Proceeding of ICITS 2022 e-ISSN: 2716-6732
7th International Conference on Information Technology & Society
October 7th & 8th, 2022, Selangor, MALAYSIA

A Review on Password Security Techniques

Siti Nurdiana Abu Bakar, Puteri Azwa Ahmad and Sabri Saep

Politeknik Tuanku Syed Sirajuddin

sitinurdiana@ptss.edu.my, puteriazwa@ptss.edu.my, sabrisaep@ptss.edu.my

Abstract. Despite advances in development of multiple authentication methods such as biometrics, smart cards and security tokens, password remains the most used tool for computer systems authentication. Password is the first line of defense in most information systems, making it an interesting attacker target. Leaked password can pose a serious threat if little attention has been given to secure the password. In this paper, a systematic literature review was carried out based on the techniques of password security proposed by previous researchers. At the same time, users' perception towards password security is discussed in this paper. In general, findings from this review have classified 5 main techniques in password security: hash method, 2-factor/multifactor authentication method, one-time password/single sign-on technique, graphical password, and authentication protocol methods. No matter how good a technique is, users' behavior towards password protection remains the main focus in the area of password security. More users' awareness needs to be taught to ensure continuous good habit in maintaining security. Furthermore, users nowadays show more awareness and more knowledgeable about the importance of password security in safeguarding their private information.

Keywords: Password, password security, password attack, user password management, password protection

INTRODUCTION

Nowadays exists numerous ways to authenticate a person but the most popular method amongst them is with passwords (Nagargoje, 2017). Passwords are used in computer and communications systems to identify users. Passwords are strings of letters, numbers and symbols used to access a user authentication resource to prove their identity in order to obtain access approval (Wakabayashi et al., 2017). Although most people in this world do not want to remember a portfolio of passwords, passwords are familiar, easy to implement and do not require users to carry anything. It is therefore unlikely that passwords will disappear completely soon (Velásquez et al., 2018). But users have a problem in memorizing the text passwords. One user may have many passwords and each new service should create a new password. Users tend to choose weak passwords, even if they know that the password may not be safe and also reuse passwords on different websites. Every day hackers gets better in their technique when they crack sophisticated passwords. Once this happens, they can access the private information and financial information of the users. The so-called password reuse refers to the behavior of the user to choose between multiple different accounts with the same password. Cognitive psychology shows that the behavior is rooted in the limitations of human memory (Bosnjak & Brumen, 2019).

The danger of reusing passwords has become obvious following sustained data breaches which have highlighted the vulnerabilities of web providers. The Ashley Madison case provides a good example (A Retrospective on the 2015 Ashley Madison Breach, 2022). Here, 36 million accounts and their hashed passwords were compromised and posted online, showing that even those users with relatively strong passwords could be vulnerable as the credentials obtained from a hacked website can be used on other potentially more valuable websites (the domino effect of password reuse).

Lists of disclosed passwords are available in bulk on the Internet. A user's password can become known if it is insecurely stored in an applications database and the contents of that database are disclosed. Another strategy for disclosing a user's password involves attempting a brute force attack by automatically attempting common password combinations until a user's password is known. Websites which do not challenge or limit high-frequency log-in attempts makes a good target for this kind of attack (Ali, 2017). 43% of users reused their passwords across multiple websites and there have been user password's breaches from high profile websites including Twitter, Yahoo and LinkedIn (Ducklin, 2020). In 2020 alone, more than 2000 violations have been confirmed leading to the leakage of billions of user records (2022 Data Breach Investigations Report). Leaked passwords may pose serious threats to users especially if the users reuse the passwords elsewhere. The use of the same or even slightly modified passwords allows an attacker to further compromise the accounts of the user in other services.

In order to restrain the effect of a password breach, governments together with organizations come out with various kinds of password security methodologies. In standards published by the United States National Institute of Standards and Technology, when storing or updating passwords, it is a requirement to ensure that they do not contain values that are commonly used, expected or compromised (Grassi, 2020). If this happens, the password will be blacklisted. Meanwhile, some organizations apply renewability mechanism. This security technique contributes to the overall efficiency and safety of the password management solution by limiting the durability of critical system elements. Limiting the lifetime of these elements shortens the amount of time an attacker has to break the component successfully.

There are tremendous number of studies based on password security. For this reason, this study is carried out to provide a systematic and comprehensive reading on password security techniques developed by researchers over the years. This paper aims to review previous studies on the techniques of password security from 2017 to 2022. Researchers, lecturers, and students in information security fields are expected to benefit from this study. This paper's structure is organized as follows: Section 2 presents the methodology used in this study, a Systematic Literature Review (SLR). Section 3 describes the results of the study on password security techniques and the perception of users about password security. This study is finally completed in the last section and a table on the limitation of password security techniques is presented.

METHOD OF STUDY

The Systematic Literature Review (SLR) is a means of evaluating and interpreting all research available relevant to a particular research problem or area of interest or phenomenon (Gusenbauer & Haddaway, 2020). The same study also noted that SLR offers methodological advantages and application for research issues. It comprises three main phases of planning, conducting and reporting. The best way to achieve this research objective is to assign research questions or a uniform description for this review. The research questions involved are: -Question 1: What are the existing passwords security techniques? Question 2: How users perceive password security?

A review protocol is essentials in SLR in order to guide the search process. The protocol defines inclusion / exclusion criteria to be selected in the primary studies, as shown in Table 1 based on research questions. The inclusion and exclusion criteria are determined after the research question has been established usually before the search is carried out. Many different factors can be used as inclusion or exclusion criteria such as peer review, date, reported outcomes, study design, participants or type of publication (Gusenbauer & Haddaway, 2020).

