BINF711 – Information Security

Project is worth 20% of the course grade

General Description

Password Management and authorization tool: This project focuses on implementing access control mechanisms through authentication and verification. It consists of two primary phases:

1. **Milestone 1:** Password Management Application
2. **Milestone 2:** Cryptography and Encryption Techniques

Milestones, Deliverables, and Dates

Milestone 1: Password Management Application

- **Deadline: 25.10.2025, @11:59 PM.**
- **Deductions will be made for late submissions.**
    - **Late Submission Penalties:**
        - The first two days (up to 48 hours late): A penalty of 50% will be deducted from your total grade.
        - From the third day to the seventh day (48 hours to 5 days late): A penalty of 75% will be deducted from your total grade.
        - Submissions beyond 5 days: Unfortunately, submissions will receive a 0 grade.
- **Teams of 2 to 3 students (Cross-tutorial teams are NOT allowed).**
- **Technologies:** Utilize programming languages such as **Python** or **Java** to create the application.
- **Submission Link: https://forms.gle/F3y6P3kw2yhA4PoR8**

Objective

The goal of this phase is to develop a Password Management Application (PMA) that ensures robust authentication through effective password management and account lockout policy.

Components:

1. Password Strength Analyzer

- **Description:** Develop a tool that evaluates the strength of user-generated passwords.
- **Functionality:**
  - Compute the password complexity.
  - Analyze the complexity of passwords using criteria such as length, character variety (uppercase, lowercase, numbers, special characters), and common patterns.
  - Provide real-time feedback to users on the strength of their passwords.

- **Research Basis:**
  - Conduct a search for the most secure password combinations and reference a relevant paper that discusses password strength evaluation techniques.
  - Critique every one of them, then select the best technique to use it for password valuation. Justify your selection.
  - Reference all relevant papers and research articles related to password strength evaluation and encryption techniques that you used in your research to support your conclusions and analysis.

- **Feedback Mechanism:** The app will compute password complexity and enforce users to create stronger passwords based on research findings.

2. Login System Implementation

- **Description**: Develop the basic functionalities found in a Login system (no need to create a UI for the functionalities)
- **Functionality**:
  - Create a Sign-up function which will save a username and password, the password policy will be the same as the one chosen in part 1. The sign-up should refuse weak passwords according to the chosen policy.
  - Create a Login function which will check if the actual password was entered. It will also need to check if the password has expired or not and if the account is locked-out or not.
  - Create a random password generator which, when called, will return a random strong password which would be accepted by the password policy.

- To implement password expiry, you could either implement it using a time-stamp (after a certain amount of time it expires) or by valid attempts (after a number of valid logins, the password should expire).
- To implement the lock-out policy, you will have to keep count of the number of wrong logins done and after e.g. 3 consecutive failed attempts, the account will login and will send a message indicating that the account is locked out and the login was not successful. (You do not have to keep track of the time between attempts, simply keep count of the wrong login attempts). The counter for wrong attempts is reset after a correct attempt (e.g. after 2 incorrect attempts the counter is 2, then after a correct login it is reset back to 0).

Reference all the resources you used in your research to find the most up-to-date security techniques.

Conclusion

This project aims to establish a comprehensive access control system through effective password management and encryption techniques. By combining a robust password strength analysis tool with secure cryptographic practices, we can enhance the security of user authentication processes.

Important Note!!

Plagiarism:

Any detected plagiarism will result in a 0% score with no second chances. This includes any similarities in the prototype design between groups. Any similar submission to online repositories, as well as using AI to generate any other required milestones, will also be penalized.