Forget your password: The future is 'passthoughts'

April 8 2013

Other than the EEG sensor, the headset is indistinguishable from a conventional Bluetooth headset.

(Phys.org) —Instead of typing your password, in the future you may only have to think your password, according to School of Information researchers. A new study explores the feasibility of brainwave-based computer authentication as a substitute for passwords.

The project was led by School of Information professor John Chuang, along with Hamilton Nguyen, an undergraduate student in electrical

engineering and computer science; Charles Wang, a first-year I School MIMS student; and Benjamin Johnson, formerly a postdoctoral scholar at the I School. Chuang presented the team's findings this week at the 2013 Workshop on Usable Security at the Seventeenth International Conference on Financial Cryptography and Data Security in Okinawa, Japan.

Since the 1980s, computer scientists have proposed the use of biometrics for computer authentication. Systems requiring fingerprint scans, retina scans, or facial or voice recognition are far more secure than passwords, since fingerprints are hard to forget and harder to steal. But such systems are also slow, intrusive, and expensive. Biometric authentication has never gained wide acceptance; other than a few high-security settings, it remains more science fiction than science fact.

In recent years, security researchers have proposed using electroencephalograms (EEGs), or brainwave measurements, for computer authentication, replacing passwords with "pass-thoughts." But if other biometric systems have proven cumbersome and expensive, brainwave authentication has been even more so; no one wants to install invasive probes under their skull every time they check their email!

All that has changed, though, with recent developments in biosensor technologies.

New consumer-grade EEG devices

Traditional clinical EEGs typically employ dense arrays of electrodes to record 32, 64, 128, or 256 channels of EEG data. New consumer-grade headsets, on the other hand, use just a single dry-contact sensor resting against the user's forehead, providing a single-channel EEG signal from the brain's left frontal lobe.

The research team used the Neurosky MindSet, which connects to a computer wirelessly using Bluetooth and can be purchased for approximately $100. "Other than the EEG sensor, the headset is indistinguishable from a conventional Bluetooth headset for use with mobile phones, music players, and other computing devices," according to the researchers.

Professor John Chuang with the Neurosky MindSet brainwave sensor.

Will it work?

But will this new technology work for computer authentication? Is it secure, accurate, and reproducible enough to replace passwords? And more importantly, would people actually be willing to use it? The research project has preliminary answers to all three of these questions: yes, yes, and (probably) yes.

The team conducted a series of experiments to determine whether the single EEG channel provided high enough signal quality for accurate authentication. For authentication, the computer needs to be able to accurately and consistently distinguish your brainwave patterns from someone else's.

By selecting customized tasks for each user and then customizing each user's authentication thresholds, the team was able to reduce error rates to below 1%, comparable to the accuracy of more invasive multi-channel EEG signals.

But accuracy isn't enough. If a system is a pain, people will refuse to use it, no matter how accurate it is. The new generation of brainwave readers are much more user-friendly than before, but the team also focused on finding mental tasks that are enjoyable to users.

Seven mental tasks

The researchers measured participants' brainwaves while they performed seven different mental tasks. Users were asked to do two types of tasks: three where everyone performed the same task and four where users had individual secrets. For tasks of the first group, participants were asked to focus on their own breathing, imagine moving their finger up and down, or listen for an audio tone and then respond to the tone by focusing on a dot on a piece of paper.

In tasks where participants could choose a personalized secret, they were asked to imagine performing a repetitive motion from a sport of their choice (like swinging a golf club or kicking a ball), imagine singing a song of their choice, watch a series of on-screen images and silently count the objects that match a color of their choice, or choose their own thought and focus on that thought for ten seconds.

All seven of the tasks provided enough information to successfully authenticate the users. In fact, the personalized tasks weren't significantly more accurate than the tasks where everyone did the same thing.

The key to the success of a brainwave authentication system, then, is finding a mental task that users won't mind repeating on a daily basis. Researchers found that users would prefer to repeat tasks that are fairly easy but not too boring. Users' favorite tasks included counting objects of a specific color, imagining singing a song of their choice, or simply focusing on their own breathing. Several users found it difficult to imagine performing an action from their favorite sport: they found it unnatural to imagine the movement of their muscles without actually moving them. Similarly, when asked to choose their own "pass-thought," many users chose a thought that was complicated or difficult to repeat. And imagining moving a finger up and down was boring to the majority of participants.

Computer systems of the future

Computers that recognize you by your brainwaves might seem like a futuristic fantasy, but these experimental results suggest that that future is more realistic than we might have suspected. "We find that brainwave signals, even those collected using low-cost non-intrusive EEG sensors in everyday settings, can be used to authenticate users with high degrees of accuracy," the researchers conclude.

Rather than being limited to ultra high-end, high-security systems, brainwave-based authentication could end up being as cheap, accessible, and straightforward as thought itself.

Provided by University of California - Berkeley