Source: *The Straits Times,* pB7
Date: 17 May 2022

TechTalks

Preventing abuse of biometrics authentication technology

Best way to reap its benefits while minimising risks is a well-informed public

Terence Sim
For The Straits Times

Do you unlock your smartphone with your face or fingerprint?

Welcome to the world of biometrics authentication – a whopping US$28 billion (S$39 billion) global market, which promises a modern, convenient, reliable and effective method to verify someone's identity.

Compared to tapping a staff card or keying in a PIN code, biometrics promise enhanced security because they cannot be lost or forgotten, and are not easily forged or duplicated.

Biometrics may be used alone, or as a second factor for authentication. For instance, many banks routinely employ voice biometrics for verification before allowing transactions over the phone to go through. There is no need for intrusive security questions asking for your date of birth and the number of credit cards you hold.

But no system is foolproof.

There have been stories of fingerprints being forged to unlock the door to one's house, or faces being scanned without authorisation to steal money from someone else's digital wallet.

For instance, a man in China reportedly lifted his sleeping former girlfriend's eyelids to unlock her phone to access her digital wallet.

Some people have also reportedly used a copied fingerprint, or a photograph, to trick the biometric sensor.

One common defence technology is Liveness Detection.

It checks if the face or finger scanned comes from a live person, using infrared light to check for vein patterns inside the finger or to compute the 3D structure of the face. Such methods require additional sensors and algorithms, and thus cheaper products may not have them.

Biometrics authentication, which uses technology such as facial recognition, promises a modern, convenient, reliable and effective way to verify someone's identity. However, no system is foolproof. Besides instances of theft using copied fingerprints, for example, there have also been concerns of privacy violations. PHOTO: REUTERS

There have also been concerns among critics of privacy violations with the use of biometrics, which does not only identify someone but reveals information about the person's health.

For example, iris patterns are said to have the potential to reveal one's kidney health. This should not be surprising, since doctors routinely measure body features for medical diagnosis.

Many data protection regimes do not allow biometrics to be used for secondary purposes, including medical diagnosis, without the person's consent.

But such a secondary purpose (called function creep) can be difficult to detect, since it can be implemented long after the original purpose the data was collected for, and in the guise of increasing customer convenience.

There should be a legal requirement for biometric systems used in Singapore – particularly those to authenticate financial or government services – to be certified or accredited.

What then can be done to minimise any potential abuse?

One way is to have an independent accreditation laboratory check for security and privacy vulnerabilities in biometric products – for a fee, of course. Regular audits done by the lab could guard against function creep.

There are only a few such labs worldwide, including in China, Australia and Britain.

Many of these labs are accredited by the Fido Alliance, founded in 2012 by tech firms, including PayPal and Lenovo, to promote open standards in online authentication.

Singapore, with its high competency in digital technology and sterling reputation for trustworthiness, could establish one such accreditation lab. It is a viable business opportunity.

In addition, there should be a legal requirement for biometric systems used in Singapore – particularly those to authenticate financial or government services – to be certified or accredited.

Another consumer safeguard is to require companies to comply with international standards.

Doing so will ensure the interoperability of biometrics devices and facilitate compliance testing.

Organisations that use standards-compliant biometrics systems will also have wider choices of data security offerings, thereby avoiding outdated and vulnerable technologies.

The Identification Technology Technical Committee (ITTC), under the auspices of Singapore's IT Standards Committee, actively monitors and contributes to various ISO standards related to biometrics.

Over the years, the ITTC has produced standards documents and usage guidelines for data interchange formats for fingerprint, facial image, iris and voice data.

These may be purchased from www.singaporestandardseshop.sg

Its work is laudable, and conducted by volunteers who receive little recognition.

As a country that increasingly adopts biometrics in daily life, the Singapore Government should incentivise more professionals to participate in this important effort, such as by subsidising work trips to ISO meetings and funding the development and testing of ISO prototypes.

Private companies can also benefit by participating in ISO standards, as they get to observe and influence decisions that may help in shaping their products and services.

Finally, best practices should be shared.

A non-profit organisation could be formed to bring together vendors and users from all sectors to share what has, and has not, worked.

This quickly raises the bar in biometrics security, and creates a strong deterrent against cyber criminals who can no longer tap users' ignorance to propagate crime.

Such an organisation can also educate the general public and debunk myths.

An example to emulate is the Sydney-based Biometrics Institute, comprising government agencies, banks, airlines, academics and observers from United Nations and European Union institutions. The institute promotes the sharing of best practices, and publishes guidelines on ethical usage and privacy.

It is known for its Biometric Vulnerability Assessment Testing, which is a framework to understand the risks associated with biometric deployment.

At the end of the day, a well-informed public is the best way to reap the benefits of biometrics while minimising its risks.

• Terence Sim is vice-dean of communications and associate professor of computer science at the National University of Singapore's School of Computing.