TABLE 1. Inclusion/Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Conference or journal between 2017-2022.	Conference or journal before 2017 or similar study that exists
Password security, password attack, user perception on password	Authentication method other than password

Search Process

Relevant papers, journals, conferences, and articles were retrieved manually from the databases as a source to the review. To make this SLR credible, studies which have no validation have been deliberately excluded. Finally, studies that passed this screening process were selected in this SLR for further analysis. This review covers preceding studies between 2017 and 2022.

Data Sources

As shown in Table 2, the following databases are chosen as the study sources. This selection is based on the previous study (Xiao & Watson, 2017), which is the most promising one. Furthermore, secondary searches are conducted based on references found in the primary sources.

TABLE 2. Electronic Database

Electronic Database
IEEE Xplore
Academia.edu
ACM Digital Library

ResearchGate
SpringerLink
ScienceDirect
Usenix.org

The availability of many data sources accessible through electronic libraries gives all relevant publications reasonable confidence. These sources include journals in Table 3.

TABLE 3. List of Journal

Journal
Institute of Electrical and Electronics Engineers (IEEE) Journal
International Journal of Research in Engineering, Science and Management
International Journal of Network Security & Its Applications
Journal of Planning Education and Research
International Journal of Engineering Research and Advanced Technology (IJERAT)
International Journal Human-Computer Studies
Journal of Information Security and Applications
International Journal of Computer Trends and Technology (IJCTT)
Journal of Cybersecurity
International Journal of Engineering Research and General Science
Journal of Computing Science and Engineering
Journal of Network and Computer Applications
Journal of Management Information Systems
International Journal of Innovative Research and Advanced Studies (IJIRAS) International Journal of Pure and Applied Mathematics

Search Terms

This section sets the search terms for searching databases. Some keywords were derived from the research questions. A search string was developed based on the research questions using relevant terms. The following search strings were used: “password security” or “password attack” or “user perception on password” or “user password management” or “password”. Before selecting the papers for the SLR, it is checked to ensure that there is no duplication, e.g., if the same study is published in two different journals with different first authors. If this occurred, the most comprehensive study or the latest study will be selected.

RQ1: EXISTING PASSWORD SECURITY TECHNIQUES

In order to investigate the above research questions, 56 studies were identified and presented as follow:

Hash technique

Client-side password hashing can be used to generate unique passwords for different websites, thus helping mitigate the risk of password reuse. However, hashing alone is not secure enough as it is prone to dictionary attacks and brute-force attacks (Adding Salt to

Hashing: A Better Way to Store Passwords, 2021). Visconti et al., (2019), suggest the use of Password-based key derivation function 2 (PBKDF2), an algorithm that incorporates password/passphrase input mechanisms; usually a short and random cryptographic key and at the same time slows down as much as possible brute force and dictionary attacks. In 2017, Ali (2017) proposes a service to validate whether a password has been breached by using an anonymized version of the password hash in a database. From his findings, justin-time fear appeal have had success at persuading users to replace breached passwords. However, there is a limitation to this method as the number of hash prefix increases in size. File management tools can struggle to handle such a vast quantity of files and, without adopting a directory structure, file systems can even reach their limit for the number of files in a single directory. While Álvarez et al., (2018) proposed Useful Password Hashes (UPHs), this technique requires servers not to store passwords in plain text, but to use password hashes. UPH also makes good use of the computer cycles used to compute password hashes by solving various cryptographic problems. Honeywords also known as false passwords; a way to improve hashed password security (Sawant et al., 2018). An adversary who steals a file of hashed passwords and tries to log in will send an alarm guarded by a honeychecker. However, there are several limitations to this technique, such as multiple system vulnerability, low DoS resistivity and overhead storage, mentioned by (Chakraborty et al., 2022). Park (2018) proposed a new one-time password (OTP) without shared secrecy and re- registration based on the hash chain. This new hash function is designed to address the weakness of the older version of OTP, consisting of finite hash algorithms generation. This new approach can be used in the future for the design of a number of cryptographic protocols.

Two-factor/multifactor authentication method

The trend towards multi-factor authentication has been strengthened by technology companies claiming that " passwords are dead" and the US government launch a national campaign to "move beyond passwords" (Terdiman, 2013). The 3D password is an example of multipassword and multifactor authentication system. This technique can eliminate brute-force attack, prevention against key-logger software and provides user options to choose the type of authentication of his/her own choice (knowledge base, token base, recognition base or biometrics base). But its main disadvantages are time and memory consuming because 3D password needs larger storage space (Nandhini & Sankar, 2019). Password and smart card authentication are commonly used in Internet-based applications such as remote user/server login, online banking, Pay-TV and electronic voting. This type of authentication, however, is prone to off- line password guessing attack in which an attacker lists all possible passwords offline to find the correct password on the lost / stolen smartcard (Yang et al., 2020). To minimize the loss or exposure to theft of smart card, biometric authentication has come into use. Biometrics refers to the automatic identification or verification of identity of living persons using their long lasting physical or behavioral characteristics (Machado et al., 2018). One example of biometrics is fingerprint. Bian et al., (2020) have introduced a secure two-factor user authentication system with password and fingerprint information. They prove that replay attacks and manin-the-middle attacks can be prevented using this method through their research. However, the existing authentication scheme based on fingerprints and the fingerprint

security itself must be improved in order to have a significant impact on the authentication of the user.

Keystroke dynamics is a biometric solution in which rhythmic keyboard typing and timing between the pressed key is used as an authentication technique for users (Mohlala et al., 2017). No extra hardware required and that only programming skills are sufficient, but high rejections occur due to different typing speeds of users. Even the legitimate user is difficult to identify.

