



Ask The Expert – May 2007

This month's expert looks at biometrics and its real-world implementations.

By Skip Sampson



The word biometrics comes from ancient Greek words bios, meaning life, and metron, meaning measure. And life measure would be an apt description for the variety of technologies used to accurately identify people through voice, fingerprint or some other unique body characteristic.

To date, identities have been confirmed by two factors: what we have and what we know. What we have is comprised of cards or documents such as driver licenses, ID cards, passports or birth certificates. What we know typically consists of passwords or PINs. But as documents get counterfeited, passports are stolen and passwords are shared or forgotten, we can no longer validate an individual's identity with any accuracy. And as a result, security – buildings, finances, computer systems, even borders – is compromised.

To solve this challenge, identities are becoming more frequently confirmed by a third component: what we are. Biometric technology helps measure what we are.

Recent advances in microprocessors have helped increase accuracy and reduce the cost of biometric systems, bringing the systems within the reach of government facilities, banks, hospitals, colleges and universities – virtually anyplace that requires a higher level of security.

In a typical biometric system, a person's biometric measurement (a fingerprint, face or iris patterns) is scanned, this information is processed by a numerical algorithm and then stored in a database. Later, when that person attempts to enter a door or access a computer, he or she presents the selected biometric to a reader. The reader processes the information into a digital template. If the template matches the information in the database, access is granted.

One advantage of a biometric system is that it can free the user from having to remember PINs, usernames and passwords – all of which can be stolen or given others.

ISSUE: Biometrics seems to be a viable options of authentication. Which industry is most receptive to the technology?

SOLUTION: Private industry is catching on to biometrics, but the biggest user is – and for the foreseeable future will be – the federal government. HSPD-12 called for all 5 million federal employees and an additional 2 million contractors to carry identification cards, including embedded fingerprints, for access to federal buildings and IT networks. The deadline for program implementation was last fall. Due to the scope of the project, total implementation likely remains months away.

A common, interoperable system used to verify identity of individuals, both within and across agencies, is a significant step in enhancing security and reducing identity fraud.

The federal government also is looking at biometrics to help identify port workers and passport owners. Ultimately, methods and standards being set by federal agencies will come to be used by state and local governments and private industry.

Standards are critical to the successful implementation of biometric systems. To that end, a number of organizations, both public and private, are working to ensure that components from one biometric vendor will work with those from another provider. Industry standards also will make it easier for end users to compare factors, such as price and performance, when reviewing systems or components from rival vendors.

(Continued to next page)

This article originally appeared in the May 2007 issue of *Security Products*

Skip Sampson, CPP, is vice president of Indianapolis-based Koorsen Fire & Security. He has 20 years of experience in the security industry.



Ask The Expert – May 2007

This month's expert looks at biometrics and its real-world implementations.

By Skip Sampson



(Continued from previous page)

ISSUE: What are some biometric measurement techniques?

SOLUTION: Currently, a number of techniques are available for biometric measurement, including the analysis of the iris, retina, fingerprints, face, voice, hand geometry and vein patterns.

Fingerprints are by far the most commonly used biometric technique. But a test several years ago by a national standards laboratory in the United Kingdom found the most accurate measurement to be iris scanning. The iris scan system never accepted a false identity. The false rejection rate was lower than two percent on the first attempt and fell to less than 0.2 percent when the subject tried as many as three times to gain access.

And for those who argue that biometrics pose an invasion of privacy, a fingerprint or iris scan reveals far less about a person than other regularly collected identification data, such as phone numbers, addresses and credit card and Social Security numbers.

Biometric technology is no longer the technology of spy movies. It has arrived and will soon be used in one form or another as a safe, accurate means of identification.

READER QUESTION: I work with a small, but growing company. Our employees wear badges and we have access readers on all entrances. During an average day, we have 10 or more vendors moving about our offices. Currently, we have them sign in and fill out an adhesive name label, but we would like to have a better and more accurate record of who comes and goes. Do you have any suggestions?

SOLUTION: Paper guest books have been around for a very long time. They are easy to use and very inexpensive. Unfortunately, most companies find the data collected is usually incomplete, often difficult to read and impossible to analyze. And perhaps more importantly, confidential information about who has recently visited your facility is out in the open and readily available to anyone who wants to flip through the book's pages.

We have seen a recent trend at many organizations of all shapes and sizes to replace outdated paper logs and adhesive name labels with electronic visitor management systems.

These systems can improve security and help enforce a company's visitor policies and procedures. Visit times can be limited, and visitors can be associated with the company's host employee. Log books are eliminated and visitor privacy is maintained.

A scanner is used to provide positive identification for visitors, capturing information from a business card, driver's license, passport or other official credential. An inexpensive USB camera can photograph and capture the visitor's picture. Printed, professional-looking badges with pertinent visitor information, including visit expiration time and date, and clearance levels are printed.

The visitor management system software provides an audit trail and a utility can generate a variety of reports from the captured information. Watch lists can be generated to prevent visits from undesirable individuals.

Systems are available from manufacturers such as EasyLobby or Honeywell's LobbyWorks. The systems use standard, off-the-shelf PCs and printers while all peripherals are USB.

This article originally appeared in the May 2007 issue of *Security Products*

Skip Sampson, CPP, is vice president of Indianapolis-based Koorsen Fire & Security. He has 20 years of experience in the security industry.