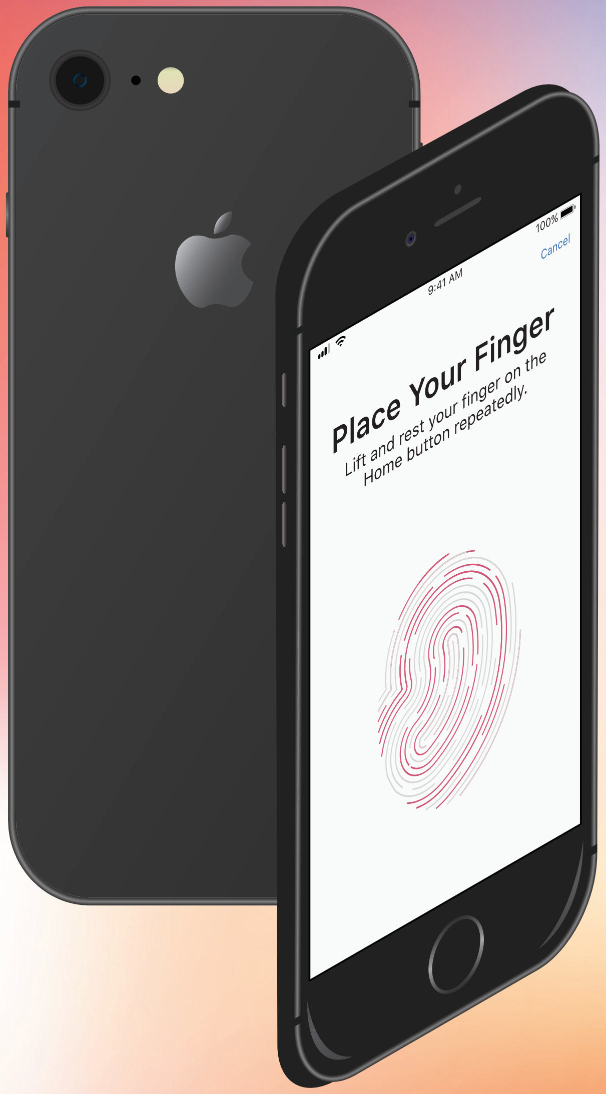
Elysia Noeng

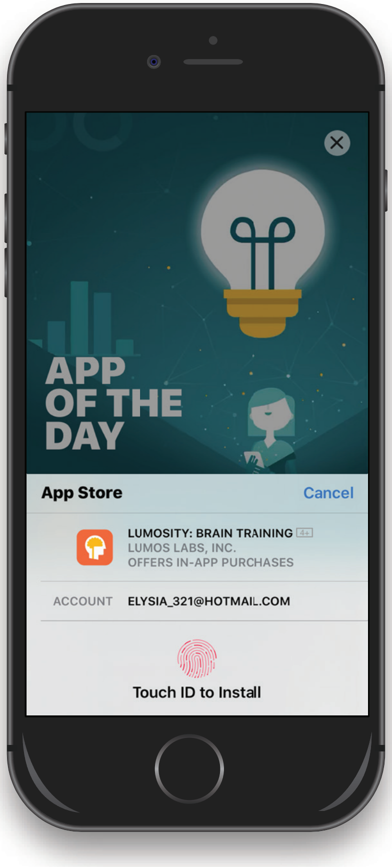
Recognise me?

Components, uses and security. How innovative is the Touch ID?



Recognise me?

Elysia Noeng



ACCOUNT ELYSIA_321@HOTMAIL.COM

Continuous improvements and advancements of Apple products allow customers to constantly contemplate what next innovative technology could arise. In September 2013, Apple first announced its initial release of the iPhone 5s. The phone has then featured many new characteristics including new display colours, a faster processor, higher camera quality, and most importantly, a Touch ID sensor. Ever since the success of the Touch ID, Apple had implemented this feature into all its phone up until the iPhone 8 plus. The Touch ID has been around for approximately four years since the introduction of the Face ID in 2017.

The Touch ID is an electronic fingerprint sensor embedded into the iPhone's home button. This feature is used for unlocking the iPhone, Apple Pay, iTunes and the App Store, and password auto fill.

It was primarily introduced for quick accessibility and purchases compared to the previous four-code or worded password. According to a survey conducted in 2015, participants said that they used the Touch ID for speed, convenience and ease when accessing their phones. Out of 173 candidates, more than 50% stated that the feature was more secure than the passcode. Its security is also prevalent for mobile payment and other transactions. Additionally, out of 41 participants, 26 found that the set up of Touch ID was easy or very easy to use, while 29 stated that it was easy or very easy to use.

