Beauty Mkombachoto

A Reality Check!

Apple’s Face ID authentication cannot tell the difference between real and fake faces

A Reality Check!

Beauty Mkombachoto

A look is all that is needed to unlock the 2017 iPhone X and access authorized services such as iTunes and Apple Pay. This is possible through biometric facial recognition captured by Apple's TrueDepth camera system and liveness detection.

It's effortless and safer than passcodes. Even Apple claims Face ID's security verifies neural engine and secure enclave are "robust authentication with a low false match rate and mitigate physical and digital spoofing", aka identity theft. However, few research findings do not match with Apple's claims.

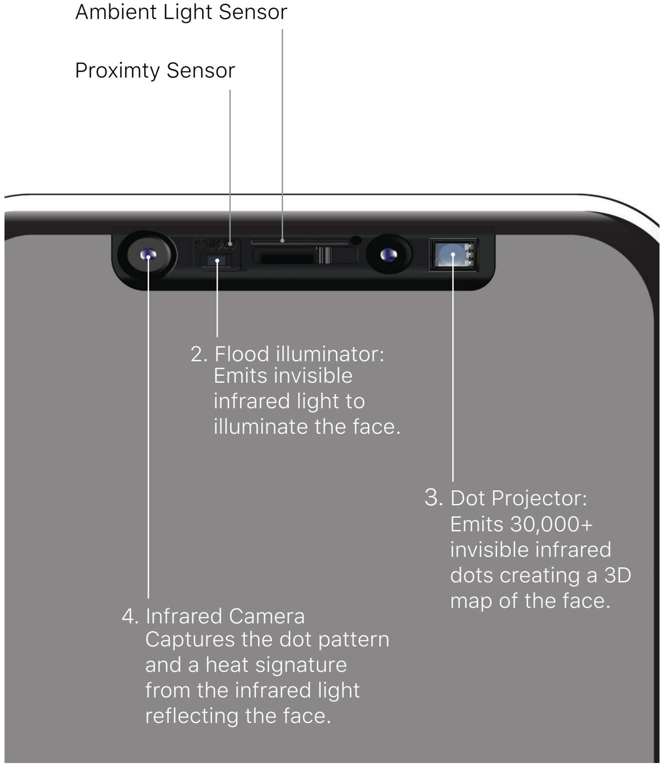
First, let's break down the TrueDepth camera system and liveness detection. The TrueDepth camera system consists of non-visible light projectors called infrared light and sensors that capture multiple images of user's facial features. To create a 3D mapping and recognition templet. Whilst liveness detection, detects a user's gaze to confirm the intent of unlocking the iPhone X. Shifting between "real" versus "fake" features on people. This process is a much safer way to unlock the iPhone X with a "one in one million chance someone else can foil it."

But, according to Andrew Bud the CEO of iProov, "Many people expressed concern that a person could be authenticated to a device without their... consent. A thief could pass a phone in front of the owner's face to unlock it." But, is it that straight forward?

Well, in 2017, Bkav a security firm in Vietnam were able to bypass Apple's Face ID liveness biometric feature. Through a $200 3D mask with 2D infrared images for eyes. In August 2019 researchers at Black Hat USA 2019 presented a session titled "Biometric Authentication Under Threat: Liveness Detection Hacking". They were able to bypass Apple's Face ID liveness detection in a specific scenario of an unconscious victim and their taped X-glasses.

The TrueDepth camera system creates a recognition templet to unlock the iPhone X.

1. Proximity Sensor and Ambient Light Sensor: Estimates lighting needed to recognise a face.



Ambient Light Sensor

Proximty Sensor

2. Flood illuminator: Emits invisible infrared light to illuminate the face.

3. Dot Projector: Emits 30,000+ invisible infrared dots creating a 3D map of the face.

4. Infrared Camera Captures the dot pattern and a heat signature from the infrared light reflecting the face.

In Black Hat's experiment researchers replaced real eyes with the black tape on lenses which were rendered as the eye and the white points as the iris.

The researchers uncovered that "liveness detection changes when users are wearing [blacked-out] glasses," because it is unable to "extract 3D information from the eye area when it recognizes the glasses." In both instances the liveness detection was hackable with cheap equipment and simple methods.

Let's image this happens to an Apple user, sadly they cannot do anything about it. Because of Face ID's secure enclave feature. A mathematical representation of a face that is used to compare "two face images and determines how similar they are," remarked by Professor Anil Jain a pattern recognition and computer vision researcher at Michigan State University.

This data is kept on one device because of secure enclave. Further explained in Face ID Security Guide, the data "is not sent to Apple, nor is it included in device backups," such as iCloud. Once liveness detection has been hacked by a criminal, digitally or physically, the iPhone X user cannot change their faces like the 4-digit passcode. Also making it impossible "to authenticate users across devices." The ability for Apple users to re-claim their phone has been snatched out of their owns hands. Making it harder to gain control of their phone.

The difficulty continues because of Face ID's neural engine. A revolutionary hardware processor chip capable of performing "over 600 billion operations per second, and it's used to do real-time processing of Face ID recognition," as stated by marketing chief at Apple, Phil Schiller. Importantly this feature is a recognition learning algorithm, "designed to work [on]...glasses, contact lenses, and many sunglasses...indoors, outdoors, and even in total darkness. Leading to the iPhone X authorizing and remembering the thefts spoofing success as a new mathematical representation template of a real face.

Apple's Face ID is certainly a robust authentication for both real and fake faces and is not flawless at mitigating spoofing digitally or physically though a cheap mask or a pair of glasses. Biometrics cannot be changed like 4-digit passcode. So, is Face ID safe and effortless?

References:

Apple Inc. (2017). Face ID security. Retrieved October, 2, 2019, from https://webcache.googleusercontent.com/search?q=cache:lBzU_0FPZ0kJ:https://www.apple.com/business/docs/site/FaceID_Security_Guide.pdf+&cd=14&hl=en&ct=clnk&gl=au

Ardalic, J., & Clark, N. (2018). Midas touch: *Consumer implications of the use of smartphone biometric data*. **Retrieved from** https://accan.org.au/our-work/research/1533-midas-touch-consumer-implications-of-the-use-of-smartphone-biometric-data

iProov, B, A. (2018). Facing the future: *The impact of apple FaceID.* //doi.org/10.1016/S0969-4765(18)30010-9. Retrieved from http://www.sciencedirect.com/science/article/pii/S0969476518300109

Chamary, J. (2017). How face ID works on iPhone X. Retrieved October, 2, 2019, from https://www.forbes.com/sites/jvchamary/2017/09/16/how-face-id-works-apple-iphone-x/#4fda71a624db

O'Donnell, L. (2019). Researchers bypass apple FaceID using biometrics 'Achilles heel'. Retrieved October, 2, 2019, from https://threatpost.com/researchers-bypass-apple-faceid-using-biometrics-achilles-heel/147109/