

Business Solutions

*Information Security*

By MICHAEL TOTTY

February 13, 2006; Page R6

## More Security, at Your Fingertips

Is it time to ditch all those hard-to-remember passwords for something that's impossible to forget and hard to lose?

Passwords are the first line of defense in keeping intruders out of corporate computer systems, and companies are getting more stringent about keeping them safe. They're insisting that employees use "strong" passwords -- at least six characters, using a mix of numbers and letters -- and that they change them more frequently. But the sheer number of codes is a real headache for users and a productivity drain for companies, as computer-support staff face loads of calls about forgotten passwords.

"People can't remember log-in names. People can't remember passwords," says Jarad Carleton, an analyst with Frost & Sullivan, a technology consulting firm in Palo Alto, Calif. "There are just too many of them."

Companies have tried alternatives, such as smart cards or security tokens that generate a constantly changing string of numbers that can be used to replace set passwords. These work well enough, though they can be lost or left behind when traveling. So some companies are turning to a solution that's always at hand: fingerprints.

### **Body Language**

A person's "biometrics" -- unique physical characteristics such as fingerprints that can be used for identification -- have been used in high-security situations for a long time. San Francisco International Airport installed hand-geometry readers to control access for employees in the early 1990s. A hospital in Bavaria, Germany, uses iris-scanning technology to limit admission to its neonatal station.

But biometrics has been slow to make headway for day-to-day business uses. Part of the problem is that biometrics readers have been expensive -- fine for locking a few doors but too costly to place on every computer in an organization. Smaller and less-expensive sensors were available, but users complained they were unreliable.

In the past couple of years, though, fingerprint scanners and the necessary software have become cheaper and more reliable, and have begun showing up on desktop and notebook computers. So far, the technology is found mostly among leading adopters, like health-care and financial-services companies. But, security experts say, if they're used properly, fingerprint log-ons can be easier to use and more secure than passwords. Using fingerprints to verify a computer user's identity, Mr. Carleton says, "is a technology that is ready for prime time."

Lenovo Group Ltd., which last year bought the PC operations of International Business Machines Corp., says it has sold more than one million laptop computers with built-in fingerprint readers since it began offering the product in October 2004. Ten-year-old Digital Persona Inc., of Redwood City, Calif., boasts 25 million users of its fingerprint systems, which use a plug-in reader about the size of a small computer mouse.

To be sure, not everyone is convinced. Peter Schwartz, chairman of Global Business Network Inc., an Emeryville, Calif., consulting firm, says he disabled the fingerprint reader on his new Lenovo laptop after he couldn't sign in when trying to make a presentation before 300 people. "It's not ready for prime time," Mr. Schwartz says. (Lenovo says that you can expect to get falsely rejected only three times in 10,000, assuming that in some cases it might take three tries to log in successfully.)

What's more, these systems don't eliminate passwords entirely; they just fix it so you don't have to type them every time you log on. Users first create passwords for their computer and store them in one central management program. Then they set up the fingerprint system by sliding their fingers over an optical scanner - - either built-in or attached -- which converts the image into a unique mathematical formula that represents the fingerprint.

After that, every time users scan their fingerprint, the computer unlocks the password manager and the required password is entered automatically. Besides making sign-ins more convenient, fingerprint systems also make it possible to create much stronger passwords, with 20 or more random characters, that would otherwise be impossible to remember.

### **Lives on the Line**

As is often the case with technologies just beginning to break out, fingerprint readers are being rolled out in settings where they can have the biggest effect. Sisters of Mercy Health System, a Chesterfield, Mo., health-care organization, began testing fingerprint readers in the emergency department of one of its St. Louis medical centers in July 2005. It now has about 40 devices in the emergency department and another 40 in administrative offices.

In the emergency department, where several physicians and nurses share the same PC, it was too time-consuming for individual users to log on and off every time they needed to pull a patient record or other information. But that meant that records could be viewed by people who didn't have authorization -- a potential violation of a federal law that protects patients' medical information.

The fingerprint readers are used in combination with identification badges. When, say, a doctor approaches the station, the computer recognizes her badge and automatically logs her in, using a system put together by Sentillion Inc., of Andover, Mass. The doctor then verifies her identity using the fingerprint reader. If the doctor then leaves the computer, the machine senses this and automatically logs her out. What's more, if she left any files open on the screen, the machine will remember and open them automatically the next time she logs in.

Mick Murphy, the hospital system's chief technology officer, says that with the old system, it took almost five minutes to access a particular record, but that has been cut to about a minute. "It lets clinicians focus on patients" instead of computers, he says.

Another common use for fingerprint scanners is locking down portable devices, such as notebook computers and PDAs. Concentra Inc., a manager of occupational health services in Addison, Texas, last year began testing about 400 fingerprint-enabled laptops from Lenovo among its mobile case managers, and so far has found that the systems make logging in a lot faster and easier. Users can access the computer and any other protected programs just by sliding their finger over the built-in reader to unlock the required password. "For the people who use it, it's indispensable," says Laura Ciavola, Concentra's chief information officer.