User Interface and Security

Michael Rogers

Grand Canyon University: CST-221

5/20/2018

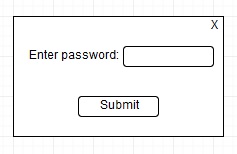
**Single Factor Authentication**

For single factor authentication, the feature I am choosing is attempting to access a password protected file in a shared folder. The authentication factor is just the password being entered. The security policies are validating the password, masking the password as it is being typed, and limiting attempts at the password.

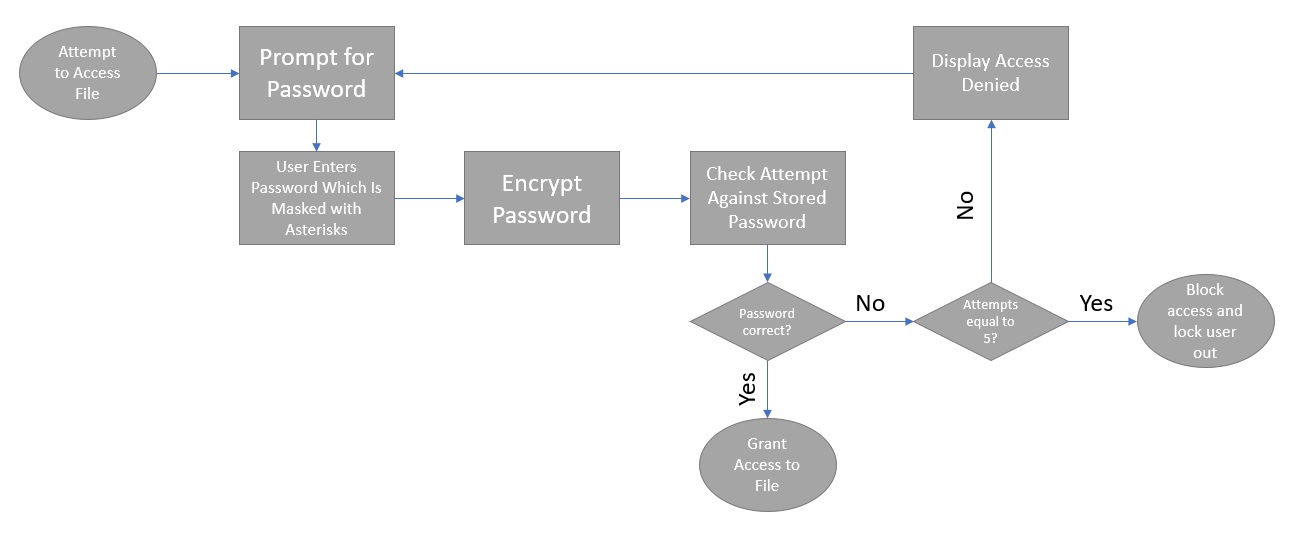
**Functional Requirements:**

* User is prompted to enter password to access file.
* Password must be 8 or more characters.
* Password must contain at least one non-alphanumeric character.
* User is locked out after 5 unsuccessful attempts.
* User input will not be displayed. Asterisks will be shown instead.
* Password will be encrypted at rest.
* Password attempt will be encrypted and checked against the password being stored.

**Wireframe:**

****

**Flowchart:**

****

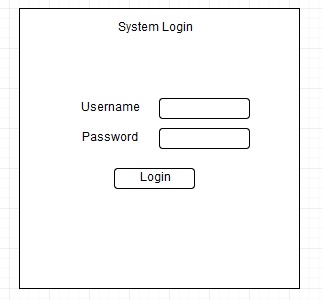
**Two Factor Authentication**

For two factor authentication, the feature I am choosing is logging into a workstation. Typically, the two factors involved would be a username and a password. Policies would include validating the username and password, masking the password with asterisks, and password encryption.

