Isadora Oliveira Grasel

Dr. Tempestt Neal

Mobile Biometrics

September 13, 2024

Homework 1 - Fall 2024

QUESTION 1 - DRAFT POLICY ON USER ABANDONMENT

According to Neal and Woodward (2016), user abandonment occurs when a device remains unlocked without its owner present. It is undoubtful that user abandonment presents a significant threat to company and customer security. Therefore, it is essential to address this issue and develop strong policies to ensure the safety of our data and technology.

Currently, the company does not cover this vital topic through any guidelines in the Employee Handbook. User abandonment leaves the company, the customers, and the employees open to a wide range of threats and liabilities, confidential information can be leaked, passwords can be used for impersonation, and so on. In fact, just this week one of the biggest cybersecurity companies in the market, Fortinet, suffered an attack that caused a customer data breach, affecting around 6 million customers and leading the company's shares to drop over 4% on Nasdaq, according to Capital Brief this Friday, September 13.

The simplest and most effective way to avoid these risks is never to abandon unlocked devices and always to stay vigilant. This can be done by lowering the time a device remains unlocked when inactive, adding biometric authentication to enter applications that contain confidential

data, and especially creating the habit of locking devices before leaving them behind. By doing that, the consequences of user abandonment are highly minimized.

Even though these actions are capable of effectively protecting from most user abandonment cases, many other vulnerabilities can be explored by cyber attackers. Therefore, it is essential to always follow the standard security and confidentiality guidelines to ensure safety for the company, customers, and employees.

QUESTION 2 - CLASSIFICATION OF BIOMETRIC SYSTEMS

The book Introduction to Biometrics, by Jain, Ross, and Nandakumar (2011), describes the multiple possible classifications for a biometric system. Users can take a cooperative or non-cooperative approach when interacting with the system, which is usually directly related to the interests and intentions of each user. In addition, a system can be overt, where the user is aware of the biometric scan, or covert when the user is unaware of such surveillance. While most biometric systems are overt by nature, covert systems are widely used by law enforcement. A system with habituated users involves frequent interaction, a very important factor when designing a biometric system because non-habituated users tend to not know how to provide accurate biometric data. If the data enrollment process for a biometric system is observed, guided, or checked by a human the biometric system is called attended. Most mobile biometric systems are fully unattended, as they do not have human supervision during enrollment or recognition, providing a faster and smoother experience for the user, but possibly less security. Biometric systems can be designed to operate within an uncontrolled or controlled environment, where conditions can be monitored and altered to help in collecting accurate biometric data. If a user's biometric data is used across multiple applications through a shared database, the system

will be considered open. Most mobile biometric systems are closed to ensure the security of a user's digital identity.

In the context of fingerprint recognition for laptops, the biometric system will be cooperative, overt, unattended, uncontrolled, closed, and it will have habituated users. Someone who owns a laptop will want to unlock and use it normally, being cooperative with the system to unlock it, and also being aware of what they have to do to unlock it, showcasing a cooperative and overt system. Fingerprint recognition in mobile devices, including laptops, has been popular for a few years now, so it is safe to assume that almost all users had some contact with this type of technology, making it a habituated system (except maybe during the enrollment process). The user's biometric enrollment and authentication are unattended and both are done in an uncontrolled environment (especially because a laptop is portable and can be used outdoors). The unattended factor is key to ensure smooth user experience and interaction. And, finally, most mobile biometric systems are closed, only allowing third-party apps to check if the user passed the biometric test made by the device's system, which is set in place to prevent someone's biometric data from being leaked and possibly used for digital impersonation.

QUESTION 3 - CONTINUOUS AUTHENTICATION

Continuous Authentication refers to authentication methods running in the background even after a user unlocked their device and it is generally used for increased security in cases when suspicious activity is detected. After a device is unlocked, more biometric data input is collected, such as face, keystroke, gait, voice, and others, (Dahia et al, 2020), and used to verify if the current user is still the same as the one during the initial authentication and not an impostor.

QUESTION 4 - SECURITY X USABILITY

Biometric systems have, by definition, very specific goals. And the most complex challenge for them is to balance usability and security in the best way possible. I believe that the biometric trait that performs best in both security and usability is fingerprint recognition. Most systems that leverage this biometric trait are cooperative, unattended, uncontrolled, overt, habituated, and closed. Fingerprint recognition in mobile devices has been popular for a few years now, so a greater number of users had some contact with this type of technology, making it most likely to be a habituated system, which entitles users to be able to provide biometric data of higher quality. In addition, due to it being a popularly and commonly used biometric trait, fingerprint sensors are also available in the market in larger numbers at a smaller price. Above all, fingerprints are easy to measure, do not change easily, and are highly unique. The closest competitor to fingerprint recognition would probably be facial recognition, however, the latter tends to produce more false negatives (which harms user interaction), as published by Samsung: "What’s more, facial recognition can be prone to false negatives, caused by glasses, makeup or just different ambient lighting. For stronger security, organizations handling sensitive data should consider fingerprint scanning."

