (e.g.: - smart card, token" and "what user is" (e.g.: - biometrics). Passwords fall under the category of "what user knows" and it can be further divided into text-based and graphic-based passwords. Password is only one component of the overall computer system security nevertheless it is the most important and essential component as well (Morris & Thompson 1979). Both Yıldırım & Mackie (2019) and Habib et al. (2018) presented that textual passwords are the most cost-effective, easiest, and fastest authentication solution with zero compatibility and technical issues. Hence, it is being widely accepted as the primary authentication mechanism from personal device login to enterprise access control in modern days as well. Lyastani et al. (2018) also supported the previous fact by presenting that textual password-based authentication is the de-facto authentication scheme on the Internet. Graphical passwords follow a different authentication procedure, and they take a considerable amount of time for the password registration and the log-in process although they provide better security than textual passwords (Taneski, Heričko & Brumen, 2014). Research by Yıldırım & Mackie (2019) found many alternative authentication mechanisms and schemes were researched and introduced which aimed to replace traditional textual passwords and to align with more security and usability. But none of them could overcome the simplicity of authentication by typing a keyboard character stream. Therefore, it is still considered the most popular primary authentication even after 61 years of the origin of the Compatible Time-Sharing System (CTTS) of Massachusetts Institute of Technology (MIT) in 1961 and is most likely to have remained as it is in the near future (Fredericks, 2018).

Over the past decade, the internet has grown exponentially, and the number of web applications and online services is also abruptly increasing along with it. To keep these web applications and online services personalized, organized, and secured, password-protected user accounts have to be created and maintained by the users (Rahalkar & Gujar, 2019). As reported by Gao et al. (2018) and Pearman et al. (2019), an average internet user has to maintain 12 to 26 password-protected accounts and an average undergraduate has to maintain 8 academic password-protected accounts separately while the majority of them forget newly created passwords within the first 12 hours. This online account maintenance comes with password management which consists of strong password creation, mitigation of password reuse, memorization, periodic renewal, and instant availability. Among the above-mentioned components of password management, memorization is the key component that defines the other components and finally the security strength of a particular account (Luevanos et al., 2017). Gao et al. (2018) discussed three psychological theories that are relevant to password memorization. Depth of processing theory – how users attend to passwords to memorize them, Decay theory – memory traces that decay over time, and interference theory – forgetting passwords due to conflicts between similar memory traces.

Due to limited human memory capability, users always tend to create passwords with a certain pattern including names, dates, keyboard layouts, etc., or associate the generating passwords with corresponding online service characteristics and features. Glory et al. (2019) have also reported that manual password creation can be inspired by common sources or personal related words, or others' passwords. They argued that when users are forced to create high entropy passwords, sometimes users tend to use random password generators to create strong passwords. But these randomly generated passwords are not user-friendly and easily forgettable. Hence, users write down passwords on a notebook or save them on the device which can easily get compromised by an intruder. So, they have proposed a methodology for an automated system that can generate robust and user-friendly passwords through a set of information such as favourite novels, secret dates, etc. taken from the user, presumably a convenience for users to remember passwords easily. 50 passwords generated through this algorithm have been tested with brute force attacks and obtained a cracking span of 90 days to 1,217,000 days. They have proved that their algorithm is generating passwords that meet the minimum password strength criteria and defend against dictionary rainbow and dictionary attacks. But they have failed to propose a procedure to defend against social attacks which can help to speed up the process of the dictionary attacks. Taneski, Heričko & Brumen (2014) argued that passwords with higher entropy are more difficult to memorize in the long term, therefore users tend to create passwords that are easily guessable and breakable.

Woods & Siponen (2019) researched the trade-off between password security and memorability and could have been able to find that the memorability of manually created passwords can be increased from 42% to 70% by forcing users to verify the password three times. They concluded that applying a repetitive password verification stage could result in a significant increase in password memorability

while not inconveniencing the users. Singh & Raj (2022) and Fredericks (2018) presented that the majority of passwords that are being manually created can be broken by an attacker through brute-force attacks, rainbow table attacks, dictionary attacks, phishing attacks, and social engineering attacks even though they are aligned with the password policy provided by the online service provider. Password strength checkers are used when users are registering to a particular web service to measure the strength and guide the users to create more secure and avoid weak passwords. But Singh & Raj (2019) have observed that password strength checkers are suffering from a lack of consistency and accuracy and are vulnerable due to a static password policy enforced on every user which will create a strong bias on particular password characteristics. Also, these strength checkers cannot demand high entropy since they cannot measure the usability or the memorability of the passwords. So, they have proposed an algorithm that can generate dynamically dependent password policies on the frequency of characters. This algorithm uses special characters in the password space which is never used in manual creation to increase the complexity and make it more difficult to initiate dictionary and rainbow attacks to crack the passwords.

Biesner et al. (2020) proposed a methodology for generating novel and realistic passwords using deep learning techniques which were already increasingly used for password guessing. This method relies on data-driven deep learning text generation and surpasses the state-of-art password generation algorithms. Smith (2022) discussed people are extremely biased toward simple passwords with a word and a number when creating passwords which are limited to a certain number of combinations, and it has reduced the number of possibilities to about 1 million common passwords from 6 quadrillion possibilities of 8-character passwords. These biases expose the account security to dictionary attacks which have a success rate of 20% - 35%. According to Smith (2020), calculations have shown that 100,000 hashes can be calculated per second by a modern computer and reasonably it can crack a password in 10 seconds. Such a significant difference presents the security and strength that a random password generator can provide for password-based user authentication. Three types of schemes for random password generating (ALPHANUM-sequence of random alpha-numeric characters, DICEWARE-list of words, and PRONOUNCE3-string of syllables) are employed. Also, high entropy can be gained by including mnemonic aids for ALPHANUM, removing obscure words from the DICEWARE word list, and combining upper case letters and punctuations to the PRONOUNCE3 schemes (Smith, 2020). Grilo, Ferreira & Almeida (2021) studied 15 password managers to understand commonly used generation algorithms, and Google, Bitwarden, and KeePass algorithms were critically reviewed since they are open-source and widely used in the industry. They defined that generated passwords must satisfy the password composition policies including password character length and different character classes to avoid passwords being easily guessed or reused. Both Google and Bitwarden algorithms support string permutation and follow similar approaches to password generation apart from the order of permutation generation and character generation with the given minimum and maximum character occurrence by the user. KeePass does not support minimum and maximum character occurrence, so the algorithm generates a random sequence of characters from a union of defined sets in the policy. Security of the generated password can be verified by the probability that the generated password is the same as any other generated password from the same policy. Therefore, a uniform distribution should be there over the entire set of possible passwords generated from the same algorithm based on the same policy.

