Enhancing Digital Security Through Strong Password’s

Password Strength Analysis Tool 

**Professor**

**Sir Naveed Naeem Abba’s**

**Presented by**

Zainab Ahmad, Nosheen, Mahnoor

Abdul Wahid, Sharf-u-d-Din

**Section**

BSCYS A

Fall🡪2024

Contents

[**Introduction** 3](#_Toc186557480)

[**Password** 4](#_Toc186557481)

[**Role of Password in Security** 4](#_Toc186557482)

[**Types of Passwords:** 4](#_Toc186557483)

[**Password Analysis** 5](#_Toc186557484)

[**Types of Password analysis** 5](#_Toc186557485)

* [**OBJ** 6](#_Toc186557486)

[**Strong passwords** 7](#_Toc186557487)

[**Characteristics of Strong Passwords** 7](#_Toc186557488)

[**Weak Password** 10](#_Toc186557489)

[**Why Password Strength Matter’s** 10](#_Toc186557490)

[**Security Breaches Due to Weak Passwords** 10](#_Toc186557491)

[**Security Threats for Weak Password’s** 11](#_Toc186557492)

[**Password Strength Analysis Tool’s** 13](#_Toc186557493)

[**Introducing Password Strength Analysis Tool** 15](#_Toc186557494)

[**Features of The Tool** 15](#_Toc186557495)

[**Work-Flow of the Tool** 15](#_Toc186557496)

[**Password Strength Criteria** 16](#_Toc186557497)

[**Functions in the Program** 16](#_Toc186557498)

[**Sample Interaction User Prompt:** 17](https://d.docs.live.net/8b6dd5aff7870375/Desktop/Cyber-Project-01.docx#_Toc186557499)

[**Real-World Use Cases** 19](#_Toc186557500)

[**Case Study** 19](#_Toc186557501)

[**Future Enhancement’s** 20](#_Toc186557502)

[**Conclusion of Report** 21](#_Toc186557503)

# Introduction

Passwords are the first line of defense against unauthorized access to our digital lives and thus their strength plays a very significant role in protecting sensitive information. Weak passwords can be easily detected and are compromised by unauthorize people like hackers and thus leading to security breach of personal information. Thus, it becomes an important duty of professional people to generate tools that even educate users to create strong passwords and such tool involves the rejection if the user does not enter strong password. Thus, this report highlights the importance of password security threats and provide best practices for generating strong passwords to safeguard our digital assets.

**Purpose of Report**

The purpose of this report is to provide deep analysis of password security and about some common password threats and thus offers and also analyze the best ways to produce or generate effective and strong passwords & to educate people about password security by performing different security measures.

# Password

A password is a secret sequence of character, number and symbols used to authenticate and authorized access to a computer system, network, or application.

It is a crucial security measure designed to protect sensitive information and prevent unauthorized access.

# Role of Password in Security

* **Protect sensitive information**

Personal information-Financial information & Confidential business data.

* **Prevent identity theft**

Minimizing the risk of online fraud.

* **Protect networks and systems**

Protect sensitive info from unauthorized access.

# Types of Passwords:

* Static Password
* Dynamic Password
* Bio-Metric Password
* **Static Password:**

A fixed password used for a specific account or application.

Static password refers to a widely used method of authentication in which a user chooses and enters a fixed password to access a system or service. This method is vulnerable to various attacks such as eavesdropping, dictionary attacks, social engineering, and phishing.

* **Dynamic Password:**

Dynamic password analysis is study of forming the design and implement dynamic password authentication systems to ensure the security of computer system and other devices. A one-time password generates for a specific transaction or session.

* **Bio-Metric Password:**

A password based in unique physical characteristic such as fingerprints facial recognition or voice recognition. Thus, this analyzes user behaviors like password changes and account activity.

# Password Analysis

Password Analysis is a process of evaluating the strength and security of passwords to determine their resistance against any unauthorized access and also hackers and thus analyzing the difficulty involves in breaking a password.

* **Importance**

Password Analysis is very important because it protects the weak password that can be easily compromised and hacked by unauthorized people and leading to the protection of confidential and sensitive data.

# Types of Password analysis

* **Static Password Analysis:**

Static password refers to a widely used method of authentication in which a user chooses and enters a fixed password to access a system or service. This method is vulnerable to various attacks such as eavesdropping, dictionary attacks, social engineering, and phishing.

