CST-221 Operation Systems

Joe Leon

User Interface.

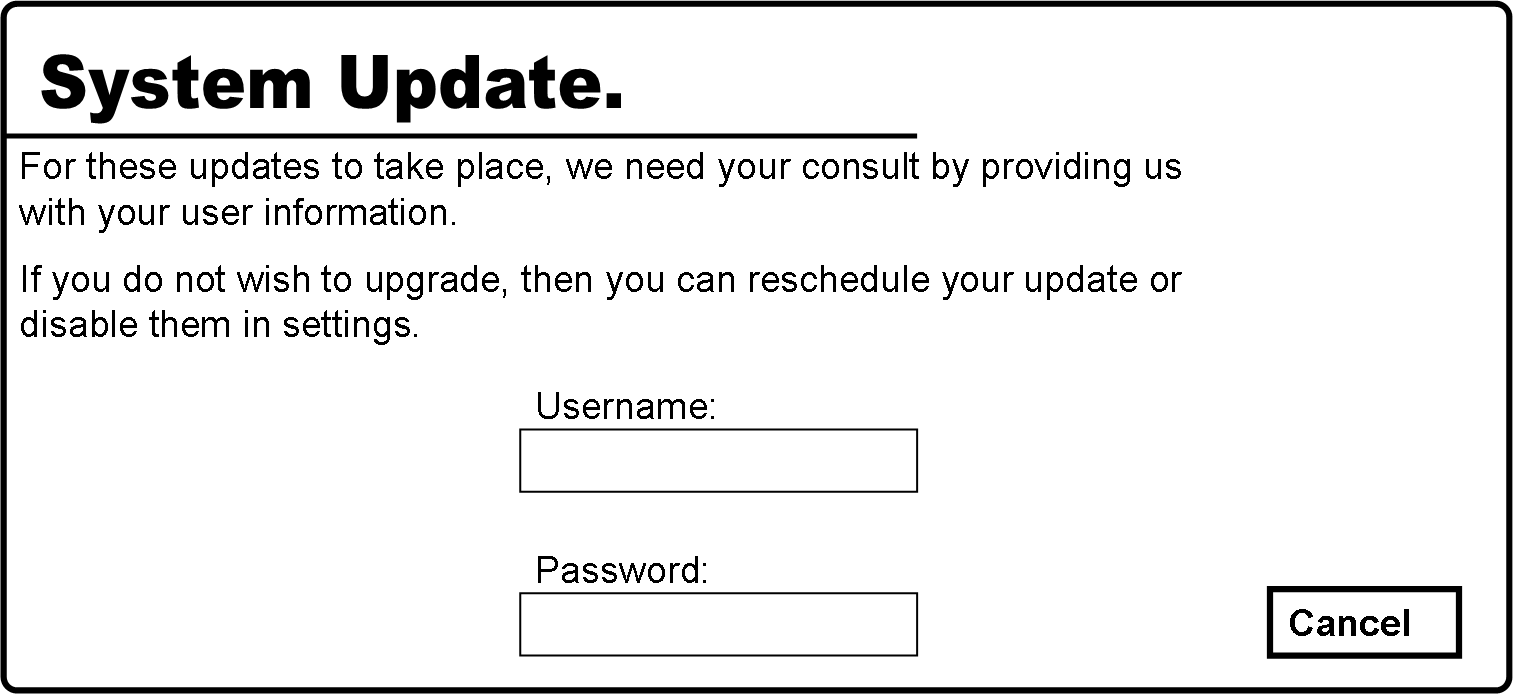
12-10-19

Github: <https://github.com/SkieXI/CST-221-Final.git>

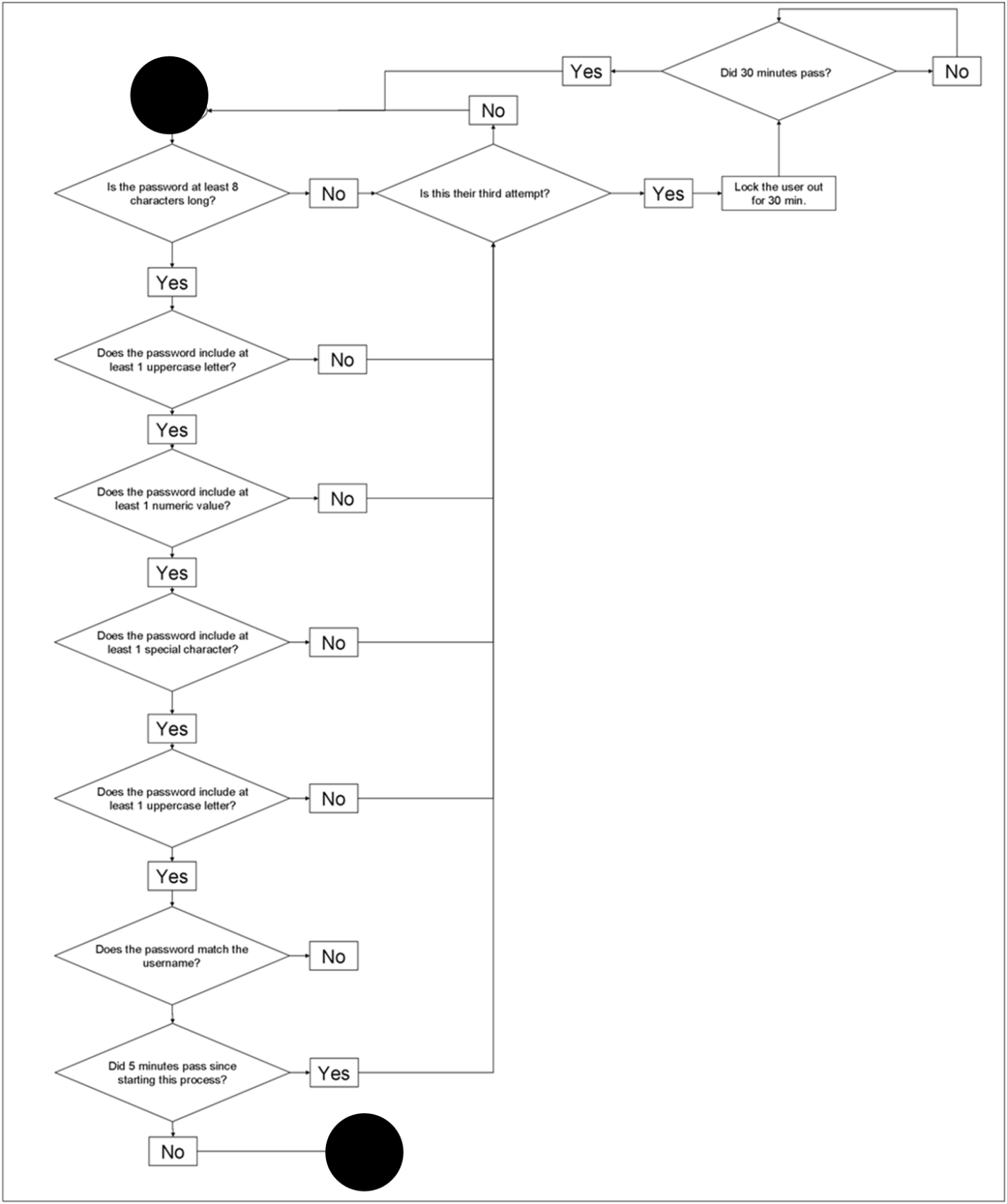
1a. For a single factor security feature, this would be a very basic operation, such as system updates or more critical software updates. In this case, the security is testing the user for something have set up themselves in the past.

* Do the username matched?
* Is the password at least 8 characters long?
* Does it include at least 1 uppercase character?
* Does it include at least 1 numeric value?
* Does it include at least 1 special character?
* Did the user enter the password correctly within three attempts?
* Did the user enter the password within 3 minutes of opening the window?

1b.

