Your reaction to pics of Leonardo DiCaprio, animals could unlock your next smartphone

By Cory Nealon

Proposed biometric system measures brainwaves; creates brain password that's 'cancelable,' meaning it can be reset if hacked

BUFFALO, N.Y. — To overcome password fatigue, many smartphones include facial recognition, fingerprint scans and other biometric systems.

The trouble with these easy-to-use tools is that once compromised — yes, they can be hacked — you can't reset them.

"You can't grow a new fingerprint or iris if that information is divulged," says Wenyao Xu, PhD, assistant professor of computer science and engineering in the University at Buffalo School of Engineering and Applied Sciences. "That's why we're developing a new type of password — one that measures your brainwaves in response to a series of pictures. Like a password, it's easy to reset; and like a biometric, it's easy to use."

The "brain password," which would require users to wear a headset, could have implications in banking, law enforcement, airport security and other areas.

"To the best of our knowledge, this is the first in-depth research study on a truly cancelable brain biometric system. We refer to this as 'hard cancellation,' meaning the original brain password can be reset without divulging the user's identity," says collaborator Zhanpeng Jin, PhD, associate professor of computer science and engineering at UB.

Their work is described in a study that will be presented June 11 at MobiSys 2018, a flagship mobile computing conference hosted in Germany by the Association for Computing Machinery. For a copy of the study, please email Cory Nealon at cmnealon@buffalo.edu.

Why celebs and animals?

Xu was motivated to create a cancelable biometric password after hackers stole the fingerprint files of 5.6 million workers from the U.S.

Office of Personal Management in 2015.

Perhaps the most accessible way to record brain activity is through electroencephalography, which uses electrodes to measure the brain's unique patterns of electrical activity.

For their system, Xu and collaborators reconfigured a virtual reality headset, reducing the number of electrodes to six. Three record brain activity, two serve as grounds and the last acts as a reference point. Typically, these headsets have 32 to 64 electrodes.

The electrodes recording brain activity measure three areas of the organ: the intraparietal sulcus (controls declarative memory), the inferior parietal lobule (processes face recognition) and the temporo parietal junction (reading comprehension).

Researchers chose specific image types to stimulate each brain region. They used animal pictures for the intraparietal sulcus because one's memory of a certain animal can be highly individualized. For example, a person who suffered a spider bite will have a different reaction than someone who hasn't.

For the inferior parietal lobule, researchers relied on recognizable celebrities such as Leonardo DiCaprio. For the temporo parietal junction, they used encouraging phrases such as "aspire to inspire."

How the brain password works

Users are shown the three images in rapid succession — 1.2 seconds to be exact. The process is repeated three additional times. By the end of the fourth time, after 4.8 seconds, the brain password is ready.

Researchers recruited 179 adults — 93 men, 86 women — to test the brain password. Test subjects' average age was 30.

Researchers collected data from three sessions, including one that occurred five months after the original test. The goal of the last test was to see how brain passwords functioned over time.

Overall, brain passwords were more than 95 percent effective. The performance dipped slightly, by 1 percent, on the last test.

Early adopters and privacy concerns

While wearing a headset may not appeal to common internet users, Xu says that may change over time, especially if the device is redesigned into something more like Google Glass.

Plus, he says, companies with deep concerns about cybersecurity may be early adopters of the technology. As for privacy concerns, Xu says the system — even if hacked — would not divulge sensitive information.

“These passwords contain information gathered from only three channels in less than five seconds. Semantic memory attacks need much more time than that,” says Xu, who plans to continue work on the system to make it more reliable and appealing to users.

The research was supported by the National Science Foundation (NSF) and NSF’s Center for Identification Technology Research.