One-Time Password/Single Sign-On Method

Researchers also come out with session password method or also known as One-Time Password (OTP) (Erdem & Sandikkaya, 2019). OTP is a password that only applies to one login session. A user can have as many passwords as he/she want but all of those passwords are only valid for one time use only. This technique is suitable to prevent replay attack. On the downside note, OTPs are difficult for humans to memorize, because they are only used once. Users must remember another set of passwords when they log in next time. Therefore, additional technology is necessary to make it work. The Single Sign- On concept (SSO) allows legal users to access different service providers in distributed computer networks using a unitary token (Tapade, 2017). You just need to authenticate once and then you can easily access multiple applications securely on different domains (Purkayastha et al., 2017). As far as security is concerned, SSO allows users to remember only one password, which users prefer to use complex, hard-to-crack passwords rather than multiple simple passwords. The system security can be improved. However, a single failure point can occur because this arrangement is prone to Denial of Service (DoS) attack because the authentication mechanism is centralized (Alaca & Oorschot, 2020). Swathi (2017) also comes out with virtual password mechanism where using secret little function, a password is generated. The secret features are kept secret. The user calculates the virtual password manually during login time using registered information while the server calculates the password. When both values are equal, users will get access to information. It is only valid for a single use. The disadvantage of this mechanism is that all registered values are hard to remember, and another storage media is required to store all the values.

Graphical password technique

FIGURE 1. Top; image without saliency mask. Bottom; image with saliency mask.

Since people interact in an environment in which vision predominates for most activities, our brains are able to easily process and store large amounts of graphic information. Graphical password systems therefore provide a way to make passwords more humane while increasing the level of security (Albalawi et al., 2019). According to Suru & Murano (2019) graphical passwords promise increased resistance to attacks due to the possibly larger password space but also prone to shoulder surfing (Por et al., 2017).

Graphical passwords can be divided into 2 types: 1) Recall-based method 2) Recognition based-method (Zimmermann & Gerber, 2020). For type (1) cued-recall graphical passwords known as PassPoints has been introduced. In this technique, user logs in by clicking the same 5-point sequence (password) in the same order to be authenticated

(Katsini et al., 2018). The user is also given a hint that helps him/her to remember the passwords he/she chose during the registration phase (Barkadehi et al., 2018). PassPoints have security problems caused by users who choose popular points or hotspot that help automated attacks to succeed (Kaja & Gupta, 2017). But in 2021, researchers Constantinides et al., (2021) comes out with an improved version to prevent users from selecting weak passwords during the registration phase by clicking on the same hotspot, the cued-recall technique combines with " saliency masks". Fig. 1 shows a sample image with and without saliency mask technique. The researchers mask the areas of the image which attract visual attention. Saliency masks enable the user to select safer passwords and thereby reduce the risk of hotspots in authentication images (Dupuis et al., 2020). Meanwhile, Lazim and Zakaria (2018) introduced distortion technique known as twirl images with clockwise slider to blur any images use as graphical password authentication in which only the genuine user knows the true meaning of the blurred images. This technique proves to cope well with shoulder surfing attack.

Meanwhile, recognition-based technique allows users to select images, logos or any preset image symbols. Users must recognize the image they choose as their password for the authentication process. Phishing attacks are harder to happen with recognition-based systems because a correct set of images must be presented to the user before entering the password. However, shoulder surfing attack appears to be a concern when an attacker stands behind the user and sees or observes user selected images during login (Shammee et al., 2020). To overcome this problem, Dupuis et al., (2020) proposed a graphical password authentication method that is resistant to shoulder surfing. The system is a combination of recognition and pure recall technique. This system offers a number of advantages, such as easy to use and memorize, easy to create the password and a random nature in the authentication phase.

CAPTCHA stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart (Srivastava et al., 2020) has been developed to distinguish between computer programs and people. A CAPTCHA protects websites from bots by generating and classifying tests that can be passed by humans, but current computer programs cannot (Chen et al., 2017). While this mechanism provides good security and limits automatic web registration, some CAPTCHAs have several weaknesses that allow hackers to infiltrate the CAPTCHA mechanism. CAPTCHA based on images needs user to select the suitable image depend on the question under the CAPTCHA. Although this type is simple there are some problems involve; some users who have low vision or learning disability will meet some issues when they are attempting to solve this CAPTCHA and probability of bot programs breaking the CAPTCHA will increase if the number of choices is decreased so it

is better to create more options in CAPTCHA to make it strong however this mechanism will consume the database (Uma et al., 2019).

Millions of users are exposed to password strength meters/ checkers in every popular web service using authentication passwords selected by the user. It tells users if they have "weak" or " strong" passwords. Stobert & Biddle (2018) examine whether password meter influence password selection and the results is users tend to choose a stronger password when they were forced to change existing password by the password meters. Apparently, a better approach is to provide adequate feedback to users on the quality of their selected passwords, with the hope that such feedback will voluntarily influence them. Password strength meters play a key role in providing feedback for this approach and should do so consistently to prevent possible user confusion. Golla & Dürmuth (2018) suggested a new measure of strength that could easily be integrated into password meters. They used a Markov N-gram model to predict characters and constructed an adaptive strength meter. However, they have not validated their meter with real users so that it is unknown to what extent their new meter can influence user behavior.