****

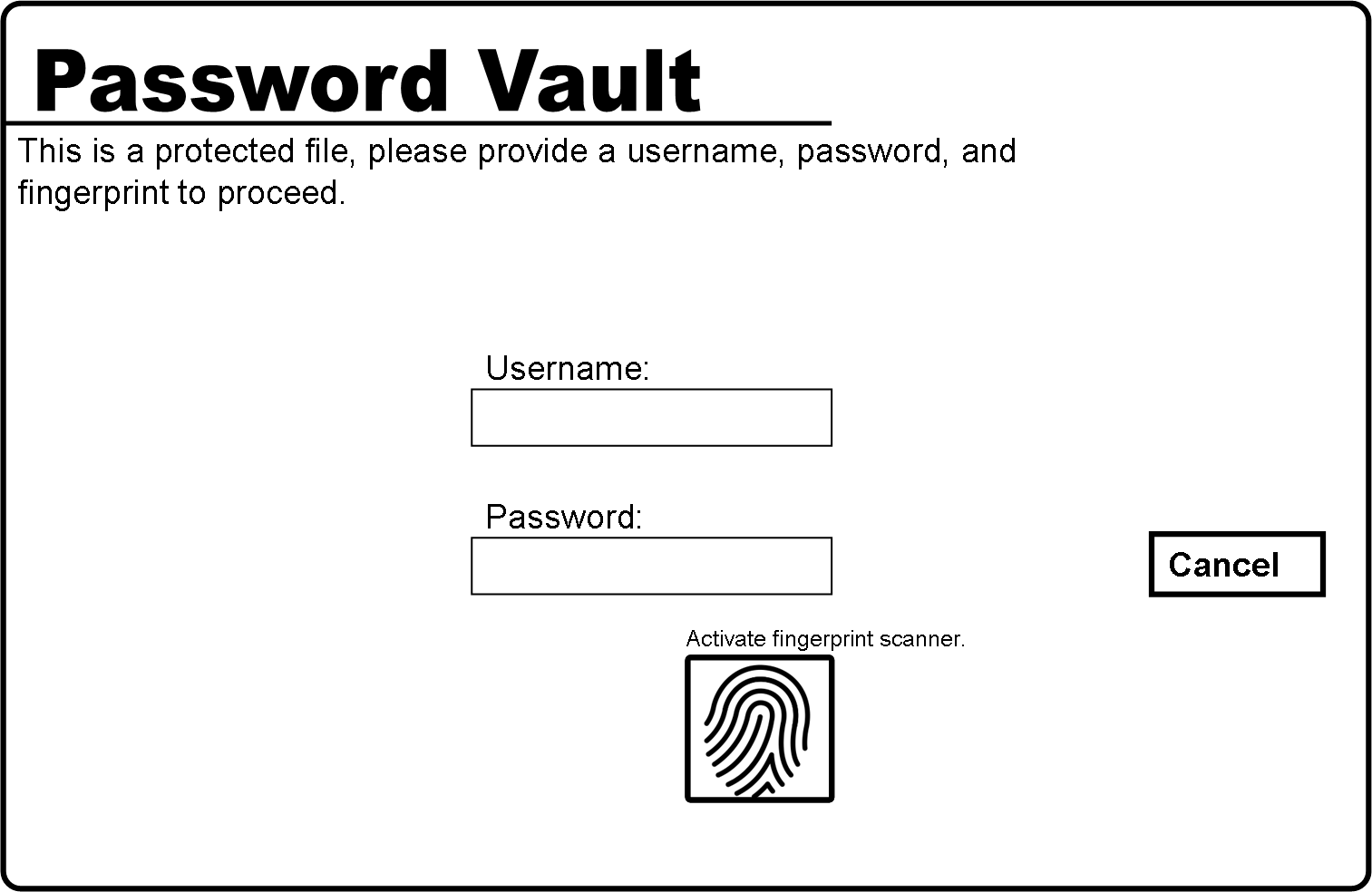
1c.

