Vol-07 Issue 01, January-2023 ISSN: 2456-9348
Impact Factor: 5.004

iJETRM
International Journal of Engineering Technology Research & Management

WHAT AFFECTS STRONG PASSWORDS TO PROTECT YOUR INFORMATION AND DATA

Khaled Almoughem
Ph.D. student in Cybersecurity
Marymount University

Abstract
Strong passwords are essential to protecting one's data and information because they make it difficult for unauthorized individuals to access one's accounts. When one creates a strong password, one uses a combination of unique characters and not easily guessable characters. It means that if someone tries to gain access to one's accounts by guessing one's password, it will take them a long time to do so, and they may ultimately be unsuccessful. In addition to making, it harder for unauthorized individuals to guess one's password, strong passwords also help protect one's data and information from being accessed through other methods, such as brute force attacks or dictionary attacks. Brute force attacks involve using a computer to try every possible combination of characters until the correct password is found. Dictionary attacks involve using a pre-defined list of words and attempting to use each one as the password. Using a strong and unique password can thwart both of these methods. Overall, strong passwords play a crucial role in protecting one's data and information, making it difficult for unauthorized individuals to access one's accounts.

Keywords:
Strong Password, Password Manager, Information and Data Security, Multi-factor Authentication

Introduction

A password is a secret word or phrase used to authenticate a user's identity. It is a fundamental aspect of computer and Internet security, as it is the first defense against unauthorized access to sensitive information (Pervan, 2022). Passwords protect a wide range of information, including personal data, financial transactions, and confidential business documents. They are typically required to log into computers, websites, and other online platforms and are often the only barrier between hackers and valuable data.

Passwords are a crucial part of securing data and information. They authenticate a user's identity and prevent unauthorized access to sensitive information. Several best practices exist for creating and using passwords to ensure data and information security. First and foremost, using a solid and unique password for each account is essential (Pervan, 2022). A strong password is too complex to guess or crack with a mix of upper- and lower-case letters, numbers, and special characters. Different passwords should be enforced while dealing with multiple accounts, as it prevents hackers from accessing the accounts with the same password.

It is also essential to avoid using personal information in passwords. It includes information such as one's name, address, or date of birth, as hackers can quickly obtain this information and use it to guess one's password (Pervan, 2022). Using a password manager to get strong passwords is advisable. A password manager is a tool that stores and securely organize one's passwords. It can automatically enter them into login forms to save one the hassle of remembering multiple passwords.

In addition to strong and unique passwords, enabling two-factor authentication (2FA) on any accounts that offer it is also a good idea. 2FA adds an extra layer of security as it establishes another form of authentication apart from the password. It could be a code sent to one's phone, a fingerprint scan, or a verification form. By following these best practices, one can significantly improve the security of one's data and information (Kanta, 2022). However, it is essential to remember that passwords are only one aspect of overall security and adopting a multi-layered approach to protect oneself and one's data is essential. It could include using antivirus software, keeping software and devices up to date, and being cautious when clicking on links or downloading attachments.

This paper focuses on how strong passwords are essential in securing data. Cases of identity theft, man-in-the-middle attacks, data breaches, and other cybersecurity often occur due to ignorance of developing solid passwords. This report highlights why companies and individuals need to develop strong passwords. Several literature sources were analyzed to obtain essential information on developing good passwords. The paper also focuses on why data security is essential.

iJETRM
International Journal of Engineering Technology Research & Management

Literature Review

Search Strategy

The initial step was to identify relevant databases to obtain the literature sources. This study utilized databases such as PubMed, Scopus, and Google Scholar, which are renowned. The next step was to define the search terms using keywords and phrases related to the research question or topic. The keywords were strong password, password managers, and multi-factor authentication. Boolean operators were used with the keywords to establish the search terms. It is essential to be as specific as possible when defining one's search terms and to consider using synonyms and variations of one's terms to ensure that one captures all relevant studies.

The search filters were selected using the eligibility criteria. Many databases allow one to use filters to narrow one's search results, such as by language, publication date, or study type. Carefully selecting the search filters can help ensure that one only retrieves studies that meet the inclusion and exclusion criteria and are relevant to the research question or topic. The next step was to search. Once one has defined the search terms and selected filters, one can search using the selected databases. It is essential to be thorough and systematic in the search and to record one's search strategy to replicate it if necessary. At this stage, one hundred articles were found.

Review and refine the search. After conducting the initial search, the articles had to be reviewed and refined since too many studies that were not relevant to the topic were found. It may involve adjusting one's search terms, adding or removing filters, or expanding one's search to include additional databases. The eligibility criteria were essential; thus, twenty-seven relevant sources were obtained.