* **Dynamic Password Analysis:**

Dynamic password analysis is study of forming the design and implement dynamic password authentication systems to ensure the security of computer system and other devices.

* **Behavioral Password Analysis:**

It is a type of password analysis that focuses on analyzing user behavior and password usage patterns to identify the potential security risks. Thus, this analyzes user behaviors like password changes and account activity.

# OBJ

* **Vulnerability Identification of Password**

When developers create some password tools thus, they also know the presence of any kind of vulnerabilities present in that password that if detected by any unauthorized user cause a lot of problem for securing confidential data of the user thus by analyzing password developer can form strong patches for its safety. Such vulnerabilities include weak characters and easily guessable information.

* **Password Cracking Detection**

Passwords if use commonly such that include just letters or characters are easily detected by many hackers because they use attacks like dictionary attacks or phishing attacks and so, it becomes very easy for hacker to breach sensitive information of user and thus cracking the passwords. Thus, by password analysis tool it becomes simple to generate a tool that contains and educate user forming such password that cannot be cracked by hackers or any attacks.

# Strong passwords

A strong password complex and unique combination of characters that include numbers and symbols including upper case and lower cases and thus, these combinations make it a strong one and particularly unguessable.

* **Guidelines**
* Add number and special characters to your password to make it more complex.
* **Avoid using information** that can be easily guessed such as your name, birthday, or common words
* **Avoid Using Common Pattern’s**: ABCD or 123456 thus these common patterns are easily guessed by anyone thus passwords should be unique that do not involve same common pattern.
* **Avoid Using Dictionary words**: Strong passwords do not contain any type of common dictionary words and thus are efficient and effective.

# Characteristics of Strong Passwords

**Length**

Length of password matters a lot in making password strong enough that cannot be then detected by anyone else and so it is important that

Password must be long and thus include as many characters as possible thus, it becomes very hard for hacker to detect the password but not as long that the user also become confuse and cannot remember the password.

* Minimum characters may be **12** or more than that but this is not compulsory and maximum for higher security purpose contain about **128** characters.

**Complexity**

There should be complexity in passwords to make passwords complex.

A password is considered to be complex only if it contains the following things:

* **Uppercase letters**

(A-Z)

* **Lowercase letters**

(a-z)

* **Different numbers**

(1-9…)

* **Special characters**

(!@#$%...)

**Ex: by Combination:**

1. Tr0ubf4d2 K1ng
2. O@sswi0rd! F4kkk203f

**Predictability**

The predictability of a password refers to how easily it can be guessed or cracked by an attacker. Predictability password are those that follow common pattern use easily guessable information or are derived from known data about the user.

**Uniqueness**

A password that is distinct and cannot be used for any other account or purpose, enhancing security by reducing the risk of unauthorized access.

**Password Manger**

Password manager is a tool that manages & stores your password so we don’t have to remember them.

It performs 3 functions:

* Encrypting password
* Generating Strong Password
* Auto-Filling Password

**Regular update of Password:**

Password should be regularly updated and should contain changes when needed so any unauthorized person would ever think what’s your next move.

* Change in password should occur at-least of about after 60-90 days max.

**Two Factor authentication:**

It helps in ensuring rather you are a legitimate user or not by performing 2 different authentication processes. It performs a double check when the user enter the password if the password is even correct the user has to face two factor authentication to verify that the source where from the user wants to enter is the correct one or not.

**Ex:**

* Sending code to a user mobile phone via text message.
* Asking Questions: (Questions that the legitimate user has entered to ask)
* Asking for the Pass Code
* Checking through your device lock pattern.

# Weak Password

A weak password is a password that is easily guessable or vulnerable to hacking. Here are some characteristics of a weak password. The length of weak password is less than 8 characters, only uses one type of character.

**Ex:**

(n a m e, birthday, common words).

Or by using a predictable pattern

**Ex:**

(q w e r t y, 1 2 3 4 5 6).

# Why Password Strength Matter’s

* Weak passwords are a major vulnerability in cybersecurity.
* 81% of hacking-related breaches are due to stolen or weak passwords.
* Average time to crack a weak password: < 1 second.
* Solution to threat is real-time password analysis and improvement.