Gao et al. (2018) raised concerns about password reuse when an average user maintains 12 to 26 online accounts, that particular user only uses 7 unique passwords for different online services. Kuka & Bahiti (2018) and Rahalkar & Gujar (2019) also argued that 52% - 56% of people overestimate their manually created passwords and reuse the same set of passwords with zero to little modifications. According to a survey by Stobert & Biddle (2018), 75% of respondents admitted to reusing passwords due to the convenience and speed of doing so. Specifically, 67% cited convenience as the reason for password reuse, while 53% mentioned speed as the main factor. A large-scale study was done by Tatli & Seker (2018) to find password reuse patterns through a 14.5 million plain text password dataset leaked during the RockYou hack and 43 different password reuse patterns were identified by an automated analysis. According to the provided literature, the majority of computer users were directed to create multiple password-protected accounts and were forced to align with strict password creation and/or renewal policies. They also argued that when people are forced to align with complexity requirement policies, people always choose to fulfill the requirements but not to secure against attacks. This conflict and frustration between IT professionals and users, and users somehow trying to follow the enforced standard policies and rules under emotional pressure had resulted in slowing down the performance of their primary tasks and reusing passwords in numerous accounts (Chaudhary et al., 2019).

As discussed by Habib et al. (2018), only 20% of password-protected online services require users to update their passwords periodically, and 67% reported creating new passwords by modifying the existing passwords. Also, 10% reported the usage of swapping passwords between accounts when they are forced to update passwords through policies. They also reported that 60% of survey participants agreed that password renewal is annoying and 45% of them have been locked out from their account at least one time within a period of a year. As presented by Abuzaraida & Zeki (2020) only 8% of survey respondents are renewing passwords regularly and only 6% renew passwords twice a year. The majority of the respondents are only changing passwords in case of security threats or felt that they have been hacked/attacked. Lyastani et al. (2018) reported that the bad practice of password reuse across multiple accounts can be seen due to the limited capacity of remembering multiple passwords.

Password Alternatives

Ever since Morris & Thompson (1979) identified textual passwords as a weak authentication mechanism for modern computer systems and a huge threat to a system's security, the search for a good alternative is still a hunt. Replacement for traditional textual passwords is subject to four important roles such as usability, security, deployability, and privacy to be widely accepted and practical usage on a scheme (Zimmermann & Gerber, 2020). Chaudhary et al. (2019) have identified several types of password practices within the process of username-password authentication mechanism: one-word passwords, passphrases, Person Identification

Number (PIN), cognitive passwords, associative passwords, gesture passwords, image passwords, image-gesture passwords. This username-password pair authentication can also be associated with other authentication mechanisms during multi-factor authentication. Furthermore, several alternative solutions such as biometrics, smart cards, hardware tokens, PIN codes, Single Sign-On, One-Time Password (OTP), Authentication apps, etc. have been implemented replacing traditional username-password authentication. But these authentication mechanisms function in their own environment with limitations and vulnerabilities. None of them have been able to successfully replace the password as the mainstream approach for user authentication on all password-protected accounts, as not a single alternative technology is capable of providing the same level of security and usability with economical and technical advantages provided by the username-password pair authentication.

Siddique, Akhtar & Kim (2017) supported the above statement by reporting that decades of dedication and attempts for replacing passwords for better authentication security have not succeeded since no single technology or approach is likely to appear as a universal solution. None of the alternative approaches can match the security evaluation statistic of traditional passwords. Every effort to escape from passwords has continually brought back the credibility and accomplishments of passwords. Instead of replacing passwords, they suggested that the union of passwords and other approaches would be more likely to be a perfect way of improving security on authentication. They also reported that 84% of survey participants supported the elimination of password usage with 76% preferring alternative authentication approaches and 59% electing fingerprint scanning over traditional textual passwords. Apart from the statistical evaluation, fingerprint-based authentication offers usability advantages and outperforms all other alternatives and most importantly, it achieves more implicit credibility for user authentication. Fingerprint authentication can be misguided through fingerprint spoof attacks but modern scanners are now evolved to observe the liveliness of the fingerprint such parameters as blood flow, pressure, etc. to be resilient to such attacks. Biometric authentication has arisen with mobile, wearable, and continuous authentication solutions but interoperability, privacy, and negative perceptions remain problematic because some sensitive data like ethnicity, age, and gender can be extracted from different biometric traits such as a thumbprint, iris images, and face images. Also, biometric accuracy depends on the quality of hardware components.

A similar study by Zimmermann & Gerber (2020), indicated that numerous studies have been conducted to compare alternative authentication approaches against traditional textual passwords and increase the efficiency, accuracy, usability, and resistance against attacks. 85 different authentication approaches were found throughout their literature study and categorized into knowledge-based (text), knowledge-based (graphic), cognitive, biometric, and token-based categories. Memorization of a secret is required in all categories except for the biometric and token-based schemes while all other approaches are insignificant in terms of cost except for biometric schemes since they are required with exclusive quality sensors. All knowledge-based schemes provide the facility to easily recover from a loss where other schemes suffer from it. They also argue that many researchers criticize biometric authentication schemes as they are resilient against identity theft, trace recordings, and targeted impersonation. Another misconception about the password being more secure due to its naturally large boundaries compared to other schemes is also discussed. They clearly showed that even though password authentication has a large password space, the actual password space is much smaller due to dictionary words, reuse patterns, and other influences and preferences. They also presented that the overall performance score of password and biometric combination outranks all other authentication schemes individually or combined in security, usability, and deployability wise.

Kurniawan et al. (2021) proposed a methodology for user authentication through the One-Time Password (OTP) system which employs AES and Blowfish algorithms to fine-tune the performance and security of the existing OTP authentication approach. They presented that 13.6% of survey participants positively responded to password sharing among others and 9.9% of account hacking events. Even though they have failed to implement OTP as a complete replacement for traditional username-password pairs, they indicated that OTP can be used to increase the security of the username-password authentication approach.