Eligibility Criteria

Table 1 presents the eligibility criteria

Criteria	Inclusion	Exclusion
Type of Study	Randomized controlled trials	Case reports
Sample size	Studies with a sample size of at least 100	Studies with a sample size of less than 100
Language	Studies wrote in English	Studies wrote in languages other than English
Study design	Prospective, observational studies	Retrospective studies

iJETRM
International Journal of Engineering Technology Research & Management

Date of publication	Studies published in the last four years	Studies published more than four years ago

History of the use of strong passwords

The use of strong passwords for protecting data and information has a long history that dates back to the early days of computing. Passwords were used to protect computer and network access. One of the earliest recorded instances of using passwords for security was in the 1960s when the Massachusetts Institute of Technology (MIT) created the Compatible Time-Sharing System (CTSS) (Kanta, 2022). This system uses passwords to allow users to access the computer system and to protect sensitive data stored on the system.

As computers and networks became more widely used, the need for strong passwords to protect data and information became increasingly important. In the 1980s, the National Institute of Standards and Technology (NIST) instituted guidelines for developing strong passwords, which included recommendations such as using a mix of upper and lower case letters, numbers, and special characters and avoiding using familiar words or personal information.

According to Singh, in the 1990s, solid passwords became even more evident with the widespread adoption of the Internet and the growing use of online accounts and services. Hackers and cybercriminals began to target online accounts and services, and solid passwords became critical in protecting against these threats. Today, strong passwords are an essential part of data and information security. They protect access to various systems and services, including computers, networks, websites, and online accounts. Individuals and organizations must create and use strong passwords to protect against unauthorized access and secure their data and information.

Characteristics of a strong password

A strong password is a crucial element of computer and internet security. It helps protect one's accounts, personal information, and assets from unauthorized access and potential theft. Here are some characteristics of a strong password: Length: According to Singh, a strong password should be at least eight characters long. The longer the password, the more secure it is. It is because longer passwords have a more significant number of possible combinations, making them more difficult for attackers to guess or crack.

Complexity: A strong password should contain a mix of upper and lower case letters, numbers, and special characters. Using a combination of different character types makes it more difficult for attackers to guess or crack one's password. For example, a password that is just a single word or a simple combination of letters and numbers is easier to guess or crack than a password that contains a mix of upper and lower-case letters, numbers, and special characters (Xie et al., 2022). Unpredictability: A strong password should not be based on easily guessable information, such as one's name, birth date, or common words. It should also not be a word found in the dictionary. Using randomly generated passwords or passphrases can help make one's password more unpredictable. For example, a password like "P@55w0rd" is more predictable than a randomly generated password like "R3dG@t3#F1ng3r".

Uniqueness: A strong password should not be used for multiple accounts. Reusing passwords across different accounts puts all of one's accounts at risk if one is compromised. If an attacker gains access to one's accounts using a password one has reused elsewhere, they could use that same password to gain access to one's other accounts (Xie et al., 2022). Security: A strong password should be kept secure and not shared with anyone. One should also be careful about where and how one enters their password, as keyloggers and other malicious software can be used to capture one's password as one types it. Using two-factor authentication whenever possible is also a good idea, as this adds an extra layer of security to one's accounts.

Updating: A strong password should be changed regularly. It helps prevent attackers from using previously obtained passwords to access one's accounts. How often one should change one's password depends on the level of security one needs and the sensitivity of the information one is protecting (Xie et al., 2022). Changing one's password at least once every three to six months is a good idea. A strong password should be long, complex, unpredictable, unique, and secure. It is also important to regularly update one's password to ensure the continued security of one's accounts. Following these guidelines can help protect one's personal information and assets from unauthorized access and potential theft.

iJETRM
International Journal of Engineering Technology Research & Management

Table 2 shows the characteristics of a good password

Characteristic .	Description
Length	Longer passwords are more secure because they have more possible combinations. Aim for at least 12 characters
Ease of remembering	It's important to remember your password, but make sure it's not too easy to guess. You can use a passphrase or mnemonic device to help you remember a strong password.
Unique	Use a different password for each account. This way, if one password is compromised, the attacker won't have access to your other accounts.
Unpredictability	Avoid using personal information (such as your name or date of birth) or quickly guessable patterns (such as "123456").
Complexity	Use a mix of uppercase and lower-case letters, numbers, and special characters. Avoid using dictionary words or everyday phrases.

Importance of protecting data and information

Securing data and information is crucial for a variety of reasons. One key aspect is protecting sensitive information. It can include personal details such as addresses, phone numbers, financial information, and confidential business information like trade secrets or intellectual property (Veroni, 2022). Failing to secure this data type can have serious consequences, including financial losses and legal liabilities.

Another important reason to secure data and information is to maintain privacy. It means protecting personal information from unauthorized access or misuse and keeping confidential information from being disclosed to the wrong parties. By doing so, organizations can help ensure that individuals' personal information is not misused or exploited (Grilo et al., 2022). Data breaches can also have serious consequences, including financial losses, reputational damage, and legal liabilities. By securing data and information, organizations can reduce the risk of data breaches and protect themselves from these negative consequences. It is imperative in today's digital age, where data breaches are becoming increasingly common.

In addition to these practical considerations, securing data and information is often necessary for compliance with relevant laws and regulations. Many organizations must adhere to specific data and information security standards, and failing can result in fines, legal action, and other consequences (Grilo et al., 2022). Organizations can ensure they comply with these regulations by securing data and information. Finally, securing data and information can help enhance trust with customers, clients, and other stakeholders. In today's digital age, people are increasingly concerned about their privacy and the security of their personal information. Organizations can build long-term relationships and enhance trust with these groups by demonstrating a commitment to protecting this information.

Benefits of strong passwords

Strong passwords provide several benefits that can help protect one's accounts and personal information from being accessed by unauthorized individuals. Some of the key benefits of strong passwords include improving security. One of the primary benefits of strong passwords is enhanced security (Shin, 2022). Strong passwords are typically harder to guess or crack than weak ones, making it more difficult for attackers to access one's accounts. It is essential to have accounts with sensitive information, such as financial or medical records.

In addition, strong passwords lead to better protection against phishing attacks. Phishing attacks are a standard method used by hackers to try and obtain login credentials or other sensitive information. Using strong passwords can reduce the risk of falling victim to these attacks. It is because solid passwords are less likely to be guessed or cracked, making it more difficult for attackers to obtain one's login credentials. Strong passwords lead to reduced risk of account takeover. Account takeover occurs when an attacker gains access to one's account and can change or access sensitive information (Simon, 2022). Strong passwords can help prevent this by making it more difficult for an attacker to guess or crack one's password. Enhanced privacy is another benefit of strong

passwords. Strong passwords can help protect one's personal information and keep it private. One must have secured accounts for sensitive information, such as financial or medical records.

Furthermore, strong passwords lead to greater peace of mind. Knowing that one's accounts are secure can give one peace of mind and allow one to use the Internet confidently. Compliance with security policies: Many organizations have security policies that require strong passwords (Simon, 2022). By using strong passwords, one can ensure that they comply with these policies and avoid potential consequences.

Enhanced protection against dictionary attacks: Dictionary attacks are an attack in which an automated program is used to try and guess a password by attempting to match it to words in a dictionary. Strong passwords not based on dictionary words can help protect against these attacks. Improved protection against brute force attacks: Brute force attacks are a type of attack in which an automated program attempts to guess a password by trying every possible combination of characters (Simon, 2022). Strong passwords that are long and use a combination of upper and lower case letters, numbers, and special characters can help protect against these attacks.

How strong passwords affect protecting data and information

Brute-force Attacks

According to Swathi, brute force attacks involve guessing a password by systematically trying all possible combinations of characters. These attacks can be automated and can run through millions of combinations in a short amount of time. Strong passwords can help prevent brute force attacks by increasing the possible combinations an attacker would need to try. It is because solid passwords are typically longer and contain a mix of letters, numbers, and special characters, significantly increasing the number of possible combinations. For example, a password that is eight characters long and contains only lower-case letters has 26^8 (208,827,064,576) possible combinations. In contrast, a password that is eight characters long and contains a mix of uppercase letters, lower-case letters, numbers, and special characters has 95^8 (6,095,689,385,410,816) possible combinations, which is significantly larger.

According to Swathi, another way solid passwords can help prevent brute force attacks is by using rate limiting, a security measure limiting the number of attempts an attacker can make to guess a password. For example, if an attacker tries to guess a password and fails, the system may temporarily lock their account or slow down the rate at which they can make further attempts. It can significantly slow down a brute-force attack and make it much more difficult for the attacker to guess the password.

In summary, strong passwords can help prevent brute force attacks by increasing the possible combinations an attacker would need to try and using rate limiting to slow down the attack. It's important to note that strong passwords are just one aspect of a robust security strategy (Pervan, 2022). Other measures, such as enabling two-factor authentication and keeping one's software and devices up to date, can also help protect against a wide range of attacks.