Ur et al., (2017) suggested using a data- driven password meter with detailed feedback so that users know whether their password is wrong or how to improve it, which automatically led users to create safer and less memorable passwords than a meter with only a bar as a strength indicator. Users would be able to make better password choices if they understood how password guessing attacks work by using infographic posters and online educational comics than just reading a set of instructions for creating strong passwords. Xu et al., (2021) suggest the use of persuasive password guidelines method which contains 3 stages; 1) exposure stage-give basic knowledge to users, 2) attention stage-grab users attention for the targeted behavior and 3) comprehension stage-provide support in engaging toward the targeted behavior. They conclude that supporting and guiding users with a clear security messages or security instructions can result in creation of strong password among users.

Authentication Protocol

There are several authentication protocols introduced in password security. oPass is a user authentication protocol developed to protect the identity of the user by creating a unique password involving a cell phone telecommunications service provider (TSP) and a participating website in the registration and recovery phases (Chakraborty et al., 2022). Users must only remember a long-term login password on all sites. But oPass needs to come out with an alternative in password recovery if users lose their mobile phone. Password Guessing Resistant Protocol (PGRP) by Ramesh et al., (2020) designed to restrict large scale online dictionary attack. This protocol limits the number of logins attempts per username from unknown remote hosts to as low as one. But legitimate users can make several failed logins attempts from known, frequently used machines before they are challenged with an Automated Turing Test (ATT). PGRP may also be used for remote login services where cookies (e.g., SSH and FTP) are not applicable. Sinha et al., (2022) proposed a Three-party Password-based Authenticated Key Exchange (3PAKE) protocol. This protocol allows two clients to authenticate each other and establish a secure session key over an insecure channel through a server. Its main goal is authentication and privacy. However, this protocol does not work because it is exposed to off-line passwords guessing attack and impersonation attack, so that they come with an improved 3PAKE protocol

(Mishra, 2017). In this improved 3PAKE, they can deter offline password guessing attack by using the server's public keys.

In 2019, researchers Shirvanian et al., comes out with a new authentication protocol yield from combination of two protocols; Schnorr's Zero Knowledge Password Proof and Fiat-Shamir Heuristic that prevents offline dictionary attacks through the combined use of a non-interactive and a sequentially memory hard one-way function. CCT also known as Cryptographic Cipher Text is a verification protocol in which the cipher text is encoded and decoded by using hash function. The secret code entered by the user will be encoded as plain text and decoded by the server as cipher text and delivered to the user's email-id as One-Time Secret Code (OTSC). The user the opens his/her email account and enters the OTSC number generated by server on the login page. This approach has been proven to thwart against secret code pilfering.

RQ2: HOW USERS PERCEIVE PASSWORD SECURITY

User behavior could be quite common issue within the area of password security and plenty of security departments treat users as a security risk that must be controlled. Users ordinarily are not mindful about the dangers and the significance of password related attacks. These are the challenges facing security organizations or services that lead to the development of useless safety mechanisms. Password cracking and survey data confirmed that many users maintain a poor strategy to maintain multiple password-protected accounts. After users has saved their passwords, they always have the chance to forget it. Users have many passwords, and the handling of forgotten passwords is clearly a large part of password management (Pearman et al., 2017).

Hundreds of research studies have been carried out at the general intersection of usability and security but few have investigated users' perceptions in particular. Folk models found that the mental models of non-expert users often differ from experts' models (Feth et al., 2017). For example, non-experts perceive the loss of a password as similar to the loss of a key, while experts perceive that same event as the loss of a credit card number and it is more serious. Many users view passwords as a burden and exhibit potentially unsafe password management behavior (Woods & Siponen, 2019). However, many of these behaviors are probably rational coping strategies for users who are asked to make passwords that are far more distinct and complex than they might recall. Users often reuse passwords across accounts even if they don't completely reuse a password, they often make only small, predictable changes (Wash & Rader, 2021).

Survey by Parkinson et al., (2022) shown that although most users are aware of and use a fixed set of passwords for content sites, most of these conscious users also reuse this fixed set of passwords for their identity or financial accounts. These indicate that although users consider their identity passwords to be significantly more important than their lower security passwords, they are not sufficiently aware of attacks that could leverage these lower security passwords to guess their identity passwords, which can lead to a domino effect. Leaked passwords may pose serious threats to users, especially if the users reuse the passwords elsewhere. The reuse of leaked passwords or even a slightly modified version of the passwords opens the door for attackers to further compromise user accounts in other services.

Users mainly concerned with targeted attacks on their passwords rather than automated large-scale attacks. As a result, some users believed that the name of their pets or birthdays

would be strong passwords because they had not posted this information on their Facebook page and did not account for the types of automated guessing attacks often seen in the wild. Users also appeared to misunderstand the effect of reuse of passwords on security. When an account is compromised, reuse becomes problematic and the attacker can attack a highvalue account with the same credentials. For each of its high-value accounts, a user should therefore have a set of separate passwords, while reuse is rational for low-value accounts (Blocki et al., 2018). In a survey by Park (2018), many participants thought it was secure by just adding a symbol at the end of the password. Users must be made aware that digits and symbols are not a shield for password security. The lack of awareness of computer security and the lack of knowledge about how to apply security measures were also identified as contributing factors to poor security practices (Menard et al., 2017).

Therefore, password mechanisms must apply a user-centric approach to design usable security in which human factors should be given priority over technological factors. Researchers have suggested that ignorant users should be informed about security mechanisms and that non-compliant users should be persuaded to follow safety best practices in password security (Maoneke et al., 2018). It was argued that if security knowledge is made more accessible, it is more likely that users are motivated to practice safety.

