

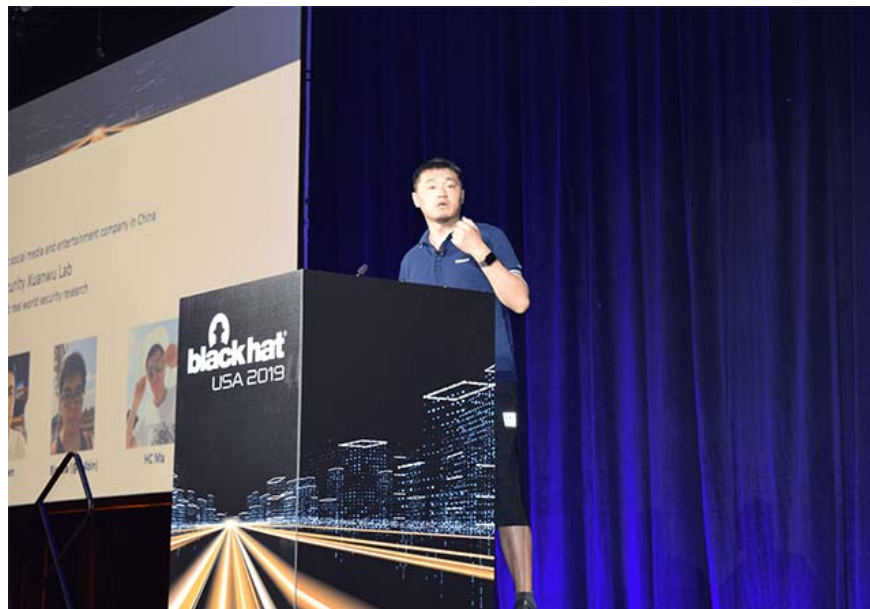
Hackers can bypass the Face ID face with just a pair of black adhesive tape

According to experts, this method can fool Face ID by making this security tool think users are opening their eyes.

Not long ago, Tencent's security researchers discovered that Apple's Face ID biometric authentication system could be fooled by using a pair of black adhesive tape, and a piece of white tape in the center of the lenses.

According to experts, this method could fool Face ID by making this security tool think users are opening their eyes, which could allow crooks to access locked iPhones while the owner is still sleep and unaware.

1. The iPhone can be hacked with just one message without requiring user interaction



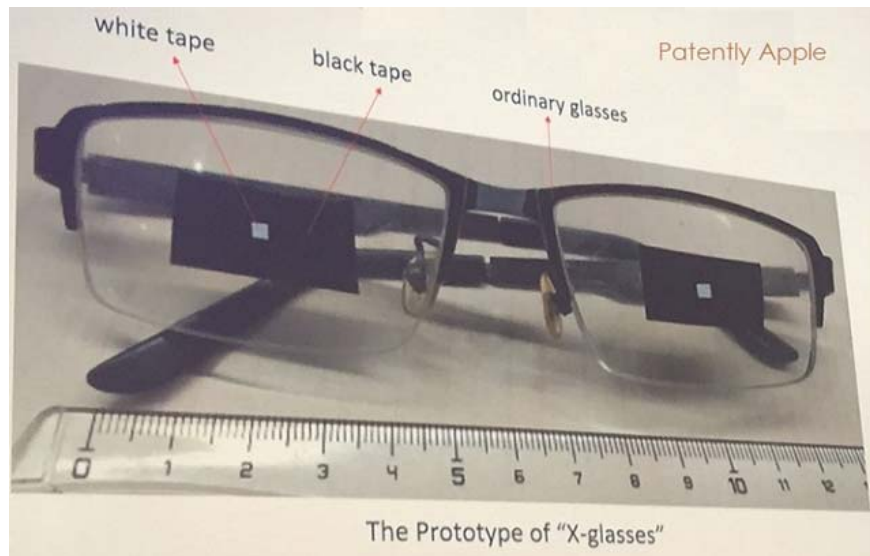
This new Face ID hack method has been announced by Tencent experts at Black Hat 2019

Theoretically, but in fact, to carry out a manual iPhone hack is not easy, and the ability to succeed is not too high, simply because it needs quite a bit. factors outside the hacker control, such as the prerequisite that the owner of the iPhone must be sleeping or close his eyes, can deceive Face ID. Also wearing glasses so that the owner of the iPhone does not wake up is a big problem.