Use of Password Managers

Chaudhary et al. (2019) discussed that security experts suggest various password policies and rules for generating more stronger and secure passwords to tighten the security of computer systems but unfortunately, these policies are often unrealistic, time-consuming, and unnecessarily cognitively overload the users. According to Kankane, DiRusso, & Buckley (2018), mandatory password policies alone are not sufficient to change user behavior or attitudes toward password management. These policies are not effective in encouraging users to adopt better password habits. In the intent of addressing this ever-lasting password management problem, password managers have come into the situation. These password managers mitigate insecure password management, and user behaviors and help to alter the user perception regarding passwords to the positive side in a secure and practicable way. (Stajano et al., 2015; Luevanos et al., 2017; Chaudhary et al., 2019). A password manager is a tool with a master password to encrypt and decrypt the vault which contains all the user's accounts' login credentials. Modern-day password managers also can generate strong and secure passwords for the user and offer other optional features such as auto-fill, data synchronization, password suggestions, store secret notes, credit/debit card details, etc. (Naing Oo, 2022). Lyastani et al. (2018) and Macgregor (2020) supported the idea that users who engaged with password managers in the process of password creation tend to create more strong, unique, secure passwords than users who practice manual creation. The main advantage of this is that users only have to remember a single password and the tool memorizes all other sensitive data for themselves (Rahalkar & Gujar, 2019).

Grilo, Ferreira & Almeida (2021) stated that security experts are strongly recommending password managers for password creation and storage which also frees the users from the cognitive burden of password management. Gupta et al. (2020b) categorized password managers into four types; Desktop Password Managers, Online Password Managers, Mobile-based Portable Password Managers, and USB-based Portable Password Managers. Guo et al. (2019) presented that password managers can mainly be divided

into two kinds. Retrieval Password Managers mainly focused on storing passwords locally encrypted or not under the protection of a master password and Generative Password Managers focused on the storage of high entropy passwords generated by itself. Retrieval Password Managers cannot mitigate password reuse and all these password managers suffer from a single point of failure derived from the master password. A forgotten master password blocks the legitimate user from accessing their own vault and an exposed master password can grant access to all the sensitive data stored inside of the password vault since this master password is vulnerable to offline attacks, shoulder surfing attacks, phishing attacks, etc. These password managers mainly can be found as software-based password managers and adopted by both individuals and corporations since they are more cost-saving and easy to deploy compared to hardware-based solutions, however, hardware-based password managers are still a work in progress to overcome these factors (Naing Oo, 2022).

Rahalkar & Gujar (2019) presented that software-based password managers typically operate in either an online or offline manner. The offline version of software-based password managers also known as desktop managers only contains the encrypted password vault on the client-side software-installed device and it has to be transported everywhere which requires additional effort from the user. The online version of the password manager, also known as online managers, stores the encrypted password vault on a cloud service or a remote location which can be accessed through the Internet anytime. As stated by Chaudhary et al. (2019) password managers are not still widely accepted by computer users although password managers ease users from annoying password management due to usability and security concerns. As reported, 60% - 63% of people use memorization as the technique of password management and around 8% use password managers for strong password generation and only 8% reported using password manager tools for password management. The reason for this low adaptation of password managers is the focus given by the developers of particular properties and features specific to the application and failing to account for significant usability and security measures. Password managers or Vault Applications should be far beyond in the level of security than general-purpose software applications since they are required to meet several security requirements to facilitate satisfactory protection for users' sensitive data. They should be constructed with a strong security architecture, highly efficient security mechanisms, and a strong defense strategy with the expectations of providing a secure data storage, processing, and a management environment to safeguard the integrity and authenticity of both users' sensitive data and the confidentiality of entrusted applications (Sabev & Petrov, 2021).

Offline password managers do not provide the ability to login from multiple devices anywhere either because some of them are platform dependent or vault inaccessibility through a network. This portability issue is a major problem for these offline managers and the cause of the low adoption rate among non-expert computer users. If the device is stolen or the vault is lost, all stored credentials and sensitive data will also be lost. Hence, it is a single-point-of-failure approach. But privacy and security are guaranteed at a certain level though it was revealed unencrypted passwords could be found on temporary files in the operating system (Pearman et al., 2019).

The online managers overcome the portability, synchronization, and single-point-of-failure issues of the desktop managers by maintaining an encrypted password vault as a centralized database stored in the cloud or remote locations. This feature gives high availability for users to access login credentials and other sensitive data anywhere anytime platform independently (Anand, Susila & Balakrishnan, 2018; Gupta et al., 2022). Chaudhary et al. (2019) and (Grilo, Ferreira & Almeida, 2021) counter-argued that online managers come with the possibility of security breaches and mistrust of the service provider since confidentiality arrangements might not be true at all times. Luevanos et al. (2017) reported that two major online password managers in the market, LastPass and Roboform have been identified for storing credentials and sensitive data in plain text on the cloud servers and offering suggestions for the other third-party vendors on product and data security. There were also critical vulnerabilities found on auto-fill browser extensions developed for LastPass and KeePass which may open up to attacks like iFrame sweep attacks, password sync exploitation, and injections. Despite the different number of password managers with different forms, they all use the same database format. Hence the vulnerabilities are repetitive among these famous password managers. According to provided literature by Pearman et al. (2019), some users admire and find the online accessibility of online managers useful, however others question the security of cloud-based storage since the internet is not a safe place.

Hardware Based Password Managers

Naing Oo (2022) argued that there is a significant research gap between software-based password managers and hardware-based password managers and there is no hardware-based password management solution in the market that is portable, cost-effective, backward compatible and which also gives full access and control over the credentials stored in their hardware wallet. For a hardware wallet to function properly as a password vault, it should interact with the user's web browser through client-side software which can facilitate two-way communication channels via USB, Bluetooth, WIFI, NFC, RFID, IR, and LAN. Aebischer et al. (2017) stated that a token-based authentication system called Common Access Card (CAC) introduced to the US Department of Defense (DoD) made a significant impact on organization productivity and a loss of $10.4 million.

