Taylor Rosby

CST – 221

User Interface and Security

December 14, 2019

**Add User**

The user interface design address authentication scheme by using one factor authentication before allowing the current logged in user to create a new user. The password must match the one that the user uses to log in before they can even access the page to put in new user information. The new password will require alphanumeric characters and be at least 8 characters long or it won’t be accepted. The system tells the user how strong the password is and will warn them against using common words but will not stop them.

* The add user button will be hidden until after the user is authenticated
* The user will need to click the unlock button to trigger the authentication process
* A popup will show after the unlock button is pressed asking for the password of the user that is currently logged in
* The user will need to enter the same password they use to log in and click the authentication button
* The user will be taken back to the original page with the add user button now visible
* The user will be taken to a page to input the new user information once they press the add user button
* The user will select if the new user account is standard or an administrative account
* The user will input the name for the account
* The user will input a username for the account which will be used for the home directory and will not have the option to change it
* The user can choose to set the new account password at that time or during the next login
* The password needs to be alphanumeric and will display the strength of the password below
* The password must be at least 8 characters
* The password will never be displayed in clear text as it is being typed or transmitted
* The password will be encrypted when it is stored
* The user will need to confirm the password by typing it again in a new input box
* The user will press the add button in the upper right corner to add the user account

**A screenshot of a cell phone

Description automatically generated**

**A screenshot of a cell phone

Description automatically generated**

**A screenshot of a cell phone

Description automatically generated**

**A screenshot of a cell phone

Description automatically generated**

**Login**

The login interface requires the user to change their passwords every 100 days. If the password has not been changed in this time, the user will be able to change it on the login screen and it needs to meet the security factors. These factors include alphanumeric characters, at least 8 characters long, cannot be similar to the last 5 passwords. If the user fails to login after 3 times their account will be locked for 1 minute, and time will be added after each subsequent failed attempt. The login user two factor authentication. The first factor is the password, the second factor is a security key that is used with the partner app on a mobile device.

* A user will require a username and password to have access to the account
  + This will be done using two-factor authentication
  + The user will input their password after clicking the account that matches their username
  + Once the password is confirmed they will use a security key that is sent from their mobile device
* The password must have alphanumeric characters and be at least 8 characters
* The password is not going to be displayed as it is being typed or transmitted
* The password will need to be changed every 100 days
* The password cannot repeat the last 5 passwords
* The user will be notified if their password is incorrect but will not show the password requirements
* If the user puts in the wrong password 3 times in a row their account will be locked
* After the account locked each subsequent failed attempt will lock the account for a longer time

**A screenshot of a cell phone

Description automatically generatedA screenshot of a cell phone

Description automatically generated**

**A close up of a sign

Description automatically generated**

**List Running Process**

The following design uses the multi factor authentication scheme by requiring the user to enter a password, a security key from a mobile device, and to enter either a face id or fingerprint from a mobile device. The design includes two types of authentication factors (type 1 – something you know and type 2 - something you are) to be utilized in the authentication scheme. The password is required to be changed every 100 days and cannot be similar to the last 5 passwords. The security key sent from the mobile device is unique to the device and will be encrypted during transfer.

* The user will select the running process application in their file system
* The user will be asked to enter their password
* The password must have alphanumeric characters and be at least 8 characters
* The password is not going to be displayed as it is being typed or transmitted
* The password will need to be changed every 100 days
* The password cannot repeat the last 5 passwords
* The user will be notified if their password is incorrect but will not show the password requirements
* Their password will be verified
* A security key will be requested
* The security key is unique to the device and will be encrypted during transfer
* A mobile device will send the security key
* The security key will be verified
* The user will be requested to use their mobile device to input either a face id or fingerprint
* The face id/fingerprint will be verified
* Once all factors have been verified the user is shown all the currently running processes on their system

**A screenshot of a social media post

Description automatically generated**

Authorize

**A screenshot of a cell phone

Description automatically generated**

**A screenshot of a cell phone

Description automatically generated A close up of a logo

Description automatically generatedA screenshot of a cell phone

Description automatically generated**

**A close up of a sign

Description automatically generated**