Your brain is unique – here's how it could be used as the ultimate security password

March 10 2017, by Palaniappan Ramaswamy

Credit: AI-generated image (disclaimer)

Biometrics – technology that can recognise individuals based on physical and behavioural traits such as their faces, voices or fingerprints – are becoming increasingly important to combat financial fraud and security threats. This is because traditional approaches, such as those based on PIN numbers or passwords, are proving too easily compromised. For

example, Barclays has introduced TouchID, whereby customers can log onto internet banking using fingerprint scanners on mobile phones.

However, this is not foolproof either – it is possible to forge such biometrics. Fingers can after all be chopped off and placed by impostors to gain fraudulent access. It has also been shown that prints lifted from glass using cellophane tape can be used with gelatine to create fake prints. So there is a real need to come up with more advanced biometrics that are difficult or impossible to forge. And a promising alternative is the brain.

Emerging biometric technology based on the electrical activity of the brain have indeed shown potential to be fraud resistant. Over the years, a number of research studies have found that "brainprints" (readings of how the brain reacts to certain words or tasks) are unique to individuals as each person's brain is wired to think differently. In fact, the brain can be used to identify someone from a pool of 102 users with more than 98% accuracy at the moment, which is very close to that of fingerprints (99.8% accuracy).

More recently, this has been confirmed by functional magnetic resonance imaging (fMRI), which measures brain activity by tracking changes in blood flow. A study using fMRI data from the Human Connectome Project was able to recognise individuals with up to 99% accuracy when performing certain mental tasks such as relaxing, listening to a story, computing maths, looking at emotional faces or imagining moving parts of their body.

However, the cost and difficulty of using fMRI (you have to lie very still in the scanner for a fairly long time) means it is clearly not practical for everyday biometric authentication. For that reason, researchers have instead looked at electroencephalography (EEG), which uses electrodes to track and record brain-wave patterns. But this is also cumbersome –

who would be willing to wear a cap of gel-based electrodes just to log in to their computer? Hence, the technology has remained in the realm of science fiction for some time.

Fingerprints are commonly used. Credit: Barclays

Promising alternatives

Recently, technological advances in recording EEG from the ear using electrodes placed on the surface of standard earphones have provided a solution – no gel needed. It is not easy though – EEG is very "noisy" since the brain is always actively processing different information. But

advanced signal-processing approaches have recently been able to reduce the noisy components, albeit this typically requires powerful computing. This is, however, becoming less of a problem now that mobile-phone processing power is growing rapidly – it should in theory be possible to perform all the required processing on a smart phone.

So why aren't brainprints everywhere already? One downside is that it can't be used by twins – they have near-identical EEG patterns. But the main problem is the lack of stability of brainprints over time.

It seems that it is not enough to just have an EEG done once – occasional re-enrolment (say, monthly) is necessary. This is because the brain connections exhibit plastic behaviour (they change with experience) and thought processes in the brain change over time. However, in ongoing work at the University of Kent, we have shown that specific tones (which can be played using earphones) can be used to minimise these changes. It is not yet clear exactly how these tones affect the brain but we speculate that they may allow the brain to calm down, allowing more focused activity.

Two-factor authentication is now a norm for many banking transactions, for example using a password and an additional code sent to the phone. Soon, banks in New York may have to comply with multi-factor authentication protocol proposed by the New York State Department of Financial Services, whereby at least three authentication mechanisms are used for enhanced security by personnel accessing internal systems with privileged access or to support functions including remote access.

While fingerprints and voice recognition are possibilities, thought-based biometric technology is more apt to be used as an add-on to meet this new cybersecurity regulation. The brain biometric template could even be updated for a different mental activity should there be a security breach on the stored template (unlike a fingerprint biometric which

remains for life and cannot be replaced once compromised).

Brainprints can also be used to generate passwords that can replace conventional alphanumeric passwords or PINs in ATM machines to withdraw cash. For example, rather than keying in the PIN, one would connect earphones and be shown a series of PIN numbers on the ATM screen. Brain patterns would change when the correct PIN number showed up – activating the transaction. By doing so, one does not have to worry about others looking over the shoulder to steal the PIN. Moreover, under coerced situations, brainprints will not work due to the stress – making them even more fraud resistant.

Given that it is difficult to copy another person's exact thought process, the technology is certainly advantageous. Considering the advancement in the technology, we will likely see uptake of biometric applications based on brainprints soon – especially as part of multi-factor system for enhanced authentication. So don't be surprised to see EEG earphones appearing in your post from the bank shortly.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Your brain is unique – here's how it could be used as the ultimate security password (2017, March 10) retrieved 24 April 2024 from https://phys.org/news/2017-03-brain-unique-ultimate-password.html