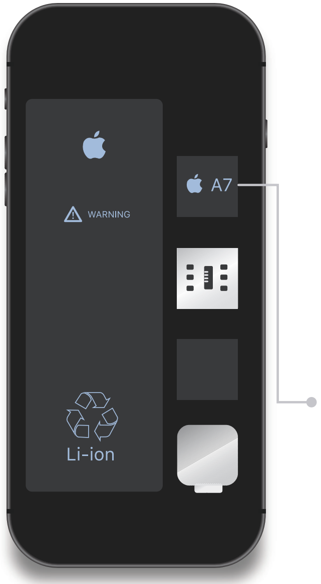
The Touch ID is made up of four components. The **laser cut sapphire crystal** is the outer most layer that is a scratch resistant glass lens that protects damages from occurring to the capacitive touch. A **stainless steel ring** that allows the phone to detect when a finger is present then surrounds it, allowing for an accurate reading of the fingerprint. Beneath this component is what allows the feature to work. The **capacitive touch** lets the phone recognise when a fingerprint is present, therefore activating the device and allowing an identification to be read. This layer is especially thin at only 170 microns, which is equivalent to 1/1 000 000th of a meter. Finally, a **tactile switch** is embedded, allowing the iPhone to process a sense of touch.

The Touch ID attribute also has a 360-degree readability, can scan sub epidermal skin layers (beneath the top skin layer) and has a sensor scan of 500ppi (pixels per inch). With a scan of such high resolution, the phone captures an image of the fingerprint and stores this representation into a **'Secure Enclave'**.

To ensure the device recognises the correct fingerprint, the identification is stored on the 'Security Enclave' within the phone's chip and not within any applications. This storage system is extremely secure and makes decryption almost impossible without proper authorisation. When accessing the device, the captured fingerprint data is compared to the one stored in the phone to determine a match. Once the mobile detects a match, authorisation is enabled. However if the identification is incorrect three times, a password/code is required.

The device also allows up to five different fingerprints to be stored on the device, as well as the ability to turn off passcodes completely. Flexibility in controlling how to access the iPhone is necessary for users who prefer convenience and quick accessibility into their devices. The iPhone also requests for the users passcode into managing the Touch ID feature, providing security into who can access the device.

It is evident here that this feature has had a significant impact in allowing users to quickly and securely activate their devices and make purchases through the process of biometric recognition. Apple's mission of creating innovative technology has then remained reliable through the introduction of the Touch ID.



The A7 is a chip in which the Secure Enclave is located, which stores all biometric data. It is used to secure sensitive data that cannot be contained within applications due to the possibility of being hacked. It also enables purchases or access to the device, dependent on whether the identification matches the one stored in the Secure Enclave.

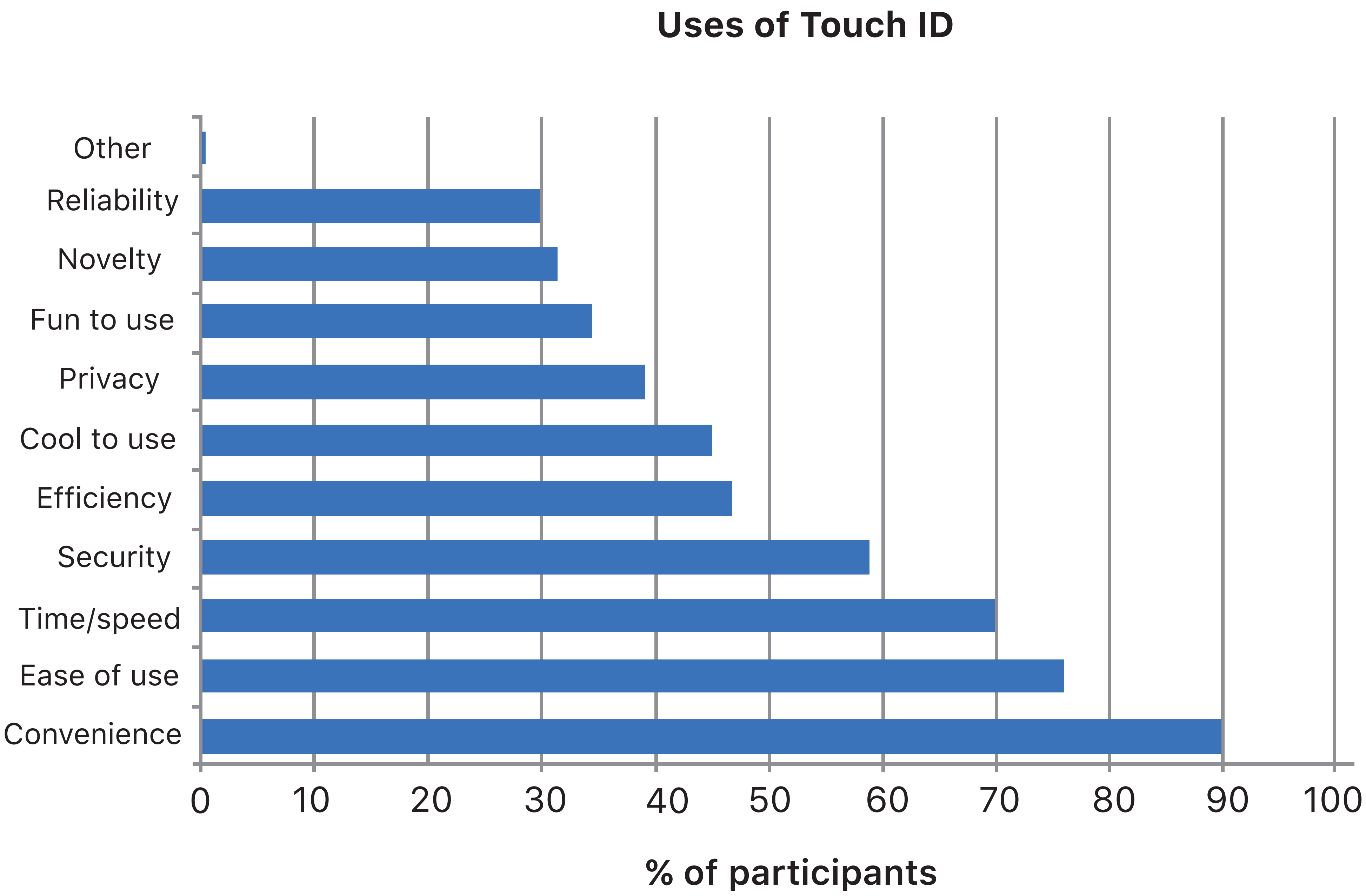
References:

