Tape, glasses allow researchers to bypass Face ID

August 11 2019, by Nancy Cohen

Credit: CC0 Public Domain

In September 2018, a tech watcher was admirably candid: If you are a normal person, Apple FaceID is basically safe, she said. But then this tech watcher, Rachel Kraus, wrote in *Mashable* that "as I sized up the

arguments for and against, I've begrudgingly come to the conclusion that my fear of Face ID is just the teensiest bit irrational....But no way in hell does that mean I'm going to use it."

She was well aware of the plus points that had Apple and Apple fans stoked but she admitted she could not budge. "Face ID may be convenient, and is probably safe...But when it comes to protecting our phones, our identities, and our lives, probably just isn't good enough."

In 2019, you still find hesitant people who wonder whether the new technology will create increased security or a new attack opening, and Tencent researchers find cause to think about that a bit harder.

At the Black Hat U.S. 2019 security event earlier this month, the researchers drew interest in their session "Biometric Authentication Under Threat: Liveness Detection Hacking."

As part of their discussion, they said, they will "introduce our arsenal of attacking liveness detection and show how to apply them to bypass several off-the-shelf biometric authentication products, including 2-D/3-D facial authentication and voiceprint authentication."

The researchers showed how to use glasses and tape to bypass Apple FaceID.

Tencent's success relied on poking into a biometric feature called liveness detection. *Threatpost* reported on what the Tencent presenters had to say:

"With the leakage of biometric data and the enhancement of AI fraud ability, liveness detection has become the Achilles' heel of biometric authentication security as it is to verify if the biometric being captured is an actual measurement from the authorized live person who is present at

the time of capture."

Black tape was placed on the lenses, and white tape inside the black tape. "Using this trick they were then able to unlock a victim's mobile phone and then transfer his money through mobile payment App by placing the tape-attached glasses above the sleeping victim's face to bypass the attention detection mechanism of both FaceID and other similar technologies," said Lindsey O'Donnell, *Threatpost*.

O'Donnell, however, said there was just one thing, if you thought this was an easy caper: The real victim would have to be out cold. Cold, as in unconscious. As in the bad actor having to put the glasses on the person without waking the person up. ("At least it's slightly more difficult than using a sleeping person's finger to unlock Touch ID," said *Gizmodo*'s Jennings Brown.)

What's going on? Why did FaceID lose its power? O'Donnell said, "the abstraction of the eye for liveness detection renders a black area (the eye) with a white point on it (the iris)." However, if a user is wearing glasses, the way that liveness detection scans the eyes changes. If a person wears glasses, FaceID won't extract 3-D information from the eye area when it recognizes the glasses.

Advice from Tencent presenters was that biometrics manufacturers add identity authentication for native cameras and increase the weight of video and audio synthesis detection, said O'Donnell.

Apple, meanwhile, provides its own story about FaceID on its site and it is reasonable to assume security has been given high priority:

"The probability that a random person in the population could look at your iPhone or iPad Pro and unlock it using Face ID is approximately 1 in 1,000,000 with a single enrolled appearance," according to its "About

FaceID advanced technology" page.

As added protection, only five unsuccessful match attempts are allowed by FacedD—and then a passcode is required. "The statistical probability is different for twins and siblings that look like you and among children under the age of 13, because their distinct facial features may not have fully developed. If you're concerned about this, we recommend using a passcode to authenticate."

Nonetheless, Tencent explored and reported their findings. "Face ID works differently if it detects glasses. When the system recognizes glasses, it apparently doesn't pull information from the eye region of the face," said *Gizmodo*'s Jennings Brown.

TNW agreed, reporting, "Well, it turns out FaceID scans eyes differently when people wear glasses. *TNW* quoted the researchers: "We found weak points in FaceID." Where? "It allows users to unlock while wearing glasses […] if you are wearing glasses, it won't extract 3-D information from the eye area when it recognizes the glasses."

One reasonable takeaway is that the setting for this feat to work is nothing short of bizarre. *9to5Mac*: "To unlock another person's phone, you would seemingly need to figure out how to put glasses on them and ensure they were still enough for Face ID to work. As the researchers note, this would be most effective when the victim is unconscious."

Juli Clover, *MacRumors*, raised another point: "It's worth noting that this isn't a situation most people are likely to run into, and there's also no secondary research on this alleged method this time."

One reader comment on *MacRumors*: "This is a bit of a reach. I think for Face ID to be fooled by such a ridiculous circumstance just goes to show how hard they've tried to 'break' it —"

On the other hand, the research shows weaknesses behind the design of liveness detection.