Stajano (2011) stated that if any mechanism is going to be invented to overcome this password problem and users are no longer needed for remembering unguessable secrets, it should fulfil at least three requirements of memoryless, scalable, secure, loss-resistance, and theft resistance. Hardware password wallets can meet all these requirements with additional advantages but with the burden of carrying a token all the time. Stajano (2011) proposed a hardware device called Pico which can bear the burden of remembering authentication credentials by transforming the traditional authentication from "something the user knows" to "something the user has". Pico communicates with user devices over the radio with public and private key encryption and it does the authentication by scanning a QR code displayed on the login screen. Also, Pico supports continuous authentication by the presence of Pico near the logged session and continuous identification through Pico-siblings, various items that the user wears every time such as spectacles, belt, wallet, jewellery items, wigs, etc. and Pico will be unlocked all the time around these Pico-siblings.

This relationship between Pico and Pico-sibling can be a many-to-many relationship and the user can authenticate to the device anywhere, anytime. Pico is also theft-resistant and loss resistant since it uses a docking station to store its encrypted backup file to a memory card while it is charging. In case of loss or theft, virgin Pico can be connected to the docking station and restore the old backup to the new device. Pico is not expected to replace passwords but to provide more usability and security simultaneously since other password replacement mechanisms trade off some usability to offer greater security and vice versa.

Stajano (2011) mentioned that smartphones are general-purpose networked devices with great ecosystems for numerous security threats and users would not enjoy the security of their sensitive data on such devices. Aebischer et al. (2017) conducted a study evaluating the Pico system for replacing passwords exploring the areas of usability, deployability, and security. With the results of prior research on the usability of token-based authentication and identified problems with the hardware-based Pico system, the Pico project was later focused on the implementation of a smartphone application. They concluded that participants disliked the QR code scanning and suggested replacing the mechanism with another modality to authenticate. However, participants liked the idea of password management being automated.

Gupta et al. (2020b) present a novel USB-based Portable Password Manager solution that consists of an Arduino Micro microcontroller to encrypt and store user credentials on the device and communicate with user devices through USB-wired connectivity. The device has an OLED display to display credentials in case of the need to log in to a non-USB-supported device. This proposed solution also uses another device named the authentication node, like the Pico-sibling in the Pico system, to authenticate the user and keep the device unlocked to support continuous user identification. This device also supports high entropy random password generation which is resistant to dictionary attacks and does credential encryption with the AES-128 algorithm. The authors have stated that the device is capable of connecting to cloud service if the user requires it. Wang & Khan (2019) proposed a methodology for a hardware-based token authentication system that facilitates users to access web services with a tamper-resistance chip that communicates to a browser app through a USB and NFC dual interface. A separate JavaScript file within a bookmark of the browser will generate the QR codes and the user has to scan it through the hardware token to authenticate to a particular web service by decrypting the stored credentials and submitting them to the remote server. A master password is used for every encryption and decryption process and then only the application can access the password vault. Same as previous works, this system also uses the AES-128 encryption algorithm. This approach is resistant to keylogger attacks but there is a vulnerability since the JavaScript file can be injected with a virus to steal credentials. This approach is theft resistant since no attacker can access the password vault is stored on tamper-resistance storage and protected with a master password but still an attacker can open the bookmark file on the browser to scan the QR code to get the user credentials. Also, they have failed to provide a loss-resistant mechanism for this proposed system and cannot act against man-in-the-browser attacks.

Guo et al. (2019) proposed a novel hardware-based password manager solution named PUFPass utilizing the uniformity of Physical Unclonable Function (PUF) to provide hardware-level security to the hardware wallet. This PUFPass system consists of a client application and hardware wallet to securely store credentials. The client application makes the request for a password and PUF implemented hardware wallet takes username-password pair from the user and generates a strong password and strengthens it using PUF. Then that generated password is sent to a remote server for user authentication. Every time a user logs into a particular web service, the user has to remember only one password and PUFPass will do the authentication afterward through the PUF-strengthened passwords. This approach can easily mitigate the threat of exposing passwords to third parties since attackers cannot generate the PUF password without physically accessing the same PUFPass devices used for password generation. A QR-based approach is also introduced in this proposed methodology to facilitate transportability among different devices and support migration from one PUFPass device to a new one in case of theft or loss.

But the major drawback is passwords cannot be recovered since they are bound to the lost or stolen device's PUF and this might raise a potential security threat in case of a theft. Even though there are proposed solutions such as using multiple PUFs to increase their reliability in case of failure, it also increases the complexity of password management significantly. Unlike traditional approaches to password management, PUFs make it nearly impossible to take backups conveniently and restore them to another device. This results in a lack of portability and adaptability. Furthermore, current studies that propose PUFs focus primarily on the servers that facilitate cloud infrastructure which is known to be targets of malicious attacks. Although password storage will be secured, there are concerns such as the reliability of in-transit data and the reliability of software that runs on these services. Even though we can solve some of the issues associated with PUFs such as slow computation and resource utilization, the overall architecture will still be dependent on obscure cloud services, which can be a major security concern when used in practice (Mohammadinodoushan et al., 2021a), (Mohammadinodoushan et al., 2021b).

Naing Oo (2022) proposed a novel hardware password manager named E2PM stored on a regular USB stick which can be plugged into the computer and access the password manager through the Midori web browser. The system consists of two main components; Core System - a runtime image and Secure Data Partition - a memory that allows reading and writing. In this case, the user has to run the E2PM password manager by live booting the USB drive or by constructing a connection to the USB through the VirtualBox Virtual Machine manager. A 16-character long master password is used to secure the password vault and the user has to manually enter the login credentials to the web service since the copy/paste option or autofill option is not available. After using the device, the user has to enter the "shutdown" Linux command to exit from the device and if the device was used in live boot, the user's computer has to be restarted as well. The author has discussed Stajano's (2011) least 3 requirements of a novel authentication method and proved that E2PM gets along with Memoryless, Scalable and Secure requirements. The author has critically reviewed the literature about PUF-based authentication schemes and agrees with the significant characteristics that it brings to the table such as theft resistance, strong password generation, and strengthened authentication while also agreeing to the major drawbacks such as

credentials recovery, usability, backward compatibility, and loss resistance.

Table 1: Summary of Literature Review

Article	**Key Findings**
Taneski, Heričko & Brumen (2014)	User authentication methods: "what user knows," "what user has," and "what user is." Text-based and graphic-based passwords are two types of "what user knows" authentication. Textual passwords are widely accepted due to cost-effectiveness and ease of use. Graphical passwords provide better security but take more time. Passwords are the most important component of computer system security.
Yıldırım & Mackie (2019)	Textual passwords are the most cost-effective and widely accepted authentication solution. Alternative authentication mechanisms have been researched but cannot replace textual passwords. Textual passwords are the primary authentication mechanism in personal and enterprise settings.
Lyastani et al. (2018)	Textual password-based authentication is the de-facto authentication scheme on the internet. Users tend to create easily guessable passwords due to limited memory capacity. High-entropy passwords are difficult to memorize in the long term. Textual passwords remain popular despite alternatives.
Gao et al. (2018)	Average internet users have to maintain multiple password-protected accounts. Users often forget newly created passwords within the first 12 hours. Password memorization is a key component of password management. Users tend to create passwords with patterns or associations for ease of memorization. Manual password creation can lead to easily guessable and breakable passwords.
Woods & Siponen (2019)	Repetitive password verification can significantly increase password memorability without inconveniencing users.
Singh & Raj (2022)	Password strength checkers lack consistency, accuracy, and usability measurement. An algorithm that dynamically generates password policies based on character frequency can increase complexity and deter dictionary and rainbow attacks.
Biesner et al. (2020)	Deep learning techniques can be used to generate novel and realistic passwords. Data-driven text generation can surpass existing password generation algorithms. Deep learning methods are increasingly used for password guessing.
Smith (2022)	Users are biased towards simple passwords with words and numbers. Biases limit the number of password combinations and increase vulnerability to dictionary attacks. Random password generators provide higher security and strength. Different password generation schemes (ALPHANUM, DICEWARE, PRONOUNCE3) can increase entropy and security.
Grilo, Ferreira & Almeida (2021)	Password managers use different generation algorithms. Google, Bitwarden, and KeePass generation algorithms are critically reviewed. Generated passwords must meet composition policies to avoid easy guessing and reuse. A uniform distribution over the entire set of possible passwords is essential for security. Security experts recommend password managers to improve password creation and storage. Password managers reduce the cognitive burden of password management. Different types of password managers exist, including desktop, online, mobile-based, and USB-based options. Usability and security concerns contribute to the low adoption rate of password managers.
Tatli & Seker (2018)	Password reuse is common due to the need to maintain multiple accounts. Users often reuse passwords with little modification. Convenience and speed are the main reasons for password reuse. An automated analysis identified 43 password reuse patterns. Users comply with complexity requirements but may not prioritize security. Conflicts and frustration exist between IT professionals and users regarding password policies.
Habib et al. (2018)	Only 20% of online services require periodic password updates. Users often modify existing passwords instead of creating new ones. Password renewal is viewed as annoying by many users. Password reuse and swapping between accounts are common practices. Users may be locked out of their accounts due to password policies. Regular password renewal and compliance with security threats are low.
Abuzaraida & Zeki (2020)	Only a small percentage of users regularly renew passwords. Most users change passwords in response to security threats or perceived attacks. Limited memory capacity leads to password reuse. Users often do not prioritize proactive password renewal.

Pearman et al. (2019)	Online password managers provide portability and accessibility but raise concerns about security breaches and data confidentiality. Some password managers have been found storing credentials in plain text or have vulnerabilities in their browser extensions. Users have mixed opinions about the security of cloud-based storage.
Guo et al. (2019)	Password managers can be retrieval-based or generative-based. Retrieval-based managers store passwords locally encrypted or not, protected by a master password. Generative-based managers generate high-entropy passwords and store them. Both types have limitations, including the risk of forgotten or exposed master passwords. Hardware-based password managers are still a work in progress.
Rahalkar & Gujar (2019)	Password managers can operate offline or online. Offline managers require the user to transport the encrypted password vault. Online managers offer high availability but raise concerns about security breaches and trust in service providers. Both offline and online managers have their advantages and limitations.
Chaudhary et al. (2019)	Password managers mitigate insecure password management and user behaviours. They help improve user perception of passwords. Users who engage with password managers tend to create stronger passwords. Password managers offer features like auto-fill, data synchronization, and secure storage of sensitive data. Different types of password managers exist, including desktop, online, mobile-based, and USB-based options. Some password managers have security vulnerabilities and single-point-of-failure risks. The adoption of password managers is still relatively low due to usability and security concerns.
Morris & Thompson (1979)	Textual passwords are weak authentication mechanisms and pose security threats.
Siddique, Akhtar & Kim (2017)	No single technology or approach is likely to replace passwords as a universal solution. Combining passwords with other authentication approaches is more likely to improve security. Users support alternative authentication approaches and prefer fingerprint scanning over passwords. Fingerprint authentication offers usability advantages but can be vulnerable to spoof attacks. Biometric authentication has interoperability, privacy, and negative perception issues. The combination of passwords and biometrics performs better than other authentication schemes.
Zimmermann & Gerber (2020)	Numerous authentication approaches have been compared against passwords. Biometrics and token-based schemes require high-quality sensors and suffer from limitations. Passwords have a large password space but are influenced by dictionary words and reuse patterns. Passwords combined with biometrics outperform other schemes in security, usability, and deployability.
Kurniawan et al. (2021)	OTP systems can increase the security of username-password authentication. Some users share passwords and experience account hacking events. OTP is not a complete replacement for passwords but can enhance their security.
Naing Oo (2022)	Proposed a hardware password manager called E2PM stored on a USB stick. The system requires live booting or a connection through VirtualBox. Supports memoryless, scalable, and secure authentication. Does not offer copy/paste or autofill options. Requires manual entry of login credentials. Lack of credentials recovery and backward compatibility.
Aebischer et al. (2017)	Studied the Common Access Card (CAC) token-based authentication system for the US Department of Defence (DoD). Showed significant impact on organization productivity.
Stajano (2011)	Proposed a hardware device called Pico for remembering authentication credentials. Pico-siblings provide continuous authentication and identification. Theft and loss resistance. Simultaneously enhances usability and security.
Gupta et al. (2020b)	Presented a USB-based Portable Password Manager solution using Arduino Micro microcontroller. Supports USB connectivity and OLED display. High entropy password generation. AES-128 encryption. Continuous user identification through an authentication node.
Wang & Khan (2019)	Proposed a hardware-based token authentication system with a tamper-resistant chip. Uses USB and NFC dual interface to communicate with browser app. Securely stores and decrypts credentials. Vulnerable to JavaScript injection and man-in-the-browser attacks. No loss-resistant mechanism.