# Security Breaches Due to Weak Passwords

* **Data breaches**

Accessing confidential data, such as personal information or trade secrets.

* **Unauthorized Access**

Accessing personal accounts or business data bases.

* **Account Takeover**

Using same pass to login in into other accounts

* **Identity Theft**

Can be used to apply for credit, impersonate individuals or engage in fraudulent activities.

# Security Threats for Weak Password’s

**Malwares**

There are also different kinds of malicious malwares including worms, viruses that if enters our systems cause harmful damage to our system by modifying the information causing lowering of availability of data to user.

* **Key Loggers**

A type of malware used to record keystrokes on an infected device

* **Phishing Attack**

Hackers tricked the users that made them disclosing their passwords and thus by creating fake e mails and other fake apps that are open by authorized users and thus they breach their information on their own.

* **Brute Force Attack**

A Brute Force attack is a type of password cracking technique in which attacker use multiple numerous kinds of hits or miss attempts of different password to crack the legitimate user’s password and to gain access on that device or app (whatever the attacker is looking for**).**

* **Ransomware Attack**

Weak passwords can lead to ransomware attack as we know that it can be easily compromised by password attacking techniques, allowing the attacker to gain access to the network through where they can easily inject the ransomware.

* **Choosing weak passwords**

When the user chooses weak passwords ignoring the facts that his confidential information can easily be breached by hacker thus it is also a kind of security threat. Thus, passwords must be strong involving many characters and letters.

* **Password Sharing**

Password sharing is also a kind of threat as the danger in this is human himself that if shares his password to someone can also cause problem like identity theft and the unauthorized user can easily detect the personal information and do many activities he wants to do.

* **Dictionary Attacks**

In this attack attackers use some lists of common password and also dictionary of passwords that are easily implement and thus by this way Attacker can easily detect password of user and breach his confidentiality and thus also can breach integrity by modifying user personal information.

# Password Strength Analysis Tool’s

Password strength tools are used to measure the effectiveness and efficiency of passwords in terms of measuring its ability and resistance against malicious attacks performed by unauthorized persons.

* Passwords testing tools helps the users and other organizations ensure that passwords are secure and users can comply on them.
* **Password Meter**

Password meter is password strength tool that is used to measure and evaluates password strength by providing feedback to its user about how weak is your password or how to make it strong by adding many or combination of characters.

* Some important features including:
* **Length**

It describes that how lengthy password’s having more characters are more secure and it takes a very long time for hacker to break it.

* **Character Variety**

This tool also checks and provide feedback about involving characters like uppercase and lowercase that make password strong and thus educates the user about adding them to make password strong. As if you make password like “123456” then this tool educates you to generate your password more complex and will not accept your simple password.

* **Pass fault**

Pass fault is also a modern and advance password strength tool that provides analysis for password security and offer suggestions and educates user for improving password strength based on current attacker paths they adopt to attack others accounts by knowing their passwords.

* **Password Analyzer**

Password analyzer is also checking strength of password and thus,

It is also used to measure password strength by checking the strength of password and thus, also check password by testing the length of password and also testing the complexity of password. Thus, this describes how important it is to secure your online accounts through secure passwords.

* **Limitations**

There are some limitations of password strength analysis tool’s which are as given below:

* Password strength testing tools are still not too advance to detect all kinds of password weakness and thus, systems are exploited by advance cracking algorithms.
* Password strength tools are also unable to detect that if a password has been reused across multiple accounts.
* Password strength tools are also unable to detect and educate user about not entering easy and guessable passwords.

# Introducing Password Strength Analysis Tool

**Powered by C++**

# Features of The Tool

**Password Strength Assessment**  
 Evaluates criteria like length, character variety, and common patterns.

Output entropy (bit-level randomness) for accuracy.  
**Password History**  
 Tracking of password & evaluates the date, strength, and password (securely).  
**Security Tips**  
 Recommends best practices for strong passwords.  
**Password Generator**  
 Randomly generates strong passwords upon request.

**Interactive User Interface**

Menu Options &User Prompts

**Strength Suggestion and Improvements**

# Work-Flow of the Tool

* Prompts the user to enter a password.
* Analyzes the strength of the entered password based on length and character variety.
* Calculates and displays the password's entropy.
* Checks if the password is common.
* Provides feedback and suggestions for improving the password.
* Offers to generate a strong password if the entered password is weak.
* Adds the analyzed password to the history.
* Provides options to check another password, view history, see tips, or exit.