iJETRM
International Journal of Engineering Technology Research & Management

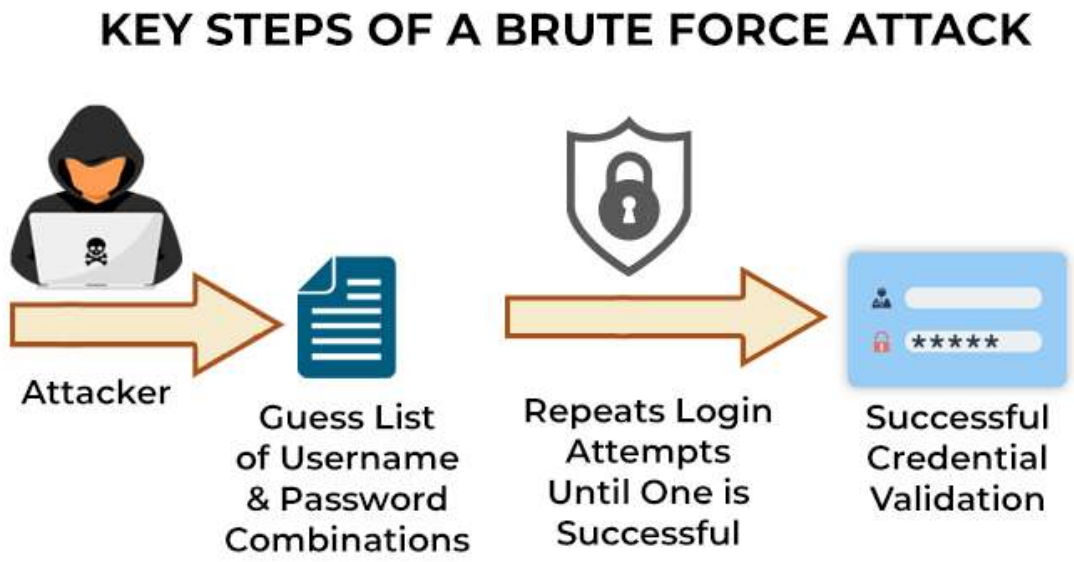

Figure 1 shows how a brute-force attack occurs

Dictionary Attacks

Dictionary attacks involve guessing passwords using a pre-computed list of common words and phrases (Djukanovic et al., 2021). These attacks can be automated and can run through millions of words in a short amount of time. Strong passwords can help prevent dictionary attacks by not using common words or phrases as passwords. Dictionary attacks rely on the assumption that people will use common words or phrases as their passwords, so if a password is not based on a common word or phrase, it will be much more difficult for an attacker to guess.

Another way solid passwords can help prevent dictionary attacks is by using random strings of characters as passwords. Random strings of characters are unlikely to be found in a pre-computed list of words and phrases so they can provide an additional layer of protection against dictionary attacks. Finally, strong passwords can also help prevent dictionary attacks by using rate limiting, a security measure limiting the number of attempts an attacker can make to guess a password(Djukanovic et al., 2021). For example, if an attacker tries to guess a password and fails, the system may temporarily lock their account or slow down the rate at which they can make further attempts. It can significantly slow down a dictionary attack and make it much more difficult for the attacker to guess the password. In summary, strong passwords can help prevent dictionary attacks by not using common words or phrases, random strings of characters, and rate limiting to slow down the attack.

