A Review Article on the role of Strong Passwords in Enhancing Online Security

Abstract:

In this era, a strong password acts as a guardian for our sensitive information. This paper will discuss the side effects of weak passwords and how necessary a strong password is. This study will provide you with more guidance on how to secure our information. In today's online era, hackers steal information. Therefore, through a brief introduction, we will understand the human factors that cause problems and encourage humans with reliable solutions on how to secure their information. Using a strong password is very important in today's digital world. With a strong password, it will be difficult for hackers to crack it. You can secure your personal information in your online account. With a strong password, information cannot go into the wrong hands. Strong passwords protect privacy, and no one can get unwanted information. With the help of this study is to enable users to generate strong passwords so that password security is improved. People can use different types of password creation methods instead of using simple passwords. Recently, hackers have been stealing a lot of sensitive information that the public has no knowledge of it.Users are often unaware of the immediate negative effects of weak passwords. In today's virtual environment, cybercriminals regularly exploit vulnerabilities, leading to the destruction of sensitive information. Strong passwords act as a barricade, protecting sensitive data. Encouraging the use of strong passwords is therefore imperative. Passwords that combine uppercase letters, lowercase letters, and special characters are difficult to crack. Long passwords enhance security. Users should regularly update their passwords to keep their information secure. By emphasizing this important information, the paper will raise awareness among users so that they can safely use their information.

Keywords:

Password security, Password Policy, Password composition rules, Brute force attacks, Dictionary attacks, Phishing attacks.

1. Introduction:

Online security means protecting your data from unauthorized access. For this, users need to use a variety of measures like strong passwords and encryption methods. Authentication is the main key concept of online security. In this process, the user is verified before accessing any information. For example, before going anywhere, the user's ID is checked. By verifying the user's identity, data integrity and security are maintained. This ensures that the data is not being used by any unauthorized person.Strong passwords are very crucial for preventing cyber-attacks. A strong password acts as a barrier between your data and cybercriminals. Users store their sensitive information like bank details and social media accounts. With the help of a strong password, this sensitive information cannot fall into the wrong hands. Cybercriminals use various methods to crack passwords, like brute-force attacks, dictionary attacks, and phishing. With strong passwords, we can be safe from such attacks. Users have many misconceptions regarding password security. Users don't regularly update their passwords, making it easy for hackers to crack them. Users use two-factor authentication for security, but this cannot replace a strong password. Even if a website is secure, information can still be stolen with a weak password.Always use a password manager for creating strong passwords because it is difficult to remember strong passwords for every single account. With a password manager, users can save their strong passwords.A password manager is an essential tool for cyber security. Even if the device is lost, the passwords remain safe within it. A password manager also protects the user from phishing attacks. The user can create complex and long passwords.With the help of a password manager, users can utilize the autofill option. Whenever you log in to a website, the password manager automatically fills in the user's credentials. This saves the user time spent typing passwords.

2. The Role of Weak Passwords in Cyber Attacks:

Nowadays, most transactions are digital. Every user uses phones and laptops for these transactions. So, it's crucial to educate users about cyber threats. There's no doubt that technology provides users with a lot of convenience. But, the fact that most organizations use What App and AI models is a very serious threat to personal and national data. Users need to adopt safe practices to protect their data. Cybercriminals use new techniques to steal data. For example, you might receive a message on your phone, and when you call that number, theymake some kind of demand for money. This could involve any type of psychological manipulation. Therefore, it's extremely important to adopt cyber safety practices to keep data safe. Google Lens is also one such tool that can be misused for stealing information. Weak passwords play a very critical role. They are an easy point of entry for attackers.

2.1 Brute Force attack:

Attackers use various techniques to try different password combinations. If the password is weak, they can crack it easily. Users often use weak passwords so they can remember them easily, but these are also easily guessed. A complex password would be more time-consuming to crack and has many more possible combinations.

2.2 Credential Stuffing:

In credential stuffing, login credentials are stolen and used to access other accounts.These types of credentials can be accessed using various automated tools. Therefore, strong passwords are essential.

2.3Targeted Credential Cracking:

In this type of attack, cybercriminals crack more than one account, using a number of different possible combinations to do so. For example, BigBank uses 6-digit PINs to access accounts. This means there are 1,000,000 possible PIN combinations. The main drawback is that the bank reuses PINs, where each 6-digit PIN is used by 10 different users. This reduces security. Cybercriminals, with the help of PINs, will try different user IDs. This increases the chances of success for the cybercriminal. This allows the attacker to access multiple accounts in a short amount of time. The system should be designed in such a way that PINs cannot be reused. [1](Dinei Florencio, Cormac Herley ˆOne Microsoft Way Redmond, WA, USA)

2.4 The Role of Weak Passwords in Data Breaches:

According to research, 80% of cyber-attacks are frequently happening due to weak passwords. These types of cyber-attacks are having a significant impact on individuals and organizations. Therefore, it is essential that users employ security measures and use strong passwords.