# Password Strength Criteria

**1. Minimum Requirements:**

At least 8 characters.

Uppercase, lowercase, digit, and special character**.**

**2. Common Password Detection:**

Flags weak passwords like 123456 or password.

**3. Entropy Calculation:**

Higher entropy = stronger password.

Formula of entropy= L\*log2 (N)

where L = length and N = character pool size

**Entropy**

* In the context of passwords, measures the randomness and unpredictability of a password
* It helps to determine how difficult it is for someone to guess or crack the password.

# Functions in the Program

* **Checking Password Strength:**

Analyzes password and provides suggestions.

* **Add Password-History:**

Logs analysis for future reference.

* **Display-Password-History:**

Displays stored history with timestamps.

* **Generate Strong-Password:**

Creates secure random passwords.

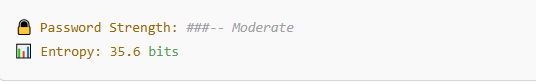
* **Calculate Entropy:**

Compute’s password randomness in bits.

# Sample Interaction User Prompt:

**Strength level**

**Enter password to check its strength: Abdul!!**

****

Password=> “Abdul!!”

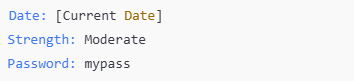
is missing digit here

**Suggestions**

**CODE 2**

Showing that the password is missing a digit & asking for Suggestion of new password

**History entry**

****

Showing the User his password History

**Security Manual**

Showing the User Security Tips  
so he can improve his password ability.

🛡 Security Tips:

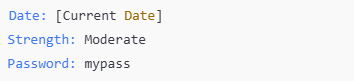
- Use a mix of uppercase, lowercase, digits, and special characters.

- Avoid common words and phrases.

- Do not reuse passwords across multiple sites.

- Change your passwords regularly.

**Pass Generator**

****

**🎲 Generated strong password: Bj6!H!#o :**

Generated Strong pass for

The user for better understanding.

**Thank You!!!....**

# Real-World Use Cases

1. **Personal Security**

Individuals checking their password strength.

1. **Enterprise Applications**

Employee password policy enforcement.

1. **Educational Tool**

Teaching secure password practices.

1. **Data Breaches**

* Over 80% of data breaches in 2020 involved lost or stolen credentials.
* We also found that 81% of data breaches were due to weak, default, or stolen passwords.

# Case Study

There are many cases related to password breakage and collection of users personal data that then cause many cyber-attacks on persons thus, all the real cases describe the importance of creation of secure password. As, one of those cases is discussed below:

**Sony PlayStation Case**

**Case Background:**

In 2011 hackers used combination of phishing and password cracking techniques implied on company system and thus hack about 77 million users accounts and thus then they compromise their personal information.

**About Attack:**

Hackers gained unauthorized access to Sony PlayStation

Systems and thus, exploiting vulnerability to their web server

Software. Thus, hackers then did implement of malicious attack on system server and then they ex filtered the personal information of users and gained access to millions of accounts of users including their names, addresses and also email addresses.

**Circumstances resulting from Attack:**

**Lack of Service Availability:**

Due to attack, there is lack of service availability by company for about 24 days that caused a lot of inconvenience to users.

**Loss of Company Reputation:**

There is also loss of reputation of company and thus, that causes a huge loss of customers and also their trust and also there was decline in sales.

**Financial Damage:**

There is loss of money of about 170 million dollars due to users and company data breach. And thus, Sony faced a lot of damage and trouble at that time.

* **Recommendations:**
* This case made all world learn about how important is security and about implementing two factor authentication and other security measures.
* Also, this case highlighted the importance of regular updating the software and also creating patch for software and in order to secure the system.

# Future Enhancement’s

* GUI integration using Qt for better usability.
* API integration for real-time breach checks.
* Multi-threading for faster performance.
* Password encryption for enhanced security.

# Conclusion of Report

In conclusion, password security is more important and critical aspect of cybersecurity. By educating people about strength and weakness of password analysis tools and implementing effective security measures, individuals and organizations can significantly reduce the risk of password related breaches and so, protecting personal information of their own