

Security is All in Vein

Alfred Poor, Contributing Editor

Security is All in Vein

by Alfred Poor, Contributing Editor



We've seen biometric scanning devices so often in movies and television shows that many people feel that they are commonplace. You even have a choice of notebook computers that have fingerprint scanners built in as a security device to limit access to the computer's contents.

Scanning a finger is certainly easier than remembering a secure password (in other words, something more robust than your spouse's birthday or "fluffycat"). But biometrics can have limitations. What if you cut your finger and it can't be scanned through the bandage? That's why many fingerprint systems have to set up more than one finger as an acceptable print. But then you have the problem of the sensor getting dirty or damaged from contact. And while retina scanners look cool in movies, they're expensive and not all that easy to use.

So Fujitsu's new PalmSecure biometric system provides an interesting alternative. It uses a non-contact sensor; just hold your hand about two inches above the scanning device and you'll get a quick approval or rejection.



(a) Visible ray image



(b) Infrared ray image



(c) Extracted vein pattern

How does it work?

This is where light comes into the story. The USB-powered scanning device bathes

Security is All in Vein

Published on Electronic Component News (<http://www.ecnmag.com>)

your hand in near-infrared light. The veins in your hand carry blood that has been depleted of oxygen back to the lungs to get recharged with more oxygen. The deoxygenated blood absorbs the near-IR light more than the rest of the tissue in your hand, creating a dark pattern of the veins.

Now, the veins in your hand consist of a complex system of branching vessels that get smaller and smaller. Imaging this network results in a complex pattern which — as the Fujitsu literature points out — makes “attempts to forge an identity are extremely difficult”. The literature goes on to make a point obliquely that could be a tad gruesome if it were stated more bluntly: “the sensor of the palm vein device can only recognize the pattern if the deoxidized hemoglobin is actively flowing within the individual’s veins.” Yes, this means that if you hack off someone’s hand, it won’t get you past the PalmSecure device.

The technology has been in use at some Japanese banks since 2004. According to Fujitsu, tests with 140,000 palms from 70,000 individuals resulting in a false acceptance rate of less than 0.00008% and a false rejection rate of 0.01%. That’s a pretty high level of security, and certainly a lot better than a PIN code.

Since the veins are inside your hand, they can’t be stolen like an ID badge or smart card. They can’t be covertly copied by photography, voice or video recording, or lifting fingerprints. And they provide you with a unique identifier; according to Fujitsu, even identical twins have individual vein patterns in their hands.

So why does the blood work so well for this scanning technology? It is because the hemoglobin actually changes color depending on the level of oxygen it carries. When you cut yourself, the blood that is exposed to air takes on oxygen immediately, and turns the familiar crimson red color. This means that it reflects light waves in the red range of the spectrum. Deplete the oxygen in the blood, however, and it turns dark blue; this is why your veins look blue where they come close to the skin, as with the backs of many people’s hands. So in this state, it absorbs light more effectively in the red spectrum.

When you light up a person’s palm with near IR light, most of the tissue will appear light colored, while the veins will be dark. This creates a good initial contrast that makes it easier to extract a map of the veins from the image.

This map then can be registered with the user and used for authentication. PalmSecure can be used in either of two ways. In the first, the vein map is stored in a company server, and scans are matched against this database to identify the user. Another method simply stores the map on a smart card that is accessed when the user’s hand is scanned. The system then simply has to verify that the vein map from the hand matches that stored on the card, and then can authorize the use of the card. Using one approach or the other, this technology can be suited for everything from ATMs to building or room access control.

A lot of smarts has gone into the development of the PalmSecure system, but you can find some interesting generalizations that can be useful for other applications. For example, the system relies on a simple situation that provides a binary choice of

Security is All in Vein

Published on Electronic Component News (<http://www.ecnmag.com>)

states: red or blue blood. Knowing that it has to be one or the other makes it easier to extract information from the subject (a hand in this case). You don't need to take a color photograph and perform complex analysis on it; the infrared light essentially creates a black and white image that makes the vein map stand out.

Too many times we look for complex solutions when there's a much simpler approach waiting to be used.

Source URL (retrieved on 04/28/2015 - 1:06pm):

http://www.ecnmag.com/articles/2009/01/security-all-vein?qt-video_of_the_day=0