Sakura Hewa Dewundarage

Taken At Face Value

How Apple's integration of biometrics revolutionised phone authentication

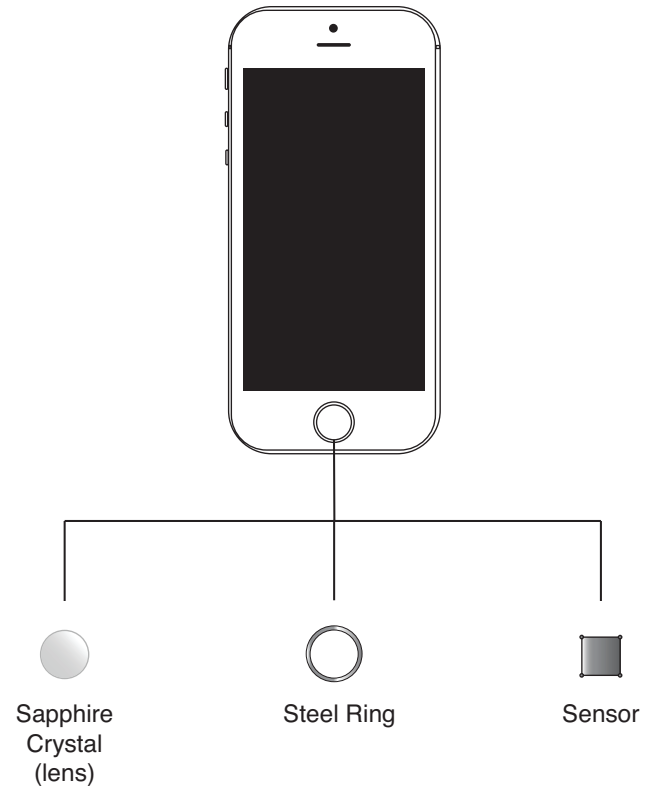
Taken at Face Value

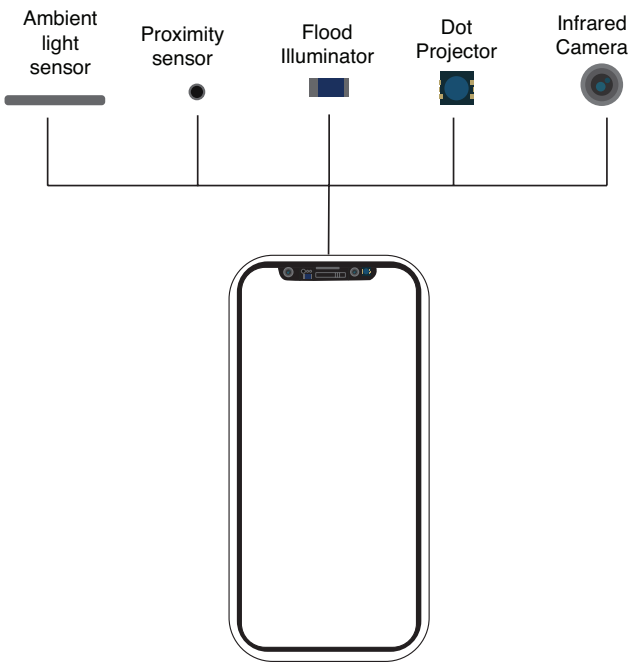
Sakura Hewa Dewundarage

Apple is constantly at the forefront of technological development, bringing new and exciting innovations like biometric technology to the table. Biometrics involves the measuring of human features and characteristics that can be used for authenticating the identity of individuals. These authentication systems are able to read characteristics such as an individual's fingerprint, facial features, iris or voice to enable access to certain things, with the most popular being fingerprint and facial authentication. Apple introduced biometrics in 2013 after they bought AuthenTec's Touch ID technology. They then followed this by introducing Face ID in 2017 making Touch ID pretty much redundant.

So how does any of it work? Apple's Touch ID system uses the home button to start the authentication process. The button is made of sapphire crystal which protects the fingerprint sensor from damage whilst simultaneously acting as lens to get a more accurate reading of the fingerprint. The steel ring around the home button detects the finger and enables the sensor to begin reading the fingerprint using capacitive technology which captures a high res image of parts of the fingerprint and categorises the fingerprint as either a whorl, arch or loop. Using this information it produces the mathematical equivalent of the fingerprint and compares it to the original to unlock the device.

The iphone uses a TrueDepth camera to enable Face ID to work. The camera includes an ambient light and proximity sensor that decides how much light on the face is needed for the flood illuminator to work, which depends on the person's location and their light settings. The flood illuminator then creates an invisible infrared light that lights up the face for the dot projector to then project around 30,000 infrared dots to obtain a 3D depth map of the face which the infrared camera records an image of. The chips, part of the neural engine (the iphones processor) then turn both the depth map and infrared image into the mathematical equivalent of the 3D model, to compare to the data of the original image in the Secure Enclave. Due to the new 'verification' image not being an exact replica of the original, the phones utilise a threshold to determine similarity, with a scale from 0 to 1, where images closer to 1 (from 0.5 onwards) are accepted for unlocking the device.





