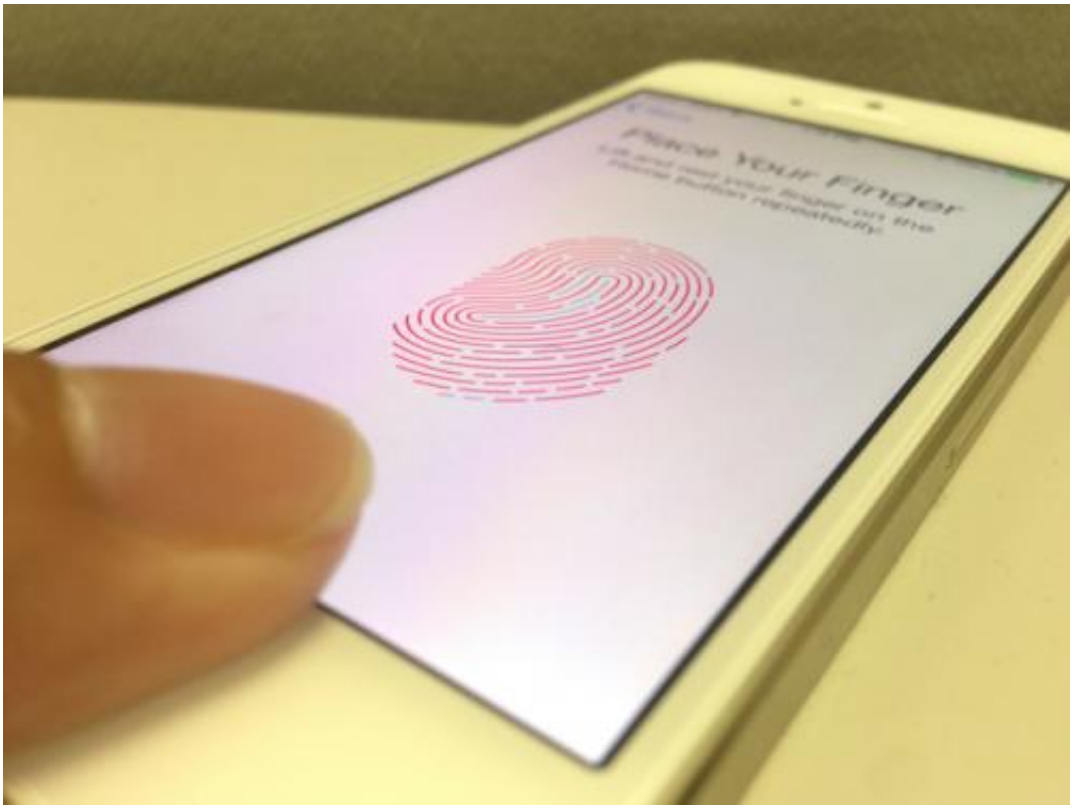
iPhone hack shows security isn't at our fingertips just yet

September 24 2013, by Eerke Boiten



Finger or falsie? It’s too hard to tell. Credit: hawaii

We've come to expect something radically different from Apple every time it launches a new product and sure enough, the fingerprint sensor unveiled as part of the iPhone 5s, seemed like a revolution in phone security.

But almost as soon as the technology was announced, fans and foes set about trying to crack the fingerprint system. Sure enough, a group in Germany now claims to have succeeded, just days after the new iPhone became available.

From the first announcement by Apple, the commentary suggested forging of fingerprints might be an issue. It looks like the German Chaos Computer Club has achieved this security breach for the Touch ID sensor. The group claims to have created a fake finger using just a fingerprint left on glass. It says the hack proves that fingerprint technology is not a suitable method for controlling access to mobile phones.

The club's technique may not have been as simple and low-tech as the legendary gummibear attack by Matsumoto, but it still looks relatively easy. There also appears to be a contradiction between the claims made by the CCC and Apple's assertion that the technology uses "sub-epidermal" scanning, which would distinguish live fingers from fakes, but the claim from the CCC is nevertheless credible.

Apple's underlying motivation for offering fingerprint locking was good: people too often do not bother to lock their phones, password-based security drives users up the wall and is increasingly at risk from brute force cracking.

There is little doubt that multi-factor authentication is the future. This involves double protection using something you know, like a password, as well as something you have, like a phone, or something you are. This last category relies heavily on a long history of biometrics research, recording characteristics of voice, eyes, writing and fingerprints.

Like any biometric technology, fingerprint sensors must have a high degree of precision. This characterises the quality of the compromise

between "false negatives" (failing to recognise someone) and "false positives" (recognising the wrong person). For individual consumers, the first is a frustrating usability issue – the second is a much less visible security problem.

The technology in the iPhone's Touch ID feature is said to be highly advanced. With the profits the company makes and the amount it can spend on research, Apple could well have achieved a breakthrough in fingerprinting sensor precision.

The promotional video for the new phone shows an awareness of the potential security problems related to losing fingerprint data. It was quick to announce that the information would only be stored in an encrypted form, and only in a secure area on the phone chip itself.

The revelations made so far about the extent to which the NSA is able to spy on consumers do not actually suggest that Apple has given the NSA full access to its iPhones, so we may still be safe when using our iPhones. Conscious that security issues are at the forefront of its customers' minds these days, Apple promised it will not allow third party applications access to Touch ID. This suggests it has learned from the privacy issues raised by its careless leaking of location and contact information. However, it does restrict the introduction of potentially improved authentication facilities.

The CCC breach is not necessarily a reason for people to junk their brand new iPhones – no more so than other problems found such as ways of circumventing lock screens. The new security feature certainly looks more user-friendly than using a pincode. Of the 50% of people who do not use any phone security right now, some may take this up, and that is a step forward. For critical operations such as iStore purchases, Apple customers will still use a password in addition to the fingerprint, so security is at least not reduced in that sense.

In the longer term, there is no doubt that passwords by themselves will become a thing of the past. A breakthrough in usable and secure multi-factor authentication would have been very welcome. As it turns out, the Apple Touch ID isn't it.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation