Mubasher Mehnaz Begum

Course: CST-221

Assignment: CST-221 User Interface and Security

Date: 19 July 2020

GIT LINK: <https://github.com/MubasherBegum/CST-221>

In this assignment, I am going to develop a user interface for **three different functions** of an operating system and how each of the functions could be secured using various authentication schemes. The assignment requires us to support one single factor, one two-factor, and one multi-factor authentication scheme in the design. The user design will address the following three main security areas:

1. Proposed Security Authentication Scheme
2. Proposed Security Authentication Factor
3. Required Security Policies

# Single Factor Authentication (SFA)

This is the traditional user authentication process for accessing computer resources. With single-factor authentication, only one category of credentials is specified, for example, username and password. The most prominent single factor identifier is the password. Other identifiers commonly used include SMS-code to a registered mobile device, one-time password (OTP) generated by a physical device or by software running on a mobile device or computer.

SFA is considered less secure than MFA, especially when the identifier is a vulnerable password.

Here I am using a login with User Id and Password to login to a test application. Login User ID and Password need to be entered in a login screen. They are validated and if there are any validation errors with respect to password they are displayed on the screen and login is un-successful. If validation is success, the user can login to the system. If the credentials are wrong for 3 consecutive times, the user account is locked for 24 hours or until a system administrator un-locks the account.

**Required Security Policies for SFA**

Following are the minimum required security policies that SFA uses

* Login Username or ID must contain all alphanumeric characters with a length between 8 and 10.
* Password must contain all alphanumeric characters with a length between 10 and 15 and at least one letter must be uppercase.
* Password needs to be prompted in order to be changed every 90 days.
* Password history is maintained so that there are no duplicate occurrences within last 10 entries.

User Interface Showcasing SFA with a Login Screen of a Test Application.

A screenshot of a cell phone

Description automatically generated

Flowchart SFA with a Login Screen of a Test Application.

A close up of a map

Description automatically generated

# TWO FACTOR AUTHENTICATION (2FA)

Two-factor authentication uses the same password/username combination, but with the addition of being asked to verify who a person is by using something only he or she owns, such as a mobile device. Two-factor authentication (2FA) requires two proofs of identity and those two proofs must be from two different factors. A common scheme first prompts you to enter a password (something you know) and then asks you to type a code generated on your phone (something you have). Many combinations of identifiers can be used, including password plus SMS-code to a registered mobile device, password plus a biometric identifier from a fingerprint sensor, passwords plus answers to knowledge-based authentication questions, and more.

**Required Security Policies for Two factor authentication are**

Security policies include but are not limited to username validation, password validation, password encryption, password anonymity, unique character processing, length verification, etc.

* Username and password tied to specific host on system
* Username will have a max length of 50 characters
* Non-alphanumeric characters are supported for username and password
* Password will have a max length of 25 characters
* Password restrictions, minimum 8 characters, 1 special character
* Encryption supported for password field only
* Password will be displayed as bullets instead of character representation
* Password reminder triggered after failed attempt
* Password locked for 1 minute after 3 failed attempts, time doubles for additional failures

User Interface Showcasing Two factor authentication with a Login Screen of a Test Application which requires Authentication code to be entered.

A screenshot of a cell phone

Description automatically generated

Flowchart for Two factor Authentication

A close up of a map

Description automatically generated

# Multi FACTOR AUTHENTICATION (MFA)

Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is). The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply the factors required for access. If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by multi-factor authentication then remains blocked.

Generally, database connections are established within the function of a program, though an interface could be used to input all the database factors and manage them as well. The multiple factors include database port, database name, root username, and root password. Security policies include but are not limited to, port authentication, username authentication, password authentication, database authentication, connectivity monitoring, etc.

**Required Security Policies for Multi factor authentication are**

* Port input checked for length and numerical data
* Username authentication compared to database entry
* Username length check, maximum characters 50
* Password restrictions, minimum 8 characters, 1 special character
* Password encryption
* Password length check, maximum characters 25
* Password authentication compared to database entry
* Target Database authentication
* Database length check, maximum characters 50

User Interface showcasing Multi Factor Authentication

A screenshot of a cell phone

Description automatically generated

Flowchart for Multi Factor Authentication

A close up of a map

Description automatically generated

GIT LINK: <https://github.com/MubasherBegum/CST-221>