iJETRM
International Journal of Engineering Technology Research & Management

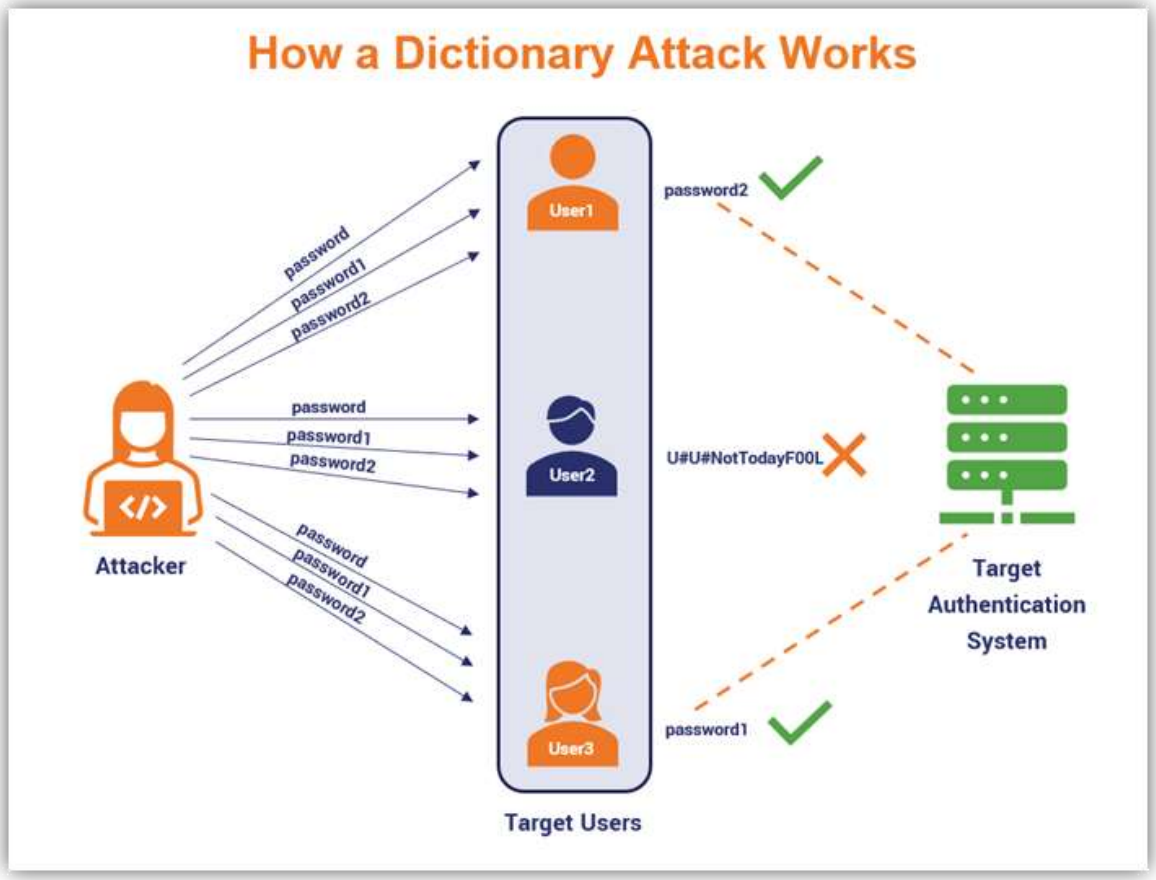

Figure 2 shows how a dictionary attack works

Rainbow table attacks

Rainbow table attacks involve using pre-computed tables of hashes to try and crack passwords. Hashes are one-way mathematical functions that convert a password into a fixed-length string of characters (Bakshi, 2023). Rainbow table attacks work by using these pre-computed tables to determine the original password from its hash quickly. Strong passwords can help prevent rainbow table attacks by making it more difficult for the attacker to find the password in the pre-computed tables. It is because solid passwords are typically long and contain a mix of letters, numbers, and special characters, significantly increasing the number of possible combinations (Bošnjak et al., 2018). For example, a password that is eight characters long and contains only lower-case letters has 26^8 (208,827,064,576) possible combinations. In contrast, a password that is eight characters long and contains a mix of uppercase letters, lower-case letters, numbers, and special characters has 95^8 (6,095,689,385,410,816) possible combinations, which is significantly larger.

Another way strong passwords can help prevent rainbow table attacks is by using salting, which involves adding random data to the password before it is hashed. This random data, called a "salt," is unique to each password and is stored with the hash in a database (Becker, 2018). When an attacker tries to crack a password using a rainbow table, they will not know the salt that was used, so they will be unable to find the original password in the pre-computed tables. Finally, strong passwords can also help prevent rainbow table attacks by using rate limiting, a security measure limiting the number of attempts an attacker can make to guess a password. For example, if an attacker tries to guess a password and fails, the system may temporarily lock their account or slow down the rate at which they can make further attempts. It can significantly slow down a rainbow table attack and make it much more difficult for the attacker to guess the password (Gautam, 2022). In summary, strong passwords can help prevent rainbow table attacks by increasing the possible combinations that an attacker would need to try, by using salting to add random data to the password before it is hashed, and by using rate limiting to slow down the attack.

Social Engineering Attacks

iJETRM
International Journal of Engineering Technology Research & Management

Social engineering attacks involve tricking people into revealing their passwords or other sensitive information. These attacks can take many forms, such as phishing emails, phone calls, or in-person interactions. They can be challenging to detect because they rely on manipulating people rather than exploiting technical vulnerabilities(Golla, 2018). One way that solid passwords can help prevent social engineering attacks is by not using easily guessable passwords. If a password is easy to guess, an attacker may be able to trick someone into revealing it by posing as a legitimate authority figure or by using other psychological manipulation techniques (Xiao, 2022). By contrast, if a password is strong and not easily guessable, it is much less likely that an attacker will be able to obtain it through social engineering.

According to Inda, solid passwords can help prevent social engineering attacks by not sharing passwords with others. Suppose a password is shared with multiple people. In that case, it becomes easier for an attacker to obtain it through social engineering, either by tricking one of the people who have the password or by obtaining it through other means and then using it to gain access to sensitive information (Grobler, 2021). Finally, strong passwords can also help prevent social engineering attacks by using rate limiting, a security measure limiting the number of attempts an attacker can make to guess a password. For example, if an attacker tries to guess a password and fails, the system may temporarily lock their account or slow down the rate at which they can make further attempts. It can significantly slow down a social engineering attack and make it much more difficult for the attacker to guess the password (Guo, 2019). Strong passwords can help prevent social engineering attacks by not being easily guessable, not being shared with others, and using rate limiting to slow attacks.