Password problem solutions mainly consist of password managers, an application that stores and enters the passwords for users, thus saving the users from remembering their passwords. For example; browser-based password managers such as Chrome save passwords when entered in the relevant fields and automatically enter them when the page is visited again. While dedicated password managers like LastPass work like a password pilot (Computer Hope, 2022). Just saved all your passwords in their database and here you go, fast and easy logging to all websites. Research on password managers shown that they are prone to attack amplification via password sync because they offer synchronization services between different devices (Wang et al., 2021). A proactive alternative should be implemented to encourage users to select appropriate passwords for each account, and website developers also could help users to link passwords to accounts by providing clues and password rules.

It is often difficult for users to create passwords according to strict requirements. Some providers provide real-time feedback during password creation to make this process easier, indicating which requirements have not yet been met. Other providers guide users through a multi-step password-creation process. Password creation feedback in real time can also help users create strong passwords with fewer errors As time changes, more users nowadays are aware of password security and the importance to create a strong password. Users tend to realize that reuse of passwords is completely unsafe. They thought that passwords based on song lyrics or relevant dates would be memorable, but realized that these passwords were also unsafe (Alomari et al., 2019). The intention of users to comply with the recommended security measures is believed to be a function of how they perceive security risks including perceptions of the likelihood of a threat, how vulnerable they feel and the perceived consequences of the threat (Thompson et al., 2017). The decisions of users to implement security measures have been demonstrated by their awareness and knowledge of password attacks and their effect on them.

DISCUSSION

In the beginning of the study, the research questions were set as follows:

Question 1: What are the existing passwords security techniques?

There are numerous and abundance of techniques on password security produced by researchers around the world. In this paper, 5 classifications of password categories were presented based on 56 studies. Fig. 2 shows 44.64% focus on graphical password technique, 12.5% based on OTP/SSO method same percentage with authentication protocol, hash techniques contribute 14.27% and 16.07% come from 2-factor/multifactor method on password security. For each class, many techniques were discussed including their limitations as listed in Table 4. Graphical password is the most discussed password security techniques. This is because the graphic password is better than the password based on text. Moreover, the graphical password scheme resists major password attacks better than others (Katsini et al., 2019).

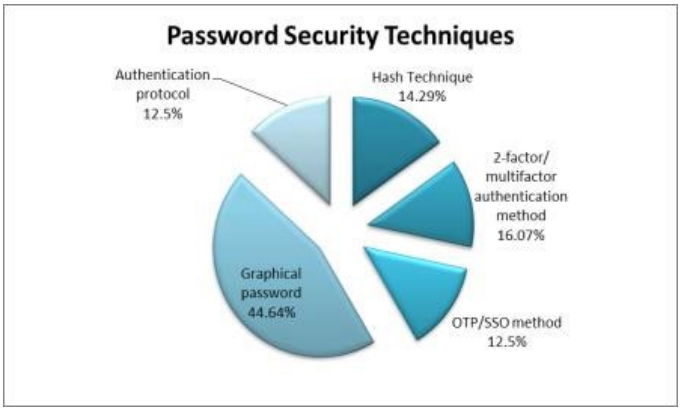

FIGURE 2. Classification of password security techniques.

Question 2: How users perceive password security?

The human factor is the most important factor in the security system; it is the weakest link. Urban user might consider password breach as important as losing all their valuable data (identity and account data) whereas for rural area users, they might not bother about password breach as long as it does not do any harm to them visibly. This knowledge gap is the main issues that need to be addresses by developers, organizations and researchers. More fact-findings need to be documented on the knowledge gap between these users.

In password security aspect, awareness education programme, password security guide and password policies should be implemented by organizations or system developer to assist users in creating a stronger password. Developer should not put the burden of creating strong password on users solely. They also have to equip their websites or systems with appropriate information at the login page for example a persuasive guideline which can assist users to create strong passwords that are easy to remember.

TABLE 4. Limitation of Several Password Security Techniques

Research Categories	Techniques	Limitation
Hash technique	PBKDF2 (Visconti et al., 2019)	Attacker still able to avoid 50% of PBKDF2's CPU intensive operations, by replacing the passphrase with pre-computed values to reduce even more the key derivation time.
	Anonymized password ha n a database (Ali, 2017)	This approach can rapidly become impractical as the number of hash prefix increases in size. File management tools can struggle to handle such a vast quantity of files and, file systems can even reach their limit for the number of files in a single directory.
	Honeyword (Sawant et al., 2018).	Multiple system vulnerability, weak DoS resistivity, and storage overhead.
Two-factor/ multifactor authentication method	3D password (Nandhini & Sankar, 2019).	Memory and time consuming because 3D password need larger storage space
	Multifactor authentication (Nandhini & Sankar, 2019).	Prone to off-line password guessing attack in which an attacker exhaustively enumerates all possible passwords in an offline manner to find out the correct password on lost/stolen smartcard.
	Keystroke dynamics (Mohlala et al., 2017)	Different typing speed of users make it harder to identify even the legitimate user
Graphical password technique	Passpoint (Katsini et al., 2018).	Users tend to choose hotspot in images which help the success of automated attacks.
	Image CAPTCHA (Chen et al., 2017	Users who have low vision or learning disability will meet some issues when they are attempting to solve this CAPTCHA Probability of bot programs breaking the CAPTCHA will increase if the number of choices is decreased however to increase the choices this mechanism will consume the database. The huge number of saved images on the server, can slow down authentication process as network traffic causes delays.
	Password meter (Stobert & Biddle, 2018)	Major password meters from high-profile web services are simplistic in nature and designed in an ad-hoc manner (provide inaccurate strength estimates).
	Recognition-based technique (Shammee et al., 2020)	Exposed to shoulder surfing attack where the attacker is standing behind the user and sees or observes the images selected by users during the login process.

	Markov N-gram model (Golla & Dürmuth, 2018)	No validation of their approach with real users.
One-time password/ single sign-on method	One-Time Password (OTP) (Park, 2018)	Difficult for human beings to memorize
	Single Sign-On (SSO) (Tapade, 2017).	Prone to DoS attack as the authentication mechanism is centralized
	Virtual password (Swathi, 2017)	Difficult to remember all the registered values, therefore another storage media is needed to store all the values.
Authentication Protocol	Password Guessing Resistant Protocol (PGRP) (Ramesh et al., 2020)	Expose to "false negative" attempt when actually the real user is trying to connect multiple times to the website.
	Three-party Password-based Authenticated Key Exchange (3PAKE) (Sinha et al., 2022)	Vulnerable to off-line password guessing attack and impersonation attack.
	oPass (Chakraborty et al., 2022).	Users will face difficulties in recovering their passwords in case of stolen/lost mobile phones.

CONCLUSION

Passwords are the first defense line in any information system, but they are still the weakest link in security. Researchers around the world had come out with various kinds of password security techniques in order to safeguard our data. There are substantial number of techniques discussed on passwords security but in this study only a number of research published between 2017 and 2022 are collected and organized into 5 main techniques. Other related techniques on password security and authentication mechanism on mobile devices that did not match this study are not taken into account. One clear finding from this study is that insufficient knowledge of password procedures among users contributes to the creation of unsecure password. Organizations and developers shift the responsibility of providing secure passwords to users. Known rules for creating secure passwords have however seldom been communicated to users. Users have been asked to create a strong password without adequate training, education or online feedback. Can users be prevented from reusing passwords? It is unlikely, given the rapid rate of increasing online services and applications. However, users can be taught or made aware of the likelihood of hacking when using weak passwords and the possible consequences if a hacking incident is successful, which can significantly increase their concern about password-related threats, and the impact of non-compliance. It's never too late to start a new habit of creating a strong password

REFERENCES

1. Adding Salt to Hashing: A Better Way to Store Passwords. (2021, February 25). Auth0 - Blog. Retrieved August 1, 2022, from https://auth0.com/blog/adding-salt-to-hashinga-better-way-to-store-passwords/
2. Alaca, F., & Oorschot, P. C. V. (2020, October 15). Comparative Analysis and Framework Evaluating Web Single Sign-on Systems. ACM Computing Surveys, 53(5), 1–34. https://doi.org/10.1145/3409452

3. Albalawi, A., Almrshed, A., Badhib, A., & Alshehri, S. (2019, April). A Survey on Authentication Techniques for the Internet of Things. 2019 International Conference on Computer and Information Sciences (ICCIS). https://doi.org/10.1109/iccisci.2019.8716401
4. Ali J. (2017). Mechanism for the prevention of password reuse through Anonymized Hashes. PeerJ Preprints 5:e3322v1 https://doi.org/10.7287/peerj.preprints.3322v1 5. Alomari, R., Martin, M. V., MacDonald, S., Maraj, A., Liscano, R., & Bellman, C. (2019, August). Inside out - A study of users' perceptions of password memorability and recall. Journal of Information Security and Applications, 47, 223–234. https://doi.org/10.1016/j.jisa.2019.05.009
6. Álvarez, R., Andrade, A., & Zamora, A. (2018, December 3). Optimizing a Password Hashing Function with Hardware-Accelerated Symmetric Encryption. Symmetry, 10(12), 705. https://doi.org/10.3390/sym10120705
7. A Retrospective on the 2015 Ashley Madison Breach. (2022, July 27). Retrieved July 30, 2022, from https://krebsonsecurity.com/2022/07/a-retrospective-on-the-2015ashley-madison-breach/
8. Barkadehi, M. H., Nilashi, M., Ibrahim, O., Zakeri Fardi, A., & Samad, S. (2018, August). Authentication systems: A literature review and classification. Telematics and Informatics, 35(5), 1491–1511. https://doi.org/10.1016/j.tele.2018.03.018
9. Bian, W., Gope, P., Cheng, Y., & Li, Q. (2020, August). Bio-AKA: An efficient fingerprint based two factor user authentication and key agreement scheme. Future Generation Computer Systems, 109, 45–55. https://doi.org/10.1016/j.future.2020.03.034
10. Bosnjak, L., & Brumen, B. (2019). Rejecting the death of passwords: Advice for the future. Computer Science and Information Systems, 16(1), 313–332. https://doi.org/10.2298/csis180328016b
11. Chakraborty, N., Li, J., Leung, V. C. M., Mondal, S., Pan, Y., Luo, C., & Mukherjee, M. (2022, August 3). Honeyword-based Authentication Techniques for Protecting Passwords: A Survey. ACM Computing Surveys. https://doi.org/10.1145/3552431
12. Chen, J., Luo, X., Guo, Y., Zhang, Y., & Gong, D. (2017). A Survey on Breaking Technique of Text-Based CAPTCHA. Security and Communication Networks, 2017, 1–15. https://doi.org/10.1155/2017/6898617
13. Computer Hope. (2022, July 31). How to View, Save, and Remove Browser Passwords. Retrieved October 1, 2022, from https://www.computerhope.com/issues/ch000731.htm
14. Constantinides, A., Belk, M., Fidas, C., & Pitsillides, A. (2020, March 4). An eye gazedriven metric for estimating the strength of graphical passwords based on image hotspots. Proceedings of the 25th International Conference on Intelligent User Interfaces. https://doi.org/10.1145/3377325.3377537
15. Ducklin, P. (2020, April 6). Serious Security: How to store your users' passwords safely. Naked Security. Retrieved July 30, 2022, from https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-yourusers-passwords-safely/
16. Dupuis, M. J., Shorb, J., Walker, J., Holt, F. B., & McIntosh, M. (2020, October 7). Do You See What I See? Proceedings of the 21st Annual Conference on Information

