The keys may be on your fingertips, but that doesn't mean biometric locks can't be picked

September 12 2014, by Andrew Smith

Keys at your fingertips, but the technology isn't there yet. Credit: Rachmaninoff, CC BY-SA

How can we ensure that someone is who they say they are? How can be sure that the person in our system, both digitally speaking or physically in front of us, is who whom they claim to be?

You may think that a good password is the answer, but with so many ways to break into a computer system these methods are clearly not always effective – as can be seen from the unfortunate hacked celebrities whose naked pictures were strewn across the internet recently, or the Oleg Pliss ransomware that locks iPhones until the extortioner is paid. Even a combination of a good username and password may not be enough.

An organic alternative to passwords

What about biometrics? This technology uses human physical attributes as locks and keys, such as fingerprints, iris scans or, as is now suggested, the veins in the human fingertip, making them highly individual ways to identify one user from another.

Using biometrics is not especially new. For example, while the likes of iris scanners may be familiar from sci-fi films, they're also (or were until recently) found in real life airports too. Often mistakenly called retinal scanners, they are based on scanning the unique pattern of the iris, the coloured part of the eye.

But the technology needed to complete an effective and trusted scan is expensive and can be tricked by technologically capable hackers. These are great for entry control systems on the buildings of large organisations, or for the occasional secret bunker seen in films. But they are extremely costly – prohibitively so if a bank was to insist that every customer had one at home – and false readings become a problem as the number of people using it scales.

On the other hand, fingerprint technology has become cheaper and more available – fingerprint scanners are now sufficiently small and accurate that they started appearing in laptops 10 years ago, and are even in small devices like the iPhone 5S. This is one way that banks could allow

smartphone and laptop users to access their financial services, with users presenting a finger rather than a passcode.

In fact it's easy to obtain a range of low-cost scanners for all sorts of authentication uses. But that doesn't mean the users will like doing so – there are ethical issues to consider, as some UK schools discovered in 2012 when their use of fingerprint scanners to monitor pupil attendance led to an outcry and a government ban without explicit consent from parents.

Weaknesses and workarounds

Despite our fingerprints all being unique, there is still the possibility to fool the systems used to protect secured buildings, large computer systems or financial institutions. There are well known ways to get around fingerprint biometric authentication, from creating false fingers (with prints) from gelatin, using good quality photographs or even a photocopy of fingerprints to fool scanners, or most upsettingly simply removing a finger from those with access rights. These and others are well known, in real life and in the semi-fictional world of Hollywood.

Barclays' recent decision to use a finger vein scanner, which scans and pattern-matches the unique structure of the blood vessels in the finger. This has the benefit of only working when the finger is attached to the rest of the body and blood is flowing, which rules out the most grisly workarounds.

Facial recognition has been available for a while, and as the majority of computers now come with webcams included this would seem a logical step. The challenge is that the software making the decisions is very sensitive to environmental conditions such as light and darkness. We don't all look our best for the camera all of the time, and the need for our real face to match the reference version the system is using means that,

while a human would recognise the same person, a computer algorithm often can't. This is why the killjoys at the UK Home Office and elsewhere refuse to let us smile in passport photos these days. But this same fact means that it's possible to log into laptops equipped with a face-recognition login by simply putting a picture of the owner in front of the webcam.

Right technology used the right way

Using biometrics for security and identification requires meeting two challenges: they must be cheap enough and sufficiently simple to be used by ordinary users. And the context of when and how they are used must also be entirely ethical, and secure. For example, systems that store too many personal details or copies of biometric data could be hacked or abused without appropriate controls in place.

Biometrics could be the answer, but it's a case of combining two or more types of authentication for added security, such as coupling fingerprints with key codes or passwords to provide greater trust that who is logging in is only who we are expecting. There may always be new picks created to open whatever new locks we invent, but if biometrics can make it that much harder, so much the better.

Source: The Conversation