David Hatcher
CAP4301

Guided Learning #1

1. According to a recent study done by Shred-it, more than 40% of data breaches can be attributed to human error or accidental loss of company devices. With many employees working remotely because of the current pandemic the need for employee diligence is at an all time high. One of the easiest ways to prevent a data breach is to focus on training for user abandonment. User abandonment is when a user leaves their device unattended for some time. By doing this the user allows the risk that the device could be stolen or have some malicious software installed on it. My suggestion to remediate this issue would be to implement continuous facial recognition on any devices that are used remotely. One of the biggest advantages to using this type of security feature is that it is completely passive. This would mean that the users would not have to actively take any steps to ensuring their devices were secure even if left unattended. Another advantage of this system would mean that anyone who is not authorized to use a specific device would not be able to access it even if left unlocked. However, this system does come with some disadvantages as well. The biggest would be acceptability, as many of these systems use machine learning to make facial matches so it may take a little time before it can accurately determine who is using the device and may cause some frustrations to the users. Another disadvantage is that it will lower the performance of the device as it will need to continuously authenticate the users during normal operation.
2. The claims being made is that Apple's touch ID is habituated, overt, and attended. These first of these are true as most users of Apple's touch ID have used it quite a bit and are used to it. The second is that it is overt. This is also true as the phone will actually inform you to place your finger on the home key in order to unlock the phone. However, the last claim, that it is attended, is incorrect, as for a biometric method to be considered attended it would require someone to guide the user through the process and this is not done with Apple's Touch ID. As such, this claim is false.
3. Continuous authentication is when some sort of authentication is done throughout the process of using a device and not just at the beginning of a single instance of use. An example of this would be if a user had to scan their iris every few minutes while using a device. Another example could be using a respiratory pattern for authentication that would constantly track and authenticate the users breathing patterns throughout the session.
4. In my opinion, the most secure method of the three types of authentication is Biometric. However, this would only apply if it was properly implemented and the systems storing the data were secure. If there were to be a breach of this data it would create a vulnerability in any other biometric authentication which was using the same modality. However, I feel that having two-factor authentication and using two different types of authentication, such as Biometric and Token-Based would be even more secure. As even if there were a biometric data breach, a token would still be needed to gain access to whatever system the leaked template data was used in.

5. For a multimodal attended system with at least two different classes of mobile sensing and multi-factor authentication I would implement the system in the following way. The first modal of biometrics authentication I would use is a fingerprint scanner. The second modal would be a face scan. In order to achieve multi-factor authentication the system could also require some sort of token-based authentication as well. In the form of either a physical token issued to each user, or a digital one on a mobile device. I would argue that the client's request for attended authentication would be impractical as this is a mobile biometric system and having an attendant to supervise the data collection would require anyone who wishes to authenticate themselves to go somewhere that a human would observe them during the data collection. If this is acceptable then it could be done by having someone supervise the facial and fingerprint scanning. If not they could possibly add some sort of knowledge-based authentication to increase the security of that application or whatever they're trying to secure. This system would achieve the Seven Biometric Properties in the following manner:
    a. Universality
        i. As everybody has a face and, hopefully, at least one finger, anyone should be able to use this system.
    b. Uniqueness
        i. Facial scanning and fingerprint scanning alone aren't always secure, as people with close familial ties are often able to unlock devices secured by facial recognition. However, with both of these used in conjunction it would be extremely unlikely that anyone would be able to fool the system without having template data.
    c. Permanence
        i. As fingerprints and facial features can change over time such as fingerprint ridges wearing out or weight gain causing facial features to change, this system would need to continuously add new template data throughout its lifecycle.
    d. Measurability
        i. There are plenty of devices that can be used for both of these biometric modalities. These biometric scanners are also included on many devices today as well.
    e. Performance
        i. As many devices today use these systems to authenticate their users the performance has been shown to be acceptable.
    f. Acceptability
        i. As facial recognition as well as fingerprint authentication are highly acceptable and most people are used to using it to access their devices, this system should have no acceptability issues.
    g. Circumvention
        i. While facial recognition and fingerprint scanning can be circumvented using different tactics, the two-factor authentication of using a token-based authenticator using a one-time pad system is highly secure and extremely difficult to circumvent.

References:

Shred-it: State of the Industry Information Security 2018

https://www.shredit.com/getmedia/b5de58fd-7e17-4d18-b718-9eca8d0665a6/Shred-it-2018-North-America-State-of-the-Industry.aspx?ext=.pdf

Fully Automatic Facial Action Recognition in Spontaneous Behavior
Marian Stewart Bartlett, et al
https://d1wqtxts1xzle7.cloudfront.net/42872290/Fully_Automatic_Facial_Action_Recognitio20160220-2304-ie6zg.pdf?1455982590=&response-content-disposition=inline%3B+filename%3DFully_Automatic_Facial_Action_Recognitio.pdf&Expires=1631225746&Signature=Di46XbKGQmZrzdNiyP~gmaIw~AwesPNDEl~QhfHmR38M7-fWzx8X0v5S42-UXEbJjBYZL-b4rcc9UB0nTjl0s0k4XDzlVKANhgw9haBFugBBpM8WeJr1HUX6~oYH-Tz2UH1RKaeadCFenrDB3hxL3oDg8x1xrArfS8L2C5RlhdfwQWYC6SE6320zDw0e1Xu9x-anrz1KBuzNWtVHsKnsRu9YZn3NDcxeVAIvZc5LTCTGFd69IHSkOgXxUiCKF9j6PqABCHo98djt6fHiJYSlAR-6JhWn8lipVG0CdONKzgjK6znMmOC3vB4PeEYQwFOkUFyXjs9hyVTi3H21oTE4rA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA