Smithsonian.com

Using Your Heartbeat as a Password

Researchers have developed a way of turning the unique rhythms of your heart into a form of identification

While the peaks and valleys on people's ECGs may look identical to the untrained eye, they’re actually anything but. (Korawig/iStock)

By Emily Matchar
smithsonian.com
January 30, 2017

Your fingerprints. Your voice. The irises of your eyes. It seems that these days any part of your body can be used for biometric authentication—the process by which your physical characteristics are used to prove your identity, allowing you access to your cell phone, your bank account or your front door.

Now, you can add your heartbeat to the list. Researchers at the State University of New York-Binghamton have developed a way to use patients’ heartbeat patterns to protect their electronic medical records, opening the door to a new method of biometric authentication.

As wearable health devices that monitor everything from blood pressure to respiratory rate become more popular, there’s an increasing need to transmit health data electronically to doctor’s offices, explains Zhanpeng Jin, a professor in the department of electrical and computer engineering at Binghamton who is working with fellow professor Linke Guo and his student Pei Huang.

“During this process, the data transmission is vulnerable to cyber attacks or data breach, which may expose sensitive user’s [electronic health] data,” Jin says.

Since mobile health devices would have already collected a patient’s electrocardiogram (ECG)—a measurement of the heart’s electrical activity—the heartbeat data can simply be reused for security purposes. This has an advantage over many existing encryption techniques, Jin says, because it's far less computing-intensive and uses less energy, which is important when working with energy-limited devices like small wearable health monitors. Since the data has already been collected, it adds little extra cost to the process as well.

While the peaks and valleys on people's ECGs may look identical to the untrained eye, they’re actually anything but. Though your heartbeat speeds up and slows down, your ECG has a signature, much like a fingerprint, based on the structure of the heart itself.

“The existing studies on ECGs have proved that the ECGs are quite unique by nature among different individuals,” says Jin.

There's only one problem: these unique patterns are also changeable. A person’s ECG can change with physical activity, mental states (like stress), age and other factors.

“We are still working on better algorithms to mitigate those influences and make the ECG-based encryption more robust and resistant to those variabilities,” Jin says.

These issues would need to be overcome in order for ECGs to become a common biometric identifier like irises or fingerprints. But, Jin says, the technology is ready to be used as a secondary form of authentication. Since, by nature, an ECG only comes from a person who is alive, it could be used in tandem with another form of identification to both authenticate a person’s identity and prove that they’re living. Gruesome as its sounds, the scenario of a plucked-out eyeball or a severed finger being used to trick security scanners is something biometrics researchers must consider. An ECG as a secondary form of ID would remove that issue.

Jin’s previous work has involved using a person’s “brainprint”—the unique electrical activity of their brain—as a password, which also solves the “plucked-out eyeball” problem. In Jin's research, volunteers' brains responded differently when presented with different words. The brainwaves reflecting those differences could be used as passwords. But unlike heartbeats, brainwaves are not recorded by a personal health monitor, which makes them less useful in the case of protecting electronic health records.

As more and more doctors diagnose and treat patients remotely through telemedicine, Jin and his team hope their new technique can help secure vulnerable data. So one day soon, your heartbeat may join your fingerprints as yet another key in an ever-increasing number of locks.

About Emily Matchar

Emily Matchar is a writer based in Hong Kong and Chapel Hill, North Carolina. Her work has appeared in *The New York Times*, *The Atlantic*, *The New Republic*, *The Washington Post* and other publications. She is the author of .

|