QUESTION 5 - MOBILE BIOMETRIC SYSTEM

"Biometrics is the utilization of unique biological traits for identification. These are unique identifiers far more reliable than a password or pin, be it fingerprints, voice recognition, or iris scans. With increasing digital transactions, including high-value trades and transfers, the need for impenetrable security is at its zenith. That's where biometrics steps in." (Forbes Finance Council, 2024).

System Design. The baking app's system would be unlocked with either face or fingerprint recognition, depending on the sensor availability of the user's mobile device. If the system is unable to confirm a user's identity through their biometrics twice, the user will be prompted to enter a password. The multi-factor authentication process would then have to be completed with a token-based authentication, using either an enrolled authenticator app or a one-time PIN sent to the user through SMS. After that, as the user navigates the banking app, more behavioral biometric data will be collected and then used to determine if any activity could be fraudulent. On top of that, different user settings could be leveraged by each client to block some actions within the app while in non-trusted locations, like Modo Rua (in English, "Street Mode") developed by Nubank, the largest neobank in Latin America.

Biometric Properties. This system would be classified as cooperative, unattended (except during user enrollment), uncontrolled, overt, habituated, and closed. The user is aware that his biometric data is being collected and checked, and wants to collaborate to be able to enjoy all the banking app's features, making the application over, habituated, and overt. One of the most important goals of a mobile banking solution is to provide the users with freedom to control their finances from anywhere at any time, which means the system is uncontrolled and unattended (mostly). To prevent any violation of user privacy and biometric data breaches, the system would be closed, not sharing any biometric data with other applications.

Challenges. Building a mobile biometric system that is multimodal and attended, especially in the context of a banking application would be significantly challenging. First, sensors are essential for capturing physical biometric data, and most phones currently offer either face or fingerprint recognition, but hardly ever both. However, to make the system multimodal,

behavioral biometrics could be used in place of an extra physical one, and leveraged for continuous user authentication. A great example of that in the context of a banking app would be geographical location, tracked by the device's GPS, and actions (making transactions, checking card statements, changing passwords, etc) within the app. Finally, an attended mobile system usually entitles remote supervision and a waiting period, possibly harming the user experience by losing the instant unlocking feature.

Alternative Solutions. To prevent the supervision of the biometric authentication from becoming a problem for seamless user experience, the systems could have an attended enrollment (where a bank employee would check and accept the user's biometric data during the first use of the banking app), but unattended verification after the initial enrollment process is completed and approved by the human supervisor.

Works Cited

America's Cyber Defense Agency. “Multi-Factor Authentication (MFA).” *Cybersecurity & Infrastructure Security Agency*, 2022, https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa. Accessed September 2024.

Dahia, Gabriel, et al. “Continuous authentication using biometrics: An advanced review.” *WIREs*, Wiley, 2020, https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1365. Accessed September 2024.

Forbes Finance Council. “Biometrics in Banking: The Future of Secure Transactions.” *Forbes Councils*, 24 May 2024, https://councils.forbes.com/blog/biometrics-in-banking. Accessed September 2024.

Jain, Anil K., et al. *Introduction to Biometrics*. Springer US, 2011. *SpringerLink*, https://link.springer.com/chapter/10.1007/978-0-387-77326-1_1. Accessed September 2024.

Khan, Hassan, et al. “Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying.” *Symposium On Usable Privacy and Security*, 2015. *Usenix*, https://www.usenix.org/conference/soups2015/proceedings/presentation/khan. Accessed September 2024.

Neal, Tempestt J., and Damon L. Woodard. “Surveying Biometric Authentication for Mobile Device Security.” *Journal of Pattern Recognition Research*, vol. 11, no. 1, 2016, pp.

74-110. *Journal of Pattern Recognition Research*, http://jprr.org/index.php/jprr/article/view/764. Accessed September 2024.

Nubank. "Nubank launches Modo Rua, an innovative safety feature that simplifies setting transaction limits - Nu International." *About Nu*, 13 October 2022, https://international.nubank.com.br/consumers/nubank-launches-modo-rua-an-innovative-safety-feature-that-simplifies-setting-transaction-limits/. Accessed September 2024.

Patel, Vishal M., et al. "Continuous User Authentication on Mobile Devices: Recent Progress and Remaining Challenges." *IEEE Signal Processing Magazine*, 2016. *Johns Hopkins Whiting School of Engineering*, https://engineering.jhu.edu/vpatel36/wp-content/uploads/2018/08/AA_SPM2015_v4.pdf. Accessed September 2024.

Samsung Business. "Which smartphone biometric authentication method is most secure?" *Samsung Insights*, 25 May 2021, https://insights.samsung.com/2021/05/25/which-biometric-authentication-method-is-most-secure-3/. Accessed September 2024.

Van Boom, Daniel, and Anthony Galloway. "Fortinet fallout." *Capital Brief*, 13 September 2024, https://www.capitalbrief.com/newsletter/fortinet-fallout-e0b496f7-d650-4cb0-abd3-893c312caa39/preview/. Accessed September 2024.