Guo et al. (2019)	Proposed a hardware-based password manager using Physical Unclonable Function (PUF). The client application and hardware wallet generate and strengthen passwords. QR-based transportability. Passwords bound to specific devices. Lack of password recovery. Dependent on cloud services.
Mohammadinodoushan et al. (2021a), (2021b)	Raised concerns about the reliance on obscure cloud services and the reliability of in-transit data and software in PUF-based authentication systems. Slow computation, lack of portability, and adaptability.
Naing Oo (2022)	Proposed a hardware password manager called E2PM stored on a USB stick. The system requires live booting or a connection through VirtualBox. Supports memoryless, scalable, and secure authentication. Does not offer copy/paste or autofill options. Requires manual entry of login credentials. Lack of credentials recovery and backward compatibility.

DISCUSSION

Password Problem

Passwords are still considered the most popular primary authentication even after 61 years of the origin of the Compatible Time-Sharing System (CTTS) in 1961 and nothing has changed for 35 years since Morris and Thompson first addressed the password problem in 1979. It is most likely to have remained as it is in the near future because none of the alternatives could overcome the simplicity of authentication by typing a keyboard character stream. With the high demand for password complexity and the increased number of password-protected accounts on web services, password mismanagement has also highly increased. But the problem is that the memory capacity of the human brain is limited and it is hard to remember 12-26 unique passwords. Therefore, users tend to create passwords that are easily guessable and reuse the same set of passwords with or without small modifications. Easy memorability, convenience, and speed are the main reasons for password reuse as discussed in the previous literature. Repetitive password verification when creating new passwords is also a good approach for increasing password memorability but it has been proven that the result of this practice is valid for a very limited period. Memorability is more dependent on human psychological factors and the frequency of utilization of a particular password. Multiple sources have discussed that manual password creation is highly biased to the person who is creating and most of them can be easily cracked through various attacks like dictionary attacks, rainbow, social engineering, etc. due to certain patterns and combinations in creation. Password strength checkers, which are used to test the strength of manually constructed passwords, lack consistency and accuracy. Furthermore, they are vulnerable owing to the static password policy that is enforced on all users, which creates a significant bias on specific password features. These strength checkers cannot require high entropy since they cannot assess the usability or memorability of passwords.

To avoid all the shortcomings of manual password creation, random password generation algorithms are used and they are comparatively stronger and more secure than most manually created passwords. Among these algorithms, Google, KeePass, and Bitwarden are well-recognized algorithms that mitigate password reuse and password guessing attacks while providing strong and unique password combinations. But since they are not relevant to the user and the user's background, these randomly generated passwords are highly likely to be forgotten easily and cost a lot of effort to memorize (Lennartsson, 2019). Another concern about these random generator algorithms is a uniform distribution should be there over the entire set of possible passwords generated from the same algorithm based on the same policy. So that could lead to a potential security risk of using randomly generated passwords.

With the time and advancement of technology, many password alternatives were developed but none of them could have been able to replace the traditional textual passwords. Biometric and PIN-based authentications have been the most utilized password alternatives but still passwords are used as the primary authentication in case of loss of access to those authentication mechanisms. Biometric authentication suffers from a lot of privacy concerns. Therefore, most password-protected accounts combine password alternatives with traditional passwords to provide better user convenience. Even though these password alternatives authentication mechanisms have failed to implement themselves as complete replacements for traditional username-password pairs, their combinations with passwords are being used to increase the security of the authentication approach.

Use of Password Managers

As reported in multiple works of literature, users have the challenge of remembering multiple complex passwords for different accounts when the human being is generally poor at memorizing more than seven characters or digits in memory. So human beings are now commonly known as the weakest link of the CIA triad and most security breaches happen from common mistakes done by human beings (Naing Oo, 2022). So basically, in such a scenario of passwords not being able to be replaced and limited human memory capacity, password managers are considered to deliver a fair deal of usability and security trade-off. Password management is about password creation, proper storage, periodical renewal, and providing availability of the credentials whenever they are wanted. Password managers are tools that can fulfil all or a few functionalities of password management. They can be categorized into software password managers and hardware password managers. Online managers and offline managers are the two subcategories of software managers. Online managers provide better usability since they can be accessed from anywhere in the world due to the high availability provided by a service provider through a cloud system.

Online managers can also be divided again into two categories; open-source password managers such as Passbolt, Encryptr, Padlock, etc., and closed-source password managers such as KeePass, LastPass, Roboform,

etc. One of the key benefits of these open-source password managers is that anybody can examine the code and help the refinement process by reporting identified vulnerabilities to developers. The ability to select a preferred server as the centralized password vault is a great feature and potentially increases security and trust in these open-source password managers. On the other hand, being open-source means the attackers can also find vulnerabilities and use them as a weapon for various attacks. Another issue raised is the technical expertise needed to configure a private server to connect to the application is somewhat out of hand for a regular user. Closed-source managers are proprietary, and users have to put complete trust in the company behind the managing service. Since the source code is hidden from the outside world, the proprietor is responsible for updating and keeping the manager clean and secure which preferably attracts more attackers than open-source managing services such as the attack initiated by LastPass in the 2017 first quarter which exploited a massive amount of assets and user data through security flaw existed on LastPass web browser extension (Luevanos et al., 2017). Online managers have a considerably low adoption rate among computer users since the sensitive data are stored in a third-party cloud service and users don't have full control over the cloud system and their data. In such a ubiquitous cyberworld, security-literate users only trust on which they have a satisfactory level of control over their data and related operations (Wang & Khan, 2019).

Offline managers only provide management functionalities within a local environment like a user computer, tab, smartphone, etc. Even though offline managers provide better security and better control over user data compared to online managers, users have to bear the burden of taking the local device everywhere or memorizing the passwords when the device is inaccessible or not available. All software-based password managers consist of a master password to authenticate the legitimate user of the password manager and sometimes it will be used as the encryption key for securing the password vault. Thus, it finally makes it the single failure point of the whole mechanism.

