Michael Weaver

CST – 221

John Zupan

3/4/2018

Github Link: <https://github.com/battousairurik/CST-221>

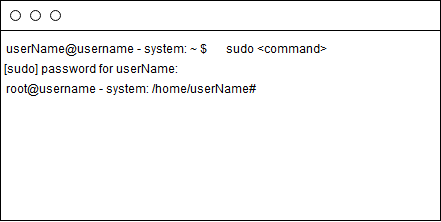
**User Interface and Security**

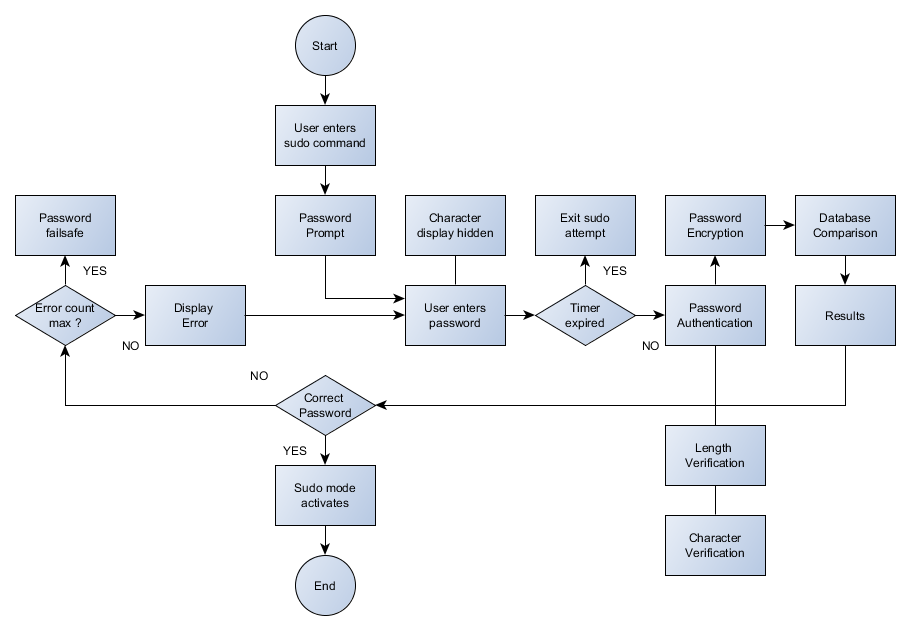
Single Factor Authentication Scheme

*Enabling sudo from the terminal*

The sudo superuser scheme is executed in the terminal, hence the user interface is blended into the terminal itself. The authentication factor would be the password entered for the superuser account. Required security policies include but are not limited to; password validation, password anonymity, password entry timeout, and unique character processing.

* Password must be entered in the terminal
* Password characters will not be displayed back to the user
* String length above max length will not be submitted and generate an error
* Non-Alphanumeric characters will not be accepted
* Password will be encrypted and compared to stored password
* Password will be stored in encrypted form
* Method will check for proper input, blank field will be rejected
* Trigger failsafe if wrong password entered too many times
* Discard sudo attempt after set duration of user idleness
* Password restrictions, minimum 8 characters, 1 special character



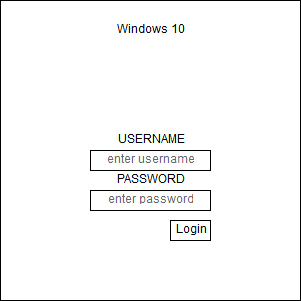


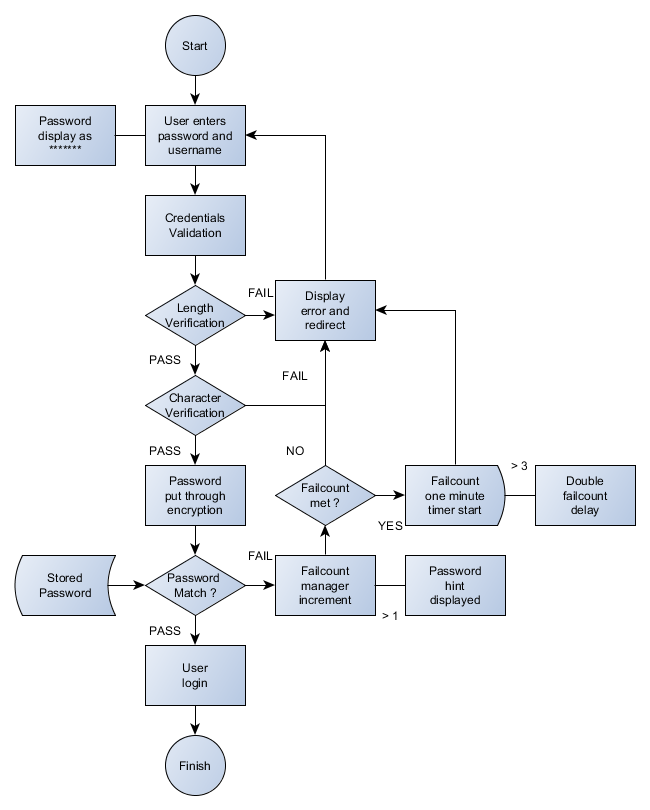
Two Factor Authentication Scheme

*Username and Password verification*

Username/Password authentication generally occurs for login purposes and would have its own dedicated screen. The two factors for such a scheme are the username and password for the selected account. 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





Multi Factor Authentication Scheme

*Database Access*

Generally, database connections are established within the function of a program, though an interface could be used to input all of 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.

* 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

