Blake McFarlane
Homework 1

1.

I. **Definition of User Abandonment**

User abandonment refers to the situation where a device remains unlocked while its owner is not present, thus posing a risk of unauthorized access. This vulnerability can lead to potential data breaches or unauthorized use of sensitive information (Neal & Woodard, 2016).

II. **Policy Guidelines**

To address the risks associated with user abandonment, the following policy guidelines are proposed:

1. **Automatic Lock**: Devices must automatically lock after a period of 30 seconds to 1 minute of inactivity. This measure helps prevent unauthorized access when the device is left unattended.
2. **Biometric Authentication**: Access to the device should require biometric authentication, such as fingerprint recognition or facial recognition. This adds an additional layer of security by ensuring that only authorized users can unlock the device.
3. **Employee Training**: Regular training sessions will be conducted to raise awareness about the risks of user abandonment and to promote secure device usage practices. This will help employees understand the importance of locking their devices when not in use and adhering to security protocols.

III**.** **Advantages and Limitations**

Advantages:

- **Enhanced Data Security**: Implementing automatic locking and biometric authentication strengthens data security by significantly reducing the risk of unauthorized access.
- **Increased Usability**: By reducing the need for manual password entries and ensuring devices lock automatically, the policy makes it easier for employees to maintain secure practices without sacrificing convenience.

. **Limitations**:

- **Potential Inconvenience**: Frequent automatic locking may cause inconvenience to users, particularly if they are interrupted frequently. This could lead to frustration if the lock time is too short.
- **Resource-Intensive Compliance**: Ensuring that all employees consistently comply with the policy may require substantial resources and ongoing monitoring, which could be resource-intensive for the organization.

IV**.** **Supporting Evidence**

Clarke and Furnell (2016) suggest that an effective mobile authentication system should enhance security beyond initial entry points and provide continuous, transparent authentication across various platforms. While physiological biometrics enhance initial security, they often lack continuous authentication and may require specific hardware. Behavioral biometrics, on the other hand, are better suited for continuous protection and mitigating user abandonment scenarios. Research shows that behavioral biometrics reduce the need for repeated authentication by 67% compared to knowledge-based methods and significantly limit unauthorized access attempts. This evidence supports the use of biometric measures and regular training to improve security and usability.

V. **Conclusion**

This policy aims to address the risks associated with user abandonment by implementing automatic locking and requiring biometric authentication. It strengthens security while striving to maintain usability. The policy is designed to mitigate potential security risks and improve overall device protection by incorporating best practices from recent research on biometric authentication and user security.

2. Classifications of fingerprint recognition technology

- **Cooperative System**: Fingerprint recognition on laptops is designed for cooperative users, as the laptop owner willingly engages with the biometric process to access their system.
- **Overt System**: It is an overt system, with users fully aware of the fingerprint scanning process, often prompted by the laptop to place their finger on the sensor.
- **Closed System**: The biometric data is stored locally on the laptop and used solely for specific functions, like logging in, without being shared across different applications or platforms.
- **Habituated Users:** Regular users become familiar with the fingerprint recognition process, improving the quality of their biometric input over time.
- **Unattended System:** The fingerprint capture operates without human supervision, requiring no assistance during the process.
- **Controlled Environment:** The system functions in a stable environment, typically indoors, where factors like lighting and temperature remain consistent and do not interfere with recognition accuracy.

3. Continuous Authentication in my own words

Continuous authentication, as defined by Patel et al. (2016), refers to the process of constantly verifying the identity of a user on a mobile device after the initial login. Unlike traditional authentication methods, which require a one-time login, continuous authentication continuously monitors user behavior (such as touch patterns, gait, or location) to ensure that the individual using the device is the legitimate owner. This approach enhances security by detecting unauthorized access in real-time, even after the device has been unlocked.

---

4. Which authentication method provides the best optimal balance between security and usability

Based on the three authentication methods that we went over in lecture 2; Knowledge-based, Token-based, and Biometric-based, I would have to say that I believe biometric based authentication provides the best balance between security and usability for its users. Below I have provided two examples for each Biometric-based feature.

I. **Security:**
   - **Unique Characteristics**: Biometric features like fingerprints and facial patterns are difficult to replicate or steal, offering a higher level of security than passwords or PINs (Muñoz, 2023).
   - **Spoof Detection:** Advanced biometric systems use technologies such as Dynamic Liveness to detect and prevent spoofing attempts, ensuring that authentication is both secure and genuine.

II. **Usability**:
   - **Seamless Experience**: Biometric authentication is intuitive and effortless, requiring only a simple action like looking at a camera or scanning a fingerprint, which enhances user satisfaction.
   - **No Need to Remember**: Users do not need to remember or manage passwords, reducing the chances of errors and making the authentication process more convenient and accessible.

---

5. Optimizing Mobile Biometric Systems: Design and Feasibility

Based on common constraints in mobile biometric systems, the feature that may often be infeasible is **"Multimodal and attended"**. This is because the requirement to be both multimodal and attended can be challenging in a mobile context where user convenience and efficiency are prioritized.

(a) System Design

Feasible Features:

1. **Multimodal System**: The system can utilize two distinct biometric modalities such as fingerprint recognition and facial recognition. These modalities complement each other in terms of security and user experience. For example:

    - **Fingerprint Recognition**: Utilizes the fingerprint sensor available on most mobile devices.
    - **Facial Recognition**: Uses the device's front camera to capture and authenticate facial features.
2. **Multi-Factor Authentication (MFA)**: Incorporates additional authentication factors to enhance security. For instance:
    - **Biometric Factor**: Use of fingerprint or facial recognition.
    - **Knowledge Factor**: Require a secure PIN or password in addition to biometric verification.

System Overview:

- **User Enrollment**: Users register their fingerprint and facial data during the initial setup. They also set up a secure PIN/password.
- **Authentication Flow**: During login, users first authenticate using biometric factors (fingerprint or facial recognition). If biometrics fail or are not recognized, the system prompts for the PIN/password.
- **Security Layers**: The system locks the account after a set number of failed authentication attempts and alerts the user of potential security breaches.

(b) Addressing the Seven Biometric Properties

1. **Universality**: The system will support users who have fingerprints and facial features. However, users with certain medical conditions that affect fingerprints or facial features may encounter difficulties.
2. **Uniqueness**: Both fingerprint and facial features are unique to each individual, providing strong uniqueness characteristics.
3. **Permanence**: Fingerprints and facial features are relatively stable over time, though facial features can change slightly due to aging or other factors.
4. **Collectability**: Modern mobile devices are equipped with fingerprint sensors and high-resolution cameras that can capture biometric data effectively.
5. **Performance**:
    - **Accuracy**: Fingerprint and facial recognition technologies are mature and can achieve high accuracy with well-maintained devices.
    - **Speed**: Both modalities offer quick authentication processes, enhancing user experience.
6. **Acceptability**: Users are generally familiar with fingerprint and facial recognition, making them acceptable biometric modalities for most individuals.
7. **Circumvention**: While biometric systems can be robust, advanced spoofing techniques might pose risks. Combining fingerprint and facial recognition with MFA helps mitigate these risks.

(c) Challenges

1. **Multimodal and Attended Constraints**:

    - **Device Limitations**: Some mobile devices may not support certain biometric modalities or have limited integration capabilities for multiple modalities.
    - **User Experience**: Maintaining a system that requires active user attention while ensuring seamless operation may be challenging.
2. **Integration Complexity**: Combining multiple biometric modalities with MFA requires careful system design and integration, which can be resource-intensive.

(d) Alternative Solutions

1. **Single Biometric Modality with MFA**:
    - **Simplified System**: Utilize one reliable biometric modality, such as fingerprint recognition, combined with MFA that includes a secure PIN or password. This approach simplifies the system while still providing enhanced security.
2. **User Education and Training**:
    - **Awareness**: Educate users on secure practices, including the importance of strong PINs and safe handling of biometric data to complement the single modality system.
3. **Advanced Biometrics**:
    - **Hybrid Solutions**: Explore emerging technologies like behavioral biometrics (e.g., typing patterns, device usage) in addition to existing modalities to enhance security without additional hardware requirements.

Sources

Neal, T. J., and Woodard, D. L. (2016). Surveying biometric authentication for mobile device security. Journal of Pattern Recognition Research, 1(74-110), 4

Jain, A. K., Ross, A. A., Nandakumar, K. (2011). Introduction. In: Introduction to Biometrics. Springer, Boston, MA

Patel, V. M., Chellappa, R., Chandra, D., and Barbello, B. (2016). Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4), 49-61

Muñoz, J. (2023, October 4). Biometric authentication vs. traditional methods: Pros and cons. Alice Biometrics. https://alicebiometrics.com/en/biometric-authentication-vs-traditional-methods-pros-and-cons/