Hardware Based Password Managers

Hardware-based password managers are much better in security and also user credentials are stored in a more isolated environment. But users have to bear the burden of traveling with the password wallet disregarding its design size. There is also a potential security risk of data leakage or data loss if the wallet is stolen or misplaced. The first hardware-based password manager was called "Pico" but it is less user-friendly since it is needed to make relationships with Pico siblings to authenticate the legitimate owner of the device. Since Pico only supports a QR-based login mechanism, all the online services should be able to provide a QR-based login approach unless the device may not be useful for online services or password-protected accounts which do not facilitate QR logins. Pico needs a docking station to be re-charged and while recharging it will make a backup of all user data and information on the device and this is the only back mechanism available for this device. So, users may have to bear the burden of spending extra money on purchasing a docking station as well for the whole backup purpose. With the results of prior research on the usability of token-based authentication and identified problems with the hardware-based Pico system, the Pico project was later focused on the implementation of a smartphone application. They concluded that participants disliked the QR code scanning and suggested replacing the mechanism with another modality to authenticate. However, participants liked the idea of password management being automated.

In PUF-based solutions, every time a user logs into a particular web service, the user has to remember only one password (master password) and they will do the authentication afterward through the PUF-strengthened passwords. This approach can easily mitigate the threat of exposing passwords to third parties since attackers cannot generate the PUF password without physically accessing the same device used for password generation. PUF-based hardware wallets are even more secure than any other available solution, but they do suffer from providing functions such as periodic password renewal, mitigating password reuse, and especially backing up data in case of theft and resistance since the generated password are bound to the physical hardware components and the virgin device cannot be able to regenerate the passwords or restore backed-up data from the old database. This results in a lack of portability and adaptability. Furthermore, current studies that propose PUFs focus primarily on the servers that facilitate cloud infrastructure which is known to be targets of malicious attacks but not on the client-side solutions.

E2PM very small hardware wallet in the size of a flash drive which facilitates better security in contrast to software-based password managers and hardware password wallets E2PM is not very usable for non-technical users since it is not hot pluggable as other hardware wallet managers, but it has increased deployability due to simplicity of hardware and software requirements. In the event of wallet theft, the attacker would not be able to access the password vault since it is protected with a 16-character master password, but it creates the mechanism more vulnerable as well since it is a single point of failure when concerned about security. The author has provided the facts that the master key stored in the RAM can be found by an attacker by initiating a Cold Boot Attack which can obtain RAM contents dumped into the attacker's machine using computer forensic tools. This approach does not provide any loss resistance since there is no backup or migration mechanism available.

CONCLUSION

Passwords have remained the most widely used form of authentication for over six decades, despite their inherent shortcomings and security vulnerabilities. The increasing number of password-protected accounts and the complexity of passwords have led to various malpractices and security breaches. While alternatives such as biometrics and PIN-based authentication have been introduced, they have not been able to completely replace passwords and are often used in combination with passwords for enhanced security. Password managers have emerged as a popular solution to address the challenges of password management. Software-based password managers, both online and offline, offer convenience and security trade-offs. However, they also present potential risks as attackers can exploit vulnerabilities. Hardware-based password managers offer better security and isolation of user credentials but come with the inconvenience of carrying the device and the risk of data loss if stolen or misplaced. The usability of some hardware-based solutions has been a concern, although advances are being made to improve the user experience. The existing password management approaches have their limitations, and there is a need for further research and

development to fully automate the process of manual password management. Future efforts should aim to address the challenges of usability, security, backup mechanisms, and resistance to attacks. By striving for more user-friendly and secure password management solutions, we can enhance the overall security of online accounts and mitigate the risks associated with password mismanagement.

REFERENCES

Abuzaraida, M., & Zeki, A. (2020). Collection of Handwritten text View project Development of Malay Online Virtual Integrated Corpus (MOVIC) for Sentiment Analysis using Web-scraping View project AWARENESS AND SECURITY ISSUES IN PASSWORD MANAGEMENT AMONG LIBYAN UNIVERSITIES STAFF MEMBERS. *Article ID: IJARET_11_12_123 International Journal of Advanced Research in Engineering and Technology*, *11*(12), 1292–1303. https://doi.org/10.34218/IJARET.11.12.2020.123

Aebischer, S., Dettoni, C., Jenkinson, G., Krol, K., Llewellyn-Jones, D., Masui, T., & Stajano, F. (2017). Pico in the Wild: Replacing Passwords, One Site at a Time. *Proceedings 2nd European Workshop on Usable Security*. https://doi.org/10.14722/eurousec.2017.23017

Anand, S., Susila, N., & Balakrishnan, S. (2018). *Challenges and issues in ensuring safe cloud-based password management to enhance security*.

Biesner, D., Cvejoski, K., Georgiev, B., Sifa, R., & Krupicka, E. (2020). Generative Deep Learning Techniques for Password Generation. *ArXiv:2012.05685 [Cs]*. http://arxiv.org/abs/2012.05685

Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M., & Berki, E. (2019). Usability, security and trust in password managers: A quest for user-centric properties and features. *Computer Science Review*, *33*, 69–90. https://doi.org/10.1016/j.cosrev.2019.03.002

Fredericks, D. (2018). *Users' Perceptions Regarding Password Policies*.

Gao, X., Yang, Y., Liu, C., Mitropoulos, C., Lindqvist, J., & Oulasvirta, A. (2018). *Forgetting of Passwords: Ecological Theory and Data Forgetting of Passwords: Ecological Theory and Data*.