Despite the accuracy and precision of Apple's Touch ID, an issue of spoofing arose with hackers using high resolution images of people's fingerprints to reproduce a replica to bypass the iphone's fingerprint sensor. One way they achieved this was by obtaining the fingerprint from residue left on glass which they then used to laser print onto a transparent film etching it onto a latex material that could pass as a fingerprint. However this method requires a lot of advanced and complex materials and technologies, making it unlikely to occur. Apple also uses Secure Enclave to store and encrypt the mathematical data of the fingerprint instead of images to ensure that hackers don't have access to photos of the fingerprint to duplicate.

Spoofing within facial recognition technology has also occurred with hackers using video replays, printed photos and 3D masks to pass off as a face. However this issue is being combated with the biometric technology able to detect aliasing in video replays to distinguish them from an actual face in addition to their anti spoofing neural networks that prevent spoofing from masks. Apple's facial recognition technology also ensures that 2D printed photos of faces and masks are not accepted as it uses the depth of the face to authenticate the user. An added security feature is Face ID's ability to detect if the user's eyes are open and if they're focused on the phone to prevent people from unlocking phones when the user is asleep.

The biometric technology within the iPhones is not limited to simply authenticating access to the device, in fact it is used for several other purposes. One example of this is the use of both Touch ID and Face ID to facilitate online payments. The same process for unlocking the device occurs when users wish to use their fingerprint or face as Apple ID to authenticate purchases from the App Store, iTunes and iBooks enabled via Apple Pay. However the threshold for facial authentication is higher for increased security, with the similarity needing to be closer to 1 (eg. 0.9).

References:

Apple (2021, September 16). *About Face ID advanced technology*. Retrieved from https://support.apple.com/en-au/HT208108

Apple (2017, September 11). *About Touch ID advanced security technology*. Retrieved from https://support.apple.com/en-us/HT204587

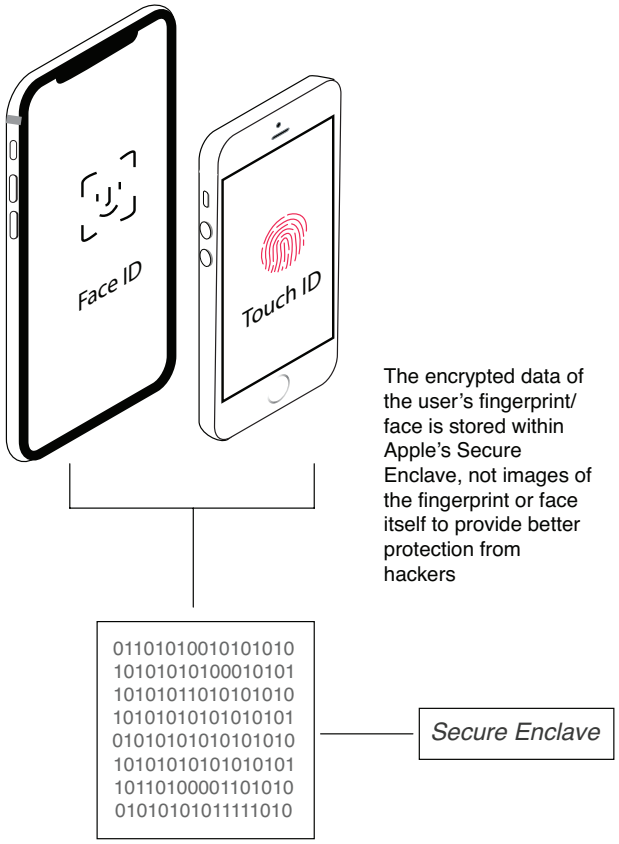
Tillman, M. (2021, September 3). *What is Apple Face ID and how does it work*? Pocket-lint. Retrieved from https://www.pocket-lint.com/phones/news/apple/142207-what-is-apple-face-id-and-how-does-it-work

Goode, A. (2014). Bring your own finger–how mobile is bringing biometrics to consumers. *Biometric Technology Today, 2014*(5), 5-9. https://doi.org/10.1016/S0969-4765(14)70088-8

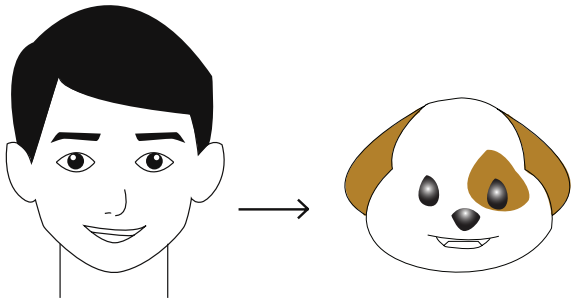
Goode, A. (2013). Mixed reception for iPhone 5S fingerprint recognition. *Biometric Technology Today, 2013*(9), 1-2. https://doi.org/10.1016/S0969-4765(14)70088-8

Face ID has introduced the addition of Animojis, which are 3D animated versions of emojis that are based on the user's current facial expression. It works by using the TrueDepth camera system to detect the user's muscle movement within their face to reflect their facial expression in the emojis. Similar to this is the Memoji also uses the TrueDepth Camera to monitor the movement of the user's facial expression, however this feature allows the emoji to look more the user, giving the user more control over how the avatar looks (changing hair, eye, skin colour).

In conclusion, although Apple may not have created biometric technology, they are responsible for revolutionising biometrics as they enhanced and expanded its capabilities within iPhones, creating a more accurate and secure system.



The encrypted data of the user's fingerprint/ face is stored within Apple's Secure Enclave, not images of the fingerprint or face itself to provide better protection from hackers



The user's facial expression is detected by the camera and represented through an emoji