



## **Biosecurity Comes of Age**

Retina, Hand, and Fingerprint Scanners Are Emerging as New Solutions to Access and Authentication Concerns.

By Matt Villano

Imagine a campus where a student enters a dorm room by waving a hand through an electronic hand scanner; where professors and teaching assistants log on to the intranet grading system with a password and electronic impressions of their fingerprints; where staff members gain access to accounts by allowing technology to "read" the unique characteristics of their retinas.

Imagine no further. Today, these biometric technologies are being used by a numbers of institutions that see their benefits over traditional smart cards.

While most schools are grappling with the question of using smart cards to eliminate keys and upgrade campus security, a select group of schools are addressing access and authentication concerns with leading-edge technologies that simply make sense: biometrics. From palm scanners to fingerprint scanners, retinal probes to voice identification devices, biometric technologies are beginning to enter the mainstream market on a large scale. Perhaps more impressively, in most cases, once schools get past a significant investment on the front end, biometric technologies also are much less expensive than most academic officials might think, notes Bill Spence, director of marketing for Recognition Systems (RSI), which makes fingerprint access control readers starting at \$800 ([www.handreader.com](http://www.handreader.com)).

Critics of the technology raise concerns about having users identified by personal, unchangeable characteristics, and argue that the very act of compiling physical identifiers is the penultimate invasion of privacy. Still, a growing number of schools are turning to the new technology to improve security and to eliminate the headaches created by lost or damaged plastic ID cards.

### **Biometrics 101**

Biometric technology uses unique biological properties to identify individual users in a confined group. Since no two humans have the same handprints, fingerprints, or retinal impressions, these are the characteristics that best lend themselves to be used as identifiers. Some devices also identify users based on voice, but because this characteristic varies widely and is not necessarily unique, it does not work as well. Put another way, the comedian Dana Carvey can make his voice sound like former President George Bush's, but when inspected by the micrometer, it's a good bet their fingerprints don't even come close.

Whatever type of physical characteristic a biometric device evaluates, when a user interacts with the device, the device captures an image, converts that image into as many as 100 points of data, and stores the resulting bits and bytes on a 9-kilobyte file that gets stored in a database. Every time a user interacts with the scanner, the scanner takes a reading and compares the data to data already on file. If this comparison yields a match, the device authenticates the user and instructs the electronic lock to grant him access; if the comparison fails to yield a match, the device rejects the user and access is denied.

"When you think about it, the data-matching concept behind biometric authentication is very similar to the concept behind password authentication," says Clain Anderson, director of marketing for wireless and security solutions at IBM in Research Triangle Park, NC ([www.ibm.com/us](http://www.ibm.com/us)). "The big difference is that anybody can type in a password, but your hand is yours, and no one is going to be able to copy that."

As Anderson explains, most biometric scanners store their data locally, performing the comparison there on-site, instantaneously. Some scanners, however, can be hooked to a campus network, capturing data on a user from an initial interaction, then sending that data to a central database that runs the comparison, grants or denies access, and returns a red- or green-light message back to the scanner itself. This latter approach is used by entities that wish to monitor which users are accessing a certain scanner, and is particularly popular among corporations that employ biometrics to keep tabs on who accesses a server room or other restricted areas. Not surprisingly, it also is one of the most common forms of biometrics used by the U.S. government.

### **The Leaders**

In the academic environment, this highly sophisticated application of biometric technology can be found in some of the 60 biometric scanners at the **University of Georgia**. Technologists here first invested in biometrics when most Trekkies only dreamed of it, way back in the 1970s. Those first systems--electronic hand scanners--were used at entrances to dining halls to verify that students who paid for meal plans were the same students that actually entered at mealtime. Today, the systems control access for 32,000 users to select facilities all over campus, from dining halls to recreational centers, dormitories to testing rooms. Fresh off a recent \$50,000 investment in new hand scanners from RSI, Georgia officials such as Donald Smith are eyeing an even bigger implementation sometime in the next two years.

"We use the devices to achieve a higher level of security," says Smith, who oversees biometrics in his job as program coordinator of the UGA Card Services department. "We tried to hook access and authentication into smart cards, but people on our campus were losing their smart cards all the time, so we figured [biometrics] just made more sense."