Glory, F. Z., Ul Aftab, A., Tremblay-Savard, O., & Mohammed, N. (2019). Strong Password Generation Based On User Inputs. *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. https://doi.org/10.1109/iemcon.2019.8936178

Grilo, M., Ferreira, J. F., & Almeida, J. B. (2021). Towards Formal Verification of Password Generation Algorithms used in Password Managers. *ArXiv:2106.03626 [Cs]*. https://arxiv.org/abs/2106.03626

Guo, Q., Ye, J., Li, B., Hu, Y., Li, X., Lan, Y., & Zhang, G. (2019). PUFPass: A password management mechanism based on software/hardware codesign. *Integration*, *64*, 173–183. https://doi.org/10.1016/j.vlsi.2018.10.003

Gupta, A., Sahu, A., Tarodia, A., & Choudhari, S. (2022). SeCrypt : A Password Manager Aniket Sahu 3 PUBLICATIONS 0 CITATIONS SEE PROFILE. *Article in International Journal of Innovative Research in Science Engineering and Technology*. https://doi.org/10.15680/IJIRSET.2022.1105125|

Gupta, P., Marur, D. R., Kalisetty, H., & Khanna, A. (2020). A novel secure and high-entropy hardware password manager. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2020.09.524

Habib, H., Naeini, P. E., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Christin, N., & Cranor, L. F. (2018). *User Behaviors and Attitudes Under Password Expiration Policies*. Www.usenix.org. https://www.usenix.org/conference/soups2018/presentation/habib-password

Kankane, S., DiRusso, C., & Buckley, C. (2018). Can We Nudge Users Toward Better Password Management? *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3170427.3188689

Kuka, E., & Bahiti, R. (2018). Information Security Management: Password Security Issues. *Academic Journal of Interdisciplinary Studies*, *7*(2), 43–47. https://doi.org/10.2478/ajis-2018-0045

Kurniawan, D. E., Iqbal, M., Friadi, J., Hidayat, F., & Permatasari, R. D. (2021). Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance. *Journal of Physics: Conference Series*, *1783*, 012041. https://doi.org/10.1088/1742-6596/1783/1/012041

Lennartsson, M. (2019). *Evaluating the Memorability of Different Password Creation Strategies: A Systematic Literature Review*.

Luevanos, C., Elizarraras, J., Hirschi, K., & Yeh, J. (2017). Analysis on the Security and Use of Password Managers. *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*. https://doi.org/10.1109/pdcat.2017.00013

Lyastani, S., Schilling, M., Fahl, S., Backes, M., & Bugiel, S. (2018). *Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse*.

Macgregor, R. (2020). *USER COMPREHENSION OF PASSWORD REUSE RISKS AND MITIGATIONS IN PASSWORD MANAGERS*.

Mohammadinodoushan, M., Cambou, B., Afghah, F., Philabaum, C. R., & Burke, I. (2021). Reliable, Secure, and Efficient Hardware Implementation of Password Manager System Using SRAM PUF. *IEEE Access*, *9*, 155711–155725. https://doi.org/10.1109/access.2021.3129499

Mohammadinodoushan, M., Cambou, B., Philabaum, C. R., & Duan, N. (2021). Resilient Password Manager Using Physical Unclonable Functions. *IEEE Access*, *9*, 17060–17070. https://doi.org/10.1109/access.2021.3053307

Morris, R., & Thompson, K. (1979). Password security: a case history. *Communications of the ACM*, *22*(11), 594–597. https://doi.org/10.1145/359168.359172

Naing Oo, A. (2022). *E2PM: Enclosed Portable Password Manager*.

Pearman, S., Zhang, S., Bauer, L., Christin, N., & Cranor, L. (2019). *Open access to the Proceedings of the Fifteenth Symposium on Usable Privacy and Security is sponsored by USENIX. Why people (don't) use password managers effectively Why people (don't) use password managers effectively*.

Rahalkar, C., & Gujar, D. (2019). A Secure Password Manager. *International Journal of Computer Applications*, *178*(44), 5–9. https://doi.org/10.5120/ijca2019919323

Sabev, P., & Petrov, M. (2021). Android Password Managers and Vault Applications: An Investigation on Data Remanence in Main Memory. *Information Systems and Grid Technologies*, *2933*, 314–328.

Sebastian, N. (2021, December 7). *Top Password Strengths and Vulnerabilities: Threats, Preventive Measures, and Recoveries*. Www.goodfirms.co. https://www.goodfirms.co/resources/top-password-strengths-and-vulnerabilities#:~:text=30%25%20of%20the%20Users%20Have

Siddique, K., Akhtar, Z., & Kim, Y. (2017). Biometrics vs passwords: a modern version of the tortoise and the hare. *Computer Fraud & Security*, *2017*(1), 13–17. https://doi.org/10.1016/s1361-3723(17)30007-6

Singh, A., & Raj, S. (2022). Securing password using dynamic password policy generator algorithm. *Journal of King Saud University - Computer and Information Sciences*, *34*(4), 1357–1361. https://doi.org/10.1016/j.jksuci.2019.06.006

Smith, K. (2022). *Random Password Generation*. https://covacci.org/wp-content/uploads/2022/04/Kirk-Smith_Random-Password-Generation.pdf

Stajano, F. (2011). Pico: No More Passwords! *Security Protocols XIX*, 49–81. https://doi.org/10.1007/978-3-642-25867-1_6

Stajano, F., Spencer, M., Jenkinson, G., & Stafford-Fraser, Q. (2015). Password-Manager Friendly (PMF): Semantic Annotations to Improve the Effectiveness of Password Managers. *Technology and Practice of Passwords*, 61–73. https://doi.org/10.1007/978-3-319-24192-0_4

Stobert, E., & Biddle, R. (2018). The Password Life Cycle. *ACM Transactions on Privacy and Security*, *21*(3), 1–32. https://doi.org/10.1145/3183341

Taneski, V., Heričko, M., & Brumen, B. (2014, May 1). *Password security — No change in 35 years?* IEEE Xplore. https://doi.org/10.1109/MIPRO.2014.6859779

Tatli, E. I., & Seker, E. (2018). Password Replacement Patterns. *2018 5th International Conference on Control, Decision and Information Technologies (CoDIT)*. https://doi.org/10.1109/codit.2018.8394966

Wang, Y., & Khan, K. M. (2019). Matrix Barcode Based Secure Authentication without Trusting Third Party. *IT Professional*, *21*(3), 41–48. https://doi.org/10.1109/mitp.2018.2876986

Woods, N., & Siponen, M. (2019). Improving password memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies*, *128*(128), 61–71. https://doi.org/10.1016/j.ijhcs.2019.02.003

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741–759. https://doi.org/10.1007/s10207-019-00429-y

Zimmermann, V., & Gerber, N. (2020). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, *133*, 26–44. https://doi.org/10.1016/j.ijhcs.2019.08.006