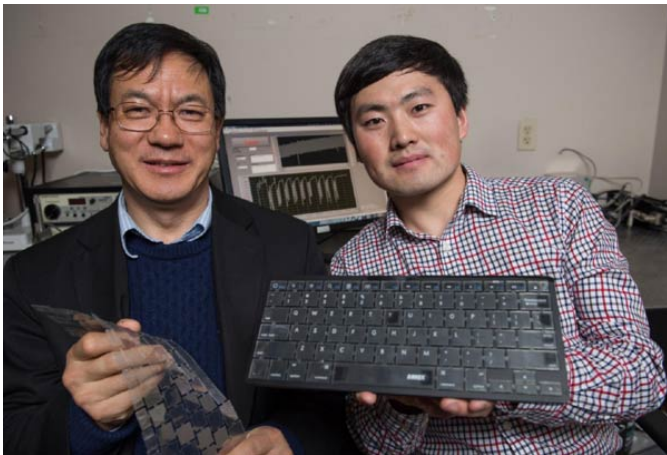


Further Security via Keyboard

Written by Marco Attard
29 January 2015

Georgia Institute of Technology researchers suggest the keyboard can provide a means of security beyond the simple password, by creating a biometric means of identification based on how the user presses the keys.



To do so, the keyboard records the force users apply to the keys, as well as the time taken between one keystroke and the next. Meanwhile the multi-layer plastic materials making the device allow it to harvest electricity from the users' fingertips (via effect called "contact electrification"), allowing it to either charge a small mobile device or power a wireless transmitter.

As researcher Zhong Lin Wang puts it, "our skin is dielectric and we have electrostatic charges in our fingers. Anything we touch can become charged."

However, the researchers insist the keyboard's most valuable asset is its means of user identification. Apparently the electrical currents generated by different people have a unique "fingerprint" of sorts when seen through signal analysis techniques, making for a "frictionless" level of extra security.

"This has the potential to be a new means for identifying users," Wang says. "With this system, a compromised password would not allow a cyber-criminal onto the computer. The way each person types even a few words is individual and unique."

Furthermore, the smart keyboard should be competitive with current keyboard, since it is made

Further Security via Keyboard

Written by Marco Attard
29 January 2015

out of inexpensive materials and actually pretty tough. According to the researchers it is even resistant to coffee, since liquids cannot hurt sheet plastic.

Go [Self-Powered Intelligent Keyboard Could Provide a New Layer of Security](#)