Although the way to proceed is relatively difficult, but the operating principle of this hack method is surprisingly simple. The reason for this pair of black adhesive tape can deceive the process of 'real' or 'fake' face recognition

because the black adhesive tape plays a role in simulating the eye area, and the white part will 'fake' is pupil of the eye. These two elements work together easily to bypass FaceID, making this authentication tool skip the user's Liveness Detection step and unlock the iPhone.

1. Apple expanded the size of the security bug detection program to receive bonuses, including macOS, a maximum bonus of \$ 1 million



"The black tape section plays a role in simulating the eye area, and the white part will 'fake' as pupil eyes"

Tencent's discovery has also shed light on an interesting way of seemingly tight operation but contains a few weaknesses in Apple's latest biometric security process. Researchers have shown that when an object wears glasses, Face ID actually only tries to find 2D information and not 3D information from the eye area. While this fake 2D information can be simulated relatively easily with just a piece of white spot black tape and stuck to the two sides as mentioned above, this makes Face ID mistakenly think it is the human eye and allow unlocking iPhone.

This is not the first time security researchers have claimed to have discovered a 'silly' vulnerability on Face ID. Back in 2017, Bkav himself announced a video recording how to unlock an iPhone using a silicon mask full of eyes, nose, lips, and mouth, all printed on paper. This mask is printed in 3D (costs about 200 USD), made of stone powder material, eye part with 2D image. In particular, the part of the eyes due to the special role should be printed with infrared photos - technology that Face ID itself uses to record face images. The iPhone X in the test was immediately unlocked.

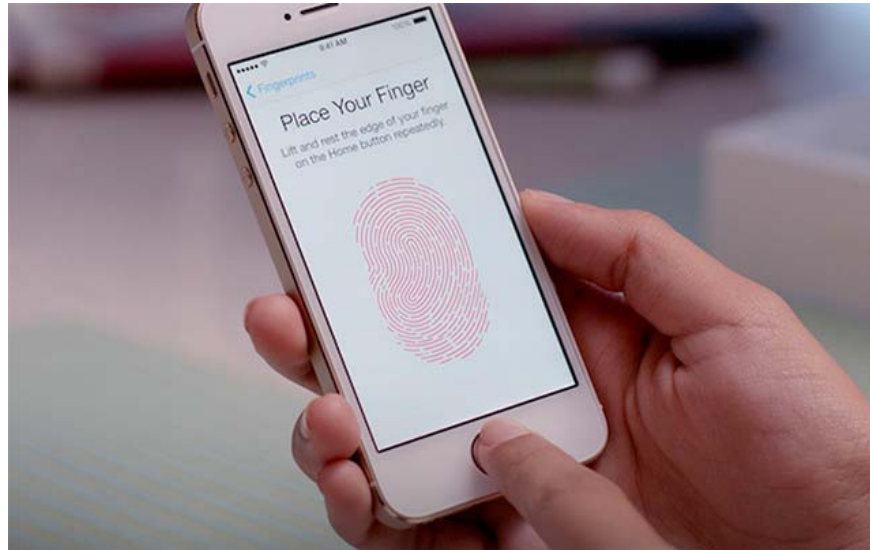
1. The fate of the smartphones in the second hand market: Removed to every detail, can restore data to steal information

Model of Bkav's Face ID hack method

These materials and supplies are not difficult to find in reality. However, this method works mostly based on the group having access to detailed measurements or digital scanning on Face ID's face, and this is in fact very unlikely.

Not only Face ID, another Apple biometric security method, Touch ID, has also been hacked successfully within 24 hours from the time the iPhone has the world's first fingerprint sensor. sold out. The way to proceed is also very simple, just print a high-resolution fingerprint image and overlap the actual scale of the fingerprint structure in a scale of 1-1.

1. Why is the Apple printed circuit board black while most other manufacturers are green?



Touch ID has been hacked successfully after only 24 hours of launch

Biometric security is a modern security method, high accuracy and will be used more widely in the future. However, to make this form of identity authentication an optimal security method, developers will have a lot of work to do. Although most of the current hacking methods are quite difficult to implement in practice, but not impossible, and the "gaps" that make the biometric authentication tool out of the way should be fixed in time. earliest.

You finished reading the article "**Hackers can bypass the Face ID face with just a pair of black adhesive tape**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.