Technology Education. https://doi.org/10.1145/3368308.3415458
17. Erdem, E., & Sandikkaya, M. T. (2019, March). OTPaaS—One Time Password as a Service. IEEE Transactions on Information Forensics and Security, 14(3), 743–756. https://doi.org/10.1109/tifs.2018.2866025
18. Feth, D., Maier, A., & Polst, S. (2017). A User-Centered Model for Usable Security and Privacy. Human Aspects of Information Security, Privacy and Trust, 74–89. https://doi.org/10.1007/978-3-319-58460-7_6
19. Golla, M., & Dürmuth, M. (2018, January 15). On the Accuracy of Password Strength Meters. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3243734.3243769
20. Grassi, P. A. (2020, January 27). Digital Identity Guidelines: Authentication and Lifecycle Management. NIST. Retrieved August 2, 2022, from https://www.nist.gov/publications/digital-identity-guidelines-authentication-andlifecycle-management
21. Gusenbauer, M., & Haddaway, N. R. (2020, January 28). Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. Research Synthesis Methods, 11(2), 181–217. https://doi.org/10.1002/jrsm.1378
22. Kaja, S., & Gupta, D. (2017, August). Graphical password scheme using persuasive cued click points. 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon). https://doi.org/10.1109/smarttechcon.2017.8358450
23. Katsini, C., Fidas, C., Belk, M., Samaras, G., & Avouris, N. (2019, February 14). A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication. International Journal of Human–Computer Interaction, 35(19), 1800–1812. https://doi.org/10.1080/10447318.2019.1574057
24. Katsini, C., Fidas, C., Raptis, G. E., Belk, M., Samaras, G., & Avouris, N. (2018, April 19). Influences of Human Cognition and Visual Behavior on Password Strength during Picture Password Composition. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3173574.3173661
25. Machado, S., D'silva, P., D'mello, S., Solaskar, S., & Chaudhari, P. (2018, August). Securing ATM Pins and Passwords Using Fingerprint Based Fuzzy Vault System. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). https://doi.org/10.1109/iccubea.2018.8697794
26. Maoneke, P. B., Flowerday, S., & Isabirye, N. (2018). The Influence of Native Language on Password Composition and Security: A Socioculture Theoretical View. ICT Systems Security and Privacy Protection, 33–46. https://doi.org/10.1007/978-3319-99828-2_3
27. Menard, P., Bott, G. J., & Crossler, R. E. (2017, October 2). User Motivations in Protecting Information Security: Protection Motivation Theory Versus SelfDetermination Theory. Journal of Management Information Systems, 34(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083
28. M. H. M. Lazim and N. H. Zakaria, "Security Evaluation of Distortion Technique for Graphical Authentication," Communications in Computer and Information Science User Science and Engineering, pp. 313–324, 2018.

29. Mishra, D. (2017, August 14). Efficient and secure two-factor dynamic ID-based password authentication scheme with provable security. Cryptologia, 42(2), 146–175. https://doi.org/10.1080/01611194.2017.1325787
30. Mohlala, M., Ikuesan, A. R., & Venter, H. S. (2017, November). User attribution based on keystroke dynamics in digital forensic readiness process. 2017 IEEE Conference on Application, Information and Network Security (AINS). https://doi.org/10.1109/ains.2017.8270436
31. Nagargoje, Y. (2017, December). Prevention Against Online Password Guessing Attacks Using Image Based Authentication Technique PCCP. Open Access International Journal of Science & Engineering, 2(12). http://oaijse.com/VolumeArticles/FullTextPDF/282_Prevention_Against_Online_Password.pdf
32. Nandhini, K., & Sankar, R. (2019, April). 3D Password for more Secure Authentication in Android Phones. International Journal of Research in Engineering, Science and Management, 2(4). https://www.ijresm.com/Vol.2_2019/Vol2_Iss4_April19/IJRESM_V2_I4_55.pdf
33. Park, C. S. (2018, June). One-time password based on hash chain without shared secret and re-registration. Computers &Amp; Security, 75, 138–146. https://doi.org/10.1016/j.cose.2018.02.010
34. Parkinson, S., Khan, S., Badea, A., Crampton, A., Liu, N., & Xu, Q. (2022b, June 27). An empirical analysis of keystroke dynamics in passwords: A longitudinal study. IET Biometrics. https://doi.org/10.1049/bme2.12087
35. Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., & Forget, A. (2017, October 30). Let's Go in for a Closer Look. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3133956.3133973
36. Por, L. Y., Ku, C. S., Islam, A., & Ang, T. F. (2017, October 18). Graphical password: prevent shoulder-surfing attack using digraph substitution rules. Frontiers of Computer Science, 11(6), 1098–1108. https://doi.org/10.1007/s11704-016-5472-z
37. Purkayastha, S., Gichoya, J. W., & Addepally, A. S. (2017). Implementation of a single sign-on system between practice, research and learning systems. Applied Clinical Informatics, 26(01), 306–312. https://doi.org/10.4338/aci-2016-10-cr-0171
38. Ramesh, K., Kumar, B. A., & Renjith, P. (2020, February). Treats based Revisiting Defences Against Password Guessing Attacks and Phishing Data Over Different Online Records. 2020 International Conference on Inventive Computation Technologies (ICICT). https://doi.org/10.1109/icict48043.2020.9112417
39. Sawant, S., Saptal, P., Lokhande, K., Gadhave, K., & Kaur, R. (2018). Honeywords: Making Password Cracking Detectable. International Journal of Engineering Research and Advanced Technology (IJERAT), 4(4). https://doi.org/10.7324/ijerat.2018.3218
40. Shammee, T. I., Akter, T., Mou, M., Chowdhury, F., & Ferdous, M. S. (2020, December 31). A Systematic Literature Review of Graphical Password Schemes. Journal of Computing Science and Engineering, 14(4), 163–185. https://doi.org/10.5626/jcse.2020.14.4.163
41. Shirvanian, M., Saxena, N., Jarecki, S., & Krawczyk, H. (2019, September 1). Building and Studying a Password Store that Perfectly Hides Passwords from Itself. IEEE