****

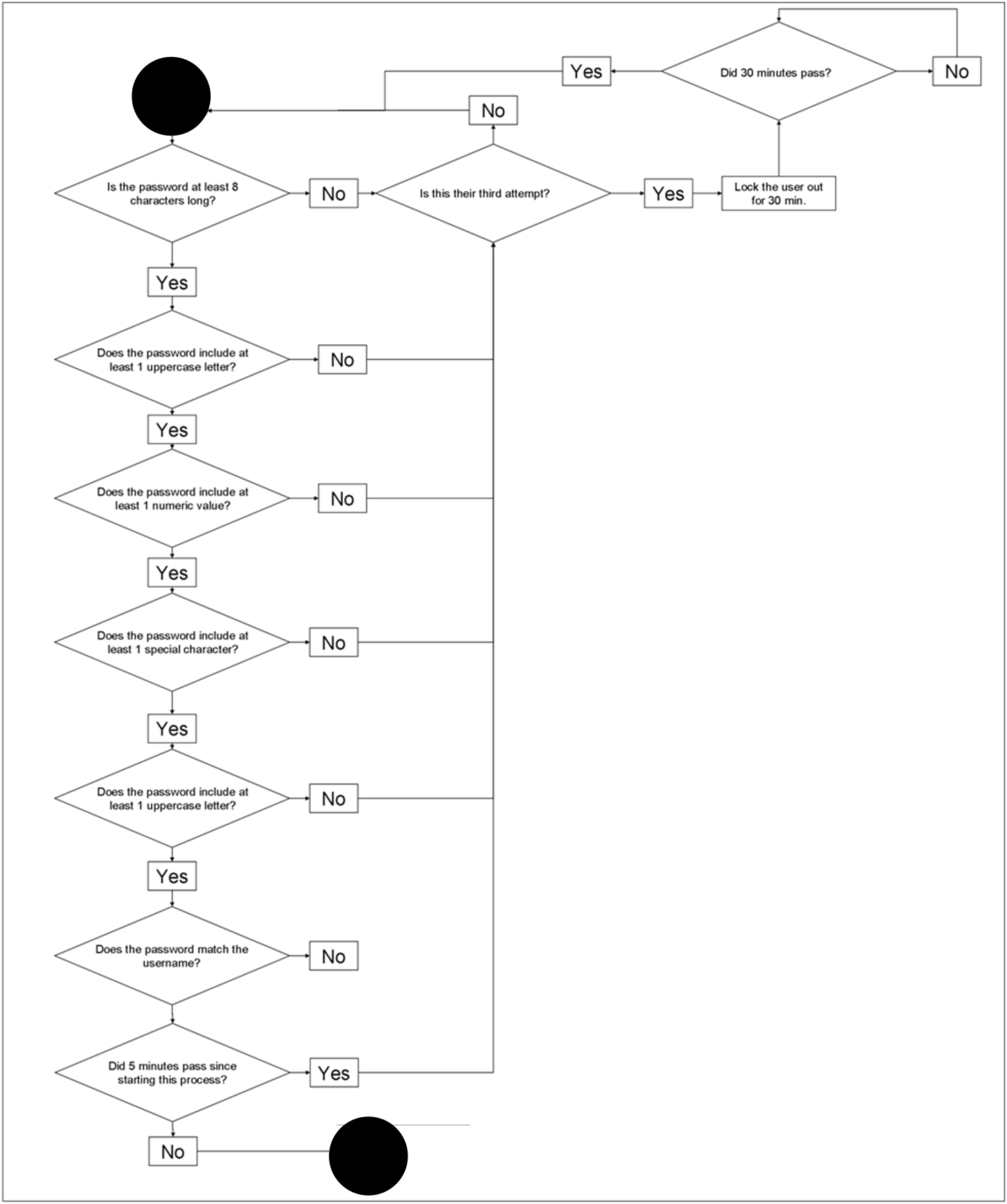
2a. For a two factor security, accessing and viewing a list of passwords, or in other words, accessing and editing a password vault would be worthy of such a system. For this system, having a means of providing a finger print of the user, as well as having a master password would prove to be secure enough for such a feature. This demonstrates a security setup that includes something that the user has set up in the past, and something that is a part of you.

* Does the Password match the one associated with the username?
* Does the Password include at least 8 characters?
* Does the password include at least 1 numeric value?
* Does the password include at least 1 special character?
* Does the fingerprint match the one associated with the username?
* Did the user complete all of this within 3 minutes?
* Did the user complete this within 3 attempts?

2b.



2c.



3a.Due to the sheer amount of information needed, the best aspect of the operating system that would use this would be remote access. The logic behind this is that you would have unlimited access to someone else’s computer as if they were logged in to the physical machine as oppose to accessing it over an undetermined distance.  
For this level of security, the second computer that is going to give the first computer access will have to provide a security code that will only be valid for a short period of time, that user would have to provide their login information, as well as provide a piece of evidence that they are who they say they are. For the sake of argument, this last piece of evidence will once again be a fingerprint.

3b.

* Did the first computer enter the “Remote access mode?”
* Did the first computer generate a new security code?
* Does the user’s password match the one that is used by the second user’s account?
* Does that password include at least 8 characters?
* Does the password include at least 1 numeric value?
* Does the password include at least 1 special character?
* Did the timer of 15 minutes for the code’s activation expire?
* Did the user do this within 3 attempts?
* Does the fingerprint match the one associated with the user?

3c.



3c.



3d.

