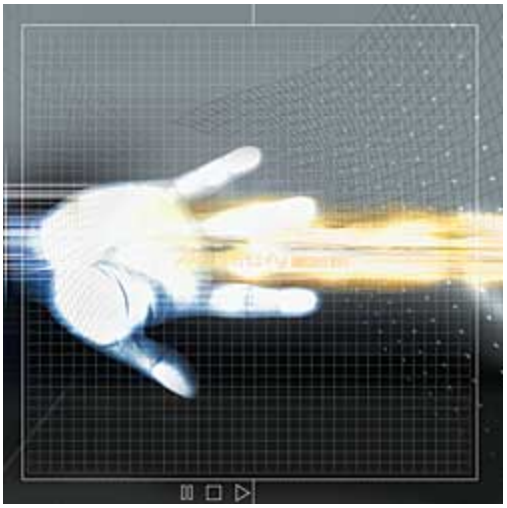
SECURITY PRODUCTS MAGAZINE
http://www.secprodonline.com/



A Fast Read

By Jon Mooney · August 2007

Biometric hand terminals provide quick verification of identity.

In some cases, companies implementing biometrics will initially encounter employee resistance, with the issues of privacy and hygiene taking center stage. This will invariably be the case if a union is involved and is looking for negotiating points.

However, when digging deeper into the concerns of employees, companies report the only real problem with the new biometric system is that it's new. Any concerns are eliminated if employees are educated upon announcement of the new system. After they have operated the biometric reader once or twice and see how easy it is to use, they prefer biometrics to alternative methods.

When installing any system, it is important that the ultimate users are educated. Nobody likes change. That is particularly true when it comes to biometrics, as there are several urban myths about biometrics that refuse to die, basically because they are brought up over and over again, especially by employee groups resisting change.

These concerns include the potential for invasion of privacy and hygiene, neither of which should be a concern, given that biometrics provide employees with increased security in access control applications and improved record-keeping in time and attendance applications.

Concerns Over Privacy

People confuse biometrics with the systems they see on TV crime shows. When considering privacy concerns associated with biometrics, an important distinction must be made between identification, a one-to-many match and authentication? one-to-one match. It's vital that users understand the difference.

A system designed to identify a person compares a biometric presented by a person against all biometric samples stored in the database. The system identifies the individual if the presented biometric matches one of the many samples on file. This is called a one-to-many match. This type of system is used by the police to identify criminals and used by governments to identify qualified recipients for benefit programs and in registration systems for voting or licensing drivers. This is the type of system seen on TV crime shows.

The authentication process, however, involves a one-to-one search. A live biometric presented by the user is compared to a stored sample, previously given by that individual during enrollment, and the match is confirmed. The hand geometry or fingerprint of the user is not stored in a database or on an ID card. Instead, a mathematical equation, or algorithm, is performed with points measured on the finger or hand. The template that results from this equation is all that is stored.

When the user presents an ID card or enters an assigned PIN, only that template is transmitted. When the employee presents his or her hand or finger, the reader runs the authentication process to determine if the template that is stored matches the biometric being presented. If there is a match, the person is authenticated.

To emphasize, the authentication of the person has been previously established. The matching of the live biometric to the established stored sample is all that is necessary to authenticate the individual as an eligible user. No search takes place to match a user's data to a central database. Palm prints or fingerprints of the "Law and Order" type are never analyzed.

And, unlike the biometric identification on television shows, authentication does not require the template be stored in a central database. This data can be stored on a smart card and kept in the possession of the individual.

Regarding privacy issues, most companies will find hand readers easier to sell to employees than fingerprint readers. After all, hand readers are never used in crime shows.

For instance, the Hilton Waterfront Beach Resort, a AAA four-diamond-rated waterfront beach resort that offers 290 rooms with luxurious accommodations situated in Huntington Beach, Calif., uses a biometric Ingersoll-Rand Recognition Systems HandPunch Reader to input time and attendance for tracking more than 330 employees. According to Romy Robb, payroll administrator at the Hilton Waterfront Beach Resort, when reviewing which biometric to use, the resort's staff did not accept fingerprint scans because the process was too similar to fingerprinting. The HandPunch reader was seen as much less intrusive. And, because it plugged right into the system, the HandPunch provided a smooth transition from the old magnetic ID card system.

Whether a hand geometry or fingerprint system is employed, an explanation of how the biometric authentication system works will calm fears.

Hygiene and Doorknobs

It is true that users frequently touch objects or surfaces that may hold risks of contamination. Initially, some hand geometry and fingerprint reader users show an opposition toward this technology, using hygiene concerns as a starting point for dispute. The bottom line is that a user is no more likely to pick up germs from a biometric reader than from other common objects or surfaces that people may touch, including doorknobs and countertops.

Nonetheless, to avoid a perception of hygiene problems, biometric units should be cleaned and disinfected more than a doorknob would be, and organizations should provide a dispenser with liquid hand sanitizer by each unit. Such measures help increase the confidence of users in the system.

