Review: Biometrics Technologies Measure Up (Part 1/3)

November 18 2005

(Part 1/3) Biometrics technologies have come a long way from a slow start in the early 80s. Now they can be found almost anywhere and soon, almost everywhere.

The basic reason is simple: biometrics uses body measurements to make positive personal identification without resorting to ID cards, passwords, PINs and other problematic security technologies. Your ID is your body – or a part of it, anyway. This makes ID counterfeiting much more difficult and also insures that ID doesn't get left behind – short or a very serious mishap, that is.

Various technologies have been used over the years and favorites are slowly emerging – along with a host of ethical and privacy issues.

Finger Print Scanners

The most common technology in use today by far is fingerprint scanning. This technology is used everywhere from top secret military installations to supermarkets, cell phones and time clocks.

Police departments have long used finger prints to track criminals because of their uniqueness – each finger print is different - making positive identification possible for any given individual.

Finger print readers use this uniqueness to generate a code – rarely do they actually use the full print for identification – based on areas where line print lines merge, fork or loop – like the round "whorl" you can find in the middle of all finger prints.

These devices work by scanning the print with a light source – either a laser or, more commonly, a LED (Light Emitting Diode) – on to a chip. The chip is either a CCD (Charged Couple Device – the same found in digital cameras) or the less expensive CMOS (Complementary Metal Oxide Semiconductor). Integrated circuits then generate the code to identify the print.

This code is stored in a database – either in a remote computer for cheaper USB models or in the device itself. When a person scans a print, this device compares the code generated by the print with one in the database to make a positive identification. These "print coding" algorithms are closely guarded secrets.

Price is probably the most attractive reason to use this technology. Securing your computer with a fingerprint reading mouse cost less than $100. Time clock systems start at around $500. This makes finger print

scanning one of the most affordable of all the biometrics technologies.

Like any relatively new technology there are problems: Finger prints can be covered by callus or worn smooth from heavy use -dirt can get into the print lines and skin can peel – all making print reading more difficult. Some users have problems with less expensive models due to the lack of a well defined center whorl in the middle – something the device needs to find the center and build a code for the print.

Since prints are converted to number codes it's possible for two prints to have the same code. This means each device is limited as to the number of prints it can read without giving a false positive. More money usually gets you models that manage more prints.

A new technology that scans the subsurface of your fingerprint – down five skin layers deep – works even when the print is scuffed or dirty. This technology is still new, however, so most fingerprint scanner systems also require a code or PIN of some type to for 100% positive identification.

Some fingerprint readers and their applications:

Biometric door lock – uses your fingerprint to open – runs off batteries and has key for emergencies

Biometric time and attendance system – works without a connection to a computer

Inexpensive print reader for PC security – comes with software – connects to computer via USB port

Print reader with magnetic card reader for extra security.

Hand Scanners

The second most popular device, which has actually been on the market and in use longer, is the hand reader. This device works by measuring the dimensions of your hand - normally the fingers.

Everybody has different length fingers. Even if you do run into someone with similar finger length, the combination of various finger lengths essentially eliminates the possibility of false identification. For example: your index finger might be the exact same length as somebody else's, but the chances that 2 of more of your fingers are the same length are vanishingly small.

Backlighting and lasers were used in early models but now electrical conduction is the method of choice to measure fingers – fewer technical problems, lower power requirements.

It works by measuring the electrical conduction of your hand. The user places his or her hand on a metal or plastic plate with two or more studs

protruding for finger alignment. A second later the device detects a small current at the point where the hand touches the plate. It then measures these areas and compares the findings to an internal database.

Unlike fingerprint scanners, hand readers do not require a computer – needed processing is done internally – although some can be connected to a computer for time clock applications via a standard network connection or serial cable.

Most units also have a keypad for entering in user data and ID numbers. Available models can store from 50 to over 500 individual hand measurements.

This technology also presents some false positives from time to time when users fail to correctly locate their hand on the scanner plate. Many require the keying of an ID code to make identification 100% positive.

These units tend to be very robust and ideal for users with dirty or worn hands like factories and assembly plants. Their self-contained nature means they can be installed virtually anywhere.

To Be Continued ... (in part 2: Eye Scanners, Face Recognition, and Pattern Recognition)