3. Qualities of a Strong Password:

A strong password provides security from unauthorized users and keeps your information safe from prying eyes. Understanding what makes a password strong is the key concept for users.

3.1 Length and complexity requirement:

Longer passwords create more possible combinations, making them more difficult for hackers to crack. Generally, passwords should be 12 to 16 characters long. A long password should also be a mixture of upper and lower case letters, numbers, and special symbols. This increases password strength and keeps users safe from attackers.

3.2 Avoid common and easy guessable password

Users should not use passwords that can be easily guessed. Do not use personal information in your password and avoid common phrases. There should be no repeated characters in the password. Use random characters in the password as much as possible. The password should always be remembered; otherwise a strong password is useless.

3.3 Protect personal information and Financial Asset:

A strong password protects your personal information. Weak passwords can lead to unauthorized access to everything from social media accounts to online banking. Strong passwords act as a barrier, keeping your information safe.

3.4 Random Generated password:

A user can generate a random password from a predefined character set. The user can choose which character set to use for password generation. Using a pseudorandom number generator, the user can create a random password. Randomly generated passwords are more difficult to crack compared to human-generated passwords. Users often employ pseudo randomly generated passwords in cryptography. [2](Chanda, Password Security: An Analysis of Password Strengths and Vulnerabilities; Dinei Florencio, Cormac Herley ˆOne Microsoft Way Redmond, WA, USA)

4. The role of Password Manager:

Complex, long passwords are difficult for users to remember. One method to address this is using a password manager. With a password manager, the user only needs to remember one master password to unlock their services.

4.1 Benefits of Using Password manager:

- Convenience: The user won't have to struggle to remember long passwords.
- Enhanced Security: Long and complex passwords are difficult to crack, thus increasing security.
- Time saving:Auto fill options save time. Sometimes users don't need to repeatedly write their credentials, which also saves time.
- Safe vault:Users can save all their passwords in one place, and high-quality password managers employ encryption techniques and zero-knowledge architecture.

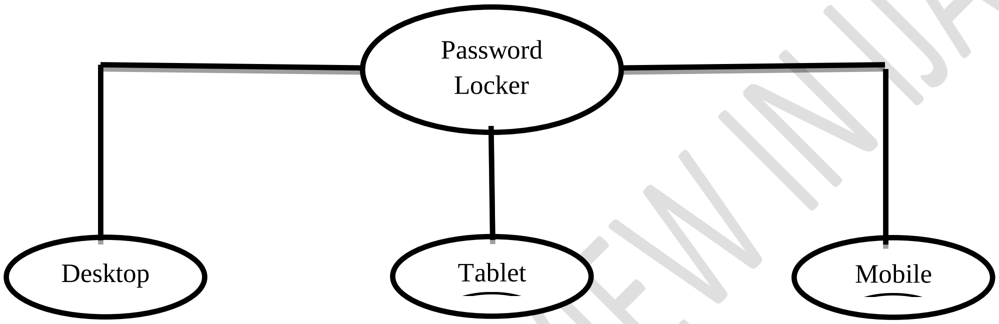

Figure 1: Working of Password Manager

Figure1 shows that how password manager works. It shows a central Password Locker which shows the storage location for all passwords then it shows various devices connected to this password locker for connection and retrieving password from this password locker. There are three open-source password managers: pass bolt, Padlock, and Encryptr. They all have their own unique properties and allow users to set up their own servers for testing purposes. Let's discuss each one in detail.

4.2 Pass bolt:Pass bolt is an open-source password manager that is publicly available for everyone. Anyone can easily review and modify it. With pass bolt, you can securely share passwords among your team and maintain proper control. It enhances security and allows for self-hosting, giving you full control over your password data.(Carlos Luevanos1,John Elizarraras2)

4.3 Padlock:Padlock is also an open source password manager. If the user shuts down the system, the system will automatically lock after a few seconds with the help of Padlock. The user can also set a maximum limit of 10 minutes. Padlock has its own password generator.

4.4 Encryptr:Encryptr is also an open-source password manager. With the help of Encryptr, data is first encrypted before transmission. Only the user can access and decrypt the data. Open source means it is publicly available for review. Encryptr also uses a built-in password generator. With the help of this, the user can create strong and unique passwords.

