taproot® security

To: Apple Product Security   October 2, 2017
Re: iPhone X Face ID

Taproot Security is a private security research and consulting firm, advising clients and policymakers on cybersecurity matters. One area of specialization is biometrics. I represented the United States on the ANSI and ISO standards governing biometrics systems used in financial services.

We look forward to testing the Face ID feature on iPhone X when it becomes available. Meanwhile I studied the Apple Face ID security white paper and have ten recommendations to offer:

Involuntary Unlock

iPhone X performs Face ID verification any time you lift it up and look at it (eyes open in direction of the camera). This will obviously lead to some unwanted unlocks, but Apple presumably assumes they pose little risk when a phone is in close proximity to its owner.

My concern is this will make it easy for thieves to unlock a stolen phone; they simply have to hold it up to the victim's face. The only defense it to quickly close one's eyes or look away. The "SOS" button combination won't help in situations where the phone is stolen from a purse or pocket.

Recommendation 1: Introduce a short 2-second delay before verification, giving the user enough time to turn away and/or close their eyes.

Recommendation 2: Program Siri to respond to a voice command such as "SOS!" or "Lock up!" by disabling Face ID, waiting 5 minutes, and then allowing unlock only via passcode.

Template Adaptation

Face ID discards post-enrollment samples, but some post-enrollment templates are retained, apparently to enable adaptation (learning from past matches to improve accuracy). Adaptation is good, but implies the phone's accuracy may be suboptimal for a period of time after enrollment. My concern is facial phone unlocks may be less trustworthy during this period, even if scores exceed the match threshold.

Recommendation 3: During the first 100 verifications after enrollment, operate with a higher than normal matching threshold, and require passcode to unlock when score falls below the threshold.

Neural Net Training

Matching is performed by an artificial neural net on the A11 chip that Apple trained on a data set of 1 billion faces with diverse ethnicity, gender, and age. Apple claims it can handle glasses, hats, contact lenses, and certain sunglasses. The sunglasses claim seems to contradict Apple's assertion that Face ID only activates if the user's eyes are open.

One reason post-enrollment templates are retained is that Apple apparently expects they may have to issue updates to the neural network. The implication is Apple expects the neural net to require global fine tuning as they gain field experience. My concern is that not enough information about the neural net or its training has been shared with security researchers for us to give informed advice to the public.

Recommendation 4: Disclose details about neural net training and data set, either to the security community at large, or a reputable independent biometrics laboratory. Were impostors included? Did lighting conditions adequately vary? How are sunglasses handled?

Matching Errors

Apple claims Face ID offers a significantly lower false match rate than TouchID: One false accept per million attempts, versus one per 50,000 on TouchID. (The Face ID rate is worse for children and twins.) This is surprising since finger systems generally outperform facial systems.

Most biometric systems have a high threshold to accept, and a lower one to reject, while a score that falls in between thresholds triggers a "try again" response or other extra verification. Apple doesn't disclose its match thresholds, but if verification fails when match quality is higher than a "certain threshold", and then the user enters a correct passcode, then Face ID creates a new reference template. This provisional template is discarded after a finite number of unlocks if you stop matching against it, but if it keeps working it may join or replace the enrollment template (unclear which).

Apple says this allows Face ID to adapt to "dramatic changes in your facial hair or makeup use, while minimizing false acceptance." My concern is this might allow a phone thief to trick Face ID into accepting a new face (the thief's) instead of the correct face (the victim's).

Recommendation 5: In the event of a “dramatic change” in the user’s facial appearance, notify the user out of band (e.g., email) that a change in appearance was detected.

Recommendation 6: Disclose technical details about scoring and matching thresholds, either to the security community at large, or a reputable independent biometrics laboratory.

Spoofing

For liveness testing, Apple says the neural net was trained to differentiate live faces from photos or masks. Apple's paper doesn't provide specifics about this, nor did they offer any impostor testing results. This is concerning. A good face recognition system includes specific liveness tests, such as blinking or saccadic eye movements. Apple may argue that the use of infrared constitutes a liveness test because photos & masks lack a normal human thermal heat map, but this was not stated in the paper.

The reality is Apple may not really understand how Face ID performs liveness testing, since it was learned by a neural net rather than human programmed. My concern is Face ID could be spoofed by a 3D mask with a plausible heat signature.

Recommendation 7: Perform impostor tests and spoof penetration tests (preferably with reputable independent biometrics laboratory) and share results with the public or security researchers.

Recommendation 8: Collect multiple images (or video) during sampling in order to confirm facial movement (e.g., blinking) that would be difficult to fake with photos or masks.

Cryptographic Key Exposure

Before iPhone X, when an iPhone locked, the keys for the highest class of Data Protection were deleted from the secure enclave. Data in that highest classification is rendered inaccessible until the user supplies a valid a passcode, at which time key derivation from the passcode occurs.

With Face ID enabled, these critical keys are no longer deleted when the device locks. Instead, they're wrapped with a key that's held in the Face ID subsystem within the secure enclave. When a user attempts to unlock an iPhone X, if Face ID recognizes their face, then the Face ID subsystem provides the key to unwrap the Data Protection keys. My concern is the most critical keys in the device remain present while locked, and could therefore be forcibly extracted without the need to unlock it.

Recommendation 9: Perform cryptographic penetration testing of the iPhone secure enclave, preferably in partnership with a reputable independent security researcher, since enclave security is more important than ever in light of the design change described above. Testing should include hardware attacks, side channel attacks, and key leakage attacks.

Recommendation 10: To shorten the attack window, disable Face ID – and delete keys from the Face ID subsystem – after the phone has remained continuously locked for more than 4 hours.

Thank you for this opportunity to share our perspective on Face ID. I'm happy to enter into a NDA with Apple if you need it in order to respond or discuss further.

Sincerely,

Michael McCormick

Michael McCormick
President, Taproot Security
www.taprootsecurity.com
mike@taprootsecurity.com