Why the use of a strong password is not enough

A strong password is essential to protecting one's online accounts and personal information. A strong password is typically one that is long, uses a combination of letters, numbers, and special characters, and is not based on common words or patterns that are easy to guess. However, relying solely on a solid password is generally not enough to ensure the security of one's accounts (Guo, 2019). A strong password is not enough because it can still be vulnerable to password-cracking attacks. Password cracking is using software to guess a password by attempting to input every possible combination of letters, numbers, and special characters. Even a strong password can be vulnerable to this attack if it is not long enough or uses commonly-used words or patterns (Abdrabou et al., 2022). For example, a password such as "Pa$$w0rd123" may be vital. However, it is still relatively easy to guess because it uses a typical pattern (substituting "s" with "$" and "o" with "0") and a common word ("password").

Another reason a strong password is insufficient is that it can be vulnerable to password reuse. If one uses the same password for multiple accounts, an attacker who successfully guesses one's password for one account will be able to access all of one's accounts. It is because many people reuse passwords, and attackers know this. They may try to guess one's password for one account and then use it to access other accounts they may have (Lee, 2022). Finally, a strong password is not enough to protect against phishing attacks. Phishing attacks are when attackers trick one into giving away one's password by pretending to be a legitimate website or service and asking one to enter one's login credentials. They may do this through fake login pages, emails, or text messages that look like they are from a legitimate source. The attackers can access one's account if one falls for a phishing attack and enter one's password (Mwagwahi,2018).

To better protect one's online accounts and personal information, it is recommended to use a combination of strong passwords and other security measures, such as two-factor authentication and password managers. Two-factor authentication requires one to enter a second form of identification, such as a code sent to one's phone and password, when logging into an account (Mwagwahi, 2018). Password managers are tools that store and manage one's passwords, making it easier to use unique passwords for all accounts and helping protect against password reuse.

How strong passwords are enforced by password managers and multi-factor authentication

Password managers

Password managers are tools that store and manage one's passwords, making it easier to use unique and strong passwords for all accounts. Password managers enforce strong passwords by automatically generating passwords for someone when creating a new account (Raptis et al., 2021). Many password managers have built-in password generators that can create complex and unique passwords. For example, a password manager might generate a password like "hjKL9876#%$@!". This password is likely solid because it is long, uses a combination of letters, numbers, and special characters, and is not based on common words or patterns.

Another way that password managers enforce strong passwords is by requiring one to use them when creating a new account. Many password managers have built-in password strength meters that will let one know if one's chosen password is strong enough. If the password is not strong enough, the password manager will often

suggest alternatives or require one to choose a stronger password (Ray et al., 2021). In addition to enforcing strong passwords, password managers help protect against password reuse. As mentioned earlier, if one uses the same password for multiple accounts, an attacker who successfully guesses the password for one account will be able to access all of one's accounts. By storing and managing one's passwords, password managers make using unique passwords for all accounts easier, helping protect against password reuse. Overall, password managers are a valuable tool for enforcing solid passwords and helping protect one's online accounts and personal information(Ray et al., 2021). They can help ensure that one uses complex and unique passwords for all accounts, making it more difficult for attackers to guess or crack one's passwords.

Multi-factor Authentication

Multi-factor authentication, also known as two-factor authentication (2FA), is a security measure requiring multiple forms of identification when logging into an account. It is designed to add an extra layer of protection beyond just a password, making it more difficult for attackers to access one's accounts. Multi-factor authentication enforces strong passwords by requiring one to enter one's password as the first form of identification (Renaud, 2019). To log into an account using multi-factor authentication, one must first enter one's password. It means that even if an attacker has one's password, they will not be able to access one's account without providing a second form of identification. It helps to ensure one's password is strong enough to withstand guessing or cracking attempts.

Another way that multi-factor authentication enforces strong passwords is by requiring one to use a unique one-time code or token as the second form of identification (Raptis et al., 2021). This code or token is typically sent to one via email, text message, or an authentication app on one's phone. To log into an account, one must enter both one's password and the one-time code or token. It means that even if an attacker has one's password, one will not be able to access one's account without access to one's phone or email account. Overall, multi-factor authentication is a helpful tool for enforcing the use of strong passwords and helping to protect one's online accounts and personal information. It adds an extra layer of protection beyond just a password, making it more difficult for attackers to access one's accounts even if they can guess or crack one's password (Scholefield, 2019).

Challenges in the use of strong passwords

Strong passwords are essential and have been proven to help individuals improve data security. However, strong passwords have several challenges in the same manner as their benefits. One common challenge with the use of strong passwords is the difficulty in remembering them. Strong passwords typically contain upper and lower case letters, numbers, and special characters, making them difficult to remember and recall accurately (Siponen, 2020). As a result, users may be tempted to write down their passwords or use the same password for multiple accounts, which can increase the risk of password theft.

