The New York Times

December 28, 2013

Reading Your Palm for Security's Sake

By ANNE EISENBERG

They aren't taking any chances at Barclays Bank in Britain. Stating an account number and other bona fides isn't enough to get to your money at the bank's wealth and investment management service. As an additional safeguard, a program analyzes customers' voices when they call in, to make sure they match a voice print on file.

At some A.T.M.'s in Japan, getting cash isn't simply a matter of entering a bank card and a password. The machine scans the vein pattern in a person's palm before issuing money.

And, since September, people have been using fingerprint sensors on their iPhone 5s to unlock their devices, or to shop at the iTunes store.

These are three examples of biometrics systems, which have long been the province of border control, military surveillance and national intelligence. Now they are rapidly moving into the consumer mainstream to unlock laptops and smartphones, or as a supplement to passwords at banks, hospitals and libraries.

But the technology also comes with a host of troublesome issues about its vulnerability to hacking and misuse.

The stakes can be high when inherently personal biometric data is hijacked, said Bruce Schneier, a security expert and author of "Liars and Outliers: Enabling the Trust That Society Needs to Thrive." "If someone steals your password, you can change it," he said. "But if someone steals your thumbprint, you can't get a new thumb. The failure modes are very different."

Despite these concerns, the technology is making its way onto the office desktop — and the laptop, too. A new Fujitsu laptop, the Celsius H730, released recently in Japan, can be ordered with a choice of biometrics: a fingerprint sensor or, for an additional $116, a palm scanner instead. To unlock the computer, you hold your palm over the sensor and the software checks your vein pattern to make sure you're the authorized user, said Joseph Dean, a Fujitsu spokesman.

Biometric devices can identify vein patterns in the finger, the back of the hand or the palm,

said Anil K. Jain, a professor and expert in biometrics at Michigan State University. The technology works quite well, he said, adding that "it's difficult to forge because the vascular patterns are inside the body." The veins are revealed by a harmless infrared light.

Palm scans are gaining the most traction in the vein-reading market, Professor Jain said. Identifying features include the thickness of the veins, and the angles and locations where they intersect. Some systems combine fingerprints and finger vein patterns.

A different biometric, voice printing, is offered by Nuance Communications to many customers, including Barclays. The voice print is based on about 100 characteristics, including pitch and accent, said Brett Beranek, a manager at Nuance.

Voice prints, even if stolen, will not lead to identity theft, he said. "If someone did compromise the database, there's nothing they could do with it," he said. "We are not storing people's voices, but characteristics of their voice."

Consumers shouldn't expect that biometric technologies will work flawlessly, Professor Jain said. They can be a good solution, balancing convenience with security. "But they are not foolproof," he said. "There could and will be situations where a person may be rejected or confused with someone else." For example, people could be barred by a fingerprint mismatch from access to their smartphones or bank accounts.

Fingerprint sensing will be the most popular biometric identifier for the next few years, said Alan Goode, author of a recent report on the mobile biometric security market and founder of Goode Intelligence in London. Apple's introduction of fingerprint scanning, and many other manufacturers' plans to offer similar services, "are going to make fingerprint sensors a common feature on mobile devices," he said. A majority will be used to unlock phones, but they will also increasingly be linked to mobile payment services.

Ram Ravi, an analyst who studies the global use of biometrics for Frost & Sullivan, agreed that fingerprints would be the leading biometric system for the next few years. "But palm reading is also developing into a huge market," he said. Iris- and facial-identification biometrics are growing rapidly as well.

Mr. Schneier, the security expert, said biometric solutions could be attractive in consumer goods so long as the processing occurs entirely on the device. (Apple has stated that all biometric processing on its iPhone occurs directly on the phone.)

When information is handled and stored on the chip, the only problem — certainly a maddening one — may be occasions when the device doesn't recognize people and won't let them in, he said.

But if the information is stored on a central server and unauthorized parties gain access to it, that is an entirely different problem.

"The centralized database is the scary part," Mr. Schneier said. "That's where the risk is. If it's hacked into, suddenly everyone's biometrics are stolen."

EMAIL: novelties@nytimes.com.