Performance + usability + acceptance = Biometric security success

Biometrics is the science of using human characteristics—such as fingerprints—to identify an individual. Its roots are firmly planted in the late 19th century, when biometrics was used for identifying criminals and for personal identification on civil contracts.

Today biometric technology encompasses a wide variety of identification systems and an even broader array of applications.

It wasn't until the early 1970s that biometric technology was used outside of the law enforcement and government communities when hand recognition was used at the University of Georgia. According to Samir Tamer, Advanced Technology Leader – Disruptive Innovation at Allegion, the first hand readers were purely mechanical, using physical springs and other gears to identify a user's hand. The next step was an optical system that worked by shining a 1,000-watt light at a user's hand, followed by modern systems that used low-power LEDs and cameras to identify the individual.

“Today, we find that hand geometry is one of the most effective biometric technologies for access control,” says Tamer. “Hand geometry doesn't have to overcome environmental challenges, like dirt or too much light, and hand geometry doesn't seem as scary to most people as other types of biometric authentication.”

Although mainstream biometric technology is safe, there is a common fear of side effects or exposure to something dangerous through the process of physical identification. Additionally, privacy can be a concern from the user standpoint.

Similar concerns also dogged iris identification, which identifies a user from the unique pattern of his or her iris.

“In the past, people were always concerned when you talked about their eyes,” says Mohammed Murad, Vice President, Global Business Development and Sales at IrisID, an Allegion aptiQ Alliance partner. “But iris identification has nothing harmful in it. It's just a camera so there is virtually no risk to the user.”

Performance: An upgrade in peace of mind

As technology has improved and overall prices have dropped, biometric technology is becoming more accessible to businesses of all sizes. In many cases, biometrics is an add-on to an existing access control solution where there is a need for a very high level of security.

Tamer explains that many businesses still rely on proximity cards with 125 kHz and no encryption for access control. “You just hold it up and get in,” he says. “The level of security is actually quite low, but with a biometric system, you are more accurately aware of who's in the building than with other solutions.”

To help clients understand the quality of security provided by biometrics, Tamer refers to three levels:

1. Things you have.
2. Things you know.
3. Things you are.

Things you have are metal keys or proximity cards. These can be lost, stolen or duplicated without authorization. Things you know are passwords or PINs. These are hard to steal, but can be forgotten or intentionally shared. Things you are refers to biometrics—that is, identification based on a person's unique physical characteristics. These characteristics can't be duplicated. According to Tamer, “things you are” or biometric identification provides the highest level of security, especially when paired with another credential like a PIN, password or card. This is an ideal option for companies that require display of a smart card or badge for entry.

“Biometrics are an upgrade in peace of mind,” says Tamer. “This is because biometrics allow a level of personal identification that no other solution can match.”
Usability: An ideal solution for a demanding workplace
It would be easy to assume that biometric access control is used only by high-tech, high-security organizations like Apple, Citibank and Google. And that's partly true.

“Biometrics were initially implemented by national research labs and nuclear power plants to protect high-tech secrets and dangerous materials,” says Tamer.

But over time, biometric access control has also become extremely effective in demanding workplaces where the system needs to process thousands of people quickly and in less than ideal conditions.

He cites the ability of biometric systems to process people quickly and accurately. In some cases, verification takes as little as two seconds per person—which is critical in factories that need to process as many as 2,000 people per shift. Biometrics also can overcome environmental challenges like ambient dirt, cold temperatures, overly bright or overly dark lighting; as well as employees wearing masks, goggles or other eye protection. In these settings, a biometric reader that doesn’t have to be touched is important so iris readers are often the solution of choice. In other settings, hand geometry like that captured by the Schlage HandKey, can be used to not only identify the user, but also track time and attendance.

Acceptance: Educating the customer makes the difference
Both Tamer and Murad agree that the biggest barrier to selling biometric technology is educating the customer. One way IrisID educates its customers is by helping them understand the return on investment. Biometric systems have fewer incidents of false acceptance, less re-enrollment of users because it didn't work the first time, and they don't require a credential investment to deliver accuracy. That means the cost is much more reasonable over the life cycle of the solution.

Murad points out that another challenge is helping people feel confident that they are choosing a solution that will stand the test of time.

“We encourage our customers to look at who is producing the product, how long that company has been around, and what they offer,” he says. “What is their life cycle of producing new technologies and what happens when they do this? Do they upset the integration or do they integrate smoothly into a legacy system? These are important issues to consider.”

Tamer says that Allegion is helping its integrators with these issues by investing in open platform security products that integrate with technology from many companies.

“The customer is looking for reliability, safety and physical durability, all of which Allegion can provide. And they are also looking for high-tech, advanced solutions, which we and aptiQ partners like IrisID provide,” says Tamer.

To learn more about biometric technologies available through Allegion and the aptiQ Alliance, visit allegion.com. To learn more about IrisID, visit irisid.com.

Learn more by calling 877-929-4350 or contacting an Allegion spec writer.