Another challenge with strong passwords is the length and complexity of the passwords themselves. Strong passwords are often long and complex, making them difficult to type accurately and leading to login failures and frustration. It can be particularly inconvenient for users who have to remember multiple strong passwords for different accounts. Using strong passwords can also be inconvenient, as it may take longer to enter them, and users may have to change their passwords to maintain their strength regularly (Siponen, 2020). It can be incredibly frustrating for users who have to remember multiple strong passwords for different accounts.

In addition, compatibility issues may be with certain types of characters commonly used in solid passwords. Some systems may not be compatible with special or non-Latin characters, which can prevent users from using specific passwords or require them to use weaker passwords compatible with the system (Tufail et al., 2021). Overall, strong passwords can present several challenges, but it is an important security measure to protect sensitive information and prevent unauthorized access to accounts.

Conclusion

In conclusion, strong passwords are an essential security measure that can help protect sensitive information and prevent unauthorized access to accounts. Strong passwords are typically long and complex and contain a mix of upper and lower-case letters, numbers, and special characters (Wang et al., 2021). While solid passwords can present challenges, such as difficulty remembering them and inconvenience, there are also several benefits. One significant benefit of strong passwords is that they can help prevent various types of attacks, including brute force attacks, dictionary attacks, and password-guessing attacks. These attacks involve automated tools to try and guess a user's password and can be much less effective against solid passwords due to their complexity.

In addition to using strong passwords, other measures can be taken to enhance security. For example, multi-factor authentication (MFA) can provide an additional layer of protection by requiring users to provide

iJETRM
International Journal of Engineering Technology Research & Management

additional information beyond their password to access an account. Similarly, password managers can help users store and manage their strong passwords securely and conveniently (Yildirim, 2019). Overall, strong passwords are an essential security measure that can help protect sensitive information and prevent unauthorized access to accounts. While it may present some challenges, the benefits of using solid passwords far outweigh the potential difficulties. By taking steps such as using MFA and password managers, users can further enhance the security of their accounts and protect against various types of attacks.

References

Abdrabou, Y., Schütte, J., Shams, A., Pfeuffer, K., Buschek, D., Khamis, M., & Alt, F. (2022, April). " Your Eyes Tell You Have Used This Password Before": Identifying Password Reuse from Gaze and Keystroke Dynamics. In *CHI Conference on Human Factors in Computing Systems* (pp. 1-16).
https://dl.acm.org/doi/abs/10.1145/3491102.3517531

Bakshi, G., Verma, R., & Chaudhry, R. (2023). Bomb Box: A Fortified Vault to Prevent Brute Force Attack. In *International Conference on Innovative Computing and Communications* (pp. 77-85). Springer, Singapore.
https://link.springer.com/chapter/10.1007/978-981-19-2535-1_5

Becker, I., Parkin, S., & Sasse, M. A. (2018). The rewards and costs of stronger passwords in a university: linking password lifetime to strength. In *27th USENIX Security Symposium (USENIX Security 18)* (pp. 239-253).
https://www.usenix.org/conference/usenixsecurity18/presentation/becker

Bošnjak, L., Sreš, J., & Brumen, B. (2018, May). Brute-force and dictionary attacks hashed real-world passwords. In *2018 41st international convention on information and communication technology, electronics, and microelectronics (micro)* (pp. 1161-1166). IEEE.
https://ieeexplore.ieee.org/abstract/document/8400211/

Djukanovic, M., Novicevic, L., Zhu, L., & Jiang, P. (2021, June). Dictionary-Based Brute Force Attack–Study Case of Montenegro and China. In *International Conference "New Technologies, Development and Applications"* (pp. 647-652). Springer, Cham.
https://link.springer.com/chapter/10.1007/978-3-030-75275-0_71

GAUTAM, T., & SINGH, U. (2022). AN APPROACH FOR DETECTING PASSWORD PATTERNS IN DICTIONARY ATTACKS.
https://www.mililink.com/upload/article/1283812570aams_vol_215_march_2022_a32_p2765-2780_tanvi_gautam_and_utkarsh_singh.pdf

Golla, M., & Dürmuth, M. (2018, October). On the accuracy of password strength meters. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1567-1582).
https://dl.acm.org/doi/abs/10.1145/3243734.3243769

Grilo, M., Campos, J., Ferreira, J. F., Almeida, J. B., & Mendes, A. (2022). Verified password generation from password composition policies. In *International Conference on Integrated Formal Methods* (pp. 271-288). Springer, Cham.
https://link.springer.com/chapter/10.1007/978-3-031-07727-2_15

