Password Strength Tester Presentation | by Rim Ferchichi

1. Brief Introduction

Our world increasingly revolves around online accounts, making strong passwords crucial for protecting our data. Studies show that a staggering percentage of users rely on weak passwords, leaving them vulnerable to cyberattacks.

This document details our password strength tester which will be presented at the end of the semester, a user-friendly tool designed to empower individuals to create robust passwords. It provides real-time feedback on password strength, mitigating the risk of data breaches and unauthorized access.

2. Solution Overview

In today's digital landscape, robust passwords are the first line of defense against cyber threats. However, crafting strong passwords that adhere to recommended criteria can be challenging. Our solution addresses this by offering a user-friendly interface. Users simply input their desired passwords and receive immediate feedback on their strength based on various factors, including length, complexity, and character diversity. This empowers them to make informed choices and create significantly more secure passwords.

3. System Architecture

The password strength tester operates through two core components: the user interface (UI) and the validation engine. The UI provides an intuitive interface for users to input passwords and displays a strength checklist. The validation engine, working

seamlessly behind the scenes, analyzes the password against predefined criteria to determine its overall strength level. This interaction between UI and engine ensures an informative and user-friendly experience.

4. Working Flows

The user journey begins with simply entering the desired password into a designated field. As each character is typed, the validation engine continuously evaluates the password against pre-defined criteria. Simultaneously, the UI updates in real-time, reflecting the current strength status through a checklist. Users can instantly see which criteria their password meets (e.g., minimum length, uppercase characters) and which areas require improvement, fostering informed password creation.

5. Roles/Users

Our solution focuses on a single user role: the end-user seeking to create a secure password. Users have the responsibility of inputting their desired password and following the feedback provided by the strength tester's checklist. This empowers them to make informed choices and create stronger passwords for their online accounts.

6. Functions and Steps

The core function of our password strength tester is to evaluate user-provided passwords. This process involves several steps:

1. **User Input:** The user enters their desired password into the designated field.
2. **Real-Time Evaluation:** The validation engine continuously analyzes the password against predefined criteria like minimum length, character type diversity (uppercase, lowercase, numbers, symbols), and dictionary word checks.

3. **Strength Feedback:** The UI updates in real-time to display the strength checklist, indicating which criteria the password meets (checkmarks) and which need improvement. This empowers users to refine their passwords until they achieve a strong security posture.

7. Data Exchange

Data exchange within the system primarily involves user-provided passwords and the corresponding strength feedback generated by the validation engine. All password transmissions utilize robust encryption methods, ensuring confidentiality and data integrity throughout the process.

8. Future Enhancements

We envision several enhancements to further elevate the user experience:

- **Integration with Password Managers:** Seamless integration with existing password managers would enhance user convenience by allowing password creation and storage within a familiar platform.
- **Advanced Strength Criteria:** Expanding the validation criteria to include factors like keyboard proximity (avoiding easily guessable sequences) can provide even more robust password creation guidance.
- **Multi-Factor Authentication Support:** Integrating support for multi-factor authentication methods (e.g., SMS verification) could offer an additional layer of security for user accounts.

By continuously evolving our solution, we strive to provide users with cutting-edge tools to navigate the ever-changing security landscape.

9. Conclusion

Our password strength tester offers a practical and user-friendly solution to elevate password security. By providing real-time feedback on password strength, we empower users to create strong and resilient passwords, significantly reducing the risk of unauthorized access and data breaches. This not only safeguards their online accounts but also fosters increased confidence and peace of mind in today's digital world.