Technology Review - Skin Chips.
By David Cameron.

08/08/2002
MIT Technology Review

Researchers at Lumidigm may have discovered that identity, like beauty, is only skin deep. The Albuquerque, NM-based company claims that it can validate a person's ID with fingerprint-like accuracy by shining an infrared light into a small section of skin and measuring the reflection-a finding that may add innovative security features to portable devices, including an accurate trigger lock for a new electronic gun.

Human skin, with all of its dermal thickness and subcutaneous layers, has a unique signature from person to person, something that was virtually unknown until last decade when medical researchers began looking for non-invasive ways to monitor patients for factors like glucose levels and blood alcohol content. Researchers at Inlight Solutions, also based in Albuquerque, discovered that light passed through skin measured individual blood-sugar levels accurately, but accuracy diminished when they applied the same procedure across a range of people.

"We discovered that this was due to individual and unique characteristics of skin, multiple layers and different structures, which would affect the different wavelengths of light," says Robert Rowe, chief technology officer of Lumidigm and formerly of Inlight. "At that point we simply thought, shouldn't this work as a **biometric**?"

So Lumidigm developed a dime-sized system containing two electronic chips. The first chip illuminates a patch of skin with light emitting diodes, then collects the rays as they reflect back. The second chip processes the signal to create a "light print" signature, which it compares to a set of authorized signatures. (Small devices, like a gun, would normally require a database of less than a dozen authorized users.) The entire process of detection and authorization takes less than a second.

According to Rowe, the signature can provide about 1.75 million discernable combinations. To date, Lumidigm has tested about 1,000 people multiple times, yielding hundreds of thousands of measurements. The company tested pregnant women through each trimester and found subtle changes in body chemistry did not affect accuracy.

Unlike **biometrics** like fingerprinting and face recognition (see "Face Recognition", TR Nov 2001), light printing doesn't rely on image-processing. Instead, the device measures wavelengths of reflected light, which requires considerably less computing power.

"Other technologies need to take the original image and then crunch a lot of numbers to extract the features," says Rowe. "That kind of front-end processing puts a lot of constraints on the hardware." Lumidigm is betting that light printing's relatively low processor demands will make it the **biometric** of choice for portable devices like cell phones-and handguns. A Shot in the Light

In May 2001, Lumidigm entered into a partnership with Springfield MA-based Smith & Wesson. According to Kevin Foley, Smith & Wesson's VP of product engineering, light print technology is currently the only **biometric** they are seriously considering for their new "authorized-user-

only handgun" (popularly known as a "smart gun," a term that Foley disavows, claiming that a gun can never be any smarter than the person shooting it).Smith & Wesson is developing a weapon in which an electronic firing system-including a **biometric** authorization system-replaces the mechanical one. The company had considered fingerprint technology and rejected it, not only because of the computing power required but also because fingerprinting is less effective for some demographics. But with light print, "if you have skin, you can use it," says Foley. The technique also does not require exact placement of the skin, so, for example, gripping the handle of the gun in slightly different ways won't compromise accuracy. Foley believes that Smith & Wesson will complete an electronic-gun prototype incorporating Lumidigm's technology by early 2004.

Additionally, this gun would be virtually impossible to foil-a problem with many **biometric** technologies. According to Richard Norton, executive director of the Washington D.C.-based International **Biometric** Industry Association, "somebody's always trying to prove that you can spoof a particular system." Last May, a Japanese researcher stunned a **biometric** conference when he revealed that he had duped 11 different security systems by lifting and then applying finger prints with a substance similar to **gummy** bears.

"I think this was slightly overblown," Norton says, "but the point is that fingerprint technology cannot determine 'liveness.' You can't foil the Lumidigm system with fake or dead tissue."

Lumidigm's technology will never be able to identify someone out of a crowd in the same way that face-and to a lesser extent, gait-recognition-can (see Walk this Way, April 23, 2002). But as Rob Rowe and his team continue to fine-tune their technology, handguns and other firearms may soon be considerably less dangerous and accident prone.

Join a discussion about this story.

David Cameron is an associate editor at Technology Review.

http://www.technologyreview.com.