Journalist puts Windows 10 face recognition feature to test

August 24 2015, by Nancy Owano

If Windows Hello could talk it would possibly be bragging: Hello Mary. Hello Merry. What, you think I can't tell?

This is the Windows 10 biometric authentication security feature that takes a fresher turn from traditional passwords for logging in. The feature enables a PC user to unlock the machine via facial recognition.

Question is, how easily can it be fooled? A Sydney-based journalist subjected Windows Hello to a twin test. If facial recognition is a biometric tool that is supposed to make it easy to sign in, is it also easy to break in?

Chris Griffith in *The Australian* introduced his effort by describing his test topic. "Windows 10, released last month by Microsoft, replaces the hackable password system with biometric recognition. You log in using your fingerprints, and with eye and face recognition."

Griffith wrote about the technology used in Windows Hello: The face recognition process involves a RealSense camera from Intel, which sits embedded above the display. Three cameras—an infra-red lens, a regular lens and a 3-D lens—use photographic analysis, heat detection and depth detection to decide who is at your computer display.

He also said, "The heat-sensing IR camera doesn't allow access to someone waving a photograph in front of the camera. The IR camera also increases reliability in cases where users wear cosmetics, have facial hair or there's a variation in lighting conditions."

Earlier this year, *Redmond Magazine* talked about Windows Hello's spoofing safeguards: "Microsoft's choice of going with infrared cameras for Windows Hello will battle spoofing attempts. Using a physical photograph or one stored on another device will cause the camera to view that as a blank image and will not authenticate the user."

Griffith also noted that "Microsoft says Windows Hello is based on 'asymmetric key cryptography', technology that powers smart cards and is used to verify web servers and mobile phone networks. It's well established but previously hasn't been adapted to consumer computing."

As for face spoofing, he devised a twin test because he wanted to find

out if it could work using identical twins. Griffith said he used the Lenovo Thinkpad Yoga 14. Would the camera let the second twin log into an account registered with the sibling's face?

Griffith turned to The Australian Twin Registry. He worked with six sets of identical twins in Melbourne and Sydney. Some twins tried fooling the camera by removing their glasses or rearranging their hair.

The only instance where the system failed was in the case of 11-year-old twin girls. In that tryout, he reported, Windows Hello was unable to log in either. "That was the only instance where the system failed. In the end, there were some cases of Windows Hello taking its time to identify a twin, but no case of it wrongly granting access. That's a win for Intel and Microsoft."

Jon Fingas of *Engadget* found it useful to note in this success story that this was a small sample. "However, this suggests that Windows' face detection is reliable enough to eliminate some of the frustrations you see elsewhere. And that's important for both security and convenience."

Griffith noted that a large number of notebooks coming on to the market with Windows 10 offer face recognition as an alternative to passwords for accessing your account.

Citation: Journalist puts Windows 10 face recognition feature to test (2015, August 24) retrieved 28 April 2024 from https://techxplore.com/news/2015-08-journalist-windows-recognition-feature.html