CST-221

User Interface and Security

Nate Ramey

Grand Canyon University: CST-221

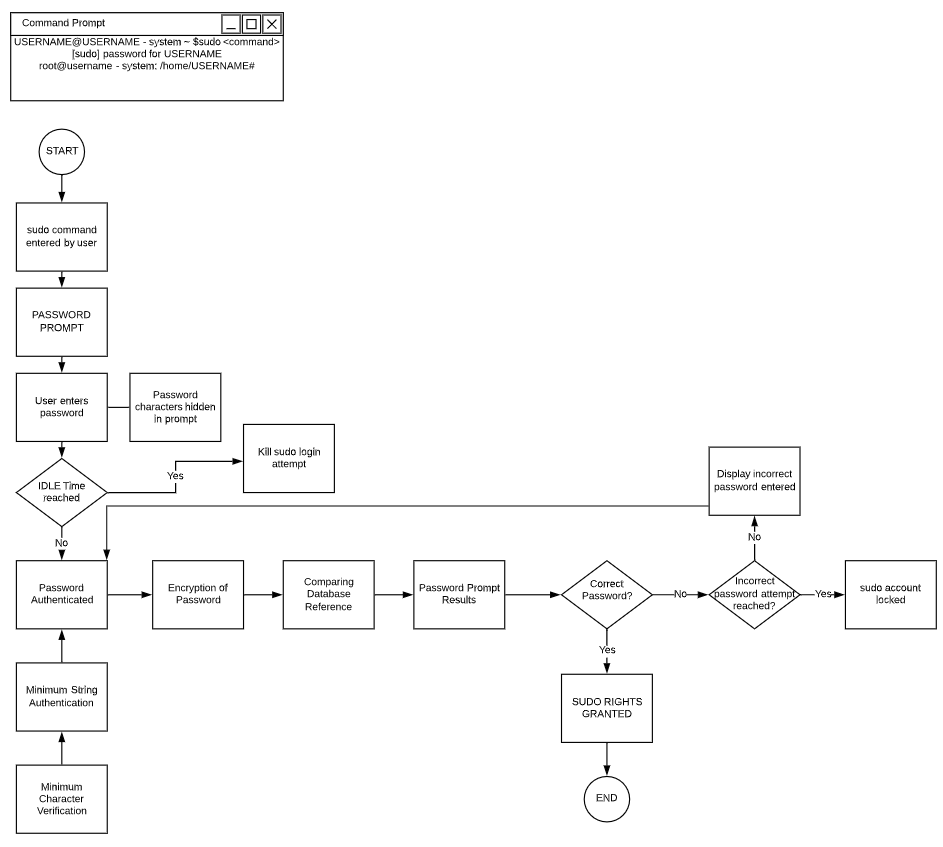
**Single Factor Authentication Scheme:**

Enabling sudo via terminal

Sudo superuser is executed in the terminal. Basically, the terminal pop-up windows act like a user interface. User authentication would be a password entered for the superuser account. Obviously, a security policy would be entering the correct password for the superuser account along with password anonymity, unique character requirements, and terminal entry timeout.