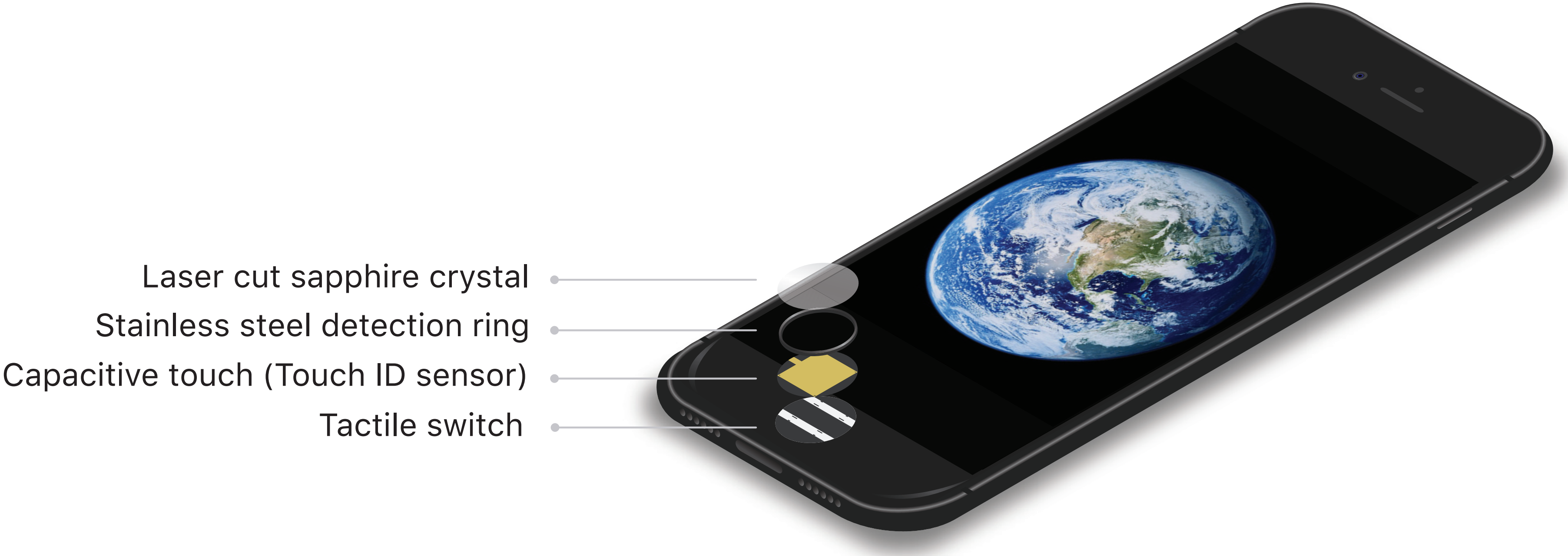
Javed, Y., & Shehab, M,. & Ogunu, E. (2016). Investigating User Comprehension and Risk Perception of Apple's Touch ID Technology. Retrieved from: https://liisp.uncc.edu/wp-content/uploads/2017/10/SIS_TC_01_2016.pdf (academic source)

Cherapau, I., & Muslukhov, I., & Asanka, N., & Beznosov, K. (2015). On the Impact of Touch ID on iPhone Passcodes. Retrieved from: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-cherapau.pdf)

Ritchie, R. (2013). How Touch ID works: Making sense of Apple's fingerprint identity sensor. Retrieved from: https://www.imore.com/how-touch-id-works

Caif, P. (2015). Biometric authentication with Touch ID. Retrieved from: https://shinesolutions.com/2015/06/12/biometric-authentication-with-touch-id/


Uses of Touch ID
Other
Reliability
Novelty
Fun to use
Privacy
Cool to use
Efficiency
Security
Time/speed
Ease of use
Convenience
0
10
20
30
40
50
60
70
80
90
100
% of participants


Laser cut sapphire crystal
Stainless steel detection ring
Capacitive touch (Touch ID sensor)
Tactile switch