5. Limitations of strong passwords in mitigating advanced cyber threats, such as AI-driven password-cracking algorithms:

Using AI-driven password-cracking algorithms even complex passwords can be cracked quickly. Phishing is also a common threat for revealing passwords. In phishing, attackers use tricks like sending fake emails that appear to be from the user's bank. People reuse passwords, so guessing them is very easy. For this, under mitigation techniques, users can use MFA (Multi-Factor Authentication) and password managers.

Mitigation Techniques:

Multi-Factor Authentication (MFA):MFA enhances security by demanding multiple verification steps during login, not just a password. Examples include email codes, security questions, and fingerprint scans. This extra layer of authentication prevents unauthorized access if a password is compromised. [4] (El-Taj)

Standard multi-factor authentication (MFA) consistently demands a fixed verification step, like a code, for every login. In contrast, Adaptive MFA uses risk analysis to determine the strength of authentication needed. Upon login, the system assesses user identity and behavior, assigning a risk score. Higher risk scores require more authentication factors before access is granted.

Password Managers:A password manager is exactly that: a program that keeps your passwords safe and organized. Instead of trying to memorize countless complicated passwords, it creates robust, distinct ones for every website and app you use. These are then locked away in an encoded database, unlocked only with your master password. To make online life easier and more secure, these tools often offer features such as automatically filling in login forms, creating new strong passwords, and checking for security weaknesses. In essence, they take the headache out of password security.

6. Barriers to adopting strong password:

People struggle to implement security best practices due to various challenges. These include difficult-to-navigate login screens on different platforms, inconsistent guidance from experts, lingering behaviors from older, non-digital systems, and the sheer volume of information and accounts we manage in our digital lives. While security guidelines often promote passwords formed from words and symbols ("hello@world") or long word phrases ("welcometomycity"), password recovery systems contradictory rely on easily discover able personal information like a mother's maiden name, birthday, or pet, which social media frequently exposes.

7. Role of cyber security in Education:

It's essential to implement user training programs to educate individuals about the risks associated with weak passwords. Training sessions should instruct users on how to generate robust and unique passwords, and also demonstrate the benefits of using password managers. Furthermore, users should be educated about the security advantages of multi-factor authentication (MFA). Consistent and recurring training sessions will foster a habit of maintaining strong password practices. These sessions will also highlight the detrimental consequences of using weak passwords.

Estimated time to crack Password:

Password Type	Five Letter	Six Letter	Seven Letter	Eight Letter	Twelve Letter
All Lower Case letters	0.0001 seconds	0.003 seconds	0.08 seconds	2 seconds	14 hours
Double Case letters	0.001 seconds	0.2 seconds	10 seconds	8 minutes	6 years
Alphanumeric (lowercase, Uppercase, numbers)	0.01 seconds	2 seconds	2 minutes	1 hour	53 years
Alphanumeric and Symbols	0.05 seconds	12 seconds	11 minutes	8 hours	226 years

F

Figure 2: Estimated time to crack Password

In this Figure 2 demonstrates how the estimated time for a computer to crack a password is directly related to its length and complexity. As passwords get longer and incorporate a wider variety of characters, the time needed for a brute-force attack grows dramatically.This data emphasizes that a strong password isn't just about length, but also about complexity. By using a mix of lowercase and uppercase letters, numbers, and symbols, you increase the computational power and time required for a brute-force attack to succeed.

8.Case Studies of major Virus Attacks:

8.1.The WannaCry ransom ware attack was a major attack that came in May 2017. This ransom ware crypto worm's target is to infect computers running on the Microsoft Windows operating system. It encrypts the user's data and demands a ransom. It is acted as a worm. It spread automatically across network without user intervention.

8.2.Stuxnet was discovered in 2010. Stuxnet was discovered in 2010. Its main aim was Iran's nuclear operations. It was specially developed to damage the Natanz nuclear site, which was being used to enrich uranium. Its main objective was to physically harm the equipment so that operations could be slowed down.

8.3. The MyDoom worm, which first came out in January 2004, is known as one of the fastest and most harmful computer viruses ever. It quickly infected millions of computers that used the Microsoft Windows operating system.

Each of these cyber-attacks, in its own way, advanced the field of cyber security. They revealed new and changing threats, showed that attacks can originate from anywhere, and led to a greater emphasis on proactive defenses, cooperation, and a comprehensive approach to security.

8.4 Watering Hole attack, also called a strategic web compromise (SWC), involves infecting a legitimate website with malicious code or malware. When visitors load the compromised page, the site silently delivers and installs malware commonly a Trojan onto their machines [10](Coatesworth).