**Single Factor Authentication Requirements:**

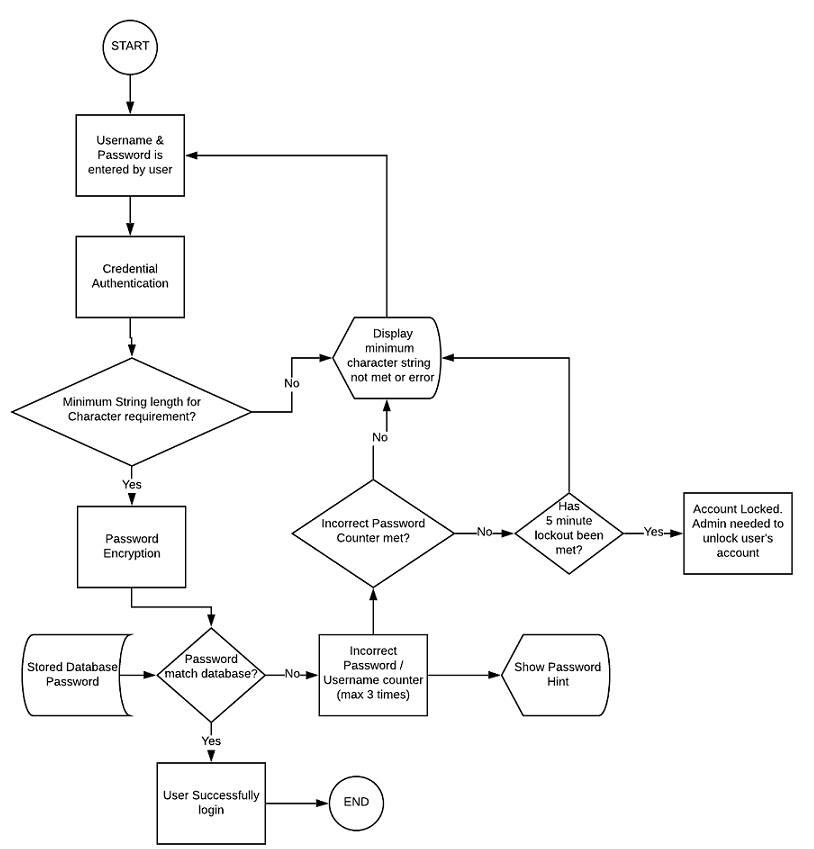
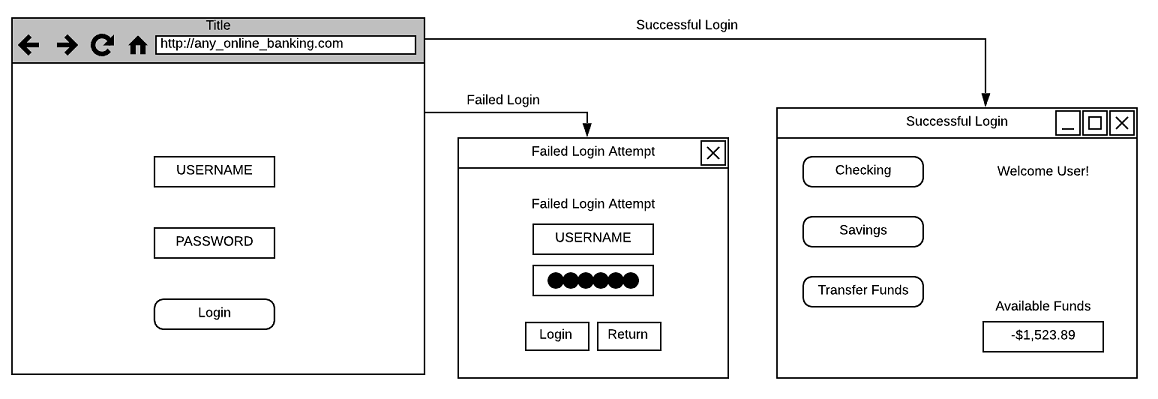
* The password is required to be entered into the terminal. No other means of input will be accepted i.e. remote terminal login.
* All password characters will not be displayed when being typed into the terminal.
* If the password string length is above the allocated length, the terminal will output an error
* Passwords will be encrypted and then compared to the stored password.
* A method would be used to ensure proper input. A blank field (on the terminal) will be rejected.
* Enable the superuser account to be locked after so many failed attempts.
* Set a time idle duration that will automatically log the user out of the superuser account.
* Password Restrictions: String of 8 characters minimum, and 1 special character.



**Two Factor Authentication:**

Two factor authentications schemes use a username and password validation for login purposes. User will be prompted to enter their information via a separate UI screen. This UI can be a pop-up window or when the user navigates to the site that is requesting the authentication. Security policies normally contain username and password verification, password encryption and anonymity. More security policies contain unique character and string length requirements.

* Host database already has a Username / Password designated to it.
* String Length of username will have a max of 25 characters.
* Non-alphanumeric characters are allowed for creation of username / password.
* String length of password will have a max of 25 characters.
* Password Restrictions: String of 8 characters minimum, and 1 special character.
* Encryption is only supported with password, not username.
* Password characters are displayed as bullets.
* Reminder is displayed after a failed login attempt. 3 failed attempts will lock the account
* Password is locked after 3 failed attempts for 5 minutes and after the 4th attempt will require administrator intervention to unlock account.



**Multi Factor Authentication:**

Multi Factor Authentication requires many four things from the user. Something the user has, something the user knows, something the user is, and somewhere the user is. Something the user has can be anything physical the user has (cellphone). Something the user knows can be their password. Something the user is mainly is biometrics such as fingerprints, or iris scans. Lastly somewhere the user is can be a physical location the user is. This can be verified by GPS location or even a MAC address associated with the user.

* Host database already has a Username / Password designated to it.
* String Length of username will have a max of 25 characters.
* Non-alphanumeric characters are allowed for creation of username / password.
* String length of password will have a max of 25 characters.
* Password Restrictions: String of 8 characters minimum, and 1 special character.
* Encryption is only supported with password, not username.
* Password characters are displayed as bullets.
* Database will see if the user’s MAC address is the same as when they made the original account.
* The site will ask for two options for verification. Which can be in the form of a text or email on file.
* A text/email while be sent to the user with a specific code they need to input. There is a 5-minute time limit to enter this code.
* If code is inputted incorrectly, another code will be sent.
* If second code fails, account is locked for an hour.
* After the allotted time is up, the user can try to log in again. If the user fails that time, admin will be needed to unlock account via security questions the user should know.

