Fingerprint and face scanners aren't as secure as we think they are

March 6 2019, by Wencheng Yang And Song Wang

Credit: Unsplash/CC0 Public Domain

Despite what every spy movie in the past 30 years would have you think, fingerprint and face scanners used to unlock your smartphone or other devices aren't nearly as secure as they're made out to be.

While it's not great if your password is made public in a data breach, at least you can easily change it. If the scan of your fingerprint or face – known as "biometric template data" – is revealed in the same way, you could be in real trouble. After all, you can't get a new fingerprint or face.

Your biometric template data are permanently and uniquely linked to you. The exposure of that data to hackers could seriously compromise user privacy and the security of a biometric system.

Current techniques provide effective security from breaches, but advances in artificial intelligence (AI) are rendering these protections obsolete.

How biometric data could be breached

If a hacker wanted to access a system that was protected by a fingerprint or face scanner, there are a number of ways they could do it:

1. your fingerprint or face scan (template data) stored in the database could be replaced by a hacker to gain unauthorised access to a system
2. a physical copy or spoof of your fingerprint or face could be created from the stored template data (with play doh, for example) to gain unauthorised access to a system
3. stolen template data could be reused to gain unauthorised access to a system
4. stolen template data could be used by a hacker to unlawfully track an individual from one system to another.

Biometric data need urgent protection

Nowadays, biometric systems are increasingly used in our civil, commercial and national defence applications.

Consumer devices equipped with biometric systems are found in everyday electronic devices like smartphones. MasterCard and Visa both offer credit cards with embedded fingerprint scanners. And wearable fitness devices are increasingly using biometrics to unlock smart cars and smart homes.

So how can we protect raw template data? A range of encryption techniques have been proposed. These fall into two categories: cancellable biometrics and biometric cryptosystems.

Read more: When your body becomes your password, the end of the login is nigh

In cancellable biometrics, complex mathematical functions are used to transform the original template data when your fingerprint or face is being scanned. This transformation is non-reversible, meaning there's no risk of the transformed template data being turned back into your original fingerprint or face scan.

In a case where the database holding the transformed template data is breached, the stored records can be deleted. Additionally, when you scan your fingerprint or face again, the scan will result in a new unique template even if you use the same finger or face.

In biometric cryptosystems, the original template data are combined with a cryptographic key to generate a "black box". The cryptographic key is the "secret" and query data are the "key" to unlock the "black box" so that the secret can be retrieved. The cryptographic key is released upon successful authentication.

AI is making security harder

In recent years, new biometric systems that incorporate AI have really come to the forefront of consumer electronics. Think: smart cameras with built-in AI capability to recognise and track specific faces.

But AI is a double-edged sword. While new developments, such as deep artificial neural networks, have enhanced the performance of biometric systems, potential threats could arise from the integration of AI.

For example, researchers at New York University created a tool called DeepMasterPrints. It uses deep learning techniques to generate fake fingerprints that can unlock a large number of mobile devices. It's similar to the way that a master key can unlock every door.

Researchers have also demonstrated how deep artificial neural networks can be trained so that the original biometric inputs (such as the image of a person's face) can be obtained from the stored template data.

Read more: Facial recognition is increasingly common, but how does it work?

New data protection techniques are needed

Thwarting these types of threats is one of the most pressing issues facing designers of secure AI-based biometric recognition systems.

Existing encryption techniques designed for non AI-based biometric systems are incompatible with AI-based biometric systems. So new protection techniques are needed.

Academic researchers and biometric scanner manufacturers should work together to secure users' sensitive biometric template data, thus minimising the risk to users' privacy and identity.

In academic research, special focus should be put on two most important aspects: recognition accuracy and security. As this research falls within Australia's science and research priority of cybersecurity, both government and private sectors should provide more resources to the development of this emerging technology.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Fingerprint and face scanners aren't as secure as we think they are (2019, March 6) retrieved 9 April 2024 from https://phys.org/news/2019-03-fingerprint-scanners.html