attendance® ON DEMAND

Biometrics

Ending Time Theft and Controlling Security Access

Summary

Once the domain of science fiction, today's biometric technology offers advanced identification and verification for employees in every industry. Because biometric systems identify people through physical measurements of unique human characteristics or behavior, they thwart attempts of "buddy punching," a form of time fraud where one employee punches for another. Biometric systems do not require easily lost or stolen badges, or other identifying objects. Employee attendance verification is a major use of biometrics today.

Biometric Technology's Use Today

Biometric technology offers an easy, secure method to make highly accurate verifications of individuals. Using biometrics, an individual's identity can be verified using physical means by scanning the fingers, hands, eyes or face.

Because biometric information is difficult to duplicate, biometric verifications are already broadly used in airports, offices, amusement parks, manufacturing centers and hospitals where security is a primary issue. Not only does biometric technology eliminate the need to carry badges or other identification, it also prevents the use of forged tickets, badges, or passports. A biometric scan can provide security access to protected areas, punch an employee in at the start of the workday, or give a user access to a laptop computer.

The use of biometrics is increasing. Australia's Department of Foreign Affairs and Trade recently announced its intention to incorporate voice-recognition and eye-scanning technology in future passports.[i] And researchers at Purdue University are studying the viability of using fingerprint or iris scans to replace passwords, increasing consumer identity management and security.[ii]

How Biometric Technologies Work

Biometric technologies rely on unique, permanent, and scannable human characteristics that are exclusive to each individual. These characteristics remain constant over time and are reliably collected using a sensor.

Different biometric technologies use different aspects of the human anatomy. Finger readers measure the space between the forks of the ridges in the finger. Hand readers can measure the orientation of veins in the hand, or the shape, length, and width of the fingers. Eye readers measure the veins in the retina or the texture of the iris. Some biometric measurements can be taken in even more innovative ways. For example, the shape, acceleration and speed of a person's signature can be used for biometric identification.

Biometric identification typically undergoes a three-step process: enrollment, identification/verification and refinement.

attendance® ON DEMAND

1. **Enrollment:** A template for every individual is established by taking a number of measurements and saving them digitally. Templates are stored in a database associated with the device or in a smartcard given to the individual.
2. **a. Identification:** When the individual attempts to be identified by scanning a finger, hand, or eye, a biometric device compares the new scan to all available templates to find a match.
   or

b. Verification: An individual must first claim an identity using a login name, smartcard, or personal identification number. Then the device compares the new scan to a known template for the individual for verification.

3. **Refinement:** As the individual continues to use the technology, the template is continually adjusted and perfected for slight changes in the measured characteristics.

Ending Time Theft with Biometric Time Clocks

Biometric time clocks, used to record employee start and end times, are popular in organizations where security is an issue or where employees might falsely record time worked.

Because biometric technology is more costly than other forms of time clock identification (such as magnetic badges or personal identification numbers), it is important to evaluate the return on investment biometric devices provide based on two key benefits: eliminating buddy punching and establishing security access.

- **Eliminating buddy punching.** With buddy punching, an employee either types a tardy employee's PIN or swipes the employee's badge earlier than he/she arrives to work or after he/she leaves work. The organizational costs of this kind of time theft can be enormous. The company loses money a few minutes at a time compounded across departments and locations. Biometrics make it almost impossible for employees to defraud a time and attendance system.
- **Establishing security access**. In this case, the biometric system works as a security access monitor to grant or deny access to restricted areas. The cost of purchasing and maintaining magnetic or proximity identification cards, which do not prevent fraudulent access, can be eliminated.

Is Biometric Attendance Verification Right for Your Organization?

attendance® ON DEMAND

The following are criteria you can use to determine if biometric time clocks are right for your organization.

1. **Evaluate the need for authentication or identification.** A workplace with employee time fraud problems or a need to control security access benefit greatly from biometric time recorders. A workplace with no security concerns or hourly workers may not need biometrics to maintain accurate employee time and attendance records.