Recognition Systems HandPunch Readers meets this problem head-on. It features an advanced plastic technology that reduces the spread of micro-organisms. A special silver-based material, using BioCote silver anti-microbial technology, is embedded into the plastics used to create the hand readers, providing a hygienic finish that resists bacterial degradation and reduces bacteria levels on the reader's surface. The active agents in BioCote products are incorporated during the manufacturing process and remain active for the life of the biometric reader.

Greatly Increased Security

In today's world, employees should welcome the increased security that biometrics provide. Too often, disgruntled employees rampage through the workplace. That's a good reason to implement biometric access control. The biometric provides additional safety for a workforce, as it will unlock and monitor doors, assuring only those authorized to enter are allowed in. Employees understand this.

Let employees know that hand geometry and fingerprint readers cover 80 percent of biometric access control and time and attendance applications. Both recognize people, not plastic, keeping the bad guys out. If there is already a card system, they provide higher security to vital entrances or doors.

Not only do biometrics help keep the bad guys out, hand geometry and fingerprint readers ensure the good guys gain access quickly and easily. After all, nobody forgets to bring hands or fingers to work.

For instance, West Virginia University's Student Recreation Center is using hand reader technology, in addition to the card swiping system already in place, to control access to the facility.

"The primary reason that we brought in this device was convenience for students," said Carolyn McDaniel, assistant director of Student Affairs Business Operations. "The students have said that they don't want to bring their card. It is one more thing for them to keep track of. The Rec Center is probably the place where cards are most often lost."

McDaniel said about five lost student ID cards are found by Rec Center employees every day, which prompted the switch to biometric access control. Students, faculty and staff interested in using the hand reader in place of the identification cards must enroll in the program. Once registered, Rec Center patrons no longer need ID cards to gain admittance. The biometric scanner lets them in.

Once it is installed, making sure the biometric works easily is key. At the 250-acre Owens Corning campus in Newark, Ohio, those seeking access to the manufacturing plant, as well as other facilities, must present their hands for a biometric scan to verify identity before being admitted. The biometric solution is integrated with an Identicard IDentiPASS System.

"We've had a positive response from our users," said Rodger Orr, IS professional. "I always double check a new enrollee's scan by entering that person's ID number and my own hand. Importantly, I can set an expiration date for contractors and salespeople.

"This system is especially efficient because multiple users with authorization can access the panel from their PCs over the computer network," Orr said. "For example, I was approached in the hallway recently by a vendor requesting hand geometry access to our building. I downloaded the software from the PC in my office, scanned the vendor's hand, keyed in his name and assigned an ID number on the spot. The entire process took only minutes."

More Accurate Time & Attendance
Hand readers also are used to record payroll hours quickly and accurately. Such biometric systems ensure that payroll information is transmitted correctly to the payroll department and that the exact time worked, including overtime, is recorded properly.

With a biometric system, the company eliminates the costs and mistakes inherent in manual data inputting. Among the costs and mistakes eliminated are those that can affect an employee's paycheck, Input errors can shortchange an employee's pay, wasting both the employee's and the employer's time in correcting the mistake, to say nothing of the frustration on the part of the employee.

Facing a new procedure, employees sometimes worry that they won't be able to use the units easily. What about a hand injury, for instance? Not to worry. Units such as the HandPunch are forgiving. Since it analyzes 90 different points to match the stored one-to-one template, a bandage on a finger will probably make little difference. However, if the bandage dramatically changes the shape of the hand, the organization will need to have a protocol to allow for these instances. Most importantly, any concerns about accuracy disappear after the first pay period when employees see that all times have been accurately processed.

Hays House Nursing Center in Nowata, Okla., uses a biometric HandPunch reader to input time and attendance for tracking its 100 employees.

"There was a lot of excitement around the hand reader when it was first installed. Employees liked it because all they had to do was enter their number and then present their hand. Previously, we had a huge rack for timecards, and it sometimes took a long time for employees to find their cards," said Charlie Lawson, nursing center administrator.

Concerns Over the Unknown
Employees resist biometric systems because they are unfamiliar, but employee concerns generally disappear after a brief system introduction. A personnel manager might say: "This new biometric reader uses the size and shape of the hand to verify an individual's identity. You punch in a short user ID code, and then the HandPunch looks at the length, width, thickness and surface area of your hand, identifying unique features from a projected image that resembles the shadow cast by your hand."

Following this up with a clear description of how biometric verification works from the very beginning demystifies the device and helps users feel at ease.

About the author

Jon Mooney
Jon Mooney is a 12-year veteran of Ingersoll Rand and is general manager of Ingersoll Rand Security Technologies' Biometric Business Unit.

SECURITY PRODUCTS MAGAZINE

For further info, please contact:
Central Time Clock, Inc.
5-23 50th Avenue
Long Island City, NY 11101
Ph#: 718-784-4900