apps
Is biometrics ready to bust out? NETWORK SECURITY: Update on biometrics.
ELLEN MESSMER

10/07/2002
Network World
24

No single network security technology arouses passionate debate like **biometrics**, which relies on authenticating identities by matching a person's body parts, voice or signature to grant access to computer resources or restricted building areas.

Proponents say authentication based on aspects of an individual's body - such as fingerprint matching or iris scanning - offers far better security than any based on re-usable passwords or hardware tokens that generate one-time passwords. "We've been doing large-scale ID systems for 12 years for [the Department of Defense] and the Department of State, and **biometrics** is a very compelling technology," says Tim Corcoran, senior systems engineer at Northrup Grumman's IT division.

"**Biometrics** is not ready for prime time," says Stephen Elky, security auditor at Software Performance Systems in Arlington, Va., which tested **biometrics** products under government contract.

But critics point out that **biometrics** can be expensive and invasive, and that none of the hundreds of **biometric** products on the market is infallible in pattern-matching a scanned body part to a **biometric** image. "It's all snake oil," scoffs Jim Kirby, network engineer at Wells-Dairy, pointing to a widely publicized experiment in Japan earlier this year that showed people could fool fingerprint scanners by using molded "**gummy** fingers" made of gelatin.

Biometrics believers

Despite the back and forth, **biometrics** continues to work its way into more environments.

A case in point is the U.S. government, which is poised to deploy **biometrics** on an unprecedented scale for improving security in the military, transportation industry and in border-crossing control. That could really give a boost to a market that has increased steadily, if not spectacularly - IDC analyst Charles Kolodgy says the market increased from $77 million in 2000 to $80 million last year and is expected to grow 15% to $92 million this year.

Northrop Grumman, which has worked with the U.S. Air Force and other parts of the Defense Department to install iris and fingerprint scanners, expects to see the U.S. government install hundreds of thousands or even millions of **biometric** products in years to come. The rollouts will be fueled in large part by mandates from Congress through the U.S. Patriot Act and the Bush administration through its homeland security efforts.

The State Department, the U.S. Customs Service and the Immigration and Naturalization Service all are being asked to collect fingerprints of foreign visitors and transportation workers, among others, to authenticate identities through the use of **biometrics**. These new systems will need to work with the FBI's Automated Fingerprint Identification System, Corcoran says.

Another user is the University of Missouri's School of Dentistry, which a year ago installed the SecuGen fingerprint scanner in 265 dental laboratory settings.

"Missouri law requires a signature from a practitioner to practice on a patient," says biomedical communications director Bill Marse. The dentistry school had moved to a system based on electronic records as part of a Year 2000 upgrade, and the school was interested in using **biometrics** for access to these electronic patient records and for a signature.

Student and faculty are now required to share a thumbprint, which is stored as a mathematical "hash" in a server on the university's Ethernet LAN so that it can be checked every time a student or faculty member accesses a patient's record. The fingerprint reader is built directly into the computer mouse.

Fingerprint scanning won out over retinal scanning, in part because at $200 per device it cost two to five times less, Marse says.

Biometrics holds a lot of appeal to hospitals seeking to carefully follow the federal government's Health Insurance Portability and Accountability Act regulations, which require authenticating user access to records.

Rich Rauscher, manager of technology architecture at Moffitt Cancer Center in Tampa, Fla., this year started using BioNetrix Systems' authentication management software to support fingerprint readers on about 1,000 desktops, providing nurses and other staff with access to clinical records.

Rauscher says he likes that BioNetrix also supports cornea scanners, face recognition and voice recognition, in addition to password-based authentication, in the event the hospital decides to make use of those technologies.

Not perfect

Even **biometrics** backers acknowledge the technology isn't perfect.

"We've had a few glitches," the University of Missouri's Marse says. "If part of the system isn't up, it creates a problem of phenomenal scale for us." When that occurs, the university shifts to paper backup.

But in general, the **biometrics**-based system has worked well and the university plans to expand use to include hand-held tablets, Marse says.

Another hospital, also using BioNetrix software, found fingerprint scanners to be ineffective for surgeons. They scrub their hands so thoroughly it makes it hard to read their fingerprints, says Gene Gretzer, a senior analyst at St. Luke's Episcopal Health System in Houston.

WorldCom steered clear of fingerprint scanning because fingerprints are so closely associated with criminal suspect bookings at police stations that employees and customers would see such scanning as invasive, says Tim Burke, manager of infrastructure services. Rather, WorldCom uses hand scanners to ensure only authorized parties access its 14 data centers.

Security experts generally prefer fingerprint **biometrics** to face, eye or hand geometry, to get a

pattern match. Facial recognition has only about an 85% success rate for matching, while fingerprints range close to 99% accuracy, says Richard Langley, an expert in identity technologies in TRW's public safety and transportation division.

Although a **biometric** fingerprint is unique, no person actually presses his finger the exact way twice onto a scanner. So software has to be designed carefully to prevent false rejections and false positives. That means **biometrics** often remains a highly customized application. It's often used in conjunction with passwords and smart cards as a back-up or double-check system.

The scalability of **biometrics** systems also is questioned. Even a supporter such as Northrop Grumman's Corcoran says "the reality is that performance is an issue" in large-scale rollouts.

James Wyman, director of the **biometrics** test lab at San Jose State University, which started doing testing back in the early days of the Clinton administration, adds: "A lot more research needs to be done on that."