2. **Consider the cost/benefit ratio.** For smaller organizations, the cost of biometric equipment may be greater than gains from eliminating time theft. However, as biometric technology advances, the price is lowering, allowing more organizations to adopt it. Lower-cost biometric time clocks have begun entering the market, becoming an option for organizations of all sizes.

3. **Assess the compatibility of the biometric technology with the work environment.** It is essential that biometric readings be as accurate as possible. For this reason, the environment in which biometric sensors are used is crucial to ensure a good read of employee biometric characteristics. An environment that is too humid or dirty can obscure the fingerprint on a finger-reader platen (or reading surface), making it more difficult to correctly scan the finger. A noisy environment can disrupt the proper collection of voice data.

   Persons being scanned with the biometric device can also impact the suitability of that device. For example, a retinal scan requires that a person gaze into an eyepiece. Without cooperation, this type of scan could be difficult. Individuals with worn finger whorls and ridges, due to years of welding or other occupations, may not be able to successfully use a finger reader.

   In any environment, a small percentage of the population cannot use the biometric system. For example, 3% of people cannot use finger readers, so it is imperative that the device has an alternate method for interaction. For time recorders, this method usually involves the entry of a PIN and passcode instead of the biometric scanner.

4. **Be sensitive to the concerns of employees.** When considering the purchase of biometric time recorders, it is important to address the privacy concerns of employees. Explain that a finger or hand reader does not store or recognize employee fingerprints—it uses hand or finger measurements to create a template for the employee. These measurements are used only for internal authentication and security access. They cannot be used to recreate biometric data such as a person's actual fingerprint.

   Furthermore, employee privacy is enhanced with biometric time clocks. When an employee accesses benefit time balances using a biometric time clock, no other employee is privy to these records, increasing the security of personal information.

   Employees may also be concerned about the potential health impact of using the same finger or hand sensor that many other employees use. As-

attendance® ON DEMAND

sure employees that the sensor is not more used than a doorknob or ATM. Furthermore, antibacterial materials are being incorporated into time clock design. For instance, the Schlage HandPunch G-Series time clock uses a silver-based anti-microbial agent that inhibits the growth of bacteria, mold and fungi.

What Does the Future Hold for Biometrics in Time and Attendance?

The possibilities of biometrics for employee authentication are endless. Experts attest that biometric technology is likely to be used increasingly in transactions requiring identity authentication since it virtually eliminates the ability to duplicate biometric characteristics. In time and attendance, biometrics improve the ease-of-use and accuracy of timekeeping systems while bolstering corporate security and enhancing employee privacy.

About Attendance on Demand, Inc.

Attendance on Demand supports the labor management needs of thousands of companies and more than a half million employees across North America. Launched in 2006, Attendance on Demand is a rapidly deployed, cloud-based solution that minimizes a company's risk and technology investment while providing advanced features for securely managing labor data—calculating pay rules, scheduling employees, budgeting labor, and automating recordkeeping for labor law compliance. With standard uptime over the industry average of 99.995% and above average customer retention rates, Attendance on Demand removes the worry of maintaining expensive infrastructure. An extensive North American distribution network helps organizations use Attendance on Demand to reduce labor expenses and improve decision making.

attendance® ON DEMAND

To find out how Attendance on Demand can help your organization, call 800-465-9980 or visit www.attendanceondemand.com

[i] "Passport Biometric Technology To Be Given Boost." Financial Review.com. 25 Nov 2013. Web. Accessed 27 Nov 2013. <http://www.afr.com/p/national/passport_biometric_technology_to_h1NUaYVlPaYg6I9wanfrUJ>

[ii] "Biometrics Move On." Euronews.com. 25 Nov 2013. Web. Accessed 27 Nov 2013. <http://www.euronews.com/2013/11/25/biometrics-move-on/>