In the early days, Smith says cutting-edge biometric technology at UGA performed two-dimensional scans, inspecting the width and length of fingers as students waved their hands through the open mouth of the hand scanner. Today, though the technology works the same way, it is sophisticated enough to perform three-dimensional scans that measure the width, length, and depth of a user's entire hand, maximizing accuracy and minimizing false positives by improving the data with each scan. Inside, at entrances to facilities such as dining halls, testing centers, and laboratories, the school uses ID3DR hand scanners from RSI. Outside, at entrances to gyms and dormitories, the school uses the more durable ID3DRW model from the same vendor, a model designed to withstand elements such as rain and snow.

In total, UGA has spent \$150,000 on its biometrics program--\$2,000 for each of the indoor models and \$3,000 for every outdoor model, says Smith. Costs are greater for the latter because they require steel enclosures to protect them from the weather.

Technologists use identical devices at **San Diego State University (CA)**, where biometric scanners handle authentication and access for 27,000 users to the Aztec Recreation Center, the school's main gym. Before the scanners, SDSU users seeking access to the center had to wait in line to hand their ID cards to a staffer sitting at a desk, who would swipe the cards through a magnetic stripe reader, confirm authorization by matching a database record to a name on the card, and allow the users to pass. Today, the scanners sit inside turnstiles at the entrance, automating the authentication process and reducing the time users spend at the front door of the facility from minutes to seconds. Eric Huth, director of campus recreation, describes the resulting increase in customer service as "refreshing," and says he never expected the system to work so well.

"Lines to get in here used to be awful," says Huth, noting that the school still employs people to sit at the door, but their function now is to troubleshoot scanner hiccups. "Today, you're in the door and through the gates before you have time to even think about it."

Huth estimates that SDSU spent \$25,000 on its biometrics system. "We determined pay back was one-year salary for a part-timer. We saw it as an immediate win for us financially."

## **The Innovators**

Biometric implementations like the ones at SDSU and UGA are large-scale implementations at huge public schools; on the flip side, technologists at smaller institutions have incorporated biometric technologies into more vertical, niche solutions that impact no more than a handful of users at a time. At **Johnson & Wales University's Denver campus**, officials recently purchased HandKey devices from RSI to guard the main entrances on each of the school's three residence halls. In one of the residence halls, the Pulliam dorm, the school deployed eight additional HandKeys, two on each opposing wing of the four-story building. Students use these interior scanners to gain access to their individual rooms--after students authenticate by waving their hands through the scanner, the device unlocks all individual room doors in that particular hallway for up to 20 seconds, enabling students literally to walk right in.

J.D. Sawyer, the school's director of campus operations, concedes that the notion of opening all six of the individual room doors in a particular hallway at the same time isn't exactly the pinnacle of safety, but notes that the doors closest to the device relock after 10 seconds, minimizing the window of opportunity for anyone--authorized or not--to access those rooms. Sawyer adds that the hallway HandKey devices only grant passage to the 10 to 12 students living in that hall, restricting access to the point where an unauthorized user would never enter the hallway unaccompanied by someone who wasn't supposed to be around.

"In general, I think students feel safer with this access control system, and ultimately, the system is more convenient [than the keys and ID card solutions that we used in the past]," he says. "Even if the students don't realize [the benefits of the new system] right away, they will realize it the next time they lose their ID card or room key, [both of] which cost them \$75 to replace."

Some schools, however, aren't ready to abandon the ID card entirely. At the **University of Utah**, technologists have signed up for an application of biometric technology that combines the conventional applications of smart cards with innovative fingerprint scanning technology to deliver a multifactor authentication process. With one device, the V-Smart MIFARE solution from vendor Bioscrypt ([www.bioscrypt.com](http://www.bioscrypt.com)), this multifactor process controls access into certain facilities such as the campus networking room and the school's Animal Resource Center. Under the system, users seeking access to the facilities in question swipe their smart cards in front of a traditional short-wave radio frequency reader for initial authentication, then immediately apply their fingers to a fingerprint scanner for a secondary read.

The solutions at the University of Utah store information on about 50 users locally, comparing user information against a database off-line and on-site at the point of authentication. The systems only will grant access after users have passed both authentication tests--a nice feature, but one that potentially could cause some problems. If, for instance, a user forgets his smart card at home, the system will decline to grant the user access on the basis that he or she failed one of the two critical authentication tests. Dan Black, a technician with FutureTech ([www.futuretechinc.biz](http://www.futuretechinc.biz)), the reseller that implemented the solution, admits that this quirk of the system is a bit severe, but says that at the end of the day, double-factor authentication always is best because it's inherently safer to double-check a user's identity than to check it only once.