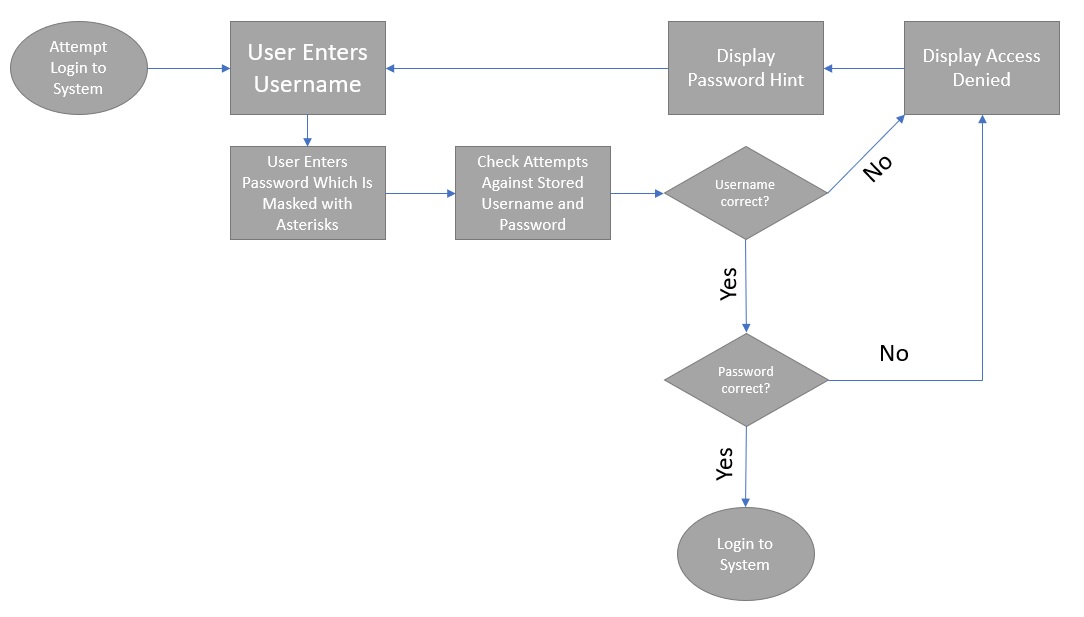
**Functional Requirements:**

* User is prompted to enter username and password to login to system.
* Username has a max length (25) but no minimum length.
* Password does not have a character requirement.
* Password can contain all types of characters.
* User password input will not be displayed. Asterisks will be shown instead.
* Password attempt will be encrypted and checked against the password being stored.
* User can be prompted to show their pre-set password reminder.

**Wireframe:**

****

**Flowchart:**

****

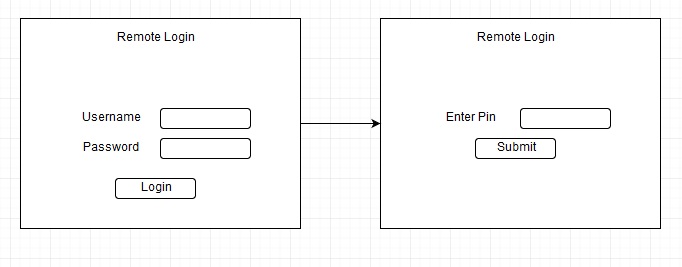
**Multi-Factor Authentication**

For multi-factor authentication, the process I am choosing is attempting to remote access into another system. The factors would be a username, password, and a PIN number that is sent as a text message to the cellphone registered to the username. Policies include validating the username, password, and PIN, masking the password with asterisks, and password encryption.

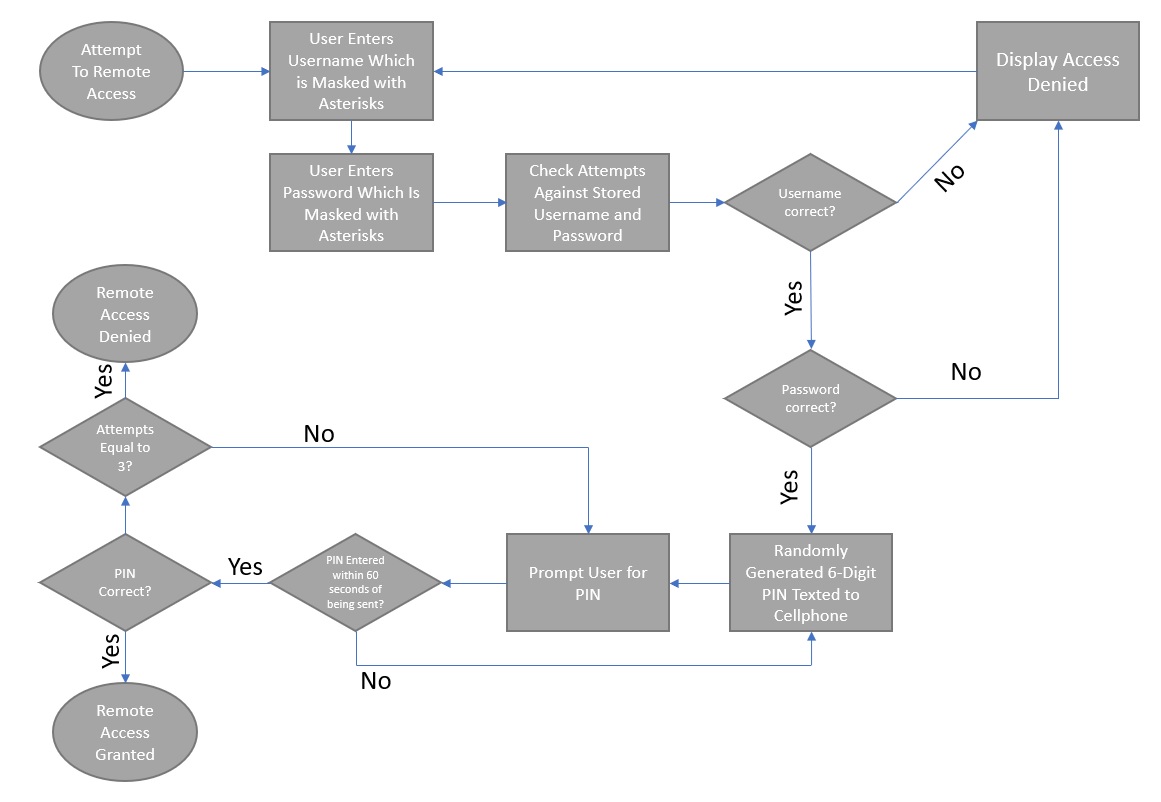
**Functional Requirements:**

* User is prompted to enter username and password to remote login.
* Username has a max length (25) but not minimum length.
* Password must be 10 or more characters.
* Password must contain at least one number and one non-alphanumeric character.
* Password must be changed every 30 days.
* New passwords cannot be the same as a previously used password.
* Both username and password will be masked with asterisks.
* Password attempt will be encrypted and checked against password being stored.
* If username and password are successful, user will be sent a randomly generated 6-digit PIN number to their pre-registered cell phone number.
* User must enter the PIN within 60 seconds.
* If 3 incorrect PINs are entered, lock user out.

**Wireframe:**

****

**Flowchart:**

****