9. Role of Artificial intelligence and Machine learning in virus detection and integration with other technologies:

AI is playing a very important role in cyber security. Its three main pillars are virus detection, automation, and intelligent decision-making. [5](Mohamed) AI can detect many patterns and anomalies that indicate malicious activity. With AI algorithms, we can analyze network traffic also. The adoption of AI in cyber security provides a defense framework that is more intelligent, adaptive, and scalable. This helps meet the dual objectives of immediate threat identification and preemptive risk reduction. Machine learning, a key part of AI, is very influential in modern cyber security. Its algorithms can learn automatically from data without needing specific instructions, making them highly effective against the complex threats that exist today. ML is generally broken down into three types: supervised, unsupervised, and reinforcement learning and each has its own distinct applications and benefits for cyber security.

Big Data Analytics helps to improve cyber security. It involves examining huge datasets to find trends and patterns that can be used for security. By using tools like Hadoop and Spark, security teams can effectively manage the data needed to train strong. [11](Moshood Yussuf)

10. Role of strong Password in Industry:

In addition to security measures, organizations also need to secure their data. It is the user's responsibility to have a strong password. Users must follow these rules when choosing their new password at the time of registration. By examining the login, register, and sign-up pages of the following web giants, it was possible to gather enough data to understand what rules they require their customers to follow when creating a new account. [6] (Chanda, Password Security: An Analysis of Password Strengths and Vulnerabilities)

- Ebay.com [7](Chanda, http://www.ebay.com/)- Minimum of six and a maximum of 20 characters
  At least one number and/or a special symbol.
  Must be case sensitive
- Amazon.com [8](Chanda, Amazon.com.)- Must have a minimum of 6 letters
  Must be a combination of upper and lower case and/or a combination of letters and numbers.
- Flipkart.com [9](Chanda, Flipkart.com) -Minimum 4 characters

From a brief analysis of the password security rules enforced by the websites mentioned, the author concludes that Flipkart.com has the weakest security. The most stringent rules are enforced by eBay.com, followed by Hotmail.com, as their restrictions require users to create passwords that are inherently difficult to brute-force.

11. Future Trends in Malware and Cyber Security.

Attacker and defender will use AI and machine learning and it strongly influence the cyber security. Attackers will use these technologies to develop more advanced and hard to detect malware on the other hand defender will use them to create more proactive and anticipatory security systems. There are so many AI enhanced attacks that make traditional attack more effective. Now cyber security will move from a reactive “detect and respond” model to proactive “predict and prevent” model. Using AI and Machine learning, security system can analyze vast amount of data from network traffic. The paper concludes by discussing the future of cybersecurity, noting that both attackers and defenders will increasingly use.

12. Conclusion:

Summary of Key Points:

“A Review Article on the role of Strong Passwords in Enhancing Online Security," explores the critical importance of strong passwords in the digital age. Strong password serves as the primary defense against unauthorized access and cyber threats. And highlights the dangers of weak passwords, which leave sensitive information vulnerable to various cyber-attacks like brute-force and phishing.

The paper outlines the key qualities of a strong password, the necessity of length, complexity (a combination of uppercase and lowercase letters, numbers, and symbols), and uniqueness. And also explain the role of password managers as essential tools for generating, storing, and managing these complex passwords, thereby enhancing overall security and user convenience.It concludes by stressing the need for continuous user education and awareness to better password hygiene, which is crucial for protecting personal and organizational data in an increasingly interconnected world.

Bibliography

1. Dinei Florencio, Cormac Herley ˆOne Microsoft Way Redmond, WA, USA. "Do Strong Web Passwords Accomplish Anything?" (2001).**[1]**
2. "Password Security: An Analysis of Password Strengths and Vulnerabilities." I. J. Computer Network and Information Security (2016).**[2][6]**

Carlos Luevanos1,John Elizarraras2. "Analysis on the Security and Use of Password Managers*." (2017).**[3]**

3. El-Taj, Homam. "Artificial Intelligence and Advanced Cybersecurity to Mitigate Credential-Stuffing Attacks in the Banking Industry." IJCESEN (2025).**[4]**
4. Mohamed, Nachaat. "Artificial intelligence and machine learning in cybersecurity:a deep dive into state-of-the-art technique future paradigmss and future." Springer (2025).**[5]**
5. http://www.ebay.com/. 2016. <http://www.ebay.com/>.**[7]**

6. Chanda, Katha. Amazon.com. n.d. <http://www.amazon.com/>.**[8]**
7. Flipkart.com. n.d. <http://www.flipkart.com/>.**[9]**

8. Coatesworth, Barry. "The psychology of social engineering." Cyber Security: A Peer-Reviewed Journal (2023).**[10]**

9. Moshood Yussuf, Adedeji O. Lamina,Olubusayo Mesioye. "Leveraging Machine Learning for Proactive Threat Analysis in Cybersecurity." International Journal of Computer Applications Technology and Research (2024).[11]