Transactions on Dependable and Secure Computing, 16(5), 770–782. https://doi.org/10.1109/tdsc.2019.2902551

42. Sinha, V. K., Anand, D., Kaur, S., Singh, P., & Noya, I. D. (2022, July 29). Security Verification of Social Network Model Using Improved Three-Party Authenticated Key Exchange Protocol. Symmetry, 14(8), 1567. https://doi.org/10.3390/sym14081567
43. Srivastava, M., Sakshi, S., Dutta, S., & Ningthoujam, C. (2020, November 28). Survey on Captcha Recognition Using Deep Learning. Advances in Intelligent Systems and Computing, 273–282. https://doi.org/10.1007/978-981-15-7394-1_26
44. Stobert, E., & Biddle, R. (2018, June 2). The Password Life Cycle. ACM Transactions on Privacy and Security, 21(3), 1–32. https://doi.org/10.1145/3183341
45. Suru, H., & Murano, P. (2019, February). Security and User Interface Usability of Graphical Authentication Systems – A Review. International Journal of Computer Trends and Technology (IJCTT), 67(2). http://pietromurano.org/Papers/Published%20Version%20Murano%20Suru.pdf
46. Swathi, S. (2017, February). Implementation Of Privacy Preservation Using Anonymization Methods for Discrimination Prevention. International Journal of Innovative Research and Advanced Studies (IJIRAS), 4(2). http://www.ijiras.com/2017/Vol_4-Issue_2/paper_54.pdf
47. Tapade, V. (2017, April). A Survey on Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks. International Journal of Engineering Research and General Science, 5(2). http://pnrsolution.org/Datacenter/Vol5/Issue2/1.pdf
48. Terdiman, D. (2013, September 10). Google security exec: "Passwords are dead." CNET. Retrieved August 1, 2022, from https://www.cnet.com/news/privacy/googlesecurity-exec-passwords-are-dead/
49. Thompson, N., McGill, T. J., & Wang, X. (2017, September). "Security begins at home": Determinants of home computer and mobile device security behavior. Computers &Amp; Security, 70, 376–391. https://doi.org/10.1016/j.cose.2017.07.003
50. Uma, P., Siddivinayak, K., & Ramachandra, P. (2019, July). Smart Captcha to Provide High Security against Bots. Proceedings of the World Congress on Engineering 2019. http://www.iaeng.org/publication/WCE2019/WCE2019_pp144-149.pdf
51. Velásquez, I., Caro, A., & Rodríguez, A. (2018, February). Authentication schemes and methods: A systematic literature review. Information and Software Technology, 94, 30–37. https://doi.org/10.1016/j.infsof.2017.09.012
52. Visconti, A., Mosnáček, O., Brož, M., & Matyáš, V. (2019, June). Examining PBKDF2 security margin—Case study of LUKS. Journal of Information Security and Applications, 46, 296–306. https://doi.org/10.1016/j.jisa.2019.03.016
53. Wakabayashi, N., Kuriyama, M., & Kanai, A. (2017). Personal authentication method against shoulder-surfing attacks for smartphone. 2017 IEEE International Conference on Consumer Electronics (ICCE). https://doi.org/10.1109/icce.2017.7889266
54. Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021, August). Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications, 188, 103080. https://doi.org/10.1016/j.jnca.2021.103080

55. Wash, R., & Rader, E. (2021). Prioritizing security over usability: Strategies for how people choose passwords. Journal of Cybersecurity.
56. Woods, N., & Siponen, M. (2019, August). Improving password memorability, while not inconveniencing the user. International Journal of Human-Computer Studies, 128. https://www.sciencedirect.com/science/article/abs/pii/S1071581919300102
57. Xiao, Y., & Watson, M. (2017, August 28). Guidance on Conducting a Systematic Literature Review. Journal of Planning Education and Research, 39(1), 93–112. https://doi.org/10.1177/0739456x17723971
58. Xu, M., Wang, C., Yu, J., Zhang, J., Zhang, K., & Han, W. (2021, November 12). Chunk-Level Password Guessing: Towards Modeling Refined Password Composition Representations. Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3460120.3484743
59. Yang, P., Wan, X., Huang, L., Cui, J., Li, J., & Shan, C. (2020, August). Cryptanalysis and Improvement of Smartcard-Based Remote User Authentication Scheme. 2020 IEEE 3rd International Conference on Computer and Communication Engineering Technology (CCET). https://doi.org/10.1109/ccet50901.2020.9213171
60. Zimmermann, V., & Gerber, N. (2020, January). The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes. International Journal of Human-Computer
61. 2022 Data Breach Investigations Report. (n.d.). Verizon Business. Retrieved July 30, 2022, from https://www.verizon.com/business/resources/reports/dbir/Studies, 133, 26–44. https://doi.org/10.1016/j.ijhcs.2019.08.006