Student:	Email:
Jacob Jeffers	jjeffers6151@ucumberlands.edu

Time on Task:	Progress:
	100%

Report Generated: Friday, May 14, 2021 at 5:38 PM

Guided Exercises

Part 1: Research Digital Identity Guidance

3. **Summarize** the process for establishing digital identity, shown in the figure below.

The left side of Figure 4-1 shows the enrollment portion of an authentication process. An applicant applies to become a subscriber. If the CSP approves this, then the applicant will indeed become a subscriber. Authenticators and credentials are established between the CSP and the subscriber. Finally, the CSP verifies and maintains the credentials while the subscriber maintains his/her authenticator. The right side of Figure 4-1 shows the processes an authenticator must take to become digitally authenticated. The claimant proves authentication through some sort of protocol with the verifier. The verifier communicates with the CSP to validate the credentials provided. Either the CSP or verifier communication with the RP to make an authentication assertion about the subscriber. If approved, the authentication is verified and a connection is established.

5. **Summarize** the requirements suggested by NIST for password-based authentication where the user is allowed to select his or her own passwords.

The NIST requires that there be an 8 character password minimum and should skip password-hints and knowledge-based security questions. In addition, NIST requires that passwords only be changed if a password is compromised. New passwords should be compared to a list of known compromised passwords.

Part 2: Design an Access Control System

1. All of your systems rely on passwords for one of their authentication factors. **Write** a password policy for the organization that is consistent with the best practices outlined in NIST 800-63b.

The password policy at ACME Corp would be involved around the NIST best practices. The passcode policy will contain the following rules: password length between 8 and 64 characters, password complexity not required but allowed, password must not be a common word, as found in a typical wordlist or dictionary, password must be checked against a database of breached passwords, password rotation not enforced, and password attempts will be limited to five.

2. Your website permits different levels of access for the general public and for authenticated users. **Describe** the authentication process for customers accessing restricted areas of the website. **Identify** each authentication factor being used by type. **Answer** whether the approach qualifies as multifactor authentication.

User authentication to restricted areas of the website will be completed using a multi-factored approach. Input validation will be implemented into the text fields to prevent XSS attacks. After entering their credentials, users will use an authenticator app that will provide a six-digit pin that should be entered into another authentication screen.

3. The human resources system requires stricter access controls than the website. **Describe** an authentication process for managers and HR staff accessing this system. **Identify** each authentication factor being used by type. **Answer** whether the approach qualifies as multifactor authentication.

For human resources personnel, the authentication process will still be a multi-factored approach and will still be able to access the restricted site. Once in that site, there will be a box that says "For HR Personnel Only". This is where they access the things they need. Each HR personnel will have an office that locks and will be provided an access card and a card reader that is connected by USB to the computer in their office. This card reader is not authorized to be removed from and will alert management immediately if the device is unplugged. The access card is the third factor for HR personnel to gain access into the system.

4. The manufacturing system also requires stricter access controls than the website, but the authentication system used must be broadly accessible to all users in the company. **Describe** an authentication process for employees accessing this system. **Identify** each authentication factor being used by type. **Answer** whether the approach qualifies as multifactor authentication.

The manufacturing system will require authentication to the regular website like the previous but the log in to their system will require an additional password.

Challenge Exercise

1. Which authentication technique(s) are used by this system?

I work at a high school. To gain access to the doors, we are provided an access card with credentials linked to an ACL. I am permitted entry into one door, and it logs when I enter and exit the building. Once inside the classroom, my log in to school resources requires me to enter a username and password.

2. For each technique used, what is the category of the authentication factor?

I feel this would be multi-factored authentication. I am required to enter the school with an access card (something you have) and to sign in with a username and password (something you know) to access network resources.

3. Does this system qualify as multifactor authentication?

I believe it does.

4. If the system does not qualify as multifactor authentication, how could you modify it to qualify?

If the system did not qualify as multifactor authentication, I would an authenticator app to be used after users enter their username and password into the computer.