"In today's day and age, you can never be too safe," he says. "By checking both a card and a biometric, there's no question at all about who's getting past the front door, and that's enough to give anyone peace of mind."

## **The Pilots**

Multifactor solutions such as the one at the University of Utah are opening eyes elsewhere, too. At **Creighton University** (NE), technologists are piloting a program that incorporates passwords with fingerprint scanning for a dual-factor authentication process that would guard access to the student help desk. This program, which launched earlier this year, revolves around brand new Gateway m275 Tablet PCs ([www.gateway.com](http://www.gateway.com)) with plug-in USB fingerprint scanners from vendor DigitalPersona ([www.digitalpersona.com](http://www.digitalpersona.com)). When technical support representatives want to log on to the network, they

must type in a password, and submit their index finger for a scan. Software on the fingerprint scanner integrates with a Microsoft Active Directory server and authenticates the user against a local database. This information is then compared with data the server already has compiled from the password entry. If the two pieces of data match, the server grants access; if they do not, the server denies access and forces the user to try again.

Though Creighton is experimenting with plug-in scanners, Michael Allington, assistant director of student support, notes that the school also is considering an effort to replace all 300 of the computers in the school's public labs with new notebooks from the Gateway 450 Series that have built-in fingerprint scanning capabilities. According to Allington, replacing the computers would cost roughly \$30,000 up front, but the move greatly would reduce the threat of nefarious students or other evildoers stealing the school's plug-in scanners at \$100 a pop. What's more, he says, the new Gateway devices would simplify life for technical support workers themselves, eliminating the need for these individuals to tote around plug-in fingerprint scanners forever.

"These biometric devices could change everything for us," Allington says of the Gateway computers. "Right now, the big question is whether we're ready to make the kind of investment we'd have to make to do it right."

Administrators at **West Virginia University** find themselves faced with a similar dilemma. The school just completed a pilot program that introduced students to biometrics in the form of electronic hand scanners, supplied by Diebold ([www.diebold.com](http://www.diebold.com)). Beginning in the spring of 2003, residents of the institution's Borman North dormitory had the option of giving up the traditional ID card authentication procedure to test a new access control system based upon Diebold's new hand-scanning technology. The system worked much like those from RSI, storing user information locally and comparing data against it every time a student swiped his or her hand. In the end, says Amir Mohammadi, WVU's associate vice president for generated revenue, the overall acceptance rate among students was 4.1 out of 5.

Now, however, comes the hard part--deciding what to do next. Mohammadi says he was pleased enough with the pilot program to consider installing biometric technology on a widespread basis across campus. The problem is a lack of funding to make it happen in a timely fashion. Mohammadi estimates that a drive to purchase and install Diebold electronic hand scanners in all of the campus dorms and dining halls would cost approximately \$50,000, and that a push to integrate the devices into the campus network so they can communicate with each other could practically double that figure overnight. Until the school's funding situation changes, and until integrating the devices becomes easier and more cost-effective, Mohammadi says his solution to the problem is to try and convince Diebold to launch another pilot as soon as possible.

"Someone once said that the trouble with our times is that the future isn't what it used to be," he quips. "Thanks to the first pilot, we know what the future of access control technology will be. The rest is up to us."

### **The Future :**

Indeed, as Mohammadi implies, at a time when university budgets are getting smaller every year, cost and integration are two significant obstacles to the widespread adoption of biometrics over the next year. Other challenges to the technology's success include mixed performance ratings on certain devices, and a general concern about the privacy ethics of storing data about someone's identifying physical characteristics. The first concern, performance, is fairly straightforward--no matter how accurate a scanning device purports to be, most vendors have not figured out how to program devices to account for temporary changes in physical data, such as cuts, scabs, and in those cases that involve voice recognition, laryngitis.

The second concern, privacy, is a much more complicated issue. Ethically speaking, it is risky for schools to store highly sensitive personal information locally on devices that can be stolen or hacked--if any of this information were to be uncovered, the victimized school could be named defendant in countless negligence and identity theft cases. Technically, however, the data retrieved during a biometric scan is just that--data--and is used not to identify individuals, but to verify them. However these issues unfold, Spence of RSI predicts a day in the not-too-distant future when biometric technologies are as prevalent and reliable in the higher education environment as they are in science fiction movies.

"All signs point to biometrics as the next big thing, both in the academic world and in the business world at large," he says. "Mark my words--with technology like this, I guarantee you, we haven't seen anything yet."

**Matt Villano** is a freelance writer in Half Moon Bay, CA.