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage, and usability: Redefining human-centric cyber security. *Frontiers in Big Data*, *4*, 583723.
https://www.frontiersin.org/articles/10.3389/fdata.2021.583723/full

Guo, Y., Zhang, Z., & Guo, Y. (2019). Optiwords: A new password policy for creating memorable and strong passwords. *Computers & Security*, *85*, 423-435.
https://www.sciencedirect.com/science/article/pii/S0167404819301105

Indu, S., & Krishna, K. R. Authentication by Encrypted Negative Password.
https://jespublication.com/upload/2022-V13I503.pdf

Kanta, A., Coisel, I., & Scanlon, M. (2022). PCWQ: A Framework for Evaluating Password Cracking Wordlist Quality. In *International Conference on Digital Forensics and Cyber Crime* (pp. 159-175). Springer, Cham.
https://link.springer.com/chapter/10.1007/978-3-031-06365-7_10

Lee, K., Sjöberg, S., & Narayanan, A. (2022). Password policies of most top websites fail to follow best practices. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (pp. 561-580).
https://www.usenix.org/conference/soups2022/presentation/lee

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems*, *42*(1), 7.
https://aisel.aisnet.org/cais/vol42/iss1/7/

iJETRM
International Journal of Engineering Technology Research & Management

Pervan, B., Knezović, J., & Guberović, E. (2022). Energy-efficient distributed password hash computation on the heterogeneous embedded system. *Automatika*, *63*(3), 399-417.
https://www.tandfonline.com/doi/abs/10.1080/00051144.2022.2042115
Raptis, G. E., Katsini, C., Cen, A. J. L., Arachchilage, N. A. G., & Nacke, L. E. (2021, May). Better, Funner, Stronger: A Gameful Approach to Nudge People into Making Less Predictable Graphical Password Choices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-17).
https://dl.acm.org/doi/abs/10.1145/3411764.3445658
Ray, H., Wolf, F., Kuber, R., & Aviv, A. J. (2021). Why older adults (Don't) use password managers. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 73-90).
https://www.usenix.org/conference/usenixsecurity21/presentation/ray
Renaud, K., & Zimmermann, V. (2019). Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy*, *3*(2), 228-258.
https://www.cambridge.org/core/journals/behavioural-public-policy/article/nudging-folks-towards-stronger-password-choices-providing-certainty-is-the-key/BAEEAC8EEB22980FA23EEFD809A5C8B7
Scholefield, S., & Shepherd, L. A. (2019, July). Gamification techniques for raising cyber security awareness. In *International Conference on Human-Computer Interaction* (pp. 191-203). Springer, Cham.
https://link.springer.com/chapter/10.1007/978-3-030-22351-9_13
Shin, Y., & Woo, S. S. (2022). PasswordTensor: Analyzing and explaining password strength using tensor decomposition. *Computers & Security*, *116*, 102634.
https://www.sciencedirect.com/science/article/pii/S0167404822000335
Singh, B., & Jesi, E. SAFE VAULT: A PASSWORD MANAGER.
https://www.ijeast.com/papers/93-97,%20Tesma612,IJEAST.pdf
Simon, J. (2022). *Protect your password so it can protect you: improving password strength through coping messages* (Bachelor's thesis, University of Twente).
http://essay.utwente.nl/89389/
Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Computers & Security*, *88*, 101617.
https://www.sciencedirect.com/science/article/pii/S0167404819301646
Swathi, K. Brute Force Attack on Real World Passwords.
https://ijrpr.com/uploads/V3ISSUE11/IJRPR7767.pdf
Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies*, *14*(18), 5894.
https://www.mdpi.com/1275136
Veroni, E., Ntantogian, C., & Xenakis, C. (2022). A large-scale analysis of Wi-Fi passwords. *Journal of Information Security and Applications*, *67*, 103190.
https://www.sciencedirect.com/science/article/pii/S2214212622000722
Wang, Z., Peng, J., Zhu, H., & Sun, L. (2021). SEIGuard: An Authentication-simplified and Deceptive Scheme to Protect Server-side Social Engineering Information Against Brute-force Attacks. *arXiv preprint arXiv:2108.06529*.
https://arxiv.org/ abs/2108.06529
Xiao, Y., & Zeng, J. (2022). Dynamically generate password policy via Zipf distribution. *IEEE Transactions on Information Forensics and Security*, *17*, 835-848.
https://ieeexplore.ieee.org/abstract/document/9715109/
Xie, J., Cheng, H., Zhu, R., Wang, P., & Liang, K. (2022, May). WordMarkov: A New Password Probability Model of Semantics. *ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 3034-3038). IEEE.
https://ieeexplore.ieee.org/abstract/document/9746203/
Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741-759.
https://link.springer.com/article/10.1007/s10207-019-00429-y

iJETRM
International Journal of Engineering Technology Research & Management